МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«УКРАЇНСЬКИЙ ДЕРЖАВНИЙ ХІМІКО-ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ»

МЕТОДИЧНІ ВКАЗІВКИ

з дипломного проектування систем автоматизації вибухонебезпечних виробництв

Дніпропетровськ ДВНЗ УДХТУ 2015

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«УКРАЇНСЬКИЙ ДЕРЖАВНИЙ ХІМІКО –ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ»

МЕТОДИЧНІ ВКАЗІВКИ

з дипломного проектування систем автоматизації вибухонебезпечних виробництв

Затверджено на засіданні кафедри комп’ютерно-інтегрованих технологій і метрології
Протокол № 1 від 31.09.2014 р.

Дніпропетровськ ДВНЗ УДХТУ 2015

Методичні вказівки з дипломного проектування систем автоматизації вибухонебезпечних виробництв / Укл. : Г.І. Манко, К.О. Довгопола. – Дніпропетровськ : ДВНЗ УДХТУ. – 2015. – 60 с.

Укладачі: Г.І. Манко, канд. техн. наук
К.О. Довгопола

Відповідальний за випуск О.П. Мисов, канд. техн. наук

Навчальне видання

Методичні вказівки

з дипломного проектування систем автоматизації вибухонебезпечних виробництв

Укладачі: МАНКО Геннадій Іванович,
ДОВГОПОЛА Ксенія Олексіївна

Редактор Л.М. Тонкошкур
Коректор Л.Я. Гоцуцова

Підписано до друку _____. Формат 60×84 1/16. Папір ксероксн. Друк різограф. Умовн.-друк. арк. _____. Облік.-вид. арк. _____. Тираж ____ прим. Зам. № ____. Свідоцтво ДК № 303 від 27.12.2000.

ДВНЗ УДХТУ, 49005, Дніпропетровськ–5, пр. Гагаріна, 8.

Видавничо-поліграфічний комплекс ІнКомЦентру

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

1oo1 – система без резервування

1oo2 – резервування «один з двох»

1oo2D – резервування «один з двох» з діагностикою

2oo2 – резервування «два з двох»

2oo3 – резервування «два з трьох»

AI (Analog Input) – аналоговий вхід

AO (Analog Output) – аналоговий вихід

DCS (Distributed Control System) – розподілена система управління

MTBF (Mean Time Between Failures) – середній час між двома послідовними відмовами

MTBFd – середній час між двома небезпечними відмовами

MTBFs – середній час між двома хибними остановами

MTTF (Mean Time To Failure) – середній час напрацювання на відмову

MTTR (Mean Time To Repair) – середній час відновлення (ремонту)

PFDavg (Probability of Failure on Demand) – середня ймовірність невиконання функції безпеки

RRF (Risk Reduction Factor) – фактор зниження риску

SCS (Safety Control Station) – контролер системи безпеки

SENG (Safety Engineering Station) – інженерна станція системи безпеки

SFF (Safety Failure Fraction) – доля безпечних відмов

SIF (Safety Instrumented Function) – інструментальна функція безпеки

SIL (Safety Integrity Level) – рівень безпеки

SIS (Safety Instrumented System) – інструментальна система безпеки

АС – автоматизована система

БД РЧ – база даних реального часу

БІС – блок іскрозахисту на стабілітронах

ВГВ – верхня границя вибуху

МЕП – мінімальна енергія підпалювання

НГВ – нижня границя вибуху

НФС – надійнісно-функціональна схема

ОДУ – оперативно-диспетчерське управління

ПАЗ – система протиаварійного захисту

РСУ – розподілена система управління

ТП – технологічний процес

ВСТУП

Нині діючі міжнародні і вітчизняні стандарти вимагають від проектантів основну увагу приділяти безпеці виробництва. За деякими оцінками щорічний збиток, що наноситься світовій економіці техногенними катастрофами і аваріями, за останні 30 років збільшився в 3 рази і досяг 200 мільярда доларів, і це без урахування екологічного збитку. На сьогоднішній день збиток від аварій і катастроф у світі складає 5 до 10 т величини валового національного продукту.

Значна частина хімічних виробництв є вибухонебезпечними. Пожежі, вибухи, викиди токсичних продуктів, інші інциденти і аварійні ситуації на виробництві ведуть до загибелі і травматизму персоналу підприємств і населення, чинять несприятливу дію на довкілля.

Сучасний підхід до промислової безпеки полягає у формуванні автоматизованих систем управління і захисту як головного елементу єдиної системи безпеки. Системи управління і захисту технологічних процесів стають усе більш потужними, але, в той же час, і усе більш уразливими Особливість електронних систем полягає в тому. що системи, призначені для управління і захисту технологічних процесів, самі по собі являють значну небезпеку. При цьому причини відмов різного роду істотним чином перетинаються, і викликають кумулятивний ефект. Це вимагає нових підходів до проектування систем автоматизації вибухонебезпечних виробництв. Погане проектування, невідповідність проектних рішень умовам виробництва і забезпечення його безпеки, а також конструктивна недосконалість технічних пристроїв і устаткування, ведуть до неприпустимо низького рівня промислової безпеки в хімічній галузі.

Метою цих методичних вказівок є дати студентам інформацію, необхідну для створення систем управління, які забезпечують прийнятний ризик експлуатації вибухонебезпечного виробництва. Тут викладаються принципи і методи проектування, спрямовані на попередження аварій і забезпечення швидкої локалізації і ліквідації наслідків вказаних аварій.

Методичні вказівки призначені для студентів напрямів підготовки 6.050202 та 6.051001 і є доповненням до відповідних методичних вказівок [12–14]. Вони можуть також використовуватись студентами технологічних напрямів при підготовці розділу дипломного проекту «Автоматизація виробництва».

Дія Методичних вказівок поширюється на всі форми навчання.

1 Загальні положення

1.1 Сучасна концепція управління

Сучасна концепція побудови систем управління передбачає наявність у складі АСКТП двох головних підсистем: розподіленої системи управління (РСУ), або, англійською, DCS (Distributed Control System), а також підсистеми протиаварійного захисту (ПАЗ), англійською SIS (Safety Instrumented System).

Спрацювання виконавчого механізму від помилкової команди контрольно-вимірювального приладу або в умовах дії «людського чинника» в одному з кіл складного технологічного процесу може спричинити, в кращому випадку, вихід з ладу дорогого устаткування, в гіршому – аварію зі шкодою для персоналу та навколишнього середовища. Щоб уникнути подібних інцидентів та аварій, в систему автоматизації виробництва інтегрується ПАЗ, що дозволяє мінімізувати можливість виникнення аварійних ситуацій, своєчасно проінформувати обслуговуючий персонал про виниклі проблеми, в автоматичному режимі відпрацювати позаштатну ситуацію. Система протиаварійного захисту паралельно з основною системою автоматизованого управління стежить за станами аварійних сигнальних датчиків, при спрацьовуванні яких ПАЗ розриває управління відсічними клапанами, засувками і двигунами від РСУ, в результаті чого вони закриваються або зупиняються.

Сьогодні наявність ПАЗ є обов'язковою вимогою для вибухонебезпечних виробничих об'єктів.

Структуру ПАЗ можна розділити на три основні частини:

- пристрої діагностики факторів, що сприяють розвитку аварії (контрольно-вимірювальні прилади, аналізатори);
- пристрої обробки отриманих даних (контролери та інші засоби обробки даних);
- виконавчі механізми (електро- та пневмоприводи запірної арматури, електровимикачі тощо).

Розділення функцій між РСУ і ПАЗ суттєво зменшує ймовірність того, що функції керування і функції захисту стануть недосяжними одночасно, і що неуважні або некваліфіковані дії персоналу впливатимуть на виконання функцій захисту.

Все обладнання ПАЗ повинно бути обов’язково сертифіковане на застосування в системах безпеки.

1.2 Інтегральні рівні безпеки

Вимоги щодо вибору обладнання засобів автоматизації, що використовуються в системах, пов'язаних із забезпеченням безпеки виробничих процесів, обумовлюються в європейських стандартах МЕК 61508 і 61511. У цих документах безпека визначається як «свобода від неприйнятних ризиків». При цьому під ризиком розуміється комбінація ймовірності виникнення збитків та тяжкості цієї шкоди. Небезпека - це потенційне джерело шкоди. Допустимим вважається ризик, прийнятний в даних обставинах, з урахуванням існуючих у цей час соціальних цінностей.

Всі дії по забезпеченню безпеки повинні ґрунтуватися на розумінні й оцінці ризику, який неминуче присутній у будь-якій системі. Стандарт МЕК 61508 поділяє заходи щодо зниження ризику на два компоненти:

а) загальні, інтегральні вимоги безпеки (Safety integrity requirements);

б) функціональні вимоги (Functional requirements).

Відповідно, специфікація вимог безпеки повинна визначати:

а) специфікацію вимог інтегральної безпеки, яка містить загальні вимоги безпеки, які повинна забезпечувати система;

б) специфікацію вимог функціональної безпеки, що містить вимоги до функцій (контурів) безпеки, які повинна виконувати система.

Згідно МЕК 61508, функціональна безпека відноситься до систем, що відповідають за функції безпеки, вихід з ладу яких створює значні ризики для людей і навколишнього середовища. Щоб домогтися функціональної безпеки, система в разі аварії повинна привести обладнання в безпечний стан або забезпечити збереження такого стану. Мова йде не про загальні небезпеки експлуатації обладнання, таких, як, наприклад, від обертових деталей, а про небезпеки, що виникають внаслідок збоїв запобіжних функцій.

Пристрої захисту, використовувані для запобігання нанесення шкоди людям, середовищу і майну, повинні відповідати певним вимогам до надійності залежно від можливого обсягу збитку, який визначається на основі так званого класу безпеки експлуатації обладнання (Safety Integrity Level - SIL).

Рівень безпеки SIL - це цифрове позначення, що привласнюється системі безпеки, яке відображає здатність системи забезпечувати функції безпеки. Стандартом IEC 61508 визначено чотири рівня безпеки. Чим вище рівень SIL, тим вище ймовірність виконання системою завдання забезпечення безпеки.

Якісно SIL може бути розглянутий як імовірний збиток, нанесений персоналу, підприємству і суспільству в разі помилки системи безпеки:

SIL 1 - потрібний незначний захист устаткування та продукції;

SIL 2 - потрібний значний захист устаткування та продукції, захист від можливих травм обслуговуючого персоналу;

SIL 3 - потрібний захист обслуговуючого персоналу та суспільства (некатастрофічний вплив);

SIL 4 - потрібний захист від катастрофічного впливу на суспільство.

Таблиця 1.1 – Рівень безпеки SIL

Рівень SIL	Необхідна надійність	Імовірність помилки при виконанні заданої задачі (PFD)	Фактор зниження ризику (RRF)
SIL 4	Більше 99,99%	Більше, або дорівнює 10^{-5}… менше 10^{-4}	100 000 … 10 000
SIL 3	99,90%	Більше, або дорівнює 10^{-4}… менше 10^{-3}	10 000 … 1 000
SIL 2	Від 99,00 до 99,90%	Більше, або дорівнює 10^{-3}… менше 10^{-2}	1 000 … 100
SIL 1	Від 90,00 до 99,00%	Більше, або дорівнює 10^{-2}… менше 10^{-1}	100 … 10

Вибір необхідного рівня SIL для конкретного виробництва - це корпоративне рішення, що грунтується на філософії управління виробництвом і рівні ризику.

Зазначений у четвертій графі табл. 1.1 фактор зниження ризику RRF (Risk Reduction Factor) являє собою відношення частоти інцидентів без прийняття заходів захисту до допустимої частоти інцидентів і є величиною, зворотною PFDavg:

$$RRF = \frac{\text{частота інцидентів без прийняття заходів захисту}}{\text{Допустима частота інцидентів}} = \frac{1}{PFDavg} \quad (1.1)$$

Для оцінки безпеки виконують такі дії.

Ідентифікація небезпечних процесів. Як правило, кількість таких процесів невелика. Наприклад, основні операції режимів регулювання, що не включають в себе функції безпеки, не розглядаються.

Визначення вимог SIL. Для кожного потенційно небезпечного процесу проводиться оцінка ступеня небезпеки та рівня збитку, що виник унаслідок збою. Для цього може застосовуватися графік ризиків (див. рис. 1.1). Залежно від ступеня небезпеки та ймовірності її виникнення робиться висновок, чи

потребує процес в захисті за допомогою функції безпеки, і який рівень SIL така функція повинна забезпечувати.

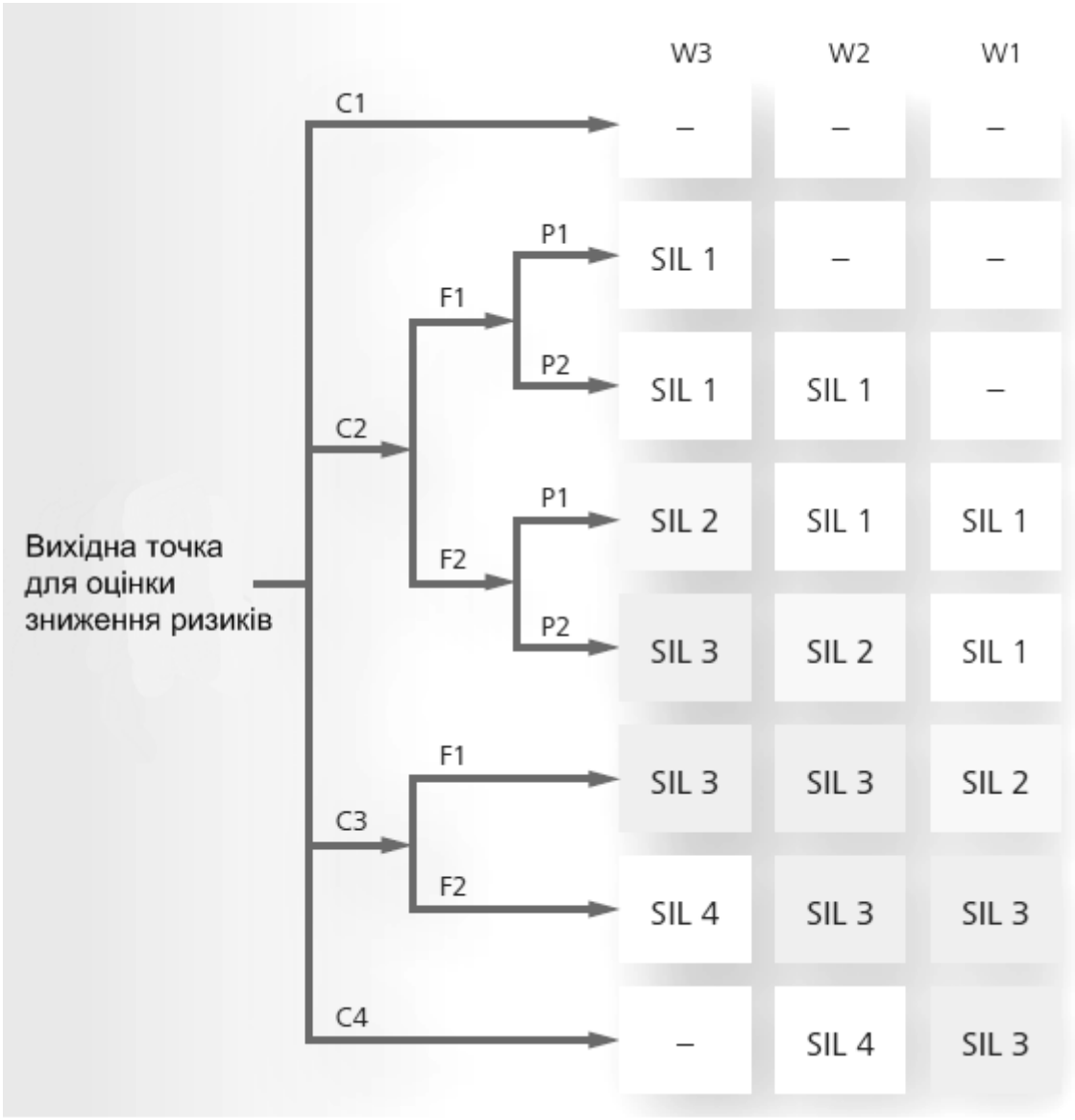

Рис. 1.1 – Графік ризиків для оцінки безпеки відповідно до МЕК 61508/61511

На рис. 1.1 використані наступні позначення.

Розмір збитку:

C1 - травма малому ступені тяжкості однієї людини або малий збиток навколишньому середовищу;

C2 - важкі незворотні травми або смерть однієї людини;

C3 - смерть кількох людей;

C4 - смерть великої кількості людей.

Запобігання небезпеки:

F1 - можливо за певних умов;

F2 - майже неможливо.

Термін перебування людини в небезпечній зоні:

P1 - від «рідко» до «часто».

P2 - від «часто» до «тривало».

Імовірність виникнення:

W1 - дуже мала;

W2 - мала;

W3 - відносно висока.

Підбір необхідних елементів. Для впровадження функції безпеки з необхідним рівнем SIL проводиться підбір необхідних елементів. Щоб спростити цей етап, виробники сьогодні вказують відповідність своєї продукції різним рівням SIL.

