https://doi.org/10.31891/2219-9365-2022-70-2-12
УДК 339

Олег САВЕНКО
Хмельницький національний університет
https://orcid.org/0000-0002-4104-745X
e-mail: savenko_oleg_st@ukr.net
Людмила КОРЕЦЬКА
Хмельницький національний університет
https://orcid.org/0000-0002-4284-4936
e-mail: koretskal@khmnu.edu.ua
Денис ХОМА
Хмельницький національний університет
https://orcid.org/0000-0001-7256-4997
e-mail: denis.khoma@gmail.com

ПІДВИЩЕННЯ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ ПРОТИПОЖЕЖНОГО КОНТУРУ АВТОМАТИЗОВАНОЇ СИСТЕМИ

В роботі наведено результати досліджень надійності, функціональної безпеки протипожежного контуру автоматизованої системи та встановлено основні методи зменшення ймовірності виходу з ладу контуру із використанням резервуванням елементів автоматизованої системи.
Ключові слова: функціональна безпека, допустима ймовірність відмов, рівень повноти безпеки, резервування.

Oleg SAVENKO, Liudmyla KORETSKA, Denis KHOMA
Khmelnytskyi National University

INCREASING THE FUNCTIONAL SECURITY OF THE FIRE PROTECTION CIRCUIT OF THE AUTOMATED SYSTEM

The use of automated systems allows to increase productivity and efficiency of technological processes, to optimize work at the enterprise. The efficiency of using automated systems is affected by reliability. There are a number of principles to maintain reliability at the required level. One of these is the reliability analysis in the form of an assessment of the fault-free operation of the automated system. However, reliability is determined by other parameters that relate to the functional safety of the automated system. The main indicator of the functional safety of an automated system is the probability of its error-free operation, the value of which can be increased in several ways. In particular, this is redundancy, duplication of some elements, circuits, or even the entire system as a whole. One or another redundancy method is used depending on the goals, economic opportunities, type of industry, and the required value of the safety integrity level SIL. The main tools for assessing the safety integrity level are the established norms of functional safety in the international standards IEC 61508, IEC 61511. Depending on the established safety integrity level SIL, the enterprise implements the necessary measures to protect employees, society, equipment and products, and the environment. This paper analyzes the risks associated with the failure of elements of the fire safety circuit of the automated system. An approach to increasing the functional safety of the fire circuit has been developed, which consists in the possibility of reserving elements of the sensor subsystem, a design evaluation of the proposed redundant system has been carried out, the result of which is a reduction in the risks of failure of the automated system and an increase in the probability of its trouble-free operation.
Keywords: functional safety, acceptable probability of failures, safety integrity level, redundancy.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

Функціональна безпека промислового обладнання потребує все більшої уваги. Особливо це стосується галузей промисловості, що пов'язанні із високими ризиками, наприклад, нафтогазова промисловість, електростанції, хімічна промисловість та ін. Для безпечного функціонування систем на таких підприємствах запроваджують системи безпеки, які у випадку виникнення аварійної ситуації відключають обладнання або переводять його у стан безпечної роботи. До систем безпеки висуваються високі вимоги щодо надійності та працездатості. Тому на етапах проектування та експлуатації систем безпеки потрібно оцінювати параметри надійності функціонування. Щоб оцінити ризики збою, ймовірність відмови системи, надійність системи використовують норми функціональної безпеки, що викладені у стандартах IEC 61508 [1], IEC 61511 [2]. Згідно стандарту IEC 61508 всі відмови обладнання класифікують на наступними ознаками: виявлені, невиявлені та небезпечні, безпечні. У сукупності за цими ознаками виділяють чотири види відмов: безпечні виявлені, небезпечні виявлені, безпечні невиявлені, небезпечні невиявлені. При розрахунках функціональної безпеки системи протиаварійного захисту враховують лише небезпечні відмови. Це пов'язано з тим, що при небезпечній відмові функція безпеки не виконується, а обладнання переводиться у небезпечний стан. Також, окрім зазначених видів відмов враховують відмову за загальними причинами, коли відбувається ситуація одночасної відмови двох або більше каналів багатоканальної системи і функція безпеки не виконується.

