НАЦІОНАЛЬНИЙ СТАНДАРТ УКРАЇНИ

Атомні електростанції

ІНФОРМАЦІЙНІ ТА КЕРІВНІ СИСТЕМИ, ВАЖЛИВІ ДЛЯ БЕЗПЕКИ

Загальні вимоги до систем

(IEC 61513:2001, IDT)

ДСТУ IEC 61513:2009

Видання офіційне

БЗ № 2–2010/251

Київ
ДЕРЖСПОЖИВСТАНДАРТ УКРАЇНИ
2014

ПЕРЕДМОВА

1 ВНЕСЕНО: Технічний комітет стандартизації «Матеріали та прилади для сцинтиляційної техніки та техніки, пов'язаної з вимірюванням іонізувальних випромінень» (ТК 99)

ПЕРЕКЛАД І НАУКОВО-ТЕХНІЧНЕ РЕДАГУВАННЯ: **В. Любинський; Ю. Даниленко; Н. Молчанова,** канд. техн. наук (науковий керівник); **Ю. Розен; М. Ястребенецький,** д-р техн. наук; **О. Клевцов,** канд. техн. наук

2 НАДАНО ЧИННОСТІ: наказ Держспоживстандарту України від 30 грудня 2009 р. № 485 з 2012–01–01

3 Національний стандарт відповідає IEC 61513:2001 Nuclear power plants — Instrumentation and control systems important to safety — General requirements for systems (Атомні електростанції. Інформаційні та керівні системи, важливі для безпеки. Загальні вимоги до систем)

Ступінь відповідності — ідентичний (IDT)
Переклад з англійської (en)

4 УВЕДЕНО ВПЕРШЕ

Право власності на цей документ належить державі.
Відтворювати, тиражувати та розповсюджувати його повністю або частково на будь-яких носіях інформації без офіційного дозволу заборонено.
Стосовно врегулювання прав власності треба звертатися до Держспоживстандарту України

Держспоживстандарт України, 2014

ЗМІСТ

НАЦІОНАЛЬНИЙ ВСТУП

Цей стандарт є переклад IEC 61513:2001 Nuclear power plants — Instrumentation and control systems important to safety — General requirements for systems (Атомні електростанції. Інформаційні та керівні системи, важливі для безпеки. Загальні вимоги до систем).

Технічний комітет, відповідальний за цей стандарт, — ТК 99 «Матеріали та прилади для сцинтиляційної техніки та техніки, пов'язаної з вимірюванням іонізувальних випромінень».

Стандарт містить вимоги, які відповідають чинному законодавству України.

До стандарту внесено такі редакційні зміни:

— структурні елементи цього стандарту: «Титульний аркуш», «Передмова», «Національний вступ», першу сторінку, «Терміни та визначення понять» і «Бібліографічні дані» — оформлено згідно з вимогами національної стандартизації України;

— слова «Цей міжнародний стандарт» замінено на «Цей стандарт»;

— із «Передмови» до IEC 61513:2001 у цей «Національний вступ» узято те, що безпосередньо стосується цього стандарту;

— у розділі 2 наведено «Національне пояснення», виділене в тексті рамкою;

— долучено додаток НА, зважаючи на інтереси користувачів.

У цьому стандарті використано терміни, установлені в ДСТУ 1.1: вимога, міжнародний стандарт, настанова, національний стандарт, нормативний документ, об'єкт стандартизації, основоположний стандарт, перевидання, положення, поправка, проект стандарту, регіональний стандарт, стандарт, стандарт загальних технічних умов, стандарт на методи випробовування, стандарт на послугу, стандарт на продукцію, стандарт на процес, стандартизація, технічні умови.

IEC 60880, IEC 60780, IEC 61000-4-1, IEC 61069-1, IEC 61226 та ISO 9001, на які є посилання в цьому стандарті, прийнято в Україні як національні. Цей перелік наведено в додатку НА. Решту стандартів в Україні не прийнято і чинних документів натомість немає.

Копії нормативних документів, на які є посилання в цьому стандарті, можна замовити в Головному фонді нормативних документів.

ВСТУП до IEC 61513:2001

Цей стандарт установлює вимоги до контрольно-вимірювальних і керівних систем (КВК-системи) й устаткування, які використовують для виконання функцій, важливих для безпеки атомних електростанцій (АЕС).

Стандарт підкреслює взаємозв'язок між:

— цілями безпеки АЕС і вимогами до загальної архітектури КВК-систем, важливих для безпеки;

— загальною архітектурою КВК-систем і вимогами до конкретних систем, важливих для безпеки.

Під час розроблення цього стандарту використано стандарти IEC та ISO, серія видань із безпеки МАГАТЕ й інші узгоджені документи, у першу чергу:

a) Стандарти IEC для ядерного сектору

Цей стандарт має посилання на інші стандарти IEC для ядерної техніки, зокрема з питань, пов'язаних із кваліфікацією, проектуванням основного щита керування, категоризацією функцій та класифікацією систем (див. 3.4 та 3.6) і мультиплексуванням.

Під час розглядання комп'ютерних систем класу 1 (див. 5.1.2.1 та додаток B) цей стандарт треба використовувати спільно з IEC 60880, IEC 60880-2 та IEC 60987 для того, щоб забезпечити повноту системних вимог до аспектів програмного забезпечення і технічних засобів;

b) Інші міжнародні стандарти

Для цього стандарту прийнято формат викладення, подібний до базової публікації з безпеки IEC 61508, що охоплює загальний життєвий цикл безпеки та життєвий цикл системи. Стандарт також забезпечує трактування загальних вимог IEC 61508, частин 1, 2 та 4, для застосування в ядерному секторі. Відповідність цьому стандарту забезпечує узгодженість із вимогами IEC 61508, витлумаченими для ядерної промисловості.

У цьому стандарті є посилання на стандарти ISO з питань забезпечення якості.

c) Серія документів із безпеки МАГАТЕ.

Цей стандарт розроблено для узгодженості з принципами й основними аспектами безпеки, які містяться в Положенні МАГАТЕ з безпеки атомних електростанцій та настановах МАГАТЕ з безпеки. Дійсно, документи МАГАТЕ застосовні до всіх стандартів Технічного комітету 45 з вимірювання та управління. Термінологію та визначення, вжиті в цьому стандарті, узгоджено з термінологією та визначеннями, які використовує МАГАТЕ (див. примітку).

Примітка. Відповідно до «Угоди співробітництва з питань загальної зацікавленості», травень 1981 р.

Цей стандарт має посилання на IAEA 50-C-QA (Rev. 1) із питань, пов'язаних із забезпеченням якості.

НАЦІОНАЛЬНИЙ СТАНДАРТ УКРАЇНИ

АТОМНІ ЕЛЕКТРОСТАНЦІЇ

ІНФОРМАЦІЙНІ ТА КЕРІВНІ СИСТЕМИ, ВАЖЛИВІ ДЛЯ БЕЗПЕКИ

Загальні вимоги до систем

АТОМНЫЕ ЭЛЕКТРОСТАНЦИИ

ИНФОРМАЦИОННЫЕ И УПРАВЛЯЮЩИЕ СИСТЕМЫ, ВАЖНЫЕ ДЛЯ БЕЗОПАСНОСТИ

Общие требования к системам

NUCLEAR POWER PLANTS

INSTRUMENTATION AND CONTROL FOR SYSTEMS IMPORTANT TO SAFETY

General requirements for systems

Чинний від 2012–01–01

1 СФЕРА ЗАСТОСУВАННЯ

1.1 Загальні положення

Цей стандарт поширюється на КВК-системи, важливі для безпеки, які можна реалізувати застосовуючи традиційне устаткування з жорстким зв'язком, комп'ютерне устаткування (КУ) або використовуючи комбінації обох цих видів. Цей стандарт передбачає вимоги та рекомендації (див. примітку) до загальної архітектури КВК-системи, яка може містити будь-яку чи обидві технології.

Примітка. Зазвичай термін «вимоги» використовують як загальний термін, що охоплює як вимоги, так і рекомендації. Різниця виявляється на рівні конкретних положень, де вимоги виражено словом «повинен», а рекомендації — «може».

Цей стандарт підкреслює потребу повних та точних вимог, отриманих із цілей безпеки станції, як попередньої умови для створення всеосяжних вимог до загальної архітектури КВК-систем й окремих систем, важливих для безпеки.

Цей стандарт установлює концепцію життєвого циклу безпеки для загальної архітектури КВК-системи та життєвого циклу безпеки індивідуальних систем. Життєві цикли, розглянуті в цьому стандарті та похідні від нього, не є унікальними. За умови досягнення викладених у цьому стандарті цілей можна дотримувати інші життєві цикли.

1.2 Застосування: нові та наявні електростанції

Цей стандарт застосовують до КВК-систем нових атомних електростанцій, а також для модернізації та реконструкції КВК-систем наявних електростанцій.

Для наявних станцій можна застосовувати тільки скорочену низку вимог, які визначають на початковій стадії проектування.

Видання офіційне

1.3 Структура

На рисунку 1 зображено загальну структуру цього стандарту з його нормативними розділами:

— у розділі 5 викладено загальну архітектуру КВК-систем, важливих для безпеки:

— визначено вимоги до функцій КВК та пов'язаних із ними систем й устаткування (КВК ФСБ), отриманих з аналізу безпеки АЕС, категоризації функцій КВК, плану розміщення й аспектів функціювання електростанції;

— побудова загальної архітектури КВК, поділ на низку систем та розподіл функцій КВК між системами. ідентифіковано проектні критерії, разом із тими, що забезпечують глибокоешелонований захист і мінімізують можливість відмови за загальною причиною (ВЗП);

— планування загальної архітектури КВК-систем;

— у розділі 6 викладено вимоги до індивідуальних КВК-систем, важливих для безпеки, зокрема вимоги до комп'ютерних систем;

— у розділах 7 та 8 викладено загальну інтеграцію, пусконалогоджувальних робіт, експлуатацію та технічне обслуговування КВК-систем;

— у додатку А зазначено взаємодію між принципами безпеки МАГАТЕ та базовими принципами безпеки, ужитими в цьому стандарті;

— додаток В містить інформацію стосовно принципів категоризації/класифікації;

— додаток С надає приклади чутливості КВК до ВЗП;

— додаток D надає відомості з відповідності цього стандарту частинам 1, 2 та 4 IEC 61508. У цьому додатку наведено основні вимоги IEC 61508, які надають змогу переконатися в тому, що проблеми безпеки освітлено повною мірою, також розглянуто використання загальних термінів та надано пояснення причини вибору різних або додаткових методів чи термінів.

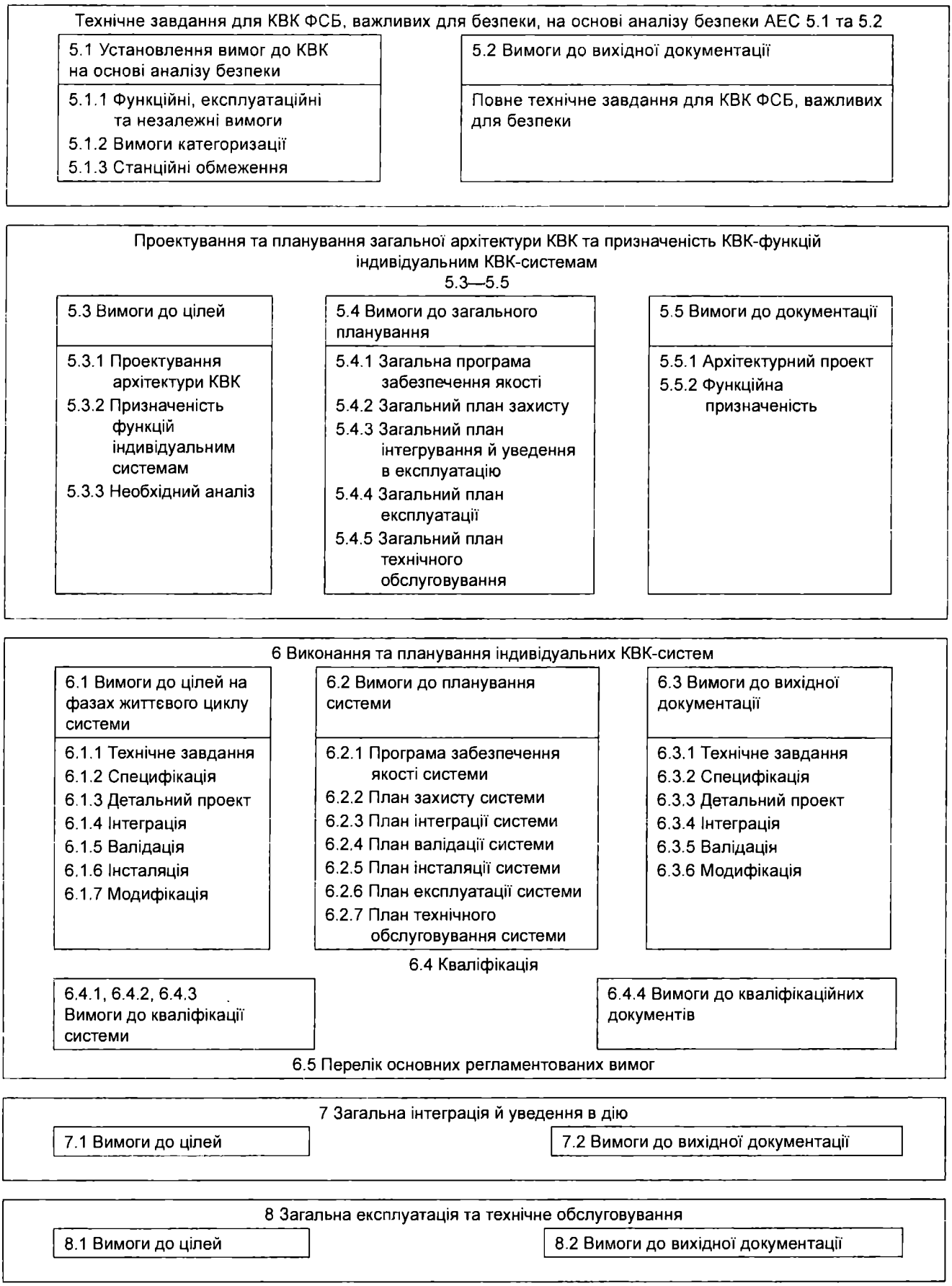


Рисунок 1 — Загальна структура цього стандарту

2 НОРМАТИВНІ ПОСИЛАННЯ

У наведених нижче нормативних документах зазначено положення, які через посилання в цьому тексті становлять положення цього стандарту. У разі датованих посилань пізніші зміни до будь-якого з цих видань або їхній перегляд не застосовують. Однак учасникам угод, базованих на цьому стандарті, рекомендовано застосовувати останнє видання нормативних документів, зазначених нижче. У разі недатованих посилань треба користуватися останнім виданням наведених документів. Члени ISO та IEC упорядковують каталоги чинних міжнародних стандартів.

IEC 60709:1981 Separation within the reactor protection system

IEC 60780:1998 Nuclear power plants — Electrical equipment of the safety system — Qualification

IEC 60880:1986 Software for computers in the safety systems of nuclear power stations

IEC 60880-2:2000 Software for computers important to safety for nuclear power plants — Part 2: Software aspects of defense against common cause failures, use of software tools and of pre-developed software

IEC 60964:1989 Design for control rooms of nuclear power plants

IEC 60965:1989 Supplementary control points for reactor shutdown without access to main control room

IEC 60987:1989 Programmed digital computers important to safety for nuclear power stations

IEC 61000-4-1:2000 Electromagnetic compatibility (EMC) — Part 4-1: Testing and measurement techniques — Overview of IEC 61000-4 series

IEC 61000-4-2:1995 Electromagnetic compatibility (EMC) — Part 4: Testing and measurement techniques — Section 2: Electrostatic discharge immunity test. Basic EMC Publication

IEC 61000-4-3:1995 Electromagnetic compatibility (EMC) — Part 4: Testing and measurement techniques — Section 3: Radiated, radio-frequency, electromagnetic field immunity test

IEC 61000-4-4:1995 Electromagnetic compatibility (EMC) — Part 4: Testing and measurement techniques — Section 4: Electrical fast transient/burst immunity test. Basic EMC Publication

IEC 61000-4-5:1995 Electromagnetic compatibility (EMC) — Part 4: Testing and measurement techniques — Section 5: Surge immunity test

IEC 61000-4-6:1996 Electromagnetic compatibility (EMC) — Part 4: Testing and measurement techniques — Section 6: Immunity to conducted disturbances, induced by radio-frequency fields

IEC 61069-1:1991 Industrial-process measurement and control — Evaluation of system properties for the purpose of system assessment — Part 1: General

IEC 61226:1993 Nuclear power plants — Instrumentation and control systems important for safety — Classification

IEC 61500:1996 Nuclear power plants — Instrumentation and control systems important for safety — Functional requirements for multiplexed data transmission

IEC 61508-1:1998 Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 1: General requirements

IEC 61508-2:2000 Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 2: Requirements for electrical/electronic/ programmable electronic safety-related systems

IEC 61508-4:1998 Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations

ISO/IEC 12207:1995 Information technology — Software life cycle processes

ISO 8402:1994 Quality management and quality assurance — Vocabulary

ISO 9000-3:1997 Quality management and quality assurance standards — Part 3: Guidelines for the application of ISO 9001:1994 to the development, supply, installation and maintenance of computer software

ISO 9001:1994 Quality system — Model for quality assurance in design, development, production, installation and servicing

IAEA Safety Series No. 50-C-D (Rev.1):1998 Code on the Safety of NPPs: Design

IAEA Safety Series No. 50-C-QA (Rev.1):1998 Code on the Safety of NPPs: Quality assurance

IAEA Safety Series No. 50-SG-D1:1998 Safety functions and Component Classification for BWR, PWR and PTR — A Safety Guide

IAEA Safety Series No. 50-SG-D3:1980 Protection system and related features in NPPs — A Safety Guide

IAEA Safety Series No. 50-SG-D8:1984 Safety-Related Instrumentation and Control Systems for NPPs — A Safety Guide

IAEA Safety Series No. 50-SG-D11:1986 General Design Safety Principles for NPPs — A Safety Guide

IAEA Safety Series No. 50-SG-D11:1986 Safety series 75-INSAG-3:1988, Basic Safety Principles for NPPs.

НАЦІОНАЛЬНЕ ПОЯСНЕННЯ

IEC 60709:1981 Розподіл у системі захисту реактора

IEC 60780:1998 Атомні електростанції. Електричне устаткування системи безпеки. Кваліфікація

IEC 60880:1986 Програмне забезпечення комп'ютерів у системі безпеки атомних електростанцій

IEC 60880-2:2000 Програмне забезпечення комп'ютерів, важливих для безпеки атомних електростанцій. Частина 2. Програмні аспекти забезпечення засобів захисту від відмов із загальних причин, використання програмних засобів і раніше розробленого програмного забезпечення

IEC 60964:1989 Проектування щитів керування атомних електростанцій

IEC 60965:1989 Додаткові пункти управління зупиненням реактора без доступу до головного щита керування

IEC 60987:1989 Програмовані цифрові комп'ютери, важливі для безпеки атомних електростанцій

IEC 61000-4-1:2000 Електромагнітна сумісність (EMC). Частина 4-1. Випробування та методи вимірювання. Огляд серії стандартів IEC 61000-4

IEC 61000-4-2:1995 Електромагнітна сумісність (EMC). Частина 4. Випробування та методи вимірювання. Розділ 2. Випробування стійкості до електростатичних розрядів. Базова публікація з EMC

IEC 61000-4-3:1995 Електромагнітна сумісність (EMC). Частина 4. Випробування та методи вимірювання. Розділ 3. Випробування стійкості до випромінювання, радіочастот, електромагнітного поля

IEC 61000-4-4:1995 Електромагнітна сумісність (EMC). Частина 4. Випробування та методи вимірювання. Розділ 4. Випробування стійкості до швидких перехідних процесів і сплесків. Базова публікація з EMC

IEC 61000-4-5:1995 Електромагнітна сумісність (EMC). Частина 4. Випробування та методи вимірювання. Розділ 5. Випробування стійкості до сплесків напруги

IEC 61000-4-6:1996 Електромагнітна сумісність (EMC). Частина 4. Випробування та методи вимірювання. Розділ 6. Стійкість до перешкод, наведених радіочастотними полями

IEC 61069-1:1991 Вимірювання та керування промисловими процесами. Визначення властивостей системи для її оцінення. Частина 1. Загальні аспекти та методологія

IEC 61226:1993 Атомні електростанції. Інформаційні та керівні системи, важливі для безпеки. Класифікація

IEC 61500:1996 Атомні електростанції. Інформаційні та керівні системи, важливі для безпеки. Функційні вимоги для мультиплексного передання даних

IEC 61508-1:1998 Функційна безпека електричних/електронних програмованих електронних систем, пов'язаних з безпекою. Частина 1. Загальні вимоги

IEC 61508-2:2000 Функційна безпека електричних/електронних програмованих систем, пов'язаних із безпекою. Частина 2. Вимоги до електричних/електронних програмованих електронних систем, пов'язаних із безпекою

IEC 61508-4:1998 Функційна безпека електричних/електронних програмованих електронних систем, пов'язаних із безпекою. Частина 4. Визначення та скорочення

ISO/IEC 12207:1995 Інформаційна технологія. Процеси життєвого циклу програмного забезпечення

ISO 8402:1994 Управління якістю та гарантія якості. Словник

ISO 9000-3:1997 Стандарти з управління та забезпечення якості. Частина 3. Настанова з використання ISO 9001:1994 під час розробляння, постачання, інсталяції та технічного обслуговування програмного забезпечення комп'ютерів

ISO 9001:1994 Система якості. Модель забезпечення якості під час проектування, розробляння, виробництва, інсталяції та обслуговування

Серія з безпеки IAEA № 50-C-D (Публікація. 1):1988. Збірник правил безпеки атомних електростанцій. Проектування

Серія з безпеки IAEA № 50-C-QA (Публікація. 1):1988. Збірник правил безпеки атомних електростанцій. Забезпечення якості

Серія з безпеки IAEA № 50-SG-D1:1979. Класифікація функцій безпеки та компонентів для BWR, PWR і PTR. Настанова з безпеки

Серія з безпеки IAEA № 50-SG-D3:1980. Система захисту та пов'язані з нею елементи АЕС. Настанова з безпеки

Серія з безпеки IAEA № 50-SG-D8:1984. Інформаційні та керівні системи АЕС, пов'язані з безпекою. Настанова з безпеки

Серія з безпеки IAEA № 50-SG-D11:1986. Основні принципи безпеки проектування АЕС. Настанова з безпеки

Серія з безпеки IAEA 75-INSAG-3:1988. Основні принципи безпеки АЕС.

3 ТЕРМІНИ ТА ВИЗНАЧЕННЯ ПОНЯТЬ

Нижче наведено терміни, ужиті в цьому стандарті, та визначення позначених ними понять

3.1 прикладна функція (*application function*)

Функція КВК-системи, що виконує завдання, пов'язане швидше з контрольованим процесом, ніж з функціюванням самої системи

[2.1 з IEC 60880, модифікований].

Примітка 1. Див. також «КВК-функція», «КВК-система», «прикладне програмне забезпечення».

Примітка 2. Прикладна функція, зазвичай, є підфункцією функції КВК

3.2 прикладне програмне забезпечення (*application software*)

Частина програмного забезпечення КВК-системи, що забезпечує виконання прикладних функцій.

Див. рисунок 2.

Примітка 1. Див. також «прикладна функція», «бібліотека прикладних програм», «системне програмне забезпечення».

Примітка 2. Прикладне програмне забезпечення має відмінності від системного програмного забезпечення

3.3 бібліотека прикладних програм (*application software library*)

Набір згрупованих програмних модулів, що забезпечують виконання типових прикладних функції.

Див. рисунок 2.

Примітка. За використання вже наявного устаткування таку бібліотеку розглядають і кваліфікують як частину програмного забезпечення

3.4 категорія функції КВК (*category of an I&C function*)

Одна з трьох можливих познак безпеки (А, В та С) функцій КВК, яку може бути встановлено внаслідок розгляду впливу функції на безпеку. Не піддається класифікації та функція, яка не має впливу на безпеку.

Примітка 1. Див. також «клас КВК-системи», «функція КВК».

Примітка 2. IEC 61226 визначає категорії КВК ФСБ. Кожній категорії відповідає низка вимог, які застосовують не тільки до функцій КВК (пов'язаних із технічним завданням, проектуванням, упровадженням, верифікацією та валідацією), але також до всього ланцюга елементів, необхідних для того, щоб реалізувати цю функцію (пов'язаних з їхніми властивостями та кваліфікацією) незалежно від того, як ці елементи розподілено між взаємопов'язаними КВК-системами. Для чіткішого розуміння цей стандарт визначає категорії функцій КВК і класи КВК-систем та встановлює взаємозв'язок між категорією функції та мінімальним необхідним класом пов'язаних із нею систем й устаткування

3.5 канал (*channel*)

Розташування взаємопов'язаних компонентів у системі, що ініціюють один вихід. Канал втрачає свою ідентичність у тому разі, якщо сигнали його одиничного виходу комбінуються із сигналами іншого каналу, такими як канал моніторингу або канал захисних дій.

[IAEA 50-SG-D8]

3.6 клас КВК-системи (*class of an I&C system*)

Одна з трьох можливих познак (1, 2 та 3) КВК-систем, важливих для безпеки, що встановлюється внаслідок розгляду вимог до виконання функцій КВК, які мають різне відношення до безпеки. КВК-систему не класифікують, якщо вона не виконує важливих для безпеки функцій.

Примітка. Див. також «категорія КВК-функції», «системи, важливі для безпеки», «системи безпеки»

3.7 відмова за загальної причини (ВЗП) (*common cause failure (ВЗП)*)

Відмова, яка є результатом одної чи більше подій, наслідком яких є одночасна відмова двох чи більше окремих каналів багатоканальної системи або кількох систем, що спричиняє відмову системи(-м)

[3.6.10 IEC 61508-4, змінений].

Примітка. Залежно від контексту ВЗП можна розглядати на рівні одної системи або на рівні кількох систем, що утворюють групу безпеки

3.8 складність (*complexity*)

Характеристика системи або компонента, проектування, упровадження чи поводження яких є складними щодо розуміння та перевірення.

[IEEE 610 [1][1)], змінений]

3.9 компонент (*component*)

Одна з частин, що утворює систему. Компонент може бути апаратним або програмним і сам може утворюватися з інших компонентів.

(IEEE 610 [1]).

Примітка 1. Див. також «КВК-система», «устаткування».

Примітка 2. Терміни «устаткування», «компонент» і «модуль» часто використовують як синоніми. Взаємодію між цими термінами до цього часу не застандартизовано

3.10 комп'ютерна система (*computer-based system*)

КВК-система, функції якої здебільшого залежать від застосування, або повністю виконуються під час застосовування мікропроцесорів, програмованого електронного устаткування або комп'ютерів.

Див. рисунок 2.

Примітка. Див. також «КВК-система»

3.11 уведення АЕС в експлуатацію (*commissioning of the NPP*)

Процес, протягом якого компоненти та системи АЕС, після завершення будівництва, уводять в експлуатацію та проходять перевірення відповідно до проектних критеріїв; ураховуючи як неядерні, так і ядерні випробування.

[IAEA 50-C-D]

3.12 управління конфігурацією (*configuration management*)

Порядок застосування технічного й адміністративного керівництва та нагляду для ідентифікації і документування функційних і фізичних характеристик об'єкта конфігурації, управління зміненням цих характеристик, реєстрування та складення звітів про змінення стану та перевірення відповідності встановленим вимогам.

[IEEE 610 [1]]

3.13 дані (*data*)

Подання інформації або інструкцій у вигляді, придатному для обміну, витлумачення чи оброблення за допомогою комп'ютера.

[IEEE 610 [1], змінений].

Див. рисунок 2

[1)] Посилання у квадратних дужках наведено в «Бібліографії».

3.14 концепція глибокоешелонованого захисту (*defence-in-depth concept*)

Див. розділ А.3

3.15 детерміністичний метод (*deterministic method*)

Див. А.2.2

3.16 різноманітність (*diversity*)

Наявність двох і більше різних способів чи засобів досягнення визначеної цілі. Різноманітність передбачають саме як захист від відмови за загальною причиною. Цього можливо досягти за допомогою систем, які фізично відрізняються одна від одної, або за допомогою функційної різноманітності, коли подібні системи виконують завдання різними способами.

[3.6 IEC 60880-2].

Примітка 1. Див. також «функційна різноманітність».

Примітка 2. Це визначення ширше, ніж те, що застосовує IAEA 50-C-D, як зазначено нижче: «Наявність резервних компонентів або систем для виконання визначеної функції, де такі компоненти або системи спільно об'єднують одну чи більше різних ознак. Прикладами таких ознак є: різні умови роботи, відмінні розміри устаткування, різні виробники, відмінні принципи роботи й типи устаткування, які використовують різні фізичні методи

3.17 устаткування (*equipment*)

Одна чи кілька частин системи. Елементом устаткування є одинична визначувана (і зазвичай змінна) частина системи.

[IEC 61226, змінений].

Примітка 1. Див. також «компонент», «КВК-система».

Примітка 2. До устаткування може входити програмне забезпечення.

Примітка 3. Терміни «устаткування», «компонент» і «модуль» часто використовують як синоніми. Взаємодію між ними до цього часу не застандартизовано

3.18 сімейство устаткування (*equipment family*)

Сукупність технічних засобів і програмних компонентів, які можуть співпрацювати в одній або кількох визначених структурах (конфігураціях). Розроблення конфігурацій для АЕС та відповідного прикладного програмного забезпечення може підтримуватися програмними засобами. Сімейство устаткування зазвичай виконує ряд стандартних функцій (із бібліотеки прикладних функцій), які можуть комбінуватися, для створення певного прикладного програмного забезпечення.

Примітка 1. Див. також «функційність», «прикладне програмне забезпечення», «бібліотека прикладного програмного забезпечення».

Примітка 2. Сімейство устаткування може бути продукцією конкретного виробника чи комплектом виробів, взаємопов'язаних й адаптованих постачальником.

Примітка 3. Термін «платформа устаткування» іноді використовують як синонім до терміносполуки «сімейство устаткування»

3.19 похибка (*error*)

Розбіжність між обчисленим, спостережуваним або виміряним значенням величини чи умови та правильним, установленим або теоретичним значенням величини чи умови.

Див. рисунок 3

3.20 оцінення (властивості системи) (*evaluation* (*of a system property*))

Віднесення властивостей даної системи до кількісного або якісного значення.

[2.2.2 IEC 61069-1]

3.21 відмова (*failure*)

Відмова виникає в разі відхилення реальної роботи від запланованої.

[3.8 IEC 60880-2].

Див. рисунок 3.

Примітка 1. Відмова є наслідком дефекту апаратури, дефекту програмного забезпечення, системи чи помилок оператора, або помилки під час технічного обслуговування, і проходження сигналу, який є наслідком відмови.

Примітка 2. Див. також «дефект», «дефект програмного забезпечення»

3.22 дефект (*fault*)

Дефект апаратури, програмного забезпечення або компонента системи.

Див. рисунок 3.

Примітка 1. Дефекти можна поділити на випадкові, які є наслідком деградації апаратури через старіння, та систематичні, що є наслідком недоліків програмного забезпечення, які виникають через помилки у проектуванні.

Примітка 2. Дефект (зокрема дефект проектування) може залишатися невизначеним, доки зберігаються певні умови, за яких він не відзначається на виконанні функції, тобто не відбудеться відмова.

Примітка 3. Див. також «дефект програмного забезпечення»

3.23 функційна різноманітність (*functional diversity*)

Використання різноманітності на функційному рівні (наприклад аварійне відключення в разі перевищення граничного значення тиску та температури).

[3.10 IEC 60880-2].

