МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІНЖЕНЕРНО-ТЕХНІЧНИЙ ФАКУЛЬТЕТ
КАФЕДРА ПРИЛАДОБУДУВАННЯ

ДО ЗАХИСТУ ДОПУЩЕНО

Завідувач кафедри

_____

Ігор ЧИЧУРА

«___» _____ 2024 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної магістерської роботи

на тему:

ОХОРОННА СИСТЕМА СКЛАДСЬКОГО ПРИМІЩЕННЯ НА ПЛК

Виконав:

Сергій ХИЛЯ _____
(ім'я та прізвищеі) (підпис)

Керівник:

к. ф.-м.наук, Михайло РЯБОЩУК _____
(вчене звання, ім'я та прізвище) (підпис)

Ужгород – 2024

РЕФЕРАТ

Пояснювальна записка магістерської роботи: 62 сторінки, 19 рисунки, 1 таблиця, 9 джерел.

ОХОРОННА СИСТЕМА, ПЛК, ІНТЕГРАЦІЯ, АВТОМАТИЗАЦІЯ

Об'єкт дослідження – автоматизована система охорони із функцією сповіщення через GSM-мережу на основі програмованого логічного контролера Siemens S7-1200 для застосування у складських приміщеннях.

Мета роботи – спроектувати автоматизовану систему охорони для складського приміщення, що забезпечує багатозональний контроль доступу, моніторинг потенційних загроз і інтеграцію з іншими системами управління складом.

Методи дослідження – аналіз сучасних охоронних систем, що використовують ПЛК; оцінка можливостей і характеристик Siemens S7-1200 для реалізації функцій безпеки; розробка структурної та принципової схем охоронної системи; створення алгоритмів для автоматизації процесів охорони та сповіщення.

Опис виконаної роботи – проведено аналіз існуючих охоронних систем для складських приміщень, особливостей їх компонентів та алгоритмів роботи. На основі отриманих даних підібрано необхідне обладнання, включно з датчиками руху, відкривання дверей, температури та модулем GSM для передачі сповіщень. Розроблено структурну та принципову схеми автоматизованої системи охорони, що передбачають використання Siemens S7-1200 для обробки даних і керування компонентами. Створено алгоритм роботи системи, який забезпечує своєчасне реагування на потенційні загрози та надсилання сповіщень відповідальним особам.

ABSTRACT

The explanatory note of the master's thesis: 62 pages, 19 figures, 1 table, 9 references.

SECURITY SYSTEM, PLC, INTEGRATION, AUTOMATION

The object of the research is an automated security system with a notification function via a GSM network based on the Siemens S7-1200 programmable logic controller for use in warehouse premises.

The aim of the work is to design an automated security system for a warehouse, ensuring multi-zone access control, threat monitoring, and integration with other warehouse management systems.

The research methods include the analysis of modern security systems using PLCs; evaluation of the capabilities and characteristics of Siemens S7-1200 for implementing security functions; development of structural and schematic diagrams of the security system; creation of algorithms for automating security and notification processes.

Description of the work performed: an analysis of existing security systems for warehouse premises, their components, and operation algorithms was conducted. Based on the results of the analysis, the necessary equipment was selected, including motion sensors, door opening detectors, temperature sensors, and a GSM module for sending notifications. Structural and schematic diagrams of the automated security system were developed, featuring the use of Siemens S7-1200 for data processing and component control. An algorithm for the system's operation was created, ensuring timely response to potential threats and sending notifications to responsible personnel.

Ужгородський національний університет

Інженерно-технічний факультет
Кафедра приладобудування
Освітньо-кваліфікаційний рівень "магістр"
Спеціальність 174 Автоматизація, комп'ютерно-інтегровані технології та робототехніка

ЗАТВЕРДЖУЮ
Завідувач кафедри
к.ф.-м.н., доцент Ігор ЧИЧУРА

_____
"___"_____ 2024 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

_____Хилі Сергію Олексійовичу_____
(прізвище, ім'я, по батькові)

1. Тема роботи «Охоронна система складського приміщення на ПЛК»
та керівник роботи Рябощук Михайло Михайлович, к.ф-м.н.,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені Розпорядженням № __ по ІТФ від _____ 2024 року.

2. Термін подання студентом роботи на кафедру: "05" грудня 2024 року.

3. Вихідні дані до роботи: об'єктом розробки є алгоритм системи автоматичного керування процесом вимірювання швидкості хімічного травлення тонких плівок інтерферометричним методом.

Умови експлуатації пристрою:

- температура навколишнього середовища: від 0°C до +60 °C;
- атмосферний тиск: від 720 до 780 мм.рт.ст.;
- відносна вологість повітря: до 95 %;
- електроживлення: 220 В змінного струму з можливістю автономної роботи (резервний акумулятор до 24 годин);
- габарити і маса: мінімально можливі.

Характеристики пристрою:

- ввід базових параметрів керування:вручну при початковій інсталяції пристрою;
- режим керування:неперервний під час експлуатації системи;
- формат вихідних інформаційних сигналів: в залежності від складових системи;
- контроль доступу (реєстрація подій входу/виходу);
- оповіщення про порушення через звукові сигнали та SMS-повідомлення;
- інтеграція з освітленням або іншими системами складського приміщення;
- віддалений моніторинг і управління через мобільний додаток або веб-інтерфейс.

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити):
Аналіз сучасних охоронних систем; визначити набір додаткових функцій для контролю і управління; зробити короткий огляд складових систем охорони; розробка структурної, монтажної та інших необхідних схем системи; розробка алгоритму для охоронної системи.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень):
- структурна схема системи (1 аркуш А3);
- принципова схема системи (1 аркуш А3);
- алгоритм програми системи (1 аркуш А3).

6. Консультанти розділів роботи:

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання: 15 жовтня 2024 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів виконання магістерської роботи	Строк виконання етапів роботи	Примітки
1	Аналіз сучасних систем охорони	30.10.2024	
2	Огляд аналогів охоронних систем із використанням ПЛК	10.11.2024	
3	Аналіз завдання та розробка структурної схеми системи	10.11.2024	
4	Вибір фізичної моделі вимірювань.	20.11.2024	
5	Підбір елементів та виготовлення креслень основних схем системи	20.11.2024	
6	Розробка алгоритму роботи охоронної системи	30.11.2024	
7	Написання пояснювальної записки	30.11.2024	
8	Оформлення роботи та креслень.	05.12.2024	

Студент _____ /_____/
(підпис) (ініціали та прізвище)

Керівник роботи _____ /_____/
(підпис) (ініціали та прізвище)

Зміст

ПЕРЕЛІК СКОРОЧЕНЬ ТА УМОВНИХ ПОЗНАЧЕНЬ

ПЛК – програмованих логічних контролерів

IoT – інтернет речей (англ. Internet of Things)

GSM – глобальна система мобільного зв'язку (англ. Global System for Mobile)

IP - «інтернет протокол» (від англ. Internet Protocol)

°C – градуси Цельсія

% – відсотки

ВСТУП

Сучасний розвиток промисловості та логістики вимагає підвищеної уваги до безпеки складських приміщень. Склади, як місця зберігання матеріальних цінностей, часто є об'єктами ризику через можливість несанкціонованого доступу, крадіжок, пошкоджень або небезпек, пов'язаних із пожежами та іншими надзвичайними ситуаціями. Забезпечення комплексної охорони складських об'єктів є важливою складовою не лише економічної безпеки компаній, але й їхньої репутації.

Інтеграція новітніх технологій у системи охорони дозволяє суттєво підвищити їх ефективність. Використання програмованих логічних контролерів (ПЛК) для автоматизації процесів забезпечення безпеки відкриває широкі можливості для створення надійних, адаптивних та економічно доцільних рішень. Сучасні ПЛК здатні об'єднувати у єдину систему різноманітні датчики, засоби оповіщення та канали зв'язку, що забезпечує комплексний контроль за станом об'єкта в режимі реального часу [1].

Охоронна система на основі ПЛК пропонує значні переваги у порівнянні з традиційними підходами. Вона дозволяє автоматизувати виявлення загроз, миттєво реагувати на них та оперативно передавати інформацію відповідальним особам. Такі системи здатні працювати в умовах різного ступеня складності: від контролю входів і периметру до моніторингу внутрішніх зон та інтеграції з іншими технологічними процесами складу.

Особливістю складських приміщень є їхня багатозональність, яка потребує диференційованого підходу до охорони. Залежно від функціонального призначення зон (зберігання, завантаження, технічні приміщення тощо).

1 АНАЛІЗ СУЧАСНИХ ОХОРОННИХ СИСТЕМ

Сучасні охоронні системи є невід'ємною частиною забезпечення безпеки в багатьох сферах діяльності, особливо коли мова йде про складські приміщення. З розвитком технологій охоронні системи стали значно більш складними, інтегрованими та адаптованими до потреб різних об’єктів. Особливу увагу приділяють автоматизації, яка дозволяє мінімізувати вплив людського фактора, підвищуючи ефективність системи в цілому.

Еволюція охоронних систем проходила в кілька етапів, кожен із яких приніс нові можливості. У перші роки акцент був зроблений на механічних засобах, таких як замки та решітки, які забезпечували базовий рівень захисту. Згодом з'явилися електромеханічні системи з простими датчиками, які могли виявляти рух чи відкриття дверей. Це стало важливим кроком у напрямку автоматизації. Однак лише з розвитком цифрових технологій охоронні системи змогли перейти на новий рівень. Сьогодні вони інтегрують програмовані логічні контролери (ПЛК), IoT-рішення, штучний інтелект і хмарні технології, що забезпечує багатофункціональність і високу адаптивність.

Основним завданням сучасної охоронної системи є не лише виявлення загроз, але й їх попередження, аналіз ситуації та оперативне реагування. Наприклад, складське приміщення, яке включає кілька зон з різним рівнем доступу, потребує комплексної системи, здатної контролювати периметр, фіксувати переміщення людей та товарів, а також своєчасно інформувати користувачів про будь-які аномалії.

Особливо важливим елементом сучасних систем є програмовані логічні контролери. Вони забезпечують централізоване управління всіма компонентами, дозволяючи легко налаштовувати сценарії роботи для конкретних умов. Наприклад, у разі спрацювання датчика руху ПЛК може автоматично активувати сирену, надіслати повідомлення відповідальному персоналу та заблокувати

доступ до певних зон. Це дозволяє значно підвищити рівень безпеки без участі людини.

Іншим важливим аспектом є інтеграція систем із сучасними технологіями. IoT-рішення дозволяють поєднувати всі компоненти системи в єдину мережу, забезпечуючи швидкий обмін даними між ними. Завдяки цьому система може автоматично реагувати на загрози: наприклад, при спрацюванні датчика в зоні складу активується камера, яка передає зображення на мобільний пристрій користувача. Штучний інтелект, у свою чергу, використовується для аналізу відео, розпізнавання облич чи номерних знаків, що особливо важливо для складських приміщень із високою пропускною здатністю.

Хмарні сервіси також відкривають нові можливості для сучасних систем охорони. Вони дозволяють зберігати великі обсяги даних і забезпечувати доступ до них з будь-якого пристрою в режимі реального часу. Це особливо зручно для великих складських комплексів, де необхідно відстежувати ситуацію на кількох об'єктах одночасно.

Особливу увагу варто приділити системам сповіщення. Завдяки використанню GSM-модулів система може надсилати повідомлення про загрози безпосередньо на мобільні пристрої користувачів. Крім того, інтеграція з мобільними додатками дозволяє дистанційно керувати системою, наприклад, активувати чи деактивувати окремі її компоненти.

Загальні принципи роботи охоронних систем

Охоронні системи забезпечують захист об’єкта шляхом виявлення, запобігання та реагування на потенційні загрози. Їх функціонування базується на трьох основних етапах:

1. Виявлення загрози: за допомогою датчиків руху, відкривання дверей/вікон, камер відеоспостереження чи інших сенсорів.

2. Обробка сигналу: отримання, аналіз і класифікація подій, що надходять від датчиків, за допомогою центрального контролера (ПЛК, сервер).

3. Реакція на загрозу: запуск звукових чи світлових оповіщувачів, блокування доступу, передача інформації відповідальним особам через мобільний зв’язок або інтернет.

Основні компоненти сучасних охоронних систем

Датчики: датчики руху (інфрачервоні, ультразвукові); контактні датчики для виявлення відкриття дверей чи вікон; датчики диму та температури для виявлення пожеж; комбіновані датчики (рух + розбиття скла).

Контролери: програмовані логічні контролери (ПЛК), що виконують функції аналізу та управління; спеціалізовані мікроконтролери для локальних завдань.

Системи відеоспостереження: камери високої роздільної здатності з підтримкою штучного інтелекту для розпізнавання осіб і аналізу ситуацій; відеосервери для зберігання та обробки даних.

Системи оповіщення: сирени, сигнальні лампи; GSM-модулі для надсилання повідомлень; хмарні платформи для віддаленого доступу.

Програмне забезпечення: інтерфейси для моніторингу та управління; аналітичні інструменти для аналізу відео та інших даних.

Особливості охоронних систем для складських приміщень

Складські приміщення мають специфічні особливості, які вимагають спеціалізованого підходу до побудови охоронних систем:

1. Різноманітність зон контролю. Зони зберігання товарів, під'їзди для вантажівок, технічні приміщення.

2. Потреба в масштабованості. Можливість додавання нових зон або пристроїв без перебудови системи.