Поняття надійності характеризує властивість зберігати у часі в установлених межах значення всіх параметрів, які характеризують здатність виконувати потрібні функції в заданих режимах та умовах застосування, технічного обслуговування, зберігання та транспортування, і є комплексною властивістю, що залежно від призначення об'єкта і умов його застосування, може містити в собі безвідмовність, довговічність, ремонтопридатність та збережуваність чи певні поєднання цих властивостей [3]. Термін безпека автоматизованої системи управління визначає властивість системи не переходити у небезпечний стан, при якому можуть виникати наслідки з великими масштабами втрат. До таких втрат можна віднести життя та здоров'я людини, екологічну безпеку навколишнього середовища, економічні та матеріальні втрати та ін.

Для уникнення критичних ситуацій автоматизовані системи повинні містити у своєму складі системи протиаварійної безпеки. Основними задачами таких систем є переведення автоматизованої системи у безпечний стан, який може виникати при виході технологічних процесів за встановлені рамки, позаштатні ситуації, відмова обладнання. До функцій систем протиаварійної безпеки відносять сукупність дій, що направлені на зниження небезпеки, яка може бути пов'язана із функціонуванням автоматизованої системи. Також функціями безпеки є: можливість автоматичного визначення зміни стану автоматизованої системи, що може бути потенційно небезпечним; автоматичне вимірювання змінних, що можуть характеризувати технологічний об'єкт як такий, який є близьким до безпечного функціонування; автоматична діагностика відмов; автоматична передаварійна сигналізація; автоматичний захист від несанкціонованого доступу до вибору режимів роботи системи протиаварійної безпеки та параметрів її налаштування.

Головною метою будь-якої автоматизованої системи є її відмовостійкість. Для підвищення відмовостійкості у системах автоматизації використовується резервування або дублювання апаратних та програмних компонентів системи, використання елементів для побудови автоматизованої системи із підвищеною надійністю, впровадження безперервного контролю за станом системи як програмно, так і людиною, а також впроваджувати можливість діагностики системи, що надає можливість попередити та не допустити факт аварійного стану системи. Резервуванням називається спосіб забезпечення надійності об'єкта за рахунок використання додаткових засобів та (або) можливостей, надлишкових відносно мінімально необхідних для виконання потрібних функцій [3]. Із використанням резервування, тобто із використанням надлишковості елементів, підвищується надійність функціонування автоматизованої системи.

Виклад основного матеріалу. Для оцінки міри функціональної безпеки існує поняття допустимої ймовірності відмови, на основі якої вводять чотири рівні повноти безпеки SIL (Safety Integrity Level) (табл. 1).

Таблиця 1

Класифікація рівнів безпеки залежно від середньої ймовірності небезпечної відмови виконання функції безпеки по запиту (режим з низькою частотою запитів) [1], [4]

Інтегральний рівень безпеки SIL	Допустима ймовірність відмов PFD_{avg}	Необхідний захист
SIL4	$10^{-5}...10^{-4}$	Незначний захист устаткування та продукції
SIL3	$10^{-4}...10^{-3}$	Значний захист устаткування та продукції, захист від можливих травм обслуговуючого персоналу
SIL2	$10^{-3}...10^{-2}$	Захист обслуговуючого персоналу та суспільства (некатастрофічний вплив)
SIL1	$10^{-2}...10^{-1}$	Захист від катастрофічного впливу на суспільство

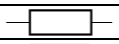
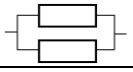
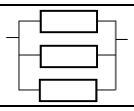
Найнижчому рівню безпеки SIL1 відповідає найменша ймовірність відмови *PFD*: $10^{-2}...10^{-1}$, а найвищому – SIL4 - $10^{-5}...10^{-4}$. Найвищий рівень безпеки SIL4 повинен забезпечуватись, наприклад, у атомній енергетиці, у інших галузях залежно від типу інструментальної функції може бути достатньо SIL3 або SIL2.

Існуючі вимоги щодо розробки системи протиаварійної безпеки автоматизованої системи включали в себе аналіз працездатності контурів безпеки та оцінку небезпеки. Щонайменше для двох типів відмов – «неспрацювання» та «хибне спрацювання» – повинні бути встановлені показники надійності та постійно перевірятись. У табл. 2 наведено типові архітектури резервування підсистем системи протиаварійної безпеки та визначені показники відмовостійкості щодо хибних та небезпечних відмов.

Наприклад, архітектуру резервування 1oo2 використовують для зниження ймовірності пропуску запиту на виконання функції безпеки. Але така архітектура є зовсім неефективною при «хибному спрацюванні», оскільки сигнал буде з'являтись одразу у двох каналах. При використанні архітектури 2oo3 ймовірність відмови на запит майже не знижується. А от тип відмови «хибне спрацювання» відбудеться у випадку, якщо хибний сигнал з'явиться у обох каналах, що є досить малоймовірною подією.