Примітка. Див. також «різноманітність»

3.24 функційна валідація (*functional validation*)

Перевірення правильності застосування технічних вимог до функцій у порівнянні ступеня відповідності прикладних функцій порівняно з первісними функційними та експлуатаційними вимогами до станції. Функційна валідація доповнює валідацію системи, за якої піддається оцінению її відповідність специфікації функцій

3.25 функційність (*functionality*)

Властивість функції, яка визначає операції, що перетворюють вхідну інформацію у вихідну.

Примітка. Функційність прикладних функцій здебільшого впливає на роботу станції. Вхідні дані може бути отримано від датчиків, операторів, іншого устаткування або іншої програми. Вихідні дані може бути спрямовано до виконавчих механізмів, операторів, іншого устаткування чи іншої програми (див. [4])

3.26 функція, важлива для безпеки (*function important to safety*)

Конкретна мета, яка має сприяти безпеці.

[IAEA 50-SG-D3 та IEC 61226, змінений].

Примітка. Див. також «КВК-функція», «КВК-підфункція», «прикладна функція»

3.27 небезпека (*hazard*)

Подія, що може завдати шкоди персоналу станції, компонентам, устаткованню або конструкціям. Небезпеку поділяють на внутрішню та зовнішню.

Примітка 1. Внутрішня небезпека — це, наприклад, пожежа та затоплення. Внутрішня небезпека може бути наслідком постульованих вихідних подій (наприклад, аварія з утратою теплоносія, розрив паропроводу).

Примітка 2. Зовнішня небезпека — це, наприклад, землетрус та удар блискавки

3.28 помилка персоналу (або похибка) (*human error* (*or mistake*))

Дія людини або процес, які призводять до непередбачуваного результату.

[3.12 IEC 60880-2]

3.29 незалежне устаткування (*independent equipment*)

Устаткування, що має такі дві характеристики:

a) здатність виконувати потрібну функцію не залежить від роботи або відмови іншого устаткування;

b) здатність виконувати свою функцію не залежить від впливу, спричиненого постульованою вихідною подією, за якої необхідно виконати функцію.

[IAEA 50-SG-D8].

Примітка. Засобами досягнення незалежності під час проектування є електроізоляція (яку, за документацією МАГАТЕ, також називають функційною ізоляцією), фізичне розподілення та комунікаційна незалежність

3.30 переривання (*interrupt*)

Призупинення процесу, наприклад виконання комп'ютерної програми, що спричинено подією, зовнішньою стосовно цього процесу.

[IEEE 610]

3.31 архітектура КВК (*I&C architecture*)

Організаційна структура КВК-систем станції, які є важливими для безпеки.

Примітка 1. Див. також «архітектура КВК-системи», «КВК-система».

Примітка 2. Організаційна структура визначає основні функції, клас і межі кожної системи, взаємозв'язки та незалежність систем, пріоритетність і метод вибирання між сигналами, що діють одночасно, інтерфейс «Людина-машина».

Примітка 3. У цьому стандарті даний термін визначає тільки частину всієї архітектури КВК-станції. Остання охоплює також некласифіковані системи й устаткування

3.32 функція КВК (*I&C function*)

Функція управління, контролювання та/або спостереження за певною частиною процесу.

Примітка 1. Див. також «підфункція КВК», «КВК ФСБ», «прикладна функція».

Примітка 2. Термін «функція КВК» використовують інженери-технологи для того, щоб мати змогу сформулювати вимоги до функціювання КВК. Функцію КВК визначають так, що вона:

— надає повне уявлення про мету виконання функції;

— може належати до певної категорії згідно зі ступенем важливості для безпеки;

— охоплює всі елементи, від датчика до виконавчого пристрою, необхідні для досягнення мети.

Примітка 3. Функція КВК може поділятися на ряд підфункцій (наприклад, функція вимірювання, функція управління, функція приведення до дії) для виділення КВК-систем

3.33 підфункція КВК (*I&C subfunction*)

Частина функції КВК, визначена для КВК-системи або підсистеми.

Примітка 1. Див. також «КВК-функція», «прикладна функція».

Примітка 2. Термін «функція» часто використовують для позначення підфункції, якщо в контексті не виникає невизначеності

3.34 КВК ФСБ: функції та системи й устаткування, що асоціюються з ними (*I&C FSE: function, and the associated systems and equipment*)

Функції виконуються в цілях або для досягнення мети. Асоційовані (пов'язані) системи й устаткування — сукупність компонентів і самі компоненти, що безпосередньо застосовуються для виконання функцій.

[IEC 61226, змінений].

Примітка. Див. також «функція КВК», «КВК-система»

3.35 КВК-система (*I&C system*)

Система, що має у своїй основі електричну та/або електронну, та/або програмовану електронну технологію, яка виконує функції КВК, а також функції обслуговування та спостереження, пов'язані безпосередньо з роботою системи.

Використовують як загальний термін, що охоплює всі елементи системи, а саме внутрішнє джерело живлення, датчики й інші пристрої вводу, шину даних та інші канали комунікації, інтерфейси виконавчих механізмів та інших пристроїв виводу (див. примітку 2). Різні функції, у межах системи, можуть використовувати спеціально визначені або розподілені ресурси.

[3.3.2 IEC 61508-4, змінений].

Примітка 1. Див. також «система», «функції КВК».

Примітка 2. Елементи, що належать до складу певної КВК-системи, визначено у специфікації в межах цієї системи.

Примітка 3. Відповідно до характеру виконуваних функцій МАГАТЕ розрізняє системи автоматизації й управління, людино-машинні системи, системи блокування та системи захисту (див. розділ В.4)

3.36 архітектура КВК-системи (*I&C system architecture*)

Організаційна структура КВК-системи.

Примітка. Див. також «КВК-архітектура»

3.37 елементи, важливі для безпеки (*items important to safety*)

Елементи, до складу яких належать:

a) конструкції, системи та компоненти, несправність або відмова яких може спричиняти надмірну кількість радіоактивного опромінення робочого персоналу або населення;

b) конструкції, системи та компоненти, що запобігають переростанню можливих порушень нормальної експлуатації в аварійну ситуацію; і

c) засоби, що забезпечують пом'якшення наслідків несправності чи відмови конструкцій, систем або компонентів.

[IAEA 50-SG-D3].

Примітка 1. Див. також «система безпеки», «клас КВК-систем».

Примітка 2. У цьому стандарті КВК-системи, важливі для безпеки, можна поділити на три класи: 1, 2 та 3.

Примітка 3. Документ IAEA 50-SG-D8 поділяє системи, важливі для безпеки, на «системи безпеки» та «системи, пов'язані з безпекою»

3.38 ремонтопридатність (*maintainability*)

Імовірність того, що певну операцію з відновлення елемента, за даних умов експлуатації, може бути виконано в межах установленого проміжку часу, якщо ремонт виконують у заздалегідь визначених умовах і з використанням завчасно встановлених процедур і ресурсів.

[2.10 IEC 60987]

3.39 повний життєвий цикл безпеки КВК (*overall safety life cycle of the I&C*)

Необхідна діяльність для КВК-архітектури за впровадження систем й устаткування, важливих для безпеки, що відбувається в проміжок часу, який починається на стадії встановлення вимог до КВК, на основі проекту безпеки станції, і закінчується тоді, коли жодна з КВК-систем більше не придатна до застосування.

[3.7 IEC 61508-4, змінений].

Примітка 1. Повний життєвий цикл безпеки КВК відповідає життєвому циклу безпеки конкретної системи.

Примітка 2. Див. також «життєвий цикл безпеки системи»

3.40 аналіз безпеки станції (*plant safety analysis*)

Див. розділ А.2

3.41 постульована вихідна подія (ПВП) (*postulated initiating event* (*PIE*))

Постульовані вихідні події ідентифікують як події, що призводять до порушень нормальної експлуатації чи аварійних умов та спричинених ними ефектів відмов.

[IAEA 50-C-D].

Примітка 1. Очікувані порушення нормальної експлуатації: сукупність процесів, що мають відхилення від нормальної експлуатації, які, очікувано, відбуваються одноразово або кілька разів протягом часу експлуатації станції, і які, враховуючи передбачені проектом заходи, не завдають жодної значної шкоди елементам, важливим для безпеки, і не спричиняють аварійних умов.

Примітка 2. Першопричинами ПВП можуть бути ймовірні відмови устаткування та помилки оператора (як у межах, так і за межами АЕС), спричинені впливом людини або природними явищами. Перелік ПВП має бути прийнято регулівним органом для АЕС

3.42 заздалегідь розроблене програмне забезпечення (*pre-developed software* (*PDS*))

Програмне забезпечення, яке наявне наразі, є в розпорядженні як комерційний власний продукт і його можна використовувати в комп'ютерній системі.

[3.17 IEC 60880-2].

Примітка. Заздалегідь розроблене програмне забезпечення може підрозділятися на: заздалегідь розроблене програмне забезпечення загальної призначеності, яке не було спеціально розроблено для певного устаткування, і заздалегідь розроблене програмне забезпечення, інтегроване до складу апаратних компонентів, яке потрібно використовувати спільно з цими компонентами

3.43 імовірнісний метод (*probabilistic method*)

Див. А.2.2

3.44 проектна організація (*project organization*)

Організація(-ї) або фізичні особи, які протягом етапів повного життєвого циклу безпеки КВК і/чи життєвих циклів безпеки КВК-систем відповідають за визначення та виконання всіх видів керування та технічних дій, що стосуються КВК-функцій, систем й устаткування, важливих для безпеки.

Примітка. Цей термін відрізняється від терміносполуки «експлуатаційна організація»

3.45 кваліфікація (*qualification*)

Процес визначання придатності системи або компонента для експлуатації. Кваліфікація виконується в контексті встановленого класу КВК-системи та певного набору кваліфікаційних вимог

3.46 якість (*quality*)

Сукупність характеристик об'єкта, які роблять його спроможним задовольняти встановлені та передбачувані потреби.

[2.1 ISO 8402]

3.47 забезпечення якості (*quality assurance*)

Сукупність усіх спланованих і систематично виконуваних заходів, необхідних для забезпечення відповідної впевненості в тому, що продукція або послуги будуть задовольняти вимоги якості.

[3.5 ISO 8402, змінений]

3.48 програма забезпечення якості (*quality plan*)

Документ, у якому викладено заходи, засоби та послідовність дій із забезпечення якості, що стосуються окремого продукту, проекту або контракту

3.49 резервування (*redundancy*)

Забезпечення альтернативних (однакових або різнотипних) елементів або систем так, що кожен із них може виконувати потрібну функцію, незалежно від стану функціювання або відмови будь-якого іншого.

[IAEA 50-SG-D8]

3.50 надійність (*reliability*)

Імовірність того, що прилад, система чи елемент буде виконувати встановлені функції задовільно протягом певного проміжку часу за певних умов експлуатації.

[IAEA 50-SG-D8].

Примітка. Надійність комп'ютерної системи охоплює надійність технічних засобів, яку зазвичай виражають кількісно, та надійність програмного забезпечення, яка зазвичай є якісним критерієм, тому що немає загальноприйнятих засобів кількісного оцінення надійності програмного забезпечення

3.51 програмне забезпечення багаторазового застосування (*reusable software*)

Модуль програмного забезпечення, який можна використовувати більше ніж в одній комп'ютерній програмі або системі з програмним забезпеченням.

(IEEE 610 [1], модифікований)

3.52 група безпеки (*safety group*)

Комплект устаткування, призначений для виконання всіх дій, що потребує окрема постульована вихідна подія, щоб мати змогу гарантувати, що межі, установлені в проекті для цієї події, не перевищуються.

[IAEA 50-SG-D3].

Примітка. Функції КВК у групі безпеки можуть належати до різних категорій

3.53 системи безпеки (*safety systems*)

Системи, важливі для безпеки, призначені для того, щоб гарантувати за будь-яких умов безпечну зупинку реактора та відведення тепла з активної зони й/чи обмежити наслідки прогнозованих порушень нормальної експлуатації й аварійних умов.

[IAEA 50-SG-D8].

Примітка 1. Див. також «система, важлива для безпеки», «клас КВК-системи».

Примітка 2. Система безпеки з МАГАТЕ цілком відповідає системам класу 1 у цьому стандарті

3.54 захищеність (*security*)

Здатність комп'ютерної системи захистити інформацію та дані від несанкційованого доступу сторонніх осіб чи інших систем для читання або коригування і дати змогу санкційованого доступу вповноваженому персоналу або системам.

[3.25 ISO/IEC 12207, змінений]

3.55 одинична відмова (*single failure*)

Випадкова відмова, яка призводить до втрати компонентом або системою можливості виконувати призначені функції. Вважають, що наступні відмови, спричинені одиничною випадковою подією, є частиною одиничної відмови.

[IAEA 50-SG-D8, змінений].

Примітка 1. Див. також «критерій одиничної відмови».

Примітка 2. Одинична відмова може бути наслідком внутрішньої або зовнішньої небезпеки

3.56 критерій одиничної відмови (*single-failure criterion*)

Комплекс устаткування задовольняє критерій одиничної відмови в тому разі, якщо він відповідає своїй цільовій призначеності, незважаючи на те, що передбачувана одинична випадкова відмова відбувається в будь-якому місці комплексу. Вважають, що наступні відмови, які відбуваються після одиничної, є її складовою частиною.

[IAEA 50-C-D].

Примітка 1. Див. також «одинична відмова», «відмова програмного забезпечення».

Примітка 2. Відмови програмного забезпечення є систематичними, а не випадковими

3.57 відмова програмного забезпечення (*software failure*)

Відмова системи, обумовлена проявом проектних дефектів у компоненті програмного забезпечення.

Примітка 1. Усі відмови програмного забезпечення обумовлено помилками під час проектування, тому що програмне забезпечення є винятково продуктом проекту і не може спрацьовуватися та зазнавати фізичних пошкоджень. Оскільки чинники, що активують дефекти у програмному забезпеченні під час роботи системи трапляються випадково, відмови програмного забезпечення також відбуваються випадково.

Примітка 2. Див. також «відмова», «дефект», «дефект програмного забезпечення»

3.58 дефект програмного забезпечення (*software fault*)

Проектний дефект у компоненті програмного забезпечення.

Примітка. Див. також «дефект»

3.59 надійність програмного забезпечення (*software reliability*)

Складова надійності системи, яка залежить від відмов програмного забезпечення

3.60 специфікація (*specification*)

Документ, який цілком, точно, у перевірений спосіб визначає вимоги, конструкцію, роботу й інші характеристики системи або компонента, а часто і методи, що визначають, чи достатньо задовольняють ці вимоги.

[3.21 IEC 60880-2 та IEEE 610 [1]]

3.61 система (*system*)

Набір компонентів, які взаємодіють відповідно до проекту, у якому елемент системи може сам бути системою, яку в такому разі називають підсистемою.

[3.3.1 IEC 61508-4, змінений].

Примітка 1. Див. також «КВК-система».

Примітка 2. КВК-системи відрізняються від механічних систем й електричних систем АЕС

3.62 систематична відмова (*systematic failure*)

Відмова, обумовлена певною причиною, яку може бути вилучено тільки за допомогою модифікації проекту або виробничого процесу, процедур експлуатації, документації або інших відповідних чинників.

[3.6.6 IEC 61508-4]

3.63 життєвий цикл безпеки системи (*system safety life cycle*)

Необхідна діяльність під час упровадження КВК-системи, важливої для безпеки, яка реалізується за проміжок часу, який розпочинається на стадії створення концепції та розроблення системних вимог і закінчується, коли система більше не придатна для використання.

Примітка 1. Життєвий цикл безпеки системи стосується повного життєвого циклу безпеки.

Примітка 2. Див. також «повний життєвий цикл безпеки КВК»

3.64 системне програмне забезпечення (*system software*)

Програмне забезпечення, розроблене для певної комп'ютерної системи або низки комп'ютерних систем, для забезпечення роботи та обслуговування комп'ютерної системи й установлених програм, наприклад операційні системи, комп'ютери, утиліти. Системне програмне забезпечення зазвичай має у своєму складі програмне забезпечення операційної системи та програмне забезпечення підтримання.

[3.24 IEC 60880-2].

Див. рисунок 2.

Примітка 1. Програмне забезпечення операційної системи: програми, що виконуються за допомогою основного процесора протягом експлуатування системи, такі як: операційна система, драйвери вводу-виводу, програма обробляння особливих ситуацій, комунікаційні програми, бібліотеки прикладних програм, програми оперативної діагностики, резервування й управління поступовою деградацією.

Примітка 2. Програмне забезпечення підтримання: програми, що допомагають під час розробляння, випробовування чи технічного обслуговування іншого програмного забезпечення, та системи, а саме такі як: компілятори, генератори кодів, графічні редактори, програми автономної діагностики, засоби валідації та верифікації тощо.

Примітка 3. Див. також «прикладне програмне забезпечення».

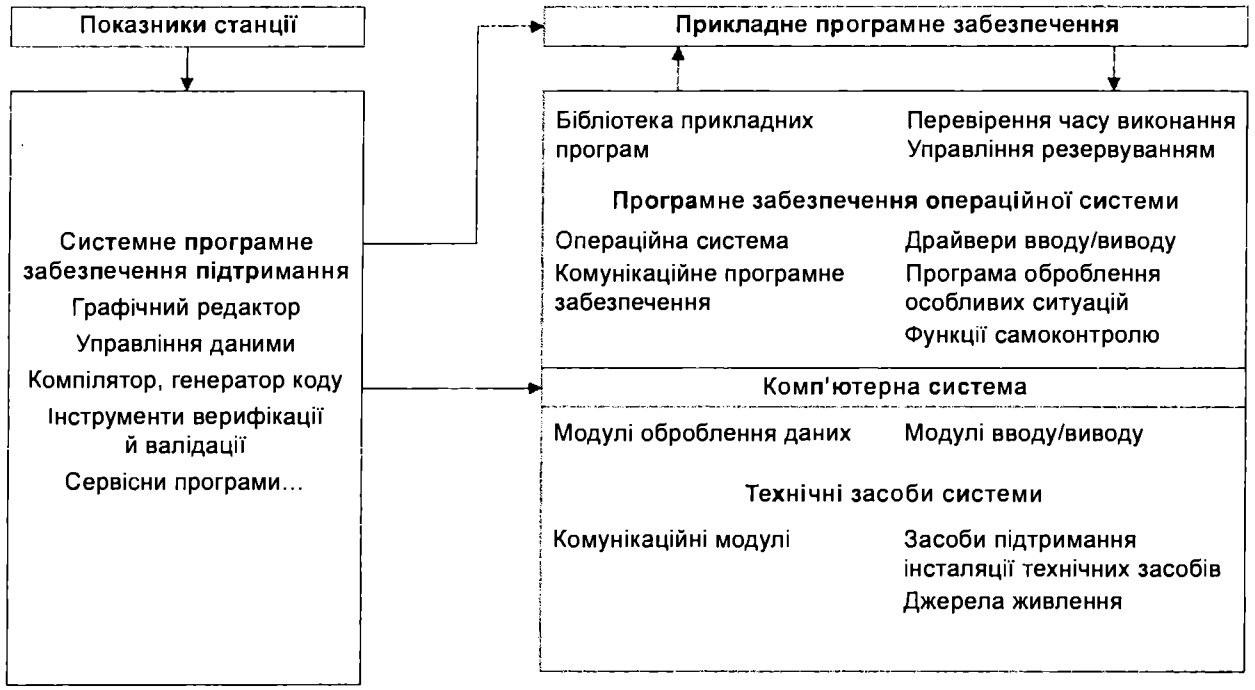


Рисунок 2 — Характерні взаємозв'язки технічних засобів і програмного забезпечення комп'ютерної системи

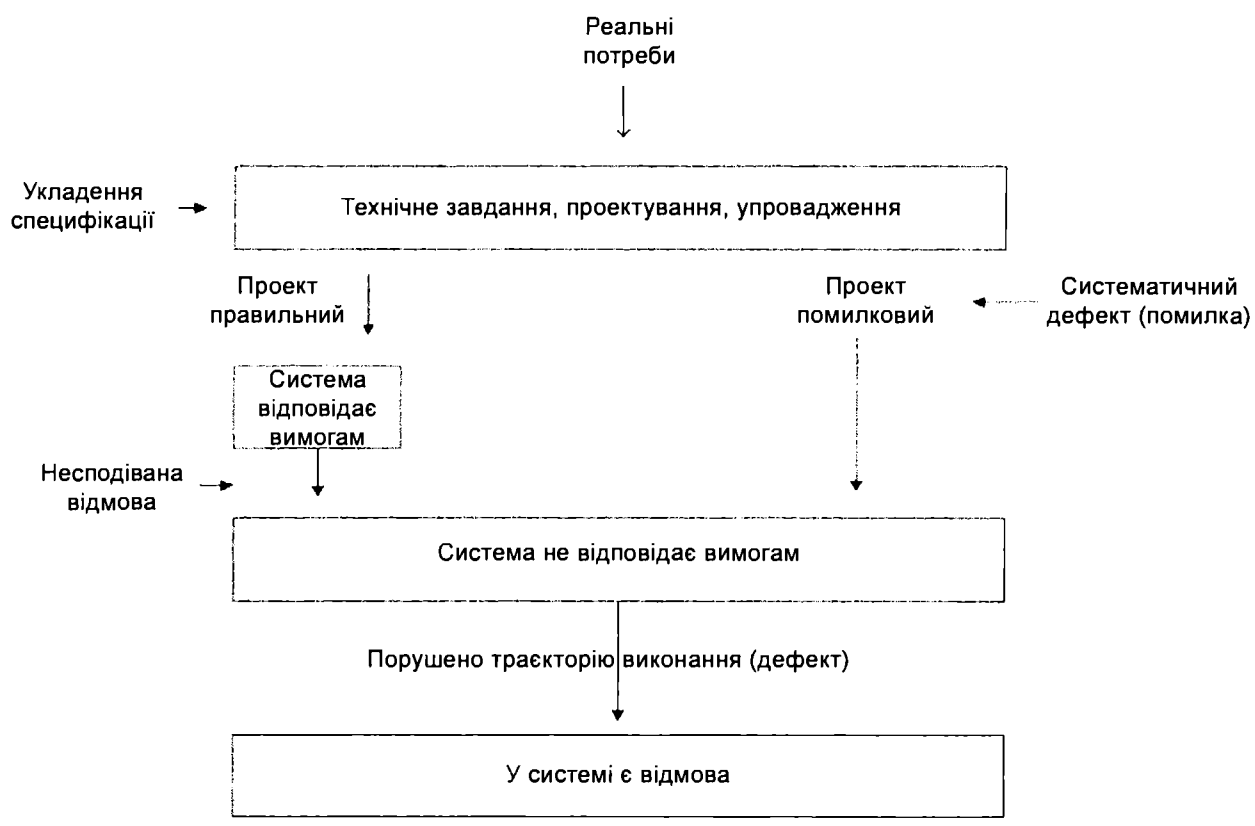


Рисунок 3 — Взаємозв'язки між відмовою системи, випадковою відмовою та систематичним дефектом

4 СИМВОЛИ ТА СКОРОЧЕННЯ

КС — Комп'ютерна система
ВЗП — Відмова за загальної причини
КП — Комерційний продукт
ЕМП — Електромагнітні перешкоди
УПК — Устаткування, що піддається керуванню
ФСБ — Функції й асоційовані з ними системи й устаткування
ІЛМ — Інтерфейс «Людина-машина»
КВК — Контрольно-вимірювальна та керівна
В/В — Ввід/вивід
АВТ — Аварія з втратою теплоносія
АЕС — Атомна електростанція
ПЗРР — Програмне забезпечення, розроблене раніше
ПВП — Постульовані вихідні події
ІОБ — Імовірнісне оцінення безпеки
ЗЯ — Забезпечення якості
РПБ — Рівень повної безпеки
Е/Е/ПЕС — Електрична/електронна/програмована електронна система

5 ПОВНИЙ ЖИТТЄВИЙ ЦИКЛ БЕЗПЕКИ КВК

Мета розділу — визначити, як саме:

— Вивести загальні вимоги до КВК ФСБ, важливих для безпеки, з основного проекту безпеки АЕС (див. розділи А.1 та А.2);

— Вивести вимоги до архітектури КВК-систем, важливих для безпеки, із загальних вимог до КВК ФСБ; і

— Установити зв'язок між вимогами до архітектури КВК та вимогами до індивідуальних КВК-систем, важливих для безпеки.

Для забезпечення того, що всі вимоги щодо безпеки для станції, які висуваються КВК, фіксовано, реалізовано та підтримано, потрібно мати системний підхід. Цього можливо досягти в процесі розробляння, упровадження й експлуатування КВК у рамках повного життєвого циклу безпеки КВК. Цей життєвий цикл пов'язано у свою чергу з життєвими циклами безпеки індивідуальних КВК-систем (див. розділ 6).

До типових етапів повного життєвого циклу безпеки КВК належать:

a) Огляд основного проекту безпеки станції, до якого належать (див. 5.1):
— Функційні, експлуатаційні вимоги та вимоги незалежності;
— Категоризація функцій;
— Станційні обмеження;

b) Визначення загального технічного завдання вимог до КВК ФСБ, важливих для безпеки (див. 5.2);

c) Проектування загальної архітектури КВК і призначеність функцій КВК індивідуальним системам й устаткованню (див. 5.3);

d) Визначення загального планування (див. 5.4);

e) Реалізація індивідуальних систем (див. розділ 6);

f) Загальна інтеграція систем та введення в експлуатацію (див. розділ 7);

g) Загальна експлуатація й обслуговування (див. розділ 8).

Числа в дужках визначають розділ або підрозділ цього стандарту, у якому описано відповідний етап, тоді як мету, вхідні й вихідні дані та сферу діяльності кожного етапу наведено в таблиці 1.

Зв'язки між цим життєвим циклом та життєвим циклом безпеки окремих КВК-систем зображено у спрощеній формі на рисунку 4.

a) Повний життєвий цикл безпеки всіх КВК — ітеративний процес, у якому вихідні дані кожного етапу треба перевірити та узгодити з вхідними даними, отриманими внаслідок попередніх дій. Етап може починатися, навіть якщо дії попереднього етапу ще не завершено, якщо застосовано відповідне управління конфігурацією, яка гарантує дотримання повної послідовності процесу розроблення;

b) Етап може бути завершено, якщо завершено попередні етапи.

Примітка. Відповідає за безпеку АЕС організація, що її експлуатує, і її відповідальність в жодному разі не може бути зменшено завдяки розробникам, постачальникам, будівникам і наглядовим органам, які займаються іншою діяльністю.

(Див. 3.1.2, IAEA 75-INSAG-3).

Таблиця 1 — Загальний огляд повного життєвого циклу безпеки КВК

Розділ, підрозділ або пункт	Вхідні дані	Мета діяльності	Сфера діяльності	Вихідні дані
5	Вимоги, що належать до повного життєвого циклу безпеки, та їхній зв'язок із життєвими циклами системи			
5.1	Вимоги до КВК, отримані з основного проекту безпеки станції			
5.1.1 Огляд функційних, експлуатаційних вимог та вимог до незалежності	Документація основного проекту безпеки станції. Принципи експлуатації станції	Установити: — загальні функційні й експлуатаційні вимоги до КВК ФСБ, важливі для безпеки; — вимоги незалежності КВК ФСБ із точки зору концепції глибокоешелонованого захисту станції; — автоматичні функції та завдання оператора	Системи станції та пов'язані з ними КВК ФСБ, важливі для безпеки	Визначення вхідних вимог для 5.2
5.1.2 Огляд вимог до категоризації	Категоризація безпеки станції	Установити категорії ФСБ, перевірити повноту та реалізованість комплексних вимог	КВК ФСБ, важливі для безпеки	Визначення вхідних вимог до 5.2
5.1.3 Огляд станційних обмежень	Документи плану розміщення станції та проектна база даних станції	Установити: — межі станції/КВК-систем; — обмеження, що походять від систем забезпечення та розміщення станції, умов навколишнього середовища; — джерела потенційної внутрішньої та зовнішньої небезпеки; — принципи експлуатації та технічного обслуговування станції	План розміщення станції. Станційні системи КВК ФСБ	Визначення обмеження для структурного проектування (див. 5.3) та для технічного завдання індивідуальних КВК-систем (див. 6.1)
5.2 Вихідна документація	Вихідні дані 5.1	Розробити загальне технічне завдання КВК ФСБ, важливих для безпеки, із точки зору функційних, експлуатаційних вимог та вимог незалежності й категоризації	КВК ФСБ	Загальне технічне завдання ФСБ до 5.3

Кінець таблиці 1

Розділ, підрозділ або пункт	Вхідні дані	Мета діяльності	Сфера діяльності	Вихідні дані
5.3	Проект загальної архітектури КВК та призначеність функцій КВК			
5.3.1 Проект архітектури КВК	Вихідні дані 5.2	Розробити проект архітектури КВК-систем, реалізовуючи загальні технічні завдання КВК ФСБ, важливих для безпеки. Ужити необхідних заходів щодо запобігання потенційним ВЗП	КВК-функції та КВК-системи	Детальний проект безпечної архітектури КВК із точки зору автоматизованих систем, ІЛМ та взаємозв'язків, інструментальних засобів (див. 5.5.1)
5.3.2 Функційна призначеність	Вихідні дані 5.3.1 та 5.4 (ітерація з вихідними даними 6.3)	Призначити функції КВК окремим КВК-системам й устаткованню. Передбачити вимоги (межі, класифікацію, функційність, надійність та інші необхідні якості) для окремих КВК-систем	КВК-функції та КВК-системи	Вимоги до прикладних функцій систем та ІЛМ, проекту КВК-систем та інструментальних засобів (див. 5.5.2)
5.3.3 Необхідний аналіз	Вихідні дані 5.3.1 та 5.3.2	Оцінити надійність і захист від ВЗП. Оцінити чинник людини	КВК-функції та КВК-системи	Оцінка надійності та захисту від ВЗП; Оцінка чинника людини
5.4 Загальне планування	Вихідні дані 5.3	Скласти плани КЯ, захисту, інтеграції, уведення в експлуатацію, експлуатації та технічного обслуговування систем	КВК-системи, що спільно працюють	Плани для визначених дій
6 Життєвий цикл безпеки системи	Вихідні дані 5.5	Визначити та створити КВК-системи, що відповідають специфікації КВК-архітектури. (див. розділ 6)	Індивідуальні КВК-системи	Вихідні дані, описані в таблиці 3
7 Загальна інтеграція й уведення в експлуатацію	Вихідні дані 5.4.3 та 6.2.5	Випробувати й увести в експлуатацію взаємопов'язані системи архітектури КВК	КВК-системи архітектури КВК	Повна інтеграція й уведення систем в експлуатацію. Звіт про загальне введення в експлуатацію (див. 7.2)
8 Загальна експлуатація та технічне обслуговування	Вихідні дані з 5.4.4 та 5.4.5, 7.1	Оперативно обслуговувати й ремонтувати системи для підтримання безпеки	КВК-системи архітектури КВК	Подальше виконання функцій. Інструкції з експлуатації та технічного обслуговування (див. 8.2)
Примітка. Для порівняння цього визначення етапів з визначенням з IEC 61508-1, див. додаток D.				

Рисунок 4 — Зв'язок між повним життєвим циклом безпеки КВК та життєвими циклами безпеки окремих КВК-систем

5.1 Вимоги до КВК, отримані з основного проекту безпеки станції

Метою вимог цього розділу є отримання вхідних вимог для технічного завдання на КВК ФСБ і вхідних обмежень для проекту архітектури КВК, отриманих з основного проекту безпеки станції та середовища станції.

IAEA C-D Rev 1 та IAEA 50-SG-D 11 визначають ряд окремих «принципів безпеки», які разом становлять «інтегрований загальний підхід до безпеки», що гарантує безпеку АЕС. Ці принципи треба застосовувати в проекті, ураховуючи всі відповідні «Постульовані вихідні події» (ПВП) і послідовність фізичних бар'єрів для дотримання норм радіаційного опромінення персоналу, населення та навколишнього середовища (див. А.1, А.2 й А.3). Застосовуючи цей метод, проектна основа станції визначає відповідний рівень якості для функцій і систем станції, потрібний для того, щоб підтримувати станцію в нормальному робочому стані, гарантувати правильну відповідну реакцію на всі ПВП та полегшити довгострокове управління станцією після аварії.