3. Автономність роботи. Забезпечення безпеки навіть у разі відсутності основного джерела живлення.

4. Інтеграція з іншими системами. Наприклад, автоматизація воріт або контроль за температурним режимом у зоні зберігання.

Аналіз сучасних технологій

IoT-технології. Об’єднання всіх компонентів системи у мережу, що дозволяє здійснювати автоматизоване управління та аналіз даних. Приклад: автоматичне сповіщення про загрози, передача сигналу до централізованої системи моніторингу.

Штучний інтелект і машинне навчання. Використовуються для аналізу відео, прогнозування можливих загроз, розпізнавання осіб. Приклад розпізнавання нестандартної поведінки у відеопотоці.

Хмарні технології. Дозволяють зберігати великі обсяги даних і забезпечують доступ до них у будь-який час з будь-якого пристрою.

GSM- і IP-системи. Забезпечують передачу даних через мобільний зв’язок або інтернет.

Сучасні охоронні системи є результатом інтеграції технологій, спрямованих на забезпечення безпеки об'єктів. Для складських приміщень актуальним є впровадження масштабованих систем із використанням ПЛК, IoT та інших сучасних рішень. Це дозволить ефективно вирішувати завдання безпеки, враховуючи специфіку кожного об'єкта.

1.1 Огляд існуючих рішень у сфері автоматизації охорони

Сучасний ринок охоронних систем є вкрай різноманітним, пропонуючи рішення для забезпечення безпеки об’єктів будь-якого масштабу та складності. Охоронні системи автоматизації активно впроваджуються як у приватному секторі, так і на комерційних об’єктах, зокрема в складських приміщеннях, де безпека є критичним фактором. У цьому розділі розглянемо основні типи систем, їх компоненти, переваги, недоліки та перспективи розвитку.

Основні типи охоронних систем

Провідні охоронні системи. провідні системи базуються на кабельних з’єднаннях між усіма компонентами. Вони забезпечують високий рівень надійності та захищені від зовнішніх втручань, що робить їх ідеальними для великих об’єктів. До недоліків належать складність встановлення та високі витрати на монтаж, особливо якщо потрібно модернізувати існуючу систему.

Бездротові охоронні системи. Ці системи передають дані через Wi-Fi, ZigBee, або інші протоколи зв’язку. Вони є гнучкими у встановленні та розширенні, проте мають обмеження у вигляді залежності від якості сигналу і регулярного обслуговування батарей.

Гібридні системи. Поєднують провідні та бездротові технології, забезпечуючи баланс між надійністю і гнучкістю. Наприклад, ключові компоненти можуть бути підключені провідним способом, тоді як додаткові пристрої — через бездротовий зв'язок.

Смарт-системи охорони. Інтегрують IoT-рішення, дозволяючи віддалено керувати охоронною системою, отримувати сповіщення та взаємодіяти з іншими компонентами "розумного будинку". Вони є зручними для користувачів, але залежні від стабільності інтернет-з’єднання.

Приклади сучасних охоронних рішень

Ajax Systems. Переваги: простота встановлення, інтеграція з мобільними додатками, доступна вартість. Недоліки: обмеження у масштабованості для великих об’єктів.

Siemens S7-1200. Використовується для автоматизації складних охоронних систем. Переваги: гнучкість, багатофункціональність, інтеграція з іншими системами. Недоліки: вища вартість у порівнянні з простішими рішеннями.

Hikvision. Спеціалізується на системах відеоспостереження з елементами штучного інтелекту. Переваги: аналіз відео, збереження даних у хмарі. Недоліки: залежність від інтернет-з’єднання.

Schneider Electric. Орієнтовані на промислові об’єкти з підвищеними вимогами до безпеки. Переваги: масштабованість, інтеграція з автоматизацією процесів.

Система на основі ПЛК є економічною та швидко адаптованою конструкцією

У багатьох галузях промисловості існує багато машин, які автоматично виконують багато завдань. Відстеження помилок під час робочого процесу та вжиття заходів у разі виникнення надзвичайної ситуації має вирішальне значення для підтримки стабільної роботи [2].

Іноді оператори можуть не визначити проблеми машини чи системи шляхом візуального спостереження. Система сигналізації може вирішити цю

проблему та підвищити ефективність. Сьогодні система сигналізації на основі ПЛК є загальноприйнятою в промисловості масових автоматичних машин.

Системи сигналізації також допомагають виявляти надзвичайні ситуації в різних програмах. Система на основі ПЛК є економічною та швидко адаптованою конструкцією. Перевагами програмованого логічного контролера (ПЛК) є просте підключення, швидка обробка, зручна робота та висока надійність.

Метою системи сигналізації є повідомляти користувачам і відповідним органам влади про будь-яку надзвичайну ситуацію. Виявлення аварійних ситуацій включає охорону, температуру, пожежу тощо. Система сигналізації ідентифікує ці аварійні ситуації за допомогою датчиків, встановлених на контрольних точках. Коли датчик отримав аномальні дані, він негайно відповів, щоб повідомити пов'язаних учасників. Тим часом диспетчерська також може прийняти рішення про надзвичайну ситуацію шляхом систематичного аналізу інформації. Це допомагає, коли система сигналізації впроваджується у великому масштабі середовища.

Системи сигналізації працюють за допомогою датчиків, які надсилають сигнали на центральну станцію моніторингу, коли виявляють щось несправне. Центральний концентратор системи сигналізації в основному розроблений як панель (HMI) , тому користувачі та відповідні органи можуть негайно отримати дані чи інформацію про ситуацію. У той же час система сигналізації повинна реагувати на основі запрограмованих налаштувань і подавати сигнал тривоги.

Коли справа доходить до рішення, який тип контролера найкраще підходить для системи, безсумнівно, система програмованого логічного контролера (PLC) є вашим першим вибором. Вам потрібен лише ПЛК і монолітна інтегральна схема для виконання завдань сигналізації.

Поєднуючи загальну картину того, як працюють системи сигналізації, ми хотіли продовжити обговорення дизайну системи суднової сигналізації на основі ПЛК. Робоча схема приведена на рис. 1.1.

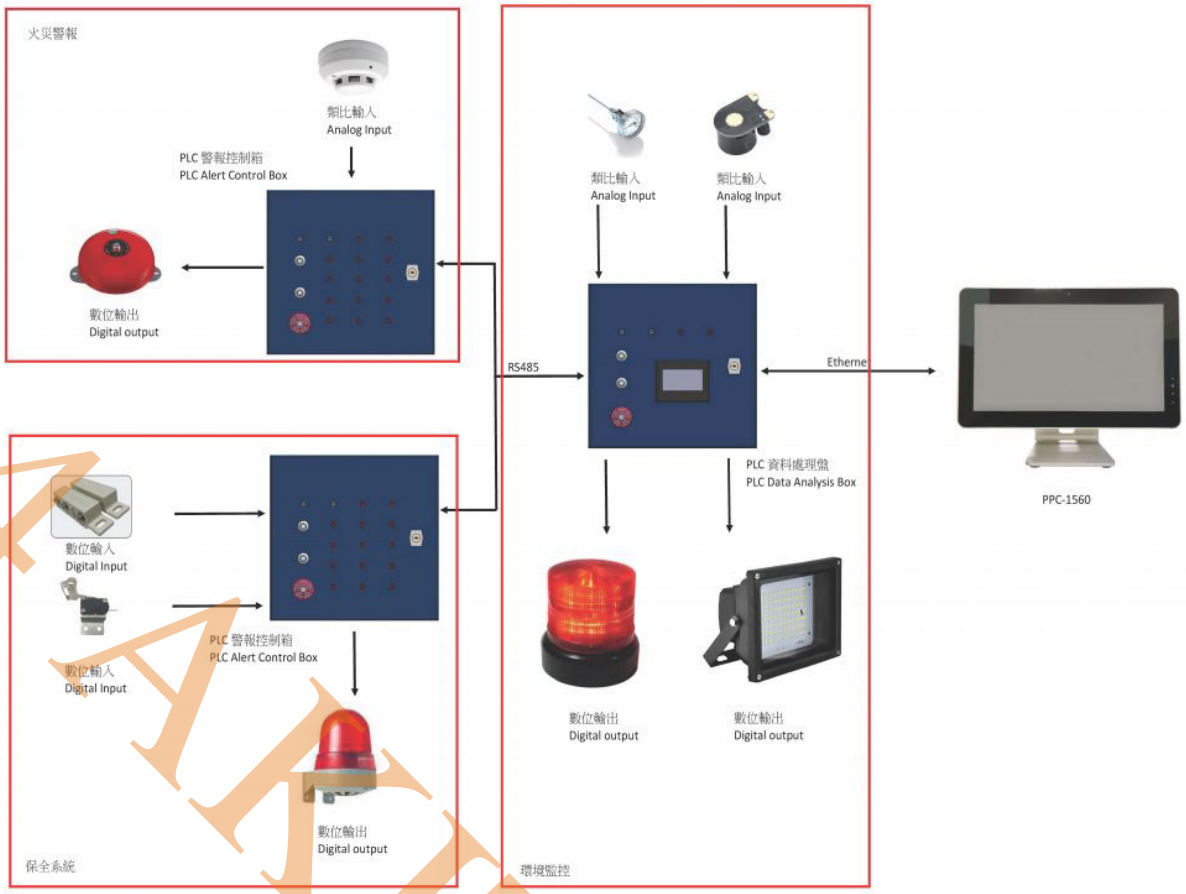


Рисунок 1.1 - Робоча схема системи сигналізації на основі ПЛК [2]

Коли виявляється проблема або небезпека, детектори (сенсори) передають вимірювальні сигнали на термінал керування ПЛК (центральний вузол системи сигналізації). Працівники складу також можуть надсилати сигнали вручну. ПЛК видаватиме керуючі інструкції, аналізуючи операції, які включають звукову та світлову сигналізацію.

Апаратна конструкція є важливою складовою системи контролю сигналізації. Він повинен включати датчики температури, диму, вогню та світла. І пристрої сигналізації, такі як дзвінки та сигнальні лампи. Він також має включати деякі візуальні відображення, щоб користувачі або управління складом могли отримати більше інформації про проблему.

Проектування програмного забезпечення системи сигналізації виконується за наступним алгоритмом рис. 1.2.

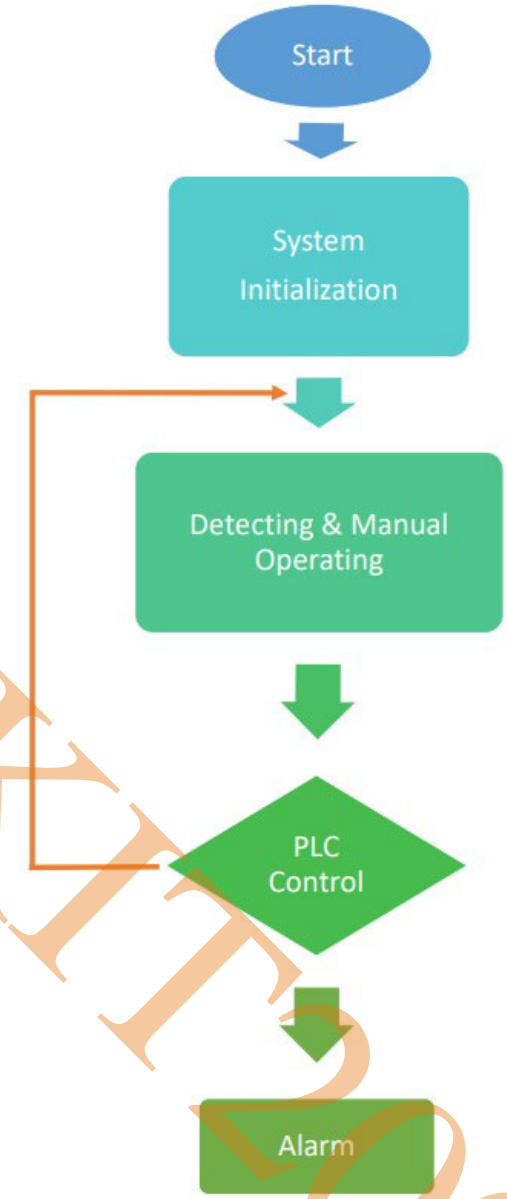


Рисунок 1.2 – Алгоритм роботи системи сигналізації [2]

Добре організований дизайн програмного забезпечення є критичною цінністю. Спроектувати програмне забезпечення означає відповідати всім пунктам, які необхідно контролювати. Таблиця імен контрольних точок необхідна для ідентифікації того, як контрольні точки підключені до терміналів інтерфейсу введення/виведення ПЛК. Таким чином, сигнали можуть бути передані та розпізнані правильно.

Застосування PLC для загальної системи сигналізації

PLC для загальної систем сигналізації. На основі загальної системи програмування ПЛК за допомогою цього прикладу (рис. 1.3).

