ПОЛТАВСЬКИЙ ДЕРЖАВНИЙ АГРАРНИЙ УНІВЕРСИТЕТ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЕКОНОМІКИ, УПРАВЛІННЯ, ПРАВА ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ

Освітньо-професійна програма
Інформаційні управляючі системи та технології
Спеціальність 126 Інформаційні системи та технології
Ступінь вищої освіти Магістр

ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ

Завідувач кафедри

_____Юрій УТКІН

«15» грудня 2022 року

КВАЛІФІКАЦІЙНА РОБОТА

на тему: **«Моделювання оцінювання готовності та функційної безпечності електричних, електронних, програмованих електронних систем»**

виконав здобувач вищої освіти денної форми навчання

Авдошин Юрій Андрійович

Керівник кваліфікаційної роботи,
д. т. н., доцент Олег ОДАРУЩЕНКО

Полтава – 2022 року

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

АК	апаратні компоненти
АЗ ПЗ	аварійний та попереджувальний захист
АСУ ТП	автоматизована система управління технологічними процесами
ASIC	Application-Specific Integrated Circuit
ПК	програмні компоненти
ПЗ	програмне забезпечення
НіФБ	надійність і функційна безпечність
БФМ	багатофрагментна марківська модель
ОФМ	однофрагментна марківська модель
СДР/ЖСДР	система диференційних рівнянь/жорстка система диференційних рівнянь
ССН	структурна схема надійності
ТККВ	технічний комплекс критичного використання
SW	Software
SIL	Safety Integrity Level
ПЛК	програмовний логічний контролер
ПТК	програмно-технічний комплекс
ПЛІС	програмовна логічна інтегральна схема
PFH	Probability of failure per hour
PFD_{avg}	Probability of failure on demand (average)
ІКС	інформаційно-керуюча система
I&C	Instrumentation and Control System
ДППЗ	проєктні дефекти програмних засобів
ДПА	проєктні дефекти апаратних засобів
ФБ	функційна безпечність
ФГ	функція готовності

ВСТУП

Актуальність теми дослідження. В наш час широко використовуються складні системи та пристрої, від коректної роботи яких, залежить життя та благополуччя багатьох людей. Кожна людина в процесі своєї життєдіяльності змушена використовувати ту чи іншу систему електронно-обчислювальної техніки. Одним із різновидів даних систем є такі, в яких «серцем» є програмована користувачем вентильна матриця (ПКВМ) [49, 50].

Системи, які побудовані на даних пристроях, мають неабияке значення. Вони використовуються в системах, які здатні обслуговувати величезну кількість людей.

Вони використовуються в системах, які здатні обслуговувати величезну кількість людей. Зокрема це галузі:

- енергетична (АЕС, ТЕС, ГЕС);
- газовидобувна;
- хімічна;
- нафтопереробна;
- газопереробна;
- транспортна.

Але природно, що від систем таких масштабів ми маємо очікувати наднадійної роботи. Сучасні технологи безперервно вдосконалюються, щоб створювати системи, які були б високонадійними і постійно готовими виконувати покладені на них функції, а також, щоб вони були зручні в обслуговуванні. Отже важливим є поняття технічної готовності системи.

Поряд з ним також є досить важливим поняття функційної безпечності, яка відноситься до систем, що відповідають за функції безпеки, вихід з ладу яких створює значні ризики для людей і навколишнього середовища [9].

Існує також міжнародний стандарт МЕК 61508, який є зведенням дійсних у всьому світі нормативів функційної безпечності для електричних, електронних і програмованих електронних систем, які виконують запобіжні функції.

Для того, щоб наділити системи тим чи іншим набором якостей, які будуть прияти досягненню вищої готовності чи функційної безпечності, виконується ряд спеціальних проєктних рішень. Крім того, так як усі елементи системи - від сенсора до виконавчого механізму - повинні забезпечувати не абстрактне "математично" очікуване, а детермінований час реакції, - система повинна володіти значною апаратною і функціональною надлишковістю по усіх компонентах системи: процесори, пам'ять, шини даних, кількість каналів введення-виведення, і т. д. Даний ряд спеціальних проєктних рішень, які дозволяють наділити системи набором якостей, які збільшують її надійність і приводить до поняття архітектури системи.

Існують різні типи архітектур обчислювальних систем, наприклад 1oo1, в якій резервування повністю відсутнє, або 1oo2, коли система має подвоєну кількість обладнання. Ці архітектури лише маленька частина всіх існуючих, кожна з яких характеризується своїми числовими значеннями і аналітичними виразами готовності та функційної безпечності. Для того щоб їх оцінити існують різні процедури та підходи (наприклад FMEDA, FMECA, FTA) [53].

Отже, актуальність обраної теми є беззаперечною і полягає в необхідності дослідження готовності та функційної безпечності електричних, електронних, програмованих електронних пов’язаних з безпекою систем, та розробці програмного забезпечення для полегшення досліджень в даній галузі.

Зв’язок роботи з науковими програмами, темами. Робота відповідає дослідженням в межах науково-дослідної тематики «Теоретичні основи, методи та інформаційні технології розробки програмно-технічних комплексів критичного застосування в умовах ресурсних обмежень» (ДР№ 0112U001058).

Мета досліджень - є розробка програмного забезпечення для оцінювання функційної безпечності систем критичного застосування, які побудовані за різною архітектурою.

Завданнями кваліфікаційної роботи є:

- виконати аналіз теоретико-методологічних підходів до аналізу і оцінювання властивостей готовності і функційної безпечності систем критичного застосування;

- проаналізувати базові архітектури побудови програмно-технічних комплексів і отримати розрахункові співвідношення для оцінювання готовності та функційної безпечності;

- розробити програмне забезпечення для розрахунку готовності та функційної безпечності базових архітектур ПТК.

Об'єкт дослідження є – програмно-технічні комплекси інформаційно-керуючих систем критичного застосування, а також процеси оцінювання їх надійності та функційної безпечності.

Предмет дослідження – методи оцінювання надійності та функційної безпечності електричних, електронних, програмованих електронних систем програмно-технічних комплексів інформаційно-керуючих систем критичного застосування.

Методи досліджень – в ході досліджень було застосовано методи теорії надійності і технічної діагностики, теорії ймовірностей та марковських випадкових процесів.

Інформаційна база кваліфікаційної роботи сформована з наукових фахових статей, наукових монографій, аналітичних звітів державних та міжнародних експертних груп щодо експлуатації критичних технічних систем, виконаних науково-дослідних та дисертаційних робот заданою тематикою.

Елементи наукової новизни роботи полягають в удосконаленні розрахункових співвідношень для розрахунку показників функційної безпечності за рахунок урахування значень міжперевірочних інтервалів.

Практична значущість роботи полягає в розроблені програмної реалізації розрахункових співвідношень.

Апробація результатів дослідження відбувалася шляхом оприлюднення доповідей на міжнародній та студентській конференціях.

Публікації. За результатами проведеного дослідження опубліковані тези: «Моделювання оцінювання готовності та функційної безпечності електричних, електронних, програмовних електронних систем», матеріали щорічної студентської наукової конференції Полтавського державного аграрного університету, 10 листопада 2022 р. Полтава: ПДАУ, 2022.

Структура та обсяг роботи. Робота складається з вступу, трьох розділів, висновків, списку використаних джерел та додатків, де: додаток А – програмний код розробленого додатку. Загальний обсяг роботи становить 82 сторінки; робота містить 18 рисунків; 5 таблиць; список використаних джерел, що включає 55 найменувань.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДОЛОГІЧНИЙ ОГЛЯД ПІДХОДІВ ДО ОЦІНЮВАННЯ ГОТОВНОСТІ ТА ФУНКЦІЙНОЇ БЕЗПЕЧНОСТІ СИСТЕМ КРИТИЧНОГО ЗАСТОСУВАННЯ

1.1 Аналіз структурної організації інформаційно-управляючих систем критичного призначення

Інформаційно-управляючі системи (ІУС) – системи, призначені для отримання, збереження, оброблення, передачі, відображення й реєстрації даних про стан і функціонування систем, елементів контрольованих об'єктів, а також для ініціювання спрацьовування технологічних систем при порушенні заданих проектних меж або умов експлуатації і безпосереднього впливу на технологічне устаткування з метою змінення стану або функціонування керованого об'єкта, у тому числі спрямованого на усунення порушень [1]. Основні (інформаційні й управляючі) функції ІУС, що є важливими для безпеки, визначаються їх призначенням. Додаткові функції сприяють досягненню необхідної якості, надійності, стійкості й незалежності виконання основних функцій. Основні інформаційні й керуючі, а також додаткові функції ІУС наведено у табл. 1.1 [1, 42].

Таблиця 1.1 – Функції ІУС

Тип		Функція	Опис
1	2	3	4
Основна	Інформаційна	Моніторинг	Отримання даних для керуючих систем і оперативного персоналу у всіх робочих режимах контрольованого об'єкта, а також інформації, необхідної для управління аваріями й ліквідації їх наслідків
		Архівація	Запам'ятовування результатів моніторингу та зберігання даних про контрольовані параметри, стан технологічних систем та обладнання, порушення проектних меж та умов нормальної експлуатації тощо

Продовження таблиці 1.1

1	2	3	4
		Відображення та сигналізація	Відображення даних дають змогу оперативному персоналу своєчасно виявляти порушення нормальної або безпечної експлуатації й спостерігати за результатами роботи керуючих систем і власних дій, спрямованих на їх усунення
		Реєстрація	Автоматичне складання звітів установленої форми на паперових носіях
		Регулювання	Автоматичне підтримання значень технологічних або інших параметрів на встановленому рівні й зменшення величини та швидкості можливих відхилень параметрів, спричинених дією вихідних подій і перехідних процесів
		Дискретне керування	Забезпечення переходу технологічного обладнання з одного дискретного стану в інший (вмикання, вимикання, запуск, зупинка тощо), що здійснюється за жорстким часовим графіком або залежно від зовнішніх подій та ін.
		Обмеження	Обмеження або примусове зменшення потужності та інші запобіжні дії, що дають змогу знизити частоту спрацьовування функцій захисту при порушенні умов нормальної експлуатації
		Захист	Запобігання порушенню меж безпечної експлуатації, а в разі виникнення аварій – зменшення тяжкості їх наслідків до рівня, передбаченого проектом
		Блокування	Запобігання важким наслідкам, які можуть бути спричинені незадовільним станом технологічного обладнання, порушеннями робочого режиму, виникненням інших умов, небезпечних для роботи обладнання, помилковими діями персоналу тощо

1.2 Аналіз вимог до надійності та безпеки інформаційно-управляючих систем критичного призначення. Огляд міжнародних і національних стандартів у сфері безпеки

До надійності й функціональної безпеки ІУС критичного застосування ставляться підвищені вимоги, безпосередньо пов'язані зі сферою їх використання

(авіаційні системи, ракетно-космічна техніка, атомні електростанції (АЕС) тощо), а також виконуваними функціями (табл. 1.1). Так, ІУС АЕС, що є важливими для безпеки, виконують функції, необхідні для того, щоб запобігти переростанню аварійної ситуації в аварію, ліквідувати аварію й надати реакторній установці контрольованого стану або обмежити наслідки аварії [1].

Аналіз статистики й причин відмов обладнання АЕС України показує, що 15-29 % від загальної кількості відмов обладнання зумовлено збоями в роботі ІУС [43, 51]. Оцінка економічних наслідків порушень, спричинених неправильним функціонуванням ІУС АЕС за період 2000 – 2010 рр., наведена в роботі [44], показує, що середній час простою енергоблока при одному порушенні через неправильне функціонування ІУС становить 8,97 год, а середній недовиробіток електроенергії – $10{,}2 \cdot 10^6$ кВт/год. За різними оцінками, година простою одного енергоблока коштує 400 тис. грн. Прийнято виділяти рівні надійності (готовності) системи [45, 46], як показано в табл. 1.2, відповідно до значень середнього часу простою системи на рік і коефіцієнта готовності $A(t)$. У зв'язку з тим, що значення показника готовності для ІУС критичного призначення мають відповідати п'яти і більше «дев'яткам», для зручності можна використовувати коефіцієнт неготовності:

$$U(t) = 1 - A(t) \qquad (1.1)$$

Таблиця 1.2 – Вимоги до надійності (готовності) ІУС

Рівень надійності	$A(t)$	$T_{простоїв}$	Характеристика системи
1	0,9	876 годин	Не обслуговується, некерована (unmanaged)
2	0,99	87 годин 36 хвилин	Обслуговується, керована (managed)
3	0,999	8 годин 46 хвилин	Добре обслуговується, добре керована (well-managed)
4	0,9999	52 хвилини 33 секунди	Стійка до відмов (fault-tolerant)
5	0,99999	5 хвилин 15 секунд	З високою готовністю (high-availability)
6	0,999999	31,54 секунди	З дуже високою готовністю (very-high-availability)
7	0,9999999	3,15 секунд	З ультрависокою готовністю (ultra-availability)

У багатьох державних стандартах України наведено вимоги до виробничих ІУС [1]. Так, ДСТУ 24.701 [47] містить вимоги до надійності ІУС, згідно з якими рівень надійності системи залежить від таких факторів:

– склад і рівень надійності технічних засобів, що використовуються, їх взаємозв'язок у структурі надійності комплексу технічних засобів ІУС (КТЗ ІУС);

– склад і рівень надійності програмних засобів, що використовуються, їх зміст і взаємозв'язок у структурі програмного забезпечення (ПЗ) ІУС;

– рівень кваліфікації персоналу, організації робіт і рівень надійності дій персоналу;

– раціональність розподілу вирішуваних завдань між КТЗ ІУС, ПЗ ІУС і персоналом ІУС;

– режими, параметри й організаційні форми технічної експлуатації КТЗ ІУС;

– ступінь використання різних видів резервування (структурного, інформаційного, часового, алгоритмічного й функціонального);

– ступінь використання методів і засобів технічної діагностики;

– реальні умови функціонування ІУС.

На критичні системи в різних сферах застосування також поширюється стандарт IEC 61508 «Функціональна безпека електричних/електронних/програмованих електронних систем (Е/Е/ПЕ), пов’язаних з безпекою» [48]. Тут наведено поняття «функціональна безпека» (ФБ): «… Це частина загальної безпеки, що належить до керованого обладнання і до керуючої цим обладнанням системи, яка залежить від правильного функціонування Е/Е/ПЕ важливої для безпеки системи, інших технологічно важливих для безпеки систем та пристроїв задля зниження зовнішнього ризику» [48, с. 12]. Основні показники ФБ відповідно до IEC 61508:

– PFDavg (англ. probability of failure on demand, average) – імовірність неспрацьовування функції безпеки після подачі сигналу на її включення;

– PFH (англ. Probability of failure per hour) – очікувана частота настання аварій і, таким чином, інтенсивність запитів на виконання відповідної функції безпеки.