5.1.1 *Огляд функційних, експлуатаційних вимог і вимог незалежності*

Функційні, експлуатаційні вимоги та вимоги незалежності для функцій КВК, важливих для безпеки, і принципи роботи станції, визначені в проектній основі безпеки станції, яка є невід'ємним елементом загального проекту КВК. У вимогах до взаємодії людина-машина розглядають принципи спільної роботи, з урахуванням ергономіки, для мінімізації відмов, пов'язаних із чинником людини.

Для основного проекту безпеки станції мають забезпечуватися такі вхідні дані:

— Концепція глибокоешелонованого захисту станції (див. розділ А.3) і сукупність функцій, які належать до послідовностей ПВП, для виконання завдань безпеки (див. розділ А.2).

Примітка 1. У разі, коли потребується дуже висока надійність функції, технічне завдання для станції та КВК передбачає різні заходи захисту для тих самих ПВП, наприклад два чи більше незалежних і функційно відмінних фізичних критеріїв спрацьовування і за потреби іншу, функційно відмінну, незалежну, резервну механічну систему управління в разі аварії.

Примітка 2. Глибокоешелонований захист має у своєму складі функції, важливі для безпеки, і може також охоплювати інші функції. Вимоги цього стандарту стосуються тільки функцій, важливих для безпеки;

— Функційні й експлуатаційні вимоги для функцій, важливих для безпеки станції, мають відповідати загальним вимогам безпеки (див. розділ А.3).

Примітка 3. Якщо потрібна функційна валідація (див. 6.1.1.1), у проектній основі установлюються умови спрацьовування, припустимі межі та припустима швидкість змінення параметрів станції, які перебувають під управлінням КВК-систем, важливих для безпеки;

— Роль автоматики та встановлених дій оператора в керуванні передбачуваними порушеннями умов експлуатації й аварійними умовами (див. розділ А.3);

— Аналіз завдання відповідно до 3.2 IEC 60964 для визначення, які функції мають виконувати оператори, а які — машини;

— Параметри, які відображаються для використання оператором за ручного управління;

— Принципи пріоритету між діями, що ініціюються автоматично або вручну, зважаючи на категорії функцій, операторські приміщення або розміщення.

5.1.2 ***Огляд вимог до категоризації***

5.1.2.1 *Припущення цього стандарту стосовно категоризації функцій і класифікації систем*

Функції, системи й устаткування АЕС покласифіковано відповідно до їхньої важливості для безпеки (див. розділ В.1). У цьому стандарті зазначено відмінності між категоризацією КВК-функцій та класифікацією КВК-систем. Логічне обґрунтування цієї схеми з подвійною градацією та взаємодію між концепціями класифікації МАГАТЕ та IEC 61226 надано в додатку В.

Примітка. Терміни «категоризація» та «класифікація» іноді використовують як синоніми. Для внесення чіткості в цьому стандарті термін «категоризація» використовують тільки стосовно функцій, а термін «класифікація» — стосовно систем.

У процесі категоризації кожній КВК-функції надають категорію відповідно до її важливості для безпеки. Ці категорії характеризуються сукупністю вимог до специфікації, проектування, реалізації, верифікації та валідації функцій КВК, а також вимогою до мінімально необхідного класу асоційованих із ними систем та устаткування, потрібного для реалізації функцій. Узгоджені вимоги застосовують до всієї послідовності елементів як потрібних для реалізації цієї функції незалежно від того, як вони розподіляються в низці взаємопов'язаних КВК (див. розділ А1 IAEA 50-SG-D1).

У процесі класифікації КВК-систем й устаткування їх розподіляють за різними класами відповідно до важливості для безпеки. Ці класи характеризують низкою вимог до властивостей системи та її кваліфікації. Виконання цих вимог надає можливість класифікованій системі бути придатною для реалізації одної чи більше функцій КВК відповідно до певної категорії. Вимоги відповідно застосовують для прикладних функцій, сервісних функцій і функцій системного програмного забезпечення системи.

Процес категоризації функцій КВК є частиною основного проекту безпеки станції і зовнішнім стосовно галузі застосування цього стандарту (див. розділ В.2). Цей стандарт передбачає, що в проектній основі безпеки станції надані КВК-функції, важливі для безпеки, належать до одної з трьох категорій А, В чи С і що основні проектні вимоги до пов'язаних із ними систем й устаткування узгоджено з вимогами розділу 8 IEC 61226. Окрім того, вимоги до категорії А узгоджено з вимогами систем безпеки МАГАТЕ.

Примітка. Нормативні посилання для категоризації можуть змінюватися в різних країнах. Унаслідок того неможлива єдина вихідна категоризація функцій КВК за застосування цього стандарту, який розглядає нові та вже наявні станції. У такому разі потрібно виконати спеціальне аналізування вихідної категоризації, щоб забезпечити відповідність між категоріями КВК-функцій і вимогами до пов'язаних із ними систем й устаткування.

Класифікацію КВК-систем визначає проектна організація КВК на етапі проектування архітектури КВК перед визначенням КВК-функцій для систем (див. 5.3.1 та 5.3.2).

5.1.2.2 *Вимоги*

a) Категоризацію функцій КВК має бути виконано у проектній основі безпеки станції і вона має базуватися на вхідних даних загального технічного завдання на КВК ФСБ (див. 5.2);

b) Організація, яка проектує КВК, повинна розглянути категоризацію та перевірити її повноту і придатність. У разі непридатності (наприклад, призначеності найвищої категорії для надто складної функції) треба виконати повторне аналізування станції та КВК-функцій, доки не буде досягнуто прийнятного рішення.

5.1.3 *Огляд проектних обмежень станції*

Проект архітектури КВК (див. 5.3) підпадає під проектні обмеження згідно з умовами станції.

a) Організація, що проектує КВК, повинна визначити обмеження на розміщення устаткування КВК, виходячи з компоновки станції, взаємодії з устаткованням станції й урахуванням подій, що виходять за рамки КВК, охоплюючи:

— Границі між КВК системами й устаткованням та системами станції, зокрема взаємодію з електричними/механічними системами й електроживленням;

— Діапазон перехідних і стабільних станів навколишнього середовища за нормальних умов, порушення нормальних умов й аварійних режимів, за яких потрібно функціювання КВК-систем;

— Діапазон перехідних і стабільних станів контролювання та керування живленням за нормальних умов, порушення нормальних умов й аварійних режимів, за яких потрібно функціювання КВК-систем;

— Основні проектні обмеження на монтування та проведення кабелю;

— Спеціальні обмеження на монтування та проведення кабелю в центрах їхнього сходження, таких як блочний пульт управління і розподільні приміщення;

— Обмеження в уземленні та розподіленні електроживлення;

— Внутрішні та зовнішні небезпеки, які розглядають із точки зору можливої потенційної небезпеки для станції. До них належить пожежа, повінь, обмерзання, блискавка, стрибок напруги чи електромагнітні перешкоди, землетрус, вибух або хімічна дія;

b) Організація, що проектує КВК, повинна визначити обмеження стосовно устаткування КВК за експлуатаційними принципами, тобто обмеження:

— захисту;

— функціювання та технічного обслуговування (див. 2.6 з IEC 60964);

— технічного обслуговування під час експлуатування КВК-систем.

5.2 Вихідна документація

Результатом діяльності, наведеної в 5.1, має бути вихідна документація у вигляді загального технічного завдання для індивідуальних КВК ФСБ, важливих для безпеки.

Примітка 1. Загальне технічне завдання охоплює всі КВК-функції — від джерел її вхідних даних (датчиків, операторів, іншого устаткування) до приймачів вихідних даних (виконавчих механізмів, операторів чи іншого устаткування). Подальший розподіл технічного завдання забезпечує розроблення технічних завдань для підфункцій, на рівні індивідуальних КВК-систем. Це буде залежати від вибраної архітектури КВК (див. 5.3) і від того, як ту функцію, що реалізують, буде розподілено за устаткованням (приладами, засобами оброблення та виконавчими механізмами).

a) Загальне технічне завдання має стосуватися кожної КВК ФСБ та охоплювати:

1) функційне технічне завдання, що визначає спосіб перетворення функцією вхідної інформації у вихідну для того, щоб упорядкувати роботу і контроль станції;

2) експлуатаційне технічне завдання, що визначає діапазон, точність і динамічні характеристики функції.

Примітка 2. Містить вимоги до часових характеристик, що було відсутнім для технічних систем у минулому;

3) Специфікація категорій функцій.

Примітка 3. Категорія неявно визначає мінімальні класифікаційні вимоги до КВК-систем, потрібних для реалізації функцій (див. таблицю 2);

b) Загальне технічне завдання має визначити будь-яку залежність між функціями, яка створює обмеження під час призначання функцій КВК-системам. Воно охоплює:

1) комбінації функцій, які мають підлягати моніторингу для керівних захисних дій;

2) комбінацію функцій, що забезпечують глибокоешелонований захист;

3) комбінацію функцій, що становлять групу безпеки;

c) Загальні технічні завдання всіх КВК ФСБ має бути перевірено для забезпечення гарантії того, що функції й обмеження визначено для призначеності функцій системам й укладення специфікації цих систем (див. 6.1).

5.3 Проект загальної архітектури КВК та призначеність КВК-функцій

Цей підрозділ описує, як саме:

— Обмеження з 5.1.3 та вимоги з 5.2 застосовують до проекту загальної архітектури КВК-систем, важливих для безпеки (скорочено «архітектура КВК»);

— КВК-функції призначено індивідуальним КВК-системам.

5.3.1 *Проект архітектури КВК*

Проект архітектури КВК забезпечує верхній рівень визначення КВК-систем АЕС (див. розділ В.4), зв'язку між цими системами, і засобів, потрібних для забезпечення відповідного інтерфейсу між цими системами.

5.3.1.1 *Загальні вимоги*

a) Проект архітектури КВК має охоплювати всі КВК, потрібні для виконання КВК-функцій, важливих для безпеки, зазначених у 5.2;

b) Проект архітектури КВК має поділити всі КВК на системи та устаткування, достатні для того, щоб задовольняти вимоги:

— Незалежність функцій у різних ешелонах захисту;

— Прийнятне розподілення систем за різними класами;

— Виконання обмежень фізичного розділення й електричної ізоляції, що походять з обмежень навколишнього середовища та компонування, аналізу небезпеки й технічного обслуговування під час експлуатування (див. 5.1.3);

c) Проект архітектури КВК повинен забезпечити достатні системи та підсистеми, у яких критерій одиничної відмови виконується для функцій категорії А, для всіх передбачених конфігурацій систем і станції (див. 7.5 з IAEA 50-SG-D3);

d) Кожну КВК-систему має бути покласифіковано згідно з її придатністю до виконання КВК-функцій певної категорії.

Таблиця 2 — Кореляція між класами КВК-систем і категоріями КВК-ФСБ

Категорія КВК-функцій, важливих для безпеки			Відповідні класи КВК-систем, важливих для безпеки
A	(B)	(C)	1
	B	(C)	2
		C	3
Примітка. Функції КВК категорії А можуть бути реалізованими тільки в системах класу 1. Функції КВК категорії В може бути реалізовано в системах класу 1 та 2. Функції КВК категорії С можуть бути реалізовані в системах класу 1, 2 та 3.			

e) Інтерфейси зі станцією та взаємозв'язок між КВК-системами треба визначати як частину проектування архітектури для того, щоб визначити:

— розділення (вимірюваних) сигналів між різними функціями, важливими для безпеки;

— вибір і пріоритети між ініціюючими сигналами від різних систем;

— шляхи проходження сигналу й устаткування, яке є спільним для автоматичного або ручного керування на різних лініях захисту;

f) Опис систем, устаткування та їхніх взаємозв'язків у проекті архітектури КВК треба робити достатньо докладним, щоб можна було аналізувати проблеми безпеки КВК.

5.3.1.2 *Інтерфейс людина-машина*

a) До складу проекту архітектури КВК належить структура ІЛМ-систем для управління та спостереження за різними ділянками станції, охоплюючи блоковий щит управління, резервний щит управління, віддалений пункт зупинки реактора (див. IEC 60965), місцеві панелі управління та центр кризового управління зі ступенем резервування, необхідним для врахування обмежень у роботі та технічному обслуговуванні станції (див. 5.1.3);

b) Проект архітектури КВК має враховувати правила експлуатації станції, визначені в основному проекті станції (див. 5.1.1), до складу яких належать:

— Принципи пріоритету між автоматичними сигналами та сигналами керування, ініційованими вручну;

— Принципи пріоритету між різними системами ІЛМ під час експлуатування за нормальних, аварійних умов і після аварії;

— Принципи пріоритету між основними та резервними системами ІЛМ;

— Принципи умов перемикання між основними та резервними системами ІЛМ;

c) Під час проектування архітектури треба визначити, як саме можливо сповістити оператора станції про дефекти та відмови, виявлені засобами діагностики індивідуальних систем. Форма повідомлення має бути такою, за якої оператор може:

— Одразу розпізнати повідомлення про відмову та відрізнити його від інших робочих сигналів;

— Прийняти рішення щодо застосування дій уручну, щоб утримати станцію в безпечному режимі;

— Ідентифікувати системи для відповідного обслуговувального персоналу;

d) Проект архітектури КВК має демонструвати узгодженість з основними рішеннями, що стосуються технології систем ІЛМ (наприклад, комп'ютеризованих або традиційних). Складніші системи треба використовувати для подання інформації на вимогу операторів станції у тому разі, якщо це зменшує вплив відмов, пов'язаних із чинником людини, та якщо цей вплив можливо зменшити отриманням докладнішої інформації. Можливість ВЗП інформаційної комп'ютерної системи треба розглядати порівняно з можливістю відмов через чинник людини;

e) Під час проектування архітектури КВК треба:

— Призначити функції ручного чи автоматичного керування відповідно до аналізу завдання основного проекту станції (див. 5.1.1);

— Визначити обчислювальну потужність КВК-системи, потрібну для оброблення інформації та реалізації завдань, визначених для взаємодії з оператором (див. 3.2.2 IEC 60964);

— Забезпечити, щоб інформація та час, які має оператор у своєму розпорядженні для виконання ручного управління, відповідали вимогам основного проекту станції (див. 5.1.1);

f) Технології, що мають у своїй основі чинник людини, згідно з IEC 60964 та IEC 60965, потрібно використовувати для забезпечення ефективності ІЛМ, під час проектування основного щита управління й інших зон управління станції;

g) Під час аналізування проекту потрібно звернути увагу на завдання оператора й оптимізацію вимог ІЛМ, причому як на завдання, важливі для безпеки, так і не важливі для неї.

5.3.1.3 *Передавання даних*

Передавання даних між системами, що становлять архітектуру КВК, охоплює всі лінії передавання одного чи кількох сигналів та повідомлень за одною чи кількома лініями, використовуючи метод багатоканальності.

a) Лінії зв'язку мають задовольняти специфікації загальних експлуатаційних вимог (див. 5.2) за будь-яких станів станції;

b) Структура та технологія ліній зв'язку мають забезпечувати виконання вимог до незалежності між системами. На додаток до фізичного розподілення й електричної ізоляції проект має містити заходи, що унеможливлюють вплив проблем із лініями зв'язку на технологічні модулі;

c) Лінії зв'язку мають містити засоби перевірення комунікаційного устаткування та цілісності даних, які передають;

d) Для унеможливлення відмов має забезпечуватися резервування ліній зв'язку;

e) Лінії зв'язку має бути спроектовано так, щоб передавання даних та виконання функції вищої категорії безпеки не піддавалися небезпеці під час передавання даних системами нижчого класу безпеки. Наприклад, перевірення під час експлуатування не мають негативно впливати на функції найвищої категорії безпеки.

5.3.1.4 *Засоби*

a) Проект архітектури КВК повинен мати у своєму складі визначення засобів, зазвичай заснованих на комп'ютерах (див. 4.2 IEC 60880-2), які використовують для забезпечення відповідності обміну даних між КВК-системами, що працюють спільно, і для забезпечення відповідності даних із базою даних станції.

Примітка. Засоби для індивідуальних систем визначають на стадії специфікації систем (див. 6.1.2.1);

b) Засоби бажано використовувати на всіх фазах загального життєвого циклу безпеки, де може бути забезпечено якість і надійність функцій, важливих для безпеки, а саме для підтримання:

— усіх аспектів, пов'язаних із проектом взаємозв'язків між КВК-системами;

— загальної інтеграції й уведення в експлуатацію розподілених функцій.

5.3.1.5 *Захист від ВЗП*

Метою проекту архітектури КВК є забезпечення заходів проти виникнення ВЗП усередині КВК-систем, які забезпечують різні ешелони захисту від одних і тих самих ПВП (див. 5.1.1). Ці заходи охоплюють:

— Проектні заходи захисту станції проти небезпечних подій. Внутрішні та зовнішні небезпеки (див. 5.1.3), які не обмежуються частиною архітектури КВК, можуть призвести до ВЗП;

— Заходи безпеки проекту проти відмов, які може бути спричинено змінеммями у вимогах до станції. Навантаження деякого устаткування, такого як підсилювачі потужності та реле або навантаження програмного забезпечення, наприклад такого, що здійснює накопичення вхідних даних, передавання даних, і перемикання експлуатаційних режимів, може залежати від подій, що відбуваються на станції;

— Заходи безпеки проекту, що мінімізують використання загальних ресурсів в архітектурі КВК та ІЛМ різних ліній захисту. Загальні ресурси можуть охоплювати використання унікальних вимірюваних сигналів або загальну реалізацію різних керівних дій;

— Заходи, що зменшують ризик через систематичні помилки. Для будь-якої КВК-системи є ризик проектних помилок або недоліків під час упровадження. Зокрема, можливість відмови програмного забезпечення через помилки не можна вилучити аналізуванням відмови будь-якої системи. Якщо одні й ті самі модулі програмного забезпечення використовуються в подібних умовах у різних комп'ютерних системах, є ризик ВЗП унаслідок помилок такого програмного забезпечення;

— Використання принципу різноманітності. Різноманітність забезпечує кілька різних шляхів визначення та реагування на значні події для збільшення рівня захисту від ВЗП. Типи різноманітності охоплюють: різноманітність людського чинника, сигнальну різноманітність (використання різних параметрів для ініціювання захисних дій), функційну різноманітність, проектну та випробувальну різноманітність, програмну різноманітність та різноманітність устаткування;

— Необхідні стратегічні рішення для обмеження складності. Використання комп'ютерів дає змогу застосовувати складніші алгоритми та процеси, ніж під час використання тільки технічних засобів. Для складніших вимог імовірність помилок та неточностей у технічному завданні та помилок під час проектування та впровадження є суттєво вищою, ніж для простих вимог.

5.3.1.5.1 Стійкість до внутрішніх і зовнішніх небезпек, що можуть призводити до ВЗП

Має бути вжито заходів для забезпечення виконання групами безпеки функцій категорії А, необхідних для того, щоб підтримати відповідну реакцію на внутрішні та зовнішні небезпеки. Ці заходи містять:

— розділення, наприклад розташування резервованих частин системи в різних приміщеннях;

— незалежність, наприклад, систем опалення, вентилювання та кондиціювання (СОВК) і джерел енергії для каналів та систем;

— попередження, наприклад, пожежі, хімічного забруднення та вібрації;

— проектування, наприклад, відповідність устаткування стандартам МЕК з електромагнітних перешкод;

— кваліфікація щодо навколишнього середовища, наприклад сейсмічних явищ (див. 6.4).

5.3.1.5.2 Захист від ВЗП унаслідок змінення вимог до станції

a) Треба визначити компоненти КВК-систем, що виконують функції категорії А, навантаження яких залежить від вимог. Треба оцінити можливість відмов або послідовність відмов (охоплюючи їхній вплив на елементи, навантаження яких не залежить від вимог) стосовно можливих джерел і наслідків ВЗП;

b) Ризик ВЗП у системах класу 1 треба зменшити використанням КВК-систем та систем підтримання, які однаково функціюють до, протягом або після змінення вимог до станції, тобто пристосовані до роботи незалежно від профілю вимог.

5.3.1.5.3 Захист за допомогою засобів проектування архітектури КВК та ІЛМ

a) Незалежні системи або підсистеми має бути забезпечено для різних ліній захисту від одних і тих самих ПВП (див. примітку 1 до 5.1.1). За використання загальних ресурсів вони мають відповідати рівню надійності, потрібної для групи безпеки;

b) Має бути забезпечено незалежні засоби для моніторингу й експлуатації функцій станції та систем, важливих для безпеки, так, щоб достатня інформація залишалася доступною для безпечної роботи станції після відмови, наприклад, мультиплексний канал передавання даних або комп'ютер;

c) Мають бути мінімізованими потенційні ВЗП у разі, якщо ручне управління використовують як резерв до автоматичного управління для функцій категорії А чи В;

d) Якщо одна функція категорії А може спричинити вмикання керівної системи безпеки, а інша функція категорії А, яку використовують за інших обставин, може спричинити її вимикання, треба виконати аналіз, щоб визначити, яка дія необхідна за відмови КВК-систем.

5.3.1.5.4 Захист від ВЗП, спричинених систематичними помилками

a) Високоякісне планування під час розробляння та виробництва різних КВК-систем, що належать до групи безпеки, має забезпечити запобігання невиявленим помилкам, щоб зробити ризик ВЗП усередині цих систем малоймовірним. Цей стандарт містить загальні положення, які треба використовувати для розроблення якісних КВК-систем різних класів;

b) Систематичні відмови потрібно виявляти за допомогою засобів самоконтролю (оброблення особливих ситуацій, вартовий таймер, перевірення достовірності) і за виявлення відмови система(-и), що відмовила, має перейти в заздалегідь визначений відмовобезпечний стан; й оператора має бути попереджено про відмову;

c) Якщо необхідна надійність безвідмовного приведення в дію функції безпеки вище, ніж надійність, прогнозована попереднім оціненням безвідмовного поводження системи, проект треба змінити.

Примітка 1. Потрібний ступінь захисту від відмов залежить від категорії виконуваних функцій.

Примітка 2. Цей підпункт призначено тільки для відома. Докладні вимоги до захисту від ВЗП унаслідок помилок програмного забезпечення для функцій категорії А надано в 4.1 IEC 60880-2.

5.3.1.5.5 Захист використанням різноманітності

a) Під час проектування архітектури КВК треба застосовувати принцип різноманітності, коли потрібна висока надійність для групи безпеки й особливо, коли є невизначеність в оціненні проекту;

b) Треба розглядати функційну і сигнальну різноманітність. Ці методи є ефективними для зменшення ризику ВЗП унаслідок помилок у технічному завданні або специфікації та в разі реалізації прикладного програмного забезпечення;

c) Різноманітність устаткування може бути ефективною від ВЗП апаратних компонентів і може забезпечувати захист від системних помилок програмного забезпечення. Зокрема її треба розглядати щодо складних систем, де обмежено досвід експлуатації;

d) Мають використовуватися різноманітні процедури або методи верифікації і валідації (наприклад, різноманітне устаткування під час експлуатаційних випробовувань, послідовні випробування із симулятором тощо). Це сприяє уникненню ВЗП без ускладнення системи, що може відбутися в разі використання інших видів різноманітності;

e) Якщо різноманітність використовують для забезпечення захисту від ВЗП, до проекту необхідно внести аналіз ефективності різних видів різноманітності, потрібних для мінімізації можливості ВЗП. Переваги та недоліки треба обґрунтовувати й документувати (див. 5.3.3).

5.3.1.5.6 Стратегічні рішення для обмеження складності

Для мінімізації можливості ВЗП у складних системах до процесу проектування архітектури КВК необхідно вмістити аналіз для демонстрації того, що ступінь застосовності комп'ютерів (див. примітку) порівняно з апаратними системами і ступінь дій людини є прийнятними для підтримання безпеки.

Примітка. Це може залежати від національного досвіду, нормативних положень і впевненості в комп'ютерній технології.

5.3.2 ***Функційне призначення***

Процес функційного призначення встановлює прийняті в 5.2 загальні вимоги до КВК ФСБ, важливих для безпеки, для конкретних систем КВК-архітектури. За потреби окремі функції можливо розкласти на деяку кількість підфункцій, що реалізуються в кількох системах. Усі функції або підфункції називають прикладними функціями КВК-систем (див. 6.1.1.1).

a) Функційне й експлуатаційне технічні завдання для прикладних функцій мають відповідати загальним вимогам до КВК ФСБ. Якщо функція реалізується більше ніж одною КВК-системою, ці взаємопов'язані системи треба компонувати так, щоб виконувалися загальні вимоги, визначені в 5.2;

b) До функційного й експлуатаційного технічних завдань для прикладних функцій мають входити всі додаткові функції перевірення, блокування та моніторингу, визначені у процесі проектування архітектури КВК, наприклад стан і режим роботи взаємопов'язаних систем, перевірення сигналів, отриманих від інших систем;

c) Присвоєння прикладних функцій системам треба узгоджувати з принципами, наведеними в таблиці 2, відповідно до класу системи та категорії функції;

d) Функції категорії А має бути призначено системам, які відповідають критерію одиничної відмови;

e) За призначення системам функції категорії А одної й тої самої групи безпеки треба брати до уваги заходи захисту від ВЗП, сформульовані в 5.3.1.5. Приклади призначеності функцій різних категорій зображено на рисунку С.1;

f) Присвоєння прикладних функцій системам має мінімізувати складність систем класу 1.

Примітка. Це найбільш значимо щодо нових станцій. У разі заміненння апаратних систем на комп'ютерні системи для них мають виконуватися такі самі вимоги до прикладних функцій, що для апаратних систем;

g) Надійність, що вимагається від кожної прикладної функції, реалізованій у системі, потрібно узгоджувати з граничними значеннями, охоплюючи ВЗП, визнаними реально досяжними.

5.3.3 ***Необхідний аналіз***

Треба виконати аналіз для перевірення проекту архітектури КВК і розподілення функцій між КВК-системами. Такий аналіз є ітераційним процесом і його потрібно виконувати спільно з процесом проектування (див. розділ 6).

5.3.3.1 *Оцінення надійності та захисту від ВЗП*

a) Треба виконати оцінення надійності функцій категорії А групи безпеки. Під час оцінювання треба враховувати залежність від загального забезпечення, наприклад електричного або пневматичного живлення та вентиляційного устаткування.

b) Оцінення може спочатку базуватися на розрахунковій надійності, досяжній для функцій різних систем, і її потрібно перевірити після завершення процесу проектування, беручи за основу оцінення надійності окремих систем (див. 6.1.3.1.2).

c) Треба виконати оцінення ефективності заходів, спрямованих на зменшення чутливості до ВЗП груп безпеки, що виконують функції категорії А.

d) Треба піддати аналізу проектну документацію систем (див 6.3.3), щоб визначити загальні або ідентичні компоненти апаратного чи програмного забезпечення, які підтримують різні функції групи безпеки, включно з функціями категорії А. Якщо в різних лініях захисту знайдено загальні або ідентичні елементи, треба надати обґрунтування того, що ймовірність ВЗП є низькою.

e) Немає загальновизнаного методу щодо кількісного оцінення ймовірності ВЗП, тому методи, які застосовують для оцінення, є по суті якісними (див. додаток С). Застосовні методи, наприклад метод бета-фактора для технічних засобів, має бути визначено на початку проектування.

Примітка 1. Мета зазначеної вище рекомендації — унеможливлення внесення пізніших змін у планування та проектування системи, у відповідь на змінення у вимогах, які через зроблені під час цього помилки можуть призвести до можливих ВЗП.

Примітка 2. Рівень деталізації аналізування ВЗП може залежати від категорії функцій, що виконують системи, і його треба обґрунтувати.

Примітка 3. Вимоги до аналізу ВЗП через програмне забезпечення наведено в 4.1.3 з IEC 60880-2.

Примітка 4. Оцінку потенційної можливості ВЗП можливо покращити в тому разі, якщо КВК-системи мають таку модульну структуру, що компоненти та компоновка системи можуть мати якісну оцінку за допомогою етапів верифікації і додатково, наскільки це можливо, кількісну оцінку.

5.3.3.2 *Оцінення чинника людини*

Верифікація проекту архітектури має охоплювати аналіз вимог до чинника людини для оптимізації проекту систем ІЛМ.

5.4 Загальне планування

У цьому підрозділі визначено вимоги до розроблення загальних планів для забезпечення того, щоб вимоги до КВК-функцій, важливих для безпеки, розподілених між КВК-системами, виконувалися протягом життєвого циклу цих систем.

Вимоги цього розділу координують і доповнюють плани, установлені в 6.2, для конкретних КВК-систем.

Примітка. Наведені нижче вимоги до планів не перешкоджають тому, що ці плани може бути організовано у вигляді різної кількості документів.

Загальні плани потрібно складати до початку робіт, яких вони стосуються.

5.4.1 *Загальні програми забезпечення якості*

У цьому стандарті передбачено, що програма забезпечення якості відповідає вимогам IAEA 50-C-QA (Rev.1), наявна як невід'ємна частина проекту АЕС і забезпечує управління дієвими елементами.

a) Програми забезпечення якості потрібно затверджувати та виконувати відповідно до розділу 2 IAEA 50-C-QA (Rev.1) для кожної роботи, пов'язаної з життєвим циклом безпеки КВК;

b) Програми забезпечення якості мають охоплювати всі роботи, необхідні для досягнення якості, і роботи, за допомогою яких перевіряють, що потрібний рівень якості було досягнуто (див. розділ 102 IAEA 50-C-QA (Rev.1));

c) Роботи з верифікації має бути визначено у планах верифікації. Плани верифікації охоплюють ресурси, процес і вихідні дані етапів життєвого циклу безпеки КВК та визначають:

— процедури та засоби для виконання верифікації;
— документацію, яку треба зберегти та перевірити;
— аспекти безпеки, які необхідно перевірити;
— процедури усунення відмов і несумісності;
— критерії завершення кожного етапу;
— мають бути підготовленими завершальні звіти, які демонструють відповідність вихідних даних етапу, вхідним вимогам та усуненню невідповідностей;

d) Програми забезпечення якості треба планувати та включати у загальну програму забезпечення якості проекту АЕС, і передбачені у них роботи має бути внесено до загального плану робіт проекту АЕС.

5.4.2 *Загальний план щодо безпеки*

Необхідні відповідні заходи щодо безпеки, щоб забезпечити захист інформації, яку обробляють у системах, важливих для безпеки, від несанкційованих змін (цілісність), несанкційованого доступу (роботоздатність) та несанкційованого розкриття (конфіденційність).

Примітка 1. Цілісність і недоступність домінують над конфіденційністю в КВК-системах атомних станцій.

Програмне забезпечення (програмний код, а також параметри та дані) може бути особливо вразливим у процесі проектування та технічного обслуговування. Треба розглянути загрозу навмисних змін, що призводять до помилкового поводження програмного забезпечення в цілому, або тих, що спричиняють певні обмеження часу або даних.

Примітка 2. Загрози, що виникають від ненавмисних змін, зазначають у технічному завданні на систему (див. 6.1.1.4).