Перевірка вимог SIL. Шляхом аналізу показників безпеки застосовуваних пристроїв перевіряється, чи забезпечує функція безпеки необхідний рівень SIL. Якщо ні, то в цьому випадку необхідно вживати додаткових заходів.

Особливе місце серед небезпечних виробництв займають такі, в яких існує безпосередня можливість виникнення пожежі або вибуху. Для таких виробництв розроблені рекомендації МЕК 79-10, що ґрунтуються на тому, що будь-яке місце, де існує ймовірність наявності вибухонебезпечного середовища, має бути віднесено до однієї з наступних трьох зон:

Zone 0 - зона, в якій вибухонебезпечна суміш повітря і газу присутня постійно або протягом тривалого проміжку часу;

Zone 1 - зона, в якій існує ймовірність появи вибухонебезпечної суміші повітря і газу при нормальній роботі;

Zone 2 - зона, в якій утворення вибухонебезпечної суміші повітря і газу малоймовірне, але якщо це відбувається, то тільки на короткий проміжок часу.

Будь-які місця, які не підпадають під жодне з наведених визначень, вважаються безпечною зоною.

Для кожної горючої речовини існує мінімальна енергія підпалювання (МЕП), яка відповідає ідеальній пропорції палива і повітря, в якій суміш найлегше запалюється. Нижче МЕП підпалювання неможливо при будь-якій концентрації.

Для концентрації нижче, ніж величина, відповідна МЕП, кількість енергії, що вимагається для запалення суміші, збільшується до тих пір, поки значення концентрації не стане менше значення, при якому суміш не може спалахнути через малу кількість палива. Ця величина називається нижньою межею вибуху (НМВ). Аналогічним чином при збільшенні концентрації кількість необхідної для займання енергії зростає, поки концентрація не перевищить значення, при якому займання не може статися через недостатню кількість окислювача. Це значення називається верхньою межею вибуху (ВМВ).

Зазвичай для Zone 0 рівень ймовірності наявності небезпечної суміші приймається рівним більш ніж 1%. Місця, що класифікуються як Zone 1, мають рівень ймовірності наявності небезпечної суміші між 0,01% і 1% (максимум 100 годин на рік), в той час як для місць, що класифікуються як Zone 2, небезпечна суміш присутня протягом не більше 1 години в рік.

1.3 Заходи для підвищення безпеки

1.3.1 Функції безпеки

Функції безпеки - це захисні заходи, які вживаються тільки в разі аварії з метою запобігання нанесення шкоди людям, навколишньому середовищу і матеріальним цінностям. Функціональна безпека забезпечується тоді, коли функції безпеки в аварійних ситуаціях працюють надійно.

До типових функцій безпеки відносяться, наприклад, аварійний останов, контроль тиску котла та ін.

При управлінні трубопровідною арматурою особлива увага приділяється наступним функціям безпеки:

а) аварійне відкриття;

б) аварійне закриття;

в) аварійний стан покою/останова;

г) контрольний сигнал кінцевого положення.

Наприклад, щоб запобігти перевищенню тиску в котлі, як функцію безпеки передбачають відкриття редукційного клапана. Датчик безперервно контролює тиск у котлі. У разі неприпустимого тиску контролер системи безпеки віддає сигнал помилки, а також відправляє на привід клапану команду ВІДКРИТИ для того, щоб скорегувати тиск в котлі.

Функція безпеки реалізується за допомогою елементів так званої інструментальної системи безпеки (англ. Safety Instrumented System, SIS). Така система стандартно складається з датчика, блоку управління верхнього рівня і виконавчого вузла. При управлінні арматурою виконавчий вузол включає в себе привід і запірну арматуру.

Оцінюючи відповідність функції безпеки необхідному рівню SIL, необхідно враховувати показники всіх елементів інструментальної системи безпеки.

1.3.2 Специфіка АСКТП

Системи протиаварійного захисту володіють рядом специфічних властивостей, властивих тільки цим системам:

а) система захисту може формально перебувати в роботі, але в момент настання небезпечної події на процесі не здатна відреагувати на нього, подібний тип відмови прийнято називати небезпечною відмовою;

б) система захисту може зробити помилковий невмотивований аварійний останов процесу, в той час як насправді нічого небезпечного на процесі не сталося. Подібний тип відмови називають "безпечною" відмовою.

Останов і запуск виробництва - це серйозні і відповідальні операції, не кажучи про економічні втрати. Процедура зупину, призначена для хисту процесу, сама по собі становить значну небезпеку, бо вимагає узгоджено зміни стану багатьох елементів технологічного обладнання, і залежить від бездоганного виконання цілком певних послідовностей операцій – як автоматичних, так і узгоджених дій технологічного персоналу. Будь-який останов – надзвичайна подія на виробництві, пов'язана з серйозним ризиком і для людей, і для обладнання. Тим більше, помилковий останов, що спричиняється системою, призначеною для запобігання аварійних ситуацій, – подія, в причинах якої необхідно розібратися.

Аналіз застосовуваних схем захисту показує, що підвищена ймовірність небезпечних відмов і помилкових спрацьовувань може бути закладена в систему спочатку на етапі проектування внаслідок неправильного вибору архітектури системи управління.

1.3.3 Архітектури систем

Архітектури систем, пов'язаних із забезпеченням безпеки, і використовувані в них компоненти вельми різноманітні. У багатьох випадках для підвищення надійності та відмовостійкості використовують системні архітектури з резервуванням, приклади яких показані на рис. 1.2.

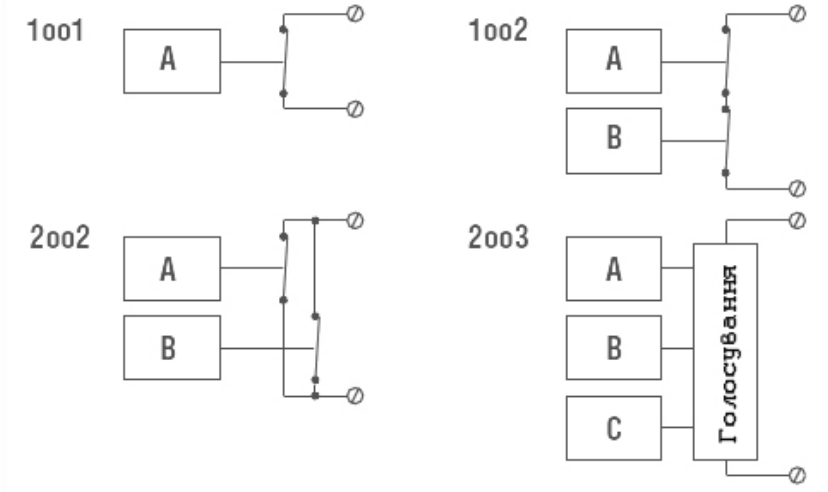

Рис. 1.2 – Приклади архітектури систем

Архітектура 1oo1 (один з одного). Для системи без резервування з архітектурою 1oo1 безпечною відмовою є розмикання релейного контакту і відключення системи, що викликає помилковий останов. Прийнята безпечна інтенсивність відмов в даному випадку дорівнює 0,04 / рік; це означає, що в заданий період часу (1 рік) існує ймовірність помилкового відключення системи, рівна 4%. Іншими словами, середній час між помилковими остановами (MTBFS) для даної системи дорівнює 25 рокам.

Прикладом небезпечної відмови може бути випадок, коли контакти реле приварюються і не можуть розімкнутися в потрібний момент. Прийнята інтенсивність такої відмови дорівнює 0,02 / рік; це означає, що ймовірність відмови системи на виконання запиту в заданий період часу (1 рік) дорівнює 2% або середній час між відмовами MTBFD (для небезпечних відмов) 50 (1/0,02) років.

Архітектура 1oo2 (один з двох). Система з дубльованої архітектурою 1oo2 має вихідні контакти, з'єднані послідовно і замкнуті при включеному живленні. Системі достатньо одного каналу, щоб забезпечити аварійне відключення. Якщо будь-який з каналів може зупинити систему, а каналів в системі в два рази більше, ніж в системі 1oo1, то і помилкових відключень може бути в два рази більше. Тому й інтенсивність таких подій збільшується з 0,04 до 0,08 / рік. Це означає, що 8 систем з 100 дадуть помилкове виключення протягом року або що MTBFS становить 12,5 років.

Небезпечна відмова для такої системи настає, коли в обох каналах одночасно сталися небезпечні відмови, оскільки, якщо тільки один вихідний контакт «залипнув», другий ще може відключити систему. Інтенсивність одночасних відмов становить 0,02 × 0,02 = 0,0004 /рік. Це означає, що MTBFD дорівнює 2500 рокам.

Системи з архітектурою 1oo2 відрізняються високою безпекою (ймовірність небезпечної відмови системи вкрай мала), проте вони мають в два рази більшу ймовірність помилкових спрацьовувань, що небажано з точки зору втрат продукції, пов'язаних з простоєм.

Архітектура 2oo2 (два з двох). Система з дубльованої архітектурою 2oo2 має вихідні контакти, з'єднані паралельно. В даному випадку обидва канали мають бути знеструмлені, щоб зупинити процес.

Відмова в роботі такої системи настає, якщо відбувається небезпечна відмова в одному з каналів. Оскільки система має в два рази більше компонентів (каналів), ніж система 1oo1, кількість небезпечних відмов у ній може бути в два рази більшою. Тому прийнята інтенсивність небезпечних відмов тут збільшується в два рази до 0,04 / рік, а MTBFD = 25 рокам.

Помилкове спрацьовування в даній системі відбувається, коли в обох каналах одночасно трапляється безпечна відмова. Інтенсивність таких одночасних відмов складає 0,04 х 0,04 = 0,0016 / рік. МТВР5 = 1 / 0,0016 = 625 років.

Таким чином, система з архітектурою 2оо2 захищає від помилкових спрацьовувань (ймовірність безпечнї відмови дуже мала), проте за частиною небезпечних відмов вона менш безпечна, ніж навіть нерезервованої система з архітектурою 1оо1.

Архітектура 2оо3 (два з трьох). Рішення в ній приймається на основі результатів голосування два з трьох. Система 2оо3 має більш високу інтенсивність помилкових спрацьовувань, ніж система 2оо2, і більшу ймовірність відмов, ніж система 1оо2. Однак архітектури 1оо2 і 2оо2 незадовільні з точки зору небезпечних відмов і помилкових спрацьовувань, в той час як системи з архітектурою 2оо3 мають хороші показники по відмовах обох видів (безпечних і небезпечних).

Завдяки вдосконаленню апаратної частини і програмного забезпечення тепер відмови в комп'ютерній системі з подвійним резервуванням можуть діагностуватися досить добре, що дозволяє визначити, який з двох каналів справний у випадку, якщо між ними виникає суперечність. У промисловості цю нову подвійну архітектуру систем називають 1оо2D.

1.3.4 Резервування та надмірність

Надійність ПАЗ повинна забезпечуватися:

а) апаратурним резервуванням;

б) часовою, алгоритмічною, інформаційною та функціональною надмірністю;

в) наявністю систем діагностики та самодіагностики.

Резервування вузлів системи підвищує ймовірність того, що у разі відмови функція безпеки спрацює правильно. Дублювати один одного можуть два або кілька компонентів системи безпеки.

Необхідно передбачати резервування ВСІХ елементів системи, що мають відношення до безпеки:

а) польове устаткування;

б) польові шини;

в) модулі введення-виведення;

г) модулі управління;

д) джерела живлення;

е) грамотний и відповідальний персонал.

В залежності від вимог безпеки застосовуються різні конфігурації MooN («М з N»). Наприклад, у конфігурації 1оо2 («один з двух») достатньо одного

пристрою, щоб забезпечити виконання функції безпеки. У конфігурації 2oo3 («два з трьох») повинні працювати два пристрої з трьох. Конкретне виконання залежить від необхідної функції безпеки. Як приклад див. на рис. 1.3 системи дублювання надійного відкриття і закриття.

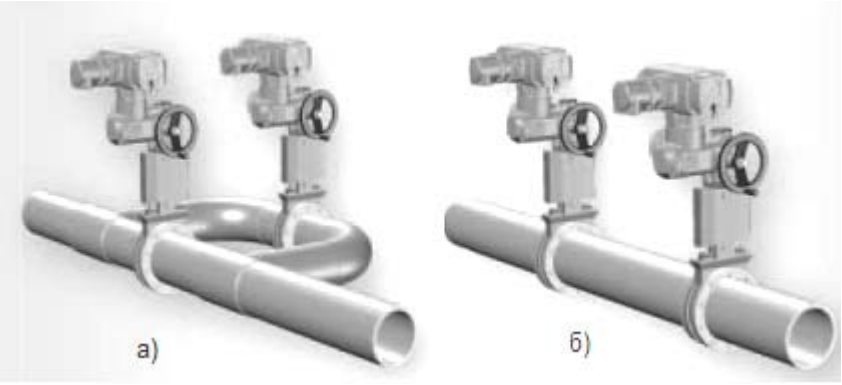

Рис. 1.3 – Системи дублювання надійного відкриття (а) та закриття (б)

Застосування дублювання може підвищити відмовостійкість обладнання та клас SIL.

Для класу SIL 3, відповідно до стандарту МЕК 61511, застосування дублювання (резервування) обов'язкове.

При альтернативному резервуванні у кожному каналі використовується інша технологія, конструкція, інше системне програмне забезпечення, прикладне програмне забезпечення, щоб зменшити ймовірність відмов загального порядку. Для альтернативного резервування використовуються такі прийоми:

а) використання різних типів вимірювань (наприклад, тиск і температура), коли відомо співвідношення між ними;

б) використання інших технологій вимірювання тієї ж самої змінної (наприклад, діафрагма і вихровий витратомір);

в) використання різних типів контролерів для кожного каналу резервування;

г) використання географічного поділу (наприклад, альтернативні маршрути для ліній зв'язку).

При проектуванні вибухонебезпечних виробництв використовують наступні методи резервування.

Резервування на рівні завдань. Багато сучасних SCADA-програм дозволяють організувати резервування системи на рівні завдань, таких як введення-виведення сигналів з підтримкою баз даних реального часу (БД РЧ), обслуговування тривоги (алармів), архівування даних, організація звітів, обробки графічної інформації та ін.

Резервування мережі. Резервування серверів та робочих станцій істотно підвищує надійність системи. Однак, якщо виходить з ладу мережа,

порушується й керування на всіх клієнтських комп'ютерах. Використання додаткової резервної мережі забезпечує стабільність роботи системи у випадку виходу з ладу основної мережі.

Резервування зв'язку з контролером. У більшості контролерів можна організувати додатковий зв'язок між сервером та пристроєм введення-виведення. Наявність додаткового каналу зв'язку гарантує збереження обміну даними при виході з ладу основного каналу. Якщо обмін даними порушується (наприклад, відбувся обрив кабелю), система повинна виконати перемикання на резервний канал. Після відновлення фізичного з'єднання звичайно відбувається зворотній перехід на основний канал.

Резервування контролерів звичайно здійснюється двома шляхами:

а) апаратне резервування складових частин контролера: при цьому резервуватися можуть як окремі вузли контролера, так і весь контролер у цілому; основні і резервні вузли контролера, як правило, розташовані в одному корпусі і зв'язок між ними здійснюється по внутрішньоконтролерній шині.

б) резервування з використанням мережі контролерів: при цьому способі резервуються контролери в цілому, і їхня взаємодія здійснюється за допомогою мережевого зв'язку.

АСУТП повинна будуватися з достатнім ступенем *надмірності*. Кожна її підсистема повинна мати 10–20% резерв як по інформаційних каналах, так і по тих, що управляють.

Разом з тим, необхідно розуміти, що вимога надмірності відноситься не тільки до устаткування, але і до всіх програмних компонентів системи. Необхідно передбачити достатні резерви по оперативній і дисковій пам'яті, а також по швидкодії мікропроцесорних обчислювачів і промислових мереж. які буде потрібно для розвитку функції системи. Запас і інформаційної, і функціональної надмірності повинен бути ніяк не менше 20%, а краще 40%, включаючи, перш за все, швидкодію.

1.3.5 Системи протиаварійного захисту

Системи протиаварійного захисту призначені для попередження і запобігання аварійних ситуацій, які можуть виникнути в ході технологічних процесів як в результаті впливу людського фактора, так і через збої в роботі устаткування.

Система протиаварійного захисту будується на спеціально сертифікованих для таких цілей моделях програмованих контролерів. Контролери повинні мати дубльовану архітектуру.

У разі виникнення небезпеки розвитку аварійної ситуації контролери ПАЗ реалізують алгоритми щодо запобігання аварійних ситуацій відповідно до

Технологічного регламенту виробництва та/або «Правилами локалізації аварійних ситуацій», прийнятими на підприємстві.

Вибір системи ПАЗ її елементів здійснюється виходячи з умов забезпечення її роботи при виконанні вимог по експлуатації, обслуговування та ремонту протягом усього міжремонтного пробігу об’єкта, що захищається.

Порушення роботи системи управління не повинно впливати на роботу системи ПАЗ.