Охоронна сигналізація

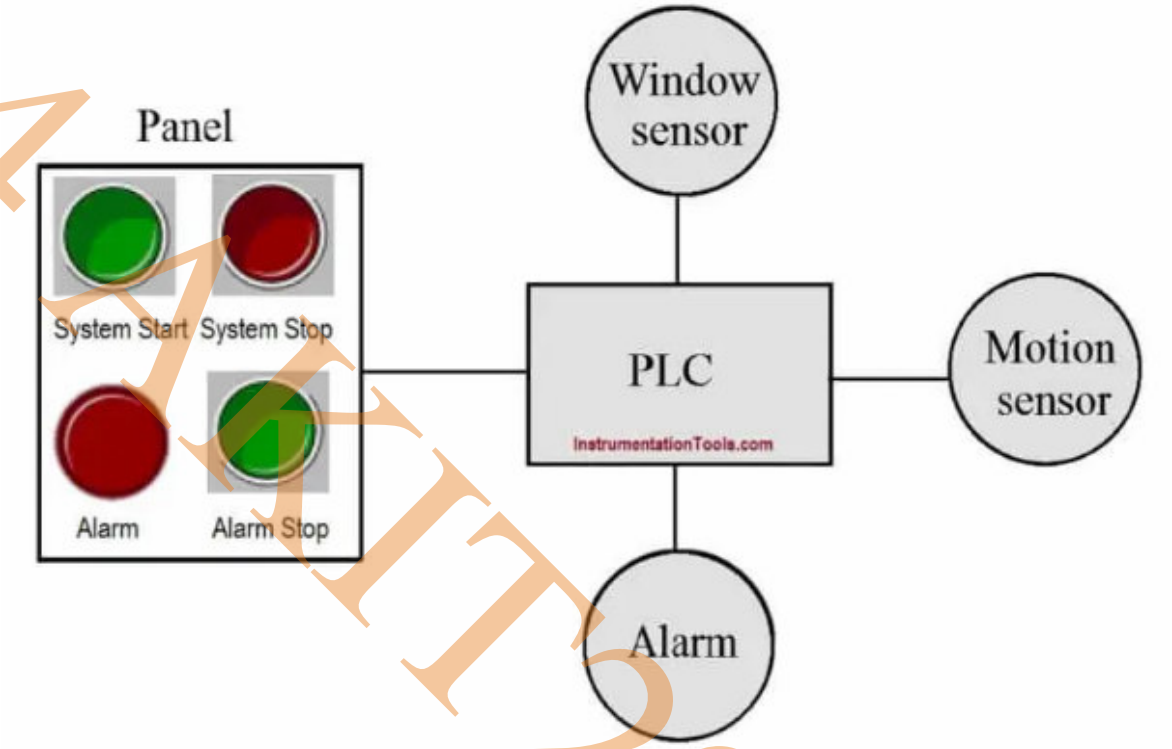


Рисунок 1.3 – Загальної систем сигналізації [3]

Рішення проблеми

Ми можемо вирішити цю проблему, використовуючи просту логіку. Тут ми можемо використовувати два датчики, один датчик руху та другий датчик вікна. Датчик вікон - це петля з проводів.

Датчик руху сконструйований таким чином, що при виявленні людини в будинку або кімнаті датчик спрацьовує (змінює його стан на 1 або 0)

Тут важливий момент у віконному датчику полягає в тому, що струм завжди проходить до тих пір, поки не станеться розбиття скла. Отже, вихід завжди істинний, і коли хтось спробує розбити віконне скло, струм не буде проходити в ланцюзі.

Список входів і виходів

Список входів

Система START:- I0.0

Система STOP:- I0.1

Детектор руху:- I0.2

Датчик вікна:- I0.3

Кнопка зупинки тривоги:- I0.4

Список виходів

Сигналізація: - Q0.0

M Пам'ять

M0.0 : - Головна котушка.

M0.1 :- Сигналізація включена.

Сходова схема PLC для системи безпеки сигналізації (рис. 1.4)

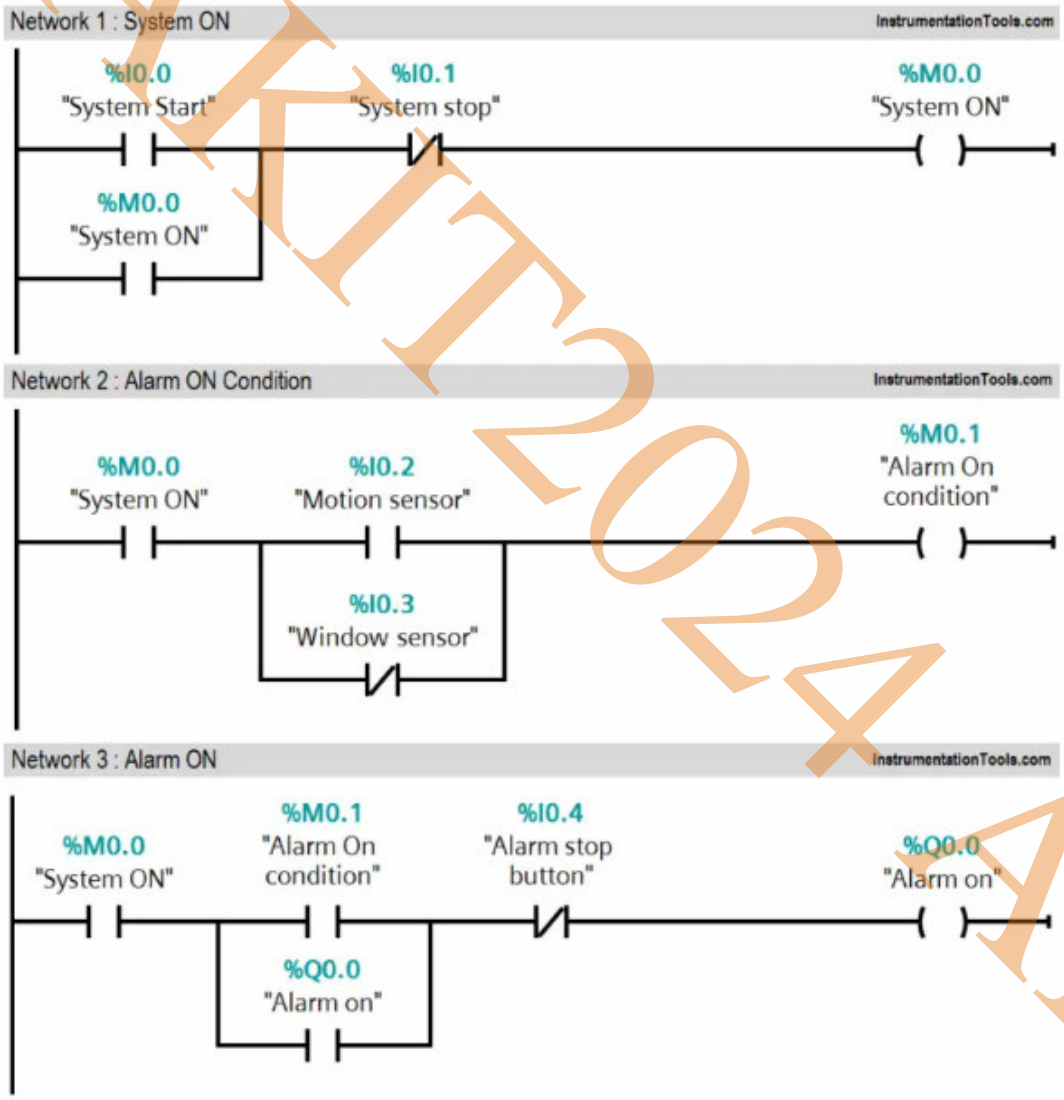


Рисунок 1.4 – Програма загальної систем сигналізації [3]

Опис програми

У цій задачі ми розглянемо ПЛК S7-1200 і програмне забезпечення порталу TIA для програмування.

Мережа 1. Ця мережа показує просту схему фіксації для увімкнення та вимкнення системи. Тут використано нормально відкритий (NO) контакт системної кнопки START (I0.0) і NC контакт системної кнопки STOP (I0.1) для активації системи.

Мережа 2. Коли система активована і датчик руху (I0.2) виявляє вхід людини, стан тривоги (M0.1) буде УВІМКНЕНО, і він активує тривогу (Q0.0).

Зазвичай NC контакт датчика вікна (I0.3) використовується паралельно, тому в нормальних умовах це вірно. Якщо виявлено розбиття скла або стан вікна, вхід датчика вікна (I0.3) стає помилковим і активує стан тривоги (M0.1).

Мережа 3. У цій мережі схема фіксації використовується для тривоги (Q0.0). Якщо виявлено стан тривоги (M0.1), тривога буде увімкнена, і її можна зупинити, натиснувши кнопку тривоги STOP PB (I0.4). Результат приведені на рис. 1.5.

Inputs	Outputs	Physical Elements
I0.0=1 &I0.2=1	Q0.0=1	Alarm ON
I0.0=1&I0.3=0	Q0.0=1	Alarm ON
I0.1=1	M0.0=0	System OFF
I0.4=1	Q0.0=0	Alarm OFF

Рисунок 1.5 – Результати програми загальної систем сигналізації [3]

Застосування PLC для системи сигналізації на складі

Є склад і два входи до нього. Перед кожним входом встановлена система перевірки електронних ключів, оснащена двома (імпульсними релейними виходами, перший із яких - замикається при прикладанні ключа на відкриття, а другий на закриття дверей.

Реалізовано контроль доступу за допомогою електромагнітних замків (YC1 та YC2), а також управління освітленням (лампи EL1) за наступним алгоритмом:

1. Доступ до складу дозволено в робочій час з 08:00 до 19:00. у вихідні дні з 10:00 до 17:00.

2. В середині складу є вимикач (SB1), дозволяє відкрити двері в будь-який час.

3. Освітлення у складі включається, при відкритті дверей, від датчика освітленості BL1 з виходом 0...10В. Недостатній освітленості відповідає значення напруги на виході датчика менше 4,5 В.

4. При відкритті дверей пролунає попереджувальний звуковий сигнал тривалістю 30 секунд скважністю 2, тривалість звучання 5 секунд.

5. При закритті дверей роздається попереджувальний звуковий сигнал тривалістю 60 секунд шпаруватістю 1.5, час звучання 3 секунди.

