



УКРАЇНА

(19) UA

(11) 130689

(13) C2

(51) МПК

G05B 9/02 (2006.01)

НАЦІОНАЛЬНИЙ ОРГАН
ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ
ДЕРЖАВНА ОРГАНІЗАЦІЯ
"УКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ
ОФІС ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ ТА ІННОВАЦІЙ"

(12) ОПИС ДО ПАТЕНТУ НА ВИНАХІД**(21)** Номер заявки: **а 2024 03764****(22)** Дата подання заявки: **10.02.2022****(24)** Дата, з якої є чинними
права інтелектуальної
власності: **16.04.2026****(41)** Публікація відомостей
про заявку: **16.10.2024, Бюл.№ 42****(46)** Публікація відомостей
про державну
реєстрацію: **15.04.2026, Бюл.№ 15****(86)** Номер та дата
подання міжнародної
заявки, поданої
відповідно до
Договору РСТ **РСТ/JP2022/005280,
10.02.2022****(72)** Винахідник(и):**Окуда Сусуму (JP)****(73)** Володілець (володільці):**МІЦУБІСІ ЕЛЕКТРІК КОРПОРЕЙШН,**7-3, Marunouchi 2-chome, Chiyoda-ku, Tokyo
1008310, Japan (JP)**(74)** Представник:**Петров Андрій Володимирович, реєстр.
№139****(56)** Перелік документів, взятих до уваги
експертизою:

JP 2011/191855 A, 29.09.2011

JP 2018/101241 A, 28.06.2018

WO 2020/090034 A1, 07.05.2020

JP 2005/249609 A, 15.09.2005

CN 103400623 A, 20.11.2013

US 9368240 B2, 14.06.2016

US 10929273 B2, 23.02.2021

(54) РЕЗЕРВНИЙ ПРИСТРІЙ СИСТЕМИ ЗАХИСТУ БЕЗПЕКИ**(57)** Реферат:

Цей резервний пристрій системи захисту безпеки виявляє стан електростанції, а потім, якщо виявлена несправність, видає команду локальному компоненту (4) системи безпеки відповідно до вихідного сигналу першої логіки (222) захисту безпеки в пристрої (2) захисту безпеки і, якщо у пристрої (2) захисту безпеки виявлена відмова із загальної причини, видає команду локальному компоненту (4) системи безпеки відповідно до вихідного сигналу другої логіки (312) захисту безпеки в пристрої (3) CCF. Перша логіка (222) захисту безпеки та друга логіка (312) захисту безпеки налаштовані на виконання обробки цифрових сигналів на основі логічних конфігурацій, що відрізняються одна від одної, в результаті чого вхідний пристрій (21) та вихідний пристрій (23) можуть бути спільними для пристрою (2) захисту безпеки та для пристрою (3) CCF, і не потрібно забезпечувати вхідний пристрій та вихідний пристрій окремо для пристрою (3) CCF, і при цьому збільшувати кількість детекторів (1) та локальних компонентів (4) системи безпеки також можна без збільшення масштабу пристрою (3) CCF.

UA 130689 C2

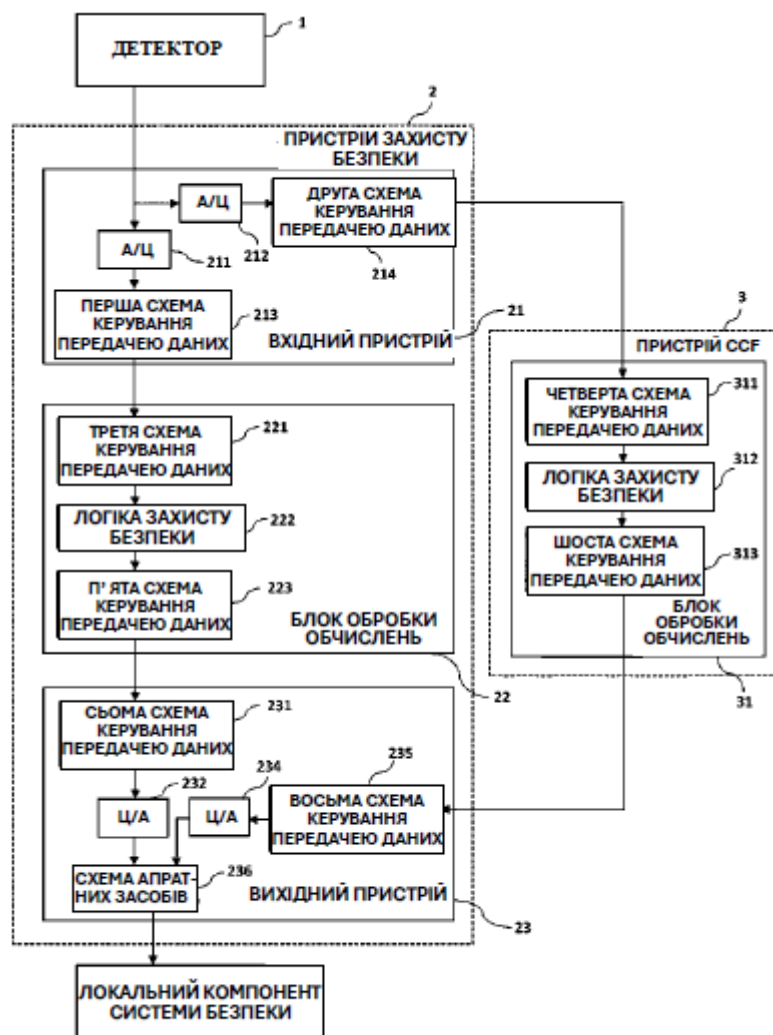


Fig. 1

ОБЛАСТЬ ТЕХНІКИ

Цей винахід відноситься до резервного пристрою системи захисту безпеки.