Система ПАЗ повинна забезпечувати:

а) автоматизований збір аналогової та дискретної інформації від датчиків технологічних параметрів і параметрів стану виконавчих механізмів, а також дискретних датчиків ДВК (довибухової концентрації), ГДК (гранично-допустимої концентрації), стану аварійної вентиляції;

б) виділення достовірної вхідної інформації;

в) аналіз і логічну обробку вхідної інформації;

г) автоматичну видачу сигналів двохпозиційного управління на виконавчі механізми;

д) дистанційне ("ручне") управління виконавчими механізмами за умови санкціонованого доступу;

е) визначення першопричини спрацьовування системи захисту і зупинки технологічного процесу;

ж) передачу оперативної інформації від системи ПАЗ в РСУ для сигналізації, реєстрації та архівування (відхилення параметрів, спрацьовування виконавчих механізмів ПАЗ, реакції на дії персоналу тощо);

з) оперативну й автономну діагностику технічних засобів системи ПАЗ та ідентифікацію несправностей з точністю до модуля (блоку).

1.3.6 Розділення та розподілення функцій АСКТП

Поділ функцій між РСК і ПАЗ здатний істотно зменшити ймовірність того, що обидві функції АСКТП - і керуючі, і функції захисту стануть недоступними одночасно, і що неуважні або некваліфіковані дії персоналу вплинуть на виконання функцій захисту. Функціональний поділ РСК і ПАЗ дає додаткову перевагу за рахунок зменшення ймовірності систематичних помилок і впливу загальних дефектів - показник, особливо важливий у приміщеннях I і II категорії вибухонебезпечності для SIL 3.

Існує чотири області, де поділ функцій особливо необхідний для задоволення вимог функціональної безпеки АСУТП:

1) польові прилади (сенсори);

2) кінцеві виконавчі пристрої;

3) логічні вирішальні пристрої;

4) зв'язок між РСК і ПАЗ.

Для кожної з цих чотирьох областей повинен бути визначений і забезпечений необхідний рівень вимог безпеки.

Щоб забезпечити необхідний рівень безпеки, необхідний поділ функцій і, відповідно, сенсорів, контролерів і виконавчих пристроїв між РСК і ПАЗ.

Зв'язок між РСК і ПАЗ підвищує інформованість технологічного персоналу та загальну безпеку АСКТП. Тим не менш, зовнішній зв'язок, особливо запис даних в ПАЗ, може вступити в конфлікт з цілісністю системи захисту. Повинні бути передбачені спеціальні процедури перевірки, щоб гарантувати, що всі записувані в систему захисту дані є достовірними і не мають негативного впливу на виконання необхідних операцій захисту. Існує декілька шляхів для зовнішнього зв'язку між РСК і ПАЗ:

а) фізичний зв'язок по каналах введення-виведення РСК і ПАЗ (наприклад, коли аналоговий або дискретний вихід від системи ПАЗ подається на фізичний вхід РСК);

б) система захисту працює за принципом "тільки читання" даних з системи ПАЗ. Це може бути прийнятним для всіх категорій вибухонебезпечності, якщо функції захисту не порушуються і немає ризику модифікації або руйнування даних системи ПАЗ.

1.3.7 Захист на рівні приладів

1.3.7.1 Методи захисту

На рівні приладів використовують три методи захисту.

Стримування вибуху – при цьому методі вибух відбувається, але він обмежений певною зоною таким чином, що поширення вибуху в навколишню атмосферу не відбувається. На цьому принципі базується вид вибухозахисту «вибухонепроникна оболонка».

Ізоляція – метод, який ґрунтується на фізичному поділі або ізоляції електричних елементів або гарячих поверхонь від вибухонебезпечних сумішей. Сюди включаються різні способи, такі як герметизація приладів і підтримання в їх корпусах підвищеного тиску.

Запобігання – метод, який обмежує енергію, як електричну, так і теплову, зберігаючи її певні рівні як при нормальній роботі, так і при аварійних обставинах. Найбільш характерним технічним прийомом тут є вид вибухозахисту «іскробезпечне електричне коло».

Вибір конкретного методу захисту залежить від ступеня безпеки, яку необхідно забезпечити.

Жоден з методів захисту не може забезпечити абсолютно надійного запобігання вибуху. Однак при правильно встановленому і такому, що підтримується у справності стандартному захисному обладнанні імовірність

вибуху прагне до нуля. Обережність, якої завжди треба дотримуватися – по можливості не розміщувати електрообладнання в небезпечних зонах.

У Європі прийняті наступні позначення типів захисту:

d – вибухонепроникна оболонка;

e – підвищена безпека;

ia – іскробезпечне електричне коло (Zone 0);

ib – іскробезпечне електричне коло (Zone 1);

h – герметична ізоляція;

m – герметизація;

n – відсутність іскроутворення;

o – занурення в масло;

p – метод підвищеного тиску;

q – заповнення порошком;

s – спеціальний захист. Цей метод стандартизований тільки у Великобританії та Німеччині.

Стандарти МЕК, які подібні до рекомендацій CENELEC (Європейський комітет з електротехнічної стандартизації), передбачають маркування приладів такого вигляду (рис. 1.4):

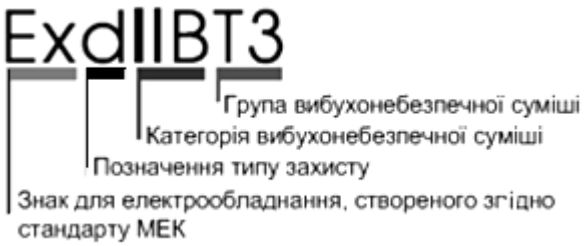

Рис 1.4 – Маркування приладів

1.3.7.2 Вид вибухозахисту "вибухонепроникна оболонка"

В даному випадку допускається, щоб джерело енергії вступило в зіткнення з небезпечною сумішшю повітря і газу. В результаті відбувається вибух, але він повинен залишатися обмеженим в оболонці, виготовленій так, щоб витримувати тиск, що виникає при вибуху усередині оболонки, і перешкоджати поширенню вибуху в навколишню атмосферу. Необхідні властивості для вибухонепроникної оболонки включають міцну механічну конструкцію, контактне з'єднання між кришкою і основною частиною оболонки і невеликі розміри щілин в оболонці.

Захисту типу "вибухонепроникна оболонка" властиві наступні проблеми при монтажі і експлуатації :

а) оболонки, особливо великогабаритні, дуже важкі, і їх установка створює механічні і будівельні складнощі;

б) корозійна атмосфера (типова для хімічних і нафтохімічних підприємств) вимагає застосування таких матеріалів, як нержавіюча сталь або бронза, що призводить до істотного збільшення вартості оболонки;

в) кабельні введення вимагають пристосувань для особливого монтажу (обтискання, кабельні хомути, металеві труби, кабель в оболонці з наповнювачем, ізоляція), що в деяких випадках обходиться дуже дорого;

г) у вологій атмосфері конденсація може створювати проблеми усередині оболонки або в трубі, що підводить;

д) безпека вибухонепроникної оболонки ґрунтується на її механічній цілісності, тому потрібні періодичні огляди.

Міра безпеки вибухонепроникної оболонки залежить від правильного використання і поточного технічного обслуговування, що виконується заводським персоналом.

Описаний метод захисту є одним з найширше використовуваних і придатний для розташованого в небезпечних зонах електроустаткування, яке має справу з високими рівнями потужності (мотори, трансформатори, лампи, комутатори, соленоїди, пускачі і інші пристрої, які роблять іскри).

1.3.7.3 Метод підвищеного тиску (очищення)

Метод підвищеного тиску ґрунтується на ідеї відділення навколишньої атмосфери від електричного устаткування. Цей метод не дозволяє небезпечної суміші повітря і газу пройти через оболонку, що містить електричні частини, які можуть робити іскри або мати небезпечні температури. Захисний газ (повітря або інертний газ), що міститься усередині оболонки, знаходиться під тиском, більш високим, ніж тиск зовнішньої атмосфери.

Для підтримки різниці тисків система підведення захисного газу має бути здатна компенсувати його втрати внаслідок витоків з оболонки або таких, що виникли через доступ персоналу.

Оскільки можливо, що небезпечна суміш може залишитися усередині оболонки після того, як система підвищення тиску буде вимкнена, необхідно видалити суміш, що залишилася, шляхом подання певної кількості захисного газу перед перезапуском електроустаткування. У разі втрати тиску автоматика або негайно відключає джерело живлення (для Zone 1), або подає звуковий або світловий сигнал (допускається для Zone 2). Іноді метод внутрішнього підвищеного тиску є єдино можливим рішенням, тобто коли жоден з видів вибухозахисту не застосовний, наприклад, у разі, коли електротехнічні пристрої мають великі габарити або панелі управління, де габаритні розміри і високі рівні енергії роблять неможливим використання вибухонепроникної оболонки або застосування методу обмеження енергії.

Використання методу підвищеного тиску обмежене захистом електроустаткування, яке не містить джерела легкозаймистої суміші. Для таких електричних засобів автоматизації, як газоаналізатори, повинен застосовуватися метод безперервного розрідження. При цьому захисний газ, повітря або інертний газ завжди зберігається в такій кількості, що концентрація легкозаймистої суміші ніколи не перевищує нижчої межі, встановленої для конкретного вибухонебезпечного газу.

Технічні засоби безпеки (датчики тиску, реле часу, витратоміри і т. д.), необхідні для активізації сигналу тривоги або виключення джерела живлення, мають бути виконані з видом вибухозахисту "вибухонепроникна оболонка" або "іскробезпечне електричне коло", тому що, як правило, вони знаходяться в зіткненні з вибухонебезпечною сумішшю як за межами оболонки, так і усередині оболонки під час стадії продування або втрати тиску.

1.3.7.4 Герметизація

Метод захисту герметизацією ґрунтується на ізоляції тих електричних елементів, які можуть викликати підпал вибухонебезпечної суміші за наявності іскри або тривалого нагріву шляхом приміщення їх в компаунд (наприклад, епоксидну смолу), який робить протидію певним умовам довкілля.

Герметизація забезпечує хороший механічний захист і є дуже ефективним засобом для відвертання контакту з вибухонебезпечною сумішшю. Як правило, вона застосовується для захисту електричних ланцюгів, що не містять рухливих елементів, окрім таких елементів (наприклад, язичкових реле), які вже знаходяться усередині оболонки. Герметизація часто застосовується як доповнення до інших методів захисту.

1.3.7.5 Метод захисту зануренням в олію

Відповідно до цього методу захисту усі електричні елементи занурюються у будь-яку незаймисту або легкозаймисту олію, яка запобігає зіткненню електричних елементів з атмосферою.

Найчастіше цей метод застосовується для нерухомого електроустаткування, такого як трансформатори.

Метод занурення в олію непридатний для контрольно-вимірювального устаткування або для електроустаткування, яке вимагає частого технічного обслуговування або огляду.

1.3.7.6 Метод захисту заповненням порошком

Цей метод захисту подібний до методу захисту зануренням в олію, за винятком того, що розділення електроустаткування і вибухонебезпечної атмосфери здійснюється заповненням оболонки порошкоподібним матеріалом так, щоб електрична дуга, генерована усередині оболонки, не викликала займання небезпечної атмосфери.

Заповнення має бути виконане так, щоб запобігти утворенню порожнин в масі. В якості заповнювача застосовується кварцовий пісок по ГОСТ 22782.2-77, його зернистість повинна відповідати стандарту.

1.3.7.7 Вид вибухозахисту "іскробезпечне електричне коло"

Метод вибухозахисту "іскробезпечне електричне коло" є найбільш прогресивною концепцією відвертання вибуху і ґрунтується на принципі обмеження енергії, запасеної в електричному колі.

Іскробезпечні електричні кола фактично не здатні генерувати електричну дугу, іскри або чинити теплову дію, що можуть викликати вибух небезпечної суміші як під час нормального функціонування, так і при певних аварійних ситуаціях.

Іскробезпечні системи можуть зберігати свої властивості при двох незалежних несправностях, таких як коротке замикання зовнішньої електропроводки і ушкодження компонентів, і при цьому система буде як і раніше безпечною.

Іскробезпечне електричне коло визначається як коло, в якому розряди або термічні дії, що виникають під час нормального режиму роботи електроустаткування, а також в аварійних режимах, не викликають займання вибухонебезпечної суміші.

Вид вибухозахисту "іскробезпечне електричне коло" ґрунтується на підтримці іскробезпечного струму (напруги, потужності або енергії) в електричному колі. При цьому під іскробезпечним струмом (напругою, потужністю або енергією) мається на увазі найбільший струм (напруга, потужність або енергія) в електричному колі, що утворює розряд, який не викликає займання вибухонебезпечної суміші в установлених відповідними стандартами умовах випробувань. Відповідно до стандарту CENELEC EN 50.020 визначаються два рівні іскробезпечних кіл : «Ex ia» і «Ex ib», що встановлюють кількість несправностей, можливих в особливих випадках, і коефіцієнти безпеки, що застосовуються на стадії проектування.

Рівень ia допускає до двох незалежних несправностей і може бути використаний в Zone 0, тоді як рівень ib допускає тільки одну несправність і може бути використаний в Zone 1. ГОСТ 22782.5-78 (Електроустаткування

вибухозахищене з видом вибухозахисту "іскробезпечне електричне коло") поширюється на вибухозахищене електроустаткування груп I і II по ГОСТ 12.2.020-76 з видом вибухозахисту "іскробезпечне електричне коло" і електроустаткування з іншими видами вибухозахисту, що має іскробезпечні і пов'язані з ними іскронебезпечні ланцюги. Стандарт повністю відповідає публікаціям МЭК 79-3 (1972 р.) і 79-11 (1976 р.) в частині основних технічних вимог і методів випробувань.

Відповідно до цього стандарту іскробезпечні електричні ланцюги розділяються на три рівні, вказаних в таблиці. 1.2.

Таблиця 1.2 - Рівні іскробезпечних електричних ланцюгів

Знак рівня іскробезпечного електричного кола для електрообладнання груп I II		Найменування рівня вибухозахисту за ГОСТ 12.2.020-76
IIa	Ia	Особливовибухобезпечний
IIb	Ib	Вибухобезпечний
IIc	Ic	Підвищена надійність проти вибуху

У стандартах на електроустаткування з видом вибухозахисту "іскробезпечне електричне коло"розглядаються три типи пристроїв:

- елементарні пристрої;
- іскробезпечне електроустаткування;
- пов'язане електроустаткування.

До елементарних пристроїв відносяться такі, в яких не перевищується жодне з наступних значень : 1,2 В; 0,1 А; 20 мкДж; 25 мВт.

До цієї категорії належать пасивні сприймаючі елементи (термопари, резистивні датчики, контакти, світлодіоди і так далі), які можуть бути безпосередньо розміщені на небезпечних ділянках. Вони не вимагають сертифікації і маркування.

Іскробезпечним електроустаткуванням є електроустаткування, у якого зовнішні і внутрішні електричні кола іскробезпечні. Зовнішнє устаткування (вихідні елементи, перетворювачі "струм-тиск", клапани соленоїдів і так далі), що застосовується у вибухонебезпечних зонах, має бути сертифіковане на іскробезпеку. Сертифікація ґрунтується на максимальному рівні енергії (група газу) і величині температури самозаймання. Пов'язане електроустаткування – таке електроустаткування або його кола, які при нормальному або аварійному режимі роботи не відокремлені гальванічно від іскробезпечних кіл.

Пасивні бар'єри, ізольовані бар'єри постійного струму і контрольно-вимірювальне устаткування, які застосовуються для сполучення і виміру сигналів, що поступають з небезпечних зон, є основною частиною цього типу

устаткування і мають бути сертифіковані на відповідність максимальному значенню енергії (група газу), яке може бути передане у вибухонебезпечну зону.

Електроустаткування повинне розміщуватися у вибухобезпечній зоні, а при розміщенні у вибухонебезпечному середовищі повинно мати відповідний вигляд вибухозахисту. У європейській практиці для пов'язаного електроустаткування, розміщеного у вибухобезпечній зоні, застосовується наступна маркування: [Ex ia] II, C.

Пов'язане електроустаткування, що розміщене у вибухонебезпечній зоні і має вигляд вибухозахисту "вибухонепроникна оболонка", маркується таким чином: Ex "d" [ia] II, C T4. Маркування в квадратних дужках вказує на те, що це пов'язане електроустаткування.

Вибухозахищене електроустаткування з видом вибухозахисту "іскробезпечне електричне коло", розміщене у вибухонебезпечній зоні, повинно бути також сертифіковане на відповідність величині температури самозаймання.

Вид вибухозахисту "іскробезпечне електричне коло" є методом, який захищає електроустаткування і пов'язану з ним електропроводку в небезпечних зонах, включаючи ушкодження, викликані розривом, коротким замиканням або випадковим заземленням сполучного кабелю. Установка є дуже спрощеною, тому що не потрібні кабелі в металевій оболонці, кабелепроводи або спеціальні пристрої. До того ж поточний ремонт і проведення контрольних перевірок може здійснюватися персоналом, навіть коли кола знаходяться під навантаженням і устаткування функціонує.