Згідно зі стандартом IEC 61508 оцінювання ФБ необхідно проводити для всіх частин Е/Е/ПЕ системи на всіх етапах життєвого циклу. Цей стандарт є базовим і використовується самостійно, а також є основою для розроблення галузевих стандартів. Необхідно зазначити, що в стандарті IEC 61513 «АЕС. ІУС, важливі для безпеки. Загальні вимоги до систем» [42] використовуються базові принципи стандарту IEC 61508 щодо ФБ ІУС, важливих для безпеки АЕС.

Одним із сучасних підходів до забезпечення й оцінювання ФБ ІУС є підхід, що ґрунтується на визначенні рівнів інтегрованості безпеки (Safety Integrity Level – SIL) (табл. 1.3) і який детально описано в IEC 61508. Наприклад, системи захисту АЕС, а також нафтогазових комплексів повинні відповідати рівню, для якого інтенсивність відмов ІУС у режимі постійної роботи становить не більше 10^{-7} 1/год [44].

Таблиця 1.3 – Вимоги до показників ФБ в залежності від режиму роботи

Рівень безпеки	Режим роботи з низькою частотою запитів	Режим роботи з високою частотою запитів
SIL	PFDavg	PFH
4	$\geq 10^{-5} \ldots < 10^{-4}$	$\geq 10^{-9} \ldots < 10^{-8}$
3	$\geq 10^{-4} \ldots < 10^{-3}$	$\geq 10^{-8} \ldots < 10^{-7}$
2	$\geq 10^{-3} \ldots < 10^{-2}$	$\geq 10^{-7} \ldots < 10^{-6}$
1	$\geq 10^{-2} \ldots < 10^{-1}$	$\geq 10^{-6} \ldots < 10^{-5}$

У шостій частини стандарту IEC 61508 було зазначено, що в деяких випадках показник *PFD(t)* може відповідати коефіцієнту неготовності *U(t)*: *PFD(t) = U(t)* [48].

Таким чином, високі вимоги, що ставляться до показників надійності (готовності) і ФБ сучасних ІУС, у свою чергу, обумовлюють вимоги до точності моделювання й оцінювання показників цих систем на етапах розроблення, виробництва й пропрацьовування. Виконати це завдання можливо лише за рахунок розроблення спеціального програмного забезпечення для оцінювання обраних властивостей і показників.

1.3 Аналіз методів оцінювання безпеки та надійності інформаційно-управляючих систем критичного призначення

Оцінювання показників безпеки та надійності ІУС, важливих для безпеки, є важливим етапом процесу їх розроблення й сертифікації у зв'язку із підвищеними вимогами до надійності й функціональної безпеки цих систем. Одним із ефективних шляхів оцінювання є використання методів математичного моделювання [61].

Процес оцінювання безпеки та надійності ІУС характеризується наявністю таких ризиків:

– *точності* – невідповідність фактично досягнутого значення точності результатів необхідному значенню, що призводить до необґрунтованого збільшення витрат або невиконання вимог щодо готовності;

– *стабільності* – нестабільність результатів і прийняття необґрунтованих рішень на їх основі;

– *ресурсів* – неприйнятні обсяги часового й обчислювального ресурсів [29].

Будь-якому кількісному аналізу безпеки та надійності системи (об'єкта) передує якісний аналіз, який може бути здійснений дедуктивним (зверху вниз) або індуктивним (знизу вверх) методом. На практиці частіше застосовується ітеративний підхід, коли дедуктивний та індуктивний аналізи доповнюють один одного.

Безліч методів математичного моделювання, що застосовуються для проведення аналізу безпеки та надійності ІУС, можна поділити на три категорії: аналітичні; імітаційні; гібридні [4].

У табл. 1.4 наведено класифікацію методів математичного моделювання для аналізу ІУС відповідно до існуючих стандартів.

Аналітичні методи можна умовно поділити на дві групи: комбінаторні й просторові. До найбільш відомих методів першої групи належать діагностування дерева відмов (FTA) та аналіз допомогою блок-схем надійності (RBD).

FTA є дедуктивним методом аналізу безпеки та надійності системи, із допомогою якого визначають та аналізують умови й фактори, які призводять до виникнення небажаної події або сприяють цьому, а також значно впливають на характеристики системи, безпеку, економічність та інші показники. RBD також належить до дедуктивних методів аналізу надійності системи, який дає змогу визначити шляхи сприятливого стану системи по тому, як зв'язані між собою її елементи й підсистеми.

Таблиця 1.4 – Класифікація методів математичного моделювання для аналізу безпеки та надійності ІУС

<table>
<tr><th>Метод</th><th>Підхід</th><th>Приклад</th><th colspan="4">Стандарт (-и)</th></tr>
<tr><td rowspan="5">Анатіличний (Analytical)</td><td rowspan="2">Непросторові моделі (Boolean approach, Non-state space)</td><td>Аналіз діагностування дерева відмов (Fault-tree analysis)</td><td>ДСТУ 2861-94</td><td>ГОСТ Р 27.302</td><td>IEC 61025</td><td>IEC 61508</td></tr>
<tr><td>Аналіз за допомогою блок-схем надійності (reliability-block diagram)</td><td>ДСТУ 2861-94</td><td>ГОСТ 5190.5</td><td>IEC 61078</td><td>IEC 61508</td></tr>
<tr><td rowspan="3">Просторові моделі (state/transition approach, state space)</td><td>Марковський аналіз (Markovian approach)</td><td>ДСТУ 2861-94</td><td>ГОСТ 5190.5</td><td>IEC 61165</td><td>IEC 61508</td></tr>
<tr><td colspan="2">Аналіз за допомогою стохастичних мереж Петрі (petri nets, place-transition nets)</td><td>ГОСТ 5190.5</td><td>ГОСТ 50779.10</td><td colspan="2">IEC 61508</td></tr>
<tr><td colspan="3">Імітаційний (discrete-event simulation)</td><td>ДСТУ 2861-94</td><td>ГОСТ 50779.10</td><td colspan="2">IEC 61508</td></tr>
<tr><td colspan="3">Гібридний (Hybrid)</td><td colspan="4">IEC 61508</td></tr>
</table>

Одними з найбільш поширених просторових методів аналізу є марковський аналіз, а також аналіз з допомогою стохастичних мереж Петрі.

Марковський аналіз – це переважно індуктивний метод аналізу, який ґрунтується на теорії марковських процесів (МП) і використовується для оцінювання функціонально складних систем і стратегій технічного

обслуговування й ремонту. Аналіз із допомогою стохастичних мереж Петрі є індуктивним методом, що дає змогу гнучко моделювати динамічні дискретні системи, зберігаючи в допустимих розмірах простір станів моделі й застосовуючи метод Монте-Карло для розрахунку необхідних значень.

Базовою перевагою просторових моделей над комбінаторними є їхня гнучкість у поданні таких важливих особливостей об'єкта, як використання «гарячого» резерву, неповне покриття виявленого дефекту, різні типи відмов, особливості стратегій технічного обслуговування тощо [36].

Імітаційне моделювання – метод, що дає змогу аналізувати безпеку та надійність системи шляхом побудови моделі, максимально близької до оригіналу, яка описує процеси так, як вони проходили б насправді. Перевагою цього підходу є високий ступінь деталізації поведінки системи, і, як наслідок, тривалий час розрахунку необхідних показників, який при реалізації високонавантаженого проекту може становити декілька днів [62]. Необхідно зазначити, що на дослідження аналітичних моделей витрачається значно менше часу порівняно з імітаційними моделями, однак застосування аналітичних моделей, у свою чергу, обмежується складністю систем.

Гібридне моделювання є методом, що дає змогу «ієрархічно» комбінувати непросторові моделі з просторовими, або аналітичні підходи з імітаційними і таким чином використовувати переваги обох підходів [48]. Необхідно зазначити, що на цей час немає стандартизованих вимог до застосування гібридного моделювання.

Із наведених методів моделювання для оцінювання безпеки та надійності ІУС зі складною апаратно-логічною структурою з урахуванням відмов і відновлень АЗ і ПЗ, а також оцінювання показника ФБ *PFD(t)* застосовується марковський аналіз [4, 5, 33, 63]. Відповідно до шостої частини стандарту IEC 61508 саме базова властивість МП є допоміжною під час розрахунку *PFD(t)* і *PFH* [48]. Однак припущення, що зумовлюють застосування теорії МП, можуть не відповідати реальному процесу функціонування ІУС. Це потребує додаткових заходів у процесі обґрунтування апарату досліджень.

Висновки до розділу 1

Виконано аналіз нормативної бази, принципів структурної організації та функціонування програмно-апаратних засобів систем обраного для досліджень класу, а саме складних технічних комплексів критичного застосування. Проаналізовано вимоги до надійності та функційної безпечності для систем означеного класу. В процесі аналізу встановлено, що підвищення вимог до показників надійності та функційної безпечності в свою чергу обумовлює підвищення вимог до оцінювання точності їх оцінювання на етапах проєктування, виробництва та приробки ІУС. Поставлено завдання на подальші дослідження.

РОЗДІЛ 2
АНАЛІЗ АРХІТЕКТУРНИХ РІШЕНЬ СУЧАСНИХ ПРОГРАМНО-ТЕХНІЧНИХ КОМПЛЕКСІВ ПОБУДОВАНИХ НА БАЗІ ПРОГРАМОВАНИХ ЛОГІЧНИХ КОНТРОЛЕРІВ

2.1 Інформаційно-управляючі системи

Інформаційно-управляюча система (ІКС) – цифрова система контролю або управління деяким реальним об'єктом. Універсальними обчислювальними системами вирішуються завдання, не пов'язані з необхідністю ухвалення рішення в реальному часі. Усі інші завдання потрапляють в область ІКС, які, за умовою їх застосування на об’єктах критичної інфраструктури, відносяться до систем критичного застосування (СКЗ). Хоча розподіл завдань достатній умовно, ІУС, які вирішують різні завдання, мають чітко виражену специфіку.

Узагальнена структура ІКС АЕС наведена на рис.2.1.

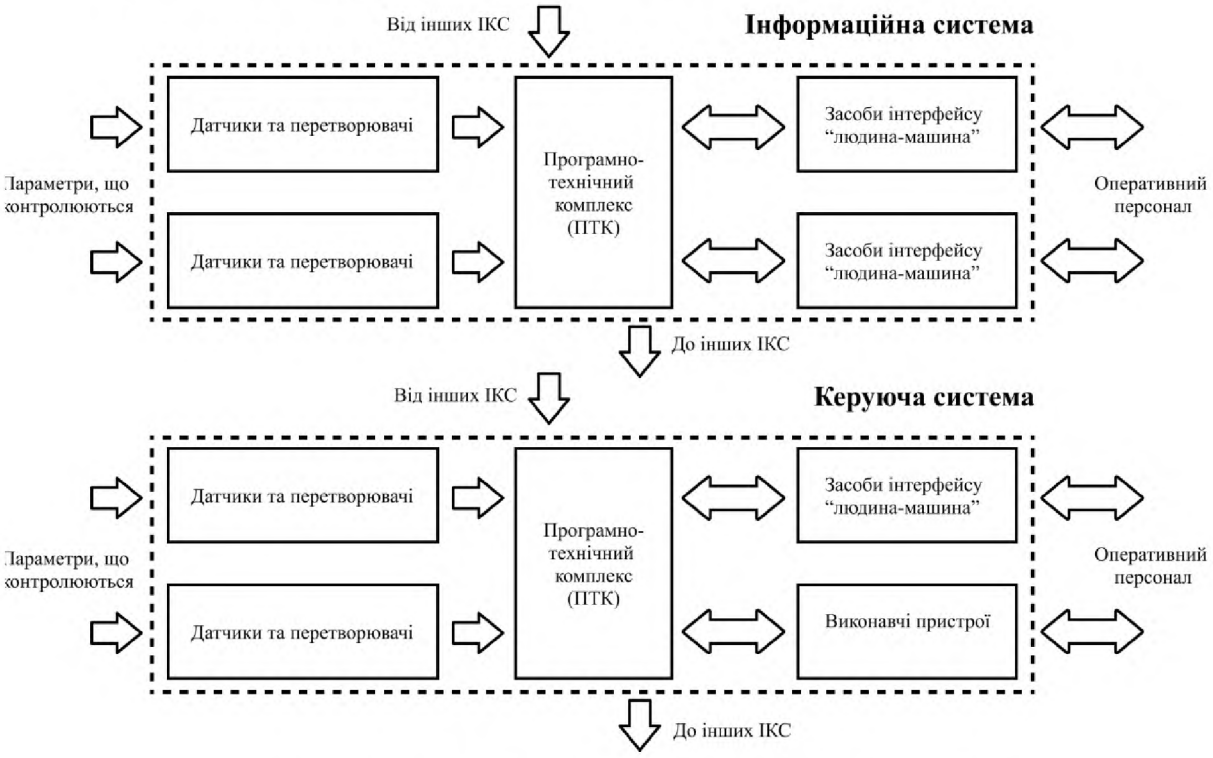


Рисунок 2.1 – Узагальнена структура ІКС АЕС

Особливості ІКС КЗ [4-22]:

- робота в реальному масштабі часу;
- специфічні вимоги по надійності і безпеки функціонування;
- експлуатаційні і інструментальні особливості;
- безперервний режим функціонування;
- оператор часто відсутній;
- нештатні ситуації повинні коректно дозволятися самій обчислювальній системі;
- специфічні вимоги до проектування і налагодження.

2.2 Поняття архітектури. Базові архітектури. Приклади

Обчислювальним ядром ІКС КЗ є програмовні логічні контролери (ПЛК). ПЛК, що входять до складу ІКС КЗ відносяться до класу безпечних. Безпечні ПЛК – це техніка спеціального призначення, яка використовується для забезпечення завдань безпеки і критичного управління в системах автоматизації. Ці контролери є центральним компонентом систем безпеки, і призначені для виявлення потенційно небезпечних технологічних ситуацій, і запобігання їх подальшого розвитку. У тому випадку, якщо подібна ситуація все-таки виникає, система безпеки програмується так, щоб автоматично перевести процес в безпечний стан.

Існують серйозні обмеження на використання ПЛК, особливо при тимчасових обмеженнях на відновлення працездатності після збою. ПЛК загального призначення, що не мають спеціального допуску на застосування в системах захисту, не можуть використовуватися в критичних по відношенню до безпеки додатках.

Розглянемо різницю між безпечним ПЛК і звичайним, і задаймося питанням: чому звичайні ПЛК не можуть використовуватися для реалізації функцій захисту і критичного по відношенню до безпеки управління. Доктор William M. Goble, лідер незалежної групи експертів Exida, чий авторитет котирується в професійному світі не нижче TUV, в статті "Conventional PLC vs.

