ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ

КВАЛІФІКАЦІЙНА РОБОТА
на тему: «ІОТ-СИСТЕМА ДЛЯ ЗАПОБІГАННЯ АВАРІЙ У ПРОМИСЛОВИХ СИСТЕМАХ НА ОСНОВІ АНАЛІЗУ СЕНСОРНИХ ДАНИХ»

на здобуття освітнього ступеня магістра
зі спеціальності 126 Інформаційні системи та технології
(код, найменування спеціальності)
освітньо-професійної програми Інформаційні системи та технології
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Сергій БОНДАРЕНКО
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. ІСДМ-61
Сергій БОНДАРЕНКО
Ім'я, ПРІЗВИЩЕ
Керівник: Ірина СРІБНА
д. т. н., доцент Ім'я, ПРІЗВИЩЕ

Рецензент: _____
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Інформаційних технологій

Кафедра Інформаційних систем та технологій

Ступінь вищої освіти Магістр

Спеціальність 126 Інформаційні системи та технології

Освітньо-професійна програма Інформаційні системи та технології

ЗАТВЕРДЖУЮ
Завідувач кафедрою ІСТ
_____Каміла СТОРЧАК
«____» _____2025р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Бондаренку Сергію Юрійовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: IoT-рішення для запобігання аварій у промислових системах на основі аналізу сенсорних даних
керівник кваліфікаційної роботи Ірина СРІБНА, д. т. н., доцент,
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «30» жовтня 2025р. № 467

2. Строк подання кваліфікаційної роботи «26» грудня 2025р.

3. Вихідні дані до кваліфікаційної роботи:
   1. Науково-технічна література;
   2. Принципи функціонування IoT;
   3. Список апаратних компонентів;
   4. Інструменти для збору та аналізу даних.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
   1. Дослідження технологій та тенденцій розвитку Інтернету речей;
   2. Принцип роботи рішень для запобігання аварій у промислових системах;
   3. Розробка IoT-рішення для запобігання аварій у промислових системах на основі аналізу сенсорних даних.

5. Перелік ілюстративного матеріалу: *презентація*

6. Дата видачі завдання «30» жовтня 2025р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз технічної літератури	30.10-06.11.25	
2	Аналіз можливостей, технологій та тенденцій розвитку IoT	07.11-14.11.25	
3	Дослідження методів та концепцій запобігання аварій у промислових системах	15.11-22.11.25	
4	Розробка архітектури апаратного забезпечення IoT-рішення	22.11-29.11.25	
5	Розробка програмного забезпечення для запобігання аварій у промислових системах	30.11-07.12.25	
6	Тестування розробленої IoT-системи	8.12-15.12.25	
7	Оформлення бакалаврської роботи: вступ, висновки, реферат	16.12-23.12.25	
8	Розробка демонстраційних матеріалів	23.12-26.12.25	

Здобувач вищої освіти _____ Сергій БОНДАРЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Ірина СРІБНА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 86 стор., 14 рис., 30 джерел.

Мета роботи – розробка апаратного модуля та програмного забезпечення IoT-рішення для запобігання аварій у промислових системах із застосуванням аналізу сенсорних даних.

Об'єкт дослідження – процес виявлення та запобігання аварій у промислових системах.

Предмет дослідження – методи та алгоритми аналізу сенсорних даних.

У роботі проведено аналіз наявних технологій та архітектури Інтернету Речей. Розглянуто технічні аспекти запобігання аварій та їх інтеграцію з IoT. Досліджено основи моніторингу стану та принципи роботи SCADA. Вивчено роботу протоколу MQTT. Підібрано апаратне та розроблено програмне забезпечення IoT системи запобігання аварій на основі сенсорного аналізу.

КЛЮЧОВІ СЛОВА: ІНТЕРНЕТ РЕЧЕЙ, ЗАПОБІГАННЯ АВАРІЙ, ПРОМИСЛОВА СИСТЕМА, СЕНСОР, СЕНСОРНІ ДАНІ, СЕНСОРНИЙ АНАЛІЗ, МОНІТОРИНГ СТАНУ, SCADA

ABSTRACT

Text part of the master's qualification work: 86 pages, 14 pictures, 30 sources.