2 ВКАЗІВКИ ДО ЗМІСТУ ОКРЕМИХ РОЗДІЛІВ ДИПЛОМНОГО ПРОЕКТА

2.1 Розробка функціональної структури АСКТП

2.1.1 Структура розділу

Згідно РД 50-34.698-90 документ «Схема функціональної структури» містить:

а) елементи функціональної структури АС (підсистеми АС); автоматизовані функції і (або) завдання (комплекси завдань), сукупності дій (операцій), що виконуються при реалізації автоматизованих функцій тільки технічними засобами (автоматично) або тільки людиною;

б) інформаційні зв'язки між елементами та зі зовнішнім середовищем з короткою вказівкою змісту повідомлень і (або) сигналів, що передаються по зв'язках, і при необхідності, зв'язки інших типів (входимості, підпорядкування і т. д.);

в) деталізовані схеми частин функціональної структури (при необхідності).

У студентських проектах АСКТП можна обмежитись першим пунктом. У окремих проектах, наприклад, при проектуванні баз даних або у бізнес-орієнтованих проектах, може виникати необхідність у розділах, що відповідають пунктам б) і в).

2.1.2 Елементи функціональної структури

У цьому підрозділі приводять:

а) по кожній підсистемі перелік функцій, завдань або їх комплексів (частин системи, що у тому числі забезпечують взаємодію), які підлягають автоматизації;

б) часовий регламент реалізації кожної функції, завдання (чи комплексу завдань);

в) вимоги до якості реалізації кожної функції (завдання або комплексу завдань), форми представлення вихідної інформації, характеристики необхідної точності і часу виконання, вимоги до одночасності виконання груп функцій, достовірності видачі результатів;

г) перелік і критерії відмов для кожної функції, по якій задаються вимоги по надійності.

У АСКТП вибухонебезпечних виробництв звичайно виділяють три підсистеми:

а) ПАЗ;

б) РСУ;

в) автоматизована система оперативно-диспетчерського управління (АС ОДУ)

Для кожної підсистеми наводиться перелік виконуваних нею функцій і завдань. Підсистема ПАЗ може включати функції і задачі, перелічені у таблиці 2.1.

Таблиця 2.1 – Перелік функцій і задач ПАЗ

Функції	Задачі
01 Збирання та обробка інформації про стан об’єкта керування	0101 Введення аналогових сигналів 0102 Введення дискретних сигналів 0103 Нормалізація і фільтрація аналогових сигналів 0104 Подавлення брязкотіння контактів 0105 Контроль виходу аналогових сигналів за апаратні уставки 0106 Контроль аналогових сигналів на припустимий тренд
02 Аналіз стану технологічного процесу	0201 Контроль виходу технологічних параметрів за аварійні уставки 0202 Контроль невідпрацювання команд керування 0203 Контроль припинення роботи насосів 0203 Контроль роботи засобів транспортування (шнеків, транспортерів, контроль протоку у трубопроводах тощо) 0204 Контроль загазованості 0205 Контроль спрацювання пожежної сигналізації 0206 Контроль припинення подачі повітря КВП 0207 Контроль припинення подачі електроенергії 0208 Контроль припинення подачі палива 0209 Контроль загасанні полум’я у печі 0210 Вироблення ознак аварійних ситуацій
03 Зберігання та резервування даних	0301 Зберігання даних 0302 Резервування даних
04 Обмін інформацією з РСУ	0401 Оброблення запитів від РСУ на видачу даних 0402 Захист даних від модифікації чи руйнування

Продовження табл. 2.1

Функції	Задачі
05 Оперативне відображення, облік (документування) ходу технологічного процесу та стану обладнання	0501 Формування попереджень про відхилення від нормального ходу ТП 0502 Формування повідомлень про аварійні ситуації 0503 Формування повідомлень про локалізацію несправностей 0504 Формування повідомлень про початок і хід аварійного останову процесу 0505 Ведення протоколу нештатних ситуацій 0506 Формування звітів
06 Діагностика комплексу технічних засобів та дій персоналу	0601 Тестування технічних засобів 0602 Контроль і блокування несанкціонованих дій оператора
07 Відпрацювання аварійних ситуацій	0701 Відпрацювання технологічних блокувань і захистів 0702 Видача пропозиції оператору виконати аварійний останов у автоматичному режимі 0703 Контроль реакції оператора на аварійну ситуацію 0704 Запуск програми аварійного останову в автоматичному режимі
08 Диспетчеризація розв’язування задач	0601 Організація черговості виконання задач 0601 Запуск задач на виконання 0603 Обробка переривань 0604 Аварійне завершення задач при необхідності

В тексті цього підрозділу має бути посилання на відповідне креслення з вказівкою його шифру. Приклад схеми функціональної структури наведений у Додатку А.

2.1.3 Інформаційні зв'язки між елементами системи та зі зовнішнім середовищем

У розділі наводиться функціональна модель, що відбиває інформаційні зв'язки між елементами (підсистемами) інформаційної системи і зовнішнім середовищем.

Модель може бути представлена діаграмою, що відбиває інформаційні зв'язки між елементами (підсистемами) інформаційної системи і зовнішнім середовищем. Призначенням використання діаграми служить візуальне

відображення потоків даних між підсистемами і потік взаємодії із зовнішніми, відносно системи, елементами.

Основними об'єктами моделі є (див. рис. 2.1):

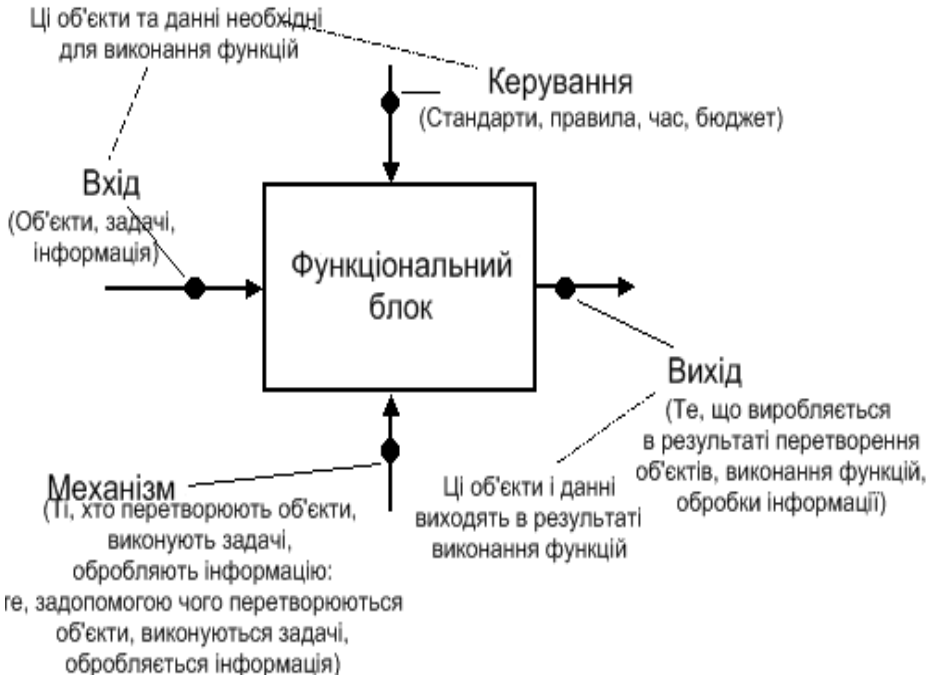

Рис. 2.1 – Умовне зображення об’єктів функціональної моделі

а) *функціональні блоки* – відображають назву функціональних елементів;

б) *стрілки управління* (згори функціонального блоку) – відображають команди (запити від користувачів або інших елементів) і інструкції, що впливають на роботу елементу;

в) *стрілки входу* (зліва від функціонального блоку) – відображають потоки даних, що входять із зовнішнього середовища або іншого елементу;

г) *стрілки виходу* (праворуч від функціонального блоку) – відображають витікаючі потоки даних (результати роботи підсистеми) в зовнішнє середовище (користувачам і адміністраторам) або в інший елемент;

д) *стрілки виконуючого механізму* (знизу функціонального блоку) – відображають засоби (програмне забезпечення, людські ресурси), які використовуються при роботі елементу.

Приклад вигляду функціональної моделі показаний на рис. 2.2.

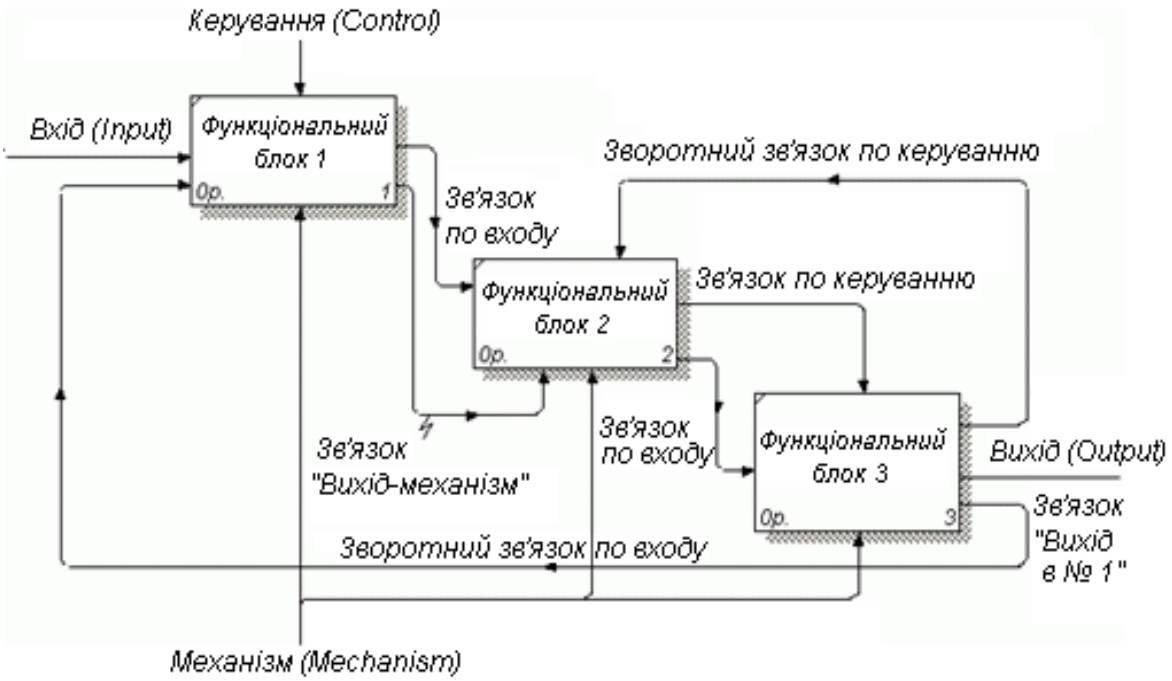

Рис. 2.2 – Структура функціональної моделі

2.1.4 Деталізовані схеми частин функціональної структури

У підрозділі наводиться деталізована модель, що відбиває інформаційні зв'язки між функціями підсистем та інших складових частин системи і їх взаємозв'язок із зовнішнім середовищем.

Призначенням відповідної діаграми служить візуальне відображення деталізованого рівня інформаційних потоків даних між функціями усередині кожної підсистеми і відображення вхідних/вихідних потоків взаємодії зі зовнішніми елементами.

2.2 Комплекс технічних засобів АСКТП

До складу ПАЗ зазвичай входять:

– контролер системи безпеки (SCS);
– інженерна станція системи безпеки (SENG);
– шина керування в реальному часі, що поєднує системи SCS та SENG.

Контролер SCS забезпечує експлуатаційну безпеку, а станція SENG виконує функції проектування та поточного обслуговування контролера SCS. Крім того, необхідно передбачати окремі, спеціалізовані власне для ПАЗ польові прилади – сенсори і виконавчі механізми.

Деякі рекомендації при виборі сенсорів :

а) в загальному випадку аналогові пристрої переважні дискретних;

б) там, де це виправдано і де це можливо, треба використати резервування або альтернативні способи отримання даних, дублюючих інформацію про одну і ту ж нерегламентовану подію;

в) пристрої, які вибрані як альтернативні, повинні мати достатню надійність, щоб можна було довіряти їх свідченням;

г) кожен сенсор, що визначає безпеку процесу, повинен мати **свій власний** (не груповий) зв'язок з контролером;

д) сенсори і трансмітери повинні мати сертифікацію на право використання в системах захисту цього класу.

Для об'єктів I і II категорії вибухонебезпеки (SIL 3) потрібне повне розділення функцій і, відповідно, установка власних клапанів РСУ і ПАЗ, щоб забезпечити необхідний рівень безпеки. Додатковий запірно-регулюючий клапан може бути використаний як для РСУ, так і ПАЗ, якщо дотримані вимоги безпеки, тобто виключені протиріччя при виконанні функцій управління і захисту. Для об'єктів III категорії вибухонебезпеки (SIL 2) за погодженням з територіальним органом технагляду для системи ПАЗ можуть бути використані ті ж контролери, що і для РСУ за умови, що система захисту відособлена від РСУ і має необхідне резервування:

а) модулів введення-виведення;

б) центральних процесорів;

в) дубльовані промислові мережі;

г) резервовані джерела живлення.

Для об'єктів I і II категорії вибухонебезпеки (SIL 3) потрібне точне розділення функцій, що виконуються контролерами РСУ і ПАЗ, щоб забезпечити необхідний рівень безпеки і виключити протиріччя при виконанні функцій управління і захисту.

У таблицю 2.2 зведені вимоги з вибору архітектури технічних засобів АСКТП.

Функції захисту мають бути реалізовані на спеціалізованому обчислювальному устаткуванні, що має Дозвіл на застосування від центральних органів технагляду.

Застосування у вибухонебезпечних зонах устаткування загальнопромислового виконання з іскробезпечними колами є одним з шляхів зниження капітальних витрат, підвищення надійності і безпеки експлуатації.

Іскрозахисні елементи забезпечують іскробезпеку електричного ланцюга за допомогою обмеження енергії в межах нижньої межі вибуху вибухонебезпечної суміші в місці установки.

Для сполучення електроустаткування, розташованого у вибухонебезпечній зоні, з електроустаткуванням, що знаходиться у вибухобезпечній зоні (пов'язане електроустаткування), повинні застосовуватися певні обмежувальні елементи, які можна розділити на дві групи :

а) діодні бар'єри безпеки, або пасивні бар'єри;

б)гальванічно ізольовані бар'єри безпеки або активні бар'єри.

Таблиця 2.2 – Вибір архітектури ПАЗ в залежності від інтегрального рівня безпеки

SIL	Зона	Архітектура			Примітка
		Входів	Контролерів	Виходів	
2	Zone 2	1oo1 або 1oo2	ПЛК з двома процесорами або резервованими модулями управління	1oo1	Періодичне тестування входів і виходів
3	Zone 1	1oo2	1oo2D або 2oo3	1oo1	Оперативне тестування входів і виходів
3	Zone 0	1oo2 або 2oo3	1oo2D або 2oo3	1oo2	Оперативне тестування входів і виходів

Пасивні розділові елементи є найбільш простими. Принцип дії таких блоків іскрозахисту полягає в наступному: у разі появи небезпечної напруги на затискачах, підключених до приладів у вибухобезпечній зоні, значення якої перевищує напругу стабілізації стабілітронів, відбувається пробій стабілітрону, в колі з'являється струм, достатній для спрацювання запобіжника. Конструктивно блок іскрозахисту є єдиним нерозбірним блоком, залитим компаундом, що є стійким до умов експлуатації.

Активні розділові пристрої – це гальванічно ізольовані активні розділові пристрої (бар'єри), які мають джерело напруги або формувачі сигналів, передають або приймають сигнали з вибухонебезпечних зон через ізольований тракт (рис. 2.3).

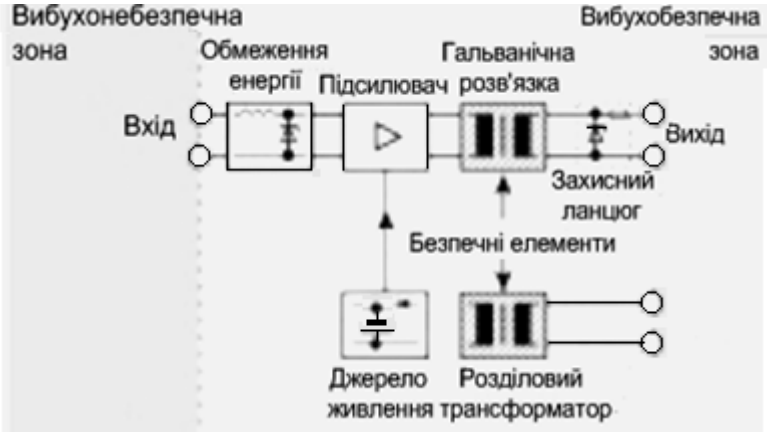

Рис. 2.3 – Схема гальванічно ізольованого бар'єра

Основна відмінність між пасивними ВІС і гальванічно ізольованими бар'єрами (активними бар'єрами) полягає у безпечних елементах, які застосовуються для ізоляції між вибухобезпечною зоною і електричними колами, що забезпечують іскробезпеку. Ця конфігурація не дозволяє небезпечній напрузі, яка прикладена до затискачів, розташованих у вибухобезпечній зоні, бути переданою у вторинні кола без обмеження за максимальною напругою при аварійній ситуації.