Таблиця 2

Відмовостійкість системи (контуру) до різних типів відмов [5]

Архітектура	Структурна схема надійності	Відмовостійкість до відмов типу	
		«неспрацювання»	«хибне спрацювання»
1oo1		–	–
1oo2		+	–
2oo2		–	+
2oo3		+	+

Для підвищення надійності автоматизованої системи окрім резервування застосовують і інші методи, які є характерними саме для автоматизованих систем та для автоматизованих систем управління технологічними процесами. Такими методами є використання блокуючих модулів, із використанням яких відбувається блокування зовнішніх впливів та забезпечується підвищення ймовірності безвідмовної роботи системи. Наприклад, для забезпечення захисту від коливання напруги у мережі застосовують блоки безперебійного живлення та стабілізатори, бар'єри та ін.

Розглянемо можливості забезпечення функціональної безпеки протипожежного контуру вентиляційної системи [6]. Вентиляційні системи є важливим елементом у роботі хімічних, нафтових та інших підприємств, часто застосовуються у жилих приміщеннях, є невід'ємною складовою у місцях скупчення людей, де забезпечити притік та відтік повітряних мас природним шляхом є досить складно, наприклад, метро, тунелі і т.д. Перебування вентиляційної системи у справному стані продовж тривалого періоду є досить важливою. Як видно із функціональної схеми автоматизованої вентиляційної системи припливного типу (рис. 1) така система обладнана додатково контуром протипожежної безпеки. Задачею контуру є під час виникнення пожежі у приміщенні перекрити приплив повітря за допомогою закриття повітряного клапану, що не дасть змогу пожежі збільшувати свої потужності. У разі виходу з ладу елементів контуру протипожежної безпеки наявність пожежі у приміщенні може бути не зафіксована, а заслінка, через яку відбувається нагнітання повітря у приміщення не перекрита, що призведе до ще більшого розповсюдження пожежі.

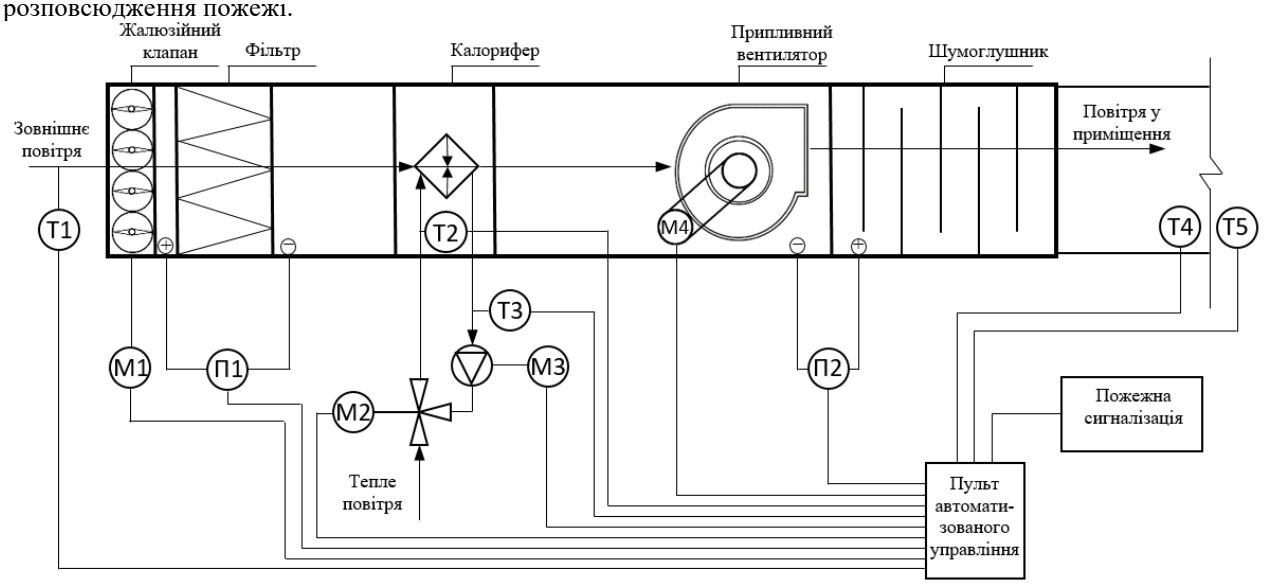


Рис. 1. Функціональна схема автоматизованої вентиляційної системи припливного типу, де давачі температури: Т1 –зовнішнього повітря, Т2 – повітря, що надходить після змішувача у калорифер, Т3 – повітря, що надходить на змішувач, Т5 – нагрітого (або охолодженого) повітря, що надходить у приміщення; Т4 – давач пожежної сигналізації; виконавчі механізми: М1 – для закриття/відкриття жалюзійного клапана, М2 – для роботи змішувача повітря, М3 – для роботи насосу, М4 – для роботи двигуна припливного вентилятора; реле перепаду тиску: П1 – на фільтрі, П2 – на вентиляторі