ПЕРЕДУМОВИ СТВОРЕННЯ ВІНАХОДУ

На атомній електростанції, застосовується вимикач аварійного захисту реактора як один із пристроїв в обладнанні системи захисту для зупинки ядерного реактора у випадку, коли сталась несправність. Пристрій приводу керуючого стрижня живиться електричною енергією від шини живлення через перетворювач електричної енергії та вимикач аварійного захисту реактора, і коли вимикач аварійного захисту реактора розмикається, пристрій приводу керуючого стрижня більше не живиться електричною енергією, і керуючий стрижень вставляється в ядерний реактор, для зупинки ядерного реактора. Крім того, окрім вимикача аварійного захисту реактора, обладнання системи захисту включає в себе обладнання системи безпеки, таке як насоси та клапани для впускання охолоджуючої води в ядерний реактор і термінового охолодження ядерного реактора у випадку несправності.

Обладнання системи захисту отримує сигнали від різних датчиків виявлення, і, якщо логіка захисту визначила, що ядерний реактор необхідно зупинити або терміново охолоджувати, то формується сигнал зупинки ядерного реактора, і сигнал запиту на операцію (розблокування) передається на вимикач аварійного захисту реактора або на обладнання системи безпеки.

Обладнання системи захисту сконфігуроване таким чином, щоб мультиплексуватись для досягнення високої надійності, однак, коли між мультиплексованими пристроями відбувається відмова із загальної причини (CCF-common cause failure), то існує імовірність того, що сигнал запиту на операцію (розблокування) не може передаватись на вимикач аварійного захисту реактора тощо, навіть у випадку, коли сталась несправність на електростанції.

Для того, щоб коректно зупинити ядерний реактор у випадку, коли в обладнанні системи захисту сталась CCF, розкрито спосіб встановлення обладнання протидії CCF, яке призначене для резервування обладнання системи захисту (наприклад, дивись патентний документ 1). Основною причиною CCF, що відбувається у мультиплексованому обладнанні системи захисту, є програмна помилка. Відповідно, обладнання протидії CCF являє собою аналогове обладнання, що складається із таких деталей електричного ланцюга, як перемикачі та реле, та, у відповідь на сигнал від датчика виявлення, обладнання протидії CCF визначає, чи необхідно зупинити ядерний реактор. Після отримання сигналу зупинки ядерного реактора від обладнання протидії CCF, пристрій перетворення електричної енергії перериває подачу електричної енергії на вимикач аварійного захисту реактора. Таким чином, пристрій приводу керуючого стрижня входить у стан без подачі електричної енергії, і керуючий стрижень вставляється у ядерний реактор, так, що ядерний реактор зупиняється.

СПИСОК ЦИТУВАННЯ

ПАТЕНТНИЙ ДОКУМЕНТ

Патентний документ 1: Японська викладена патентна публікація № 2012-122907

КОРОТКИЙ ОПИС ВІНАХОДУ

ЗАДАЧА, ЯКУ ВИРІШУЄ ВІНАХІД

Однак, коли обладнання протидії CCF складається із аналогового обладнання, яке включає в себе перемикачі, реле, та подібне, як описано у Патентному документі 1, то потрібні пристрої входження сигналу, що відповідають кількості детекторів. Крім того, потрібні пристрої виходу сигналу, що відповідають кількості пристроїв об'єкту в обладнанні системи захисту.

Крім того, забезпечується таке проектування та виготовлення пристрою CCF, що його рівень проектування є спрощеним порівняно із рівнем проектування обладнання системи захисту в якості звичайного системного обладнання, однак, для того, щоб запобігти впливу електричної несправності в пристрої CCF на обладнання системи захисту, між пристроєм CCF та обладнанням системи захисту необхідно передбачити роздільний пристрій, такий як реле або плавкий запобіжник, з тим, щоб припинити вплив електричної несправності. Таким чином, збільшується кількість функцій, реалізованих в пристрої CCF, збільшуючи тим самим масштаб пристрою CCF відповідно до кількості вхідних та вихідних пристроїв.

Цей винахід був задуманий для вирішення зазначеної вище задачі, і метою цього винаходу є забезпечення резервного пристрою системи захисту безпеки, у якому масштаб пристрою CCF не збільшується, навіть якщо збільшується кількість детекторів та локальних компонентів системи безпеки.

ЗАСІБ ВИРІШЕННЯ ЗАДАЧІ

Резервний пристрій системи захисту безпеки відповідно до цього винаходу виявляє стан електростанції, і, якщо виявлена несправність, видає команду локальному компоненту системи безпеки відповідно до вихідного сигналу першої логіки захисту безпеки у пристрої захисту безпеки і, якщо у пристрої захисту безпеки виявлена відмова із загальної причини, то видає