Переваги активних бар'єрів :

а) немає необхідності в системі заземлення;

б) можуть бути застосовані заземлені первинні перетворювачі;

в) гальванічна ізоляція знімає проблеми зворотних струмів і забезпечує високий коефіцієнт подавлення завади загального вигляду;

г) досягається більш висока точність вимірів;

д) безпосередньо можуть використовуватися вихідні сигнали.

Недоліки гальванічно ізольованих бар'єрів :

а) висока вартість елементів, порівнянна з вартістю установки;

б) вони спроектовані для особливих застосувань, тому є менш гнучкими.

Іскробезпечне електроустаткування ніколи не застосовується окремо. Як правило, воно є частиною системи, в якій застосовуються сертифіковані елементи, що гарантують безпеку системи.

Така система включає:

а) електроустаткування, розміщене у вибухонебезпечній зоні;

б) електроустаткування, розміщене у вибухобезпечній зоні;

в) електропроводку між ними.

Аналіз іскробезпечних систем виходить з критеріїв, які підтверджують, що максимальне значення електричної і теплової енергії, яке виділяється у вибухонебезпечній зоні, є нижчим, ніж межі займання потенційно вибухонебезпечної суміші при нормальному або аварійному режимах роботи.

2.3 Схема автоматизації

Схема автоматизації — основний технічний документ, що визначає структуру (ієрархію) систем автоматизації, функції систем контролю і керування об'єктом, що автоматизується, оснащення систем технічними засобами: приладами та засобами автоматизації, щитами, пультами, обчислювальною технікою тощо. Вона використовується для обґрунтування основних проектних рішень при експертизі і затвердженні проекту, для підготовки та виконання робіт з монтажу та налагодження систем автоматизації, навчання операторів-технологів роботі на автоматизованій установці.

Очевидно, що схеми автоматизації вибухонебезпечних виробництв мають містити інформацію про функції і засоби безпеки.

У нормативних документах нема прямих вказівок, як позначати на схемах засоби безпеки. Проте в ДСТУ Б А.2.4-16:2008 говориться: «Допускається використовувати додаткові графічні зображення, не передбачені стандартом. Додаткові графічні зображення повинні бути розшифровані на схемі». Тому в дипломному проекті рекомендується використання умовних позначень, передбачених міжнародним стандартом ANSI/ISA–S5.1–1984 (R1992), які показані в табл. 2.3.

Таблиця 2.3 – Позначення приладів або функцій на схемі автоматизації

	Польові прилади	Розміщені на щиті	Розміщені за щитом (у шафі)	Розміщені на місцевому пульті
1	2	3	4	5
Локальні прилади				
Прилади РСУ				
Прилади ПАЗ				
Функція комп’ютера				

На схемі автоматизації треба передбачити відсічні клапани ПАЗ, які призначені для припинення подачі сировини на технологічну установку і відбору продуктів у разі виникнення аварійної ситуації. Для таких клапанів рекомендується позначення  .

2.4 Розробка систем діагностики

При проектуванні систем діагностики технічних засобів АСКТП слід керуватися наступними правилами.

Зовнішня діагностика повинна надавати інформацію у вигляді розгорнутої структури відеокадрів. На кореневому відеокадрі повинна бути представлена інформація про поточний режим і стан об'єкта керування, його основних компонентів, основна технологічна інформація, аварійна сигналізація. Докладна інформація з поточного стану, локалізації джерел і причин порушення нормального стану, заходах відновлення необхідного стану й інша специфічна інформація, у тому числі стосовна до конкретних елементів устаткування, повинна надаватися окремими відеокадрами.

На усіх відеокадрах повинна бути наскрізна інформація (умовний сигнал чи рядок текстового повідомлення) про наявність інформації про аварію, несправності, останови і попередження. Повинна бути реалізована функція вказівки швидкого переходу до екранів, призначених для візуалізації розгорнутих варіантів вказаних повідомлень.

При представленні інформації треба дотримуватись загальноприйнятих угод по кольорам:

- червоний - аварії і несправності;
- жовтий - попередження;
- зелений - нормальні, відповідні технології сигнали, повідомлення і стани;
- інші - кольори для інформації, що не відповідає призначенням червоного, жовтого і зеленого кольорів, вибираються по зручності сприйняття;
- миготіння - може використовуватися для виділення, локалізації першоджерела інформації, щоб привернути увагу до зміни стану якого-небудь сигналу або до підказки оператору про шлях доступу до інформації і т. д.

Повинна бути розроблена система допомоги (підказки) з роз'ясненнями по змісту, умовним позначкам і активним клавішам.

Також повинен бути розроблений відеокадр самої системи діагностики, що відображає справність окремих (складових) частин системи діагностики.

Обсяг інформації, наданий системою діагностики, повинен включати діагностичну, технологічну і статистичну інформацію, як по усіх функціях технологічного устаткування, так і по роботі системи керування.

Діагностична інформація повинна формуватися і надаватися у відповідності з наступними рівнями пріоритету:

а) аварії – аномалії, при яких необхідно перервати будь-який режим роботи з ввімкненням аварійних ланцюгів, щоб уникнути погрози травмування обслуговуючого персоналу, поломки устаткування чи випуску бракованої продукції;

б) несправності – аномалії в роботі пристроїв, механізмів, що виявляються в невиконанні ними своїх функцій:

в) останови – припинення роботи устаткування за допомогою виконання штатних функцій без включення аварійних ланцюгів, включаючи технологічні останови;

г) попередження – повідомлення про події, що вимагають від обслуговуючого персоналу виконання яких-небудь дій для забезпечення ефективної, надійної і якісної роботи устаткування відповідно до обраного режиму і технологічного процесу;

д) інформація, що відображає стан устаткування технологічного процесу і зв'язків із суміжним устаткуванням.

Для однозначного визначення причини будь-якого переривання в роботі об'єкта керування, викликаного аваріями, несправностями чи остановами, або причини невиконання керуючих дій діагностика повинна:

а) стежити за поточним станом систем і елементів устаткування і за тим, що повинно виконуватися в кожен момент часу по всіх задачах керування (наприклад, при натиснутій кнопці переміщення виконавчого механізму в ручному режимі);

б) при перериванні в роботі устаткування чи невиконанні керуючих дій – аналізувати виконання робочої програми і стан елементів та систем устаткування з метою виявлення всіх діючих першопричин цих відхилень;

в) видавати інформацію про всі діючі першопричини відхилень у наступному вигляді:

1) тип відхилення в роботі устаткування (аварія, несправність, останов, невиконання керуючого впливу);

2) відповідний сигнал контролера з коментарем, що стан цього сигналу є першопричиною відхилення в роботі устаткування;

3) для виконуючих механізмів: адреса (з коментарем) вихідного сигналу, у результаті вмикання/вимикання якого повинен установитися необхідний стан вхідного сигналу;

4) локалізація джерела сигналу-першопричини відхилення в роботі устаткування за допомогою умовного символу на мнемосхемі устаткування відповідно до територіального розташування джерела відхилення;

г) діагностика повинна реєструвати і зберігати інформацію про причини відхилень у роботі устаткування.

Діагностика повинна також забезпечити виявлення причини короткочасних несанкціонованих вмикань/вимикань вихідних сигналів (наприклад, через несправність датчиків). За запитом оператора повинна зареєструвати і надати оператору на станції діагностики адресу і коментар вхідного сигналу контролера, що є причиною короткочасного несанкціонованого вмикання чи вимикання заданого оператором вихідного сигналу.

Діагностика повинна відображати поточні режими роботи і стан основних систем та функціональних частин устаткування. Інформація повинна видаватись з режимам роботи, несправностям і помилкам окремих електронних пристроїв АСКТП і її елементів (джерело і код помилки з коментарями) з точністю до замінного модуля чи окремої електронної плати, із указівками на необхідність заміни цих пристроїв.

Станція діагностики повинна відображати також статистичну інформацію:

- статистику простоїв устаткування за поточну і попередню зміни;
- таблиці продуктивності виробництва за поточну і попередню зміни;
- поточний графік робочого часу, централізований календарний час у контролерах, що виконують статистичні функції;
- іншу необхідну інформацію.

У протоколі, що друкується на станції діагностики, повинна фіксуватися інформація про аварії, несправності і попередження з указівкою першопричини і часу початку та закінчення подій. Діючі (неусунуті) причини повинні бути виділені окремо.

2.5 Інтерфейс користувача

Інтерфейси користувача включають:

- інтерфейси оператора :
- інтерфейси технічного обслуговування, проектування і розробки.

Як правило, операторський відеоінтерфейс системи захисту вбудовується в робочі станції РСУ.

Відеозображення на РСУ можуть поєднувати обробку функцій забезпечення безпеки і в той же час здійснювати функції РСУ, що власне управляють. Дані з системи безпеки, що відображаються для оператора, повинні оновлюватися з частотою, необхідною для своєчасній реакції у разі виникнення пепередбачених умов. Відеозображення, що мають відношення до ПАЗ, повинні ясно ідентифікуватися як такі, унеможливлюючи неоднозначну інтерпретацію, або потенційної нерозберихи в непередбаченій ситуації.

Оператори повинні мати легкий доступ до пов'язаних з безпекою відеозображень, переважно за допомогою єдиного натиснення на ключову клавішу або сенсорно-екранним способом, що дає прямий вхід в ієрархію зображень.

У системах ПАЗ передбачають також оперативні панелі. Панелі мають бути розташовані так, щоб забезпечувати легкий доступ операторів. Розміщення кнопок, сигнальних табло, ключів на панелі має бути таким, щоб гарантувати, що положення кнопок, ламп, перемикачів, написів і інша інформація не заплутує оператора і не надає можливості зробити помилку в стресовій ситуації.

Має бути передбачена кнопка тестування усіх світлових і звукових індикаторів.

Інтерфейси технічного обслуговування, проектування і розробки складаються із засобів програмування, тестування і технічного обслуговування системи ПАЗ.

Ці інтерфейси є тими засобами, які використовуються для:

- конфігурації апаратних засобів;
- програмної розробки, документування, завантаження системи ПАЗ;
- доступу до прикладного програмного забезпечення для зміни, тестування і перегляду;
- контролю ефективності використання системних ресурсів ПАЗ і діагности;
- зміни рівня секретності системи ПАЗ і доступу до змінних прикладного програмного забезпечення.

Інтерфейси технічного обслуговування, проектування і розробки повинні мати можливість відображення робочого стану і діагностичного статусу усіх компонентів ПАЗ (модулів введення-виведення, процесорів, і тому подібне), включаючи стан каналів зв'язку між ними. Інтерфейси технічного обслуговування, проектування і розробки повинні мати засоби для копіювання застосовних програм на зовнішній носій. Інтерфейси технічного обслуговування, проектування і розробки мають бути доступні тільки:

- із спеціально призначеної для цих цілей станції;
- по спеціальному дозволу;
- і тільки для спеціально допущеного персоналу.

3 РОЗРАХУНКОВА ЧАСТИНА

3.1 Склад розрахункової частини

Пояснювальна записка проекту АСУТП вибухонебезпечних виробництв може включати наступні специфічні розрахунки:

а) розрахунок характеристик безпеки;

г) оцінку іскробезпеки електричних кіл;

д) проектний розрахунок надійності АСКТП.

3.2 Розрахунок характеристик безпеки

Визначення рівня SIL для конкретної інструментальної функції безпеки SIF (Safety Instrumented Function) проводиться на основі результатів аналізу небезпек і ризиків, притаманних контрольованому технологічному процесу.

Характеристики безпеки докладно описані в частині 4 стандарту МЕК 61508. MTTF (Mean Time To Failure) – середній час напрацювання на відмову – є показником середнього часу успішної роботи пристрою (системи) до настання відмови будь-якого виду. Цей показник може інтерпретуватися і як термін служби пристрою, якщо він не підлягає відновленню або ремонту.

Характеристикою ремонтопридатності пристроїв є середній час їх відновлення MTTR (Mean Time Te Repair). Середній час між двома послідовними відмовами MTBF (Mean Time Between Failures) зазвичай виражається в роках. Між даними показниками існують наступні співвідношення (рис. 3.1):

• MTBF = MTTF + MTTR;

• MTTF = MTBF – MTTR.

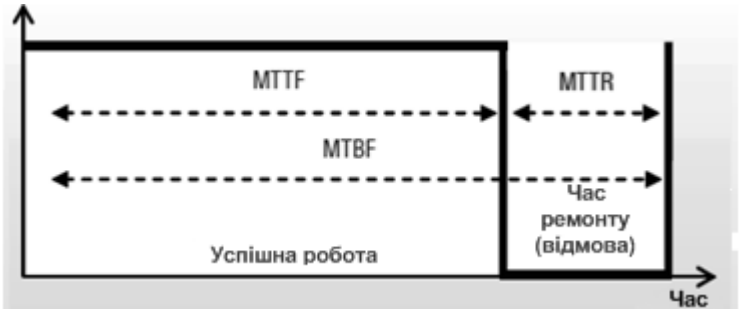

Рис 3.1 – Схематичне представлення MTTF, MTBF та MTTR

Зворотна до MTBF величинаλ = 1 / MTBF – це інтенсивність відмов компонента або пристрою:

$$\lambda = \frac{N_в}{N}, \tag{3.1}$$

де $N_в$ - кількість відмов за одиницю часу;

N - кількість компонентів, що можуть відмовити.

Загальна інтенсивність відмов λ_{tot} ділиться на дві основні категорії: інтенсивність безпечних відмов λ_s та інтенсивність небезпечних відмов λ_d:

$$\lambda_{tot} = \lambda_s + \lambda_d \quad (3.2)$$

Небезпечними є відмови, які призводять до втрати функціональної безпеки системи та/або до втрати її безпечного стану. Безпечними вважаються відмови, які призводять до помилкового відключення виходу і останову контрольованого технологічного процесу (помилкове спрацювання).

Величина, зворотна λ_s - це MTBFs або середній час (в роках) між можливими помилковими остановами. У свою чергу, величина, зворотна λ_d - це MTBFd, середній час (в роках) між можливими небезпечними відмовами.

У кожній із зазначених категорій відмови, в свою чергу, поділяються на детектовані (λ_{sd}, λ_{dd}) і недетектовані (λ_{su}, λ_{du}) онлайновою діагностикою:

$$\lambda_s = \lambda_{sd} + \lambda_{su}, \quad \lambda_d = \lambda_{dd} + \lambda_{du} \quad (3.3)$$

Першим параметром, що визначає інтегральний рівень безпеки SIL, є середня ймовірність відмови на запит виконання функції безпеки PFDavg (Probability of Failure on Demand). Для систем з архітектурою 1oo1 формула розрахунку PFDavg має вигляд:

$$\text{PFDavg}(TI) = \lambda_{dd} \times RT + \lambda_{du} \times TI / 2, \quad (3.4)$$

де RT - час відновлення в годинах (зазвичай 8 годин);

TI - інтервал часу між функціональними перевірочними тестами (1–5–10 років), що позначається також Tproof.

У багатьох випадках, наприклад, коли ефективність періодичних тестів з виявлення небезпечних відмов дорівнює 100%, формула для розрахунку PFDavg спрощується:

$$\text{PFDavg}(TI) = \lambda_{du} \times TI / 2. \quad (3.5)$$

Другим параметром, що визначає інтегральний рівень безпеки, є частка безпечних відмов SFF (Safety Failure Fraction).

$$\text{SFF} = \frac{\sum \lambda_{dd} + \sum \lambda_{sd} + \sum \lambda_{su}}{\sum \lambda_{dd} + \sum \lambda_{du} + \sum \lambda_{sd} + \sum \lambda_{su}} = 1 - \frac{\sum \lambda_{du}}{\sum \lambda_{dd} + \sum \lambda_{du} + \sum \lambda_{sd} + \sum \lambda_{su}}. \quad (3.6)$$

Відповідно до стандарту МЕК 61508 компоненти або підсистеми відносяться до типу А або В (див. табл. 3.1 і табл. 3.2):

а) компоненти типу А – це прості пристрої, поведінка і види відмов яких добре відомі;

б) компоненти типу В – це комплексні компоненти з потенційно невідомими видами відмов, наприклад мікропроцесори, спеціалізовані процесори і т.п. В табл. 3.1 і 3.2 представлені обмеження на використання простих і резервованих архітектур в системах з різними рівнями SIL.

Таблиця 3.1 – SFF для компонентів типу А

SFF	Стійкість до апаратних відмов 0	Стійкість до апаратних відмов 1	Стійкість до апаратних відмов 2
Менше 60%	SIL 1	SIL 2	SIL 3
Від 60 до 90%	SIL 2	SIL 3	SIL 4
Від 90 до 99%	SIL 3	SIL 4	SIL 4
Більше 99%	SIL 3	SIL 4	SIL 4

Таблиця 3.2 – SFF для компонентів типу В

SFF	Стійкість до апаратних відмов 0	Стійкість до апаратних відмов 1	Стійкість до апаратних відмов 2
Менше 60%	Не допускається	SIL 1	SIL 2
Від 60 до 90%	SIL 1	SIL 2	SIL 3
Від 90 до 99%	SIL 2	SIL 3	SIL 4
Більше 99%	SIL 3	SIL 4	SIL 4

Примітка. Стійкість до апаратних відмов N означає, що (N+1)-а відмова може призвести до порушення функції безпеки пристрою.