Із використанням контролера, який знаходиться у щитку, відбувається управління вентиляційною автоматизованою системою та забезпечується автоматичне підтримування необхідного значення температури у приміщенні. Основним елементом контуру протипожежної безпеки є давач пожежної сигналізації, який фіксує наявність диму (пожежі) у приміщенні.

Для оцінки надійності автоматизованої системи використовуються показники ймовірностей працездатності системи згідно стандартів IEC 61508 [1] та 61511 [2]. До основних показників безпеки відносять середню ймовірність відмов PFD_{avg}, інтенсивність відмов λ, частка безпечних відмов *SFF*, відмовостійкість обладнання *HFT*.

Середню ймовірність відмов контуру визначають як суму ймовірностей відмов трьох підсистем: підсистеми давачів, логічної підсистеми, підсистеми виконавчих елементів (1):

$$PFD_K = PFD_S + PFD_L + PFD_{FE}, \quad (1)$$

де PFD_S, PFD_L, PFD_{FE}, PFD_K - середні ймовірності відмов за запитом підсистеми давачів, підсистеми логічних елементів, підсистеми виконавчих елементів та контуру відповідно.

Функція безпеки для запропонованої автоматизованої вентиляційної системи полягає у перекритті потоку повітря у приміщення у разі виникнення пожежі у ньому. *PFD* визначатиметься окремо для кожної підсистеми контуру пожежної безпеки (рис. 2), за формулою (1).

Рис. 2. Узагальнена структурна блок-схема контуру безпеки

А загальна ймовірність відмов є сумою ймовірностей відмов кожного елементу та підсистем окремо. Для цього на основі значень *PFD* кожного елемента та підсистем визначають PFD_K контуру протипожежної безпеки автоматизованої системи.

З метою виявлення можливих комбінацій відмов будується блок-схема надійності системи безпеки із врахуванням архітектури побудови кожної з підсистем: підсистема давачів побудована за архітектурою голосування 2oo3, логічна підсистема та підсистема виконавчих елементів – 1oo1 (рис. 3).

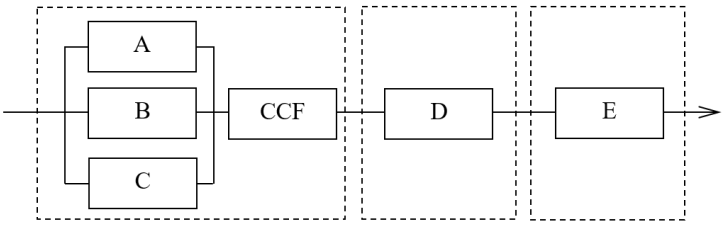


Рис. 3. Блок-схема надійності системи безпеки

Блок-схема надійності системи безпеки вказує на наявність можливих чотирьох відмов: (A, B, C) – потрійна відмова каналів у підсистемі давачів, (CCF), (D), (E) – одиночні відмови, де CCF – відмова за загальними причинами.

Підсистема давачів реалізована за архітектурою 2oo3 і складається із давачів, блокуючих елементів (бар'єри іскрозахисту), та інтерфейсів вводу/виводу. Для послідовного уточнення обчислювальної моделі підсистеми давачів застосовано метод багаторівневої структурної декомпозиції, який полягає у розбитті всієї моделі на її складові (рис. 4).