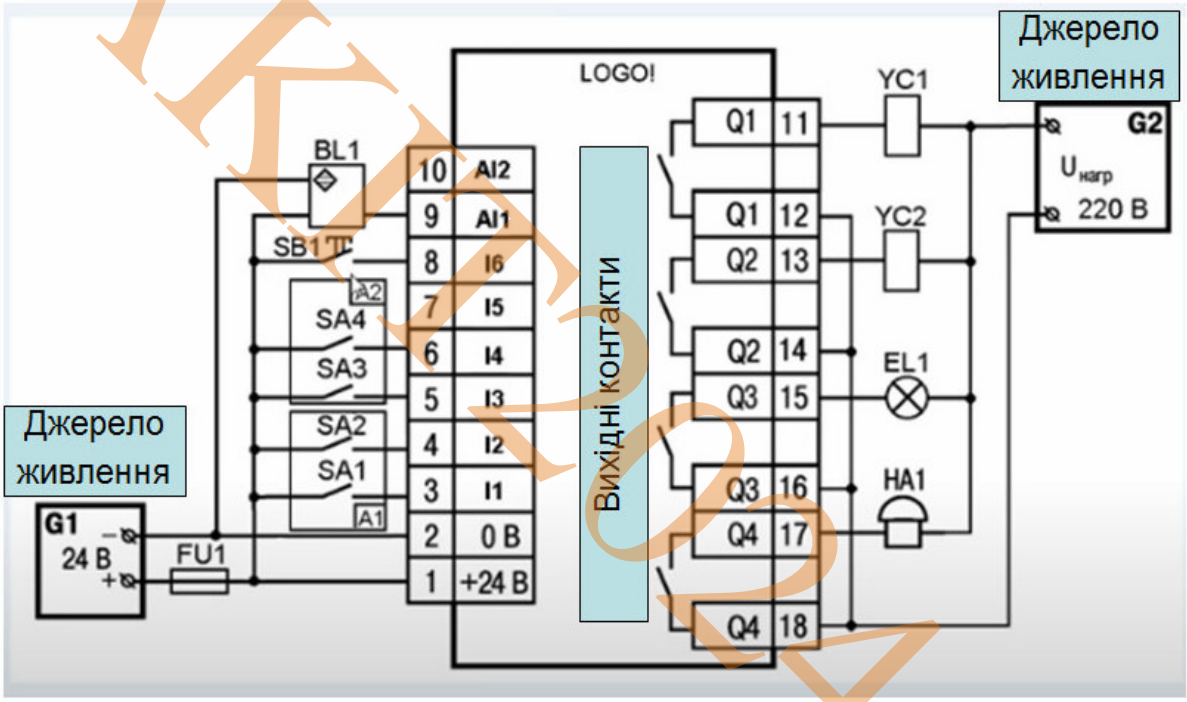


Рисунок 1.6 – Схема зєднання PLC для системи сигналізації на складі

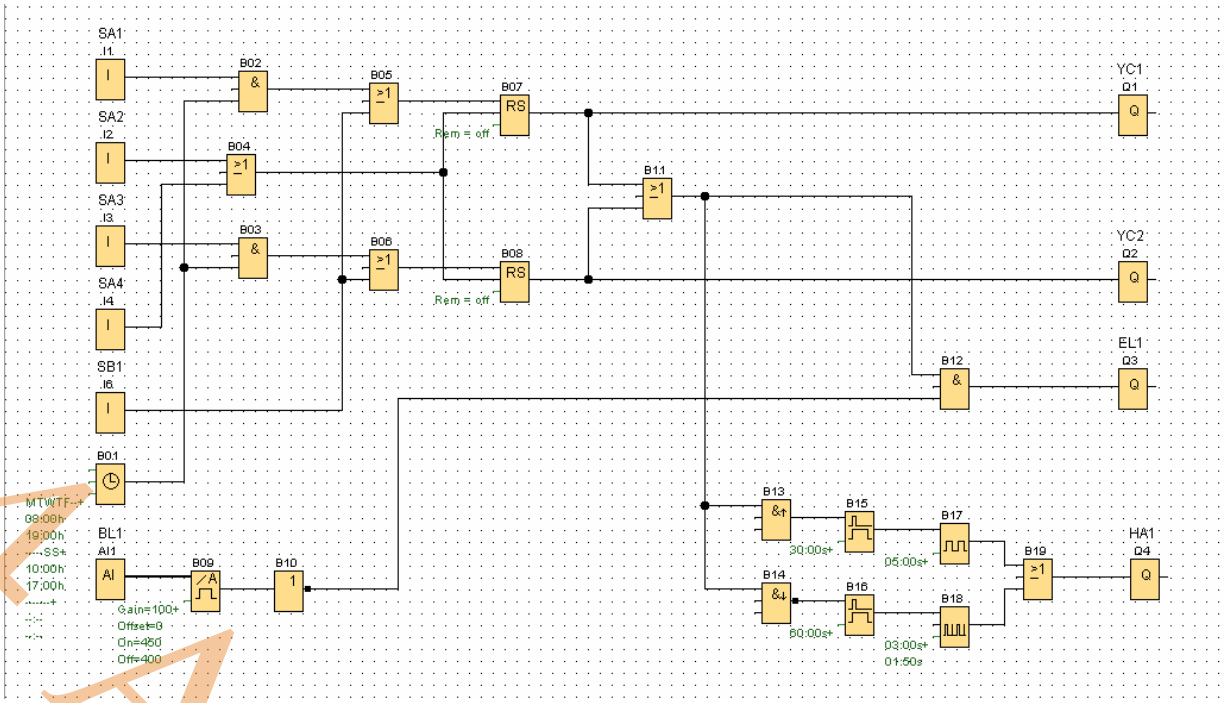


Рисунок 1.7 – Програма PLC для системи сигналізації на складі

1.2 Роль і переваги ПЛК Siemens S7-1200 у розробці систем

У сучасному світі автоматизація охоронних систем відіграє ключову роль у забезпеченні безпеки складських та інших промислових об’єктів. Одним із центральних елементів таких систем є програмовані логічні контролери (ПЛК), які виступають «мозком» автоматизованої системи. Вони забезпечують обробку сигналів від датчиків, управління виконавчими механізмами та інтеграцію з іншими компонентами [4, 5].

Siemens S7-1200 є одним із провідних ПЛК на ринку завдяки своїй багатофункціональності, надійності та здатності адаптуватися до специфічних умов роботи. Цей контролер широко застосовується в промисловості, зокрема у системах охорони, через поєднання високої продуктивності, простоти програмування та підтримки сучасних технологій.

Також Siemens S7-1200 виконує декілька критично важливих функцій:

1) Централізоване управління. Контролер є центральним вузлом системи, що забезпечує збирання, обробку та аналіз даних від датчиків різних типів (руху, відкривання дверей, диму, температури тощо). Він об'єднує всі елементи в єдину

мережу, координуючи їх роботу для досягнення загальної мети – забезпечення безпеки об’єкта.

2) Реалізація складних алгоритмів. Дозволяє програмувати складні сценарії роботи охоронної системи, наприклад: Автоматичне блокування входів у разі тривоги; Ввімкнення камер відеоспостереження у визначених зонах; Надсилання сповіщень користувачам через GSM або інтернет.

3) Моніторинг і діагностика. Контролер забезпечує безперервний моніторинг стану системи та дозволяє виявляти несправності на ранніх етапах. Це значно знижує ризик збоїв у роботі системи.

4) Інтеграція з іншими системами. Завдяки підтримці стандартних протоколів зв’язку, таких як Modbus і Profinet, Siemens S7-1200 може взаємодіяти з різними пристроями та підсистемами: Системи відеоспостереження (наприклад, Hikvision); Автоматизовані ворота; Системи управління кліматом і освітленням.

Переваги Siemens S7-1200

Використання середовища розробки TIA Portal значно спрощує програмування контролера. Інтуїтивний інтерфейс дозволяє швидко створювати програми для реалізації функцій охоронної системи.

Контролер розроблений для роботи в складних умовах:

Температурний діапазон: від -25°C до +60°C.

Захист від пилу та вологи (ступінь захисту IP20).

Стійкість до електромагнітних перешкод.

Siemens S7-1200 легко масштабується завдяки можливості додавання модулів введення/виведення, що робить його придатним як для невеликих систем, так і для масштабних проектів.

Контролер споживає мінімум енергії, що дозволяє знижувати експлуатаційні витрати, особливо при цілодобовій роботі.

Завдяки підтримці IoT-рішень, Siemens S7-1200 може працювати з хмарними платформами, що дозволяє:

Зберігати дані для подальшого аналізу.

Надавати віддалений доступ до системи через веб-інтерфейс.

Контролер підходить для вирішення найрізноманітніших завдань: від управління окремими датчиками до побудови інтегрованої системи охорони з декількома рівнями захисту.

Практичні приклади використання Siemens S7-1200:

Складські приміщення. Контролер використовується для: моніторингу зон доступу; контролю умов зберігання (температура, вологість); автоматизації роботи воріт і освітлення.

Промислові об’єкти. Siemens S7-1200 управляє системами охорони на підприємствах, інтегруючи відеоспостереження, контроль доступу та пожежну сигналізацію в одну систему.

Комерційні об’єкти. Контролер дозволяє автоматизувати охоронні процеси у магазинах, офісах і торгових центрах.

2 ФУНКЦІЇ ОХОРОННИХ СИСТЕМ

2.1 Базові функції охоронної системи

Автоматизована охоронна система виконує широкий спектр завдань, які забезпечують захист об’єкта та оперативне реагування на загрози. У контексті складських приміщень, де необхідно забезпечити безперервний моніторинг і контроль, базові функції системи набувають особливого значення. Їх реалізація дозволяє ефективно керувати процесами захисту, знижуючи ризик людських помилок та оптимізуючи операційні витрати.

Перш за все, ключовою функцією охоронної системи є контроль доступу. Система забезпечує управління входами і виходами на об’єкті, дозволяючи фіксувати час та ідентифікувати користувачів, які здійснюють доступ до певних зон. Для цього використовуються ідентифікаційні картки, біометричні дані або кодові пристрої. Такий підхід дозволяє вести детальний журнал подій, що є необхідним для подальшого аналізу.

Другою важливою функцією є периметральний захист, що передбачає виявлення несанкціонованого проникнення на територію складу. Виявлення здійснюється за допомогою датчиків руху, відкривання дверей і вікон, а також камер відеоспостереження. Спрацювання таких датчиків дозволяє миттєво активувати механізми захисту, як-от блокування дверей, активація сирен або передача сповіщення відповідальним особам.

Особливе місце серед базових функцій займає сигналізація, яка забезпечує звукове та візуальне попередження про загрозу. Системи оповіщення, такі як сирени чи сигнальні лампи, дозволяють швидко привернути увагу персоналу до потенційної небезпеки. Це є важливим елементом швидкого реагування у критичних ситуаціях.

Наступною функцією є сповіщення користувачів. У разі виявлення загрози система автоматично надсилає повідомлення відповідальним особам через мобільний зв’язок або інтернет. Для цього використовуються GSM-модулі, які забезпечують передачу тривожних сигналів у вигляді SMS або телефонних

дзвінків. Також можливе сповіщення через мобільний додаток чи веб-інтерфейс, що дозволяє оперативно керувати системою.

Важливим аспектом роботи є моніторинг середовища, який передбачає контроль температури, вологості та інших умов, що впливають на збереження матеріальних цінностей у складі. Система автоматично фіксує відхилення від заданих параметрів та повідомляє про це операторів або адміністраторів.

Окрім цього, базовим елементом є автономність системи, що гарантує її безперебійну роботу навіть у разі відключення основного джерела живлення. Використання резервних батарей забезпечує автономну роботу системи протягом 24 годин, що є критично важливим для охоронних комплексів.

Не менш важливою є функція інтеграції з іншими системами, такими як відеоспостереження, контроль клімату чи автоматизовані ворота. Це дозволяє створити єдиний інформаційно-керуючий простір, що спрощує роботу персоналу та підвищує ефективність управління складським об’єктом.

Усі ці функції забезпечують комплексний підхід до охорони складських приміщень, створюючи систему, яка не лише запобігає загрозам, а й оперативно реагує на будь-які небезпеки. Впровадження таких рішень дозволяє значно підвищити безпеку об’єкта, мінімізувати ризики втрат та забезпечити збереження матеріальних цінностей у складних умовах експлуатації.

2.2 Додаткові функції системи для складських приміщень

Окрім базових функцій, які забезпечують основні потреби у захисті об'єкта, сучасна охоронна система для складських приміщень повинна враховувати специфічні вимоги, зумовлені особливостями їх експлуатації. Це дозволяє не лише підвищити рівень безпеки, а й оптимізувати процеси управління об’єктом. Додаткові функції спрямовані на створення інтегрованої системи, здатної реагувати на широкий спектр загроз та завдань [6].

Однією з ключових додаткових функцій є інтеграція з системою управління складом. Завдяки цій функції охоронна система може контролювати переміщення товарів у режимі реального часу, відслідковувати залишки продукції та

взаємодіяти з іншими модулями управління. Такий підхід сприяє зниженню витрат та запобігає помилкам, пов’язаним із людським фактором.

Важливим аспектом є гнучке зонування простору складського приміщення. Охоронна система повинна підтримувати розподіл території на зони з різними рівнями доступу. Наприклад, зони зберігання, завантаження або технічні приміщення можуть мати різні правила доступу, які автоматично коригуються залежно від часу доби чи ситуації. У разі виникнення тривоги система може автоматично заблокувати доступ до критичних зон.

Ще однією значущою функцією є моніторинг умов зберігання. У складських приміщеннях часто зберігаються товари, чутливі до змін температури, вологості чи інших зовнішніх умов. Система охорони може бути оснащена датчиками, що фіксують ці параметри, попереджаючи персонал про можливі відхилення від норми. Це дозволяє зберегти якість продукції та уникнути збитків.

Інтеграція з пожежною системою також є критичною функцією для складських приміщень. Сучасні охоронні системи можуть взаємодіяти з датчиками диму та температури, активуючи механізми пожежогасіння у разі виникнення загрози. Така інтеграція забезпечує комплексний захист об’єкта, мінімізуючи час реагування на надзвичайні ситуації.

Функція віддаленого доступу та керування стає невід'ємною частиною сучасних охоронних систем. Завдяки інтеграції з мобільними додатками чи веб-інтерфейсами, користувачі отримують можливість керувати системою, переглядати події та отримувати сповіщення у режимі реального часу з будь-якого місця. Це особливо важливо для об’єктів із великими територіями або для віддалених складських комплексів.

Додатково важливою є функція системи ідентифікації персоналу, яка забезпечує контроль доступу співробітників до різних зон приміщення. Використання RFID-карток або біометричних даних дозволяє не лише запобігти несанкціонованому доступу, а й реєструвати час роботи персоналу, оптимізуючи кадровий облік.

Отже, додаткові функції охоронної системи для складських приміщень дозволяють створити багатофункціональну, інтегровану та гнучку систему, що

відповідає сучасним вимогам безпеки. Їх впровадження сприяє покращенню управління складським об’єктом, зниженню ризиків втрат і забезпеченню безперебійної роботи навіть у складних умовах.

2.3 Вимоги до реальних умов експлуатації системи

Охоронна система складського приміщення повинна відповідати суворим вимогам, пов’язаним із особливостями умов її роботи. Це зумовлено не лише необхідністю забезпечення безпеки об’єкта, а й забезпеченням надійності, автономності та довговічності роботи системи в різноманітних експлуатаційних ситуаціях. Нижче наведено основні вимоги, які висуваються до охоронної системи в реальних умовах.

Стійкість до зовнішніх факторів є першочерговою вимогою до охоронних систем. У складських приміщеннях, особливо тих, що знаходяться у промислових зонах або працюють на відкритих територіях, система повинна забезпечувати безперебійну роботу в широкому діапазоні температур (наприклад, від -10°C до +50°C) та за умов підвищеної вологості (до 85%). Усі компоненти системи мають бути захищені від пилу та вологи відповідно до стандартів IP-захисту, щоб уникнути пошкоджень та збоїв у роботі.

Наступною критичною вимогою є автономність роботи. У разі перебоїв з електропостачанням охоронна система має зберігати працездатність завдяки резервному живленню. Резервні акумулятори повинні забезпечувати роботу системи щонайменше протягом 24 годин без додаткового підзаряджання, що особливо важливо для великих об’єктів, де доступ до живлення може бути обмеженим.

Сучасні охоронні системи також повинні відповідати вимогам до стабільності зв’язку. Це включає використання надійних каналів передачі даних, таких як GSM, Ethernet чи Wi-Fi. У разі втрати основного каналу зв’язку має бути передбачений резервний, щоб забезпечити безперервну передачу сигналів тривоги або даних про стан системи. Такий підхід мінімізує ризики втрати критичної інформації.

Масштабованість є ще однією важливою вимогою до охоронних систем складських приміщень. З огляду на те, що складські об’єкти часто розширюють свої території або додають нові функціональні зони, система повинна мати можливість легко адаптуватися до таких змін. Це включає додавання нових датчиків, камер, модулів управління або інших компонентів без значних змін у загальній архітектурі системи.