Safety PLC", Exida, 2000, вказує на принципову різницю між звичайними і безпечними ПЛК [48].

Безпечні програмовані логічні контролери спеціально спроєктовані для досягнення двох найважливіших цілей:

- забезпечення безвідмовності за рахунок достатнього рівня резервування і, якщо відмови все ж не вдається уникнути;
- відмова повинна позначатися на процесі тільки передбачуваним, безпечним чином.

Для того, щоб наділити системи цим набором якостей, робиться ряд спеціальних проєктних рішень. Безпечні ПЛК мають витончену внутрісистемну апаратну і програмну діагностику, яка дозволяє програмно-технічному комплексу з великою мірою достовірності визначати власну нештатну роботу:

- безпечні ПЛК мають спеціальні засоби для перевірки правильності і надійності програмного забезпечення;
- безпечні ПЛК за визначенням використовують резервування, яке дозволяє підтримувати безпеку технологічного процесу навіть при відмові частини устаткування;
- безпечні ПЛК мають додаткові кошти захисту операцій читання і запису по каналах зв'язку. Проте доктор William M. Goble не згадує про найважливішу якість систем безпеки, ядро яких складають безпечні ПЛК :

Системи, призначені для виконання завдань безпеки, – це детерміновані системи, тобто такі системи, які повинні забезпечувати реакцію на подію впродовж відомого зумовленого інтервалу часу за будь-яких обставин.

Усі елементи системи – від сенсора до виконавчого механізму – повинні забезпечувати не абстрактне "математично" очікуване, а точний відомий час реакції. Сказане означає, що детермінована система повинна володіти значною апаратною і функціональною надлишковістю по усіх компонентах системи: процесори, пам'ять, шини даних і т. д. Промислові мережі також повинні підкорятися цим вимогам:

Характеристикою промислової мережі має бути гарантований час реакції на подію, а не середня швидкість передачі.

Системи безпеки за своєю природою є пасивними. Тому в режимі on-line виявити усі види відмов за допомогою однієї внутрішньо системної діагностики неможливо. Небезпечна відмова може існувати абсолютно невиявленою до тих пір, поки система неактивна. Система безпеки може відмовити одним з двох способів.

По-перше, вона може викликати або ініціювати помилкову, невмотивовану зупинку, і зупинити виробництво, тоді як фактично нічого небезпечного не сталося. Якщо вихідні ланцюги спроектовані таким чином, що в нормальних робочих умовах реле знаходяться під напругою і контакти замкнуті, то у разі відмови системи захисту електроживлення з контактів знімається, і вони розмикаються, викликаючи зупинку робочого процесу. Іноді подібну ситуацію називають "безпечною" відмовою [33].

По-друге, система захисту може відмовити прямо протилежним чином, тобто НЕ виконати функцію захисту, тоді як це дійсно потрібно з боку процесу. Прикладом подібної ситуації являються реле з контактами, що залипнули, які не можуть розімкнутися для правильного спрацьовування блокування, або виконавчий механізм відсікача, що заклинив. Подібні відмови називають небезпечними відмовами.

Отже, все вищесказане приводить до поняття архітектури.

Архітектура (Architecture) – специфічна конфігурація елементів устаткування і програмного забезпечення системи.

В наш час існують різноманітні типи архітектур, кожна з яких має свої особливості. Далі розглянемо приклади архітектур, які вважаються базовими.

2.2.1 Архітектура lool

Особливістю архітектури є наступне: резервування відсутнє, тому система lool (рис. 2.2) має властиву їй проблему загального порядку, якщо який-небудь з одиничних елементів в ланцюзі відмовляє, то і уся система перестає працювати.

Живлення з реле знімається, викликаючи розмикання контактів, і відбувається жорсткий, програмно- неконтрольований, фізичний ("безпечний") останов [33].

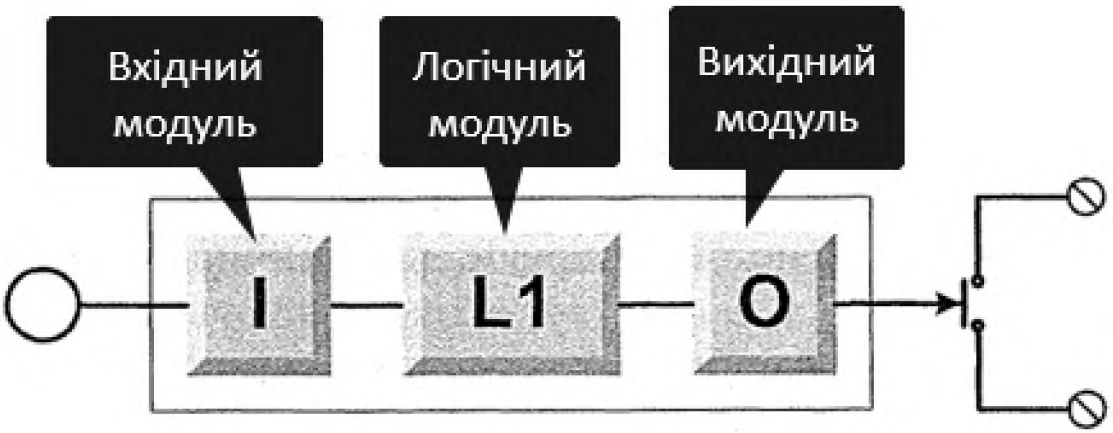


Рисунок 2.2 – Структурна схема архітектури ПЛК lool

Перш ніж розглянути різницю між показниками надійності і безпеки одноканальної системи і системами більш високого порядку, введемо два визначення:

1. Якщо вхідний сигнал не піддається ніякому аналізу, то будь-який брязкіт контакту призводить до помилкового сигналу на спрацьовування блокування. Позначимо ймовірність помилкового спрацьовування для одноканальної системи протягом 1 року як p_s: $p_s^{1oo1} = p_s$.

2. Якщо вихідні контакти залипнули, виникає небезпечна відмова, яку можна виявити тільки після деблокування і наступного тестування. Або, що найнеприємніше, після того, як блокування в потрібний момент не спрацювало. Позначимо ймовірність небезпечної відмови протягом одного року як p_D: $p_D^{1oo1} = p_D$.

2.2.2 Архітектура loo2

Дана конфігурація системи (рис. 2.3) означає, що помилковий останов станеться у тому випадку, якщо контакти будь-якого з двох послідовних реле розімкнутися. Оскільки в порівнянні з системою lool ця система має подвоєну

кількість устаткування, ймовірність помилкового спрацьовування подвоюється, і складає $p_s^{1oo2} = 2 \cdot p_s$.

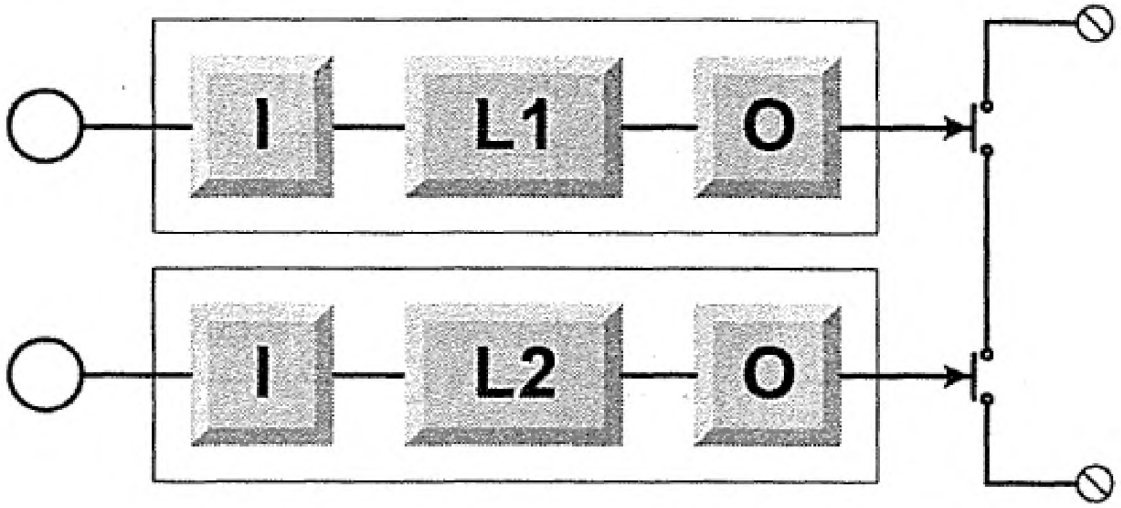


Рисунок 2.3 – Структурна схема архітектури 1oo2

Небезпечна відмова станеться тільки у тому випадку, якщо обидва канали відмовлять одночасно. Для незалежних подій ймовірність відмови обох каналів одночасно визначатиметься як квадрат вірогідності небезпечної відмови одноканальної системи : $p_D^{1oo2} = p_D^2$

Оскільки ця ймовірність досить мала, система 1oo2 має високу міру безпеки. Проте частота помилкових спрацьовувань в порівнянні з одноканальною системою подвоюється.[32].

2.2.3 Архітектура 2oo2

Система 2oo2 (рис. 2.4) має два набори контактів, встановлених паралельно. Для того, щоб стався помилковий останов, обидва канали повинні здійснити помилковий останов одночасно. Тому для незалежних подій ймовірність одночасного помилкового спрацьовування обох каналів визначається добутком ймовірностей: $p_s^{2oo2} = p_s \cdot p_s = p_s^2$

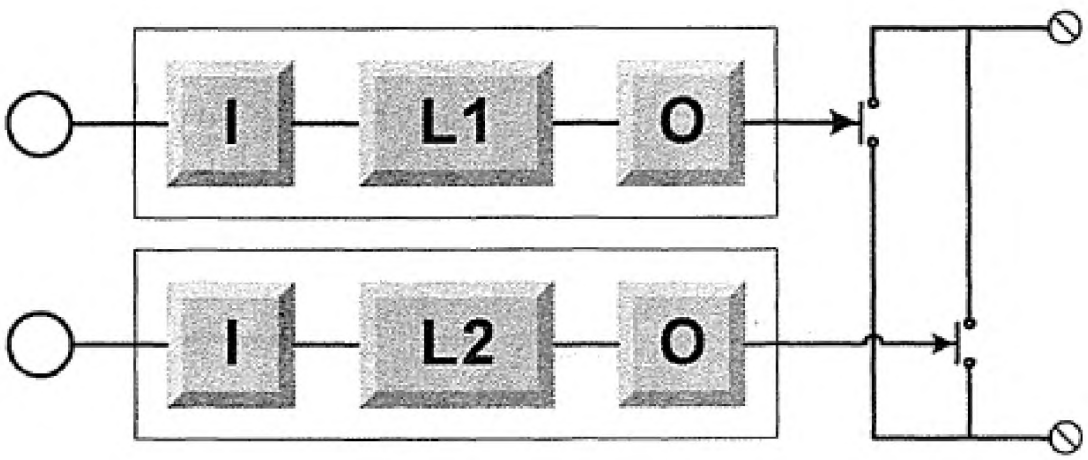


Рисунок 2.4 – Структурна схема архітектури 2oo2

Ця ймовірність надзвичайно мала, але ймовірність неспрацьовування виявляється дуже високою:

Для небезпечної відмови досить, щоб відмовив один з двох каналів. І оскільки ця система має подвоєну кількість устаткування, то ймовірність небезпечної відмови (неспрацьовування) подвоюється: $p_D^{2oo2} = 2 \cdot p_D$.

Таким чином, як це не парадоксально, але система 2oo2 поступається по безпеці одноканальній системі lool в два рази.

2.2.4 Архітектура 1oo1D

У простому варіанті в цю архітектуру додається додатковий електронний ключ, керований діагностичним ланцюгом (рис. 2.5). В якості засобу діагностики виступає звичайний сторожовий таймер (Watchdog). У тому випадку, коли діагностика виявляє небезпечну відмову, ключ може зняти живлення з виходу, перетворюючи небезпечну відмову в майже "безпечну".

Суфікс "D" в даному випадку відбиває розширені можливості самодіагностики, внесені до каналу.

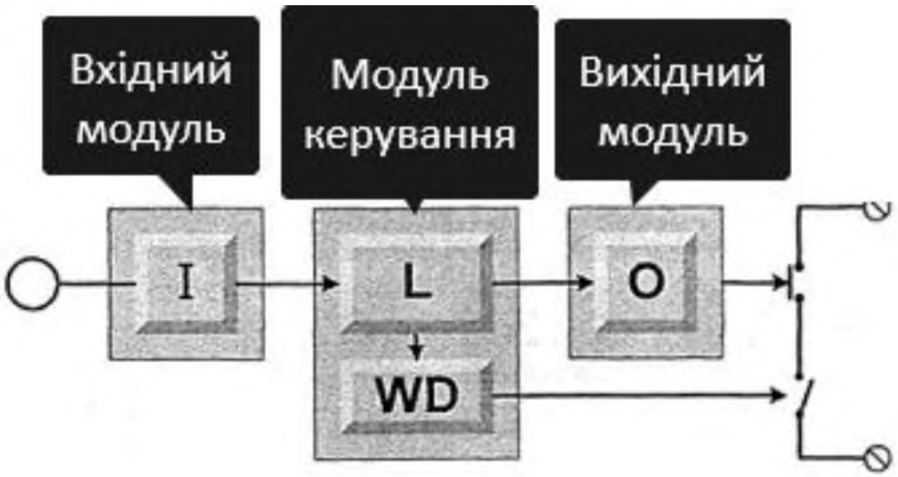


Рисунок 2.5 – Структурна схема архітектури 1oo1D

У стандартній конфігурації ця архітектура має додаткові діагностичні ланцюги і на модулях введення-виводу (рис. 2.6):

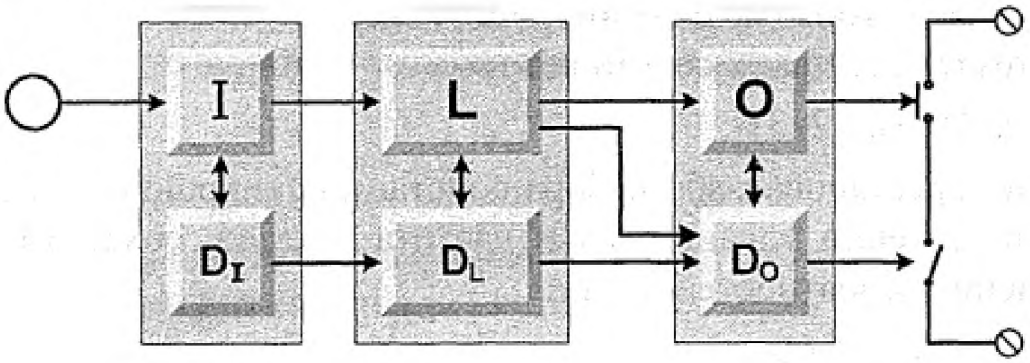


Рисунок 2.6 – Схема діагностичних ланцюгів архітектури 1oo1D у стандартній конфігурації

2.2.5 Архітектура 1oo2D

Важливо розуміти різницю між системами 1oo2 і loo2D. Щоб відразу внести визначеність, приведемо схему системи 1oo2 (рис. 2.7), яка часто позначається як система з архітектурою loo2D, проте такою не являється. У черговий раз звертається увага, що, не дивлячись на те, що в представленій схемі на кожному управляючому модулі PE, A і PE B розміщено по два процесори - PSU A1 і PSU A2, PSU B1 і PSU.B2, і, крім того, додані діагностичні ланцюги і міжпроцесорна взаємодія, Архітектура системи залишається незмінною - 1oo2 [33].