Загальний план безпеки визначає процедурні та технічні заходи захисту архітектури КВК-систем від навмисних й усвідомлених нападів, які можуть піддати ризику виконання функцій, важливих для безпеки.

a) Вимоги безпеки функцій і систем, важливих для безпеки, має бути визначено у плані безпеки системи (див. 6.2.2);

b) Треба систематично контролювати ризик, що виникає за несанкційованого доступу та змін, протягом усіх етапів життєвого циклу від виникнення до усунення;

c) Умови безпеки системи мають бути такими, щоб вони суттєво не впливали на її надійність і роботоздатність;

d) Суворість вимог щодо безпеки для конкретної системи і пов'язаного з нею устаткування визначається функціями, які виконує система. До безпеки комп'ютерних систем, які виконують функції категорії А, застосовують вищі вимоги, ніж до безпеки систем, що виконують функції категорій В чи С;

e) Для безперервного підтримання безпеки систем на високому рівні треба розробити політику безпеки, визначену з урахуванням специфіки станції. До її складу мають входити процедури, пов'язані з інтерфейсом між адміністрацією й органом технічної безпеки, доступом до систем, аспектами безпеки обробляння даних, аспектами безпеки під час змінювання й технічного обслуговування, перевірянням безпеки, звітністю та тренуванням;

f) Системи, що виконують важливі для безпеки функції, мають бути фізично захищеними від несанкційованого доступу. Контроль за доступом має охоплювати ідентифікацію й аутентифікацію персоналу для систем, що виконують функції категорії А, та надійну ідентифікацію персоналу для систем, що виконують функції категорій В та С (див. 7.12 IAEA 50-SG-D3);

g) Стосовно систем, що виконують функції категорії А, не повинна передбачатися можливість віддаленого доступу (зовнішнього відносно станції). Якщо віддалений доступ передбачено всередині станції, треба проаналізувати та продемонструвати, що він не завдає додаткового ризику несанкційованого доступу до системи та додаткових джерел потенційно можливих відмов системи;

h) Доступ до систем треба зазначати у журналі, реєструючи персонал, тип доступу, час і виконувані дії;

i) Записи журналу, що стосуються захисту, треба офіційно інспектувати через певні проміжки часу для систем, що виконують функції категорії А, і періодично перевіряти для систем, що виконують функції категорії В та С.

5.4.3 ***Загальні плани інтеграції й уведення в експлуатацію***

Загальна інтеграція — це комбінація всіх передбачених на станції технічних й адміністративних дій для встановлення, з'єднання, випробування, калібрування та повного підготування КВК-систем до експлуатації.

Уведення в експлуатацію — це комбінація всіх передбачених на станції технічних й адміністративних дій, необхідних для гарантування придатності встановлених систем і станції до обслуговування перед тим, як вони розпочнуть функціювання (див. 4.4 IAEA 75-INSAG-3).

Примітка. Загальне введення в експлуатацію КВК-системи є частиною введення в експлуатацію АЕС (див. 3.11).

На завершальному етапі загальної інтеграції та введення в експлуатацію виконується валідація й інсталяція окремих систем (див. 6.1.5 та 6.1.6).

a) Після інтеграції КВК-систем на станції загальне функційне та експлуатаційне технічні завдання для функцій, важливих для безпеки, що виконуються КВК-системами, має бути перевірено в усіх передбачених режимах роботи станції;

b) Обсяг робіт, який треба виконати під час інтеграції й уведення в експлуатацію на загальному рівні, можливо зменшити, якщо комплексні випробування виконано на заводі або станції, або якщо АЕС не є першою станцією, на якій упроваджується ця система. Зменшення загальних робіт із верифікації та валідації треба обґрунтовувати й документувати.

5.4.3.1 *Загальний план інтеграції*

Треба розробити загальний план інтеграції КВК-систем у рамках програми забезпечення якості. До загальних вимог 5.4.1 із забезпечення якості та верифікації долучено наведені нижче технічні вимоги:

a) Випробування взаємопов'язаних систем потрібно виконувати для підтвердження того, що:
   — Усі інтерфейси взаємопов'язаних систем працюють правильно;
   — Виявлення відмов, коригувальні дії та надання відповідних даних виконується відповідно до технічного завдання КВК-функцій;

b) Випробування щодо несприйнятливості взаємопов'язаних систем до електромагнітних перешкод треба виконувати відповідно до вимог IEC 61000-4-1—IEC 61000-4-6;

c) Треба контролювати уземлення й еквіпотенційне з'єднання всього устаткування та захисного кабелю уземлення;

d) Для перевірення поводження та роботоздатності систем у разі переривання та відновлення електроживлення треба виконати їхнє випробування за умови втрати зовнішнього живлення;

e) Треба контролювати умови навколишнього середовища за місцем експлуатації КВК-систем на їхню відповідність установленим вимогам;

f) Треба виконати випробування безперервних і логічних сигналів, якими обмінюються системи, для того щоб підтвердити, що забезпечуються правильні значення та стани для різних функцій, важливих для безпеки. У разі коли функції відображення інформації, аварійної сигналізації, реєстрування й обчислення виконує система, яка є неважливою для безпеки, це випробування треба виконувати разом із цією системою, доки не буде розроблено простіший метод демонстрації правильності всіх отриманих даних;

g) Функції управління із замкнутим контуром та функції логічного управління треба випробовувати від вхідних до вихідних сигналів, включно з виконавчими механізмами й інтерфейсом оператора;

h) Випробування мають підтвердити, що в разі відмови резервного устаткування, комунікаційних ліній, датчиків або керівних приводів, кожну систему буде забезпечено правильною інформацією. Випробування мають підтвердити правильність перемикання режимів управління та часових характеристик;

i) Необхідно виконати випробування багатоканального управління для перевірення правильності передавання даних і часу реакції від моменту подавання команд до отримання достовірної інформації про стан приводів. Випробування потрібно виконувати за нормальних робочих умов, аварійних умов, найгірших умов і в умовах імітації відмови технічних засобів.

5.4.3.2 *Загальний план уведення в експлуатацію*

Треба розробити загальний план валідації КВК ФСБ у рамках програми введення в експлуатацію систем станції (див. **4.4**.200 IAEA 75-INSAG-3). Застосовують наведені нижче вимоги:

a) Задані уставки, граничні значення та калібрувальні значення вимірювальної апаратури треба перевірити та відрегулювати під час уведення в експлуатацію систем станції для підтвердження того, що функційність і робочі характеристики систем відповідають загальному технічному завданню;

b) Експлуатаційні процедури КВК-систем треба перевірити й оновити під час уведення станції в експлуатацію.

5.4.4 ***Загальний план експлуатації***

Загальний план експлуатації відповідає експлуатації взаємопов'язаних КВК-систем. Загальний план експлуатації доповнює плани експлуатації окремих КВК-систем (див. 6.2.6).

Загальний план експлуатації треба розробляти в рамках програми забезпечення якості. На додаток до загальних вимог 5.**4**.1 до забезпечення якості та верифікації застосовують наведені нижче вимоги:

a) План має містити опис:

— засобів запуску, ініціалізації та підтримання взаємопов'язаних систем у повному робочому стані;

— засобів перевірення того, що системи здатні виконувати функції, важливі для безпеки;

— стандартних операцій, наприклад періодичних випробувань, які треба виконувати під час роботи станції для підтримання необхідної надійності функцій, важливих для безпеки;

b) У плані має бути визначено умови, за яких може виконуватися модифікація параметрів системи або управління, та вплив цих змін на роботу систем і на роботу та безпеку станції. У ньому також має бути зазначено, які модифікації можуть виконуватися:

— за адміністративного управління;

— за адміністративного управління та після затвердження розробником відповідних випробувань та верифікації.

Примітка. Процес модифікації і дозвіл на ці зміни наглядових органів можуть залежати від норм експлуатаційної організації та національних норм;

c) У плані має бути визначено всі режими експлуатації взаємопов'язаних систем, а також те, як ці системи мають працювати в кожному режимі, охоплюючи:

— необхідні дії й обмеження в роботі систем та станції в разі відмови системи або зовнішньої небезпеки для систем;

— обмеження в роботі систем та станції під час періодичних випробовувань, технічного обслуговування та/або виконання модифікацій;

— процедури приведення до нормальної експлуатації та підтвердження виходу в нормальний робочий режим після скасування цих обмежень.

5.4.5 ***Загальний план технічного обслуговування***

Загальний план технічного обслуговування призначено для технічного обслуговування на рівні взаємопов'язаних КВК-систем. Він доповнює та координує плани технічного обслуговування окремих КВК-систем (див. 6.2.7).

Загальний план технічного обслуговування треба розробляти в рамках програми забезпечення якості. На додаток до загальних вимог 5.**4**.1 із забезпечення якості та верифікації використовують наведені нижче вимоги:

a) Треба ввести обмеження на заходи з технічного обслуговування окремих КВК-систем, щоб мати гарантію того, що будь-який вплив на безпеку станції є припустимим. Зокрема, системи мають

задовольняти критерій одиничної відмови під час технічного обслуговування там, де це потрібно (див. 6.1.1.2.5). У плані має бути визначено, яке устаткування можливо вивести з роботи, наслідки цього та засоби, які забезпечують повернення до роботи та верифікацію правильності повернення;

b) Треба виконувати систематичні випробування та заміни для того, щоб ВЗП була малоймовірною в тих елементах КВК-архітектури, які опиняються в змінених умовах навколишнього середовища в разі аварії. Методика має гарантувати, що ті елементи, які піддаються радіації і, унаслідок цього, швидкому старінню або зміненням фізичних властивостей (кабелі, датчики), або навантаження яких змінюється відповідно до виконуваного завдання (наприклад, вмикання підсилювачів потужності, реле), не можуть призвести до невиявлених відмов.

Примітка. Проміжки між замінами можна визначати за допомогою прискореного старіння;

c) У разі, коли заходи з технічного обслуговування містять коригування даних конфігурації або калібрування, ними також потрібно управляти за допомогою документально встановлених процедур, які забезпечують, що:

— коригування під час технічного обслуговування відбувається в певних межах (такі межі можна установлювати на основі проекту системи та проекту станції у вигляді неформальних обмежень щодо персоналу, який виконує технічне обслуговування);
— застосовуються вимоги 5.4.4, викладені вище, у разі виконання такого коригування під час роботи системи;
— виконується реєстрація всіх коригувань, виконаних під час технічного обслуговування.

5.5 Вихідна документація

Вихідна документація проекту архітектури КВК та процесів розподілу функцій забезпечує необхідні вхідні дані для технічного завдання до конкретних систем КВК-архітектури (див. 6.1.1).

5.5.1 *Документація проекту архітектури*

a) Вихідна документація має визначати для конкретних КВК-систем:
— проектні обмеження, які визначають на станції (див. 5.1.3);
— обмеження, які визначають у проекті архітектури (див. 5.3.1);
— фізичні й функційні границі між системами;

b) Для інженерних інструментальних засобів, які використовують, треба визначити:
— як проектні дії життєвого циклу системи підтримуються такими засобами;
— як потрібно використовувати такі засоби; і
— як перевірити вихідні дані таких засобів.

Примітка. Вимоги до методів й інструментальних засобів інженерного програмного забезпечення для систем класу 1 наведено в 4.2 та 4.3 IEC 60880-2.

5.5.2 *Документація функційної призначеності*

a) Вихідна документація має визначати вимоги до функціювання, характеристик і надійності виконання прикладних функцій, установлених для кожної системи (див. 5.3.2). Вимоги може бути подано за допомогою тексту, діаграм послідовності операцій, матриць, логічних діаграм тощо, які чітко виражають виконання функцій;

b) Технічні завдання для прикладних функцій комп'ютерних систем не повинні залежати від технології їхньої реалізації, тобто комп'ютерів, реле;

c) Програмне забезпечення та інженерні методи й інструментальні засоби потрібно використовувати для того, щоб створити документи з вимогами, які можуть бути легко зрозумілими для авторів технічних завдань на систему та операторів станції.

6 ЖИТТЄВИЙ ЦИКЛ БЕЗПЕКИ СИСТЕМИ

Проект КВК-архітектури визначає конкретні КВК-системи, які виконують функції, важливі для безпеки (див. 5.3.1). Цей розділ визначає завдання та вимоги до окремих таких КВК-систем. Вимоги цього розділу належать до комп'ютерних систем.

Примітка. Більшість цих вимог можливо також застосовувати до традиційних КВК-систем.

Для забезпечення того, що всі вимоги безпеки, які висувають до системи, виявлено, реалізовано та підтримано, необхідно застосовувати системний підхід. Цього можна досягти за допомогою діяльності, пов'язаної з розробленням, реалізацією й експлуатацією системи в рамках життєвого

циклу безпеки системи. Цей життєвий цикл відповідає у свою чергу діяльності в рамках повного життєвого циклу безпеки КВК (див. розділ 5 та рисунок 4).

Етапи типового життєвого циклу безпеки системи охоплюють:

— специфікацію вимог до системи;

— специфікацію системи;

— детальний проект і реалізацію системи;

— інтеграцію системи;

— валідацію системи;

— інсталяцію системи;

— модифікації проекту системи (якщо є).

Кваліфікацію системи розглядають окремо, тому що її можна виконувати частково незалежно від життєвого циклу розроблення системи. Такий підхід відповідає практиці, яка все більше покладається на наявне устаткування.

На рисунку 5 зображено типовий життєвий цикл безпеки системи та зазначено взаємозв'язки між життєвими циклами програмного забезпечення й технічного забезпечення з IEC 60880 та IEC 60987.

У таблиці 3 наведено короткий огляд мети діяльності, вхідних і вихідних даних типового життєвого циклу системи, а також наведено посилання на відповідні підрозділи.

До цього розділу належать:

— вимоги, що однаково застосовують до всіх систем, важливих для безпеки;

— вимоги, що застосовують додатково до попередніх вимог, до певних класів систем або категорій функцій. Специфічні вимоги наведено в таблиці 4.

Життєвий цикл системи є ітераційним процесом; етап може розпочатися до того, коли дії попереднього етапу буде завершено; проте етап можна вважати завершеним тільки в тому разі, якщо попередні етапи завершено та якщо його вихідні дані відповідають вхідним даним, отриманим із попередніх етапів.

Примітка. Ця вимога відрізняється від вимоги, сформульованої в 6.1 IEC 60880. Щодо програмного забезпечення — не вважають за потрібне, хоча бажано, завершення попереднього етапу проектування до того, як розпочато наступний етап, що забезпечує вимоги, описані вище.

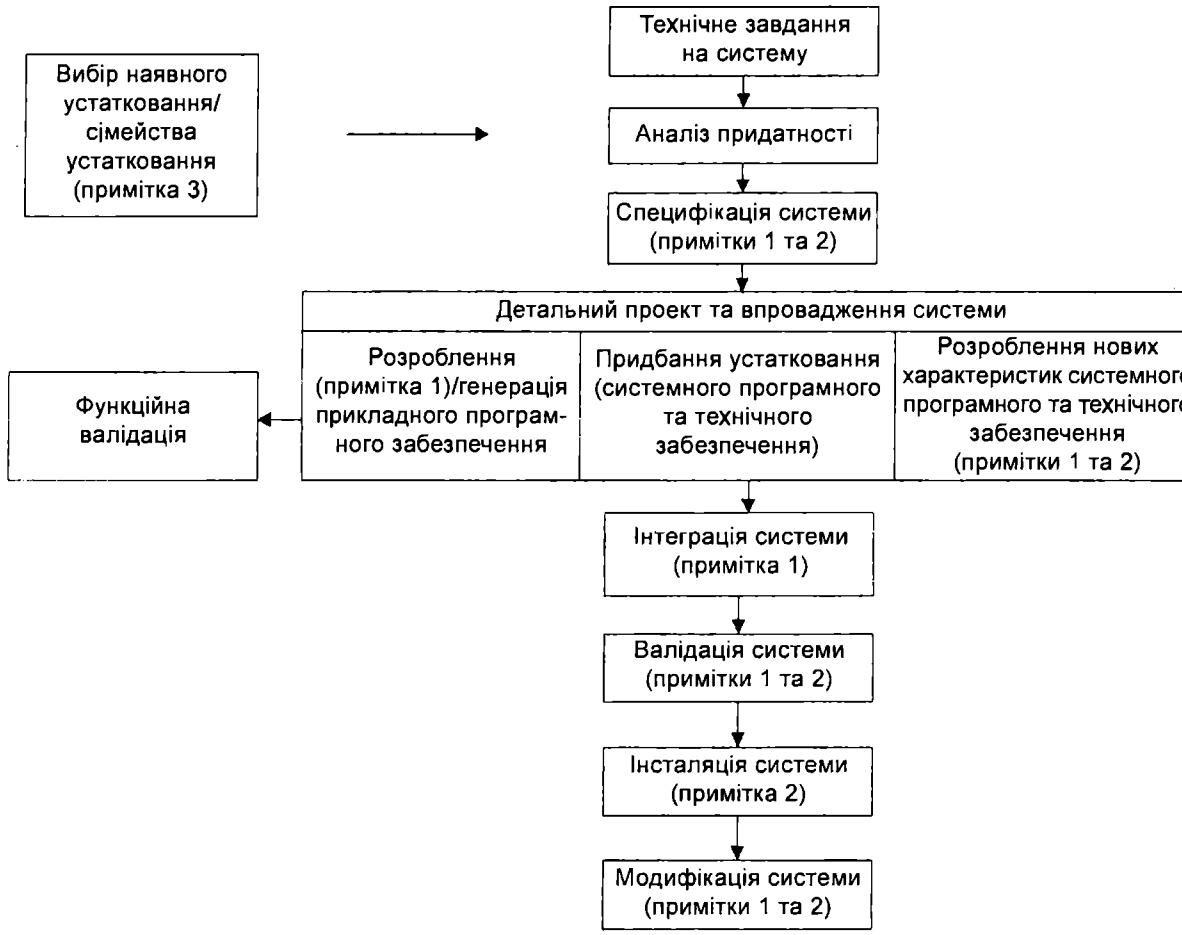
Таблиця 3 — Огляд життєвого циклу безпеки системи

Розділ або підрозділ	Вхід	Мета діяльності	Вихід
6	Вимоги до життєвого циклу системи та їхній зв'язок із повним життєвим циклом безпеки		
6.1.1 Технічне завдання на систему	Вихід згідно з 5.5 та 5.4 Вихід згідно з 6.2.1 та 6.2.2	Розробити технічне завдання до системи стосовно: — функцій; — проектних обмежень; — границь й інтерфейсів з іншими системами та інструментальними засобами; — інтерфейсів із персоналом; — умов навколишнього середовища	Технічне завдання на систему Технічне завдання до прикладних функцій
6.1.2 Специфікація системи	Вихід згідно з 6.1.1 Документація наявного устаткування, яке можливо використовувати Вихід згідно з 6.2.1 та 6.2.2	Визначити й оцінити придатність наявного устаткування, яке може бути інтегровано в проект системи Розробити проект архітектури системи для реалізації технічного завдання на систему Призначити підсистемам прикладні функції	Документація специфікації системи (див. 6.3.2) охоплює: — ідентифікацію вибраного устаткування й аналіз придатності; — архітектуру системи; — специфікацію програмного забезпечення

Кінець таблиці 3

Розділ або підрозділ	Вхід	Мета діяльності	Вихід
6.1.3 Детальний проект та впровадження системи	Вихід згідно з 6.1.2 Вихід згідно з 5.1.1 Вихід згідно з 6.2.1 та 6.2.2	Розширити й удосконалити проект архітектури Розробити технічне та системне/прикладне програмне забезпечення Виконати валідацію вимог до прикладних функцій	Документація детального проекту системи (див 6.3.3) Функційна валідація й оцінення надійності (див. 6.1.3.1) Підсистеми й компоненти технічного та програмного забезпечення
6.1.4 Інтеграція системи	Вихід згідно з 6.1.3 Вихід згідно з 6.2.1, 6.2.2 та 6.2.3	Компонування окремих технічних та програмних компонентів, з яких складено систему	Звіт з інтеграції Інтегрована система
6.1.5 Валідація системи	Вихід згідно з 6.1.2 та 6.1.4 Вихід згідно з 6.2.1, 6.2.2 та 6.2.4	Валідація специфікації системи	Звіт із валідації системи
6.1.6 Інсталяція системи	Вихід згідно з 6.1.5 Вихід згідно з 6.2.1, 6.2.2 та 6.2.5	Інсталяція та випробування системи	Звіт з інсталяції Систему інстальовано та випробувано на станції
6.1.7 Модифікації проекту системи	Запит на модифікацію (якщо є) Вихід згідно з 6.2.1, 6.2.2 та 6.2.7	Виконати коригування, поліпшення чи адаптацію системи	Звіти з модифікації; Систему змінено
6.2 Планування системи	Вихід згідно з 5.4 та 6.1	Розробити план валідації, план інсталяції, план експлуатації та технічного обслуговування, план захисту	Плани системи
6.4 Кваліфікація системи	Вихід за 6.2.1 та 6.2.2	Розробити план кваліфікації	Документація з кваліфікації

Примітка. Для порівняння цього визначення етапів з IEC 61508-2 див. додаток D.



Примітка 1. Для систем класу 1 вимоги до програмного забезпечення цього виду діяльності визначено IEC 60880.
Примітка 2. Для систем класу 1 вимоги до технічного забезпечення цього виду діяльності визначено IEC 60987.
Примітка 3. Для систем класу 1 вимоги до розробленого раніше програмного забезпечення цього виду діяльності визначено IEC 60880-2.

Рисунок 5 — Життєвий цикл безпеки системи

6.1 Вимоги

Цей підрозділ визначає вимоги до життєвого циклу безпеки системи.

Ці вимоги охоплюють властивості, які стосуються:

— певних функцій, призначених системі у процесі функційного призначення;

— загальних характеристик, які згідно з класифікацією системи визначають її придатність до виконання функцій, важливих для установлених категорій безпеки.

Примітка. Розділ 8 IEC 61226 містить основні вимоги до КВК ФСБ та спеціальні вимоги до різних категорій КВК ФСБ. Такі вимоги беруть до уваги в цьому стандарті за розроблення вимог до систем або функцій відповідно.

6.1.1 *Технічне завдання на систему*

Метою цього етапу є забезпечення високого рівня опису вимог до системи незалежно від прийнятого технічного рішення.

Вихідна документація, що описує архітектуру КВК та функційне призначення (див. 5.5), є вхідними даними для технічного завдання на системи.

Вихідною документацією цього етапу є базовий документ, який застосовують для комунікації між тим, хто встановлює завдання, та тим, хто буде реалізовувати технічне рішення.

Технічне завдання на систему має встановлювати:

— функції системи;

— проектні обмеження;

— межі та взаємозв'язки з іншими системами;

— інтерфейс із персоналом;
— умови навколишнього середовища;
— необхідну кваліфікацію.

6.1.1.1 *Функції*

До вимог, які розглядають, належать вимоги до конкретних прикладних функцій і сервісних функцій системи. Застосовують наведені нижче:

6.1.1.1.1 Прикладні функції

Технічне завдання до прикладних функцій, важливих для безпеки, визначають у процесі функційного призначення (див. 5.5.2).

a) Технічне завдання до кожної прикладної функції має встановлювати:

1) функційність, охоплюючи діапазон вводу/виводу та уставки. Стосовно функцій відімкнення технічне завдання визначає припустимі розбіжності між уставками та прийнятним значенням (охоплюючи всі невизначеності через помилки калібрування чи похибки вимірювальної апаратури);
2) робочі характеристики, охоплюючи точність та час реагування. Якщо це можливо, вимоги до робочих характеристик визначають для різних початкових умов станції та постульованих вихідних подій.

Примітка. IEC 61069-2 [6] може бути корисним під час ідентифікації та визначання критеріїв щодо робочих характеристик;

b) Технічне завдання до кожної прикладної функції має встановлювати її категорію та незалежність від інших функцій у групі безпеки. Такі вимоги стосуються встановлення якісних вимог до надійності функцій.

Процес функційного призначення визначає для кожної категорії функцій мінімальний клас КВК-системи. Разом із вимогами незалежності між функціями в одній групі безпеки (критерій одиничної відмови, захисний проект проти ВЗП) такі чинники дають змогу якісно оцінити надійність функції або групи функцій у групі безпеки.

Кількісна оцінка надійності прикладних функцій може знадобитися для верифікації проекту системи та базового проекту станції (див. A.2.2 IEC 60880). Це оцінення зазвичай виконують щодо проекту технічного забезпечення системи, де наявні добре перевірені методи, однак немає загальновизнаного методу щодо кількісної оцінки надійності програмного забезпечення (див. 6.1.3.1.2).

6.1.1.1.2 Сервісні функції

Сервісні функції на відміну від прикладних функцій безпосередньо не стосуються виконання функцій процесу, але належать до певних дій системи, потрібних, наприклад, для конфігурації, валідації, кваліфікації, інсталяції, уведення в дію, експлуатації, періодичних випробувань, технічного обслуговування, унесення проектних змін і захисту.

Технічне завдання до сервісних функцій визначається специфікатором системи. Точність вимог до таких функцій визначають у кожному конкретному випадку. У деяких випадках це визначено в специфікації системи та на стадії проектування архітектури після вибору необхідних технічних рішень для апаратного та програмного забезпечення.

У вимогах до сервісних функцій треба враховувати взаємодію й обмеження, передбачені планами системи (див. 6.2).

Примітка. Наприклад, контроль за зміненням параметрів має відповідати умовам, передбаченим планом захисту системи (див. 6.2.2), планом експлуатації системи (див. 6.2.6) і планом технічного обслуговування системи (див. 6.2.7).

6.1.1.1.3 Функції системного програмного забезпечення

Зазвичай технічне завдання на систему не розглядає функції системного програмного забезпечення в явному вигляді. Ці функції, пов'язані з експлуатацією та самоконтролем системи, визначають для наявного устаткування (див. 6.1.2.1) і їх може бути краще визначено на стадії специфікації системи. Проте вимоги до системного програмного забезпечення в неявному вигляді визначаються вимогами до прикладних функцій та вимогами до проектних обмежень системи (див. 6.1.1.2.1).

Треба чітко визначити вимоги до функцій системного програмного забезпечення, якщо системне програмне забезпечення вперше розроблено або придбано.

6.1.1.2 *Проектні обмеження*

Наведені нижче вимоги визначають обмеження під час вибирання можливих рішень щодо проекту системи та призначення функцій системи. Обмеження залежать від класу системи та категорії функцій і їх треба враховувати в специфікації системи та проекті архітектури для того, щоб:

— задовольняти вимоги, пов'язані з категоріями прикладних функцій;

— забезпечувати передбачене функціювання системи;

— забезпечувати або сприяти демонстрації правильної роботи системи.

6.1.1.2.1 Архітектура системи

Архітектуру системи обумовлено категоріями функцій, що виконуються цією системою (див. 5.3.2) і концепцією глибокоешелонованого захисту (див. 5.2 та 7.8.1 IAEA-50-SG-D3).

a) Система може виконувати функції найвищої категорії, які дозволено для її класу (див. 5.3.2), і функції нижчих категорій. Система може охоплювати підсистеми нижчих класів за умови виконання таких вимог:

1) проектні вимоги для кожної підсистеми не повинні бути нижчими, ніж вимоги до функцій найвищої категорії, що виконує ця підсистема;
2) проект системи має забезпечувати виконання вимог до підсистем або устаткування вищих класів у разі відмови устаткування нижчих класів;

b) Проект системи повинен мати у своєму складі резервування або інші заходи для забезпечення стійкості до відмов (див. 6.1.2.2.3) та для забезпечення призначення прикладних функцій, важливих для безпеки (див. 6.1.2.4).

Примітка. Система може передбачати резервування для виконання вимог до готовності. Необхідність резервування визначають на рівні проектування системи;

c) Проект системи має задовольняти вимоги незалежності (див. 6.1.2.2.2) щодо:

— запобігання поширенню відмов від систем, менш важливих для безпеки;

— запобігання поширенню відмов між резервними каналами, що реалізують функції категорії А;

d) Проект систем класу **1** має забезпечувати резервування, що дає змогу задовольняти критерій одиничної відмови для функцій категорії А під час експлуатування та технічного обслуговування (див. 6.1.2.4 e)).

Примітка. Відмови програмного забезпечення є систематичними та невипадковими. Тому критерій одиничної відмови не можна застосовувати до проекту програмного забезпечення системи так, як його застосовують до проекту технічного забезпечення. Можливі наслідки ВЗП, спричинених програмним забезпеченням усередині кожного рівня захисту та між резервованими рівнями, треба враховувати на рівні кожної системи та архітектури КВК (див. 4.1.1 з IEC 60880-2).

6.1.1.2.2 Внутрішня поведінка системи

a) Проект комп'ютерної системи має забезпечувати детерміністичну поведінку, що відповідає вимогам до робочих характеристик виконуваних функцій.

Примітка 1. Зауважимо, що комп'ютерна система має детерміністичну поведінку, якщо затримання часу між збудженням і відповіддю має гарантований максимум і мінімум за всіх необхідних умов (визначення, отримане з [4]);

b) Технологію передавання даних має бути вибрано так, щоб задовольняти вимоги робочих характеристик під час завантажування всіх даних, що генеруються за прогнозованих перехідних процесів станції (охоплюючи лавину змін стану в разі загальної втрати живлення);

c) Для забезпечення високого ступеня надійності детерміністичної поведінки системи класу **1** потрібно розробляти за методикою, зазначеною в додатку B IEC 60880 (а саме B.2.d — щодо часу виконання та B.2.e — щодо переривання). Методи, які використовують статичну послідовність дій (див. примітку 2), є такими, яким надають перевагу, порівняно з використанням переривань.

Примітка 2. Статичність визначають як те, що стосується події або процесу, який відбувається поза участю комп'ютерної програми (IEEE 610). Тому за статичної послідовності дій порядок виконання інструкцій не залежить від роботи комп'ютера — хоча може бути кінцеве число різних послідовностей дій залежно від шляху виконання.

Примітка 3. Див. розділ 1 IEC 60880, що стосується значення додатків у стандарті та настанов, якщо практика відрізняється від зазначеного в додатках;

d) Системи класу 2 може бути розроблено за технологіями, відмінними від передбачених у в). У таких випадках проект системи має забезпечувати відповідну роботу системи щодо всіх передбачених умов станції;

e) Для збільшення спроможності систем класів 1 та **2** витримувати непередбачувані стани:

— треба обґрунтувати відповідний набір проектних обмежень для використання ресурсів (таких як: потужність центрального процесора, пам'ять, пропускна здатність обміну даними, ресурси операційної системи) і внутрішню синхронізацію системи;

— треба передбачити засоби контролю будь-яких відхилень від детерміністичної поведінки та відновлення нормального стану станції в разі тимчасових втрат вхідної інформації, наприклад охоронний таймер, циклічне поновлення для змінення стану, активованого виявленням подій на станції.

6.1.1.2.3 Самоконтроль і стійкість до відмов

a) Системи має бути спроектовано так, щоб помилки та відмови виявлялися в достатньо ранній період для збереження потрібної готовності системи до роботи. Виявлення відмов за допомогою елементів самоконтролю устаткування має бути збалансовано з упровадженою складністю системи. По можливості треба дотримуватися вимог 4.8 та A.**2**.8 IEC 60880 щодо самоконтролю для систем кожного класу;

b) Для того щоб оператори станції мали можливість виконувати відповідні коригувальні дії, треба їх забезпечити достатньою, своєчасною, належно виділеною діагностичною інформацією про відмови;

c) Проект системи має передбачати можливість безпечного переходу до відповідного резервного режиму роботи в разі виявлення відмов (поступову деградацію);

d) Для систем класу 1 елементи самоконтролю мають відповідати IEC 60880 та IEC 60987.

6.1.1.2.4 Перевірюваність

a) Системи має бути обладнано засобами тестування, які виконують перевіряння їхньої спроможності виконувати свої функції, важливі для безпеки.

Примітка 1. Згідно з МАГАТЕ (див. 4.12 IAEA 50-SG-D8) під час тестування найкращими вважаються загальні перевірення, починаючи від входу датчиків до впливу на виході, але тестування, які частково перекриваються, також припустимі. Зокрема, тестування стосуються наведені нижче моменти:

a) зміни стану або значення будь-якого вхідного сигналу та спостереження за змінами на приймальному устаткованні;

b) переривання передавання та підтвердження того, що приймальне устаткування спроможне це виявити та вжити необхідних заходів;

c) перевірення та калібрування датчиків (див. 7.10.2 IAEA 50-SG-D3);

d) перевірення дій на виході (див. 7.10.3 IAEA 50-SG-D3);

b) Проміжки між перевіреннями має бути регламентовано у планах експлуатації та технічного обслуговування системи (див. 6.**2**), які базуються на потрібній надійності функцій (див. 4.5 IAEA 50-SG-D8), надійності устаткування та передбачуваних діапазонах похибки калібрування;

c) Якщо інтервали випробувань є такими, що потрібне періодичне тестування системи під час експлуатування, до проекту системи треба залучити устаткування для тестування та калібрування, яке дає змогу виконувати такі випробування під час експлуатування.