Розрахуємо значення MTBF, MTBFs для помилкових спрацьовувань, PFDavg, RRF і можливий рівень SIL для функції безпеки системи, представленої на рис. 3.2. Ця система складається з датчика-перетворювача Tx, бар'єру іскробезпеки, програмованого логічного контролера (ПЛК) та електромагнітного клапана, який є кінцевим виконавчим елементом.

Як вихідні дані при розрахунку використані значення параметрів компонентів системи (MTBFλ_{du}, λ_{dd}, λ_s), які можна знайти в посібниках з безпеки, що надаються їх виробниками.

Вихідні та розрахункові дані зведені в табл. 3.3. З таблиці видно, що основним критерієм визначення рівня SIL є PFDavg або фактор зниження ризику RRF.

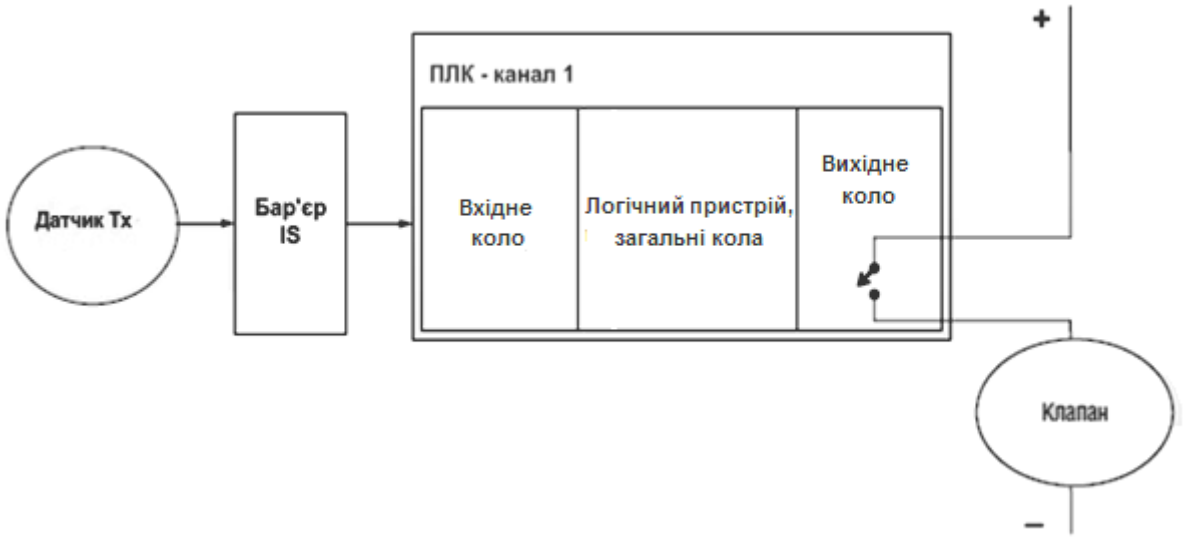

Рис.3.2 – Система з архітектурою 1oo1

Таблиця 3.3 – Вихідні та розрахункові дані для системи з архітектурою 1oo1 та між тестовим інтервалом 1 рік

Підсистеми	MTBF (р.)	λ/рік	MTBFs (р.)	λ_s/рік	λ_{dd} /рік	λ_{du}/рік	PFDavg= λ_{dd} /2	% від общої PFDavg	RRF = 1/PFDavg	SFF	SIL
Датчик Tx	102	0,00980	125	0,00800	0,0010	0,00080	0,000400	3,40%	2500	91,8%	2
Бар'єр 010145	314	0,00318	629	0,00159	0,0014	0,00019	0,000095	0,81%	10 526	94,0%	3
ПЛК	685	0,00146	741	0,00135	0,0001	0,00001	0,000005	0,04%	200 000	99,3%	3
Клапан	12	0,08333	24	0,04150	0,0200	0,02183	0,010915	92,87%	92	73,8%	1
Джерело живлення	167	0,00600	189	0,00530	0,0000	0,00070	0,000350	2,97%	2 857	88,3%	3
Загальна (БГТ)	10	0,10377	17	0,05774	0,0225	0,02353	0,011765	100%	85	—	1

У випадках, коли значення PFDavg кінцевого елемента таке високе, як в розглянутому прикладі, інші компоненти системи повинні мати рівні безпеки не нижче SIL 3. Таким чином, компоненти з рівнем SIL 3 використовуються не тільки тоді, коли необхідно забезпечити рівень SIL 3 для всієї системи, але і в тих випадках, коли для системи потрібно рівень SIL 1, а один з її компонентів, маючи високу інтенсивність відмов, вносить великий внесок у загальну PFDavg.

Датчик, який має високий RRF (2500), тим не менш, придатний тільки для використання в системах з рівнем не вище SIL 2 (компонент типу B із стійкістю до апаратних відмов 0 - табл. 2), оскільки його SFF не відповідає застосуванням з рівнем SIL 3.

3.3 Оцінка іскробезпеки електричних кіл

3.3.1 Теоретичні відомості

Електричні параметри, приведені в Сертифікаті відповідності кожної одиниці обладнання, не можуть бути безпосередньо використані для оцінки загальної іскробезпеки комплекту. Підключене пов'язане енергоустаткування повинно розглядатися єдиним електричним пристроєм, для якого розраховуються нові граничні значення електричних параметрів.

У залежності від виду і порядку з'єднання або можливого аварійного режиму повинні розглядатися послідовне, паралельне або змішане з'єднання, особливо при аварійному режимі, при якому можлива зміна електричних і конструктивних параметрів елементів, що впливають на іскробезпеку кола (послідовна або паралельна схема з'єднання).

Допустимі значення напруги холостого ходу U_0 і струму короткого замикання I_0 для різних видів з'єднань обчислюються по різних критеріях:

а) для паралельного з'єднання (рис. 3.3) U_0 визначається по найбільшому значенню окремих напруг холостого ходу, I_0 – по сумі значень окремих допустимих струмів короткого замикання.

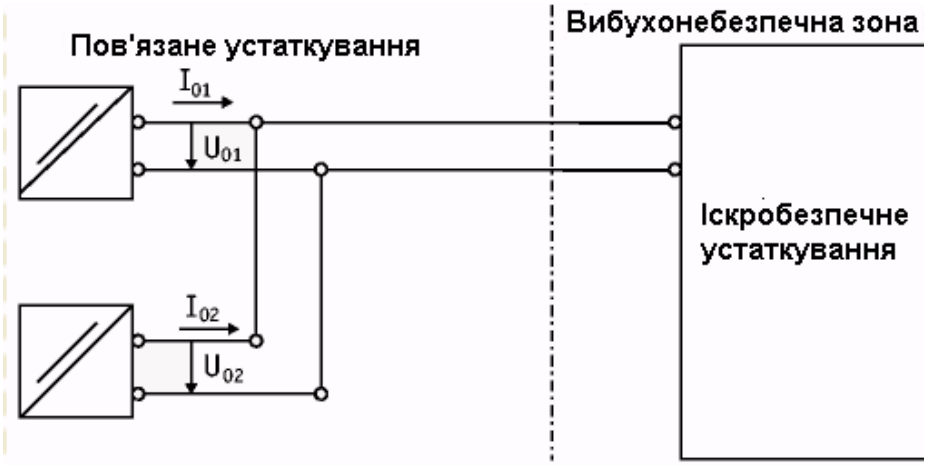

Рис. 3.3 – Паралельне з'єднання

б) для послідовного з'єднання (рис. 3.4) U_0 обчислюється по сумі окремих значень напруг холостого ходу, I_0 – по найбільшому значенню окремих допустимих струмів короткого замикання.

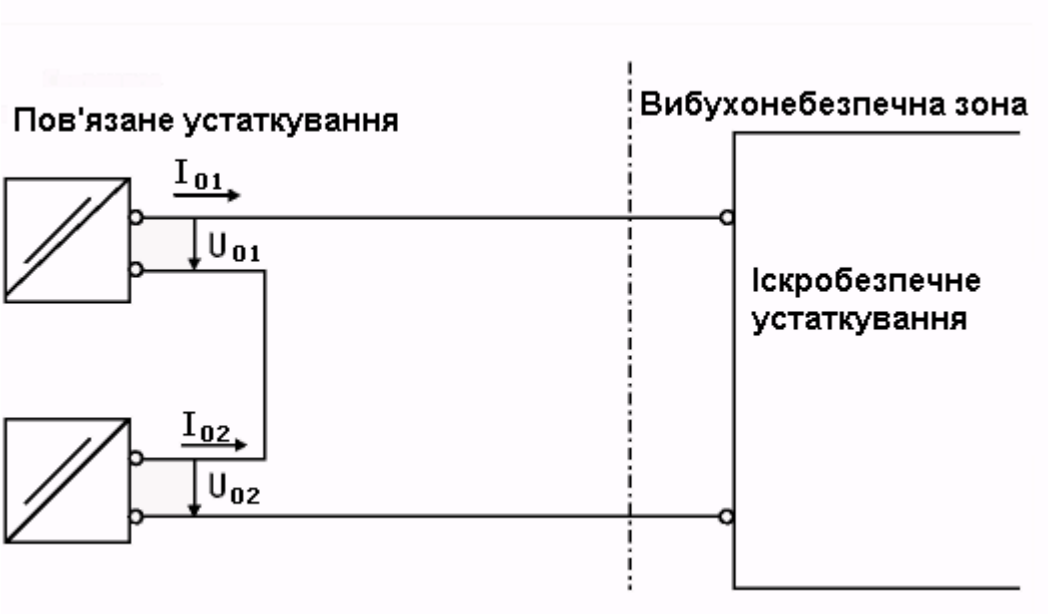

Рис. 3.4 – Послідовне з'єднання

в) для послідовно-паралельного з'єднання (рис. 3.5) U_0 або I_0 обчислюються по сумі відповідних окремих значень U_{0n} або I_0

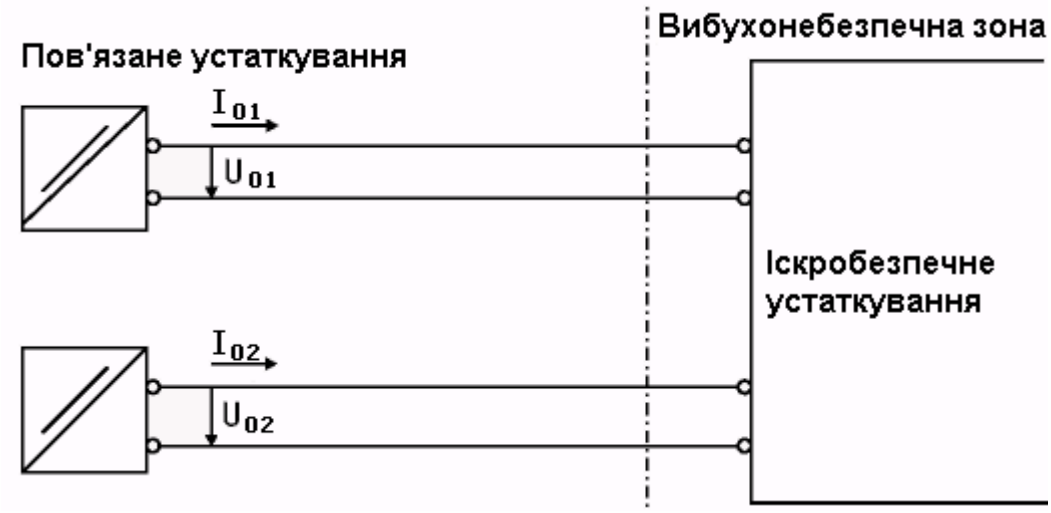

Рис. 3.5 – Послідовно-паралельне з'єднання

Цей метод визначення максимально допустимих параметрів потрібно застосовувати, в основному, у разі простих або ясно скомпонованих з'єднань. Метод передбачає план дій для найгіршого випадку і тому дає вищу міру безпеки. Максимально допустимі значення U_0, I_0, L_o и C_0 можуть бути отримані по графіках залежності мінімальних запалюючих струмів і напруг для вибухонебезпечних сумішей оптимального складу, приведених в ГОСТ 22782.5-78 «Електрообладнання вибухозахищене з видом вибухозахисту "іскробезпечне електричне коло"».

Для визначення іскробезпечного значення струму (напруги) необхідно для заданих електричних параметрів кола знайти значення мінімального запалюючого струму (напруги) для даної вибухонебезпечної суміші і потім

розділити його на коефіцієнт іскробезпеки, тобто на 1,5. При розрахунку кіл змінного струму необхідно приймати амплітудні значення струму і напруги.

Індуктивність і ємність іскробезпечних кіл (в тому числі з'єднувальних кабелів і проводів, ємність і індуктивність яких визначається за довідковими характеристиками, розрахунком або вимірюванням) не повинні перевищувати максимальних значень, обумовлених в технічній документації на ці кола.

3.3.2 Приклад оцінки іскробезпечності схеми для тензовимірювань

3.3.2.1 Зусилля, що прикладається, може бути виміряне тензодавачем – перетворювачем, який перетворює зміну зусилля, що прикладається, в зміну електричного опору. Як правило, такий перетворювач застосовується разом з мостом Уїтстона, в якому одне, два або навіть всі чотири плечі являють собою тензодавачі, а вихідна напруга змінюється у відповідь на варіації вимірюваного зусилля. Давач зусилля встановлений у вибухонебезпечній зоні. Як розділові елементи між іскробезпечними і іскронебезпечними колами застосовані блоки іскрозахисту на стабілітронах (БІС). Схема зображена на рис. 3.6.

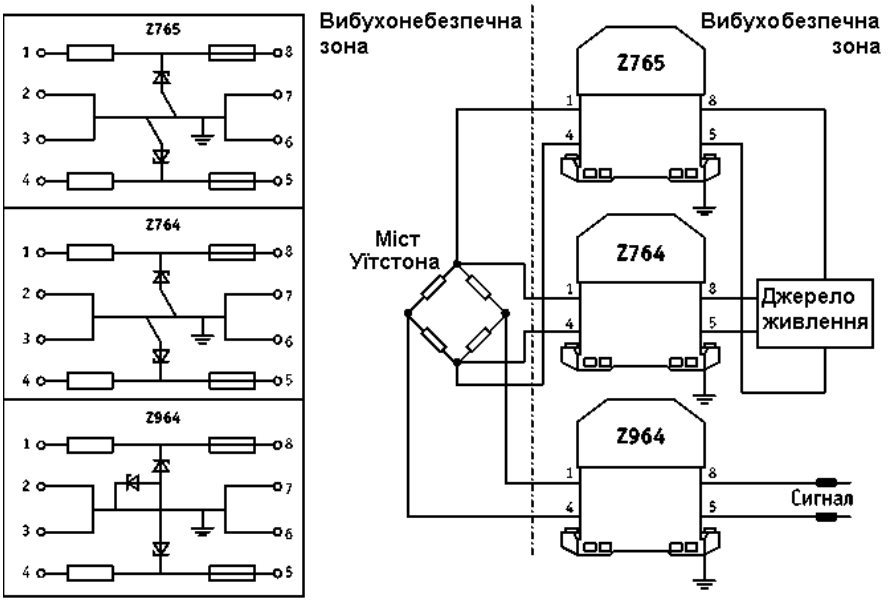

Рис. 3.6 – Іскробезпечна схема для тензовимірювань

Міст Уїтстона живиться через БІС Z765, який забезпечує живлення з номінальним значенням напруги 8 В вимірювального моста з внутрішнім опором 350 Ом. Коло зворотного зв'язку через БІС Z764 може не використовуватися. Сигнал мілівольтового діапазону передається в безпечну зону через БІС Z964.

3.3.3.2 Оцінка іскробезпечності проводиться поетапно:

а) на першому етапі зіставляються електричні параметри енергоустаткування (табл. 3.4 і 3.5);

б) на другому етапі визначаються граничні значення електричних параметрів системи, як показано далі.

Таблиця 3.4 – Електричні параметри БІС

Вибухозахищене електроустаткування		Виробник	Сертифікат відповідності	U_0, В	I_0, мА	P_0, мВт	L_0, мГн	C_0, нФ	Залежність
Опис	Модель								
Блок іскрозахисту	Z765	Pepperl + Fuchs GmbH	D.95C.050 (ИСЦ ВЭ)	14,7	75	276	15	750	лінійна
Блок іскрозахисту	Z764			11,6	12	30	230	1600	лінійна
Блок іскрозахисту	Z964			11,6	12	30	230	1600	

Таблиця 3.5 – Електричні параметри тензодавача

Вибухозахищене електроустаткування		Виробник	Сертифікат відповідності	U_i, В	I_i, мА	P_i, мВт	L_i, мГн	C_i, нФ
Опис	Модель							
Тензодавач	Z6H	Hottinger Baldwin	Ex-90.C2094	23	196	1130	0	0
Індуктівність і ємність з'єднувального кабелю: L_c= 1 мГн/км C_c=110нФ/км або технічні дані, надані виробником кабелю для l=500 м							0,5	55
Суммарні значення індуктивності та ємності: SL_i і SC_i							0,5	55

3.3.3.3 Визначаються найбільші значення напруги і струму в системі по значеннях параметрів U_0 і I_0, вказаних для пов'язаного енергоустаткування.