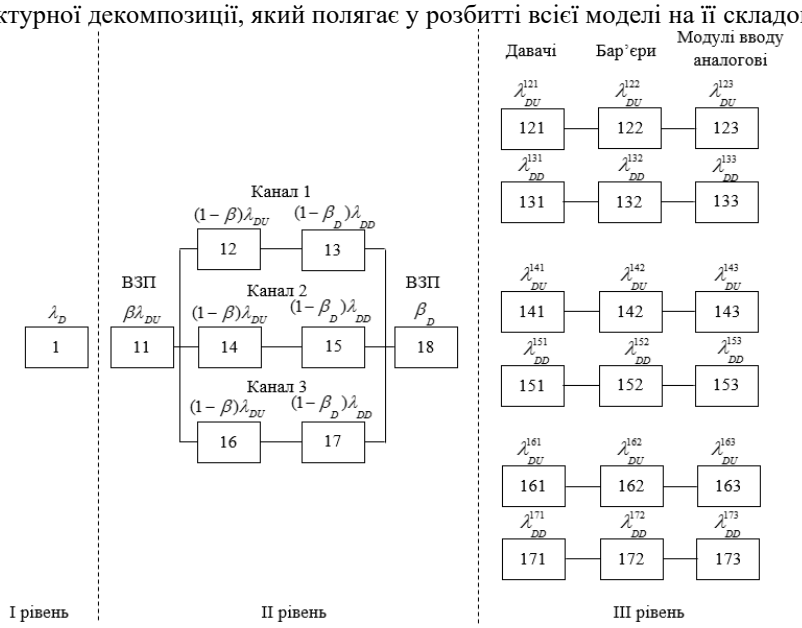


Рис. 4. Схема функціональної цілісності підсистеми давачів за архітектурою 2oo3

Така модель складається з трьох рівнів декомпозиції. На першому рівні підсистема давачів представлена у вигляді блоку 1. На другому рівні, що знаходиться всередині блоку 1, схема побудована за архітектурою 2oo3 представлена у вигляді трьох пар елементів, інтенсивність відмов яких λ_{DU} та λ_{DD} відповідно. Канали 1, 2, 3 представлені парами елементів 12 та 13, 14 та 15, 16 та 17. Блоками 11 та 18 враховуються відмови за загальними причинами (ВЗП). Елементний склад каналів уточняється на рівні третьому. Представлення обчислювальної моделі із використанням технології багаторівневої декомпозиції дає можливість зобразити структуру підсистеми з метою проведення подальшого аналізу та визначення показників функції безпеки системи [1].

Після побудови уточненої схеми функціональної цілісності підсистеми давачів згідно [1] послідовність розрахунку показника PFD_S містить наступні кроки:

- визначити всі елементи, які входять у підсистему давачів;
- провести представлення елементів групи 2oo3 підсистеми давачів;
- визначити показники PFD за формулами (2), (3);
- визначити PFD_S для підсистеми давачів додавши PFD всіх елементів підсистеми.

$$PFD_{1oo1} = \lambda_{DU}\left(\frac{T_1}{2} + MTTR\right) + \lambda_{DD} MRT \tag{2}$$

$$PFD_{2oo3} = 6((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MRT\right) \tag{3}$$

де T_1 - інтервал часу між контрольними перевірками, год.; $MTTR$ - середній час відновлення, год.; MRT - середній час ремонту, год.; β - частка невиявлених відмов за загальними причинами, %; β_D - частка виявлених відмов діагностичними тестами та мають загальну причину, $\beta = 2\beta_D$, %; λ_{DU}, λ_{DD} - інтенсивності небезпечних невиявлених та виявлених відмов відповідно, відмова/год., t_{CE}, t_{GE} – еквівалентний середній час простою каналу та голосуючої групи відповідно, год.

Значення β-фактору пов’язують ймовірність ВЗП та ймовірність випадкової відмови [6]. Такі відмови можуть бути навіть якщо у системі реалізовано резервування. В цьому випадку відбувається одночасна відмова каналів багатоканальної системи, що призводить до відмови функції безпеки.

Розрахунок середньої ймовірності відмови на запит всієї підсистеми давачів визначається за формулою (3), а для кожного з трьох каналів - за формулою (2), оскільки елементи кожного каналу з’єднані за архітектурою 1oo1, а канали поєднуються у підсистему давачів за архітектурою 2oo3. Для розрахунків середній час відновлення $MTTR$ та ремонту MRT обираються рівними 8 годин; діагностичне покриття DC – 60%, 90%, 99%; β та β_D – 2% та 1%, 10% та 5%, 20% та 10% відповідно.