Примітка 2. Використання автоматичного устаткування сприяє виконанню періодичних випробувань. Цей тип устаткування здатен уводити змодельовані вхідні сигнали, реєструвати результівні вихідні стани та порівнювати результати спостереження з передбачуваними результатами;

d) Проект систем класу 1 та їхні випробувальні заходи мають бути такими, щоб забезпечити безпеку станції під час випробовування та мінімізувати помилковий запуск будь-якої захисної дії та будь-який несприятливий вплив випробування на роботоздатність станції. Метод тестування має мінімізувати час, на який канал захисту виводиться для обслуговування.

6.1.1.2.5 Ремонтопридатність

a) Систему треба проектувати так, щоб полегшити технічне обслуговування і в разі відмови легке діагностування, безпечне відновлення або заміну та повторне калібрування (див. 4.5 IAEA 50-SG-D8);

b) Треба враховувати здібності й обмеження людини, пов'язані з чинниками навколишнього середовища, для зменшення ризику та завантаженості персоналу під час технічного обслуговування;

c) Систему має бути спроектовано так, щоб повторне калібрування системи після ремонту підтверджувало його правильність. Потрібно охоплювати перевіренням:

— правильне відновлення нерозривності ланцюгів;

— правильне калібрування аналогових вимірювань та всіх відповідних порогових значень сигналу тривоги;

— спроможність системи виконувати регламентовані функції, важливі для безпеки.

Примітка. Вимоги до перевірення та технічного обслуговування в розділі 10 IEC 60987 застосовують до комп'ютерних систем, важливих для безпеки. Підрозділи IAEA 50-SG-D3: 7.10 (Перевірюваність), 7.11 (Експлуатаційні байпаси) та 7.12 (Контроль доступу) застосовують до комп'ютерних систем класу 1. Підрозділи IAEA 50-SG-D8: 4.5 (Перевірюваність) та 4.6 (Ремонтопридатність) — застосовують до комп'ютерних систем класу 2.

6.1.1.3 *Границі та взаємодія з іншими системами й засобами*

Для забезпечення інтеграції системи в КВК-архітектуру треба регламентувати наведену нижче інформацію згідно з відповідними вимогами розділу 5:

— передбачуване розміщення та фізичні обмеження, пов'язані з установленням системи на станції (див. 5.1.3);

— фізичні та функційні інтерфейси системи з допоміжними системами й устаткованням (див. 5.1.3);

— фізичні та функційні інтерфейси системи з іншими системами й устаткованням, з якими відбувається обмін інформацією (див. 5.3.1.3);

— інтерфейси з програмними інструментальними засобами, які використовують для визначення обміну даними між системами, і перевірення узгодженості цих даних (див. 5.3.1.4).

6.1.1.4 *Інтерфейси з користувачами*

Вимоги до ІЛМ мають гарантувати, що ризик людської помилки мінімізовано, наприклад, помилки через неуважність, промахи, недогляди, помилки під час установлювання, експлуатування, перевірювання і технічного обслуговування системи та станції або під час внесення змін у проект.

Примітка. Захист від навмисних змін має бути описано в плані забезпечення захисту (див. 6.2.2).

6.1.1.5 *Умови навколишнього середовища*

Треба визначити діапазони нормальних і граничних умов навколишнього середовища, які система має витримувати відповідно до обмежень, що походять зі стану станції (див. 5.1.3). Визначені умови навколишнього середовища охоплюють:

— зовнішні умови, а саме температуру, вологість, тиск, випромінення й електромагнітні перешкоди під час нормального експлуатування й аварійних умов.

Примітка 1. Зовнішні умови для ЕМП визначають згідно з IEC 61000-4-1—IEC-61000-4-6;

— зовнішні умови внаслідок потенційних зовнішніх небезпек для системи, охоплюючи сейсмічні умови;

— умови електроживлення та відведення тепла.

Примітка 2. Вимоги до електроживлення КВК-систем, важливих для безпеки, визначають згідно з IEC 61225.

6.1.1.6 *Кваліфікація*

Системи класів 1 або 2 мають пройти кваліфікацію. Для комп'ютерних систем кваліфікація охоплює технічні засоби, системне програмне забезпечення та прикладне програмне забезпечення, сполучене з технічними засобами (див. 6.4).

6.1.2 ***Специфікація системи***

Завдання цього етапу — забезпечення докладного опису архітектури технічного та програмного забезпечення системи, точне визначення устаткування, яке використовують або розробляють для її реалізації, та призначення прикладних функцій.

Специфікація вимог до системи та документація щодо наявного устаткування належить до специфікації системи.

Вихідна документація на цьому етапі (див. 6.3.2) формує вхідні дані для діяльності, у процесі якої реалізується об'єднання технічного та програмного забезпечення під час наступних етапів життєвого циклу системи.

Відповідно до розділу А.1 IEC 60880 цей етап охоплює діяльність, потрібну для формування вимог до програмного забезпечення, вимог до технічного забезпечення та вимог до інтеграції системи.

Специфікація системи має визначати:

— устаткування, що використовують;

— архітектуру системи;

— вимоги до програмного забезпечення;

— призначення прикладних функцій у підсистемах.

6.1.2.1 *Вибір наявних компонентів*

Зазвичай наявне устаткування (окремі компоненти програмного та технічного забезпечення або компоненти сімейства устаткування) застосовують для реалізації частини системи або всієї «нової» системи.

Примітка 1. Наявні компоненти можуть бути стандартною серійною продукцією («ССП») або власною продукцією виробника.

Примітка 2. У 4.3 IEC 60880-2 наведено критерії приймання наявного програмного забезпечення, яке використовують для виконання функцій категорії А.

a) Треба виконати оцінення придатності відібраних компонентів, щоб продемонструвати відповідність характеристик устаткування технічним завданням на систему;

b) Аналіз й оцінення придатності відібраних компонентів має ґрунтуватися на порівнянні двох комплектів документів: технічних завдань на систему та документації на наявні компоненти. Остання охоплює специфікацію виробу і (якщо є) звіти із кваліфікації;

c) Застосовують наведені нижче вимоги:

— подана документація має чітко визначати функційність і властивості всіх компонентів.

Примітка. Це охоплює час виконання та необхідний обсяг пам'яті компонентів програмного забезпечення, інтенсивність відмов компонентів, умови навколишнього середовища для конфігурації системи, вимоги до монтажу в шафах, до монтажу кабелів та під'єднання до електроживлення, споживання електроенергії, сервісні засоби;

— властивості, які чітко не зазначено, треба визначити за допомогою аналізу або випробування;
— документація має містити визначену надійність і характеристики прикладних функцій станції за очікуваної конфігурації(-ій) компонентів;
— документація має визначати функційність і властивості тих методів й інструментальних засобів, які застосовують у розробленні програмного забезпечення;
— треба визначити функції, які не виконуються системою (тобто функції устаткування, які передбачені, але не застосовуються). Треба продемонструвати неможливість впливу цих функцій на необхідні функції.

d) У разі виявлення невідповідностей між технічним завданням на систему та специфікацією до сімейства устаткування, що призводить до непридатності устаткування системи конкретного класу, устаткування має бути визнано непридатним. Оцінення придатності має встановити відповідність специфікації вибраного устаткування його призначенню, визначеному в технічному завданні на систему (див. 6.3.2.2);

e) Щодо систем класів 1 та 2 необхідно перевірити кваліфікацію відповідно до вимог 6.4;

f) За потреби попередньої кваліфікації треба чітко визначити властивості, які потрібно оцінити під час кваліфікації. Також треба ідентифікувати всі додаткові роботи з кваліфікації на станції.

6.1.2.2 *Архітектура системи*

Архітектуру системи можна поділити на ряд взаємопов'язаних підсистем і компонентів з урахуванням вимог до резервування та реконфігурації. Метою розподілення системи є досягнення оптимально простого компонування технічного та програмного забезпечення, що задовольняє функційні та експлуатаційні вимоги, та відповідає вимогам до надійності та ремонтопридатності.

Компонування підсистем у системі має:

— задовольняти проектні обмеження 6.1.1.2;
— ураховувати вимоги до функційного призначення прикладних функцій (див. 6.1.2.4);
— відповідати вимогам до надійності прикладних функцій, важливих для безпеки (див. 6.1.1.1.1).

6.1.2.2.1 Територіальне розташування підсистем (централізоване/децентралізоване)

a) Під час визначання територіального розміщення підсистем на станції та шляхів передавання даних між підсистемами треба враховувати наведені нижче чинники:

— розділення резервованих каналів більшості устаткування може бути необхідним для зменшення впливу локальних ризиків, таких як пожежа, і відповідності критерію одиничної відмови (див. 6.1.1.2.1);
— централізація функцій, важливих для захисту, може бути необхідною для досягнення відповідності вимогам до контролю за несанкційованим доступом (див. 5.4.2);
— централізація складного устаткування може сприяти полегшенню експлуатації, періодичних випробовувань, технічного обслуговування та контролю за навколишнім середовищем;
— використання мультиплексного передавання даних може знижувати складність кабельної проводки;

b) Для систем класу 1 засоби резервування передавання даних використовують для передавання інформації з важкодоступних місць (наприклад, розміщених усередині захисної оболонки реактора). Вимоги до мультиплексного передавання даних наведено в IEC 61500.

6.1.2.2.2 Незалежність

Незалежність забезпечує умови попередження небажаної взаємодії між підсистемами системи або з іншими системами, яка може відбутися внаслідок неправильної експлуатації або відмови якого-небудь компонента будь-якої підсистеми або системи. Небажані взаємодії можуть відбуватися внаслідок таких явищ, як електромагнітна індукція, короткі замикання, дефекти уземлення, пожежі, хімічний вибух, авіакатастрофа та поширення правильних даних.

a) Якщо потрібна незалежність (див. 6.1.1.2.1), її можна досягти, використовуючи:

— електричну ізоляцію, яку можна отримати, застосовуючи волоконну оптику, оптичні ізолятори, захисний екран для кабелю;

— фізичне розділення, яке можна отримати за допомогою збільшення відстані, використання бар'єрів або комбінацій того й іншого;

— незалежність зв'язків для комп'ютерних систем, якої можна досягти за допомогою вибору відповідних структур і протоколів обміну даними (див. 5.3.1.3).

Примітка 1. Вимоги до електричної ізоляції та фізичного розділення наведено в 4.3 IAEA 50-SG-D8 та 7.8 IAEA 50-SG-D3;

b) У системі класу 1 фізичне розділення й електрична ізоляція між підсистемами різних ланцюгів безпеки мають задовольняти вимоги IEC 60709;

c) Розділення й ізоляція між системами класу 1 та системами й устаткованням, неважливими для безпеки, мають задовольняти вимоги IEC 60709.

Примітка 2. Найкращим методом фізичного розділення та захисту кабельної проводки систем безпеки, що передають електричні або оптичні сигнали, є використання спеціальних кабельних оболонок чи кабельних каналів, що забезпечують повний захист від небезпеки.

6.1.2.2.3 Захист від поширення та побічного впливу відмов

Окрім поширення відмов, яким можливо запобігти, використовуючи незалежність, у комп'ютерних системах треба враховувати інші типи поширення відмов, наприклад:

— непередбачене захоплення загальних ресурсів (обчислювальної потужності, смуги пропускання, пам'яті, ресурсів операційної системи тощо);

— відмова обміну ресурсами;

— порушення синхронізації всередині системи чи всередині архітектури КВК.

Окрім того, помилка у програмі, яка впливає на виконання певної функції, може призвести до відмов інших програм, що виконують інші функції в цій самій системі (стороння дія). Відмова може відбутися через помилку в загальних даних, програмах або технічному забезпеченні, що використовують для різних функцій, наприклад, процесор може бути причиною помилки в інших функціях унаслідок виключення або зациклювання однієї з функцій.

Архітектура системи має зменшити ризик і наслідки поширення відмов та сторонніх дій відмов. Можна розглянути наведені нижче методи:

— внутрішня ізоляція, за якої неможливо поширення відмов через відсутність шляхів поширення та загальних ресурсів;

— контроль системи за допомогою вбудованих засобів (тобто самоконтроль) або зовнішніх засобів (тобто інших систем й операторів), що дає змогу своєчасно виявити неправильні дані та/або пошкоджені ресурси;

— захисний інтерфейс, що дає змогу системі та її підсистемам визначати неправильні вхідні параметри та/або небажані взаємодії;

— оперативне (он-лайн) перевірення резервних вхідних сигналів, які використовують як вхідні параметри для наступного оброблення;

— використання добре відомих режимів роботи за виявлення відмов, що дають змогу системі зменшити їхню можливість та/або вплив поширення відмов.

Примітка. Докладні вимоги для уникнення використання помилкових структур програмного забезпечення і для перевірення й тестування модулів програмного забезпечення наведено в IEC 60880 та IEC 60880-2.

6.1.2.3 *Специфікація програмного забезпечення*

Специфікація програмного забезпечення містить:

— специфікацію прикладних функцій (специфікації прикладного програмного забезпечення);

— специфікацію архітектури програмного забезпечення.

Примітка 1. Архітектура програмного забезпечення визначає основні компоненти та підсистеми програмного забезпечення, як їх взаємопов'язано та як буде досягнуто необхідних якостей. Цей стандарт не містить вимог до архітектури програмного забезпечення (для систем класу 1 див. IEC 60880 та IEC 60880-2);

— специфікацію сервісних функцій та функцій системного програмного забезпечення.

Примітка 2. У разі використання наявного сімейства устаткування специфікації системного програмного забезпечення є частиною документації устаткування.

a) Для полегшення складання специфікації, верифікації та валідації прикладних функцій архітектура програмного забезпечення має чітко розподілятися між прикладним програмним забезпеченням та системним програмним забезпеченням (див. B.**2**.a IEC 60880). У такому разі верифікація та валідація прикладного програмного забезпечення може виконуватися незалежно;

b) Специфікацію прикладного програмного забезпечення можна отримати з технічного завдання до прикладних функцій (див. 6.1.1.1). За потреби специфікацію можна розширити за допомогою введення взаємозв'язку із функціями управління та моніторингу системи;

c) Для зменшення кількості помилок у специфікації та зусиль із верифікації треба, наскільки це можливо, визначити прикладне програмне забезпечення окремих прикладних функцій конфігурацією та встановленням компонентів із доведеною стандартною функційністю.

Примітка 3. Дуже часто для наявного устаткування прикладне програмне забезпечення можна визначити та розробити за допомогою відповідних інструментальних засобів, використовуючи наявні компоненти з бібліотеки прикладного програмного забезпечення;

d) Відповідну фільтрацію сигналу, перевірення та блокування сигналу має бути визначено для виконання резервних режимів роботи та мінімізації потенційної можливості випадкових дій.

6.1.2.4 *Призначення прикладних функцій у системі*

Це охоплює призначення:

— вхідних сигналів функціям та функцій певним вузлам оброблення;

— вибіркових процесів, пріоритетів обслуговування, захисних функцій устаткування;

— вихідних ліній управління діями виконавчих механізмів.

a) Призначення прикладних функцій, важливих для безпеки системи й підсистем, має задовольняти функційні, експлуатаційні вимоги та категоризацію технічного завдання функції (див. 6.1.1.1.1).

b) Призначення має передбачати стримування відмов;

c) Резервні функції та сигнали, важливі для безпеки, не повинна оброблювати одна й та сама підсистема, щоб у разі відмови або локалізації небезпеки в одному з каналів система зберігала можливість виконувати функції;

d) Функції різних категорій, призначені до одної й тої самої системи або підсистеми, мають стосуватися найвищої категорії безпеки, за винятком випадків, коли можливо продемонструвати, що дані або функції нижчої категорії не піддають ризику функції вищих категорій, наприклад, спричинюючи зупинку чи помилкове спрацьовування функцій вищої категорії. Це може призвести до рознесення функцій у різні підсистеми або рішення виконувати функції нижчої категорії в інших системах (ітерація процесу загального призначення — див. 5.**3**);

e) Стосовно функцій категорії A резервування оброблення не повинно виконуватися в тій самій підсистемі, а резервні дані не мають передаватися в однаковий спосіб.

f) Стосовно функцій категорії A має задовольнятися критерій одиничної відмови під час експлуатування, а також коли один резервний канал захисту виведено з експлуатації для технічного обслуговування.

6.1.3 ***Детальне проектування та реалізація системи***

Завданнями цього етапу є:

— розроблення/отримання детального проекту технічного забезпечення системи;

— розроблення (проектування та кодування)/придбання комп'ютерних програм, що становлять операційне та сервісне програмне забезпечення системи.

Примітка 1. Нормальною ситуацією (див. 6.1.2.2) є обмежена кількість нових розроблень, наприклад, інтерфейсів з іншими системами;

— розроблення (проектування та кодування)/генерація прикладного програмного забезпечення системи.

Примітка 2. Під час використання наявних сімейств устаткування програмні коди зазвичай автоматично генеруються інструментальними засобами зі специфікації прикладного програмного забезпечення (див. 6.1.2.3).

Документація специфікації системи і план інтеграції системи є основними вхідними даними етапу детального проектування та реалізації.

Вихідними даними цього етапу є:

— підсистеми та компоненти технічного та програмного забезпечення наступного етапу інтеграції системи;

— комп'ютерні програми для запуску в системі.

Розроблення/придбання технічного та програмного забезпечення є частиною життєвого циклу технічного та програмного забезпечення та виходить за межі цього стандарту.

Для систем класу 1 вимоги до розроблення програмного забезпечення наведено в IEC 60880 та IEC 60880-2, а вимоги до технічного забезпечення — в IEC 60987.

6.1.3.1 *Необхідний аналіз*

6.1.3.1.1 Функційна валідація технічного завдання до прикладних функцій

Метою функційної валідації є виявлення помилок і неточностей у специфікації прикладних функцій, які неможливо виявити під час валідації системи (див. 6.1.5). До складу функційної валідації входить моделювання роботи виконавчого устаткування й АЕС.

a) Правильність специфікації прикладної функції на відміну від вимог до функційності та характеристик функцій станції (див. 5.1.1) має пройти валідацію щодо функцій категорії А;

b) Для валідації треба використовувати остаточне прикладне програмне забезпечення, розроблене згідно з детальним проектом, і відповідне середовище технічного забезпечення.

6.1.3.1.2 Оцінення надійності

a) Має бути продемонстровано відповідну надійність прикладних функцій, які виконує система. Суворість демонстрації має бути вищою для функцій найвищої категорії:

— демонстрація має ґрунтуватися на балансі детерміністичних критеріїв та кількісного аналізу надійності;

— треба виконати оцінення впливу можливих відмов устаткування на надійність функції за допомогою ймовірнісного кількісного аналізу на основі інтенсивності відмов компонентів. Аналіз охоплює архітектуру та компоненти системи й має враховувати постійні та тимчасові відмови;

— оцінення впливу можливих проектних помилок програмного забезпечення на надійність функції треба виконувати на основі якісної оцінки, ураховуючи складність проекту, якість процесу розроблянння і зворотний зв'язок досвіду експлуатації. Оцінення повинно мати в основі попередньо узгоджений метод та має продемонструвати відповідність якості програмного забезпечення вимогам надійності.

Примітка. Результати аналізу та моделювальних випробувань можна застосовувати для кількісної оцінки, але немає визнаної методики, яку б можна було застосовувати. Для апаратних систем зазвичай не подають кількісної оцінки відмов унаслідок проектних помилок;

b) Треба проаналізувати ступінь ймовірної небезпеки впливу сервісних функцій системи на прикладні функції із суворістю, що відповідає важливості прикладних функцій для безпеки;

c) Аналіз надійності має ураховувати вплив одиничних відмов, відмов із загальної причини та поширення відмов усередині всіх систем, що належать до групи безпеки там, де функція, яку виконує система, є частиною групи безпеки, та є вимоги надійності, покладені на дану групу безпеки, виходячи з архітектури КВК (див. 5.3.3.1);

d) Для систем класу 1 аналіз надійності має також оцінювати відповідність випробувальних засобів вимогам 6.1.1.2.4.

6.1.4 ***Інтеграція системи***

Метою цього етапу є з'єднання модулів технічного та програмного забезпечення і перевірення сумісності програмного забезпечення, завантаженого в технічні засоби (див. розділ 7 IEC 60880).

Основними вхідними даними на етапі інтеграції системи є підсистеми та компоненти системи, документація детального проекту та план інтеграції системи.

Вихідними даними цього етапу є інтегрована система.

a) Інтеграцію треба виконувати згідно з планом інтеграції, визначеним у 6.2.3;

b) Після того як усе прикладне програмне забезпечення (раніше розроблене для сімейства устаткування або спеціально розроблене) інтегровано в систему, треба верифікувати експлуатаційні вимоги;

c) На етапі інтеграції необхідно виконати випробування, які показують, що кожна вибрана прикладна функція виконує своє завдання.

Примітка. Залежно від тих методів, які використовують під час проектування, для гарантування детерміністичної поведінки системи (див. 6.1.1.2.2) може бути потрібно виконувати випробування з випадковими даними, з високою частотою змінення вхідних даних від інших функцій усередині одної й тої самої комп'ютерної системи.

6.1.5 *Валідація системи*

Метою даного етапу є тестування інтегрованої системи для демонстрації її відповідності функційній, експлуатаційній специфікаціям й інтерфейсу (див. розділ 8 IEC 60880).

Інтегрована система, документація специфікації системи та план валідації системи є основними вхідними даними етапу валідації системи.

a) Валідацію системи необхідно виконувати відповідно до плану валідації, визначеного в 6.2.4;

b) Вимоги розділу 8 IEC 60880 потрібно застосовувати до валідації функцій категорії A;

c) Вимоги розділу 8 IEC 60880 потрібно застосовувати до валідації функцій категорій B та C з наведеними нижче поправками:

— потрібно застосовувати такий самий рівень деталізації, але об'єм випробування можна зменшити відповідно до цілей забезпечення безпеки функцій, важливих для безпеки;

— незалежність між групою, відповідальною за оцінку валідаційних випробувань, і проектувальниками необов'язкова.

6.1.6 *Інсталяція системи*

Метою даного етапу є монтування, з'єднання та випробування системи за місцем експлуатації.

Подальші дії, пов'язані із загальною інтеграцією системи з іншими системами та загальним уведенням до експлуатації, є частиною загального життєвого циклу КВК-системи (див. розділ 7).

a) Інсталяцію системи потрібно виконувати відповідно до плану інсталяції, визначеного в 6.2.**5**;

b) Необхідні засоби, наприклад маркування або колірне кодування, має бути використано для однозначного розпізнавання компонентів, кабелів й устаткування системи, і тим самим зменшити ймовірність помилок під час інсталяції, експлуатування та технічного обслуговування.

6.1.7 *Модифікація проекту системи*

Модифікація проекту системи може бути потрібною внаслідок установлення нових вимог до системи або прояву проектних дефектів, виявлених після оцінення експлуатаційних записів і звітів.

a) Унесення модифікацій до системи потрібно виконувати відповідно до встановлених процедур (див. 6.3.6);

b) Необхідно виконати випробування правильності роботи системи після модифікації;

c) Не дозволено вносити зміни до іншого технічного/програмного забезпечення, окрім зазначеного процедурами технічного обслуговування;

d) Після замінення устаткування необхідно продемонструвати/обґрунтувати, що воно відповідає всім специфікаціям первісного устаткування;

e) Для систем класу 1 процес модифікації програмного забезпечення має проходити відповідно до розділу 9 IEC 60880, а процес модифікації технічного забезпечення — до розділу 11 IEC 60987.

6.2 Системне планування

Метою вимог цього підрозділу є розроблення системних планів для того, щоб забезпечити досягнення та підтримання вимог до функцій, важливих для безпеки, реалізованих у КВК-системі.

Вимоги 5.4 описують додаткові загальні плани щодо функцій, реалізованих у взаємопов'язаних системах.

Примітка. Наведені нижче вимоги до планів не унеможливлюють оформлення цих планів у вигляді певного числа різних документів.

Треба починати складання системних планів на ранній стадії життєвого циклу системи до початку будь-якої діяльності.

6.2.1 ***Програма забезпечення якості системи***

a) Програму забезпечення якості системи треба створювати та реалізовувати, охоплюючи всі види діяльності, пов'язані з життєвим циклом системи. Вимоги до програми забезпечення якості системи необхідно брати з IAEA 50-C-QA (Rev.1) та ISO 9001;

b) Програма забезпечення якості системи має охоплювати діяльність, потрібну для досягнення відповідної якості системи, для верифікації відповідності вимог до якості, та надання об'єктивних доказів результату (див. розділ 102 IAEA 50-C-QA (Rev.1)). Вимоги до процедур верифікації затверджують у плані верифікації системи (див. 6.2.1.1);

c) Програма забезпечення якості системи розглядає якість системи та аспекти якості, пов'язані з інтеграцією технічного та програмного забезпечення. Конкретні програми забезпечення якості технічного та програмного забезпечення знаходяться поза сферою дії цього стандарту.

Примітка. Вимоги до програми забезпечення якості програмного забезпечення систем безпеки визначено в розділі 3 IEC 60880;

d) Програма забезпечення якості системи має охоплювати:

- визначення керівних стандартів і процедур, які треба використовувати в проекті (відповідно до 4.2.2 ISO 9001);
- ідентифікацію етапів життєвого циклу системи, первинних завдань й очікуваних результатів кожного етапу (відповідно до 4.4.2 ISO 9001);
- опис взаємодій і взаємозв'язків між різними завданнями (відповідно до 4.4.3 ISO 9001);
- опис організаційної структури (відповідно до 4.1.2 ISO 9001);
- комплектацію компонентами від зовнішніх постачальників (відповідно до 4.6 та 4.7 ISO 9001);
- ідентифікацію та трасування продукту (відповідно до 4.8 ISO 9000-3). Відповідні вимоги встановлено в плані управління конфігурацією (див. 6.2.1.2);
- ідентифікацію всіх процедур перевірянь і випробувань (відповідно до 4.10 ISO 9001);
- ідентифікацію діяльності та завдань із забезпечення якості;
- ідентифікацію персоналу/організацій, відповідальних за діяльність та виконання завдань із забезпечення якості, охоплюючи забезпечення незалежності (згідно з IAEA 50-C-QA (Rev.1));
- процедури обліку й усунення невідповідності вимогам, стандартам і процедурам. Процедури мають охоплювати розгляд впливу на безпеку АЕС і мають гарантувати, що всі впливи невідповідностей буде ідентифіковано, наприклад, взаємозамінність, технічне обслуговування, запчастини, інструкції з експлуатації тощо (відповідно до 4.13 ISO 9001);

e) Програма забезпечення якості має складатися на ранній стадії життєвого циклу системи та входити до загального списку інших дій життєвого циклу безпеки КВК. Програма може бути частиною специфікації системи або супровідним документом (див. 3.2 IEC 60880).

6.2.1.1 *План верифікації системи*

a) План верифікації треба розробляти разом з описом:

- процесу верифікації на всіх етапах життєвого циклу безпеки;
- відповідної організації та відповідальності;

b) Вихідні дані, отримані на кожному етапі життєвого циклу безпеки системи, потрібно перевіряти за точно визначеними вхідними даними;

c) На кожному кроці верифікації треба складати звіт щодо виконаного аналізу й отриманих результатів. Наприкінці етапу необхідно складати завершальний звіт, демонструючи відповідність результатів етапу вхідним вимогам, та усунення відхилень;

d) Верифікацію має виконувати персонал, компетентний у даному питанні, який добре розуміє вхідні дані, за якими виконують перевірення;

e) Ретельність плану верифікації має відповідати класу безпеки системи. План верифікації має відображати відповідні аспекти безпеки, які підлягають перевіренню, а також ураховувати те, що ймовірність відмови або упущення в складних елементах вища, ніж у простіших;

f) У програмі забезпечення якості системи визначають документи, що підлягають розгляду під час верифікації;

g) Документи, які розглядають під час верифікації, тобто вхідні та вихідні дії, звіти з верифікації й інструментальні засоби, що використовують у підготовленні вихідних даних, потрібно піддавати управлінню конфігурацією;

h) Для систем класу 1 план верифікації мають виконувати фахівці, які не є розробниками системи (відповідно до 6.2.1 IEC 60880).

6.2.1.2 *Програма управління конфігурацією системи*

Примітка. Частину наведених нижче вимог до програми управління конфігурацією системи отримано з IEEE 828 [3].

a) Ідентифікація конфігурації:
- — відповідні базові лінії має бути визначено як контрольні точки в межах життєвого циклу системи та має бути визначено елементи, які мають управлятися в базових лініях. Контрольовані елементи можуть бути проміжною й остаточною продукцією (такою, як технічне та програмне забезпечення; документи з верифікації; користувальницька документація) й елементами для підтримання середовища (такими, як компілятори, інструментальні засоби, випробувальні стенди);
- — треба ідентифікувати всі елементи, які підлягають контролю. Кожен окремий елемент повинен мати унікальну познаку та різні версії має бути однозначно ідентифіковано;
- — зв'язки між елементами базових ліній та елементом(-ами), з яких їх розроблено, має бути встановлено та зафіксовано;
- — систему управління конфігурацією має бути налаштовано на реконструкцію конфігурації всіх базових ліній системи;
- — необхідно передбачити засоби пошуку, здатні легко ідентифікувати зв'язки та різноманітні екземпляри елементів;

b) Управління конфігурацією:
- — управління конфігурацією має забезпечувати засоби, потрібні для ініціювання призупинення проекту. Необхідно визначити процедури та повноваження, необхідні для будь-якої наступної модифікації після призупинення проекту;
- — необхідно відстежувати стан кожного контрольованого елемента; це охоплює інформацію про початкову затверджену версію, стан необхідних змін та виконання затверджених змін;

c) Програму управління конфігурацією системи необхідно визначити на початку проектування системи та підтримувати протягом усього життєвого циклу системи.

6.2.2 ***План забезпечення захисту системи***

План забезпечення захисту системи визначають відповідно до загального плану забезпечення захисту (див. 5.4.**2**).

a) У процесі розробляння специфікації та проектування системи вимоги до технічних контрзаходів, визначених для системи в загальному плані забезпечення захисту (див. 5.4.**2**), має бути перетворено у вимоги технічного проекту й задокументовано;

b) Оцінення проектної документації потрібно виконувати для перевірення правильності реалізації контрзаходів, визначених під час аналізування захисту системи;

c) Під час верифікації та валідації системи ефективність функцій захисту має бути продемонстровано відповідними випробуваннями системи в її остаточній конфігурації.

6.2.3 ***План інтеграції системи***

План інтеграції системи охоплює процедурні та технічні заходи з об'єднання підсистем у систему й об'єднання технічного та програмного забезпечення. Він описує дії, визначені в 7.4 IEC 60880.

a) План інтеграції системи має визначати типи випробувань, зовнішні умови випробування та критерії приймання;

b) Випробування з інтеграції мають ґрунтуватися на концепції поетапної інтеграції;

c) Треба розрізняти випробування, пов'язані із системою (функції програмного чи технічного забезпечення системи), та специфічні випробування станції (прикладні функції).

Примітка. Випробування модулів (технічного, програмного забезпечення та комбінованих модулів), виконуваних під час типових випробовувань або попередніх проектів, проводять для уникнення повторів ідентичних або непотрібних випробувань.

6.2.4 ***План валідації системи***

План валідації системи охоплює необхідні методичні та технічні заходи для демонстрації того, що система задовольняє своє технічне завдання. Валідацію вимог до прикладних функцій розглядають на етапі функційної валідації (див. 6.1.3.1.1).

a) План валідації системи треба розробляти разом з описом конфігурації системи, яка піддається валідації, тих випробувань й аналізу, які необхідно виконувати, а також тих звітів, які має бути підготовлено.

1) Документація з валідації має встановлювати конфігурацію тої системи, яку піддають випробуванням, вхідні дані, методи, інструментальні засоби, засоби калібрування та відповідні критерії приймання. За потреби оцінюють точність і вплив інструментальних засобів на поводження системи;
2) У документації з аналізу валідації потрібно визначити те, що аналіз має продемонструвати, очікувані результати та необхідні критерії приймання;

b) Для функцій категорії А план валідації системи має розробляти, а роботу з валідації має виконувати група спеціалістів, незалежних від тих осіб, які проектували, реалізовували та/або модифікували систему (див. розділ 8 IEC 60880).