команду локальному компоненту системи безпеки відповідно до вихідного сигналу другої логіки захисту безпеки в пристрої CCF. Резервний пристрій системи захисту безпеки включає в себе: детектор, який виявляє стан електростанції; першу та другу схеми аналого-цифрового перетворення, які розташовані у вхідному пристрої пристрою захисту безпеки та виконують цифрові перетворення вихідного сигналу детектора; першу схему керування передачею даних, яка розташована у вхідному пристрої та передає на блок обробки обчислень сигнал, що виходить із першої схеми аналого-цифрового перетворення; другу схему керування передачею даних, яка розташована у вхідному пристрої та передає на пристрій CCF сигнал, що виходить із другої схеми аналого-цифрового перетворення; третю схему керування передачею даних, яка розташована у першому блоці обробки обчислень пристрою захисту безпеки, отримує вихідний сигнал першої схеми керування передачею даних, та передає вихідний сигнал до першої логіки захисту безпеки блоку обробки обчислень; четверту схему керування передачею даних, яка отримує вихідний сигнал другої схеми керування передачею даних та передає вихідний сигнал до другої логіки захисту безпеки, розташованої у другому блоці обробки обчислень пристрою CCF; п'яту схему керування передачею даних, яка розташована у першому блоці обробки обчислень та передає вихідний сигнал першої логіки захисту безпеки; шосту схему керування передачею даних, яка розташована у другому блоці обробки обчислень та передає вихідний сигнал другої логіки захисту безпеки; сьому схему керування передачею даних, яка отримує сигнал, переданий від п'ятої схеми керування передачею даних, та розташована в області вихідного пристрою пристрою захисту безпеки; восьму схему керування передачею даних, яка отримує сигнал, переданий від шостої схеми керування передачею даних, та розташована в області вихідного пристрою; першу схему цифро-аналогового перетворення, яка розташована в області вихідного пристрою та виконує аналогове перетворення сигналу сьомої схеми керування передачею даних; другу схему цифро-аналогового перетворення, яка розташована в області вихідного пристрою та виконує аналогове перетворення сигналу восьмої схеми керування передачею даних; а також схему апаратних засобів, в яку вводиться сигнал першої або другої схеми цифро-аналогового перетворення і яка виконує виведення на локальний компонент системи безпеки. Перша логіка захисту безпеки та друга логіка захисту безпеки виконують обробки цифрових сигналів на основі логічних конфігурацій, що відрізняються одна від одної. Перша схема аналого-цифрового перетворення та друга схема аналого-цифрового перетворення складаються із схем або частин, що відрізняються одна від одної. Перша схема цифро-аналогового перетворення та друга схема цифро-аналогового перетворення складаються із схем або частин, що відрізняються одна від одної. Протокол передачі даних між першою схемою керування передачею даних та третьою схемою керування передачею даних відрізняється від протоколу передачі даних між другою схемою керування передачею даних та четвертою схемою керування передачею даних. Протокол передачі даних між п'ятою схемою керування передачею даних та сьомою схемою керування передачею даних відрізняється від протоколу передачі даних між шостою схемою керування передачею даних та восьмою схемою керування передачею даних.

ЕФЕКТ ВІД ВІНАХОДУ

В резервному пристрої системи захисту безпеки відповідно до цього винаходу, перша логіка захисту безпеки в пристрої захисту безпеки та друга логіка захисту безпеки в пристрої CCF налаштовані відповідно на виконання різного прикладного програмного забезпечення, в результаті чого вхідний пристрій та вихідний пристрій можуть бути спільними для пристрою захисту безпеки та пристрою CCF, таким чином, не потрібно забезпечувати вхідний пристрій та вихідний пристрій окремо для пристрою CCF, і при цьому збільшувати кількість детекторів та локальних компонентів системи безпеки також можна без збільшення масштабу пристрою CCF.

КОРОТКИЙ ОПИС ГРАФІЧНИХ МАТЕРІАЛІВ

[ФІГ. 1] ФІГ. 1 являє собою схематичний вигляд структури резервного пристрою системи захисту безпеки відповідно до варіанту здійснення 1.

[ФІГ. 2] ФІГ. 2 являє собою схематичний вигляд структури резервного пристрою системи захисту безпеки відповідно до варіанту здійснення 2.

[ФІГ. 3] ФІГ. 3 являє собою схематичний вигляд структури резервного пристрою системи захисту безпеки відповідно до варіанту здійснення 3.

[ФІГ. 4] ФІГ. 4 являє собою схематичний вигляд структури резервного пристрою системи захисту безпеки відповідно до варіанту здійснення 4.

[ФІГ. 5] ФІГ. 5 являє собою схему конфігурації апаратних засобів логіки захисту безпеки відповідно до варіантів здійснення 1-4.

ОПИС ВАРІАНТІВ ЗДІЙСНЕННЯ

Далі, будуть описані переважні варіанти здійснення резервного пристрою системи захисту

безпеки відповідно до цього винаходу із посиланням на графічні матеріали. Ті самі або відповідні об'єкти та частини позначаються однаковими посилальним позначеннями, а їх детальний опис не наводиться. Також, у наведених далі варіантах здійснення, компоненти, позначені однаковими посилальним позначеннями, не будуть описуватись повторно.

5 Варіант здійснення 1

ФІГ. 1 являє собою схематичний вигляд структури резервного пристрою системи захисту безпеки цього варіанту здійснення. Буде описано випадок, коли цей варіант здійснення застосовується до атомної електростанції, але цей варіант здійснення ним не обмежується. Детектор 1 контролює стан атомної електростанції, та передає сигнал виявлення на пристрій 2 захисту безпеки, який є обладнанням системи захисту. Переданий сигнал виявлення вводиться у вхідний пристрій 21 пристрою 2 захисту безпеки, та електрично розподіляється у вхідному пристрої 21. Один із розподілених сигналів вводиться на схему 211 аналого-цифрового (А/Ц) перетворення пристрою 2 захисту безпеки, а інший з них вводиться на схему 212 А/Ц перетворення для пристрою 3 ССФ.

15 Сигнал виявлення перетворюється на цифровий сигнал за допомогою схеми 211 А/Ц перетворення, і цифровий сигнал передається на блок 22 обробки обчислень через першу схему 213 керування передачею даних пристрою 2 захисту безпеки. Переданий цифровий сигнал отримується третьою схемою 221 керування передачею даних, яка розташована на вході у блок 22 обробки обчислень, та застосовується логікою 222 захисту безпеки, реалізованою у вигляді здійснення попередньо розробленої логіки захисту (яку надалі називають прикладним програмним забезпеченням) мікропроцесором або ПЛІС (програмованої логічної інтегральної схеми), для формування сигналу керування операцією обладнання системи захисту на локальний компонент 4 системи безпеки. Сигнал керування операцією, сформований логікою 222 захисту безпеки, на локальний компонент 4 системи безпеки, 20 передається на вихідний пристрій 23 через п'яту схему 223 керування передачею даних, яка розташована на виході із блоку 22 обробки обчислень. У даному випадку, функція прикладного програмного забезпечення включає в себе чотири аналогові арифметичні операції, на додаток до логічної операції.