Сучасні охоронні системи також потребують технологій самодіагностики, які дозволяють виявляти несправності на ранніх етапах. Це включає автоматичну перевірку стану датчиків, модулів живлення чи зв’язку, а також сповіщення користувачів про необхідність обслуговування.

Швидкість реагування на загрози також є невід’ємною характеристикою охоронної системи. У сучасних умовах будь-яке зволікання може призвести до суттєвих втрат. Тому час від виявлення загрози до активації захисних механізмів має бути мінімізований. Це включає швидке спрацювання сирен, надсилання сповіщень чи блокування доступу до критичних зон.

У сучасних умовах інтеграція системи в інтернет-мережі робить кібербезпеку важливою складовою. Захист даних за допомогою шифрування, багаторівнева автентифікація та резервне зберігання даних у хмарі або локально є обов’язковими вимогами. Це дозволяє уникнути несанкціонованого доступу та забезпечити стабільність роботи.

Додатково, охоронна система має забезпечувати сумісність із сучасними технологіями. Це включає підтримку стандартних протоколів зв’язку, таких як Modbus, Profinet чи MQTT [7]., що дозволяє інтегрувати систему з іншими технологічними процесами на об’єкті. Наприклад, автоматизація клімат-контролю чи освітлення може бути частиною загальної системи управління складом.

Для забезпечення фізичної безпеки пристроїв передбачається стійкість до саботажу. Спеціальні механізми повинні реагувати на спроби фізичного пошкодження або відключення компонентів, запобігаючи порушенню роботи системи.

Окрім технічних аспектів, важливою є ергономіка користування. Інтерфейс управління має бути простим та інтуїтивно зрозумілим, що дозволяє оператору

швидко налаштовувати систему та реагувати на події без спеціальних технічних знань.

Нарешті, система повинна відповідати сучасним стандартам безпеки, наприклад EN 50131, а також екологічним нормам, таким як RoHS, які регулюють використання безпечних матеріалів.

Таким чином, охоронна система, що відповідає цим вимогам, забезпечує не лише базову безпеку об’єкта, але й інтеграцію з іншими технологічними процесами, мінімізацію ризиків і високу ефективність роботи у складних умовах.

3 ПРОЄКТУВАННЯ СИСТЕМИ ОХОРОНИ

Проєктування охоронної системи є ключовим етапом у її створенні, оскільки на цьому етапі визначаються архітектура, компоненти та алгоритми роботи системи. Основна мета проєктування — розробити ефективну, масштабовану та надійну систему, яка відповідатиме специфічним вимогам складських приміщень. Нижче наведено основні аспекти, які враховуються під час розробки.

3.1 Розробка структурної схеми системи охорони

Для проектування пристрою, потрібно окреслити, його основні функціональні блок згідно ТЗ і на основі цього побудувати структурну схему. На рисунку 3.1. представлена узагальнена структурна схема.

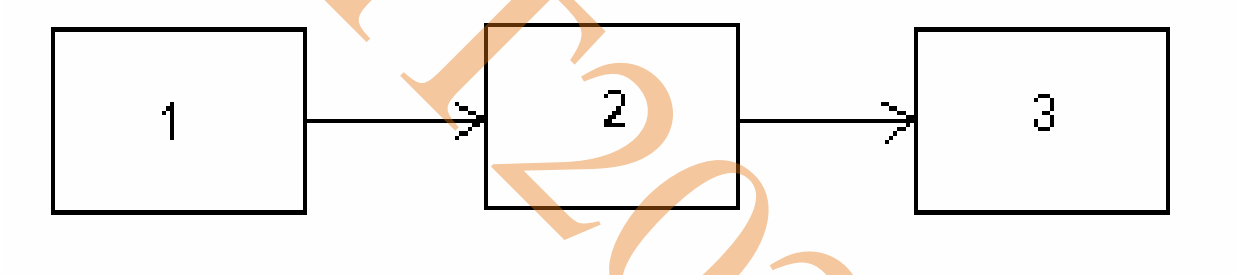


Рисунок 3.1 - Узагальнена структурна схема

1. Блок датчіків.
2. Блок обробки сигналів і утворення керуючих сигналів.
3. Блок сповіщення.

Враховуючі неопхідність узгодження елементів, наша структурна схема набере вигляду рис. 3.2.

Рисунок 3.2 - Структурна схема системи охорони

Структурна схема є основою проєктування, оскільки вона визначає загальну архітектуру системи та взаємозв'язки між її компонентами. Основні елементи схеми:

ПЛК Siemens S7-1200 - центральний вузол управління, який координує всі процеси системи [4].

Вхідні пристрої: датчики руху, відкриття дверей/вікон, температури та диму, які передають сигнали до ПЛК.

Вихідні пристрої: сирени та сигнальні лампи для звукового та світлового оповіщення про загрозу.

Модулі зв'язку: GSM- та інтернет-модулі забезпечують передачу даних та повідомлень користувачам.

Камери відеоспостереження: інтегровані для забезпечення візуального контролю та передачі зображень користувачам.

Система контролю доступу: електронні замки та ворота, керовані ПЛК, обмежують доступ до об’єкта.

Резервне живлення - забезпечує автономну роботу системи у разі відключення основного живлення.

Користувач - взаємодіє з системою через мобільний додаток чи ПК, отримує сповіщення та може керувати компонентами системи.

Центральний вузол управління. Програмований логічний контролер (ПЛК), який виконує функції збору та обробки даних від датчиків, управління виконавчими механізмами та взаємодії з іншими системами. Siemens S7-1200 обрано через його гнучкість, масштабованість та підтримку сучасних протоколів зв’язку.

Датчики та сенсори. Датчики руху, відкриття дверей/вікон, температури та диму. Комбіновані датчики для забезпечення багаторівневого контролю.

Системи оповіщення. Сирени, сигнальні лампи. GSM-модуль для передачі сповіщень користувачам.

Комунікаційні модулі. Ethernet-модулі для інтеграції з локальною мережею. GSM або Wi-Fi модулі для резервного зв’язку.

Додаткові системи: Камери відеоспостереження, інтегровані із системою для запису та аналізу подій. Виконавчі механізми (замки, шлагбауми, автоматичні ворота).

3.2 Вибір компонентів системи

Автоматизована система охорони складського приміщення повинна включати набір компонентів, які забезпечують її ефективну роботу. До ключових елементів відносяться датчики, засоби оповіщення, модулі зв’язку та програмовані логічні контролери (ПЛК) [5]. Вибір компонентів базується на аналізі функціональних вимог до системи, специфіки складського об’єкта та доступних технологій.

Датчики

Датчики руху:

1) інфрачервоні (IR) - виявляють зміни у тепловому полі, викликані рухом людини;

Рисунок 3.3 - Датчики руху інфрачервоні

2) ультразвукові - використовують високочастотні звукові хвилі для виявлення руху;

Рисунок 3.4 - Датчики руху ультразвукові

3) мікрохвильові - створюють електромагнітне поле, реагуючи на зміну його параметрів.

Рисунок 3.5 - Датчики руху

Контактні датчики:

1) використовуються для моніторингу відкриття дверей і вікон;

2) підходять для периметрального контролю.

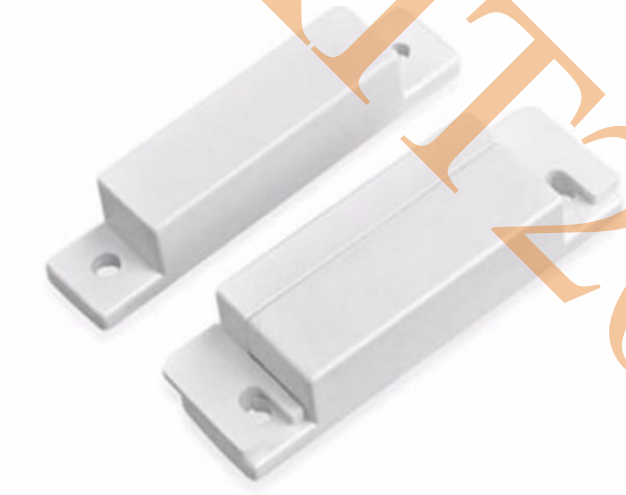


Рисунок 3.6 - Датчики контактні

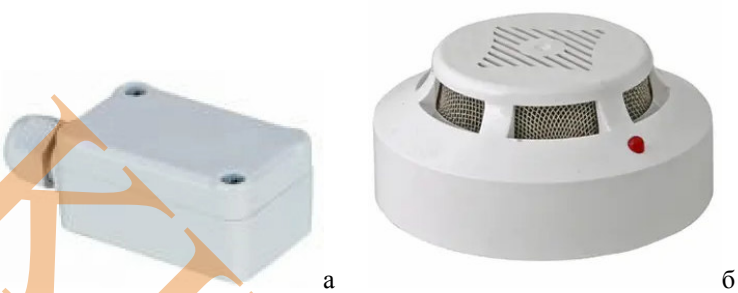
Комбіновані датчики:

1) поєднують функції виявлення руху та розбиття скла;

2) забезпечують багаторівневий захист.

Рисунок 3.7 - Датчики комбіновані

Датчики температури і диму: Контролюють умови зберігання і сигналізують про загрозу пожежі.



а б

Рисунок 3.8 - датчики температури і диму

Засоби оповіщення

Сирени та сигнальні лампи:

1) генерують звукові і візуальні сигнали у разі тривоги;

2) підвищують рівень реагування на загрози.

Рисунок 3.9 - Засоби оповіщення сирени

GSM-модулі:

1) надсилають повідомлення через SMS або здійснюють дзвінок на запрограмовані номери;

2) використовуються для миттєвого сповіщення відповідальних осіб.

Рисунок 3.10 - GSM-модулі

IP-системи сповіщення: інтегруються з локальними мережами та забезпечують передачу тривожних сигналів через інтернет.

Комунікаційні модулі

Ethernet-модулі: забезпечують інтеграцію ПЛК із системами моніторингу.

Wi-Fi/LoRa модулі: використовуються для бездротового зв'язку між компонентами.

GSM-модулі:

1) підтримують зв'язок із системою через мобільні мережі;

2) забезпечують резервний канал зв'язку у разі збоїв основної мережі.

Програмовані логічні контролери (ПЛК)

У системі використовується Siemens S7-1200, який:

1) підтримує підключення різних типів датчиків;

2) забезпечує централізоване управління системою;

3) дозволяє реалізовувати складні алгоритми автоматизації.

Критерії вибору компонентів

Сумісність із ПЛК Siemens S7-1200:

1) компоненти мають підтримувати стандартні інтерфейси зв'язку (Modbus, Ethernet);

2) Легкість інтеграції з програмним забезпеченням контролера.

Енергоефективність: вибір компонентів із низьким енергоспоживанням для забезпечення автономної роботи.

Надійність та довговічність: використання пристроїв, здатних працювати в умовах підвищеної вологості та температурних коливань.

Гнучкість у масштабуванні: можливість додавання нових датчиків і модулів без значних змін у системі.

Переваги обраних компонентів

Модульність. Легке розширення системи за рахунок додавання нових модулів і датчиків.

Швидкість реагування. Миттєве виявлення загроз і сповіщення відповідальних осіб.

Інтеграція. Можливість підключення до інших систем управління об’єктом.

Автономність. Робота навіть за відсутності зовнішніх джерел живлення.

3.3 Розробка принципової схеми

Принципова схема деталізує електричні з’єднання між компонентами системи. Вона визначає: типи входів/виходів, які використовуються ПЛК; підключення датчиків до центрального контролера; канали зв’язку для передачі даних; розподіл живлення між компонентами.

Програмування алгоритмів роботи

На основі принципової схеми розробляються алгоритми роботи системи, які включають: обробку сигналів від датчиків (виявлення руху, відкриття дверей чи вікон, аналіз температури або диму); реакцію системи на загрози (активація сирен, блокування доступу, надсилання сповіщень через GSM-модуль або Інтернет); моніторинг і самодіагностику (автоматична перевірка працездатності компонентів, інформування оператора про несправності).

Створення інтеграційного середовища. Система проєктується з урахуванням можливості її інтеграції з іншими технологічними рішеннями: відеоспостереження (автоматичне ввімкнення камер у разі тривоги, передача зображень у реальному часі на мобільний додаток); системи управління складом (інтеграція з базами даних про залишки товарів, автоматизація роботи воріт і освітлення).

Розробка принципової схеми з урахуванням роботи ПЛК Siemens S7-1200

Принципова схема охоронної системи на основі ПЛК Siemens S7-1200 відображає деталі електричних з'єднань між компонентами системи. Вона є ключовим етапом проєктування, оскільки визначає правильну взаємодію обладнання та його функціональність.

Основні елементи принципової схеми

ПЛК Siemens S7-1200:

Централізований модуль, який обробляє сигнали від датчиків і керує виконавчими механізмами.

Забезпечує підключення вхідних і вихідних пристроїв через цифрові (DI/DO) або аналогові порти (AI/AO).

Підтримує протоколи зв'язку, такі як PROFINET, Modbus TCP [8]..

Датчики:

Датчик руху (цифровий вхід): Зазвичай підключається через нормально розімкнений контакт.

Датчик відкриття дверей (цифровий вхід): Контролює стан дверей або вікон (відкрито/закрито).

Датчик температури (аналоговий вхід): Подає сигнал про поточну температуру у вигляді змінного напруги або струму (наприклад, 0–10 В або 4–20 мА).