Максимальне значення з окремих значень напруг U_0 = 14,7 В.

Сумарний струм в паралельному електричному колі I_0 = (75+12+12) мА = 99,0 мА.

3.3.3.4 Перевіряється умова: найбільше значення струму в системі (I_0), помножене на коефіцієнт іскробезпеки 1,5, не повинне перевищувати значення струму, отриманого із залежності мінімального запалюючого струму $I_{з\ min}$ від напруги джерела $U_{дж}$ в омічному колі для відповідної групи енергоустаткування при максимальному значенні напруги в системі U_0 (рис. 3.5).

З графіків на рис. 3.7 видно, що при напрузі U_0 = 14,7 В для вибухонебезпечної суміші підгрупи IIC (воднево-повітряна) максимальне допустиме значення струму короткого замикання $I_{макс}$ = 980 мА, що істотно перевищує $I_0 \cdot 1{,}5 = 99 \cdot 1{,}5 = 148{,}5$ мА.

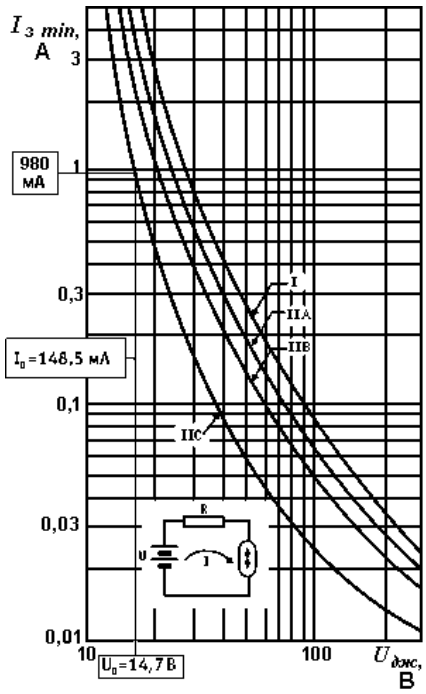

Рис. 3.7 – Залежність мінімального запалюючого струму від напруги джерела $U_{дж}$

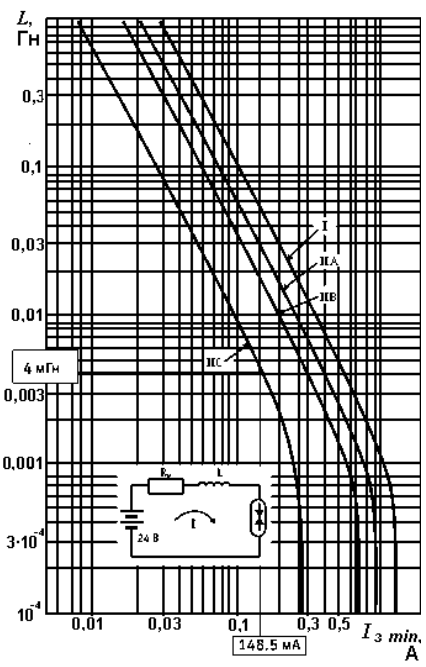

Рис. 3.8 – Залежність мінімального запалюючого струму від індуктивності кола L

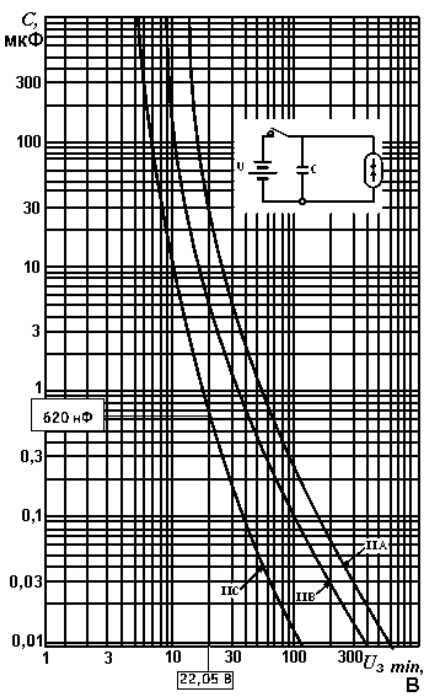

Рис. 3.9 – Залежність мінімальної запалюючої напруги $U_{з\ min}$ від ємності кола C

Отже, умову іскробезпеки відповідно до залежності мінімального запалюючого струму від напруги джерела для омічного кола можна вважати виконаною.

3.3.3.5 Максимально допустиме значення індуктивності L_0 визначається із залежності мінімального запалюючого струму від індуктивності кола і напруги джерела для відповідної підгрупи енергоустаткування по найбільшому значенню струму в системі (I_0), помноженому на коефіцієнт іскробезпечності 1,5 (рис. 3.8).

Для значення струму 148,5 мА отримуємо індуктивність 4 мГн для підгрупи енергоустаткування IIC**.**

3.3.3.6 Максимально допустиме значення ємності C_0 визначається із залежності мінімальної запалюючої напруги від ємності кола водне-повітряної суміші (підгрупа IIC) по найбільшому значенню напруги в системі U_0**,** помноженому на коефіцієнт іскробезпеки 1,5 (рис. 3.9).

З рис. 3.7 видно, що при напрузі 14,7 · 1,5 = 22,05 В для водневоповітряної суміші (підгрупа IIC) максимально допустиме значення ємності дорівнює 620 нФ.

3.3.3.7 Перевіряється умова: максимально допустимі значення C_0 і L_0 повинні задовольняти вимогам іскробезпеки електричного кола. Ці вимоги визначають умови іскробезпеки електричного кола тільки з одним пов'язаним електропристроєм.

При оцінці іскробезпеки враховується з'єднувальна лінія довжиною 500 м з параметрами C_c=55 нФ, L_c=0,5 мГн (табл. 3.6).

Таблиця 3.6 – Перевірка умов іскробезпеки кола

Іскробезпечне енергоустаткування + параметри з'єднувальної лінії	Умова іскробезпеки	Пов'язане енергоустатку-вання
(0+55) нФ	Менше або дорівнює	620 нФ
(0+0,5) мГн	Менше або дорівнює	4мГн
23 В	Більше	14,7 В
196 мА	Більше	99,0 мА
1130 мВт	Більше	364 мВт

3.3.3.8 Визначається група вибухозахищеного енергоустаткування системи, з урахуванням того, для якого типу вибухонебезпечної суміші вибиралася залежність мінімальних запалюючих струмів і напруг.

Все енергоустаткування схвалене для використання у воднево-повітряній суміші IIC. Всі значення параметрів отримані із залежності мінімальних запалюючих струмів і напруг для воднево-повітряної суміші (підгрупа IIC). Оскільки іскробезпека підтверджена відповідно до цих параметрів, система задовольняє вимогам для підгрупи вибухозахищеного енергоустаткування IIC.

3.3.3.9 Визначається група вибухонебезпечної суміші газів і пари в залежності від величини температури самозапалення. Для вибухозахищеного енергоустаткування групи II в залежності від значення максимальної температури поверхні встановлюються температурні класи, вказані в таблиці 3.7. Максимальна температура поверхні визначається формулою:

$$T = P_0 \cdot R_{th} + T_{нвк}, \qquad (3.7)$$

де T — максимальна температура поверхні, °С;

P_O — максимальна потужність, що виділяється джерелами енергії з лінійними вольтамперними характеристиками, визначається з співвідношення $P_O = U_0 I_0/4$;

R_{th} — специфікується виробником комплектуючих виробів;

$T_{нвк}$ — температура навколишнього середовища (звичайно приймається 40°С).

Таблиця 3.7 – Визначення температурних класів

Температурний клас	Максимальна температура поверхні, °С
Т1	450
Т2	300
Т3	200
Т4	135
Т5	100
Т6	85

3.4 Проектний розрахунок надійності АСКТП

3.4.1 Теоретичні відомості

Відповідно до ГОСТ 24.701, оцінка надійності проводиться за наступними показниками:

а) надійність реалізації функцій системи;

б) небезпека виникнення в системі аварійних ситуацій.

Для опису безвідмовності і ремонтопридатності по безперервним функціям встановлюються наступні показники:

а) середнє напрацювання системи на відмову у виконанні *i*-тої функції (відповідні показники стандарту IEC 61508 – MTTF або MTBF);

б) ймовірність безвідмовного виконання системою *i*-тої функції протягом заданого часу (1 – PFD).

Допускається використовувати такі показники:

а) середнє напрацювання системи до відмови у виконанні *i*-тої функції (MTTP);

б) інтенсивність відмов системи у виконанні *i*-тої функції.

Для оцінки інтегрального рівня безпеки абсолютна більшість постачальників і розробників систем управління і захисту спирається на Технічний звіт безпечного технічного допуску dTR84.02 - ISA TR84.0.02 "Safety Instrumented Systems (SIS) – Safety Integrity Level (SIL) Evaluation Techniques" (Обладнані під безпеку системи – Техніка оцінки інтегрального рівня безпеки), розроблений підкомісією ISA SP84.02.

Технічний звіт рекомендує наступні методики аналізу ризиків для систем безпеки, що дозволяють отримати відповідь на основне питання, чи буде система в змозі виконати зумовлені функції, коли в цьому виникне необхідність:

- метод логічних блок-діаграм;
- аналіз дерева відмов;
- марковський аналіз.

Для кожної з перерахованих методик першим кроком є отримання вихідної інформації для розрахунку інтенсивностей відмови, визначених і заданих виробником обладнання для кожного елемента, модуля, блоку, або комплектної підсистеми.

Для методу логічних блок-діаграм наступним кроком буде об'єднання (логічне додавання і множення) ймовірностей відмов окремих компонентів по кожній функції безпеки (управління/захисту).

Для всіх функцій і задач АСКТП визначаються критерії відмов і необхідні показники надійності. Далі будуються надійнісно-функціональні схеми (НФС) задач і функцій. Елементами НФС є технічні засоби. Елементи з'єднуються послідовно, якщо відмова кожного з них веде до відмови задачі. Елементи з'єднуються паралельно, якщо невиконання задачі має місце тільки тоді, коли відмовлять усі елементи.

Для НФС, що являють собою послідовні структури, оцінка імовірності безвідмовної праці проводиться за формулами:

$$\lambda_i = \lambda_{i1} + \lambda_{i2} + \ldots + \lambda_{in}; \tag{3.8}$$

$$P_i(t) = \prod_{j=1}^{n} P_{ij}(t), \tag{3.9}$$

де λ_{ij} та P_{ij} – інтенсивність відмов та імовірність безвідмовної праці j-го елемента при реалізації i-тої задачі (або функції);

n – кількість елементів, що беруть участь у реалізації задачі (функції).

Імовірність безвідмовної роботи паралельних структур за наявністю резервування розраховується за формулами:

$$\lambda_i = \lambda_{i1} + \lambda_{i2} + \ldots \lambda_{in}; \tag{3.10}$$

$$P_i(t) = 1 - \left[1 - \prod_{i=1}^{n} P_i(t)\right]^m, \tag{3.11}$$

де $P_i(t)$ – імовірність безвідмовної роботи елементів у групі, яка складається з однотипних елементів;

m – кількість паралельних гілок.

Для однотипних відновлюваних елементів

$$\lambda_i = 2 \cdot \lambda_{ij}^m \cdot \mathrm{MTTR}. \tag{3.12}$$

Часто систему керування вважають працездатною і при відмові частини технічних засобів автоматизації. Наприклад, оцінюючи надійність задачі «Введення аналогових сигналів», за критерій відмови приймають вихід за апаратні уставки більше як заданого числа сигналів m. В цьому випадку імовірність безвідмовної роботи можна визначити за теоремою про повторення

дослідів. Нехай подія A – це вихід за уставку одного з сигналів. Для сукупності таких незалежних подій:

$$P_{m,n} = P_1 P_2 \ldots P_m\, q_{m+1} \ldots q + \ldots + P_1\, q_2\, P_3 \ldots q_{n-1}\, P_n + \ldots + \\ + q_1\, q_2 \ldots q_{n-m}\, P_{n-m+1} \ldots P_m\,, \qquad (3.13)$$

де $P_{m,n}$ – імовірність появи події A m разів у n дослідах;

m – кількість одночасно з'явившихся відмов;

n – загальна кількість дослідів (сигналів);

P_i – імовірність появи події A в і-ом досліді;

$q_i = 1 - P_i$ – імовірність непояви події A.

Знаючи імовірність безвідмовної роботи $P_i(t)$, розраховують середній час безвідмовної роботи задачі:

$$T_{cp} = \frac{-t}{\ln P(t)}. \qquad (3.14)$$

На основі розрахованих значень характеристик надійності задач визначаються характеристики надійності функцій. Їх значення порівнюються з тими, що задані технічним завданням на розробку АСК ТП. Якщо надійність не задовольняє вимогам технічного завдання, необхідно застосувати резервування технічних засобів.

3.4.2 Приклад розрахунку надійності підсистеми ПАЗ

3.4.2.1 Вибір показників надійності і методики розрахунку

Вибираємо необхідні показники надійності функцій і задач ПАЗ. Критерії відмов та необхідні показники надійності функцій ПАЗ приведені в таблиці 3.8.

Таблиця 3.8 – Перелік критеріїв відмов і необхідні показники надійності функцій ПАЗ

Функція	Критерії відмов	Середнє напрацювання на відмову, годин
01 Збирання та обробка інформації про стан об'єкта керування	Відмова розв'язання будь-якої зі задач функції	4 000
02 Аналіз стану технологічного процесу	Те ж саме	4000
03 Зберігання та резервування даних	Те ж саме	4000
04 Обмін інформацією з РСУ	Те ж саме	4000
05 Оперативне відображення, облік (документування) ходу технологічного процесу та стану обладнання	Те ж саме	4000

Продовження табл. 3.8

Функція	Критерії відмов	Середнє напрацювання на відмову, годин
06 Діагностика комплекса технічних засобів та дій персоналу	Відмова розв'язання будь-якої зі задач функції	4000
07 Відпрацювання аварійних ситуацій	Те ж саме	10000
08 Диспетчеризація розв'язування задач	Те ж саме	10000

Виконання функцій забезпечується розв'язуванням відповідних задач. Необхідні показники надійності задач по кожній з функцій подаються, як показано в табл. 3.9.

Таблиця 3.9 – Перелік задач, критерії відмов та характеристики надійності для функції 01 ПАЗ

Задача	Вид відмови	Критерий відмови	Середнє напрацювання на відмову, годин
0101 Введення аналогових сигналів	Раптова, незалежна	Вихід за аппаратні уставки більш як 10 сигналів	5000
0102 Введення дискретних сигналів	Те ж саме	Відсутність реакції на вхідні сигнали більш як по 10 каналах	5000
0103 Нормализація і фільтрація аналогових сигналів	Те ж саме	Те ж саме	5000
0104 Подавлення брязкотіння контактів	Те ж саме	Відмова розв'язання задачі	5000
0105 Контроль виходу аналогових сигналів за апаратні уставки	Те ж саме	Те ж саме	5000
0106 Контроль аналогових сигналів на припустимий тренд	Те ж саме	Те ж саме	5000

Вибираємо необхідні показники надійності для елементів комплексу технічних засобів, що реалізують задачі та функції ПАЗ. Для відновлювальних технічних засобів як числова характеристика надійності використовуються інтенсивність відмов λ, середній час між двома послідовними відмовами MTBF

або імовірність *P* безвідмовної роботи засобу за 1000 годин. Характеристики надійності деяких технічних засобів ПАЗ приведені в Додатку Б

3.4.2.2 Розрахунок характеристик надійності технічних засобів ПАЗ

Будуємо НФС технічних засобів ПАЗ з архітектурою 2оо3 (рис. 3.10).

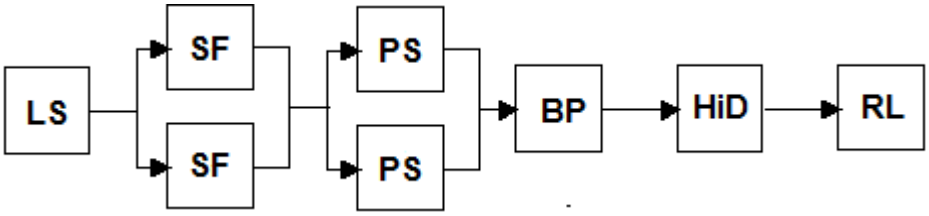

Рис. 3.10 – НФС технічних засобів ПАЗ з архітектурою 2оо3

Позначення позицій на НФС:

LS - контролер 2оо3 + модулі вводу-виводу;

SF - автомат живлення, 5 дубльованих пар;

PS - блок живлення бар'єрів, 3 дубльовані пари;

BP - панель для установки бар'єрів, 3 шт .;

HiD - бар'єр аналогових входів, 16 шт .;

RL - реле, 250 шт.