Не дивлячись на те, що система має по два процесори і сторожовий таймер на кожному з двох керівних модулів, а також може здійснювати міжпроцесорну взаємодію, – ця схема класифікується як система з архітектурою 1oo2.

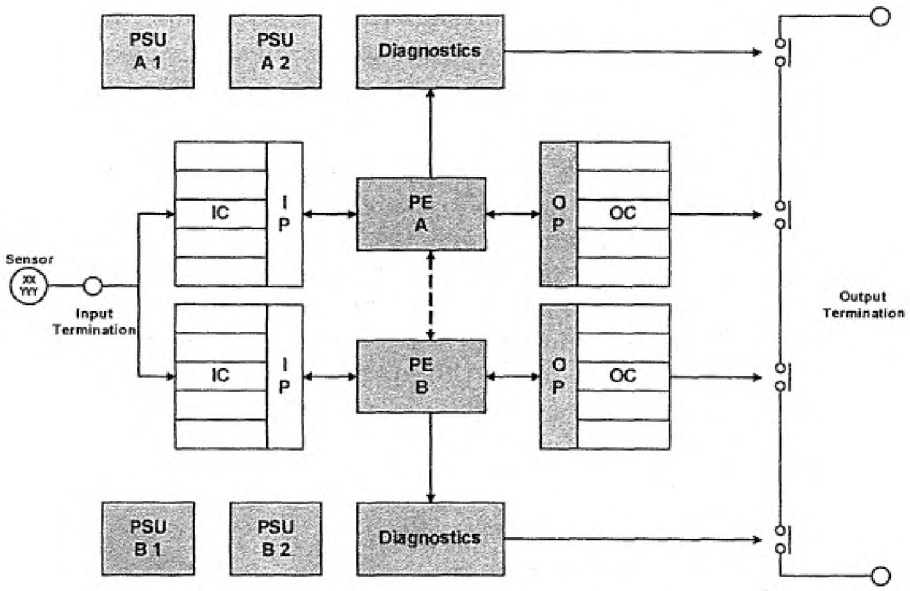


Рисунок 2.7 – Архітектура 1oo2 з додатковими процесорами і діагностичними ланцюгами

Таким чином, ні кількість процесорів на одному управляючому модулі, ні наявність діагностичних ланцюгів, ні міжпроцесорна взаємодія не є відмітною ознакою системи loo2D, і не переводить автоматично систему 1oo2 в систему loo2D: У разі відмови будь-якого з каналів живлення з вихідних реле знімається, і процес зупиняється.

Було знайдено рішення, яке дозволяє поєднувати стійкість архітектури 2oo2 по відношенню до помилкових зупинок, і стійкість архітектури 1oo2 по відношенню до небезпечних відмов (неспрацьовуванню в потрібний момент). Вирішення проблеми полягає в тій специфічній організації взаємодії управляючих модулів, вхідних, вихідних, і, головне, діагностичних ланцюгів обох каналів, яка дістала назву чотириполюсної архітектури loo2D.

2.2.6 Архітектура 2oo2D

Слід звернути увагу на ту обставину, що наявність діагностичних ланцюгів і міжпроцесорної взаємодії не перетворює архітектуру 2oo2 на архітектуру

2oo2D, оскільки ця обставина тільки підвищує рівень самодіагностики, але ніяк не міняє принцип дії системи. Саме з цієї причини архітектуру loolD часто не виділяють особливо з сімейства lool, і якщо це не викликає непорозумінь, позначають просто як систему lool. Ось що говорить про архітектуру 2oo2 стандарт IEC 61508 (Part 6, Annex B, пункт B. 2.2.3, стор. 55): "Ця архітектура складається з двох каналів, сполучених паралельно, так що обидва канали повинні виконати функцію безпеки, щоб вона змогла мати місце. Передбачається, що будь-яке діагностичне тестування тільки сповіщатиме про виявлені збої і не змінюватиме стани виходів або не змінюватиме вихідне голосування" [4].

Щоб виробити аварійний останов, обидва канали повинні дати відповідну команду. Для того, щоб стався помилковий останов, обидва канали повинні здійснити помилковий останов одночасно. Щоб сталася небезпечна відмова – неспрацьовування в потрібний момент, – досить, щоб відмовив будь-який з каналів. Відповідно, ймовірність небезпечної відмови системи 2oo2 в два рази вища, ніж у системи lool.

З цієї причини в чистому вигляді системи 2oo2 для захисту технологічних об'єктів не застосовуються.

Важливо розуміти, що кількість процесорів на одному модулі, що управляє, ніяк не може змінити архітектуру системи.

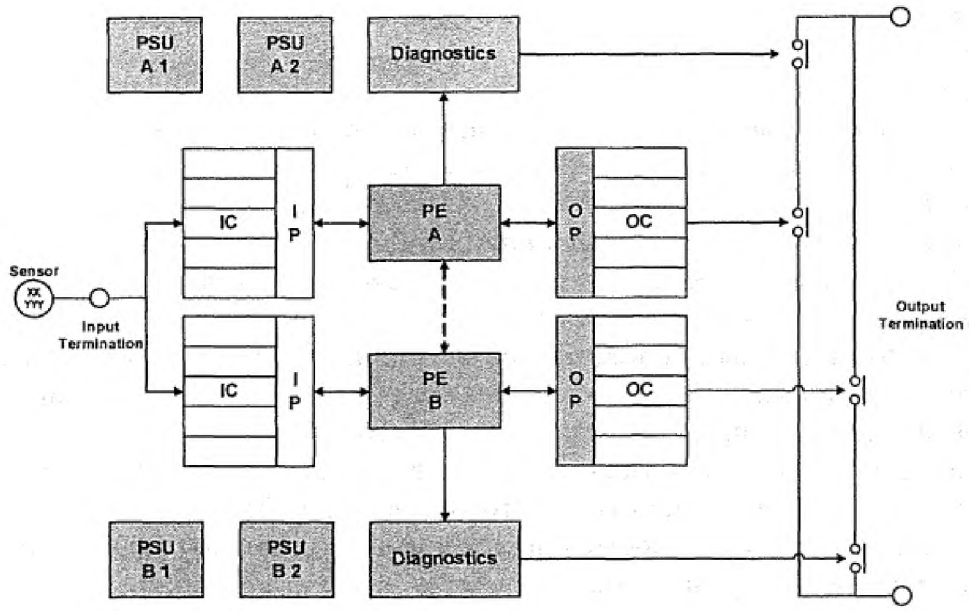


Рисунок 2.8 – Архітектура 1oo2 з додатковими процесорами і діагностичними ланцюгами

У представленій вище схемі (рис. 2.8) на кожному керуючому модулі PE, A і PE B розміщено по два процесори, - PSU A1 і PSU A2, PSU B1 і PSU B2 [5].

2.2.7 Системи сімейства QUADLOG (Siemens Energy & Automation)

Система критичного управління і забезпечення безпеки технологічних процесів QUADLOG призначена для створення додатків, що пред'являють особливо високі вимоги до надійності, відмовостійкості і безпеки: системи протиаварійного захисту (ПАЗ), системи пожежо- і газобезпеки, системи управління критичними процесами [37].

Система QUADLOG може бути безпосередньо інтегрована з розподіленою системою управління технологічним процесом у складі АСУ ТП.

На відміну від звичайних контролерів і систем управління, в архітектуру QUADLOG на усіх рівнях вбудовані апаратні і програмні механізми що забезпечують безпеку, надійність і відмовостійкість, які потрібні в найвідповідальніших застосуваннях.

Система QUADLOG неодноразово проходила незалежну міжнародну сертифікацію, що підтвердила її найвищий для програмованих електронних систем управління рівень безпеки. Апаратура QUADLOG призначена для

багаторічної безаварійної експлуатації і ефективного рішення критичних завдань управління і захисту в найтяжчих виробничих умовах.

Технологічна ефективність QUADLOG отримала широке визнання на промислових підприємствах у всьому світі. Технічні можливості QUADLOG підтверджені усіма ведучими міжнародними і багатьма національними сертифікаційними органами:

- Сертифікат TUV для систем забезпечення безпеки рівня АК 6.
- Сертифікат IEC 61508 для систем забезпечення інтегрального рівня безпеки SIL3.
- Сертифікат відповідності стандартам і вимогам CG.
- Атестат FM для використання у вибухонебезпечних зонах класу I, розділ 2.
- Атестат CSA для використання у вибухонебезпечних зонах класу I, розділ 2.
- Сертифікат ABS.
- Сертифікат UL 508.

Ці сертифікати підтверджують відповідність системи QUADLOG жорстким промисловим стандартам і вимогам різних галузей промисловості [6].

Архітектура QUADLOG loolD - RC4, SIL2 (рис. 2.9) – масштабована модульна архітектура, яка забезпечує успішне застосування QUADLOG в різних критичних застосуваннях, гарантуючи безпеку, надійність і відмовостійкість. Функціональні конфігуровані модулі QUADLOG, дозволяють скоротити витрати при впровадженні невеликих систем початкового рівня, забезпечуючи, в той же час, простоту і ефективність їх розширення в майбутньому. У архітектурі QUADLOG реалізований цілісний комплекс різноманітних заходів, що забезпечують відмовостійкість систем, що запобігають появі несправностей.

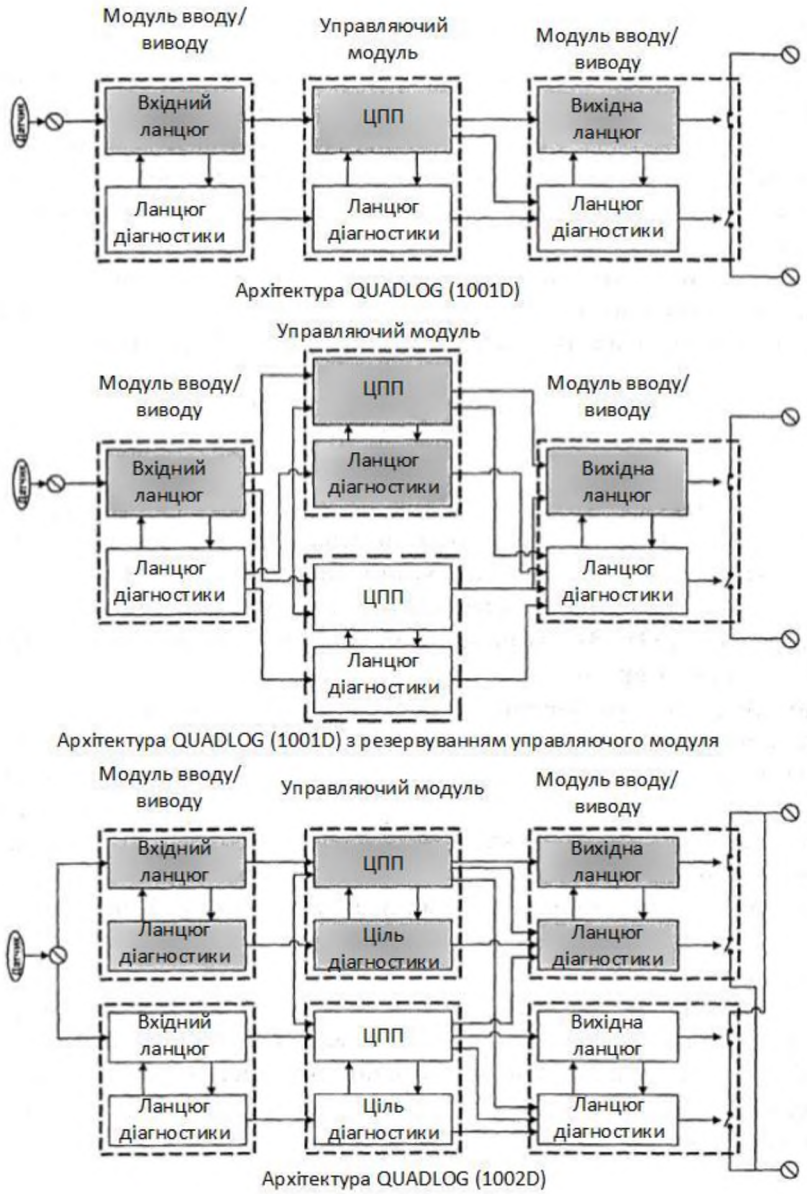


Рисунок 2. 9 – Архітектура QUADLOG loolD – RC4, SIL2

Системна архітектура QUADLOG loolD атестована на відповідність рівню безпеки SIL2 відповідно до стандарту IEC 61508, а також класу вимог RC4 по DIN. Цей варіант архітектури відповідає найбільш простій структурі системи. Високі показники безпеки забезпечуються усебічною незалежною системою діагностики, яка дозволяє переводити об'єкт в безпечний стан у разі виходу з ладу основних елементів системи. У цій архітектурі передбачені дубльовані схеми керуючих модулів, захист вихідних ланцюгів і інші механізми, що забезпечують істотно безпечніші рішення, ніж традиційна архітектура програмованих логічних контролерів і систем управління.

У вихідних каналах QUADLOG використовуються дублюючі різнотипні елементи. Нормальний вихід основного каналу управляючого контролера побудований на твердотілому напівпровідниковому ключі.

Вихідне електромагнітне реле, кероване вбудованою системою діагностики, надає додаткову можливість управління станом виходу. При виявленні небезпечної відмови у вихідному каналі реле може бути автоматично знеструмлено, що забезпечує безпечне відключення системи.

Висока відмовостійкість архітектури QUADLOG looID досягається також завдяки резервуванню таких ключових елементів системи, як джерела живлення і комунікаційні магістралі [7].

Для додаткового підвищення відмовостійкості у рамках цієї архітектури в системі можуть бути встановлені резервовані управляючі модулі (рис. 2.9, середня схема).