У вихідному пристрої 23, сигнал керування операцією, переданий від п'ятої схеми 223 керування передачею даних отримується сьомою схемою 231 керування передачею даних і потім перетворюється на аналоговий сигнал за допомогою схеми 232 цифро-аналогового (Ц/А) перетворення, і аналоговий сигнал передається на схему 236 апаратних засобів (АЗ), яка являє собою кінцевий вихідний компонент. Схема АЗ виконує пріоритетну обробку введеного сигналу. Приклади схеми АЗ включають в себе логічну схему АБО, логічну схему ТА, схему пріоритету 35 ВКЛ, та схему пріоритету ВИКЛ. Однак, схема АЗ цим не обмежується.

Разом з тим, цифровий сигнал, введений у схему 212 А/Ц перетворення, передається на другу схему 214 керування передачею даних для пристрою 3 ССФ.

Схема 211 А/Ц перетворення та схема 212 А/Ц перетворення, відповідно, складаються із схем або пристроїв (частин), що відрізняються один від одного, та відповідним чином 40 реалізовані ними. Подібним чином, перша схема 213 керування передачею даних та друга схема 214 керування передачею даних також, відповідно, складаються із схем або частин, що відрізняються одна від одної, та відповідним чином реалізовані ними.

Друга схема 214 керування передачею даних передає введений цифровий сигнал на четверту схему 311 керування передачею даних, з'єднану із блоком 31 обробки обчислень пристрою 3 ССФ, таким самим чином, як і для блоку 22 обробки обчислень. Переданий 45 цифровий сигнал отримується четвертою схемою 311 керування передачею даних, і потім застосовується логікою 312 захисту безпеки, сконфігурованою мікропроцесором або програмованою логічною інтегральною схемою (ПЛІС), в якій реалізоване прикладне програмне забезпечення, для формування сигналу запиту на операцію на локальний компонент 4 системи 50 безпеки.

У даному випадку, для забезпечення рознесення, до кожного компоненту застосовується наступне:

(1) В якості протоколу передачі даних між другою схемою 214 керування передачею даних та четвертою схемою 311 керування передачею даних, застосовується протокол передачі 55 даних, який відрізняється від протоколу передачі даних, який має застосовуватись між першою схемою 213 керування передачею даних та третьою схемою 221 керування передачею даних.

(2) Блок 31 обробки обчислень та блок 22 обробки обчислень, відповідно, виконують подібні обробки цифрових сигналів із застосуванням різних схем. Наприклад, в якості мікропроцесора блоку 31 обробки обчислень застосовується пристрій, що відрізняється від мікропроцесора 60 блоку 22 обробки обчислень, або ж у блоці 31 обробки обчислень застосовується ПЛІС.

(3) Логіка 312 захисту безпеки та логіка 222 захисту безпеки, відповідно, розроблені на основі різних ідей для подібної обробки цифрових сигналів. Наприклад, у випадку, коли у блоці 31 обробки обчислень та у блоці 22 обробки обчислень застосовуються мікропроцесори, то концепції розробок прикладного програмного забезпечення, яке має бути реалізоване, є різними, і при цьому мікропроцесори розроблені різними розробниками, таким чином, щоб не здійснювати визначення на основі однієї і тієї ж логічної конфігурації. У випадку, коли у блоці 31 обробки обчислень застосовується ПЛІС, то ПЛІС програмується іншим розробником, таким чином, щоб обробка, подібна до обробки цифрового сигналу мікропроцесором у блоці 22 обробки обчислень, мала логічну конфігурацію на основі іншої концепції розробки.

(4) Пристрій 3 CCF та пристрій 2 захисту безпеки розроблені різними розробниками в різних департаментах, таким чином, щоб мати різні концепції розробок та забезпечувати захист на основі різних логічних конфігурацій, відповідно.

Сигнал запиту на операцію, сформований логікою 312 захисту безпеки, на локальний компонент 4 системи безпеки, передається на вихідний пристрій 23 пристрою 2 захисту безпеки від шостої схеми 313 керування передачею даних, яка розташована на виході із блоку 31 обробки обчислень. Переданий сигнал запиту на операцію отримується восьмою схемою 235 керування передачею даних для пристрою 3 CCF і потім перетворюється на аналоговий сигнал за допомогою схеми 234 Ц/А перетворення для пристрою 3 CCF, а потім аналоговий сигнал виводиться на схему 236 АЗ.

Схема 232 Ц/А перетворення та схема 234 Ц/А перетворення, відповідно, складаються із схем або пристроїв (частин), що відрізняються один від одного, та реалізовані ними. Подібним чином, сьома схема 231 керування передачею даних та восьма схема 235 керування передачею даних, відповідно, складаються із схем або частин, що відрізняються одна від одної. Крім того, в якості протоколу передачі даних між шостою схемою 313 керування передачею даних та восьмою схемою 235 керування передачею даних застосовується протокол передачі даних, що відрізняється від протоколу передачі даних між п'ятою схемою 223 керування передачею даних та сьомою схемою 231 керування передачею даних.

Резервний пристрій системи захисту безпеки сконфігурований, як описано вище, в результаті чого вхідний пристрій та вихідний пристрій можуть бути спільними для обладнання захисту безпеки та для пристрою CCF. Таким чином, не потрібно забезпечувати вхідний пристрій та вихідний пристрій окремо для пристрою CCF, і при цьому збільшувати кількість детекторів та локальних компонентів системи безпеки також можна без збільшення масштабу пристрою CCF.

Варіант здійснення 2

В конфігурації варіанту здійснення 1, застосовуються схема 24 фотоелектричного (Е/О) перетворення, яка перетворює електричний сигнал, переданий від другої схеми 214 керування передачею даних пристрою 2 захисту безпеки, на оптичний сигнал, і схема 32 О/Е перетворення, яка перетворює оптичний сигнал, отриманий пристроєм CCF, на електричний сигнал.

Подібним чином, застосовуються схема 33 Е/О перетворення, яка перетворює вихідний сигнал шостої схеми 313 керування передачею даних пристрою 3 CCF на оптичний сигнал, і схема 25 О/Е перетворення, яка перетворює сигнал, отриманий пристроєм 2 захисту безпеки, на електричний сигнал.