Датчик диму (цифровий вхід): Спрацьовує у разі виявлення диму (реле на замикання).

Система оповіщення:

Сирена (цифровий вихід): Керована ПЛК через реле для активації у разі тривоги.

Сигнальна лампа (цифровий вихід): Підключається аналогічно сирені.

Виконавчі механізми:

Електронні замки (цифровий вихід): Контролюються через реле, що забезпечує подачу напруги на замок.

Камери відеоспостереження:

Можуть працювати через окремий Ethernet-роз'єм ПЛК, що забезпечує інтеграцію відеопотоку в систему.

GSM-модуль:

Підключається до послідовного порту ПЛК через стандарт RS-232 або RS-485.

Забезпечує віддалене сповіщення через SMS або дзвінки.

Резервне живлення:

Забезпечує безперервну роботу ПЛК і критичних компонентів під час зникнення основного живлення.

Реалізується через безперебійне джерело живлення (UPS) або акумуляторний модуль.

Вхідні сигнали:

Датчики руху, диму, відкриття дверей підключаються до цифрових входів ПЛК (DI1, DI2 тощо).

Аналогові датчики (температури, вологості) підключаються до аналогових входів (AI1, AI2).

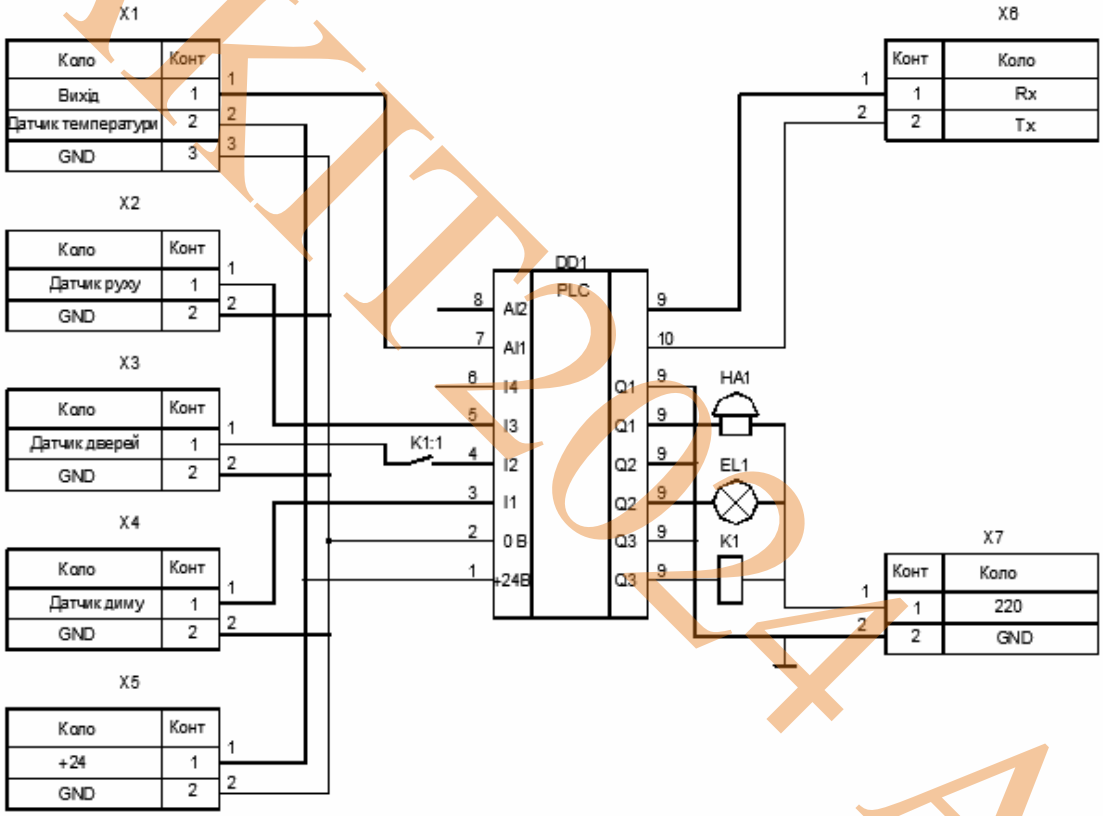


Рисунок 3.11 - Схема електрична принципова

Вихідні сигнали:

Сирена та сигнальна лампа підключаються через релейні виходи (DO1, DO2).

Електронні замки керуються через окреме реле для подачі живлення.

Комунікаційні модулі:

Ethernet-з’єднання для інтеграції з системою моніторингу або управління через PROFINET.

GSM-модуль через RS-232/RS-485 для надсилання повідомлень.

Живлення:

Основне джерело живлення 24 В DC для роботи ПЛК.

Резервне живлення автоматично активується у разі відсутності основного.

4 АЛГОРИТМ РОБОТИ СИСТЕМИ

Стан готовності. ПЛК постійно моніторить вхідні сигнали від датчиків. У нормальних умовах система підтримує пасивний режим.

Активність. Спрацювання будь-якого датчика ініціює відповідну реакцію: датчик руху → активується сирена; датчик диму → активується сирена, надсилається SMS; температурні аномалії → надсилається повідомлення.

Реакція. ПЛК активує сигнальну лампу, блокує доступ через електронні замки. Передає дані на сервер або мобільний додаток.

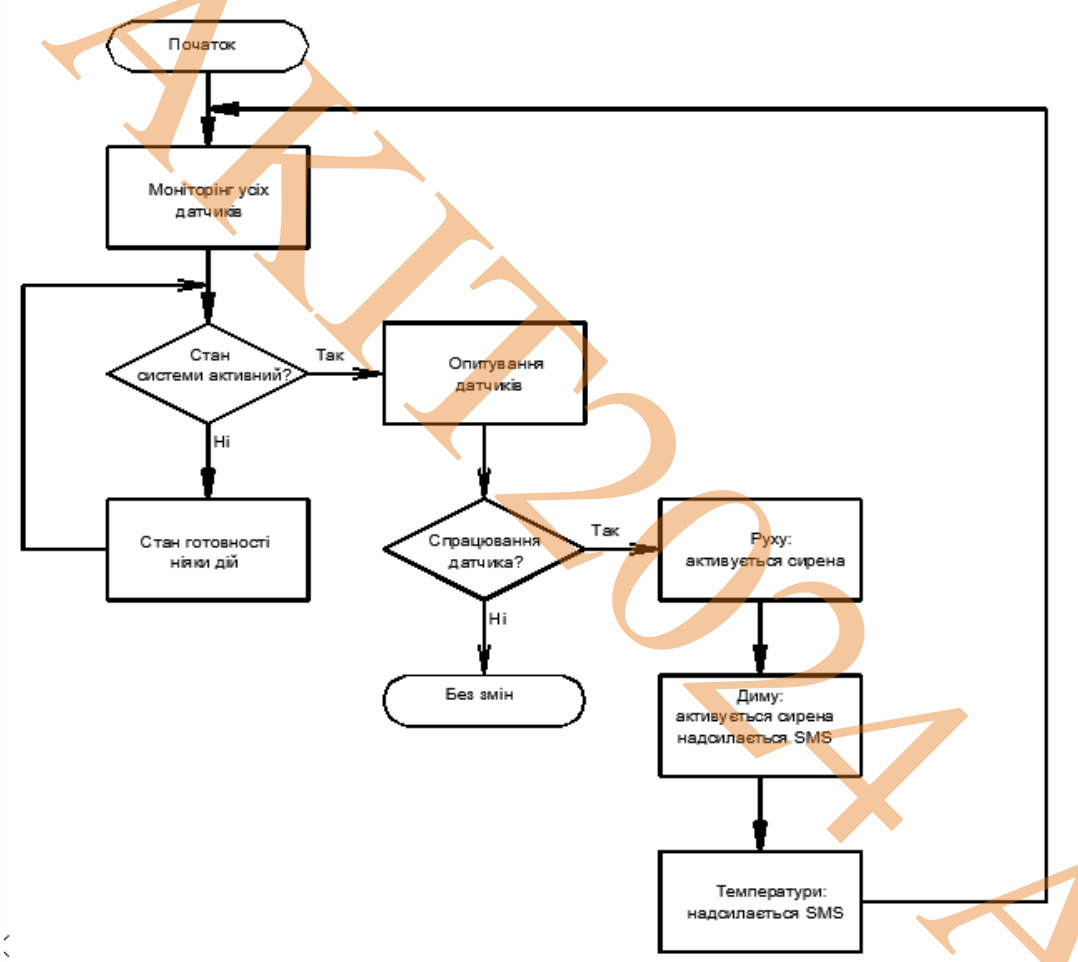


Рисунок 4.1 – Алгоритм програми

4.1 Програмування логіки для ПЛК Siemens S7-1200

Програмування логіки для ПЛК (програмованого логічного контролера) Siemens S7-1200 виконується у середовищі TIA Portal (Totally Integrated

Automation). Цей процес включає створення програми, яка керує підключеними пристроями, аналізує сигнали від датчиків та виконує необхідні дії.

Ось детальна покрокова інструкція для програмування логіки ПЛК Siemens S7-1200:

1. Встановлення програмного забезпечення. Завантажте та встановіть Siemens TIA Portal (версія відповідає моделі ПЛК). Переконайтесь, що ви маєте драйвери для підключення до ПЛК.

2. Підготовка до програмування. Перевірте специфікацію ПЛК. Переконайтесь, що всі входи/виходи (I/O) визначені, а модулі встановлені. Наприклад: DI1 для датчика руху, DO1 для сирени. Створіть план логіки: сформулюйте, які події повинні викликати певні дії. Наприклад: спрацювання датчика руху активація сирени; зниження температури активація нагрівача.

3. Підключення до ПЛК. З'єднання з ПЛК: підключіть ПЛК до комп'ютера через Ethernet або USB; у TIA Portal створіть новий проєкт і додайте пристрій (Add Device); виберіть модель ПЛК Siemens S7-1200 і задайте IP-адресу. Тестування з'єднання: відкрийте "Online & Diagnostics" у TIA Portal; переконайтесь, що ваш ПЛК правильно виявлено.

4. Налаштування входів і виходів. Оголосіть входи/виходи: у розділі Device Configuration вкажіть використані входи/виходи. Наприклад: DI1 -датчик руху; DI2 - датчик відкриття дверей; DO1 - сирена; DO2 - сигнальна лампа. Задайте типи сигналів: аналогові датчики (наприклад, температури) прив'яжіть до аналогових входів (AI); цифрові датчики до цифрових входів (DI).

5. Створення програми. Виберіть мову програмування: TIA Portal підтримує кілька мов: LAD (Ladder Diagram) – графічна мова для логічних зв'язків. FBD (Function Block Diagram) – блочна мова для складних алгоритмів. STL (Statement List) – текстова мова для досвідчених програмістів. Програмування логіки: Приклад 1: Активація сирени при спрацюванні датчика руху (LAD): I0.1 (Датчик руху) ---> Q0.1 (Сирена). Приклад 2: Включення сигнальної лампи при відкритті дверей (FBD): Вхід: DI2 (Датчик відкриття); Вихід: DO2 (Лампа); Умови: Якщо DI2 = 1, активувати DO2. Обробка аналогових сигналів: Наприклад, для датчика температури (0–10 В): Масштабуйте сигнал в

інтервалі 0–100°C. Умови: Якщо температура < 15°C, активувати DO3 (нагрівач). Обмін даними: для відправки повідомлення через GSM-модуль: використовуйте блоки AT-команд для ініціації передачі SMS.

6. Тестування програми. Симуляція: У TIA Portal є вбудований симулятор, який дозволяє тестувати програму без підключення до реального ПЛК. Перевірте всі сценарії: як програма реагує на різні входи. Завантаження в ПЛК: Завантажте програму у ПЛК через опцію Download to Device. Переведіть ПЛК у режим виконання RUN. Тестування на реальному обладнанні: Перевірте, як датчики, виконавчі механізми, і GSM-модуль працюють відповідно до вашої програми.

7. Оптимізація та документація

Оптимізація програми: Переконайтесь, що програма не містить зайвих блоків і працює ефективно. Використовуйте таймери та лічильники для складніших задач.

Приклад програми для охоронної системи: (Датчик руху) I0.1 ----> Q0.1 (Сирена); (Датчик відкриття) I0.2 ----> Q0.2 (Лампа); (Температурний сигнал AI1 < 15°C) ----> Q0.3 (Нагрівач).

Розробка повної LAD-схеми (Ladder Diagram) для охоронної системи включає всі основні функції, які забезпечують моніторинг та управління компонентами системи, такими як датчики, виконавчі пристрої та модулі сповіщення.

Ось повна логіка, яку ми інтегруємо в LAD-схему:

Функціональність охоронної системи:

1. Активація сирени при виявленні руху.
2. Увімкнення сигнальної лампи при відкритті дверей.
3. Управління нагрівачем залежно від температури.
4. Сповіщення через GSM-модуль у разі задимлення.
5. Затримка активації сирени після виявлення руху.
6. Автоматичне блокування замків у разі тривоги.