Архітектура QUADLOG loo2D - RC6, SIL3 (рис. 2.9) – Архітектура QUADLOG loo2D атестована на відповідність рівням безпеки SIL3 і RC6. Вона забезпечує найвищий рівень безпеки і відмовостійкості.

Архітектура loo2D включає усі основні можливості архітектури loolD. Високий рівень безпеки і відмовостійкості в архітектурі loo2D досягається за рахунок дублювання усіх модулів – і керівників, і введення-виводу. Система loo2D – повністю резервована архітектура з усебічною діагностикою і додатковим трактом безпечного відключення системи, який управляється незалежним діагностичним каналом кожного модуля. Далека не самоочевидна обставина, але в системах QUADLOG з архітектурою loo2D паралельно працюють чотири канали - два основних і два діагностичних, завдяки чому досягається найвищий для програмованих електронних систем рівень безпеки і відмовостійкості.

Уся система розділена на дві еквівалентні підсистеми, що резервують один одного. У тому випадку, коли система діагностики виявляє несправність в одній з підсистем, ця підсистема відключається, і контроль і управління підтримується іншою підсистемою.

Після того, як працездатність несправної підсистеми буде відновлена, вона включається в роботу, повністю відновлюючи подвійну схему резервування архітектури loo2D. Ця архітектура також відрізняється великою загальною стабільністю і стійкістю до зовнішніх несприятливих дій загального характеру.

Архітектура QUADLOG loo2D дозволяє монтувати підсистеми, що резервують один одного, на роздільних шасі, які можуть розміщуватися в роздільних шафах і в різних приміщеннях.

Така можливість мінімізує схильність підсистем, що резервують один одного, загальним зовнішнім діям, таким як підвищення температури або обрив лінії живлення в одній з шаф, пожежа в одному з приміщень та ін.

Повна і усебічна діагностика. Повна і усебічна система вбудованої діагностики QUADLOG випробувана і сертифікована незалежними центрами сертифікації, які підтвердили її високий рівень. Швидка, вичерпна діагностика забезпечує безпеку систем, високий коефіцієнт готовності, а також істотно полегшує і прискорює монтажні і пускові роботи. Система діагностики QUADLOG охоплює більше 99.5% можливих порушень в роботі і відмов.

Для того, щоб систему можна було використовувати в додатках, критичних з точки зору безпеки, система діагностики повинна виявляти будь-які внутрішні експлуатаційні збої, які можуть перешкодити перевести технологічну установку в безпечний стан. Діагностика повинна також гарантувати безпечну поведінку системи, і сповіщення обслуговуючого персоналу про збій, що стався. Система діагностики QUADLOG повністю відповідає цим вимогам, незалежно від типу використовуваної архітектури.

Високий коефіцієнт готовності. Висока готовність системи залежить від її здатності раннього виявлення незначних проблем, і швидкої, точної реакції на них для запобігання можливості виникнення великих проблем. QUADLOG точно визначає проблеми за частки секунди.

Діагностична інформація забезпечується тимчасовою міткою і зберігається в точці виявлення (модулі, що управляє, або модулі введення-виводу). QUADLOG здійснює діагностику не лише внутрішніх ланцюгів, але і зовнішніх

сигналів. Для цього із змінними введення-виводу зв'язується діагностичний параметр якості сигналу. Значення цього параметра характеризує достовірність даних, отримуваних системою по зовнішніх сигнальних лініях.

Діагностична інформація модуля введення-виводу передається в модуль управління і об'єднується з даними самодіагностики модуля управління. Модуль управління підтримує базу актуальної діагностичної інформації і архів діагностичних повідомлень [12].

Доступ до діагностичної інформації QUADLOG може бути наданий споживачам різного типу: операторським і інженерним станціям, контролерам, системам управління і іншим пристроям. Програмне забезпечення інтерфейсу оператора QUADLOG включає функції і утиліти опитування, сигналізації і архівації повідомлень системної діагностики.

Пристрої сторонніх виробників, такі, як системи управління технологічним процесом, можуть безперешкодно отримувати усю діагностику QUADLOG, використовуючи послідовний інтерфейс, протокол MODBUS, а також через DDE або OPC-сервер.

Прискорене введення в експлуатацію. Повна і усебічна діагностика QUADLOG дозволяє істотно прискорити установку, монтаж і введення в експлуатацію нових систем, забезпечуючи автоматичну діагностичну перевірку дефектів зовнішніх електричних з'єднань і внутрішніх програмних і апаратних збоїв системи. Модулі введення-виводу проводять перевірку правильності підключення польової шини. Надійність. Окрім безпеки і повної, усебічної самодіагностики, система QUADLOG істотно перевершує звичайні програмовані логічні контролери, розподілені системи управління по надійності і відмовостійкості. Такий високий рівень надійності і відмовостійкості QUADLOG став можливим завдяки потужним захисним механізмам, закладеним в основу архітектури і конструкції QUADLOG, що забезпечує чудову стійкість до тяжких промислових умов. Захисні механізми передбачені і вбудовані в систему QUADLOG з самого початку її розробки. Їх надійність і ефективність

була перевірена під час усебічних інтенсивних випробувань спеціальною групою інженерів Siemens Moore, а також в багатьох незалежних лабораторіях [15].

Таблиця 2. 5 – Перелік стресорів та захист від них

Стресор	Захист
1	2
Тепло	Литі алюмінієві корпуси модулів QUADLOG служать ефективним радіатором - тепловідводом для електронних компонентів. Випробування, що проводяться при температурі, що перевищує 70 °З, гарантують великий запас надійності. Модулі управління можуть працювати при температурі 100 °З і вище.
Вологість і хімічні домішки в атмосфері	Захисне покриття усіх електронних компонентів Роз'єми з позолоченими контактами, покритими антикорозійним "контактним мастилом" для забезпечення щільного газонепроникного з'єднання.
Удари і вібрація	Кріплення модулів гвинтами до жорсткого монтажного каркаса. Клемні панелі і роз'єми з гвинтовим і затискним кріпленням. Незалежні лабораторні випробування на відповідність стандартам IEC, MIL, ABS і DIN.
Скачки напруги, електростатичні розряди	Електрична ізоляція каналів введення-виводу. У канали введення-виводу і ланцюга живлення вбудовані схеми пригнічення викидів, захисту від перешкод і перенапружень. Незалежні лабораторні випробування на відповідність стандартам ANSI/ IEEE, IEC і TUV.
Електромагнітні завади	Схемні і конструктивні рішення: екрануючі вимірювальні елементи і електронні компоненти від електромагнітних завад. Незалежні лабораторні випробування на відповідність стандартам IEC і TUV по стійкості до дії електромагнітних полів і по рівню випромінюваних перешкод.
Вибухонебезпечна атмосфера	Система сертифікована відповідно до вимог стандартів CSA і FM, як іскробезпечне устаткування, дозволене для використання в небезпечних зонах Класу 1, Розділ 2.
Помилки операторів і обслуговуючого персоналу	Модулі можна виймати і вставляти в каркас, не вимикаючи напруги живлення. Місце кожного модуля в каркасі захищене механічним ключем, що не дозволяє вставити на це місце модуль іншого типу Кабельні роз'єми також мають ключ механічного захисту. Настановні перемички і DIP -перемикачі в системі не використовуються. Цифрове автоматичне самокалібрування каналів введення-виводу. Багаторівневий захист для запобігання несанкціонованому доступу і зміні програмної конфігурації і бази даних системи. Програмна конфігурація і база даних зберігаються в незалежному ОЗУ модулів. Тимчасові відмітки усіх змін конфігурації.

Інструменти розробки. На відміну від традиційних систем безпеки, що використовують окремі, незалежні програмні продукти для конфігурації

системи, роботи операторів і зберігання даних, до складу QUADLOG входить інтегрований, функціонально-повний програмний пакет засобів автоматизації технологічних процесів на базі ОС Windows NT і Windows 2000. Використання цього пакету дозволяє істотно скоротити складність і вартість розробки додатків.

Конфігураційне програмне забезпечення. Конфігурація QUADLOG для виконання функцій конкретного застосування здійснюється за допомогою конфігураційного програмного забезпечення 4-mation™.

Це програмне забезпечення засноване на відкритому міжнародному стандарті IEC 61131-3 мов конфігурації програмованих контролерів, і дозволяє використовувати будь-яку із стандартних мов програмування (функціональні блоки, релейна логіка, послідовні функціональні схеми, структурований текст) в єдиній базі даних модуля управління.

Інші можливості 4-mation:

- конфігурація здійснюється без етапу компіляції, що забезпечує миттєву перевірку правильності синтаксису, істотно скорочуючи кількість помилок і виправлень;
- механізм управління версіями і утиліта порівняння конфігурацій спрощують управління змінами при розробці додатків;
- функції захисту додатка від несанкціонованого доступу і зміни, такі як адміністративний пароль, паролі операторів, засоби управління доступом і апаратний захисний перемикач;
- примусова установка значень сигналів введення-виводу з метою тестування роботи системи і зовнішнього устаткування супроводжується установкою попереджувальних прапорів і формуванням списку таких сигналів;
- можливість редагування конфігурації і бази даних в режимі on - line істотно спрощує відладку і усунення помилок;
- для адресації зовнішніх сигналів і внутрішніх змінних конфігурації використовуються імена тегів, а не апаратні адреси, що спрощує розробку і наступне обслуговування додатків;

- конфігурація додатка зберігається в графічному виді в незалежній пам'яті QUADLOG;
- можливість конфігурації QUADLOG і РСУ APACS+ за допомогою єдиного інструменту істотно скорочує час навчання персоналу і розробки додатків;
- існує вбудований механізм оперативних діагностичних повідомлень і їх реєстрації для швидкого пошуку помилок.

Матриця безпеки (рис. 2.10) QUADLOG (Safety Matrix) – це інструментальний програмний засіб, який призначений для опису і документування стратегії безпеки у вигляді таблиці, що зв'язує події технологічного процесу, і реакцію на ці події з боку системи безпеки.

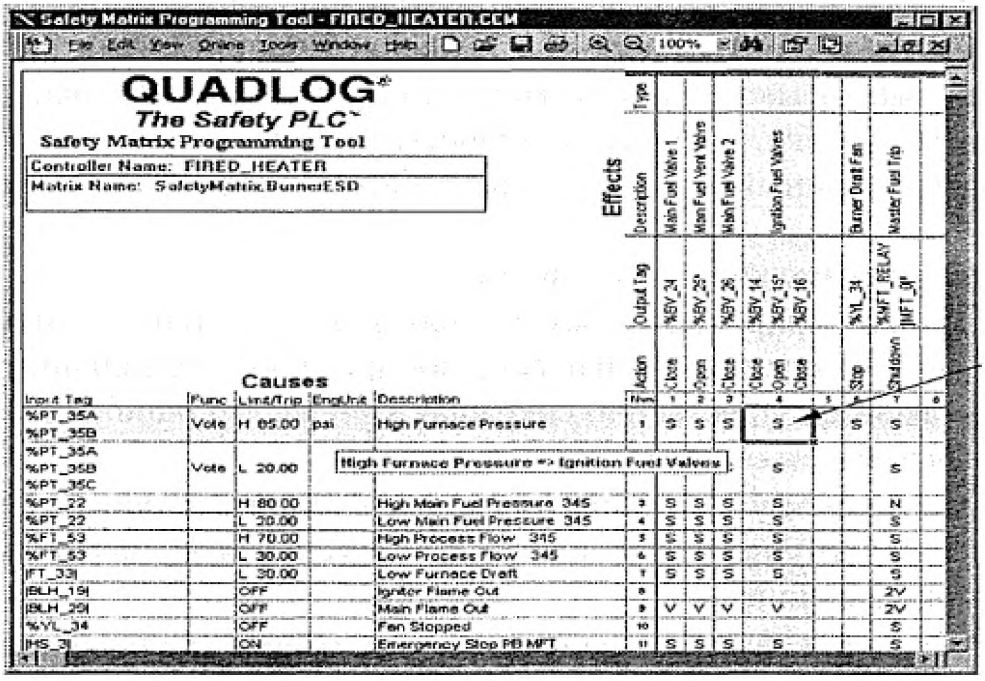


Рисунок 2.10 – Матриця безпеки

Матриця безпеки QUADLOG використовується спільно з пакетом конфігурації 4-mation і дозволяє істотно спростити конфігурацію додатків в частині опису основних функцій безпеки. Цей пакет інструментальних засобів також служить засобом перевірки правильності створеної логіки забезпечення безпеки. В період експлуатації системи безпеки матриця безпеки забезпечує

оперативний моніторинг стану об'єкту і можливість тимчасового відключення функцій безпеки на період обслуговування і тестування [19].

Матриця безпеки:

- забезпечує чітке і ясне документування додатка, полегшуючи тим самим його розробку і аналіз;
- спрощує відстеження документації;
- полегшує розробку додатка завдяки автоматичному перетворенню стратегії з матриці в конфігурацію додатку. Формує адекватне документування, вимагаючи попередньої зміни матриці при внесенні змін конфігурації.

Емулятор QUADLOG. Емулятор QUADLOG (Control Simulator) дозволяє здійснити повністю автономну розробку, моделювання і тестування конфігурації QUADLOG, а також навчання персоналу, не використовуючи устаткування QUADLOG.

Ця можливість істотно прискорює розробку і перевірку додатків, і зменшує витрати на навчання [20].

Інтерфейс оператора. Відкрита архітектура QUADLOG підтримує широкий вибір програмних засобів операторського інтерфейсу. До складу стандартного набору інструментальних засобів QUADLOG входить програмне забезпечення операторського інтерфейсу Process SuiteVision, що дозволяє легко створювати відеокадри для графічного представлення технологічного процесу, і забезпечувати їх візуалізацію в режимі реального часу. Інтерфейс Vision є повною, безпечною і масштабованою оболонкою операторського інтерфейсу, і містить потужні і різноманітні функції, які істотно прискорюють розробку додатків.

Запис послідовності подій. QUADLOG надає механізм запису послідовності змін зовнішніх сигналів (Sequence Of Events Recording - SOER) з високим тимчасовим розділенням для високоточної фіксації, наступного аналізу і діагностики подій на технологічній установці, що привели до її останову, а також подій, що сталися безпосередньо до і після останову. При реалізації цієї функції QUADLOG забезпечує безпрецедентний тимчасовий дозвіл - 3 мс. Цей

дозвіл не залежить від частоти сканування контролера. Для перегляду подій, записаних з високим розділенням, використовується спеціалізована утиліта інтегрованого інструментального пакету Process Suite® - SOER Viewer.

Пряма інтеграція з системами управління технологічним процесом. Промислові і корпоративні стандарти містять вимоги незалежності функціонування систем забезпечення безпеки (системи протиаварійного захисту, пожежовиявлення, контроль загазованості та ін.) і основної системи управління технологічним процесом.