Таким чином, між пристроєм 2 захисту безпеки та пристроєм 3 CCF передаються та отримуються оптичні сигнали, завдяки чому, у випадку, коли в пристрої 3 CCF сталась електрична несправність або подібне, то вплив відмови упереджується від поширення на пристрій 2 захисту безпеки. Крім того, оскільки сигнали передаються через оптичні кабелі, то відстань передачі може бути збільшена порівняно із випадком, коли використовуються електричні сигнали, і обмежувальна умова стосовно місця встановлення пристрою 3 CCF може пом'якшуватись.

Як описано вище, в конфігурації варіанту здійснення 2, пристрій CCF з'єднаний із вхідним пристроєм та із вихідним пристроєм через оптичні кабелі, завдяки чому можна запобігти впливу електричної несправності в пристрої CCF на систему захисту безпеки, і при цьому не потрібно забезпечувати роздільний пристрій.

Варіант здійснення 3

Як показано на ФІГ. 3, в конфігурації варіанту здійснення 1 або варіанту здійснення 2, сигнали виявлення від ряду детекторів 11, 12, 13 передаються на пристрій 2 захисту безпеки, який являє собою обладнання системи захисту. Передані сигнали виявлення вводяться у вхідні пристрої 2101, 2102, 2103 пристрою 2 захисту безпеки, та електрично розподіляються у вхідних пристроях 2101, 2102, 2103. Сигнали, що розподіляються на одну сторону, вводяться у схеми

211a, 211b, 211c A/Ц перетворення пристрою 2 захисту безпеки, і сигнали, що розподіляються на іншу сторону, вводяться у схеми 212a, 212b, 212c A/Ц перетворення для пристрою 3 CCF. Вихідні сигнали від схем 212a, 212b, 212c A/Ц перетворення вводяться у схеми 26a, 26b, 26c повторювачів, кожна із яких при цьому має функцію агрегації сигналів, через ряд других схем 214a, 214b, 214c керування передачею даних, відповідно. Схеми 26a, 26b, 26c повторювачів, кожна із яких являє собою електричну схему підсилення, яка включає в себе мультиплексор, двопортовий запам'ятовуючий пристрій, та подібне. Підсилені сигнали передаються на пристрій 3 CCF через схему 24 E/O перетворення. У випадку такої конфігурації, сигнали виявлення від ряду детекторів 11, 12, 13 можуть передаватись на пристрій 3 CCF без збільшення кількості ліній передач. У цьому варіанті здійснення показано приклад, у якому сигнали від трьох детекторів вводяться до трьох вхідних пристроїв, однак кількість детекторів та кількість вхідних пристроїв цим не обмежується.

Варіант здійснення 4

Як показано на ФІГ. 4, сигнали виявлення, передані від детекторів 11, 12, 13, відповідно, вводяться у ряд вхідних пристроїв 2101, 2102, 2103, та електрично розподіляються у вхідних пристроях 2101, 2102, 2103. Сигнали, що розподіляються на одну сторону, вводяться у схеми 211a, 211b, 211c A/Ц перетворення пристрою 2 захисту безпеки, і сигнали, що розподіляються на іншу сторону, вводяться до схеми 212 A/Ц перетворення для пристрою 3 CCF в одному вхідному пристрої (наприклад, у вхідному пристрої 2101). Вихідний сигнал від схеми 212 A/Ц перетворення вводиться у схему 26 повторювача через другу схему 214 керування передачею даних. Сигнал, підсилений схемою 26 повторювача, передається на пристрій 3 CCF через схему 24 E/O перетворення. Таким чином, схеми A/Ц перетворення для пристрою 3 CCF у двох вхідних пристроях 2102, 2103, другі схеми керування передачею даних, а також схеми повторювачів не потрібні, і вхідний пристрій можна зменшити в розмірі. У цьому варіанті здійснення, показано приклад, у якому сигнали від трьох детекторів вводяться до трьох вхідних пристроїв, однак кількість детекторів та кількість вхідних пристроїв цим не обмежується. Крім того, у цьому варіанті здійснення показано приклад, у якому схема A/Ц перетворення, друга схема керування передачею даних, та схема повторювача, розташовані в одному вхідному пристрої, використовуються спільно із іншими вхідними пристроями, однак лише схема A/Ц перетворення або схема A/Ц перетворення і друга схема керування передачею даних можуть бути спільними.

Один із прикладів апаратних засобів логік 222, 312 захисту безпеки показано на ФІГ. 5. Як описано вище, кожна із логік 222, 312 захисту безпеки складається із мікропроцесора 50 та накопичуючого пристрою 60. Хоча це не показано, накопичуючий пристрій 60 включає в себе енергозалежний накопичуючий пристрій, такий як оперативний запам'ятовуючий пристрій, та енергонезалежний допоміжний накопичуючий пристрій, такий як постійний запам'ятовуючий пристрій, що електрично перепрограмовується. Накопичуючий пристрій 60 може включати в себе допоміжний накопичуючий пристрій, такий як жорсткий диск, замість постійного запам'ятовуючого пристрою, що електрично перепрограмовується. Мікропроцесор 50 виконує прикладне програмне забезпечення, завантажуваче із накопичуючого пристрою 60. У цьому випадку, програма завантажується на мікропроцесор 50 через енергозалежний накопичуючий пристрій із допоміжного накопичуючого пристрою. Мікропроцесор 50 може виводити дані, такі як результат обчислень, в енергозалежний накопичуючий пристрій накопичуючого пристрою 60, або зберігати такі дані в допоміжний накопичуючий пристрій через енергозалежний накопичуючий пристрій. В якості апаратних засобів логіки 312 захисту безпеки, замість мікропроцесора може застосовуватись ПЛІС, як описано вище.