Примітка. Незалежність не потрібна особам, зайнятим виконанням плану валідації та підготовленням звіту;

c) Для функцій категорії В розроблення плану валідації має перебувати під наглядом відповідальних осіб, які не беруть участі в проектуванні, реалізації та/або модифікації системи;

d) Для функцій категорій А та В план валідації системи має забезпечувати відстеження специфікації за допомогою відповідних випробувань та перевірень;

e) Для функцій категорії С доцільно, щоб план валідації системи забезпечував відстеження специфікації за допомогою відповідних випробувань та перевірень.

6.2.5 *План інсталяції системи*

План інсталяції системи передбачає методичні та технічні заходи для інсталяції системи на місці експлуатації та для перевірення, необхідного для забезпечення гарантії того, що система придатна до експлуатації. План інсталяції доповнює загальні плани інтеграції та вводу в експлуатацію (див. 5.4.3).

a) План інсталяції системи треба розробляти для описання заходів забезпечення та перевірення правильності конфігурації системи та будь-яких змінюваних параметрів, а також того, що система є повною, належно встановленою, зібраною, приєднаною та працює відповідно до вимог специфікації;

b) Для систем класу 1 план інсталяції має задовольняти вимоги розділу 9 IEC 60987 та 10.1.1 IEC 60880;

c) Для функцій категорії А правильність роботи кожного каналу треба продемонструвати за місцем експлуатації.

6.2.6 *План експлуатації системи*

План експлуатації системи визначає, як систему потрібно експлуатувати та які вимоги висувають під час експлуатування системи.

a) План експлуатації системи має визначати, як система буде працювати в усіх режимах експлуатації. План має бути погодженим із планом технічного обслуговування системи (див. 6.2.7) і загальними планами експлуатації та технічного обслуговування (див. 5.4.4 та 5.4.5);

b) У плані експлуатації системи треба визначити умови, які мають бути виконаними до введення системи в експлуатацію. Зокрема:

— для системи має бути виконано інсталяцію, інтеграцію та пусконалагоджувальні роботи (див. 5.4.3);
— мають бути наявними план технічного обслуговування та експлуатаційна документація системи;

c) За потреби періодичних випробувань (див 6.1.1.2.4) у плані експлуатації системи має бути визначено:

— частоту та тривалість кожного випробування, умови до початку випробування і вплив, якщо є, на роботу системи та станції;
— етапи, необхідні для виконання кожного випробування, використовувані інструментальні засоби та засоби калібрування, аналіз правильності результатів;
— перевірення повноти відновлення до нормального стану, якщо потрібні тимчасові змінення системи.

Примітка. У періодичних випробуваннях бере участь група спеціалістів з експлуатації та технічного обслуговування. Цю діяльність можна розглядати як частину поточного ремонту (див. 6.2.7);

d) У плані експлуатації системи треба визначити документацію, що ведеться під час експлуатування. Вона має містити докладний опис відмов, документи з випробування системи та перелік зауваг до системи;

e) План експлуатації системи має ураховувати можливий вплив на безпеку станції;

f) Для систем 1 та 2 класів план експлуатації системи має передбачати періодичні випробування системи відповідно до будь-яких вимог, що походять з імовірнісного аналізу;

g) Для систем 3 класу план експлуатації системи має передбачати періодичні випробування системи через відповідні проміжки часу, якщо безперервна робота не гарантує виявлення відмов.

6.2.7 ***План технічного обслуговування системи***

Технічне обслуговування системи передбачає методичні та технічні заходи, необхідні для підтримання функційності під час експлуатування системи. План технічного обслуговування системи розробляють відповідно до плану експлуатації системи та загальних планів експлуатації й технічного обслуговування (див. 5.4.4 та 5.4.5).

a) Необхідно розробити план технічного обслуговування системи, що встановлює:

— порядок дій та методи, використовувані для виявлення прихованих відмов системи та підтримання «проектного» функціювання та надійності системи (планово-попереджувальне технічне обслуговування);

— дії та методи, які виконують для відновлення системи до цілком робочого стану (позапланове технічне обслуговування);

b) Обсяги планово-попереджувального технічного обслуговування потрібно визначати за допомогою методу систематичного аналізу, такого як аналіз видів та наслідків відмов або застосування централізованої надійної моделі технічного обслуговування, або розгляду дерев відмов для функцій системи;

c) Методи замінювання компонентів мають гарантувати, що:

— компоненти, які замінюються, є функційно однаковими з тими, що замінюють, і задовольняють вимоги якості;

— якщо замінення виконують у робочому режимі, її вплив на функціювання системи оцінюють і документують до замінення;

— зберігають реєстрацію щодо всіх замін, що дає змогу забезпечувати будь-які вимоги до простежуваності;

d) Методи перекалібрування мають гарантувати, що:

— нове калібрування виконують у певних межах (коли такі межі визначено системою, технічний персонал не піддають формальним обмеженням);

— якщо перекалібрування виконують у робочому режимі, її вплив на функціювання системи оцінюють і документують до перекалібрування;

— зберігають реєстрацію щодо всіх перекалібрувань, що дає змогу забезпечувати будь-які вимоги до простежуваності.

6.3 Вихідна документація

Цей підрозділ визначає вихідну документацію етапів життєвого циклу системи: зміст, характеристики й основні елементи, які необхідно піддати верифікації.

Вихідну документацію потрібно комплектувати взаємно узгодженими документами, які мають перехресні посилання та які гарантовано відстежують відповідність остаточного проекту вхідним вимогам.

6.3.1 ***Документація технічного завдання на систему***

6.3.1.1 *Зміст*

Технічне завдання на систему має бути повним і забезпечувати всю інформацію, необхідну для подальших дій життєвого циклу системи та кваліфікації системи.

6.3.1.2 *Характеристики*

Характеристики технічного завдання на систему:

a) вимоги мають припускати можливість перевірення.

Примітка 1. Підрозділ 4.3 IEEE 830 [2]) є настановою з перевірення вимог;

b) вимоги мають бути зрозумілими та чіткими настільки, щоб їх однаково розуміли всі охочі читачі, особливо рецензенти, та відповідальні за специфікацію системи та функційну валідацію.

Примітка 2. Наприклад, документ забезпечує точне та повне визначення вимог на противагу розлогим поясненням й іншій додатковій інформації, а також для обмеження ризику різних тлумачень. Найпридатнішим методом вирішення цих завдань є написання технічного завдання на систему за допомогою настанов, таких як IEEE 830 [2] та Меморандум EWICS No. 6 [5];

c) вимоги до прикладних функцій треба формулювати за допомогою функційних термінів, а не термінів комп'ютерної технології для того, щоб верифікацію могли виконувати спеціалісти з функціювання КВК й оператори станції, які можуть мати обмежені знання у сфері комп'ютерних технологій;

d) вимоги потрібно встановлювати з використанням документально обґрунтованих системотехнічних методів, інструментальних засобів і настанов.

Примітка 3. Докладні вимоги, що стосуються інструментальних засобів програмного забезпечення для систем класу 1, наведено в 4.2 IEC 60880-2;

e) вимоги має бути написано та структуровано так, щоб полегшити оцінення відповідності специфікації системи, а також забезпечити зв'язок із планом кваліфікації системи.

6.3.1.3 *Верифікація*

Наведені нижче елементи необхідно піддати верифікації:

a) вимоги мають бути простежуваними та повинні відповідати вимогам до системи, установленим у проекті архітектури, та функційній призначеності (див. 5.5);

b) вимоги до інтерфейсу мають відповідати вимогам до систем та устаткування, з якими пов'язано цю систему;

c) вимоги, які необґрунтовано ускладнюють систему, треба ідентифікувати (складність може збільшити ризик помилок у технічному завданні та/або самій системі).

6.3.2 ***Документація специфікації системи***

6.3.2.1 *Зміст*

a) Документація специфікації системи має бути повною та містити всю інформацію, необхідну для подальших дій життєвого циклу безпеки системи, особливо для етапів проектування системи та валідації;

b) Документація специфікації системи має визначати, яке наявне устаткування треба використовувати та яке треба розробити. Придатність вибраного устаткування треба обґрунтувати;

c) Документація специфікації системи має описувати структуру системи:

- розкладання системи на підсистеми та/або компоненти технічного та програмного забезпечення;
- внутрішнє поводження системи (див. 6.1.1.2.2), охоплюючи опис основних подій усередині системи та її захист від цих подій (див. 6.1.2.2.3);
- межі, умови навколишнього середовища, розрахункова надійність технічного забезпечення, поводження, функції, характеристики й інтерфейси кожної підсистеми;
- класифікація кожної підсистеми; необхідне підтвердження, якщо клас підсистеми нижче, ніж клас системи або підсистеми, до складу якої вона належить;
- умови використання та зв'язок певних підсистем у системі.

Примітка. Опис підсистем може бути побудовано за ієрархією, щоб спростити розуміння, від загального опису до елементарних підсистем (тобто підсистем, які не піддаються подальшому розкладанню в проектній документації системи). «Горизонтальна» інформація також може бути корисною;

d) Документація, що стосується програмного забезпечення, має містити специфікацію програмного забезпечення (див. 6.1.2.3);

e) У системах класів 1 або 2 треба визначити призначеність функцій підсистемам, тобто в специфікації системи треба зазначити, яка підсистема сприяє та/або необхідна для виконання цієї функції.

6.3.2.2 *Характеристики*

Характеристики документації специфікації системи:

a) документація має бути зрозумілою та чіткою, щоб її розуміли однозначно всі охочі читачі, особливо рецензенти та відповідальні за виконання проекту системи, інтеграцію та валідацію;

b) специфікацію прикладних функцій має бути сформульовано такими термінами, які полегшують верифікацію та роблять їх зрозумілими для спеціалістів, які займаються функціями КВК, й операторів станції;

c) специфікацію системи потрібно розробляти з використанням відповідних документально обґрунтованих системотехнічних методів, інструментальних засобів і настанов. Ці методи, інструментальні засоби та настанови мають мінімізувати «розбіжність» між методами, інструментальними засобами й настановами, використаними в технічному завданні на систему.

Примітка. Методи й інструментальні засоби розроблення програмного забезпечення можуть поліпшити якість специфікації остаточного проекту системи навіть порівняно зі специфікацією проекту апаратної системи;

d) специфікацію системи має бути написано та структуровано так, щоб полегшити оцінення її відповідності технічному завданню на систему, а також забезпечити ефективний зв'язок із валідацією системи, тобто полегшити повну ідентифікацію специфікації (на противагу просторих пояснень й іншої інформації).

6.3.2.3 *Верифікація*

a) Верифікацію специфікації системи стосовно технічного завдання на систему треба виконувати до завершення детального проектування. Коригувальні дії потрібно виконати перед завершенням монтування й інтеграції системи;

b) Треба встановити ефективні взаємозв'язки між особами, відповідальними за специфікацію системи, й постачальниками для перевірення придатності вибраного устаткування;

c) Верифікація має документально підтвердити та зафіксувати будь-яку невідповідність специфікації системи стосовно технічного завдання на систему;

d) Необхідно перевірити правильність переведення технічного завдання до прикладних функцій у специфікацію прикладного програмного забезпечення;

e) У системах класів 1 та 2 будь-яку невідповідність має бути виправлено чи обґрунтовано стосовно безпеки з урахуванням можливих заходів компенсації;

f) Властивості систем класів 1 та 2, що ускладнюють систему і не входять у технічне завдання на систему, має бути ідентифіковано й обґрунтовано стосовно безпеки.

Примітка. Наявність властивостей системи, що не входять у технічне завдання на систему, може значно ускладнити систему та потенційно знизити впевненість у її правильній роботі.

6.3.3 ***Документація детального проекту системи***

Детальний проект системи може бути виконано за кілька ітерацій. Вимоги цього пункту висувають до завершальної документації системи, наявної, коли завершено детальний проект, інтеграцію та валідацію системи, і система готова до відправлення та монтування за місцем експлуатації.

Документацію детального проекту системи можна поділити на чотири групи документів:

— проектна документація системи;

— необхідний аналіз (див. 6.1.3.1);

— документація проекту прикладного програмного забезпечення;

— документація компонентів технічного забезпечення системи та проекту системного програмного забезпечення.

Примітка 1. Якщо система реалізується на наявному устаткованні, документація проекту технічного та програмного забезпечення системи є частиною документації наявного устаткування.

Тільки дві перші групи розглянуто, тому що проектування технічного та програмного забезпечення перебуває поза сферою дії цього стандарту (див. 6.1.3).

Примітка 2. У системах класу 1 вимоги до документації програмного забезпечення встановлено в IEC 60880 та IEC 60880-2, а вимоги до документації технічного забезпечення — в IEC 60987.

6.3.3.1 *Зміст*

a) Документи проекту системи мають бути повними та містити всю інформацію, необхідну для наступних дій життєвого циклу системи, охоплюючи інтеграцію, валідацію, монтування, експлуатацію та технічне обслуговування;

b) Документи проекту системи розширюють обсяг документів на специфікацію та повинні забезпечувати докладний опис внутрішньої структури та внутрішнього поводження системи. Рівень деталізації опису залежить від класу безпеки системи;

c) Документи на проект системи мають містити опис монтування устаткування станції й умови випробування системи;

d) Документи на проект системи мають містити опис валідації функціювання та характеристик системи, зокрема, очікуваного часу реакції за різних режимів роботи станції, номінальні безпечні значення уставок й алгоритмів управління, та допуски уставок безпеки.

6.3.3.2 *Характеристики*

Характеристики документації проекту системи:

a) Документація має бути зрозумілою та чіткою, щоб вона могла бути однаково зрозумілою всім охочим читачам, зокрема авторам і рецензентам плану інтеграції системи, плану кваліфікації системи, плану монтування й уведення в експлуатацію, та плану технічного обслуговування системи, технічному персоналу, авторам і рецензентам модифікацій проекту;

b) Документацію детального проекту потрібно зберігати під час розробляння системи для гарантії того, що остаточна версія документів відповідає реалізованому проекту.

6.3.3.3 *Верифікація*

a) Верифікацію детального проекту системи та його документацію треба виконувати до застосування нового технічного та програмного забезпечення; треба також залишати досить часу для виконання будь-яких коригувальних дій, обумовлених результатами верифікації;

b) Виконання встановлених вимог до надійності прикладних функцій системи (див. 6.1.3.1.1) треба піддавати верифікації, наскільки це можливо, на ранньому етапі детального проектування.

Примітка. Аналіз надійності системи може потребувати коригування детального проекту, архітектури системи, наприклад ступеня резервування та навіть вибір загальних архітектурних рішень КВК;

c) Потенційну здатність сервісних функцій системи піддавати ризику виконання прикладних функцій потрібно піддавати суворому аналізу відповідно до важливості прикладних функцій для безпеки;

d) Допущення, зроблені під час верифікації детального проекту, має бути чітко сформульовано та задокументовано.

6.3.4 ***Документація з інтеграції системи***

6.3.4.1 *Зміст*

Документація з інтеграції системи має містити план інтеграції, звіти про випробування щодо інтеграції й усю інформацію, необхідну для наступного етапу валідації.

6.3.4.2 *Характеристики*

a) Звіти про випробування з інтеграції мають містити наведену нижче інформацію:

— версії технічних і програмних модулів, специфікацію випробувань, інструментальні засоби й устаткування разом із будь-якими відповідними даними калібрування;

— результати кожного випробування із зазначенням розбіжностей між очікуваними та дійсними результатами й для кожної розбіжності дані щодо виконаного аналізу та прийнятих рішень із продовження випробування або реалізації змін.

b) У системах класу 1 застосовують вимоги 7.7 IEC 60880.

6.3.4.3 *Верифікація*

a) Верифікацію звітів з інтеграції системи відповідно до плану інтеграції системи потрібно виконувати до проведення валідації;

b) Для системи класу 1 простежуваність від детальної проектної документації до відповідного компонента й інтеграційних тестів і аналізів має бути забезпечено так, щоб мати можливість оцінювати тести й аналізи щодо тестового покриття;

c) Для систем класу 2 простежуваність від детальної проектної документації до відповідного компонента й інтеграційних тестів і аналізів має бути забезпечено так, щоб мати можливість оцінювати тести й аналізи щодо тестового покриття.

6.3.5 ***Документація з валідації системи***

6.3.5.1 *Зміст*

Документація з валідації системи має містити план валідації, звіти з валідації й усю інформацію, необхідну для кваліфікації системи.

6.3.5.2 *Характеристики*

У системах класу 1 застосовують вимоги 8.1 IEC 60880.

6.3.5.3 *Верифікація*

Результати валідації й аналіз мають бути задокументовано та розглянуто на відповідність вимогам, установленим у плані валідації, для підтвердження того, що функційні характеристики системи задовольняють ці вимоги.

Примітка. Документація з валідації разом із документацією функційної валідації (див. 6.3.3.1 d)) підтверджує, що система відповідає специфікації системи та технічному завданню на систему.

6.3.6 ***Документація з модифікації системи***

6.3.6.1 *Зміст*

a) Запит на модифікацію

У документі має бути сформульовано:

— обґрунтування зміни та його вплив (якщо є) на безпеку АЕС;

— функційний опис зміни (з відміченими кресленнями, графіками виконання, кресленником конфігурації тощо) і запропоновані засоби виконання зміни;

— взаємозв'язок модифікації з будь-якими іншими модифікаціями на станції.

b) Пакет документів із модифікації

Після завершення змінення проекту, тобто коли компоненти програмного забезпечення, компоненти технічного забезпечення та документація відображають переглянутий проект, треба підготувати пакет змін у діючу систему. Пакет документів має містити опис модулів технічного забезпечення, модулів програмного забезпечення та засобів виконання змін, тобто визначати, яке устаткування має знизити споживання енергії, яка процедура має відбуватися після завантаження нового програмного забезпечення або рекомендації щодо використання наявних схвалених методів модифікації.

6.3.6.2 *Характеристики*

Запит на модифікацію треба чітко визначити і піддати оціненню компетентного персоналу. Результат оцінення (прийняти чи забракувати) треба зареєструвати.

6.3.6.3 *Верифікація*

a) Для систем класу **1** пакет документів з упровадження має бути перевірено з приводу завершеності та технічної правильності особами, не задіяними безпосередньо в модифікації проекту, але технічно компетентними, щоб мати змогу оцінити зміни;

b) Пакет документів із модифікації не повинен вводитися до системи без оцінення змін.

6.4 Кваліфікація системи

Цей підрозділ містить вимоги до процесу кваліфікації КВК-систем класів **1** та **2** (див. 6.1.1.6). Цей процес гарантує, що будь-яка КВК-система здатна протягом тривалого часу задовольняти установлені в основі проекту вимоги до характеристик, необхідні для функцій, важливих для безпеки, за встановлених умов навколишнього середовища.

6.4.1 ***План кваліфікації***

План кваліфікації має визначати всі питання, які необхідно оцінити для досягнення та підтримання кваліфікації системи та її функцій, важливих для безпеки.

6.4.1.1 *Кваліфікація функціювання та впливу навколишнього середовища*

Примітка. Кваліфікацію функціювання та впливу навколишнього середовища також називають «кваліфікацією технічного забезпечення».

Різноманітні методи можна застосовувати для демонстрування кваліфікації системи щодо функціювання та впливу навколишнього середовища. Вони містять типові випробування, функційні випробування, теоретичне оцінення та досвід практичного застосування аналогів. Типові випробування є найкращим методом (див. **4**.1 IEC 60780).

a) Систему треба кваліфікувати для умов навколишнього середовища відповідно до вимог IEC 60780 та IEC 60987. Умови навколишнього середовища мають охоплювати визначені в 6.1.1.5;

b) Послідовність випробування має бути визначено для типових випробувань компонентів або конфігурацій компонентів, чи всієї системи відповідно, для того щоб:

— контролювати функційні характеристики за нормальних умов навколишнього середовища та в усіх визначених межах експлуатації;

— продемонструвати стійкість до сейсмічних впливів.

6.4.1.2 *Аналіз й оцінення програмного забезпечення*

Примітка 1. Аналіз й оцінення програмного забезпечення також називають «кваліфікацією програмного забезпечення».

Аналіз й оцінення програмного забезпечення враховує суворість процесу розроблення програмного забезпечення й обсяг випробувань і валідації, виконаних після інтеграції системи. Для програмного забезпечення, розробленого раніше (ПЗРР), зворотний зв'язок за результатами досвіду експлуатації за певних умов може стати компенсувальним чинником, у разі нестачі інформації щодо процесу розробляння.

Програмне забезпечення комп'ютерних систем, що є об'єктом кваліфікації, містить:

— системне програмне забезпечення, що може бути раніше розробленим програмним забезпеченням, та не враховує специфіку станції;

— прикладне програмне забезпечення, інтегроване в систему, що враховує специфіку станції.

a) Під час кваліфікації має виконуватися оцінення системного та прикладного програмного забезпечення, щоб забезпечити відповідну якість програмного забезпечення для досягнення необхідної надійності функцій, які виконує система;

b) Для систем класу 1 знову розроблюване програмне забезпечення треба оцінювати відповідно до вимог IEC 60880;

c) Програмне забезпечення наявного устаткування, яке вибрали для систем класу 1, треба розробляти відповідно до визнаного настановами та стандартами відповідного високого рівня якості, необхідного для виконання функцій категорії A (див. 8.1.2 IEC 61226). Зокрема, має бути виконано вимоги IEC 60880-2 щодо раніше розробленого програмного забезпечення й інструментальних засобів та вимоги IEC 60987.

Примітка 2. IEC 60880-2 визначає критерії приймання й обмеження з використання документів зворотного досвіду експлуатації у процесі кваліфікації;

d) Програмне забезпечення наявного устаткування, вибране для систем класу 2, треба розробляти й виготовляти відповідно до визнаних настанов та стандартів. Інакше кажучи, може бути використано програмне забезпечення кваліфікованого серійного устаткування, що має документовану історію про задовільну експлуатацію під час подібного використання (див. 8.1.2 IEC 61226).

Примітка 3. Критерії приймання програмного забезпечення класу 2 серійного устаткування, з документацією про задовільну експлуатацію, стосуються сфери поширення майбутнього стандарту IEC для програмного забезпечення класу 2.

6.4.1.3 *Кваліфікація станції та обладнання*

Як зображено на рисунку 6, кваліфікація системи містить:

— аспекти, що стосуються обладнання, які можливо не специфікувати для даної станції й можливо оцінити попередньо;

— аспекти, специфіковані для даної системи, оцінення яких можливо виконати за час життєвого циклу системи, яку використовують на станції.

a) Кваліфікацію технічного та програмного забезпечення системи, скомпоновану з одної серії устаткування (див. 6.1.2.1), можливо отримати з попередньо виконаної кваліфікації індивідуальних компонентів і конфігурації взаємопов'язаних компонентів. У таких випадках необхідно виконати аналіз, який демонструє, що виконана кваліфікація містить остаточну конфігурацію системи, яку використовують на станції, охоплюючи схему розміщення, навантаження та розподіл температури всередині шаф;

b) Маючи за основу виконаний аналіз, план кваліфікації має описувати всі нові особливості проекту системи та визначати необхідність додаткових кваліфікаційних випробувань та оцінень.

6.4.2 ***Додаткова кваліфікація взаємопов'язаних систем***

a) Потрібно скласти план додаткових випробувань, які можуть бути необхідними на рівні взаємопов'язаних КВК-систем для завершення індивідуальної кваліфікації, наприклад випробування стійкості інтерфейсів до електромагнітних перешкод за конкретного компонування та уземлення;

b) Реалізацію та послідовність додаткових випробувань потрібно верифікувати як частину верифікації проекту архітектури КВК.

6.4.3 ***Кваліфікація технічного обслуговування***

a) Потрібно скласти додатковий план для кваліфікації технічного обслуговування під час експлуатування та технічного обслуговування системи, коли частину системи замінюють неідентичними запасними частинами та в разі функційних модифікацій;

b) Додатковий план має визначати модулі, що виконують функції категорій A та B відповідно, для забезпечення відповідності тим версіям, що пройшли валідацію.

6.4.4 *Документація*

a) Треба описати відомості, які подають до органів ліцензування;

b) У цьому списку мають бути відмінності між відомостями, потрібними до монтування системи, та відомостями, які надає заявник під час монтування й уведення в експлуатацію, наприклад звіти про випробування. Необхідні відомості містять:

— опис (докладний опис фактів);
— роз'яснення (опис фактів із поясненнями);
— демонстрацію;
— підтвердження;
— докази (заяви, які відстежують і доводять твердження);

c) Документацію поділяють на групи відповідно до цілей, для яких ця документація необхідна, але її зміст має містити:

— попередній звіт з аналізу безпеки та підсумкові документи для оцінення концептуального та базового проекту системи;
— докладний опис усієї системи або її частин для виконання незалежних верифікації та валідації. Ця документація має містити докладні відомості щодо типових випробувань компонентів;
— докладні або підсумкові роз'яснення, демонстрація або докази, потрібні для обґрунтування проектних вирішень та спрощення процесів незалежних верифікації та валідації;
— відомості щодо монтування, інтеграції, уведення в експлуатацію, приймальних випробувань на заводі та випробувань за місцем експлуатації для верифікації тих частин життєвого циклу безпеки, які перебувають між проектуванням й експлуатацією;
— документацію, що містять відомості, необхідні під час експлуатування системи для перевірення процедур, що підтримують якісний стан системи протягом довгого періоду часу.

Теми, пов'язані з обладнанням (сімейство устаткування)

Теми, пов'язані зі станцією (КВК-система)

1

Забезпечення якості виробником

2

Забезпечення якості плану кваліфікації системи

3

Кваліфікація функційності та впливу навколишнього середовища на компоненти й конфігурацію устаткування

Неявне тестування функційності та продуктивності програмного забезпечення системи, інтегрованого в устаткування

4

Додаткова кваліфікація функційності та впливу навколишнього середовища (якщо архітектура системи охоплює нові компоненти, нові конфігурації, нові умови навколишнього середовища, не охоплені в п. 3).
Неявне тестування функційності та продуктивності програмного забезпечення системи

5

Агналіз й оцінення якості програмного забезпечення системи, інтегрованого в устаткування, й оцінення інструментальних засобів

6

Додатковий аналіз й оцінення якості програмного забезпечення системи (нові компоненти, нові конфігурації)

7

Аналіз й оцінення якості
— прикладного програмного забезпечення;
— спеціально заново розробленого програмного/технічного забезпечення системи;
— ПЗРР загальної призначеності (якщо є)

8

Валідація інтегрованої системи (після інтеграції всього програмного забезпечення)

9

Додаткова кваліфікація взаємопов'язаних систем

10

Підтримання кваліфікації під час експлуатування станції, технічного обслуговування та модифікації проекту програмного/технічного забезпечення

Рисунок 6 — Питання, розглянуті в плані кваліфікації системи

6.5 Перелік основних спеціальних вимог для різних класів і категорій

Таблиця 4 — Вимоги до проекту та кваліфікації КВК-систем й устаткування

Клас 1	Клас 2	Клас 3
Типове устаткування, що задовольняє вимоги		
Розроблене відповідно до ядерних стандартів МЕК (6.1.2.1)	Вибрано кваліфікований КП	Вибрано КП
Вимоги до необхідних умов щодо устаткування/сімейства устаткування		
Дає змогу окремого резервування для задоволення критерію одиничної відмови (6.1.1.2.1)		
Детерміністичне поводження під час стаціонарного планування (6.1.1.2.2)	Детерміністичне поводження також за допомогою методики, визначеної в 6.1.1.2.2	
Мінімізація залежності роботи системи від вимог станції (5.3.1.5.3)		
Засоби самотестування IEC 60880 та IEC 60987 (6.1.1.2.3)		
Перевірюваність (6.1.1.2.4 та 6.1.3.1.2)		
Властивості, що забезпечують незалежність: IEC 60709 (6.1.2.2.2)		
Кваліфікаційні вимоги (6.4)		
Технічне забезпечення: IEC 60780 Програмне забезпечення: IEC 60880 та IEC 60880-2	Технічне забезпечення: IEC 60780 Програмне забезпечення	

Таблиця 5 — Вимоги до специфікації й уведення в експлуатацію ФСБ

Категорія А	Категорія В	Категорія С
Незалежні підсистеми для резервованих функцій (6.1.2.4) Експлуатація та технічне обслуговування, що задовольняють критерій одиничної відмови (6.1.2.4)		
Незалежність від дублювальних засобів ручного управління (5.3.1.5) Функційна валідація (6.1.3.1.1) Аналіз надійності (6.1.3.1.2) (Суворість залежить від категорії)	Аналіз надійності (6.1.3.1.2) (Суворість залежить від категорії)	Аналіз надійності (6.1.3.1.2) (Суворість залежить від категорії)
Валідація: IEC 60880 (6.2.4)	Валідація: IEC 60880 з можливими винятками (6.2.4)	Валідація: IEC 60880 з можливими винятками (6.2.4)
Верифікація кожного каналу безпеки на станції (6.2.5)		
Модифікації проекту: IEC 60880 та IEC 60987 (6.1.7)		

Кінець таблиці 5

Категорія А	Категорія В	Категорія С
Планування системи		
План верифікації незалежною групою спеціалістів (6.2.1.1) План валідації незалежною групою спеціалістів (6.2.4)	План валідації, що охоплює незалежних експертів (6.2.4)	План валідації, що охоплює незалежних експертів (6.2.4)
Документація та верифікація		
Потрібні всеохоплювальні інтеграційні тести (6.3.4.3)	Потрібні всеохоплювальні інтеграційні тести (6.3.4.3)	

7 ЗАГАЛЬНА ІНТЕГРАЦІЯ Й УВЕДЕННЯ В ЕКСПЛУАТАЦІЮ

Метою цієї фази є інтеграція КВК-систем за місцем експлуатації та забезпечення гарантії того, що всі КВК-функції, важливі для безпеки, виконуються належно під час приймальних випробувань на станції. План уведення в експлуатацію КВК-систем долучають до програми введення в експлуатацію систем станцій (див. 4.4 IAEA 75-INSAG-3).

7.1 Вимоги до цілей, яких має бути досягнуто

a) Ці роботи треба виконувати систематично, використовуючи стратегію, розроблену відповідно до планів монтування системи, загальної інтеграції й уведення в експлуатацію і планів захисту, визначених у 5.4 та 6.2;

b) Роботу із загальної інтеграції потрібно виконувати з усіма КВК-системами, змонтованими й індивідуально випробуваними (див. 6.1.6);

c) Потрібно виконати завантаження всіх баз даних, а збережені значення треба підтвердити та випробувати;

d) Апаратне та програмне забезпечення комп'ютерних систем має перебувати під управлінням конфігурацією;

e) Для нових станцій треба перед завантаженням реактора завершити верифікацію та валідацію за місцем експлуатації всіх функцій, важливих для безпеки.

7.2 Вихідна документація

a) До початку експлуатації має бути наявною документація з інтеграції всіх КВК-систем із реєстрацією у хронологічному порядку всіх робіт із верифікації та валідації, виконаних на місці експлуатації;

b) Звіт із загального введення в експлуатацію має підтверджувати, що КВК-системи відповідають усім очікуванням щодо використання за призначеністю, а функції, важливі для безпеки, відповідають загальним технічним завданням (див. 5.2);

c) Виявлені відхилення від проекту оцінюють, коригують і відправляють до експлуатації організації для того, щоб їхній вплив на роботу станції можна було взяти до уваги (див. 4.4.2 IAEA 75-INSAG-3).

Примітка. Точні вимоги до документації будуть залежати від особливостей експлуатаційної організації.

8 ЗАГАЛЬНА ЕКСПЛУАТАЦІЯ ТА ТЕХНІЧНЕ ОБСЛУГОВУВАННЯ

Експлуатацію КВК-системи можливо розпочинати після того, як оцінення звітів з уведення в експлуатацію продемонструє, що цю стадію успішно завершено. Експлуатацію можливо продовжувати, доки відповідно до записів технічного обслуговування не буде потрібно робити ремонт або модифікацію. Експлуатацію можна продовжити після успішного завершення ремонту або модифікації й оцінення відповідних звітів.