В той же час добре інтегрована система автоматизації вимагає ефективної комунікації між усіма складовими її підсистемами. Система QUADLOG безпосередньо інтегрується в розподілені системи управління технологічними процесами APACS+ виробництва Siemens Energy & Automation і PCS7 виробництва Siemens Automation & Drives (рис. 2.11).

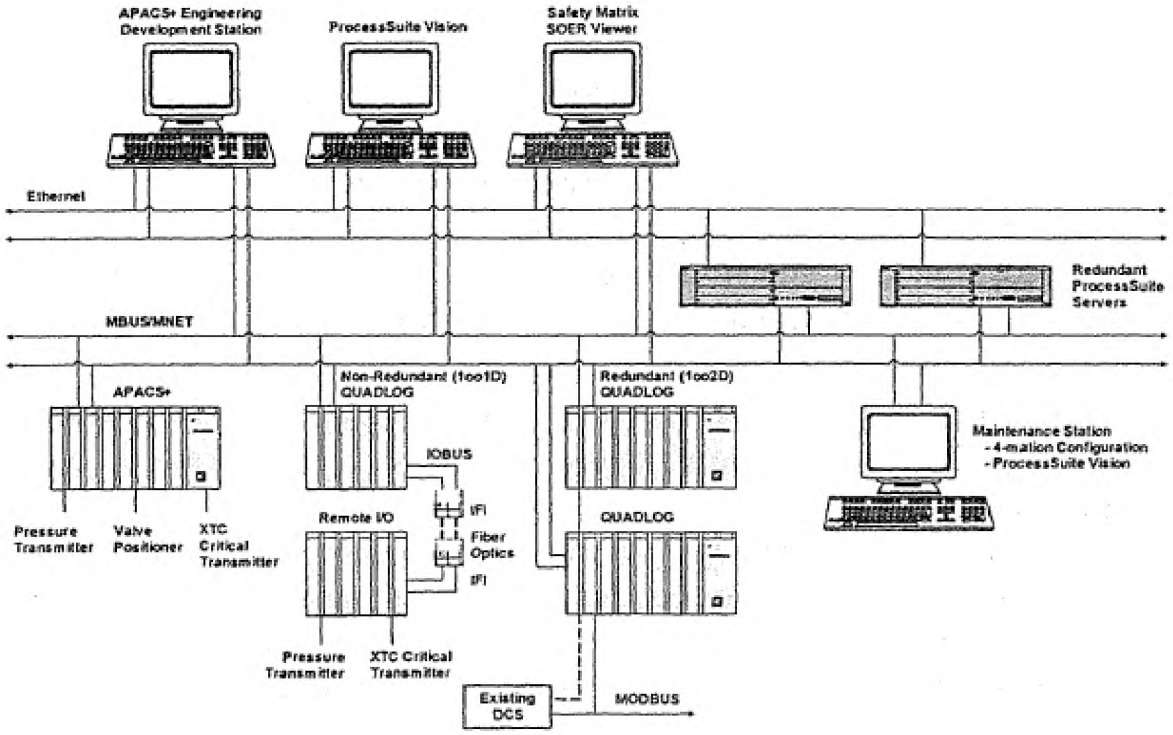


Рисунок 2.11 – Розподілена система управління APACS+.

Система забезпечення безпеки QUADLOG

Завдяки підтримці широкого спектру промислових комунікаційних стандартів (OPC, MODBUS, DDE та ін.), а також доступності прикладних

інтерфейсів програмування, QUADLOG легко інтегрується з розподіленими системами управління і промисловими контролерами інших виробників.

Вбудована потужна і гнучка система захисту комунікацій QUADLOG дозволяє гарантувати незалежність, надійність і повну безпеку його роботи з будь-яким устаткуванням, забезпечуючи виконання вимог усіх міжнародних і національних стандартів, що регламентують використання систем автоматизації і забезпечення безпеки технологічних процесів [21].

2.3 Платформа RadiCS

Інформаційно-управляюча цифрова платформа (ЦІУП) RadICS™, це продукт нового покоління, розроблений в 2010-2020 роках на основі більш ніж 20-тирічного досвіду розробки, виробництва, експлуатації і обслуговування цифрової ЦІУП платформи Radiy.

Рисунок 2.12 – Платформа RadiCS

Платформа RadICS™ є сукупністю різних типів модулів, заснованих на використанні чіпів FPGA в якості обчислювальних, оброблюючих інформацію і

системних управляючих пристроїв, для кожного з модулів, а також програмних засобів для їх програмування.

Мінімальна канальна конфігурація інформаційно управляючих систем безпеки, заснована на платформі RadICS™, складається з 1 логічного каналу, який містить 2 резервованих логічних модуля (що виконують функції логічної обробки, управління і діагностики), що покращує безпеку і надійність платформи, і до 14 інших модулів (вхідних/вихідних і оптичних зв'язків) в будь-якій їх комбінації. Основний комплект типів вхідних/вихідних модулів містить модуль аналогових входів, модуль дискретних входів, модуль дискретних виходів і модуль аналогових виходів (модуль управління силовими приводами). Також є вхідний модуль входу/виходу спеціального призначення для прийому сигналів з ультранизьким рівнем струмів – модуль виміру нейтронного потоку. Модуль оптичного зв'язку може бути використаний для розширення систем до конфігурації, що включає безліч шасі. Крім того, можливе забезпечення міжканальних зв'язків між 2, 3 або 4 каналами ІУС за допомогою оптоволоконних зв'язків безпосередньо між їх логічними модулями або утворених за допомогою модулів оптичного зв'язку.

Логічні модулі збирають вхідні дані від модулів входів відповідно до конфігурованої користувачем логіки, оновлюють величини сигналів, що управляють, для модулів виходів, збирає діагностичні дані і дані про загальний стан працездатності системи від усіх модулів входів/виходів і від другого логічного модуля, встановлених в тому ж шасі. Модулі входів/виходів забезпечують інтерфейси з іншими пристроями (наприклад, детекторами, сенсорами, приводами, пристроями сигналізації). Функціональність кожного модуля визначається логікою, запрограмованою у відповідній ПЛІС.

Кваліфікований за результатами випробувань, інформаційно управляючий канал, на основі платформи RadICS™ забезпечує захищені зовнішні інтерфейси для роботи входів/виходів, 2 незалежні блоки електроживлення, лінії зв'язку, локальні входи/виходи (від вбудованих в шасі/шафи детекторів/сенсорів/ключів або до індикаторів). Внутрішні інтерфейси шасі забезпечують зв'язки різних

модулів, які встановлені в шасі, за допомогою виділених, ізольованих, високошвидкісних комунікаційних ліній зв'язку (LVDS).

2.3.1 Аналіз структури інформаційно-управляючої системи аварійного захисту

Для забезпечення надійності функціонування ІУС застосовуються спеціальні методи структурного резервування апаратних засобів і версійного резервування програмних засобів. Спосіб резервування вибирають таким чином, щоб забезпечити для кожної функції прийнятний баланс між імовірністю відмов видів «неспрацьовування» і «помилкове спрацьовування» [1].

З метою мінімізації впливу всіх або частини помилок, які можуть виникати на стадіях створення й упровадження ІУС і бути загальною причиною одночасної відмови декількох резервних частин, застосовується принцип різноманітності. Дотримання цього принципу забезпечується, наприклад, застосуванням у складі однієї системи двох програмно-технічних комплексів (ПТК), які можуть виконувати функції безпеки незалежно й у повному обсязі, але досягають постановленої мети різними способами та (або) фізично відрізняються один від одного [1].

Проаналізуємо базові принципи побудови ПТК аварійного й запобіжного захисту (АЗЗ) виробництва НВП «Радій».

ПТК АЗЗ призначено для застосування як технічної бази при створенні нових і реконструкції існуючих систем АЗЗ реактора типу ВВЕР на енергоблоках АЕС [49]. Цей комплекс складається з двох незалежних функціонально ідентичних ПТК, кожний із яких може бути виведений із роботи для перевірки працездатності (правильності формування керуючих сигналів при імітації порушення меж та умов безпечної експлуатації).

До складу комплекту входять:

− три ідентичні шафи формування сигналів, які утворюють три незалежні канали захисту резервуючі один одного;

– кросова вихідна шафа, яка формує вихідні сигнали комплекту на основі даних, отриманих від шаф формування сигналів;

– робоча станція, яка здійснює архівування, відображення й реєстрацію даних;

– автоматизоване робоче місце оператора, призначене для відображення контрольованих параметрів, станів дискретних входів і виходів, а також причин спрацьовування захисту.

Спільним для обох комплектів є автоматизоване робоче місце технолога, на якому можуть здійснюватися перевірка працездатності ПТК АЗЗ, а також змінення й запис уставок спрацьовування захисту. Таким чином, ПТК розроблено на основі «жорсткої логіки» з реалізацією трьох рівнів формування вихідних сигналів на основі мажоритарної логіки «два з трьох». На рис. 2.13 зображено двоканальну архітектуру ПТК АЗЗ із логікою «m-n» у кожному каналі [50].

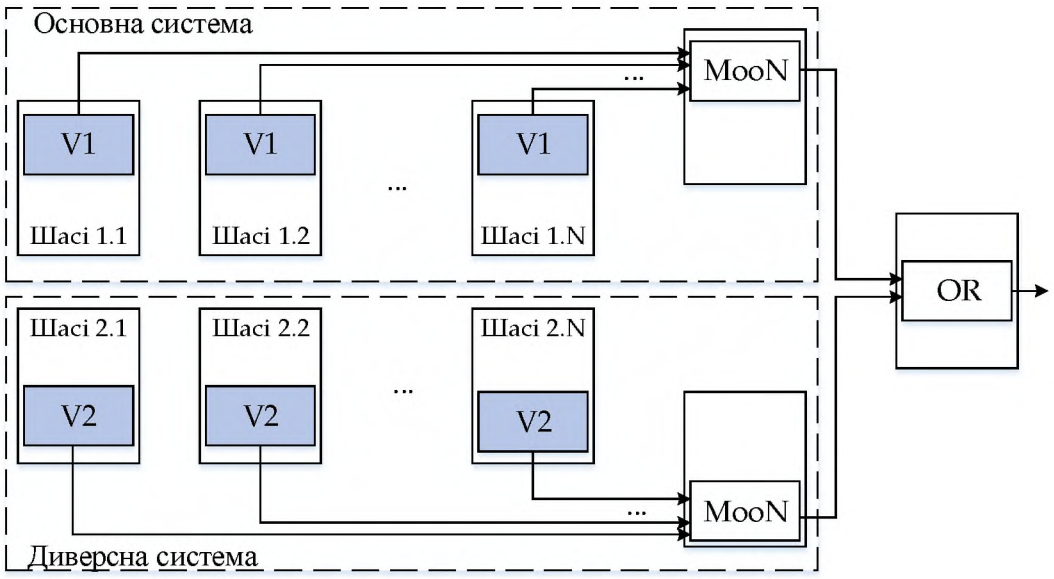


Рисунок 2.13 – Приклад архітектури ПТК АЗ-ПЗ

Необхідно зазначити, що в цьому комплексі використовуються дві функціонально ідентичні версії (V1, V2). Наведена архітектура побудови ПТК є однією з базових [49] і поширених для побудови ІУС АЕС. Зараз ПТК АЗЗ успішно експлуатуються на блоках № 1 і 3 Запорізької АЕС (три комплекти),

блоках № 3 і 4 Рівненської АЕС (три комплекти), блоках № 1 і 3 Південно-Української АЕС (два комплекти).

2.4 Аналіз ІУС. Показники готовності

2.4.1 Показники які оцінюються

Головними показниками, які оцінюються є:

$\mathrm{PFH_{AVG}} = \lambda_{\mathrm{AVG}}$ – середня інтенсивність (частота) небезпечних відмов за годину

PFD_{AVG} – (Probability of failure on demand) ймовірність небезпечної відмови виконання необхідній функції протягом зумовленого міжперевірочного інтервалу – інтервалу автономного функціонального тестування (наприклад, 1 рік) [2, 9].

Для їх визначення необхідно розглянути ще такі величини:

MTTR – Mean Time To Repair – середній час на відновлення (заміни).

Середній час відновлення MTTR (Mean Time To Restore). Складається з інтервалу часу, на початку якого було виявлено, що система безпеки знаходиться в непрацездатному стані, часу визначення причини відмови, часу відновлення працездатності, і часу автономного тестування. Це значення вкрай залежить від обставин і умов, в яких працює система. Система, яка працює без мінімального набору необхідних запасних частин, матиме неймовірний час відновлення. У розрахунках стандарту IEC 61508 MTTR приймається в інтервалі від 8 до 24 годин.

PFH – Probability (Intensity) of Failures per Hour – Ймовірність (інтенсивність) небезпечних відмов (неспрацьовування) за годину.

Дослідження будуть здійснюватися для двох випадків – з наявною та відсутньою самодіагностикою.

У стандарті IEC 61508 загальних рішень не просто відсутні.

Навіть для конкретних представлених в стандарті IEC 61508-6 рішень для архітектури lool, 1oo2, 2oo2, loo2D, 2oo3 не вказується, і тим більше не

розглядається спосіб їх отримання. У цьому розділі представлені загальні співвідношення для розрахунку вірогідності відмови систем безпеці довільної архітектури MooN (m out of n) на межах інтервалу діагностики.

Загальне рішення для PFD у разі виявлення небезпечних відмов тільки під час автономного тестування (DC=0). Ймовірність небезпечної невиявленої відмови поодинокого каналу на момент часу t рівна $\lambda_{DU}t$. Для резервованих систем безпеки типу MooN (M out of N) ймовірність відмови (n - m+1) каналів на момент часу t в загальному випадку визначатиметься числом комбінацій (n - m+1) каналів, що відмовили, з n можливих, і теоремою множення вірогідності незалежних подій.

Тоді середнє значення вірогідності відмови протягом міжперевірочного інтервалу визначиться усереднюванням за часом:

$$FD_{AVG}[DC=0] = C_n^{n-m+1} \cdot \int_0^{T1} \frac{(\lambda_{DU} \cdot t)^{n-m+1}}{T_1} \cdot dt \tag{2.1}$$

або

$$PFD_{AVG}[DC=0] = \frac{C_n^{n-m+1} \cdot (\lambda_{DU} \cdot T_1)^{n-m+1}}{n-m+2} \tag{2.2}$$

де C_n^{n-m+1}- число комбінацій (n-m+1) каналів, що відмовили із n можливих:

$$C_n^{n-m+1} = \frac{n!}{(n-m+1)!\,(m-1)!} \tag{2.3}$$

Отже, якщо самодіагностика відсутня (DC=0), то остаточною формулою для знаходження PFD_{AVG} буде:

$$PFD_{AVG} = \frac{n!}{(n-m+1)!\,(m-1)!} \cdot \frac{(\lambda_{DU}T_1)^{n-m+1}}{(n-m+2)} \tag{2.4}$$

Загальне рішення для PFH у разі виявлення небезпечних відмов тільки під час автономного тестування (DC=0). Аналогічно попередньому, для резервованих систем безпеки типу MooN (M out of N) ймовірність небезпечної відмови одного каналу, і ймовірність відмови (n – m + 1) каналів в інтервалі часу $[0, T_1]$ рівні $\lambda_{DU}T_1$ і C_n^{n-m+1} відповідно.