Хоча винахід описано вище з точки зору різних примірних варіантів здійснення та реалізацій, необхідно розуміти, що різні ознаки, аспекти, та функціональні можливості, описані в одному або в декількох окремих варіантах здійснення, не обмежуються у своїй застосовності конкретним варіантом здійснення, відповідно до якого вони описані, а замість цього можуть застосовуватись окремо або в різних комбінаціях до одного або декількох варіантів здійснення винаходу.

Таким чином, необхідно розуміти, що при цьому можуть бути розроблені численні модифікації, які не були приведені в якості прикладу, не виходячи за межі цього винаходу. Наприклад, принаймні один із складових компонентів може бути модифікований, доданий, або вилучений. Принаймні один із складових компонентів, згаданих принаймні у одному із переважних варіантів здійснення, може вибиратись та комбінуватись із складовими компонентами, згаданими в іншому переважному варіанті здійснення.

ОПИС ПОСИЛАЛЬНИХ ПОЗНАЧЕНЬ

1, 11, 12, 13 детектор

	2 пристрій захисту безпеки
	3 пристрій CCF
	4 локальний компонент системи безпеки
	21, 2101, 2102, 2103 вхідний пристрій
5	22 блок обробки обчислень
	23 вихідний пристрій
	24 схема Е/О перетворення
	25 схема О/Е перетворення
	26, 26a, 26b, 26c схема повторювача
10	31 блок обробки обчислень
	32 схема О/Е перетворення
	33 схема Е/О перетворення
	50 мікропроцесор
	60 накопичуючий пристрій
15	211, 211a, 211b, 211c, 212, 212a, 212b, 212c схема А/Ц перетворення
	213 перша схема керування передачею даних
	214, 214a, 214b, 214c друга схема керування передачею даних
	221 третя схема керування передачею даних
	222 логіка захисту безпеки
20	223 п'ята схема керування передачею даних
	231 сьома схема керування передачею даних
	232, 234 схема Ц/А перетворення
	235 восьма схема керування передачею даних
	236 схема АЗ
25	311 четверта схема керування передачею даних
	312 логіка захисту безпеки
	313 шоста схема керування передачею даних

ФОРМУЛА ВИНАХОДУ

30	1. Резервний пристрій системи захисту безпеки, виконаний з можливістю виявлення стану електростанції, який у разі виявлення несправності здатний видавати команду локальному компоненту системи безпеки відповідно до вихідного сигналу першої логіки захисту безпеки у пристрої захисту безпеки, а у разі виявлення у пристрої захисту безпеки відмови із загальних причин здатний видавати команду локальному компоненту системи безпеки відповідно до вихідного сигналу другої логіки захисту безпеки в пристрої CCF, причому система захисту безпеки містить:
	детектор, виконаний з можливістю виявлення стану електростанції;
	першу та другу схеми аналого-цифрового перетворення, які розташовані у вхідному пристрої
40	пристрою захисту безпеки та здатні виконувати цифрові перетворення вихідного сигналу детектора;
	першу схему керування передачею даних, яка розташована у вхідному пристрої та здатна передавати на блок обробки обчислень сигнал із першої схеми аналого-цифрового перетворення;
45	другу схему керування передачею даних, яка розташована у вхідному пристрої та здатна передавати на пристрій CCF сигнал із другої схеми аналого-цифрового перетворення;
	третю схему керування передачею даних, яка розташована у першому блоці обробки обчислень пристрою захисту безпеки та здатна отримувати вихідний сигнал першої схеми керування передачею даних і передавати вихідний сигнал до першої логіки захисту безпеки блока обробки
50	обчислень;
	четверту схему керування передачею даних, яка здатна отримувати вихідний сигнал другої схеми керування передачею даних та передавати вихідний сигнал до другої логіки захисту безпеки, розташованої у другому блоці обробки обчислень пристрою CCF;
	п'яту схему керування передачею даних, яка розташована у першому блоці обробки обчислень
55	та здатна передавати вихідний сигнал першої логіки захисту безпеки;
	шосту схему керування передачею даних, яка розташована у другому блоці обробки обчислень та здатна передавати вихідний сигнал другої логіки захисту безпеки;
	сьому схему керування передачею даних, яка здатна отримувати сигнал, переданий від п'ятої схеми керування передачею даних, і розташована в області вихідного пристрою пристрою
60	захисту безпеки;

- восьму схему керування передачею даних, яка здатна отримувати сигнал, переданий від шостої схеми керування передачею даних, і розташована в області вихідного пристрою;
 першу схему цифро-аналогового перетворення, яка розташована в області вихідного пристрою та здатна виконувати аналогове перетворення сигналу сьомої схеми керування передачею даних;
 другу схему цифро-аналогового перетворення, яка розташована в області вихідного пристрою та здатна виконувати аналогове перетворення сигналу восьмої схеми керування передачею даних; і
 схему апаратних засобів, яка виконана з можливістю введення до неї сигналу першої або другої схеми цифро-аналогового перетворення, і здатна виконувати виведення на локальний компонент системи безпеки, причому
 перша логіка захисту безпеки та друга логіка захисту безпеки здатні виконувати обробку цифрових сигналів на основі логічних конфігурацій, що відрізняються одна від одної,
 перша схема аналого-цифрового перетворення та друга схема аналого-цифрового перетворення складаються із схем або частин, що відрізняються одна від одної,
 перша схема цифро-аналогового перетворення та друга схема цифро-аналогового перетворення складаються із схем або частин, що відрізняються одна від одної,
 протокол передачі даних між першою схемою керування передачею даних та третьою схемою керування передачею даних відрізняється від протоколу передачі даних між другою схемою керування передачею даних та четвертою схемою керування передачею даних, і
 протокол передачі даних між п'ятою схемою керування передачею даних та сьомою схемою керування передачею даних відрізняється від протоколу передачі даних між шостою схемою керування передачею даних та восьмою схемою керування передачею даних.
2. Резервний пристрій системи захисту безпеки за п. 1, причому
 перша фотоелектрична схема перетворення підключена до каскаду, розташованого за другою схемою керування передачею даних,
 друга фотоелектрична схема перетворення підключена до каскаду, що передуює четвертій схемі керування передачею даних,
 перша фотоелектрична схема перетворення та друга фотоелектрична схема перетворення з'єднані оптоволоконним кабелем,
 третя фотоелектрична схема перетворення підключена до каскаду, розташованого за шостою схемою керування передачею даних,
 четверта фотоелектрична схема перетворення підключена до каскаду, що передуює восьмій схемі керування передачею даних, і
 третя фотоелектрична схема перетворення та четверта фотоелектрична схема перетворення з'єднані оптоволоконним кабелем.
3. Резервний пристрій системи захисту безпеки за п. 1 або 2, причому
 у разі цифрових перетворень вихідних сигналів ряду детекторів за допомогою ряду других схем аналого-цифрового перетворення, розташованих в ряді вхідних пристроїв, з наступною передачею на пристрій CCF через ряд других схем керування передачею даних, вихідні сигнали від ряду других схем керування передачею даних здатні передаватися через схеми повторювачів.
4. Резервний пристрій системи захисту безпеки за п. 1 або 2, причому
 у разі введення вхідних сигналів ряду детекторів на ряд вхідних пристроїв з наступною передачею на пристрій CCF, вихідні сигнали ряду детекторів здатні перетворюватися за допомогою другої схеми аналого-цифрового перетворення, розташованої в одному із вхідних пристроїв.