Проведемо орієнтовну проектну оцінку функції безпеки. Як було вже зазначено, на відміну від розрахунків надійності, при визначені показників функції безпеки враховують лише небезпечні відмови. При цьому вважається, що на етапі проектування дані про точну номенклатуру відсутні, тому оберемо статистичні значення надійності елементів підсистеми давачів. Інтенсивність відмов елементів визначається за формулою (4):

$$\lambda = \frac{1}{MTTF}. \tag{4}$$

А інтенсивність небезпечних відмов (у припущенні 50% невизначених небезпечних відмов та 50% визначених небезпечних відмов) (5):

$$\lambda_D = \lambda_{DU} + \lambda_{DD} = \frac{\lambda}{2}. \tag{5}$$

За формулами (6) визначають значення показників невизначених та визначених небезпечних відмов

$$\lambda_{DU} = \lambda_D(1-DC), \qquad \lambda_{DD} = \lambda_D DC. \tag{6}$$

Аналогічним чином обчислювальна модель уточняється для логічної підсистеми та підсистеми виконавчих елементів. На рис. 5 наведено схема функціональної цілісності логічної підсистеми протипожежного контуру автоматизованої вентиляційної системи.

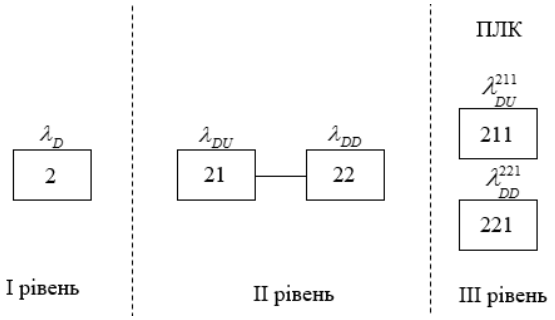


Рис. 5. Схема функціональної цілісності логічної підсистеми

На першому рівні декомпозиції підсистема представлена вершиною 2, на другому рівні декомпозиції структура 1oo1 логічної підсистеми – парою елементів 21 та 22 з інтенсивністю відмов λ_{DU} та λ_{DD}, яка представляє собою програмований логічний контролер. На третьому рівні декомпозиції уточняється елементний склад каналу у вигляді вершини 211, що відповідає невиявленим небезпечним відмовам, та 221 – виявленим небезпечним відмовам логічного елементу системи.

Підсистема виконавчих елементів наведена у складі: інтерфейсний модуль, модуль дискретного виходу, реле, повітряна заслінка. Обчислювальна модель для підсистеми виконавчих елементів зображена на рис. 6

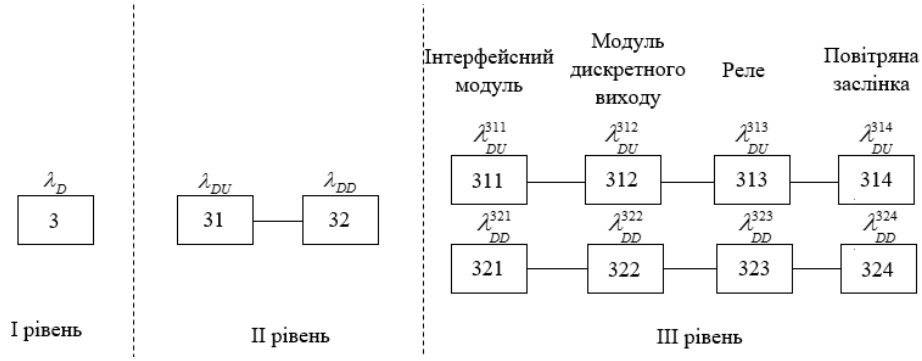


Рис. 6. Схема функціональної цілісності підсистеми виконавчих елементів

Система виконавчих елементів на першому рівні декомпозиції представлена вершиною 3. На другому рівні – представлена парою елементів 31 та 32 з інтенсивністю відмов λ_{DU} та λ_{DD}. На третьому рівні декомпозиції уточняється елементний склад каналу у вигляді вершин 311-314 та 321-324, що відповідають невиявленим та виявленим небезпечним відмовам.

Вихідні та отримані значення показників надійності для елементів кожної підсистеми наведено у табл. 3.

Таблиця 3

Показники надійності підсистем контуру протипожежної безпеки

	MTTF, год $\cdot 10^6$	λ, TIF	λ_D, TIF	λ_{DU}, TIF			λ_{DD}, TIF		
				DC=60%	*DC*=90%	*DC*=99%	*DC*=60%	*DC*=90%	*DC*=99%
Підсистема давачів									
Давачі	1,3	769	385	154	38	4	231	346	381
Бар'єри	2	500	250	100	25	3	150	225	248
Модуль аналогового вводу	0,5	2000	1000	400	100	10	600	900	990
Підсистема логічних елементів									
ПЛК	5,2	192	96	39	9,6	1	58	87	95
Підсистема виконавчих елементів									
Інтерфейсний модуль	1,9	526	263	105	26	2,6	158	237	261
Модуль дискретного виходу	1,5	667	333	133	33	3,3	200	300	330
Реле	0,55	1818	909	364	91	9,1	545	818	900
Повітряна заслінка	0,2	5000	2500	1000	250	25	1500	2245	2475