Інтенсивність відмов системи ПАЗ і підключених до неї пристроїв в цілому може бути знайдена за виразом:

$$\lambda_{ESD}=\lambda_{LS}+5(2\cdot\lambda_{SF}^2 MTTR)+3(2\cdot\lambda_{PS}^2\cdot MTTR)+3\lambda_{BP}+16\lambda_{HiD}+250\lambda_{RL}, \quad (3.15)$$

де λ_{ESD} - інтенсивність відмов системи ПАЗ;

λ_{LS} - інтенсивність відмов контролера;

λ_{SF} - інтенсивність відмов автомата харчування;

λ_{PS} - інтенсивність відмов блоку живлення бар'єрів;

λ_{BP} - інтенсивність відмов панелі для установки бар'єрів;

λ_{HiD} - інтенсивність відмов бар'єрів аналогових;

λ_{RL} - інтенсивність відмов реле.

На часовому відрізку без відмов і відновлення значення надійності P (t) і готовності A (t) збігаються. Готовність контролера ПАЗ і підключених пристроїв в цілому може бути знайдена з наступного співвідношення.

$$A_{ESD} = A_{LS}\ \ (1-(1-A_{SF})^2)^5\cdot(1-(1-A_{PS})^2)^3\ \ (A_{BP})^3\ \ (A_{HiD})^{16}\ \ (A_{RL})^{250}, \quad (3.16)$$

де A_{ESD} – готовність системи ПАЗ;

A_{LS} – готовність контролера;

A_{SF} – готовність автомата харчування;

A_{PS} – готовність блоку живлення бар'єрів;

A_{BP} – готовність панелі для установки бар'єрів;

A_{HiD} – готовність бар'єрів аналогових входів;

A_{RL} – готовність реле.

Результати розрахунку зведені в таблицю 3.10.

Таблиця 3.10 – Результати розрахунку надійності технічних засобів ПАЗ

Параметр		Значення
Інтенсивність відмов системи ПАЗ	λ_{ESD}	$1{,}66 \cdot 10^{-4}$
MTBF для системи ПАЗ (в годинах)	MTBF	6000
Готовність обладнання ПАЗ	A_{ESD}	0,998666

3.4.2.3 Розрахунок надійності функції ПАЗ

Критерієм відмов для функції 01 «Збирання та обробка інформації про стан об'єкта керування» (див. табл. 3.8) вважається розв'язання будь-якої із задач функції. Критерієм відмов задачі 0101 «Введення аналогових сигналів» є вихід за апаратні уставки більш як 10 сигналів. Вихід за апаратні уставки можливий при відмові відповідного датчика.

Оскільки критерієм відмови для задачі є вихід за апаратні уставки більше як 10 сигналів, то визначити імовірність безвідмовної роботи з заданою кількістю появ подій (відмов) A можна за теоремою про повторення дослідів. Ймовірність $P_{m,n}$ того, що подія A в n дослідах, в кожному з яких ймовірність її появи p (а ймовірність непояви q=1–p), з'явиться рівно m раз

$$P_{m,n} = C_n^m p^m q^{n-m}; \tag{3.17}$$

$$C_n^m = \frac{n!}{m!(n-m)!}; \tag{3.18}$$

Імовірність того, що подія A відбудеться не менше, ніж k раз, визначиться за формулою:

$$P(m \geq k) = 1 - \sum_{m=0}^{k-1} C_n^m p^m q^{n-m} \tag{3.19}$$

Для розрахунку надійності задачі 0101 задаємося кількістю вхідних аналогових сигналів n = 42. Згідно критерію відмов k =10. Розрахунок імовірності безвідмовного введення аналогових сигналів

$$P_{ан} = \sum_{m=0}^{k} C_n^m p^m q^{n-m} \cdot \tag{3.20}$$

зручно виконувати у програмі Microsoft Excel. Будується таблиця у формі, показаній на рис. 3.11.

У комірку С3 вводиться ймовірність відмови датчика аналогового сигналу, у комірку Е3 формула

=ФАКТР(С2)/(ФАКТР(D3)*ФАКТР(С2-D3)).

	B	C	D	E	F	G
2	n	42	m	C_n^m	$C_n^m p^m q^{n-m}$	P_{0101}
3	p	0,09	0	1	0,019	0,019043
4	q	0,91	1	42	0,079	0,098145
5			2	861	0,16	0,258523
6			3	11480	0,211	0,47001
7			4	111930	0,204	0,673944
8			5	850668	0,153	0,827231
9			6	5245786	0,093	0,920719
10			7	26978328	0,048	0,96827
11			8	118030185	0,021	0,988845
12			9	445891810	0,008	0,996532
13			10	1471442973	0,003	0,999041

Рис. 3.11 – Вигляд таблиці Microsoft Excel

У комірку F3 вводиться формула

=E3*C3^D3*(1-C3)^(C2-D3).

Зміст E3 і F3 розповсюджується вниз до кінця таблиці.

У комірку G3 переноситься вміст F3. У комірку G4 – формула =G3+F4, яка розповсюджується вниз до кінця таблиці. У комірці G13 одержуємо результат розрахунку $P_{ан}$=0,999.

Тепер можна розрахувати ймовірність безвідмовного виконання задачі 0101:

$$P_{0101} = P_{ан} \cdot A_{ESD} = 0{,}999 \cdot 0{,}998666 = 0{,}997667.$$

Середній час безвідмовного виконання задачі:

$$T_{ср} = \frac{-1000}{\ln P(1000)} = -\frac{-1000}{\ln 0{,}997667} = 428193 \text{ годин}.$$

Аналогічно виконується розрахунок надійності інших задач ПАЗ. НФС функцій можна розглядати як послідовне з'єднання задач, що входять в функцію.

Імовірність $P_{ПАЗ}$ безвідмовної роботи ПАЗ визначається як добуток ймовірностей безвідмовної роботи всіх функцій.

Середній час безвідмовної роботи ПАЗ :

$$T_{ср} = -\frac{-1000}{\ln P_{ПАЗ}}. \qquad (3.20)$$

Ці значення порівнюються з тим, що задано технічним завданням на розробку ПАЗ. Низькі показники надійності вимагають застосування додаткового резервування технічних засобів.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Андреев, Е.Б. Автоматизация технологических процессов добычи и подготовки нефти и газа: Учебное пособие для вузов / Е.Б. Андреев, А.И. Ключников, А.В. Кротов, В.Е. Попадько, И.Я. Шарова. – М.: ООО ≪Недра-Бизнесцентр≫, 2008. – 399 с
2. Бабіченко, А.К. Промислові засоби автоматизації. Ч. 1. Вимірювальні пристрої : навч. посібник / За заг. ред. А.К. Бабіченка. – Харків : НТУ "ХПІ", 2001. – 470 с.
3. Дранчук М.М. Проектування систем автоматизації технологічних процесів в нафтовій і в газовій промисловості : Навчальний посібник / М.М. Дранчук. - Івано-Франківськ : Факел, 2005. – 448 с.
4. Дружинин, Е.А. Проектирование автоматизированных производственных систем : учеб. пособие / Е.А. Дружинин, М.А. Латкин. – Харьков : Нац. аэрокосмический ун-т «Харьк. авиац. ин-т», 2002. – 41 с.
5. Жданкин, В.К. Некоторые вопросы обеспечения взрывоопасности оборудования / В.К.Жданкин // Современные технологи автоматизации. – 1998. – № 2. – С. 98–106.
6. Жданкин, В.К. Вид взрывозащиты «искробезопасная электрическая цепь» / В.К.Жданкин // Современные технологии автоматизации. – 1999. – № 2. – С. 72-83.
7. Жданкин, В.К. Оценка искробезопасности электрических цепей / В.К.Жданкин // Современные технологии автоматизации. – 2000. – № 3. – С. 72–80.
8. Компьютерный справочник проектировщика АСУТП [эл. ресурс] / Сост. Г.И.Манко. – Днепропетровск : УГХТУ, 2003–2012.
9. Ландрини, Г. Интегральные уровни безопасности в соответствии со стандартами МЭК 61508 и 61511 и анализ их связи с техническим обслуживанием / Глизенте Ландрини // Современные технологии автоматизации. — 2009. — № 1.– С. 72-79.
10. Ландрини, Г. Критерии выбора компонентов с уровнем SIL 3 для РСУ и систем ПАЗ в соответствии со стандартами МЭК. Часть 1 / Глизенте Ландрини // Современные технологии автоматизации. — 2009. — № 3.– С. 110–114.
11. Ландрини, Г. Критерии выбора компонентов с уровнем SIL 3 для РСУ и систем ПАЗ в соответствии со стандартами МЭК. Часть 2 / Глизенте Ландрини // Современные технологии автоматизации. — 2009. — № 4.– С. 86–88.
12. Методичні вказівки до виконання дипломного проекту (роботи) бакалавра для студентів IV–V курсів усіх форм навчання з напряму підготовки 6.050202 «Автоматизація та комп'ютерно-інтегровані технології» / Укл.: Г.І. Манко, І.Ю. Лапунов. – Дніпропетровськ: ДВНЗ УДХТУ. – 2013. – 32 с.
13. Методичні вказівки до виконання дипломних проектів за спеціальністю 7.05020201 для студентів V–VI курсів усіх форм навчання / Укл. : І.Л.

Левчук,Г.І. Манко, В. Є. Мартиненко, В.Я. Тришкін, О.Ф. Шуть. – Дніпропетровськ : ДВНЗ УДХТУ, 2012. – 50 с.
14. Методичні вказівки до виконання атестаційної роботи бакалавра за напрямом 6.051001 «Метрологія та інформаційно-вимірювальні технології» / Укл.: Г.І. Манко, В.Я. Тришкін, І.Г. Каюн, Є.В. Чернецький. – Дніпропетровськ: УДХТУ, 2010. – 30 с.
15. Нестеров, А.Л. Проектирование АСУТП. Методическое пособие. Книга 1 / А.Л.Нестеров. — СПб : Изд-во ДЕАН, 2006. – 552 с.
16. Нестеров, А.Л. Проектирование АСУТП. Методическое пособие. Книга 2 / А.Л.Нестеров. — СПб : Изд-во ДЕАН, 2006. – 944 с.
17. Справочник инженера по контрольно-измерительным приборам и автоматике / Под ред. А.В. Калиниченко. – М. : «Инфро-Инженерия», 2008. - 576 с.
18. Справочник проектировщика автоматизированных систем управления технологическими процессами / Под ред. Г.Л. Смилянского. – К. : Техніка, 1983. – 528 с.
19. Таланчук, П.М. Засоби вимірювання в автоматичних інформаційних та керуючих системах / П.М. Таланчук та ін.. – К. : Райдуга, 1994. – 372 с.
20. Федоров, Ю.Н. Основы построения АСУТП взрывоопасных производств. Т.2 "Проектирование" / Ю.Н. Федоров. - М. : СИНТЕГ, 2006. - 632 с.
21. Федоров, Ю.Н. Порядок создания, модеризации и сопровождения АСУТП – М.: Инфра-Инженерия, 2011. – 576 с.
22. Федоров, Ю.Н. Справочник инженера по АСУТП. Проектирование и разработка : учебно-методическое пособие / Ю.Н. Федоров. – М. : Инфра-Инженерия, 2008. – 928 с.

ДОДАТОК А

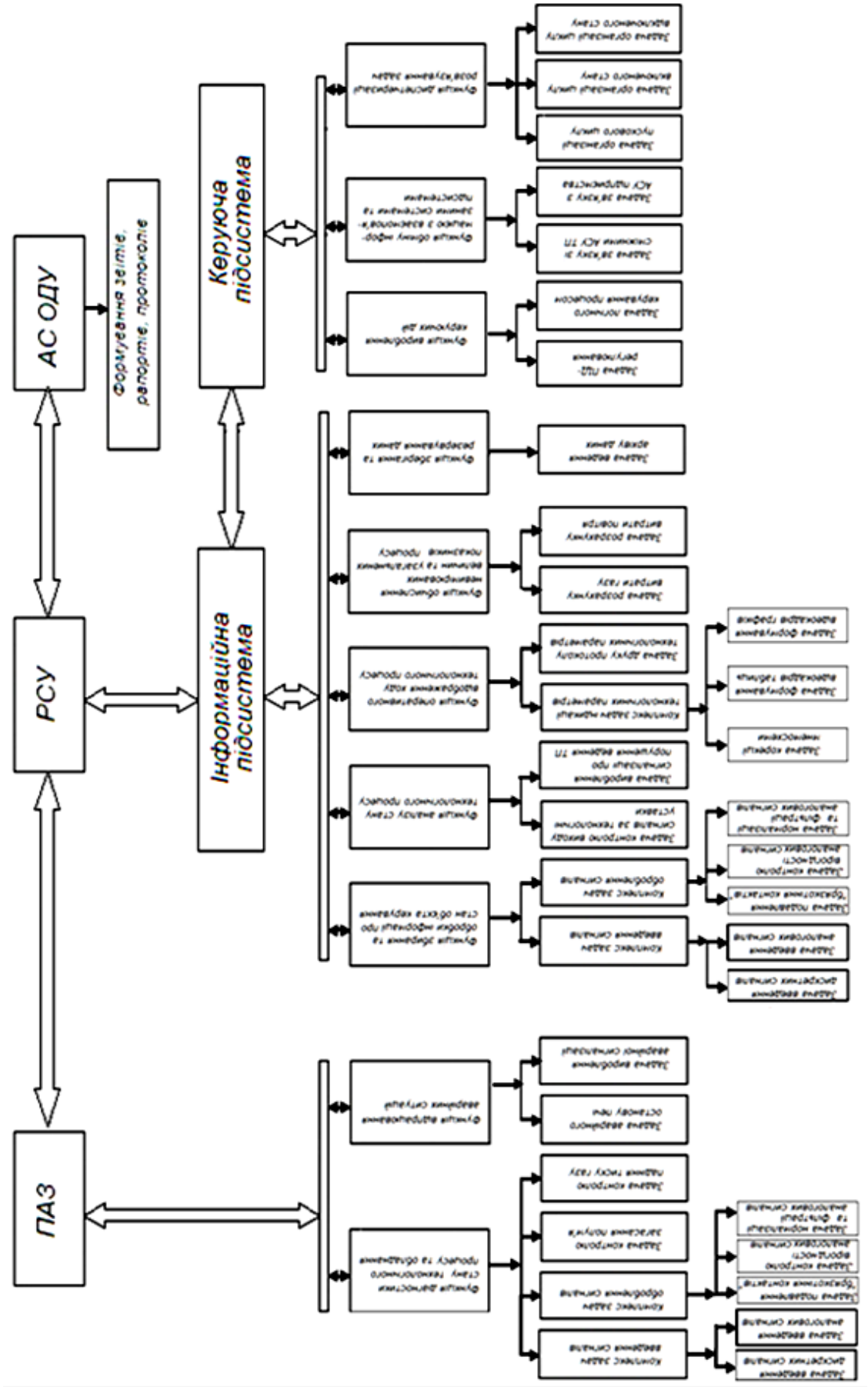

Рис. А.1 – Приклад схеми функціональної структури

ДОДАТОК Б

Таблиця Б.2 – Характеристики надійності технічних засобів АСКТП

Обладнання	Інтенсивність відмов (1091/год)	MTBF (год)
Аналоговий вхідний модуль (4–20 мА, 16-канальний, неізольований)	3 000	333 333
Аналоговий модуль введення-виведення (вход 4–20 мА, вихід 4–20 мА, 8 вхідних каналів / 8 вихідних каналів, неізольовані)	3 200	312 500
Частотний вхідний модуль (8-канальний, лічильник імпульсів, 0- 10 кГц, канали ізольовані)	6 500	153 846
Дискретний вхідний модуль (64 канали, 24 В, 25 мА, ізольований)	1 600	625 000
Дискретний вхідний модуль (64 канали, ізольований, загальний мінус на кожні 16 каналів)	2 900	344 828
Дискретний вихідний модуль (64 канали, ізольований, загальний мінус на кожні 16 каналів)	4 400	227 273
RS-422 / RS-485 Комунікаційний модуль (2 порти)	2 400	416 667
Іскробезпечний бар'єр для AI 4-20 мА, двоканальний	119	8 370 000
Іскробезпечний бар'єр для термометра опору (термопари) двоканальний	586	1 700 000
Іскробезпечний бар'єр для AT 4-20 мА, двоканальний	147	6 800 000
Панель об'єднавча для 16 активних іскробезпечних бар'єрів	500	2 000 000
Релейна панель дискретних входів (32 каналу / зовнішнє живлення ~ 220 В)	600	1 666 666
Релейна панель дискретних входів (32 каналу / зовнішнє живлення = 24 В)	600	1 666 666
Автомати живлення	300	3 333 333
Джерело живлення 24 В 12 А	7 407	135 000

Продовження табл. Б.1

Обладнання	Інтенсивність відмов (1091/год)	MTBF (год)
Реле (пускач)	400	2 500 000
Пристрій автоматичного вибору резерву	1 000	1 000 000
Джерело безперебійного живлення	237	4211 412
Трансформатор	11 415	87 600

Примітка. В інтенсивності відмов модулів враховані відмови, пов'язані з відмовами з'єднувачів.