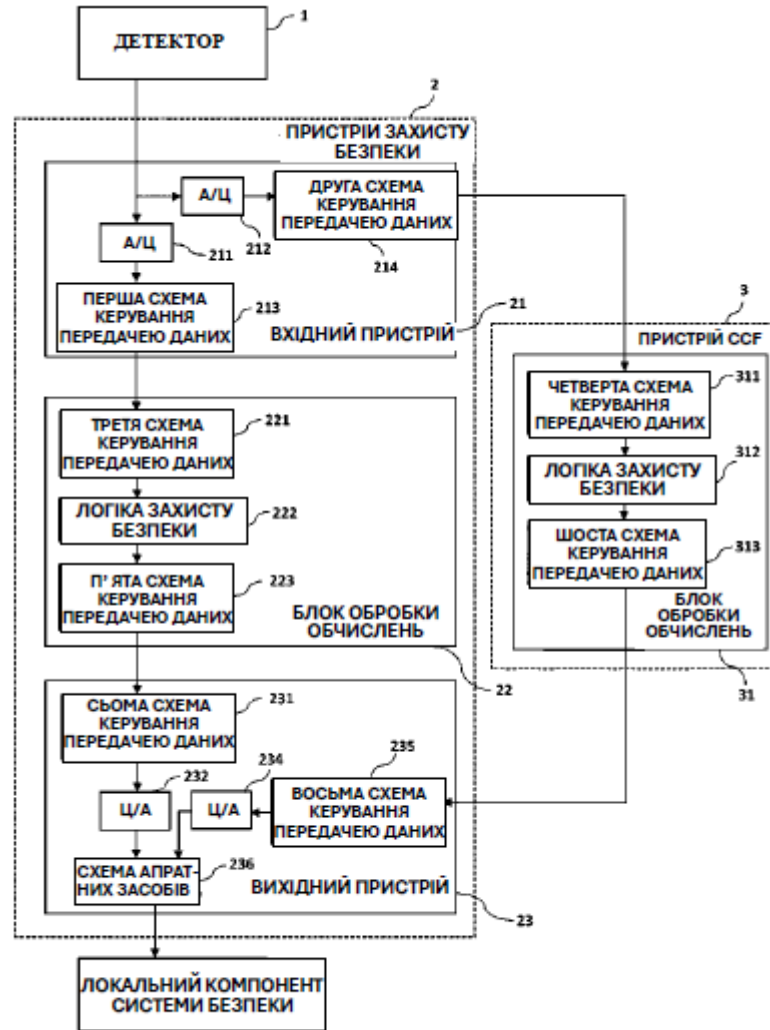
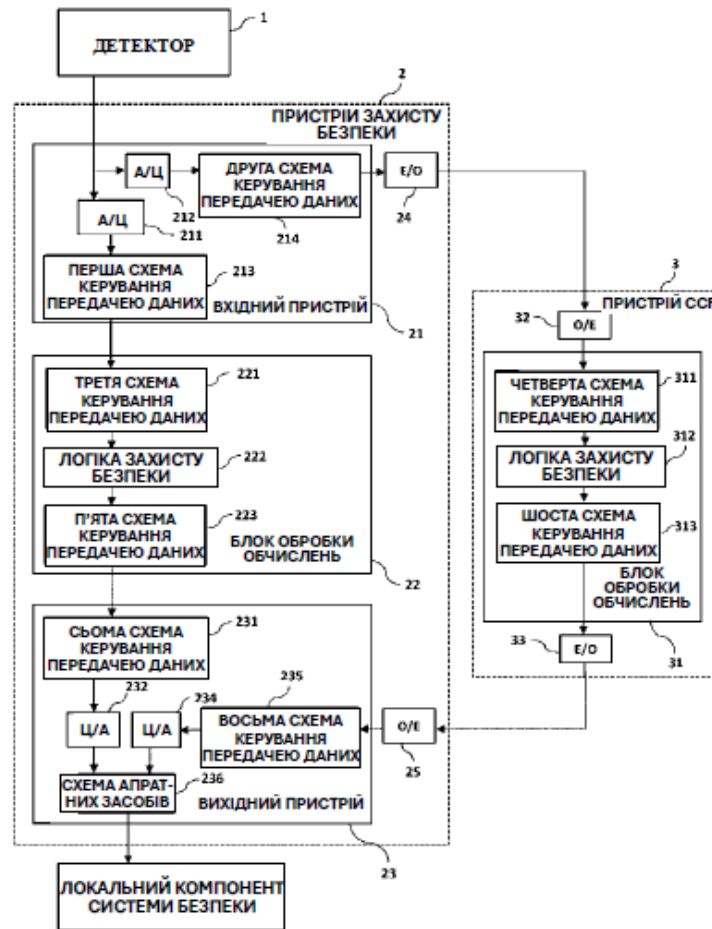
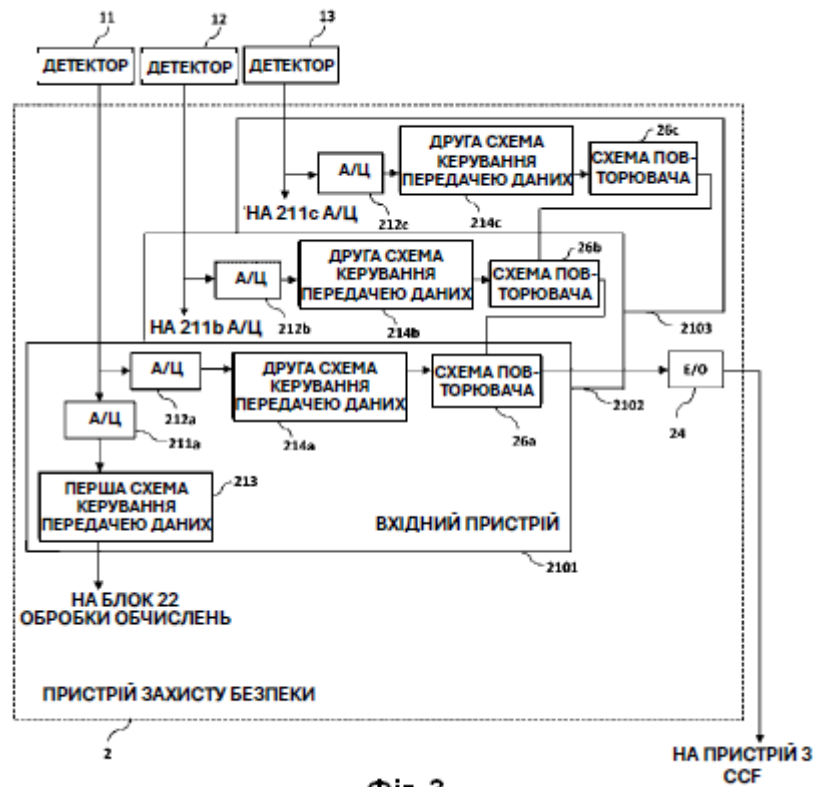