Тоді можна отримати середню інтенсивність відмов системи в інтервалі часу $[0, T_1]$:

$$FH_{AVG}[DC = 0] = \lambda_{sys} = C_n^{n-m+1} \cdot \frac{(\lambda_{DU} \cdot T_1)^{n-m+1}}{T_1} = \\ = \frac{n!}{(n-m+1)!\,(m-1)!} \cdot \lambda_{DU}^{n-m+1} \cdot T_1^{n-m} \quad (2.5)$$

Саме це співвідношення лежить в основі усіх співвідношень стандарту IEC 61508, частина 6. Але спектр можливих станів досліджуваної архітектури цим співвідношенням не вичерпується.

Загальне рішення для PFD у разі повного діагностичного охоплення (DC=1). Оскільки відмова негайно виявляється, то усереднювання вірогідності за часом існування відмови в даному випадку не вимагається. Неготовність, або ймовірність виявленої небезпечної відмови резервованої системи MooN в загальному випадку визначатиметься безпосередньо теоремою множення вірогідності:

$$PFD_{AVG}[DC = 1] = C_n^{n-m+1} \cdot (\lambda_{DD} \cdot MTTR)^{n-m+1} = \\ = \frac{n!}{(n-m+1)!\,(m-1)!} \cdot (\lambda_{DD} \cdot MTTR)^{n-m+1} \quad (2.6)$$

де C_n^{n-m+1}- число можливих комбінацій (n-m+1) каналів, що відмовили із n можливих:

Загальне рішення для PFH у разі повного діагностичного охоплення (DC=1). Рішення для PFH [DC=1] проведемо за допомогою математичної індукції. Середня частота відмови однієї з n початкових каналів складає $n - \lambda$. Оскільки DC=1, відмова негайно виявляється, і канал, що відмовив, відновлюється протягом інтервалу часу MTTR.

Ймовірність відмови наступного каналу з (n-1) каналів, що залишилися, визначиться, як (n-1) · λ · MTTR. Отже, інтенсивність відмови систем типу (N-1) ooN (наприклад, 1oo2 або 2oo3) виразиться, як:

$$PFH_{AVG}[DC = 1] = n \cdot (n-1) \cdot \lambda_{DD}^2 \cdot MTTR \quad (2.7)$$

Для PFH систем 1oo2 і 2oo3 отримуємо:

$$PFH_{1oo2}[DC=1] = 2 \cdot \lambda_{DD}^2 \cdot MTTR \quad (2.8)$$

$$PFH_{2oo3}[DC=1] = 6 \cdot \lambda_{DD}^2 \cdot MTTR \quad (2.9)$$

Наступним кроком для систем типу (N - 2)ooN, тобто з трьома відмовами, необхідними для повної відмови системи:

$$PFH_{AVG}[DC=1] = n \cdot (n-1) \cdot (n-2) \cdot \lambda_{DD}^3 \cdot MTTR^2 \quad (2.10)$$

Для систем 1oo3 і 2oo4 це означає, що

$$PFH_{1oo3}[DC=1] = 6 \cdot \lambda_{DD}^3 \cdot MTTR^2 \quad (2.11)$$

$$PFH_{2oo4}[DC=1] = 24 \cdot \lambda_{DD}^3 \cdot MTTR^2 \quad (2.12)$$

У загальному випадку для нормальної роботи системи з архітектурою MooN необхідно M працюючих каналів. За допомогою математичної індукції інтенсивність небезпечних відмов систем MooN виразиться таким чином:

$$FH_{AVG}[DC=1] = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot m \cdot \lambda_{DD}^{n-m+1} \cdot MTTR^{n-m} = \quad (2.13)$$

$$= (n-m+1)! \cdot C_n^{n-m+1} \cdot \lambda_{DD}^{n-m+1} \cdot MTTR^{n-m}$$

Зведемо отримані співвідношення воєдино:

$$PFD_{AVG}[DC=0] = \frac{C_n^{n-m+1} \cdot (\lambda_{DU} \cdot T_1)^{n-m+1}}{n-m+2} = \quad (2.14)$$

$$= \frac{n!}{(n-m+1)! \cdot (m-1)!} \cdot \frac{(\lambda_{DU} \cdot T_1)^{n-m+1}}{n-m+2}$$

$$PFH_{AVG}[DC=0] = \lambda_{sys} = C_n^{n-m+1} \cdot \frac{(\lambda_{DU} T_1)^{n-m+1}}{T_1} = \quad (2.15)$$

$$= \frac{n!}{(n-m+1)! \cdot (m-1)!} \cdot \lambda_{DU}^{n-m+1} \cdot T_1^{n-m}$$

$$PFD_{AVG}[DC=0] = C_n^{n-m+1} \cdot (\lambda_{DD} \cdot MTTR)^{n-m+1} = \quad (2.16)$$

$$= \frac{n!}{(n-m+1)! \cdot (m-1)!} \cdot (\lambda_{DD} \cdot MTTR)^{n-m+1}$$

$$PFH_{AVG}[DC=1] = n \cdot (n-1) \cdot \ldots \cdot m \cdot \lambda_{DD}^{n-m+1} \cdot MTTR^{n-m} \quad (2.17)$$

$$= (n-m+1)! \cdot C_n^{n-m+1} \cdot \lambda_{DD}^{n-m+1} \cdot MTTR^{n-m}$$

Отримані результати дають можливість знайти загальні співвідношення, що зв'язують ймовірність відмови низького і високого рівня вимог безпеки.

Із співвідношень (2.1) – (2.4) витікає, що в загальному вигляді зв'язок вірогідності небезпечної відмови низького і високого рівня вимог визначатиметься наступними виразами:

$$PFD_{DC=0} = PFH_{DC=0} \cdot \frac{T_1}{n-m+2} \tag{2.18}$$

$$PFD_{DC=1} = PFH_{DC=1} \cdot \frac{MTTR}{(n-m+1)!} \tag{2.19}$$

Розглянемо докладніше базові архітектури

Мінімальна конфігурація архітектури 1oo1 представлена на рис.2.14:

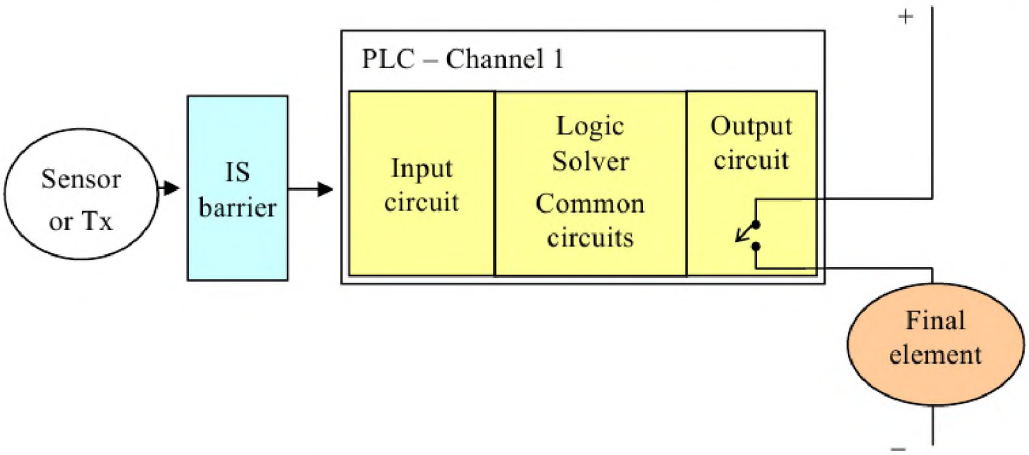


Рисунок 2.14 – Мінімальна конфігурація архітектури 1oo1

У системі може статися небезпечна відмова для виявленого або не виявленого відхилення λ_{DD} або λ_{DU}.

$$PFD_{avg} = \lambda_{DD} \cdot RT + \lambda_{DU} \cdot \frac{TI}{2} \tag{2.20}$$

де, RT – час на відновлення (зазвичай приймається 8 год).

TI – інтервал часу між двома ручними незалежними випробуваннями (зазвичай приймається 1, 3, 5 або 10 років).

для TI = 1:

$$PFD_{avg} = \lambda_{DD} \cdot 8 + \lambda_{DU} \cdot 4380 \quad (2.21)$$

Дуже часто значення $\lambda_{DD} \cdot 8$ набагато менше, ніж $\lambda_{DD} \cdot 4380$, отже приблизно:

$$PFD_{avg} = \lambda_{DU} \cdot \frac{TI}{2} \quad (2.22)$$

Обчислення PFD_{avg} здійснюється для усіх компонентів системи тому оцінка повної системи PFD_{avg} буде наступною:

$$D_{avg}\ system = PFD_{avg}\ sensor + PFD_{avg}\ barrier + \quad (2.23)$$

$$+ PFD_{avg}\ PLC\ controller + PFD_{avg}\ actuator/valve$$

Наприклад:

Припустимо, що інтенсивність відмов, для небезпечних невиявлених відмов (λ_{DU}), дорівнює 0.0025 р.

Для TI = 1 р. $PFD_{avg} = \lambda_{DU} \cdot \frac{TI}{2} = 0{,}0025 \cdot \frac{1}{2} = 0.00125$ р.

Для TI = 3 р. $PFD_{avg} = \lambda_{DU} \cdot \frac{TI}{2} = 0.00375$ р.

Для TI = 5 р. $PFD_{avg} = \lambda_{DU} \cdot \frac{TI}{2} = 0.00626$ р.

На основі даних міркувань та стандарту МЕК 61508 одержуємо базові формули для розрахунків і для інших архітектур (табл. 2.6):

Таблиця 2.6 – Розрахункові формули $\mathrm{PFD_{avg}}$ для декількох базових архітектур

Архітектура	Розрахункові формули
1oo1	$PFD_{avg} = \lambda_{DU} \cdot \frac{TI}{2}$
1oo2	$PFD_{avg} = \lambda_{DU_1} \cdot \lambda_{DU_2} \cdot \frac{TI^2}{2}$ $PFD_{avg} = \lambda_{DU}^2 \cdot \frac{TI^2}{2}$
2oo2	$PFD_{avg} = (\lambda_{DU_1} \cdot \lambda_{DU_2}) \cdot \frac{TI}{2}$ $PFD_{avg} = \lambda_{DU} \cdot TI$

Таблиця 2.7 – Розрахунок впливу інтервалу часу і тривалості періодичних випробувань на $\mathrm{PFD_{avg}}$ для надлишкових рівнозначних компонентів

Архітектура	Розрахункові формули
1oo1	$PFD_{avg} = \lambda_{DU} \cdot \frac{TI}{2} + \left(\frac{TD}{TI}\right)$
1oo2	$PFD_{avg} = \lambda_{DU}^2 \cdot \frac{TI^2}{2} + \left(2 \cdot TD \cdot \lambda_{DU} \cdot \frac{\frac{TI}{2} + MTTR}{TI}\right)$
2oo2	$PFD_{avg} = \lambda_{DU} \cdot TI + \left(\frac{TD}{TI}\right)$

Нижче наведені таблиці порівняння для значень $\mathrm{PFD_{avg}}$, для різних архітектур, а також різних інтервалів TI, з постійним значенням для небезпечних відмов ($\lambda_{DU} = 0{,}01$ р.), і постійним середнім часом на відмову (MTTR = 8 годин = 0,0009 років):

Таблиця 2.8 – TI = 1 р, TD = 0.0009 р.

Architecture	λdu/yr	PFDavg	RRF	Possible SIL level
1oo1	0,01	0,005900000	169	SIL 2
1oo2	0,01	0,000042350	23613	SIL 4
2oo2	0,01	0,010900000	92	SIL 1
2oo3	0,01	0,000127049	7871	SIL 3

Таблиця 2.9 – TI = 3 р, TD = 0.0009 р.

Architecture	λdu/yr	PFDavg	RRF	Possible SIL level
1oo1	0,01	0,0153	65	SIL 1
1oo2	0,01	0,000309	3236	SIL 3
2oo2	0,01	0,0303	33	SIL 1
2oo3	0,01	0,000927	1079	SIL 3

Таблиця 2.10 – = 5 р, TD = 0.0009 р.

Architecture	λdu/yr	PFDavg	RRF	Possible SIL level
1oo1	0,01	0,015300000	65	SIL 1
1oo2	0,01	0,000309005	3236	SIL 3
2oo2	0,01	0,030300000	33	SIL 1
2oo3	0,01	0,000927016	1079	SIL 2

Таблиця 2.11 – TI = 10 р, TD = 0.0009 р.

Architecture	λdu/yr	PFDavg	RRF	Possible SIL level
1oo1	0,01	0,025180000	40	SIL 1
1oo2	0,01	0,000842337	1187	SIL 2
2oo2	0,01	0,050180000	20	SIL 0
2oo3	0,01	0,002527010	396	SIL 1

Висновки з розділу 2

В розділі розглянуто узагальнену структуру інформаційно-керуючої системи АЕС, та її складова програмно-технічний комплекс. Введено поняття базової архітектури. Надано опис безпечних програмовних логічник контролерів та їх властивості порівняні з звичайними ПЛК.

Виконано детальний огляд базових архітектур побудови ПТК, а саме:

1oo1; 1oo2; 1oo1D; 1oo2D; 2oo2D. Виконано їх порівняння з точки зору надійності. Розглянуто системи сімейства QUADLOG, які призначені для створення додатків, що пред'являють особливо високі вимоги до надійності,

відмовостійкості і безпеки: системи протиаварійного захисту, системи пожежо і газобезпеки, системи управління критичними процесами.

Розглянуто інформаційно-управляючу цифрова платформу (ЦІУП) RadICS™, як продукт нового покоління, розроблений в 2010-2020 роках на основі більш ніж 20-тирічного досвіду розробки, виробництва, експлуатації і обслуговування цифрової ЦІУП платформи Radiy.