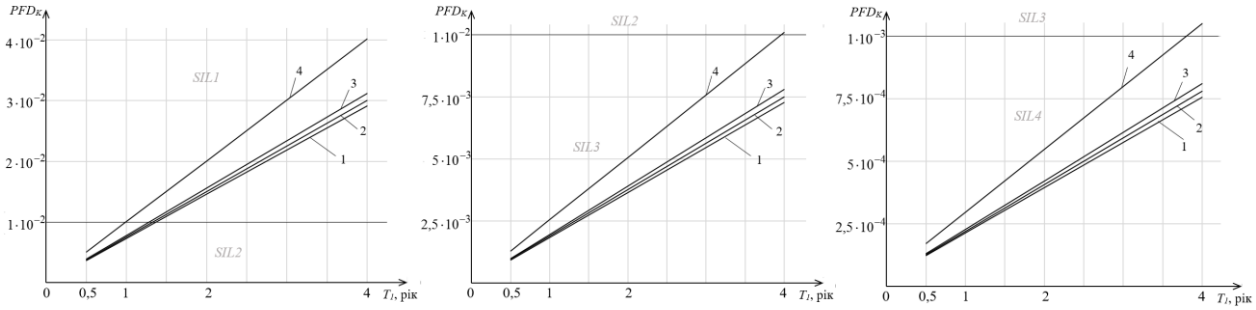
Для кожної підсистеми розраховано значення середньої ймовірності відмов контуру з резервування і без резервування (табл. 4) та наведено графіки залежностей середньої ймовірності відмов PFD_K контуру з резервування при різних значеннях інтервалу між контрольними перевірками для протипожежного контуру вентиляційної системи, при різних значеннях діагностичного покриття контуру та різних значеннях β-фактору для підсистеми давачів відповідно, 4 – графік PFD_K для нерезервованого контуру (рис. 7).

Аналіз отриманих графіків показав, що на значення середньої ймовірності відмови на запит велике значення має відсоток діагностичного покриття. Наприклад, при DC=60% PFD_K відповідає рівню безпеки SIL1 (при значенні інтервалу між контрольними перевірками більше 1 року). Зменшивши інтервал між контрольними перевірками до 0,5-1 рік рівень безпеки підвищується до SIL2 (рис. 7, а). При збільшенні значення діагностичного покриття рівень безпеки може бути підвищений до SIL3 та навіть до SIL4.

Таблиця 4

Результати розрахунку середньої ймовірності відмов контуру з резервування та без резервування

Контур	DC, %	β,%	β_D,%	PFD_K			
				$T_1 = 6$ місяців	$T_1 = 1$ рік	$T_1 = 2$ роки	$T_1 = 4$ роки
протипожежної безпеки вентиляційної системи (із резервуванням елементів підсистеми давачів)	60	2	1	$3{,}66 \cdot 10^{-3}$	$7{,}28 \cdot 10^{-3}$	$1{,}46 \cdot 10^{-2}$	$2{,}91 \cdot 10^{-2}$
		10	5	$3{,}77 \cdot 10^{-3}$	$7{,}51 \cdot 10^{-3}$	$1{,}5 \cdot 10^{-2}$	$3 \cdot 10^{-2}$
		20	10	$3{,}92 \cdot 10^{-3}$	$7{,}80 \cdot 10^{-3}$	$1{,}56 \cdot 10^{-2}$	$3{,}12 \cdot 10^{-2}$
	90	2	1	$9{,}39 \cdot 10^{-4}$	$1{,}84 \cdot 10^{-3}$	$3{,}66 \cdot 10^{-3}$	$7{,}28 \cdot 10^{-3}$
		10	5	$9{,}68 \cdot 10^{-4}$	$1{,}9 \cdot 10^{-3}$	$3{,}77 \cdot 10^{-3}$	$7{,}51 \cdot 10^{-3}$
		20	10	$1 \cdot 10^{-3}$	$1{,}97 \cdot 10^{-3}$	$3{,}92 \cdot 10^{-3}$	$7{,}8 \cdot 10^{-3}$
	99	2	1	$1{,}23 \cdot 10^{-4}$	$2{,}14 \cdot 10^{-4}$	$3{,}95 \cdot 10^{-4}$	$7{,}57 \cdot 10^{-4}$
		10	5	$1{,}27 \cdot 10^{-4}$	$2{,}2 \cdot 10^{-4}$	$4{,}07 \cdot 10^{-4}$	$7{,}81 \cdot 10^{-4}$
		20	10	$1{,}31 \cdot 10^{-4}$	$2{,}28 \cdot 10^{-4}$	$4{,}22 \cdot 10^{-4}$	$8{,}1 \cdot 10^{-4}$
протипожежної безпеки вентиляційної системи (без резервування)	60	-	-	$5{,}07 \cdot 10^{-3}$	$1{,}01 \cdot 10^{-2}$	$2{,}01 \cdot 10^{-2}$	$4{,}02 \cdot 10^{-2}$
	90	-	-	$1{,}30 \cdot 10^{-3}$	$2{,}56 \cdot 10^{-3}$	$5{,}07 \cdot 10^{-3}$	$1{,}01 \cdot 10^{-2}$
	99	-	-	$1{,}72 \cdot 10^{-4}$	$2{,}97 \cdot 10^{-4}$	$5{,}48 \cdot 10^{-4}$	$1{,}05 \cdot 10^{-3}$