Fig. 1



Фиг. 2



Фиг. 3

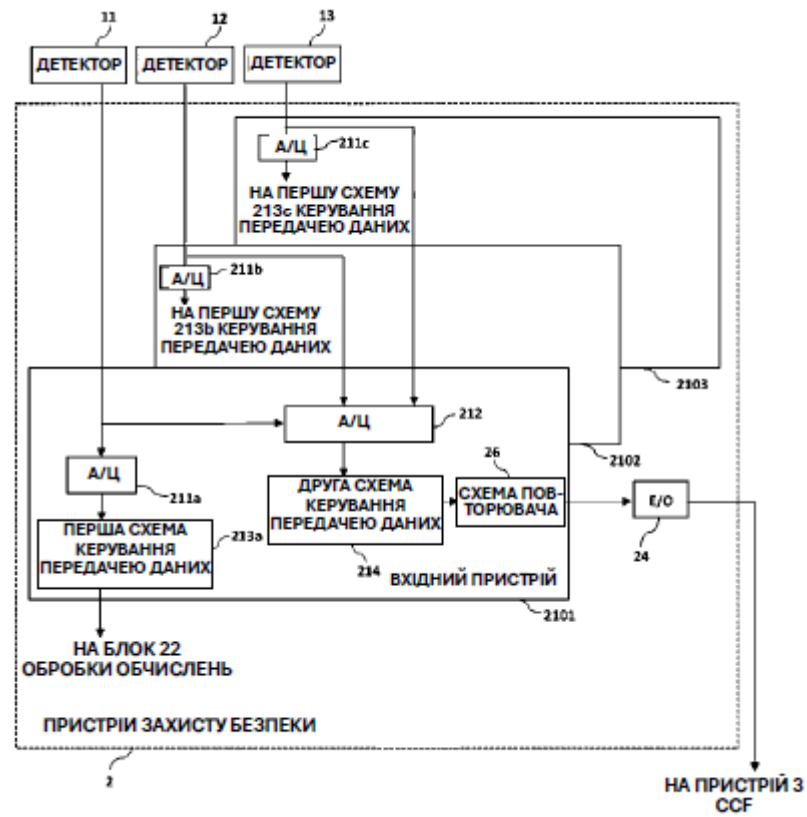


Fig. 4

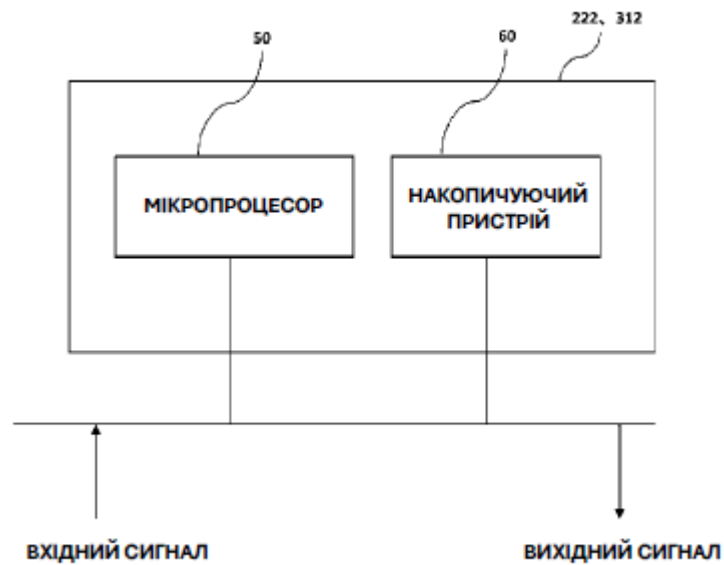


Fig. 5