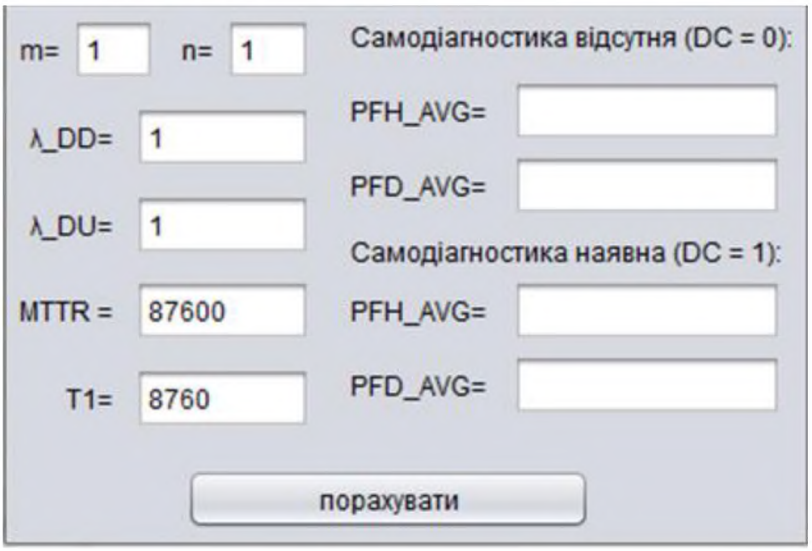
Доведено, для забезпечення надійності функціонування ІУС застосовуються спеціальні методи структурного резервування апаратних засобів і версійного резервування програмних засобів. Спосіб резервування вибирають таким чином, щоб забезпечити для кожної функції прийнятний баланс між імовірністю відмов видів «неспрацьовування» і «помилкове спрацьовування». З метою мінімізації впливу всіх або частини помилок, які можуть виникати на стадіях створення й упровадження ІУС і бути загальною причиною одночасної відмови декількох резервних частин, застосовується принцип різноманітності. Дотримання цього принципу забезпечується, наприклад, застосуванням у складі однієї системи двох програмно-технічних комплексів (ПТК), які можуть виконувати функції безпеки незалежно й у повному обсязі, але досягають постановленої мети різними способами та (або) фізично відрізняються один від одного

РОЗДІЛ 3
РОЗРОБЛЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ОЦІНЮВАННЯ ГОТОВНОСТІ ТА ФУНКЦІЙНОЇ БЕЗПЕЧНОСТІ ТА АНАЛІЗ РЕЗУЛЬТАТІВ ОЦІНЮВАННЯ СИСТЕМ З РІЗНОЮ АРХІТЕКТУРОЮ

3.1 Опис програми

За допомогою мови програмування java було розроблено програмний продукт для точних розрахунків значень $\mathrm{PFD}_{\mathrm{avg}}$ та $\mathrm{PFH}_{\mathrm{avg}}$. Було розглянуто два випадки і приведено значення для кожного з цих випадків відповідно. Випадок коли самодіагностика відсутня і випадок – коли наявна.

Вікно програми виглядає так:



В залежності від введених значень можна порахувати необхідні параметри. Програмний код наведений у додатках.

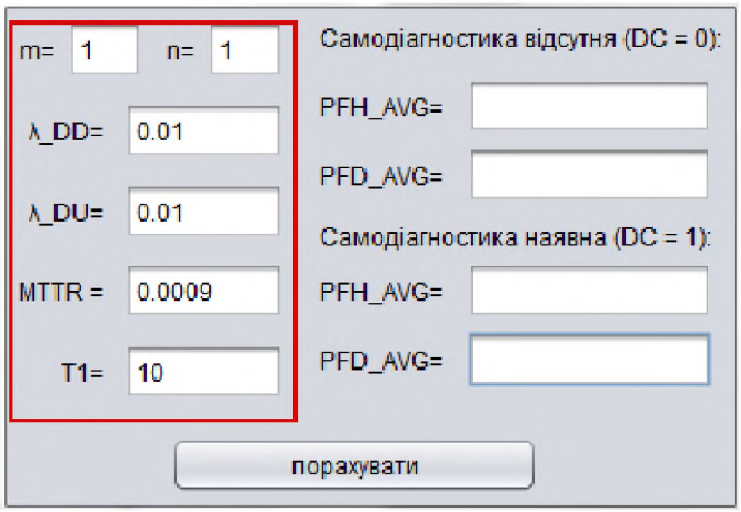
3.2 Інструкція щодо використання

Програма реалізована на мові програмування Java, що забезпечує кросплатформеність додатку. Для роботи програми на комп'ютері має бути встановлена java машина (JDK - Java Development Kit або JRE - Java Runtime

Environment), яку можна встановити з офіційного сайту oracle (http://www.oracle.com/).

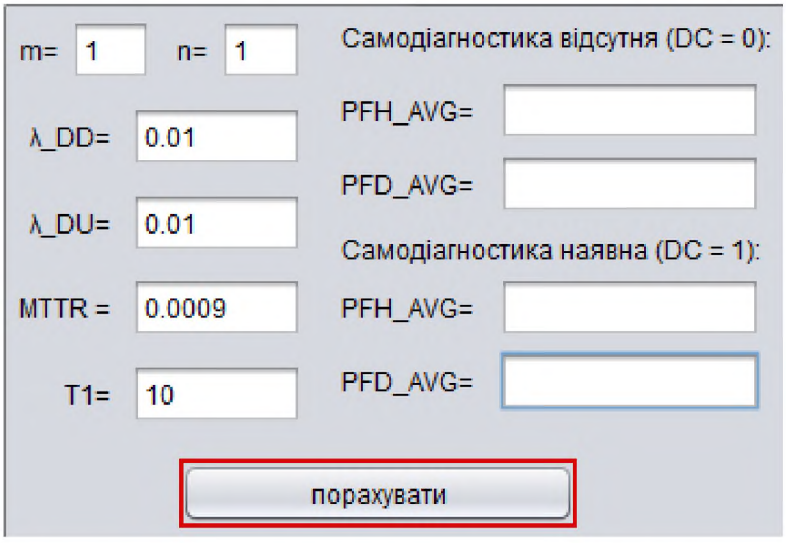
Для того щоб виконувати необхідні розрахунки – потрібно відкрити *.jar файл.

Щоб порахувати значення PFD_{avg} і PFH_{avg} спочатку треба ввести відповідні значення констант:

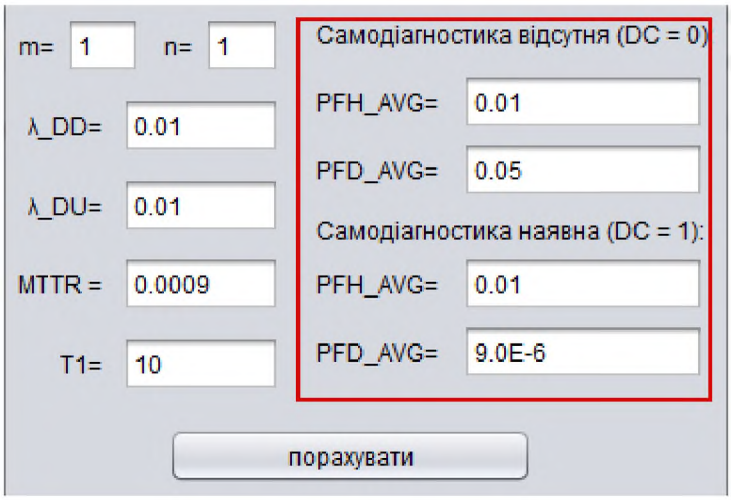


Константи m і n визначають архітектуру MooN.

Після того, як константи введені – натискаємо на кнопку «порахувати»:



Після цього ми побачимо значення шуканих величин у відповідних текстових полях програми:



3.3 Аналіз результатів і порівняння архітектур

Аналіз і порівняння архітектур визначались за допомогою розробленої програми. На вхід подавалися аналогічні дані, а результати порівнювалися.

Для архітектури 1oo1(D), якщо $\lambda_{DD} = \lambda_{DU} = 0.01, MTTR = 0.0009, T_1 = 10$ маємо:

$$PFH_{avg}[DC = 0] = 0.01;$$

$$PFD_{avg}[DC = 0] = 0.05;$$

$$PFH_{avg}[DC = 1] = 0.01;$$

$$PFD_{avg}[DC = 1] = 0.0223.$$

Для архітектури 1oo2(D), якщо $\lambda_{DD} = \lambda_{DU} = 0.01, MTTR = 0.0009, T_1 = 10$ маємо:

$$PFH_{avg}[DC = 0] = 0.001;$$

$$PFD_{avg}[DC = 0] = 0.0033;$$

$$PFH_{avg}[DC = 1] = 0{,}0016;$$

$$PFD_{avg}[DC = 1] = 0{,}00013.$$

Для архітектури 2oo2(D), якщо $\lambda_{DD} = \lambda_{DU} = 0.01, MTTR = 0.0009, T_1 = 10$ маємо:

$$PFH_{avg}[DC = 0] = 0.02;$$

$$PFD_{avg}[DC = 0] = 0.1;$$

$$PFH_{avg}[DC = 1] = 0{,}2;$$

$$PFD_{avg}[DC = 1] = 0{,}012.$$

Отже, як видно з розрахунків – середня інтенсивність (частота) небезпечних відмов за годину є найменшою для архітектури 1oo2.

Ймовірність небезпечної відмови виконання необхідній функції протягом зумовленого міжперевірочного інтервалу – інтервалу автономного функціонального тестування (10 років) – теж є найменшою для архітектури 1oo2.

Отже, архітектура 1oo2D є найбільш надійною з розглянутих базових архітектур.

3.4 Техніко-економічне обґрунтування розробки програмного продукту

Витрати на розроблення ПЗ здійснюються за формулою:

$$Кп = Кпр + Кпк + Кт\ , \qquad (3.1)$$

де *Кпр* – витрати на проєктування ПЗ;

Кпк – витрати на створення компонент ПЗ, з яких складається продукт;

Кт – витрати на тестування та відлагодження ПЗ.

Загальний розрахунок на розробку ПЗ можливо виконати за формулою

$$Кп = Фз/п\ [(1+βд)(1+βс)+βн+βпр]+t_{ПЕОМ}, \qquad (3.2)$$

де *Фз/п* – фонд основної заробітної платні розробників та інших виконавців;

βд – коефіцієнт додаткової заробітної платні, можливо прийняти 0,10...0,15;

βс – коефіцієнт відрахування, який дорівнює 0,26;

βн – коефіцієнт накладних витрат організації 0,6...0,8;

βпр – коефіцієнт інших витрат 0,1...0,2;

$t_{ПЕОМ}$ — машинний час, затрачений час на тестування та відлагодження, г.

Відповідно до цього підходу обчислено, що загальний час роботи одного програміста над ПЗ становив 156 годин. За умови оплати праці 20 грн на годину, загальна суму розробки склала 3120 грн.

Висновки з розділу 3

Розділ присвячено зробленню програмної утіліти оцінювання властивостей готовності та функційної безпечності програмно-технічних комплексів критичного застосування. Надано детальний опис користувацького інтерфейсу, розроблено інструкцію користувача.

Виконано розрахунки показників готовності та функційної безпечності обраних базових архітектур побудови систем та здійснено аналіз результатів розрахунків. Встановлено, що ймовірність небезпечної відмови виконання необхідній функції протягом зумовленого міжперевірочного інтервалу – інтервалу автономного функціонального тестування (10 років) – є найменшою для архітектури 1oo2D. Отже, архітектура 1oo2D є найбільш надійною з розглянутих базових архітектур. Виконано техніко-економічне обґрунтування розробки програмного продукту.

ВИСНОВКИ

В першому розділі роботи виконано аналіз нормативної бази, принципів структурної організації та функціонування програмно-апаратних засобів систем обраного для досліджень класу, а саме складних технічних комплексів критичного застосування. Проаналізовано вимоги до надійності та функційної безпечності для систем означеного класу. В процесі аналізу встановлено, що підвищення вимог до показників надійності та функційної безпечності в свою чергу обумовлює підвищення вимог до оцінювання точності їх оцінювання на етапах проєктування, виробництва та приробки ІУС. Поставлено завдання на подальші дослідження.

В процесі виконання кваліфікаційної роботи було розроблено програмне забезпечення, за допомогою якої можна здійснювати оцінку готовності та функційної безпечності електричних, електронних, програмованих електронних пов’язаних з безпекою систем. А також, відповідно до поставленого завдання, у роботі досліджено показники готовності та функційної безпечності електричних, електронних, програмованих електронних пов’язаних з безпекою систем.

В другому розділі роботи розглянуто узагальнену структуру інформаційно-керуючої системи АЕС, та її складова програмно-технічний комплекс. Введено поняття базової архітектури. Надано опис безпечних програмовних логічник контролерів та їх властивості порівняні з звичайними ПЛК. Виконано детальний огляд базових архітектур побудови ПТК, а саме: 1oo1; 1oo2; 1oo1D; 1oo2D; 2oo2D. Виконано їх порівняння з точки зору надійності. Розглянуто системи сімейства QUADLOG, які призначені для створення додатків, що пред'являють особливо високі вимоги до надійності, відмовостійкості і безпеки: системи протиаварійного захисту, системи пожежо і газобезпеки, системи управління критичними процесами.

Розглянуто інформаційно-управляючу цифрова платформу (ЦІУП) RadICS™, як продукт нового покоління, розроблений в 2010-2020 роках на

основі більш ніж 20-тирічного досвіду розробки, виробництва, експлуатації і обслуговування цифрової ЦІУП платформи Radiy.

Третій розділ присвячено розробці програмної утиліти оцінювання властивостей готовності та функційної безпечності програмно-технічних комплексів критичного застосування. Надано детальний опис користувацького інтерфейсу, розроблено інструкцію користувача.

Виконано розрахунки показників готовності та функційної безпечності обраних базових архітектур побудови систем та здійснено аналіз результатів розрахунків. Встановлено, що ймовірність небезпечної відмови виконання необхідній функції протягом зумовленого міжперевірочного інтервалу – інтервалу автономного функціонального тестування (10 років) – є найменшою для архітектури 1oo2D. Отже, архітектура 1oo2D є найбільш надійною з розглянутих базових архітектур. Виконано техніко-економічне обґрунтування розробки програмного продукту.

В подальшому розроблену програму можна використовувати як підпрограму для інших програм, які будуть здійснювати більш глибокий аналіз систем, а також включатимуть в себе більш широкий спектр архітектур.

Ймовірність небезпечної відмови виконання необхідній функції протягом обраного міжперевірочного інтервалу – інтервалу автономного функціонування (10 років) – є найменшою для архітектури 1oo2D.

Отже, архітектура 1oo2D є найбільш надійною з розглянутих базових архітектур. Її показники: У порівнянні з показниками для інших архітектур, дана – має беззаперечну перевагу і рекомендується особам що приймають рішення до обрання.