Реалізація LAD-схеми

1. Структура LAD-схеми

Вхід (I)	Функція	Вихід (Q)
I0.1 (Датчик руху)	Активація сирени	Q0.1 (Сирена)
I0.2 (Датчик дверей)	Увімкнення лампи	Q0.2 (Лампа)
AI1 (Температура)	Контроль нагрівача	Q0.3 (Нагрівач)
I0.3 (Датчик диму)	Сповіщення через GSM	Q0.4 (GSM-модуль)
I0.1 + I0.3	Блокування замків	Q0.5 (Замки)

2. LAD-схема

// Логіка активації сирени при спрацюванні датчика руху

[I0.1] ---- [TON] ---- (Q0.1)

// Таймер (TON) затримує активацію на 5 секунд

// Логіка увімкнення лампи при відкритті дверей

[I0.2] ---------- (Q0.2)

// Контроль нагрівача при низькій температурі

[AI1 < 15°C] ---------- (Q0.3)

// Надсилання сигналу через GSM при виявленні диму

[I0.3] ---------- (Q0.4)

// Блокування замків при тривозі

[I0.1] ----+--- (Q0.5)

|

[I0.3] ----+

Пояснення схеми

Сирена (Q0.1):

Датчик руху (I0.1) активує таймер (TON).

Через 5 секунд таймер подає сигнал на сирену (Q0.1).

Сигнальна лампа (Q0.2):

При відкритті дверей (I0.2) лампа (Q0.2) активується одразу.

Нагрівач (Q0.3):

Датчик температури (AI1) зчитує значення. Якщо температура нижча за 15°C, вмикається нагрівач (Q0.3).

GSM-модуль (Q0.4):

Якщо виявлено дим (I0.3), GSM-модуль (Q0.4) надсилає SMS.

Замки (Q0.5):

При активації датчика руху (I0.1) або датчика диму (I0.3), замки (Q0.5) автоматично блокуються.

Реалізація в TIA Portal

Створення проєкту: Додайте пристрій Siemens S7-1200. Визначте входи (I0.1, I0.2, I0.3, AI1) і виходи (Q0.1, Q0.2, Q0.3, Q0.4, Q0.5).

Додайте блок OB1 (Main): Створіть логічні сходинки для кожної функції.

Налаштуйте таймер TON: Додайте таймер із затримкою 5 секунд для активації сирени.

Використовуйте блоки порівняння: Для контролю температури (AI1 < 15°C) використовуйте порівняльний блок.

Завантажте програму у ПЛК: Підключіть ПЛК до комп'ютера через Ethernet. Переведіть ПЛК у режим RUN.

4.2 Опис роботи системи охорони від виявлення загрози до сповіщення користувачів

Охоронна система на основі ПЛК Siemens S7-1200 інтегрує датчики, виконавчі механізми, модулі зв'язку та автоматизації для забезпечення безпеки складського приміщення. Нижче наведено детальний опис роботи системи:

1. Виявлення загрози

Датчик руху (I0.1):

Виявляє рух у контрольованій зоні.

Передає сигнал на вхід ПЛК.

Датчик відкриття дверей (I0.2):

Спрацьовує при відкритті дверей чи вікон.

Датчик температури (AI1):

Аналізує поточну температуру. Якщо температура виходить за межі нормального діапазону (<15°C), активує нагрівач.

Датчик диму (I0.3):

Фіксує задимлення, що може свідчити про пожежу.

2. Обробка сигналів у ПЛК. Сигнали від датчиків надходять на входи ПЛК. ПЛК обробляє ці сигнали відповідно до запрограмованої логіки: Якщо спрацьовує датчик руху (I0.1), активується таймер затримки TON. Якщо спрацьовує датчик диму (I0.3), сигнал обробляється негайно.

Прийняття рішень

Сирена (Q0.1):

Активується після 5-секундної затримки, якщо датчик руху зафіксував загрозу.

Сигнальна лампа (Q0.2):

Вмикається одразу при відкритті дверей або вікон.

Нагрівач (Q0.3):

Вмикається, якщо температура падає нижче 15°C.

GSM-модуль (Q0.4):

Надсилає тривожне повідомлення, якщо активується датчик диму.

Електронні замки (Q0.5):

Блокуються автоматично при виявленні руху чи диму.

3. Реакція системи

Локальні дії

Активація виконавчих пристроїв: Сирена створює гучний звуковий сигнал, попереджаючи про небезпеку. Сигнальна лампа візуально сигналізує про тривогу. Електронні замки блокують доступ до приміщення.

Віддалені дії

Сповіщення користувачів: GSM-модуль надсилає SMS або здійснює дзвінок на задані номери з інформацією про тип загрози (наприклад, "Задимлення в зоні 1"). За наявності камери відеоспостереження система передає фото або відео в реальному часі через мобільний додаток.

4. Моніторинг стану системи

Інтерфейс оператора. Усі події реєструються в системі моніторингу. Оператор або власник приміщення може перевіряти статус датчиків, сирен і замків через веб-інтерфейс або мобільний додаток.

Само діагностика. ПЛК регулярно перевіряє працездатність датчиків і модулів. У разі несправності користувач отримує повідомлення про необхідність технічного обслуговування.

5. Скасування тривоги

Умови скасування. Тривога автоматично скасовується, якщо загроза більше не фіксується. Користувач може вручну скасувати тривогу через інтерфейс або кнопку розблокування (I0.4).

Відновлення стану. Система повертається у режим очікування. Замки розблоковуються, сирена та лампа вимикаються.

6. Резервне живлення

Автономна робота. У разі зникнення основного електропостачання система переходить на резервне живлення. ПЛК та критичні модулі (замки, GSM) продовжують функціонувати.

7. Сценарії роботи системи

Виявлення руху. Датчик руху фіксує активність. Через 5 секунд активується сирена. Замки блокуються.

Виявлення диму. Датчик диму фіксує задимлення. Замки блокуються. Надсилається SMS через GSM-модуль.

Відкриття дверей. Датчик дверей спрацьовує. Увімкнена сигнальна лампа.

Зниження температури. Датчик температури реєструє значення нижче 15°C. Активується нагрівач.

Переваги системи

1. Автоматизація: Повністю автоматизовані процеси виявлення та реагування.

2. Інтеграція: Можливість підключення до зовнішніх систем моніторингу.

3. Безперебійна робота: Резервне живлення забезпечує стабільність навіть під час відключень електроенергії.

4. Швидке реагування: Висока швидкість передачі даних і активації виконавчих механізмів.

Ця система забезпечує комплексний підхід до безпеки, від виявлення загрози до оперативного сповіщення користувачів і автоматизації дій.

5 ІМІТАЦІЙНЕ ТЕСТУВАННЯ АЛГОРИТМІВ РОБОТИ ОХОРОННОЇ СИСТЕМИ

Імітаційне тестування дозволяє перевірити правильність реалізації алгоритмів у програмі ПЛК, оцінити її реакцію на різні події та виявити можливі помилки до запуску системи в реальних умовах. Тестування виконується в середовищі TIA Portal, використовуючи вбудований симулятор або підключений ПЛК.

Підготовка до тестування

Налаштування симуляції. Запустіть TIA Portal і відкрийте проєкт. Активуйте симуляцію через "PLC Simulation (PLCSIM)". Завантажте програму в симулятор.

Створіть таблицю спостереження (Watch Table). Додайте всі необхідні входи (I0.1, I0.2, I0.3, AI1, I0.4) та виходи (Q0.1, Q0.2, Q0.3, Q0.4, Q0.5). Таблиця дозволяє вручну змінювати стан входів та відслідковувати реакцію виходів.

Етапи імітаційного тестування

1. Виявлення руху. У таблиці спостереження - встановіть сигнал I0.1 = 1 (спрацювання датчика руху). Очікуваний результат. Таймер TON запускається, після 5 секунд активується: Q0.1 (Сирена) = 1, Q0.5 (Замки) = 1. Перевірте затримку. У таблиці спостереження спостерігайте значення таймера ET (Elapsed Time).

2. Виявлення диму. У таблиці спостереження - становіть сигнал I0.3 = 1 (спрацювання датчика диму). Очікуваний результат - Замки негайно блокуються: Q0.5 = 1, GSM-модуль активується: Q0.4 = 1, Тривожне повідомлення надсилається.

3. Відкриття дверей. У таблиці спостереження - Встановіть сигнал I0.2 = 1 (відкриття дверей). Очікуваний результат - Сигнальна лампа активується: Q0.2= 1.

4. Зниження температури. У таблиці спостереження - Встановіть аналогове значення AI1 < 15°C. Очікуваний результат - Нагрівач активується: Q0.3 = 1.

5. Ручне розблокування. У таблиці спостереження - Встановіть сигнал I0.4 = 1 (натискання кнопки розблокування). Очікуваний результат - Замки розблоковуються: Q0.5 = 0, Сирена та лампа вимикаються.

Аналіз результатів

1. Реакція на події. Переконайтесь, що система правильно реагує на всі вхідні сигнали. Затримки, задані таймерами, працюють у відповідності до налаштувань.

2. Логічна коректність. Перевірте, чи відсутній конфлікт сигналів (наприклад, замки не блокуються, якщо двері відчинені вручну).

3. Робота резервного живлення. Уявіть сценарій втрати основного живлення. Переконайтеся, що система продовжує працювати через резервне живлення.

Тестування сценаріїв

1. Рух і дим одночасно: I0.1 = 1 і I0.3 = 1; Замки блокуються, сирена активується, GSM надсилає повідомлення.

2. Відкриття дверей і ручне розблокування: I0.2 = 1, потім I0.4 = 1; Лампа вмикається, але замки розблоковуються після натискання кнопки.

3. Зниження температури і рух: AI1 < 15°C і I0.1 = 1; Нагрівач активується, сирена включається із затримкою.

Документування результатів. Журнал тестування - Фіксуйте всі вхідні та вихідні значення для кожного сценарію. Аналіз помилок - Запишіть виявлені помилки та шляхи їх усунення.

Для розробки імітації роботи алгоритмів в середовищі TIA Portal, зокрема для перевірки активації сирени, потрібно виконати наступні кроки. Це дозволить повністю відтворити логіку роботи системи на основі LAD-програми, яку ми описали раніше.

5.1 Кроки для імітації роботи алгоритму активації сирени в TIA Portal

1. Створення проекту. Відкрийте TIA Portal:

Створіть новий проект;

Додайте пристрій Siemens S7-1200 у конфігурацію обладнання;

Налаштуйте модулі вводу-виводу відповідно до фізичних портів (I0.1 для датчика руху, Q0.1 для сирени).

Прив'яжіть адресацію. Вхідні сигнали - I0.1 — датчик руху. Вихідні сигнали - Q0.1 — сирена.

2. Реалізація LAD-логіки. Відкрийте блок OB1 (Main).

Реалізуйте наступну логіку: Використовуйте контакт NO для вводу сигналу від датчика руху (I0.1); Додайте таймер TON (Time On Delay) для затримки активації сирени; Підключіть вихід таймера до котушки Q0.1 (сирена).

LAD-схема:

[I0.1] ---- [TON] ---- (Q0.1)

Налаштуйте таймер:

PT (Preset Time): 5 секунд.

3. Підготовка стимулятора. Увімкніть симуляцію: Перейдіть до меню "Online" → "Start Simulation"; Запустіть симулятор PLCSIM для віртуального ПЛК.

Завантажте програму: Завантажте створену LAD-логіку у симулятор.

Перевірте зв'язок: У вікні моніторингу переконайтеся, що програма працює в режимі RUN.

4. Тестування логіки. Додайте таблицю спостереження (Watch Table) - Увімкніть таблицю спостереження та додайте наступні змінні: I0.1 — вхідний сигнал від датчика руху; Q0.1 — вихідний сигнал сирени; TON.ET — значення таймера.

Імітація спрацювання датчика руху. У таблиці спостереження встановіть I0.1 = 1 (активний сигнал від датчика руху).

Очікуваний результат. Після встановлення I0.1 = 1 таймер TON запускається. Через 5 секунд вихід Q0.1 = 1, що відповідає увімкненню сирени.

Зупинка сигналу. Встановіть I0.1 = 0 (датчик руху більше не фіксує активність). Переконайтеся, що Q0.1 повертається до 0 (сирена вимикається).

5. Аналіз результатів. Перевірка таймера: У таблиці спостереження відслідковуйте значення TON.ET (Elapsed Time); Переконайтеся, що час збігається з налаштуванням таймера.

Логічна коректність. Перевірте, чи система повертається у початковий стан після вимкнення входу I0.1.

Діагностика. Якщо система працює некоректно, скористайтеся діагностичними функціями TIA Portal.

6. Додаткове тестування. Симуляція роботи інших елементів - Додайте вхідні сигнали для датчика диму (I0.3) або температури (AI1) і перевірте інтегровану роботу системи. Створення комбінованих сценаріїв - Активуйте кілька входів одночасно (наприклад, I0.1 і I0.3), щоб перевірити реакцію системи.

Результати імітації:

- Сирена активується через заданий час після виявлення руху.

- Таймер працює згідно з налаштуваннями.

- Система коректно повертається до початкового стану після усунення загрози.

5.2 Результати роботи охоронної системи в змодельованих умовах

В умовах симуляції роботи алгоритму активації сирени у TIA Portal результати демонструють відповідність логіки очікуваним сценаріям [9]. Ось детальний опис результатів для кожного етапу:

1. Початковий стан. Змінні:

- o I0.1 (Датчик руху) = 0 (немає сигналу).
- o Q0.1 (Сирена) = 0 (не активна).
- o TON.ET (Час виконання таймера) = 0.
- • Система: Очікує на вхідний сигнал.

2. Активація датчика руху. Дії - У таблиці спостереження змінено значення I0.1 = 1. Результати - Таймер TON починає рахувати час (значення TON.ET збільшується від 0 до 5000 мс). Сирена залишається неактивною під час виконання таймера.