Перед початком етапу експлуатації необхідно погодити всі умови з передання керування від організації, відповідальної за загальне уведення в експлуатацію, до експлуатаційної організації. Наведені нижче вимоги не залежать від цього договору:

— системи мають витримати достатні випробування для підтвердження того, що забезпечено визначену функційність. У разі виявлення дефектів під час випробовування їх треба документально зафіксувати та, по можливості, усунути до передання;

— необхідно мати відповідну експлуатаційну документацію та плани технічного обслуговування.

8.1 Вимоги до цілей, яких має бути досягнуто

КВК-системи експлуатують та виконують технічне обслуговування, щоб підтримувати відповідність вимогам до КВК-функцій, важливих для безпеки.

a) Необхідно виконати плани експлуатації, технічного обслуговування та захисту, визначені в 5.4 та 6.2;

b) Список процедур, яких повинні дотримувати оператори станції або персонал із технічного обслуговування за нормальної експлуатації й аварійних умов, має перебувати у приміщенні щита керування чи поблизу від нього. Форма та зміст мають задовольняти міжнародні та національні правила;

c) Для систем класу 1 необхідно виконувати процедури експлуатації та технічного обслуговування програмного забезпечення згідно з IEC 60880.

8.2 Вихідна документація

У документації з експлуатації, ремонту та технічного обслуговування необхідно зберігати хронологічну послідовність. Також треба виконувати оцінення записів і звітів із певною періодичністю для визначення й ініціації необхідності технічного обслуговування або модифікації.

Примітка. Точні вимоги щодо документації будуть залежати від особливостей експлуатаційної організації.

ДОДАТОК А
(довідковий)

ОСНОВНІ АСПЕКТИ БЕЗПЕКИ АЕС

У цьому додатку визначено основні концепції безпеки, розглянуті в цьому стандарті для проекту КВК-систем АЕС.

А.1 Завдання безпеки станції

Промислова діяльність, що становить загрозу для працівників, населення та навколишнього середовища, потребує від оператора прийняття розумних практичних заходів для зниження цієї загрози. Одним із типових ризиків ядерної енергії є небезпека іонізуючого випромінення (див. розділ 201 IAEA 50-C-D).

Основним завданням ядерної безпеки є захист людей, суспільства та навколишнього середовища установленням та підтриманням на АЕС ефективного захисту від радіаційної небезпеки (див. 2.1 IAEA 75-INSAG-3 та розділ 2 IAEA 50-C-D).

Технічною метою безпеки для наявних АЕС є «показник імовірності» важкого пошкодження активної зони нижче ніж 10^{-4} подій за рік експлуатації станції. Дотримання принципів безпеки майбутніх станцій має привести до поліпшення ситуації — не більше ніж 10^{-5} випадків за експлуатаційний рік станції. Керування важкими аваріями та вживання необхідних заходів мають знизити в десять разів імовірність великого викиду за межі станції, що спричинить потребу вжиття необхідних заходів поза територією станції (див. 2.3 IAEA 75-INSAG-3).

А.2 Дослідження безпеки станції

Дослідження безпеки проекту атомної станції виконується для встановлення та підтвердження основи проекту щодо аспектів, важливих для безпеки, й отримання гарантії того, що загальний проект станції задовольняє граничні значення та контрольні рівні для радіаційних доз і викидів, визначених регулівним органом для кожної категорії стану станції (див. розділ 6 IAEA 50-SG-D11).

Сфера дослідження безпеки може охоплювати:

— демонстрацію дотримання експлуатаційних граничних значень і станів для нормальної роботи станції;

— характеристики постульованих вихідних подій, визначених у проекті станції, та їхню локалізацію;

— аналіз та оцінення наслідків, що виникають як результат постульованих вихідних подій;

— порівняння результатів аналізу з припустимими радіаційними критеріями та проектними граничними значеннями;

— установлення та підтвердження основи проекту;

— демонстрація можливості керування передбачуваними експлуатаційними подіями й аварійними умовами за допомогою автоматичних систем захисту разом із передбаченими діями оператора.

Цей аналіз безпеки станції є ітераційною процедурою, яка виконується від початкового концептуального проекту станції до остаточного оцінення безпеки станції, і враховує всі особливості конфігурації станції, здатні впливати на безпеку. Аналіз безпеки станції враховує можливі помилки людини під час експлуатування й аварійних умов.

Такий аналіз має продемонструвати, що певні дії, які виконуються автоматичними системами й операторами, призведуть до такого поводження станції, коли радіаційні дози опромінення персоналу та населення залишаться нижче від припустимих граничних значень за нормальної експлуатації станції, передбачуваних подіях під час експлуатування й аварійних умов.

А.2.1 ***Аналіз послідовності подій***

Метою аналізу послідовності подій є систематичне та детальне визначення всіх можливих наслідків постульованої вихідної події на станції, охоплюючи події, пов'язані з допоміжними та забезпечувальними системами, а також можливою помилкою оператора. Результати такого аналізу послідовності подій може бути використано для визначення відповідності проекту вимогам безпеки, установленим у правилах МАГАТЕ (див. додаток до IAEA 50-C-D).

Аналіз дерев подій (якісний) й аналіз дерев відмов (кількісний) є корисними аналітичними інструментами для визначення можливих станів станції, спричинених постульованою вихідною подією.

Треба зазначити, що неможливо та немає потреби вміщувати в аналіз безпеки кожну ймовірну послідовність подій. Однак за аналізу безпеки треба визначати та докладно розглядати ті постульовані вихідні події та послідовність подій, що є граничними для проекту безпеки. Під час вибирання таких послідовностей подій враховують досвід наявних станцій.

Навіть з обмеженням на випадок граничних послідовностей подій, як описано вище, суворе застосування методології дерев подій у багатьох практичних ситуаціях приведе до визначення значно більшого числа конфігурацій станції для кожної постульованої вихідної події, ніж це може бути реально проаналізовано в деталях. Тому зазвичай припустимо обмеження детального аналізу деяким числом характерних послідовностей подій.

А.2.2 ***Оцінення основи проекту: детерміністичні/ймовірнісні методи***

Розроблено методи для оцінення досягнень цілей безпеки (див. 3.3.4 IAEA 75-INSAG-3).

За детерміністичного підходу в основі проекту події вибирають так, щоб обмежити діапазон пов'язаних можливих первісних подій, які можуть призвести до загрози безпеки станції.

Імовірнісний аналіз використовують для оцінення ймовірності певних послідовностей та їхніх наслідків. Таке оцінення може враховувати вплив захисних заходів усередині та ззовні станції.

Порівняння детерміністичного та ймовірнісного методів: недостатність повних даних щодо поводження компонента чи системи або нездатність установити потрібний режим може перешкодити використанню точного кількісного ймовірнісного методу. Однак частковий імовірнісний метод може часто бути доповнено якісним інженерним обґрунтуванням. З іншого боку, детерміністичний підхід потребує інженерного аналізу, що явно містить кількісний імовірнісний розгляд.

По суті, у сучасній практиці використовують детерміністичний підхід до проектування систем та ймовірнісний підхід для оптимізації необхідних частин проекту й оцінення загальної безпеки.

А.3 Глибокоешелонований захист

Основним внеском у філософію безпеки є концепція глибокоешелонованого захисту. Цю концепцію потрібно застосовувати до всієї діяльності з безпеки як організаційної та експлуатаційної, так і пов'язаної з проектуванням, для забезпечення перекриття норм безпеки так, щоб у разі відмови відбувалося її компенсування або виправлення (див. розділ 2 IAEA 50-C-D; 3.2 та додаток до IAEA 75-INSAG-3; 3.3 IAEA 50-SG-D8 та 4.3 IAEA 50-SG-D11).

Перше застосування концепції глибокоешелонованого захисту до процесу проектування має забезпечити незалежні додаткові комплекти устаткування та процедури для попередження аварій або для забезпечення необхідного захисту, якщо подію неможливо попередити. Приклади багаторівневого захисту:

— наявність багатьох засобів, що забезпечують кожну з основних функцій безпеки, тобто керування реактивністю, відвід тепловиділення й утримання радіоактивності;

— використання надійних захисних пристроїв на додаток до внутрішньо притаманного устаткування для безпеки;

— доповнення керування станцією автоматичними та ручними діями;

— забезпечення устаткованням і процедурами, що пом'якшують наслідки аварій.

Загалом, усі ешелони захисту мають працювати весь час так, як визначено для різних режимів експлуатації.

— Метою першого ешелону захисту є запобігання відхиленню від нормальної експлуатації станції. Це потребує, щоб станцію було спроектовано, побудовано та щоб її експлуатували якісно та консервативно, відповідно до необхідних рівнів якості й інженерної практики;

— Метою другого ешелону захисту є виявлення та усунення відхилів від нормальних умов експлуатації для запобігання розвитку передбачуваних експлуатаційних неполадок в аварійну ситуацію;

— Третій ешелон захисту забезпечують додатковим устаткованням і процедурами, які в разі, хоча це малоймовірно, коли розвиток певного експлуатаційного порушення не можливо відвернути попередніми ешелонами захисту, дає змогу керувати наслідками аварійних умов. Інша основна мета цього ешелону захисту полягає в досягненні стабільних та прийнятних умов після аварії;

— За межами третього ешелону захисту передбачають подальше сприяння захисту населення за допомогою додаткових засобів станції (які не визначено як важливі для безпеки) і планів миттєвої готовності, які переважно не залежать від проекту реактора.

Друге застосування концепції глибокоешелонованого захисту — це будівництво й експлуатація АЕС у такій спосіб, щоб радіоактивні матеріали утримувалися в межах послідовних фізичних бар'єрів. Такі фізичні бар'єри в основному пасивні та зазвичай охоплюють саме паливо, його оболонку, границі системи охолодження реактора й оболонку контайнмента. Проект має забезпечувати необхідну ефективність і захист кожного з цих бар'єрів.

Додатковим застосуванням концепції глибокоешелонованого захисту є використання одиничних або численних резервних КВК-систем. Для мінімізації значущості пошкоджень і досягнення глибокоешелонованого захисту можливо використовувати більше ніж одну КВК-систему, які діють послідовно, коли контрольовані параметри відхиляються від установлених величин. Спочатку, у зв'язку з відхилом параметрів від нормальних умов, діють некласифіковані керівні системи. Услід за дією цих керівних систем перед включенням систем захисту можуть вступати в дію один чи більше рівнів додаткових керівних систем, важливих для безпеки, у міру того, як подія перетворюється з незначного експлуатаційного порушення в незначний перехідний режим, а потім у суттєвий нестійкий режим. Мета кожної стадії — припинення події та повернення системи до нормальної роботи за незначних подій та безпечного зупинення для серйозніших подій.

ДОДАТОК В
(довідковий)

КАТЕГОРИЗАЦІЯ ФУНКЦІЙ ТА КЛАСИФІКАЦІЯ СИСТЕМ

В.1 Обґрунтування схеми категоризації/класифікації

IAEA 50-SG-D1 установлює перелік функцій безпеки, які дають можливість у проекті станції виконувати основні вимоги щодо безпеки — від засобів безпечного зупинення реактора до відводу залишкового тепла з активної зони та зменшення ймовірності викиду радіоактивного матеріалу. Унаслідок цього виникла ідея класифікувати компоненти, потрібні для виконання функції безпеки, відповідно до їхньої важливості для безпеки. Упроваджують методологію ранжирування функцій безпеки та призначеності проектних вимог, в основі якої лежать наслідки відмови функції безпеки, імовірності того, що функція буде потрібна, та ймовірності, що її не буде виконано, коли буде потрібно.

IAEA 50-SG-D8 розглядає ідею класифікації інформаційних і керівних систем. КВК-системи поділяються на «системи, важливі для безпеки» та «системи, не важливі для безпеки». Потім системи, важливі для безпеки, підрозділяються на «системи безпеки» та «системи, пов'язані з безпекою» (див. рисунок 1 і «визначення» в IAEA 50-SG-D8). IAEA 50-SG-D3 та IAEA 50-SG-D8 вводять проектні вимоги відповідно для систем захисту та систем, пов'язаних із безпекою. IEC 60880 та IEC 60987 мають посилання на цю класифікацію МАГАТЕ.

IEC 61226 класифікує функції та пов'язані з ними системи й устаткування, важливі для безпеки, на три категорії: А, В та С. У ньому введено критерії для призначення категорій функцій КВК і проектні вимоги для пов'язаних систем й устаткування (див. розділ 8 IEC 61226).

Число класів, визначених МАГАТЕ, відрізняється від IEC 61226 (системи безпеки та системи, пов'язані з безпекою проти категорій А, В та С). Окрім того, МАГАТЕ та МЕК користуються неідентичними визначеннями та концепціями (система класифікації в МАГАТЕ проти класифікації ФСБ у МЕК), і ці суперечності можуть призвести до різних тлумачень.

Цей стандарт спирається на IEC 61226 стосовно поділу на три класи, це типово щодо подання різних рівнів забезпечення потрібних характеристик і досяжної надійності за використання наявних КВК технологій і продуктів (розроблених відповідно до ядерних стандартів, відібраних і кваліфікованих КП, відібраних КП). Проте з метою уникнення невизначеності під час тлумачення вимог приймають окрему градацію відповідно до ФСБ і систем.

У цьому стандарті розроблено такі базові вихідні дані для категоризації/класифікації.

В.2 Опис принципів категоризації та класифікації, прийнятих у цьому стандарті

Функції, системи й устаткування АЕС необхідно розглядати з двох точок зору (рисунок В.1):

— Функційна точка зору.

Із цього боку розглядають тільки виконувані функції. Коли відомо, що датчики, процесорні пристрої, інтерфейсні пристрої тощо потрібні для виконання функцій, то з функційної точки зору їх не розглядають, тому що вони можуть входити до більших угруповань устаткування та виконувати також інші функції (див. «системну точку зору»). Засоби, потрібні для виконання функцій, називають системами й устаткуванням, асоційованими з цією функцією.

— Системна точка зору.

Із цього боку розглядають системи як організовану сукупність устаткування, що виконує багато функцій/підфункцій, наприклад система захисту, автоматизована система керування, система інтерфейсу «людина-машина». Конкретні функції, виконувані одною системою, можуть стосуватися різних категорій.

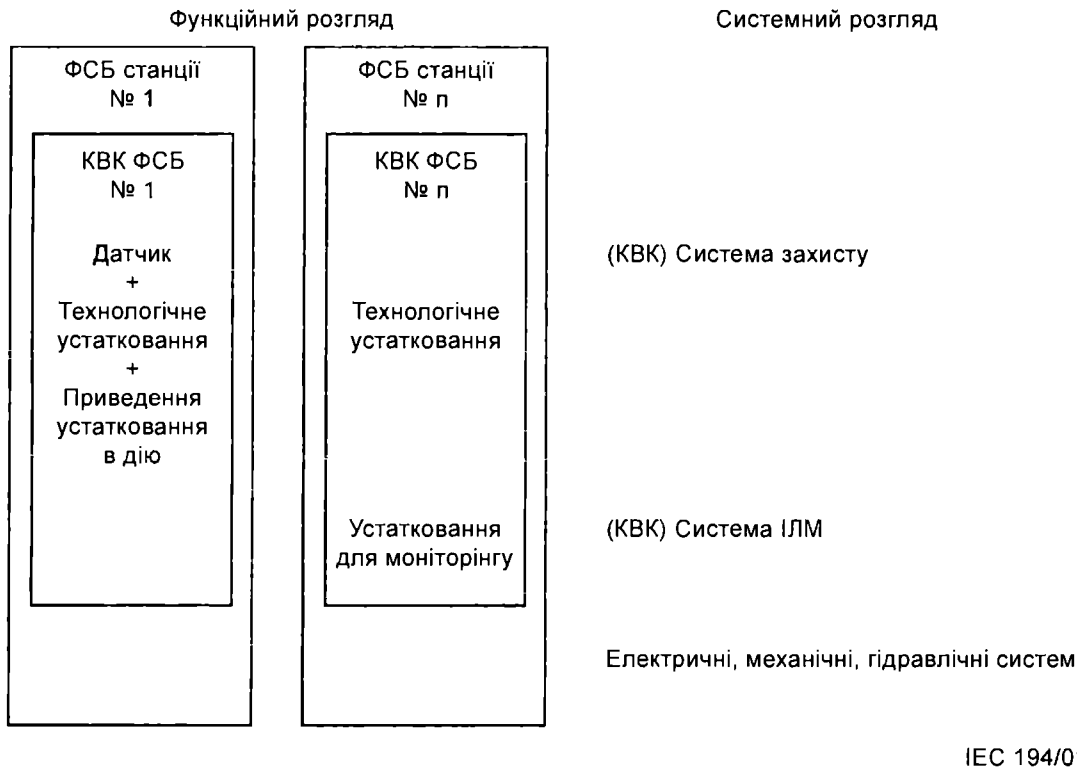


Рисунок В.1 — Взаємозв'язок між КВК-функціями та КВК-системами

В.2.1 *Етап проектування технології на АЕС*

Проектувальники технології на АЕС аналізують станцію та відповідні системи з функційної точки зору. Вони визначають специфічні постульовані вихідні події станції та реактора, а також функції, важливі для безпеки, які треба виконувати для попередження можливості переростання цих постульованих вихідних подій в аварійні умови. Кількість незалежних функцій (або підфункцій), яка може потребуватися для кожної ПВП, визначають відповідно до принципу глибокоешелонованого захисту. Ці функції (або підфункції) стосуються категорій А, В чи С залежно від того, яку роль у безпеці атомної станції вони виконують: основну, додаткову, допоміжну або непряму.

Методи категоризації зазвичай мають у своїй основі детерміністський, імовірнісний розгляд та розгляд з точки зору зниження ризику. Вони враховують різні чинники, такі як імовірність і потенційна можливість серйозних наслідків ПВП у разі, якщо відбувається відмова КВК-системи, проміжок часу, потрібний для миттєвого приведення КВК-системи в дію, своєчасність і надійність, з якою може бути розпочато будь-які альтернативні дії або може бути виправлено будь-яку відмову КВК-системи.

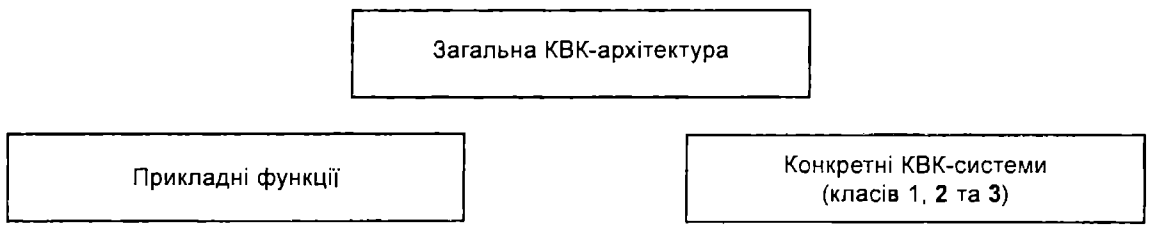
Процеси категоризації можуть давати змогу, щоб функції КВК-системи в групі безпеки належали до різних категорій, наприклад різноманітне відімкнення реактора може знадобитися тільки за умови малоймовірного очікуваного перехідного режиму за одночасної відмови первісної функції захисту. У цьому разі КВК-функції категорії А (яку впроваджено в системі класу 1) може бути переведено до нижчої категорії В чи С.

Категорії визначають рівень проектних вимог, а також мінімальний необхідний клас асоційованих систем й устаткування, потрібних для реалізації функції.

B.2.2 *Етап проектування КВК АЕС*

Проектувальники КВК АЕС аналізують КВК-функції й асоційовані з ними системи й устаткування із системної точки зору. Їхнє завдання — забезпечити ряд КВК-систем, які виконують КВК-функції, із таким рівнем якості та незалежності, який установлено проектувальниками процесів. Класи систем встановлюються залежно від досяжного рівня якості.

Архітектурний і системний проект КВК, функційна призначеність



Процес класифікації та призначення функцій у комп'ютерних системах відрізняється від того, що застосовують в апаратнореалізованих системах, тому що:

— в апаратнореалізованих системах функції зазвичай виконуються в ланцюгах окремих електронних компонентів або реле, тоді як у комп'ютерних системах можливо виконання ряду функцій одними й тими самими компонентами технічного забезпечення;

— комп'ютерні системи вміщують ряд допоміжних функцій, наприклад, функції самоконтролю, функції діагностики, які не є частиною категоризації проекту станції. Ці функції можуть мати нижчий рівень кваліфікації, але потребують функційної ізоляції;

— вибір архітектури системи може обмежувати складність, щоб полегшити виконання функцій високої категорії безпеки;

— у проектувальника є потенційна можливість умістити вимоги до архітектури систем, наприклад, функційний розподіл, внутрішнє поводження, складність, заходи проти ВЗП, пов'язані не з конкретними функціями, а з КВК-системами та властивостями сімейства устаткування, що використовується для реалізації та кваліфікації таких систем.

Це може привести до усвідомленої потреби встановити систему класифікації для КВК-систем залежно від функції найвищої категорії, яку вони виконують.

B.3 Категоризація КВК-функцій, важливих для безпеки

У цьому стандарті передбачено, що проектна основа безпеки станції, розроблена проектувальниками процесів, визначає розподіл конкретних КВК-функцій, важливих для безпеки, за трьома категоріями A, B та C. Вимоги категоризації встановлюють ступінь якості одиниць устаткування, які використовують для виконання функцій.

Категоризацію КВК-функцій виконують до рівня підфункцій (див. примітку), щоб розробникам КВК не треба було робити додатковий аналіз на рівні процесів для її завершення.

Примітка. Одну й ту саму функцію, важливу для безпеки, можна виконувати з використанням ряду підфункцій або унікальної функції, до складу якої належать усі підфункції. Це може створити двотлумачність під час визначання вимог до категоризації, тому що підфункції можуть мати різну важливість для безпеки і, як наслідок, різні категорії, призначені кожній із них.

На додаток до вимог категоризації в проектній основі безпеки станції визначають вимоги до незалежності та різноманітності конкретних функцій, відповідно до принципу глибокоешелонованого захисту. Незалежність потрібна між функціями, що забезпечують різні ешелони захисту в одній групі безпеки, між деякою функцією та функцією, що зменшує ризик.

Вимоги незалежності та різноманітності є вхідними даними для процесу призначання КВК-функцій КВК-системам. «Асоційовані з функцією системи та устаткування» може бути розподілено до різних КВК-систем за умови, що в них однакова класифікація безпеки (див. B.2).

B.4 Класифікація КВК-систем

КВК-системи, що становлять усю КВК-архітектуру, зазвичай містять групу з кількох КВК-функцій або підфункцій, які разом виконують подібні завдання для станції. Зазвичай системи характеризуються функціями, які вони реалізують. Кількість КВК-систем та їхні функції визначають для конкретної станції. Типові приклади КВК-систем, важливих для безпеки, наведено нижче.

a) Системи автоматизації й управління

Системи управляють параметрами станції чи устаткування:

— для підтримання параметрів процесу в межах, установлених під час аналізу безпеки станції;

— для підтримання безпечної роботи систем й устаткування станції, важливих для безпеки;

— для мінімізації величини та швидкості можливих порушень;

— для мінімізації частоти виникнення подій, що спричиняють дію системи захисту. Цього можна досягти, забезпечуючи високоякісні, резервовані різноманітні системи автоматизації й управління чи забезпечуючи більше ніж один рівень дії. Наприклад, комбінація автоматичних керівних дій та ручних дій, якщо є достатньо часу щодо правильної реакції або забезпечення двох чи більше комбінацій, наведених вище.

Системи автоматизації й управління можуть впливати на безпеку, оскільки їхні характеристики, надійність і наслідки відмов становлять частину основного проекту для системи захисту (див. 3.3 IAEA 50-SG-D8). Системи автоматизацій та управління також можуть бути головним засобом виконання функцій, важливих для безпеки, наприклад, коли є великий проміжок часу для дій із коригування.

Типові функції даних систем охоплюють керування в розімкненому контурі, керування в замкненому контурі та виконання керівних дій, ініційованих уручну;

b) ІЛМ-системи

Системи забезпечують інформацією оператора станції й інших співробітників про стан станції та її систем, важливих для безпеки. Їх також використовують для підтримання процесу прийняття рішень оператором та надання дозволу на керування вручну для підтримання безпеки станції.

Типові функції даних систем:

— перетворення інформації датчиків або сигналів від інших систем в інформацію, зручну для відображення або реєстрації на індикаторах, дисплеях, принтерах тощо. Система виводить таку інформацію, як загальний огляд, небезпечне змінення стану та робочі інструкції;

— відображення тривожної сигналізації, попередження й іншої інформації;

— підтримання інтерфейсів ручного керування;

c) Системи захисту та безпеки

Ці системи гарантують, що встановлені в проекті граничні значення не буде перевищено внаслідок прогнозованих експлуатаційних подій і що наслідки аварій розглянуто в проектній основі.

Програма безпеки МАГАТЕ (див. IAEA 50-SG-D3) визначає типові функції таких систем:

— виявлення аварійного стану й автоматичне ініціювання дій відповідних систем, охоплюючи зупинку реактора;

— установлення пріоритетів для функцій різних категорій (наприклад, скасування дії системи керування);

d) Аварійна система живлення

Типові функції:

— скидання навантаження;

— послідовне навантаження дизель-генераторів й інших джерел живлення.

КВК-системи, що виконують функції, важливі для безпеки, розподіляють за трьома класами, яким відповідають визначені в проекті вимоги до виготовлення та кваліфікації, щоб ці системи були прийнятними для виконання функцій одної чи кількох категорій А, В чи С або некласифікованих (див. В.2). Типову класифікацію КВК-систем наведено в таблиці В.1.

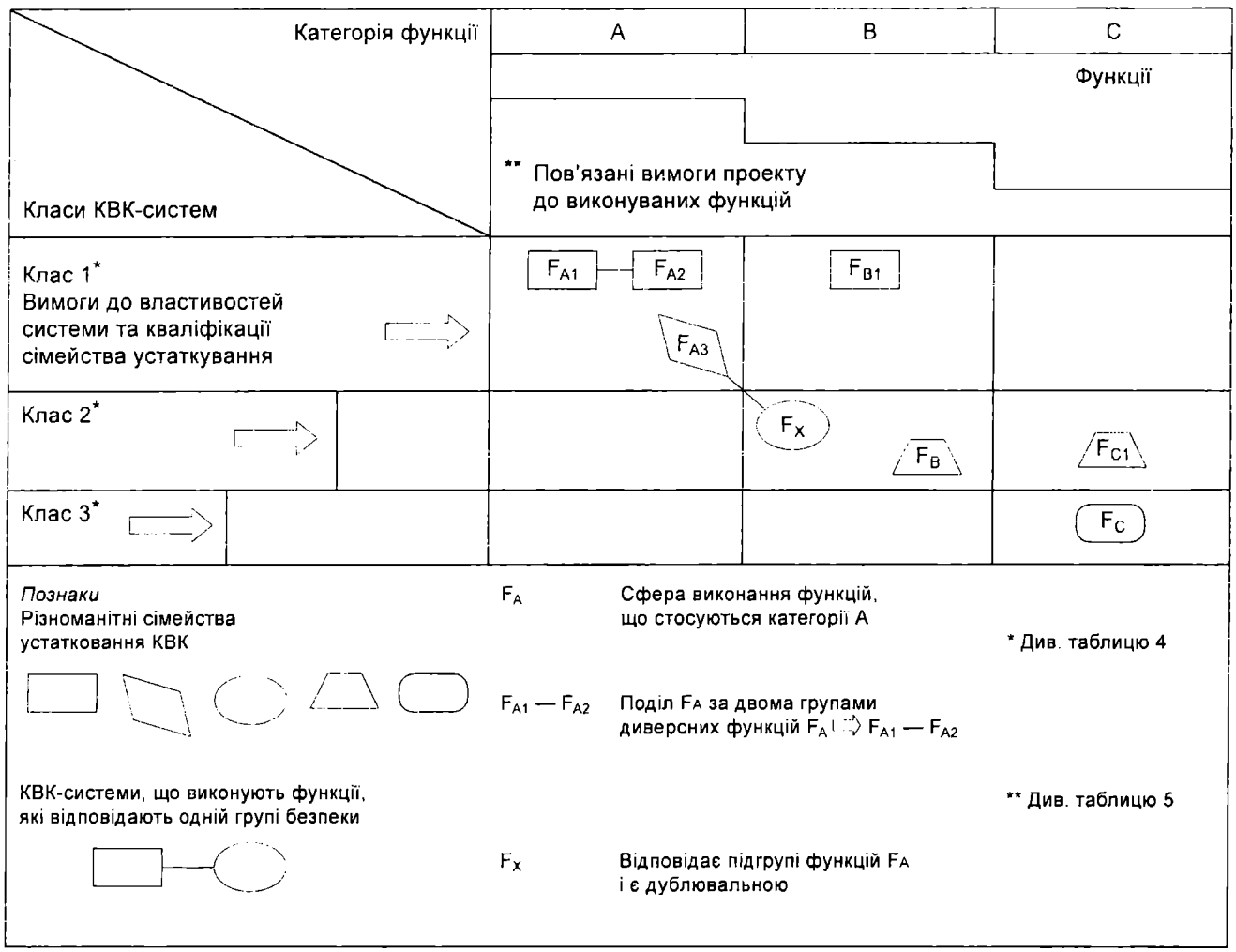
Таблиця В.1 — Типова класифікація КВК-систем

	Клас 1	Клас 2	Клас 3	Не класифікують
Системи автоматизації й управління станції		X	X	X
ІЛМ-системи		X	X	X
Система захисту та система безпеки	X			
Аварійна система живлення	X			

Вимоги до функції вищої категорії безпеки визначають клас системи.

ДОДАТОК С
(довідковий)

ЯКІСНИЙ ПІДХІД ДО ЗАХИСТУ ВІД ВЗП



IEC 195/01

Рисунок С.1 — Приклади призначеності функцій групи безпеки для КВК-систем

С.1 Приклад призначеності функцій групі систем безпеки

Рисунок С.1 розроблено згідно з даними таблиць 4 та 5 підрозділу 6.5, і він пов'язує відповідні розділи цього стандарту. Таблиця 4 наводить вимоги до властивостей і кваліфікації сімейств устаткування, призначеного для реалізації КВК-систем різних класів. Таблиця 5 наводить вимоги до КВК-систем, призначених для виконання функцій, для яких встановлено категорію згідно з цим стандартом. Вимоги до характеристик і кваліфікації устаткування, такі як надійність програмного забезпечення і стійкість до впливу навколишнього середовища, може бути задоволено за допомогою вибирання відповідного сімейства устаткування. Вимоги до систем фокусуються на таких проектних характеристиках, як, наприклад, нечутливість архітектури системи до дефектів та відповідність методів верифікації та валідації, прийнятих у проекті для гарантування правильності функціювання.

На рисунку С.1 зображено кілька прикладів призначеності функцій групи безпеки КВК-системам, які відображають різні проектні стратегії для виконання вимог до надійності. Ці стратегії вибирають на основі аналізу ефективності різних заходів захисту від ВЗП (див. 5.3.3.1).

FA1—FA2. До складу цієї групи безпеки входять дві функційно різні функції FA1 та FA2 категорії A. Виконання аналізу стійкості до ВЗП потрібно для того, щоб показати, що в цьому разі застосування функційної різноманітності (див. 5.3.1.5.5b)) забезпечує ефективний захист від ВЗП. Обидві функції виконуються в незалежних системах класу 1, які базуються на однаковому сімействі устаткування.