а) при DC=60% **б) при DC=90%** **в) при DC=99%**

Рис. 7. Результати розрахунку середньої ймовірності відмови на запит PFDK, де 1, 2, 3 – графіки PFDK для резервованого контуру при ($\beta = 2\%$ і $\beta_D = 1\%$), ($\beta = 10\%$ і $\beta_D = 5\%$) та ($\beta = 20\%$ і $\beta_D = 10\%$) для підсистеми давачів відповідно, 4 – графік PFDK для нерезервованого контуру

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

На основі методу розрахунку середньої ймовірності небезпечної відмови та використання методів структурно-логічного моделювання, багаторівневої структурної декомпозиції проведено проектну оцінку відповідності запропонованого протипожежного контуру автоматизованої системи певному рівню повноти безпеки. Визначено, які фактори найбільше впливають на функціональну безпеку контуру та шляхи її підвищення. Встановлено, що найбільший вплив на рівень повноти безпеки контуру впливають діагностичне покриття та інтервал між контрольними перевірками (для запропонованих параметрів елементної бази контуру автоматизованої системи). Збільшуючи діагностичне покриття, зменшуючи інтервал між контрольними перевірками, обираючи елементну базу з кращими показниками надійності досягають необхідного рівня повноти безпеки автоматизованої системи.

Література

1. IEC 61508. Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems. Geneva: The International Electrotechnical Commission, 2010.

2. IEC 61511. Functional Safety – Safety Instrumented Systems for the Process Industry Sector. Geneva: The International Electrotechnical Commission, 2003.

3. ДСТУ 2860-94. Надійність техніки. Терміни та визначення. [Чинний від 1996-01-01].

4. Розрахунки систем контролю та керування : навчальний посібник / Г.І. Манко та ін. Дніпро : УДХТУ, 2018. 191 с.

5. Guedelines for Safe Automation of Chemical Process. New York: CCPS, AIChE, 2013. P.633.

6. Боженко М. Ф. Системи опалення, вентиляції і кондиціювання повітря будівель [Електронний ресурс] : навчальний посібник. КПІ ім. Ігоря Сікорського, 2019. 380 с.

7. Rausand M. Reliability of safety-critical systems : theory and application. Wiley, 2013. P. 468.

ISSN 2219-9365

References

1. IEC 61508. Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems. Geneva: The International Electrotechnical Commission, 2010.

2. IEC 61511. Functional Safety – Safety Instrumented Systems for the Process Industry Sector. Geneva: The International Electrotechnical Commission, 2003.

3. DSTU 2860-94. Nadiinist tekhniky. Terminy ta vyznachennia. [Chynnyi vid 1996-01-01].

4. Rozrakhunky system kontroliu ta keruvannia : navchalnyi posibnyk / H.I. Manko ta in. Dnipro : UDKhTU, 2018. 191 s.

5. Guedelines for Safe Automation of Chemical Process. New York: CCPS, AIChE, 2013. P.633.

6. Bozhenko M. F. Systemy opalennia, ventyliatsii i kondytsiiuvannia povitria budivel [Elektronnyi resurs] : navchalnyi posibnyk. KPI im. Ihoria Sikorskoho, 2019. 380 s.

7. Rausand M. Reliability of safety-critical systems : theory and application. Wiley, 2013. P. 468.