3. Спрацювання таймера. Дії - Таймер досяг значення TON.ET = 5000 мс. Результати - Вихід Q0.1 (Сирена) активується (значення = 1). Сирена починає сигналізувати про небезпеку.

4. Зняття сигналу з датчика руху. Дії - У таблиці спостереження змінено значення I0.1 = 0. Результати - Сирена вимикається (Q0.1 = 0); Таймер повертається у початковий стан (TON.ET = 0).

Аналіз роботи системи.

1. Точність виконання таймера - Затримка в 5 секунд працює коректно.

2. Правильна реакція виходу - Сирена активується після завершення роботи таймера. Вихід повертається до нуля після відключення сигналу датчика.

Можливі покращення:

1. Візуалізація стану системи - Додати лампу (Q0.2) для візуальної індикації роботи таймера.

2. Додаткові сценарії - Перевірити інтеграцію з іншими вхідними сигналами (наприклад, датчик диму).

Висновки.

Система працює стабільно та відповідає заданій логіці: 1. Таймер правильно обробляє вхідний сигнал і забезпечує затримку перед активацією сирени; 2. Зняття сигналу з датчика повертає систему в початковий стан.

5.3 Аналіз точності роботи системи

1. Точність спрацювання системи. Часова затримка (таймер TON): Таймер забезпечує стабільну затримку активації сирени у 5 секунд; Похибка роботи таймера залежить від частоти виконання циклу програми ПЛК: Для Siemens S7-1200 типова частота циклу становить кілька мілісекунд (зазвичай 1–10 мс); Таймер працює з високою точністю, що є достатнім для охоронних систем.

Реакція на вхідний сигнал: Час реакції системи (з моменту виявлення руху до активації сирени) відповідає встановленій затримці; При знятті сигналу (I0.1 = 0) система негайно вимикає сирену, що підтверджує правильну логіку.

2. Надійність логіки. Логіка працює коректно у симуляторі TIA Portal, забезпечуючи: Стабільне виконання алгоритму; Відсутність конфліктів між вхідними та вихідними сигналами.

3. Аналіз похибок. Вплив циклу виконання програми: Якщо цикл виконання програми ПЛК довший за 10 мс, може виникати затримка в реакції системи; У

реальних умовах це малоймовірно, оскільки Siemens S7-1200 здатний працювати з короткими циклами.

Чутливість датчиків. Затримка спрацювання або помилкові сигнали можуть виникнути через особливості датчиків (наприклад, помилкові спрацьовування при слабкому освітленні або раптовому русі).

Можливі вдосконалення системи

1. Вдосконалення точності. Оптимізація циклу ПЛК: Мінімізуйте час циклу виконання програми до 5–10 мс у конфігурації TIA Portal; Перевірте використання ресурсів ПЛК, щоб уникнути перевантаження.

Використання фільтрування сигналів. Впровадьте фільтрування для датчика руху: Додайте затримку на вході датчика для уникнення короткочасних помилкових спрацювань; Наприклад, реалізуйте блок DEBOUNCE для підтвердження сигналу.

2. Розширення функціональності.

Індикація стану системи. Додайте сигнальну лампу для візуального відображення стану: Наприклад, лампа блимає під час активації таймера.

[TON.RUN] ---- (Q0.2)

Додаткові умови активації. Інтегруйте в алгоритм кілька датчиків (наприклад, руху та диму): Сирена активується лише при одночасному спрацюванні обох датчиків.

[I0.1] --- [I0.3] ---- (Q0.1)

3. Підвищення надійності. Резервне живлення - Перевірте роботу системи при відсутності основного живлення: Забезпечте безперебійну роботу ПЛК, датчиків і сирени.

Діагностика датчиків. Впровадьте самодіагностику датчиків: ПЛК перевіряє наявність сигналу від датчика через заданий інтервал часу; У разі несправності надсилається сповіщення через GSM-модуль.

4. Інтеграція зі сторонніми системами. Додайте підтримку Ethernet або OPC UA для передачі даних на сервер. Використовуйте SCADA-систему для моніторингу роботи в реальному часі.

Пропозиції для вдосконалення. Автоматичне тестування системи: Впровадьте регулярну перевірку роботи сирени, замків та датчиків.

Гнучка конфігурація - Додайте налаштування часу таймера (TON) через зовнішній інтерфейс або мобільний додаток.

Захист від помилкових спрацювань - Використовуйте логічні умови для перевірки, наприклад. Сирена активується лише тоді, коли сигнал від датчика триває понад 1 секунду.

ВИСНОВКИ

В процесі виконання кваліфікаційної роботи " Охоронна система складського приміщення на ПЛК " виходячи із поставлених у технічному завданні вимог і виходячи із огляду існуючих аналогів, розроблено структурну схему. Основні результати роботи: реалізовано алгоритм роботи охоронної системи на основі ПЛК Siemens S7-1200, який забезпечує: виявлення загроз (руху, задимлення, відкриття дверей, аномальної температури).

Управління виконавчими пристроями, такими як сирена, лампа, нагрівач і електронні замки. Відправлення сповіщень через GSM-модуль у разі виявлення небезпеки. Проведено симуляційне тестування алгоритмів у середовищі TIA Portal: Підтверджено коректність роботи таймера для затримки активації сирени.

Система є надійною і забезпечує високий рівень автоматизації охоронних функцій. Реалізована логіка роботи є адаптивною до різних сценаріїв: Затримка активації сирени дозволяє уникнути помилкових тривог. Інтеграція з кількома датчиками дозволяє підвищити функціональність системи. Підтверджена точність виконання алгоритмів, що відповідає вимогам охоронних систем.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Frank Petruzella “Programmable Logic Controllers”. (Petruzella, Frank D., author. Programmable logic controllers / Frank D. Petruzella.—Fifth edition. pages cm. Includes index. ISBN 978-0-07-337384-3

2. PLC Based Alarm System. Fundamental Structure. [Електронний ресурс]. – Режим доступу: https://www.netiotek.com/en/knowledge-004-en/

3. PLC Program for Alarm Security System. [Електронний ресурс]. – Режим доступу: https://instrumentationtools.com/plc-program-for-burglar-alarm-security-system/

4. Siemens S7-1200 System Manual [Електронний ресурс]. – Режим доступу: https://cache.industry.siemens.com/dl/files/241/109797241/att_1066673/v1/s71200_system_manual_en-US_en-US.pdf

5. John R. Programmable Logic Controllers: Programming Methods and Applications /John R. Hackworth, Frederick D. Hackworth/ Pearson/Prentice Hall, 2004. 303 стор. ISBN: 0130607185, 9780130607188

6. All About Automation [Електронний ресурс]. – Режим доступу: https://www.allaboutautomation.de/en/

7. Стандарт IEC 61131-3 [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/IEC_61131-3

8. Siemens Industry Online Support [Електронний ресурс]. – Режим доступу: https://support.industry.siemens.com/cs/start?lc=en-UA

9. OpenPLC [Електронний ресурс]. – Режим доступу: https://autonomylogic.com/

ДОДАТКИ

Додаток А

Структурна схема

Додаток Б

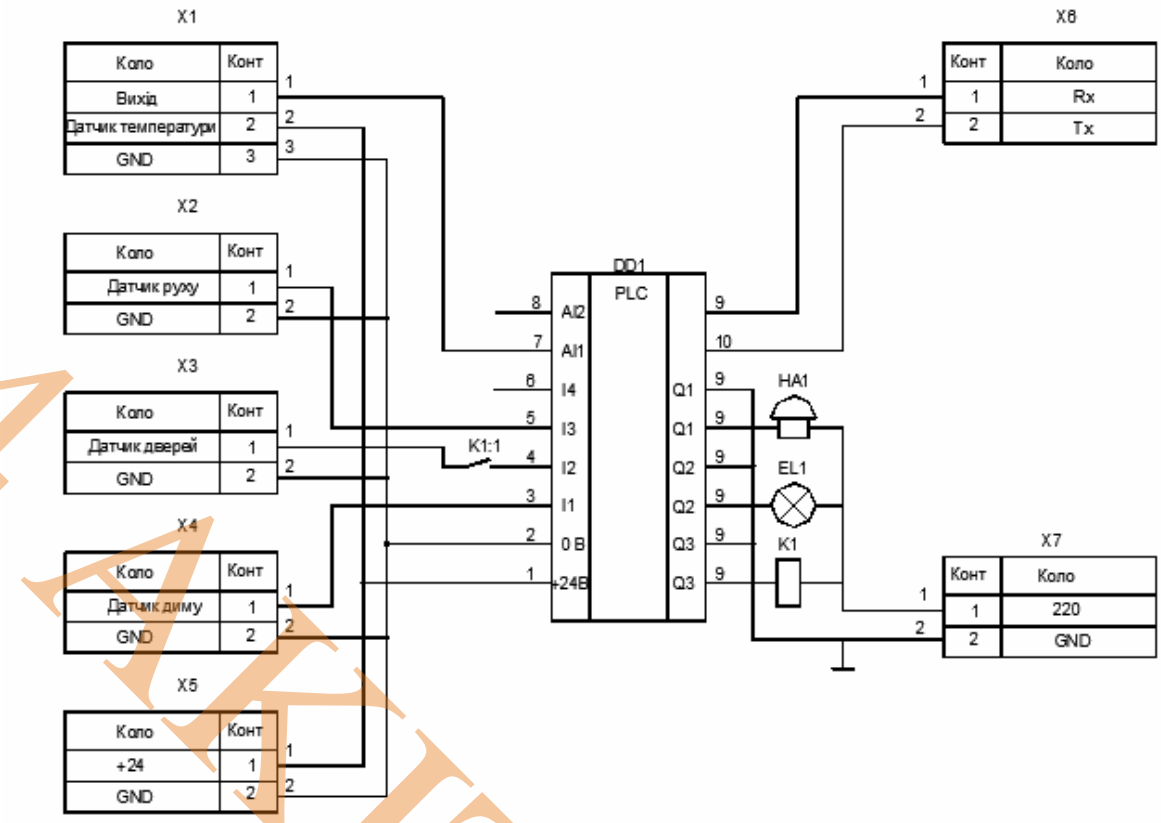
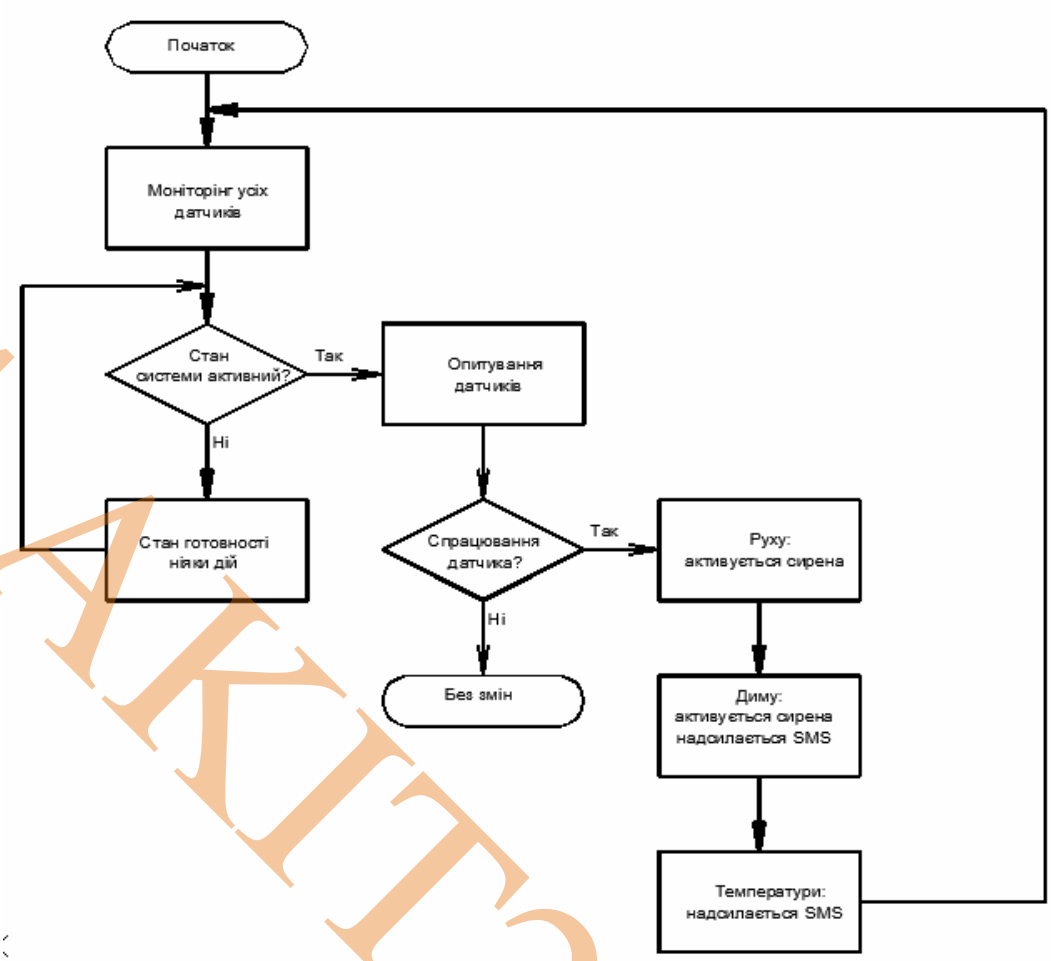


Схема електрична принципова

Додаток в



Алгоритм