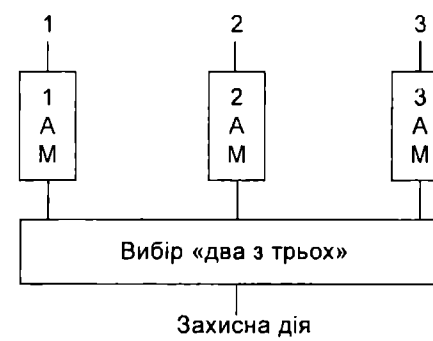
FA—FX. До складу цієї групи безпеки входить основна функція FA1 категорії A та додаткові функції категорій B та C, і функція FX як засіб дублювання. Аналіз має показувати, що в цьому разі застосування різноманітного устаткування (див. 5.3.1.5.5d)) забезпечує достатньо ефективний захист від ВЗП. Функцію FA призначають системі класу 1, а функцію FX — системі класу 2, виконаній на іншому сімействі устаткування для забезпечення апаратної різноманітності.

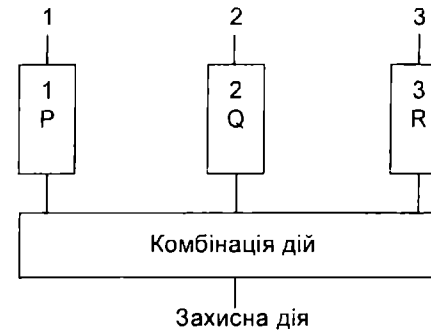
FB1—FB. До складу цієї групи безпеки належать дві функційно різні функції FB1 та FB категорії B. Аналіз має показувати, що застосування різноманітного устаткування та функційної різноманітності забезпечують достатньо ефективний захист від ВЗП. Функцію FB1 призначають системі класу 1, а функцію FB — системі класу 2, виконаній на іншому сімействі устаткування, для забезпечення апаратної різноманітності.

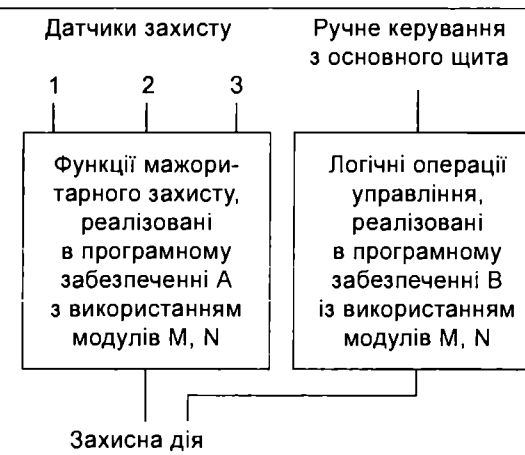
Випадки FC1 та FC подібні до попереднього.

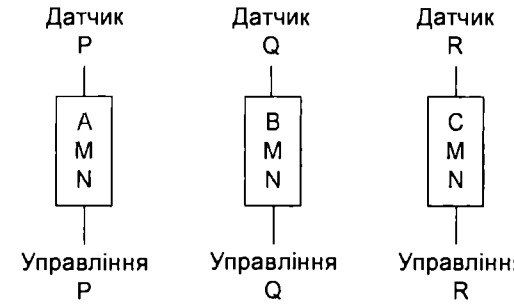
C.2 Приклади чутливості до ВЗП у групах безпеки

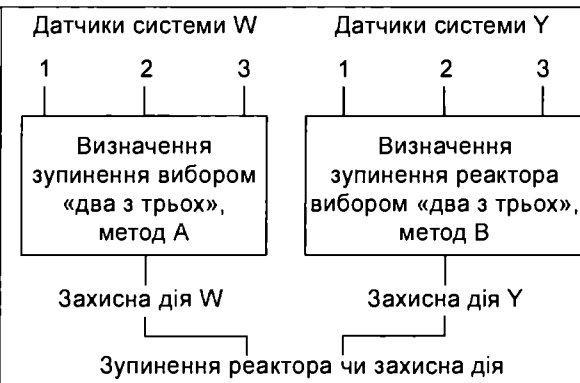
Можуть відбуватися наведені нижче типові ситуації.

***Приклад* 1** Група безпеки, що складається із системи з трьох однакових резервних каналів, які виконують єдину функцію захисту A	
Імовірність виникнення ВЗП Імовірність: (H) = висока; (M) = середня; (L) = низька	Можливий захист Ефективність: (H) = висока; (M) = середня; (L) = низька
Помилка в технічному завданні до прикладної функції A(H)	Незалежна верифікація технічного завдання (M)
Дефект у специфікації або під час розробляння прикладного програмного забезпечення, або дефект у модулі системного програмного забезпечення (M). Відмова може бути наслідком проходження однакових сигналів за трьома каналами ((L) для систем класу 1)	Розроблення системи класу 1 (H)
Одночасна відмова технічного забезпечення трьох каналів унаслідок небезпеки для станції	Фізична, електрична незалежність (H)
Відмова під час вибирання «2 з 3» (або за інших дій, ужитих каналами)	Розроблення системи класу 1(H); надійний зворотний зв'язок від досвіду експлуатації (стандартний модуль) (H)

Приклад 2 Група безпеки, що складається із системи з резервованими каналами, які виконують єдину функцію захисту A, з однаковим технічним завданням і різним програмним забезпеченням (блоки P, Q, R)	
Можливі випадки ВЗП Імовірність: (H) = висока; (M) = середня; (L) = низька	Можливий захист Ефективність: (H) = висока; (M) = середня; (L) = низька
Помилка в технічному завданні до прикладної функції A (H)	Те саме, що в прикладі 1
Дефект у специфікації або під час розробляння прикладного програмного забезпечення, або дефект у модулі (M) системного програмного забезпечення. Відмова може бути наслідком проходження однакових сигналів за трьома каналами (L)	Розроблення системи класу 1 (H) Недоліки: багаторазове впровадження програмного забезпечення
Одночасна відмова апаратури трьох каналів унаслідок небезпеки для станції	Те саме, що в прикладі 1
Відмова під час вибирання «2 з 3» (або за інших дій, ужитих каналами)	Те саме, що в прикладі 1

Приклад 3 Група безпеки, що складається із системи з двома каналами, що виконують одну захисну дію в різний спосіб * * Вважають, що оператор має достатньо часу й інформації, щоб зреагувати	
Можливі випадки ВЗП Імовірність: (H) = висока; (M) = середня; (L) = низька	Можливий захист Ефективність: (H) = висока; (M) = середня; (L) = низька
Помилка в технічному завданні обох функцій (L)	Захист забезпечується внаслідок використання функційної різноманітності (автоматично, уручну) (H)
Дефект у специфікації або під час розробляння прикладного програмного забезпечення, або дефект у модулях M, N загального системного програмного забезпечення ((L) за асинхронної роботи)	Розроблення системи класу 1 (H)
Одночасна відмова апаратури каналів системи внаслідок небезпеки для станції	Те саме, що в прикладі 1
Відмова під час вибирання «2 з 3» (або під час інших дій, ужитих каналами)	Ручне керування, що діє після вибору (H)

***Приклад* 4** Група безпеки, що має у своєму складі розподілені різні функції захисту P, Q, R, які використовують різні датчики та виконавчі механізми й однакове апаратне забезпечення в кожному каналі керування	
Можливі випадки ВЗП Імовірність: (H) = висока; (M) = середня; (L) = низька	Можливий захист Ефективність: (H) = висока; (M) = середня; (L) = низька
Помилка в технічному завданні до трьох функцій (L)	Захист забезпечується внаслідок використання функційної різноманітності (P, Q, R) (H)
Дефект у специфікації або під час розробляння прикладного програмного забезпечення або дефект у модулях M, N загального системного програмного забезпечення ((L) за асинхронної роботи). Траєкторії сигналу різні (L)	Цілком незалежне апаратне забезпечення. Розроблення системи класу 1(H)
Одночасна відмова апаратного забезпечення каналів системи внаслідок небезпеки для станції	Те саме, що в прикладі 1
Відмова під час вибирання «2 з 3» (або за інших дій, ужитих каналами)	Ручне керування, що діє після вибору (H)

***Приклад* 5** Група безпеки, що складається з диверсних функцій захисту W та Y, розподілених за двома різними системами (диверсне апаратне та програмне забезпечення з можливою подібністю, наприклад, можливі подібні алгоритми, час виконання операцій, документація та загальний персонал)	
Можливі випадки ВЗП Імовірність: (H) = висока; (M) = середня; (L) = низька	Можливий захист Ефективність: (H) = висока; (M) = середня; (L) = низька
Помилка в технічному завданні до обох функцій (L)	Захист забезпечується внаслідок використання функційної різноманітності (W, Y) (H)
Дефект у специфікації або під час розробляння прикладного програмного забезпечення, або дефект у модулях M, N загального системного програмного забезпечення ((L) за асинхронної роботи). Траєкторії сигналу різні (L). Імовірність кількох подібних траєкторій сигналу	Цілком незалежне апаратне забезпечення. Розроблення системи класу 1(H)
Одночасна відмова апаратного забезпечення каналів системи внаслідок небезпеки для станції	Те саме, що в прикладі 1
Відмова в обох виконавчих діях захисту (L)	Різні (різноманітні) виконавчі системи (H)

ДОДАТОК D
(довідковий)

ВЗАЄМОЗВ'ЯЗОК IEC 61508 з IEC 61513 ТА СТАНДАРТАМИ, ЯКІ ЗАСТОСОВУЮТЬ В ЯДЕРНОМУ СЕКТОРІ

У наведеному додатку цей стандарт порівнюють із частинами 1, 2 та 4 IEC 61508.

Частини 3, 5, 6 та 7 з IEC 61508 не розглядають, тому що вони виходять за межі дії цього стандарту. Наприклад, область дії частини 3 IEC 61508, що стосується програмного забезпечення, частково відображено в IEC 60880.

Цей додаток містить 4 розділи:

— D.1 ідентифікує основні відмінності між областями дії та концепціями двох стандартів;

— D.2 порівнює цей стандарт з IEC 61508-1 (загальні вимоги);

— D.3 порівнює цей стандарт з IEC 61508-2 (системні аспекти);

— D.4 порівнює цей стандарт з IEC 61508-4 (визначення).

D.1 Область дії і концепції

Перш за все під час порівняння розглядають деякі важливі відмінності в області дії двох стандартів.

Системи, описані в IEC 61508, можуть бути електричними, електронними або мати в основі програмовану електронну технологію, і хоча цей стандарт містить принципи архітектурних вимог до цих трьох технологій, його основну увагу зосереджено на комп'ютерних системах.

IEC 61508 стосується «систем, пов'язаних із безпекою», тоді як цей стандарт, спираючись на практику МАГАТЕ, стосується «систем, важливих для безпеки».

a) Область дії повного життєвого циклу безпеки

Повний життєвий цикл безпеки в IEC 61508 містить усі системи, визначені в проекті безпеки для устаткування, яке перебуває під керуванням, охоплюючи КВК-системи (E/E/ПЕ), інші технологічні системи та засоби захисту від зовнішньої небезпеки.

У цьому стандарті не описано окремо аналіз безпеки станції та засоби оцінення відповідності вимогам до характеристик та надійності, що випливають із цього аналізу. Практикою щодо ядерного сектору є виконання проекту безпеки станції відповідно до специфічних принципів МАГАТЕ, правил МЕК та національних норм, які не розглянуто в цьому стандарті. У проектній основі станції визначено постульовані вихідні події, їхні послідовності, концепція глибокоешелонованого захисту станції, категоризація функцій, потрібних для забезпечення захисту. Однак цей стандарт визначає вхідну інформацію, яку вимагають від основного проекту станції й аналіз безпеки, який має бути в розпорядженні розробників КВК-систем для настанов під час наступного проектування КВК-систем;

b) Загальна валідація/оцінка безпеки

У цьому стандарті загальну верифікацію та валідацію кожної розподіленої функції, важливої для безпеки, відображено у звіті із загальної інтеграції й уведення в експлуатацію.

В ядерному секторі оцінення достатності такого звіту стосовно безпеки регулюють рамками процедур ліцензування;

c) КВК-системи та КВК-архітектура

КВК-системи в цьому стандарті рівнозначні (E/E/ПЕ) IEC 61508. У цьому стандарті архітектура системи (див. розділ 5) визначає сукупність окремих систем певних класів та вимоги до незалежності виконання функцій, важливих для безпеки. Для кожної конкретної системи в розділі 6 визначають індивідуальний життєвий цикл безпеки. В IEC 61508 будь-який поділ на кілька систем розглянуто в частині 2.

Цю відмінність необхідно враховувати для уникнення непорозумінь;

d) Рівень цілісності безпеки та класифікація

IEC 61508 установлює градації вимог до цілісності безпеки щодо комп'ютерної системи залежно від ступеня зниження ризику, який має забезпечити ця система. Цього можна досягти визначенням жорсткої залежності між ступенем ризику, пов'язаним із небезпекою, й оціночною частотою небезпек та тим захистом, який має забезпечити ця система для зниження ризику від небезпеки до припустимого рівня.

Атомна промисловість традиційно використовує детерміністичний метод для визначення значимості системи для безпеки та її вплив на величину ризику, пов'язаного з можливим погіршенням її діяльності (див. настанови з безпеки МАГАТЕ та IEC 61226).

Зазвичай максимально можливу цілісність вважають необхідною для будь-якої системи, що запобігає або зменшує наслідки радіоактивних викидів. Нижчий рівень цілісності може бути прийнятним для систем, що забезпечують захист у разі таких викидів, але безпосередньо не запобігають або не знижують їх. Отже, в атомному секторі немає схеми для загального користування, рівнозначної запропонованій в IEC 61508, для зниження рівня цілісності безпеки системи залежно від надійності/ризику. Такий детерміністичний підхід вважають достатнім для ядерної індустрії, він приводить на практиці до встановлення вищих завдань для всіх захисних функцій. Однак у ядерному секторі визнають і кількісний підхід, а методи ймовірнісного аналізу безпеки можуть забезпечувати чіткіші завдання для надійності комп'ютерних систем.

Призначеність «рівнів цілісності» згідно з IEC 61508 майже цілком відповідає встановленню категорій в ядерній індустрії. Однак наявні значні відмінності в процедурі призначення:

— в IEC 61508 призначеність рівнів цілісності безпеки має в основі аналіз імовірності небезпеки та ризику;

— в IEC 61226 призначеність категорій має в основі детерміністичний критерій та інженерне судження щодо наслідків у разі несправності.

D.2 Відповідність між IEC 61508-1 та цим стандартом

IEC 61508-1	IEC 61513
5 Документація	5.5 Вихідна документація
6 Керування функційною безпекою	5.4.1 Згідно з IAEA 50-C-QA (Редакція 1) уся діяльність, пов'язана з атомними станціями, підпадає під програму забезпечення якості
7 Вимоги до повного життєвого циклу безпеки	5 Границі життєвого циклу безпеки КВК
7.1 Загальна частина	
Загальний життєвий цикл безпеки охоплює: електронні, електричні, електронні системи, що програмують/Інші технології/Зниження зовнішньої небезпеки	Загальний життєвий цикл безпеки охоплює КВК ФСБ, важливі для безпеки, й усю архітектуру систем (див. а) розділу D.1)
7.2 Концепція	
Опис керованого устаткування (УПК), необхідних функцій управління та фізичного навколишнього середовища	Огляд основного проекту безпеки станції (5.1): — визначення умов навколишнього середовища (5.1.3); — функції КВК, важливі для безпеки; — протиставлення автоматики та дій оператора
Ідентифікація джерел небезпек	Внутрішні та зовнішні небезпеки визначено в проектній основі безпеки станції і вони є вхідними даними для КВК (5.1.3) (див. а) розділу D.1)
7.3 Визначення загальної області дії	
Визначення границь УПК	Ідентифікація встановлених границь станції/КВК (5.1.3)
Визначити обсяг аналізу небезпеки, ризику та подій, що призводять до аварії	Постульовані вихідні події (ПВП) визначено в проектній основі безпеки станції і є вхідними даними для КВК (5.1) (див. а) розділу D.1)
7.4 Аналіз небезпеки та ризику	
Установлення небезпеки УПК	Не розглянуто в цьому стандарті, є частиною основного проекту безпеки (див. а) розділу D.1)
...і системи керування УПК	Детерміністичні обмеження для КВК, наприклад, критерії одиничної відмови для функцій категорії А, функційна ізоляція, що походять з основного проекту станції

IEC 61508-1	IEC 61513
Визначити послідовність подій, що перетворюються в небезпечні події	Послідовність постульованих вихідних подій (ПВП) визначено в основі проекту безпеки станції і є вихідними даними для КВК-систем (див. 5.1) (див. а) розділу D.1)
Визначити ризик УПК	Категоризація КВК ФСБ є вхідними даними для КВК (див. 5.1.2) (див. а) розділу D.1)
7.5 Загальні вимоги щодо безпеки	5.2 Загальне технічне завдання до КВК ФСБ
Специфікація необхідних функцій безпеки Вони охоплюють:	Загальне технічне завдання до функцій КВК, важливих для безпеки, що походять з основи проекту станції. Вони охоплюють:
— технічне завдання до функцій безпеки	— технічне завдання до функцій і характеристик (а)1) з 5.2))
— технічне завдання до цілісності безпеки	— Специфікацію категорій КВК ФСБ (а)3) з 5.2)) — технічне завдання до незалежності (а)3) з 5.2))
Загальне технічне завдання до безпеки охоплює КВК (Е/Е/ПЕ системи), системи інших технологій і засоби зниження ризику	Інша технологія та заходи зниження ризику визначено в проектній основі безпеки станції відповідно до принципів глибокоешелонованого захисту. Вони перебувають поза сферою дії цього стандарту (див. а) розділу D.1)
7.6 Призначення вимог щодо безпеки	5.3.1 Проект архітектури КВК 5.3.2 Призначення функцій
Призначення системам функцій безпеки та призначення рівня цілісності безпеки кожній функції. Розглядають імовірність ВЗП (7.6.2.7), а завдання цілісності безпеки обмежено для одної Е/Е/ПЕ (7.6.2.11)	Розкладання всіх КВК на індивідуальні КВК-системи відповідного класу. Призначення системам функції КВК відповідно до класифікації, глибокоешелонованого захисту, враховуючи ВЗП
Загальне планування	5.4 Загальне планування
6 Керування функційною безпекою	5.4.1 Загальні програми забезпечення якості
7.8 Загальне планування валідації безпеки	5.4.3 Загальні плани інтеграції й уведення в експлуатацію
	5.4.2 Загальний план захисту
7.9 Загальний план установлення й уведення в експлуатацію	5.4.3 Загальні плани інтеграції й уведення в експлуатацію
7.7 Загальне планування експлуатації та технічного обслуговування	5.4.4 Загальний план експлуатації
	5.4.5 Загальний план технічного обслуговування
7.10 Реалізація Е/Е/ПЕС	6 Життєвий цикл безпеки системи
Див. IEC 61508-2 (системні аспекти)	Див. розділ 6 (життєвий цикл безпеки системи)
Див. IEC 61508-3 (вимоги до програмного забезпечення)	Програмне забезпечення перебуває поза сферою дії цього стандарту
7.11 Реалізація: інша технологія	Перебуває поза сферою дії цього стандарту (див. а) розділу D.1)
7.12 Реалізація: зовнішні засоби зменшення ризику	Перебуває поза сферою дії цього стандарту (див. а) розділу D.1)
7.13 Загальне установлення й уведення в експлуатацію	7 Загальна інтеграція й уведення в експлуатацію
7.14 Загальна валідація безпеки Валідація Е/Е/ПЕ, згідно з загальним технічним завданням, відповідно до призначеності	7.1 Загальне введення в експлуатацію Верифікація та валідація функцій, важливих для безпеки, виконуваних у більше ніж одній системі 6.4 Кваліфікація системи

IEC 61508-1	IEC 61513
7.15 Загальна експлуатація, технічне обслуговування та ремонт	8 Загальна експлуатація та технічне обслуговування
7.16 Загальна модифікація та вдосконалення	1 Сфера дії стандарту Цей стандарт (або підмножина) застосовний до КВК нових АЕС, а також до модернізованих або вдосконалених
7.17 Виведення з експлуатації або утилізація	Перебуває поза сферою дії цього стандарту
7.18 Верифікація	5.4.1 Загальні програми забезпечення якості
8 Оцінка функційної безпеки Отримання відомостей і підтвердження досягнень функційної безпеки Е/Е/ПЕ-систем	В ядерному секторі таке оцінення пов'язано з процесом ліцензування та залежить від органів контролю за безпекою та національних норм

D.3 Відповідність між IEC 61508-2 та цим стандартом

IEC 61508-2	IEC 61513
5 Документація	6.3 Вихідна документація
6 Керування функційною безпекою	5.4.1 Загальні програми забезпечення якості
7 Вимоги до життєвого циклу безпеки Е/Е/ПЕ-систем Життєвий цикл безпеки Е/Е/ПЕ-систем охоплює цілі та вимоги до Е/Е/ПЕ-систем	6 Життєвий цикл безпеки системи Життєвий цикл безпеки системи охоплює цілі та вимоги до конкретних КВК-систем архітектури КВК (див. позицію с) розділу D.1)
7.1 Загальні положення У таблиці 1 для всіх етапів зазначено цілі та вимоги, обсяг етапу, необхідні вхідні дані етапу, необхідні вихідні дані	У таблиці 3 для всіх етапів зазначено цілі та вимоги, необхідні для етапу вхідні дані, необхідні вихідні дані
7.2 Технічне завдання з безпеки Е/Е/ПЕС містить:	6.1.1 Технічне завдання до системи містить:
— технічне завдання до функції безпеки;	— технічне завдання до прикладних функцій; — технічне завдання до сервісних функцій; — умови навколишнього середовища (6.1.1.5)
— технічне завдання до цілісності безпеки	— категоризацію КВК-функцій (вхідні дані з 5.2); вимоги до проектних обмежень системи (6.1.1.2); — класифікацію системи
Примітка. Зазначені розділи з IEC 61508 та цього стандарту охоплюють однакові проблеми, але в цьому стандарті є розбіжності між вимогами до КВК-функцій та вимогами до КВК-систем, які виконують такі функції.	
7.3 Планування валідації безпеки Е/Е/ПЕС	6.2 Планування системи
	— План валідації системи (6.2.4); — Функційна валідація технічного завдання до прикладних функцій (6.1.3.1.1); — Кваліфікація системи (6.4)
7.4 Розроблення та проектування Е/Е/ПЕС	6.1.2 Специфікація системи 6.1.3 Детальний проект та реалізація системи
7.4.2 Загальні вимоги	— Проектні обмеження (6.1.1.2) — Архітектура системи (6.1.2.2)
7.4.3 Вимоги цілісності безпеки технічного забезпечення	— Вимоги, пов'язані з проектними обмеженнями (6.1.1.2) — Додаток С — Вимоги до перевірюваності
7.4.4 Вимоги до запобігання відмовам	— Цикл безпеки системи (розділ 6)
7.4.5 Вимоги до керування систематичними дефектами	— Захист від поширення та побічних дій відмов (6.1.2.2.3)

IEC 61508-2	IEC 61513
7.4.6 Вимоги щодо поводження системи в разі виявлення дефектів	— Архітектура системи (6.1.1.2.1) — Самоконтроль і стійкість до відмов (6.1.1.2.3)
7.4.7 Вимоги до введення в експлуатацію Е/Е/ПЕС-систем	— Вибір устаткування (6.1.2.1)
7.4.8 Вимоги до передавання даних	— Внутрішнє поводження системи (6.1.2.2.2)
7.5 Інтеграція Е/Е/ПЕ-систем	6.1.4 Інтеграція системи
7.6 Експлуатація та технічне обслуговування Е/Е/ПЕ-систем	6.2.6 План експлуатації системи
7.7 Валідація безпеки Е/Е/ПЕ-систем	6.1.5 Валідація системи
7.8 Модифікація Е/Е/ПЕ-систем	6.1.7 Модифікація системи
7.9 Верифікація Е/Е/ПЕ-систем	6.2.1.1 План верифікації системи
8 Оцінення функційної безпеки див. IEC 61508-1	Див. розділ D.2

D.4 Відповідність між деякими важливими термінами IEC 61508-4 та визначеннями цього стандарту в секторі ядерного застосування

Тема: Аналіз ризику	
IEC 61508-4	**IEC 61513**
3.1.2 Небезпека Потенційне джерело шкоди (настанова ISO/IEC 512) **Примітка.** Термін містить поняття небезпеки для персоналу, що виникає за короткий проміжок часу (наприклад, пожежа та вибух), а також небезпеки, що довгостроково впливає на здоров'я людини (наприклад, викид токсичної речовини)	**3.27 Небезпека**
Тема: Глибокоешелонований захист	
IEC 61508-4	**IEC 61513**
3.4.3 Зовнішні засоби зменшення ризику Засоби зменшення або пом'якшення ризиків, окремі або ті, що не використовують Е/Е/ПЕ чи інші технології систем, пов'язаних із безпекою	**Концепція глибокоешелонованого захисту (див. розділ А.3)** Концепцію зменшення зовнішнього ризику неявно реалізують в аналізі безпеки атомної станції на основі концепції глибокоешелонованого захисту і ліній захисту
Тема: Системи, важливі для безпеки	
IEC 61508-4	**IEC 61513**
3.4.1 Система, пов'язана з безпекою позначає систему, що одночасно: — виконує необхідні функції безпеки, потрібні для забезпечення або підтримання безпечного стану УПК; і — призначена досягати своїми засобами або разом з іншими Е/Е/ПЕ-системами, пов'язаними з безпекою, і системами інших технологій, пов'язаними з безпекою, або зовнішніми засобами для зменшення ризику, необхідної цілісності безпеки, якої вимагають функції безпеки	**3.37 Елементи, важливі для безпеки**
Тема: КВК-системи	
IEC 61508-4	**IEC 61513**
3.2.6 Електрична/електронна/програмована електронна (Е/Е/ПЕ) На основі електричної (Е) та/або електронної (Е), та/або програмованої електронної (ПЕ) технології	**3.35 КВК-системи**

Тема: Надійність	
IEC 61508-4	**IEC 61513**
3.5.2 Цілісність безпеки Імовірність задовільного виконання системою, пов'язаною з безпекою, необхідних функцій безпеки за будь-яких заданих умов протягом установленого проміжку часу. **Примітка 3.** У визначення цілісності безпеки треба включити всі причини відмов (як випадкові відмови технічного забезпечення, так і систематичні відмови), які призводять до небезпечного стану, наприклад відмови апаратного забезпечення, відмови програмного забезпечення та відмови, спричинені електричними перешкодами. Деякі типи відмов, зокрема випадкові відмови технічного забезпечення, можуть бути виражені кількісно з використанням таких параметрів, як інтенсивність відмов у небезпечному режимі відмов або ймовірність того, що систему захисту, пов'язану з безпекою, не буде приведено до дії на вимогу. Однак цілісність безпеки системи також залежить від багатьох чинників, які не можна точно виразити кількісно, а тільки якісно	**3.50 Надійність** У цьому стандарті оцінка надійності зазвичай якісна (див. 6.1.1.1.1) (див. 6.1.1.1 та 6.1.3.1.1)
Тема: Класифікація систем, важливих для безпеки	
IEC 61508-4	**IEC 61513**
3.5.6 Рівень цілісності безпеки Дискретний рівень (один із чотирьох можливих) для визначення вимог до цілісності безпеки, які треба висувати до функцій безпеки, що виконують E/E/ПЕ-системи, де рівень цілісності безпеки 4 є найвищим рівнем цілісності безпеки, а рівень 1 — найнижчим	**3.6 Клас КВК-систем** Усі компоненти, структури та системи, пов'язані з безпекою, класифікують на основі їхніх функцій і важливості з погляду безпеки, і проектують, виробляють та вводять у дію так, що їхня якість відповідає класифікації (розділ 68 IAEA 75-INSAG-**3**). 8.2.2 IEC 61226 накладає обмеження на надійність до потрібного значення (10^{-4}) для систем, до яких належить програмне забезпечення. Для деяких систем цільові показники надійності може бути перевищено величинами, які можна продемонструвати. Якщо це необхідно для забезпечення вищої функційної надійності, застосовують додаткові незалежні системи, кожна з яких здатна виконувати призначену їй функцію безпеки. Різноманітність і фізичне розділення даних систем зменшують можливість відмов за загальною причиною (цільові показники надійності 4.2.2.3.132 IAEA 75-INSAG-3)
Тема: Відмова за загальною причиною	
IEC 61508-4	**IEC 61513**
3.6.10 Відмова за загальною причиною Відмова, що є результатом одної або кількох подій, які спричиняють одночасні відмови двох чи більше окремих каналів у багатоканальній системі, що призводить до відмови системи. **Примітка.** У 7.6.2.7 IEC 61508-1 наведено вимоги до незалежності двох систем. У 7.6.2.8 показано, що достатню незалежність може бути продемонстровано за допомогою аналізу, навіть якщо не всі вимоги може бути виконано	**3.7 Відмова за загальною причиною** Див. 5.3.1.5

БІБЛІОГРАФІЯ

1 IEEE 610:1992 IEEE standard Computer Dictionary, Compilation of IEEE Standard Computer Glossaries (Стандартний комп'ютерний словник IEEE, компіляція стандартних комп'ютерних словників IEEE)

2 IEEE 830:1998 IEEE Recommended Practice for Software Requirements Specifications (Рекомендована IEEE-практика специфікації вимог до програмного забезпечення)

3 IEEE 828:1998 IEEE Standard for Software Configuration Management Plants (Стандарт IEEE за планами управління конфігурацією програмного забезпечення)

4 NUGER-0800 USNRS Standard Review Plan. Section 7.0 (6/97) (Національні ядерні стандарти США. Стандартний план експертизи. Розділ 7.0 (6/97))

5 EWICS Position paper 6 (1/85) System requirements specification for safety related systems (Специфікація системних вимог для систем, пов'язаних із безпекою)

6 CEI 61069-2:1993 Industrial-process measurement and control — Evolution of system properties for the purpose of system assessment — Part 2: Assessment methodology (Вимірювання та керування у виробничих процесах. Визначення властивостей системи з метою оцінення системи. Частина 2. Методологія оцінювання)

7 CEI 61131-1:1992 Programmable controllers — Part 1: General information (Програмовані контролери. Частина 1. Загальна інформація)

8 CEI 61225:1993 Nuclear power plants-Instrumentation and control systems important for safety — Requirements for electrical supplies (Атомні електростанції. Інформаційні та керівні системи, важливі для безпеки. Вимоги до електроживлення).

ДОДАТОК НА
(довідковий)

ПЕРЕЛІК НАЦІОНАЛЬНИХ СТАНДАРТІВ, ЗГАРМОНІЗОВАНИХ ІЗ МІЖНАРОДНИМИ НОРМАТИВНИМИ ДОКУМЕНТАМИ, НА ЯКІ Є ПОСИЛАННЯ В ЦЬОМУ СТАНДАРТІ

ДСТУ IEC 60780:2007 Атомні електростанції. Обладнання системи безпеки електричне. Кваліфікація (IEC 60780:1998, IDT)

ДСТУ IEC 60880:2008 Атомні електростанції. Інформаційні та керувальні системи, важливі для безпеки. Програмні аспекти комп'ютерних систем, які виконують функції категорії А (IEC 60880:2006, IDT)

ДСТУ IEC 61000-4-1:2007 Електромагнітна сумісність. Частина 4-1. Методики випробування та вимірювання. Огляд стандартів серії IEC 61000-4 (IEC 61000-4-1:2006, IDT)

ДСТУ IEC 61069-1:2007 Вимірювання та керування в промислових процесах. Визначення властивостей системи для її оцінення. Частина 1. Загальні аспекти та методологія (IEC 61069-1:1991, IDT)

ДСТУ IEC 61226:2007 Атомні електростанції. Інформаційні та керівні системи, важливі для безпеки. Класифікація контрольно-вимірювальних та керівних функцій (IEC 61226:2005, IDT)

ДСТУ ISO 9001–2001 Системи управління якістю. Вимоги (ISO 9001:2000, IDT).

Код УКНД 27.120.20

Ключові слова: атомна електростанція; вимоги щодо безпеки; контрольно-вимірювальна та керівна система (КВК): життєвий цикл, структура; програмне забезпечення; функції категорії А, В та С.