The purpose of the work is to develop hardware module and software of an IoT solution for accident prevention in industrial systems using sensory data analysis.

Object of research – the process of detecting and preventing accidents in industrial systems.

Subject of research – methods and algorithms of sensory data analysis.

The work analyzes existing technologies and the architecture of the Internet of Things. The technical aspects of accident prevention and their integration with IoT were examined. The basics of condition monitoring and the principles of SCADA operation were researched. The operation of the MQTT protocol was studied. Hardware was selected and software was developed for an IoT accident prevention system based on sensory analysis.

KEYWORDS: INTERNET OF THINGS, ACCIDENT PREVENTION, INDUSTRAL SYSTEM, SENSOR, SENSORY DATA, SENSORY ANALYSIS, CONDITION MONITORING, SCADA

ЗМІСТ

ВСТУП

Актуальність теми. Розвиток промисловості передбачає зростання потреби у сучасних заходах безпеки. З удосконаленням технологій Інтернет речей (IoT) став рушійною силою у підвищенні безпеки на робочому місці. Інтеграція IoT рішень дозволяє компаніям ефективніше управляти заходами безпеки. Ця тенденція простежується у різних секторах, від охорони здоров'я до виробництва. Через неї організації усвідомлюють, як потенціал IoT допомагає створити безпечніші робочі середовища. Традиційні методи безпеки включають паперову документацію, ручні перевірки та реактивні заходи у випадку появи інцидентів. Завдяки IoT ця динаміка змінюється, а безпека на робочому місці стає оперативною та динамічною системою а не статичним набором правил.

Проактивний характер моніторингу стану на багатьох рівнях є інноваційним кроком вперед для виробників. По-перше, персонал підприємства стає більш захищеним. По-друге, він дозволяє керівникам підприємств запобігти незапланованим простоям через вихід з ладу обладнання та одночасно найефективніше використати заплановані простої для технічного обслуговування декількох машин і вирішення всіх наявних проблем. Крім того, моніторинг стану усуває непотрібні витрати, пов'язані з надмірним обслуговуванням справного обладнання на основі лише статичних показників робочого часу.

Мета і завдання дослідження. Метою роботи є розробка апаратного модуля та програмного забезпечення IoT-рішення для запобігання аварій у промислових системах із застосуванням аналізу сенсорних даних.

Для досягнення цієї мети необхідно виконати наступні завдання:

— провести аналіз можливостей, технологій та тенденцій розвитку IoT та методів запобігання аварій у промислових системах;

— розробити архітектуру апаратного та програмного забезпечення IoT-рішення, включаючи вибір компонентів та протоколів зв'язку;

— провести тестування розробленої IoT-системи;

Об'єкт дослідження – процес виявлення та запобігання аварій у промислових системах.

Предмет дослідження – методи та алгоритми аналізу сенсорних даних.

Методи дослідження. Під час написання магістерської кваліфікаційної роботи були використані методи теоретичного аналізу літературних джерел, імітаційного моделювання IoT-системи, експериментальне дослідження результатів роботи прототипу.

Наукова новизна. В роботі розроблено новий підхід до запобігання аварій, який враховує як прогнозовані, так і реальні дані роботи промислових систем, а також представлено модель створеної IoT-системи.

Апробація результатів та публікації.

Апробація результатів здійснювалась у формі участі в III Всеукраїнській науково-технічній конференції «Технологічні горизонти: дослідження та застосування інформаційних технологій для технологічного прогресу України і світу» та Науково-практичній конференції «Проблеми комп'ютерної інженерії».

Практична значущість отриманих результатів. Отримані наукові результати надають ефективне рішення для виявлення та запобігання промислових аварій на основі сенсорного аналізу.

1 АНАЛІЗ ОСНОВНИХ ТЕХНОЛОГІЙ ТА ТЕНДЕНЦІЙ РОЗВИТКУ ІНТЕРНЕТУ РЕЧЕЙ У СФЕРІ ЗАПОБІГАННЯ АВАРІЙ

1.1 Огляд наявних технологій та розробок Інтернету Речей

IoT продовжує змінювати наше життя, завдяки новим технологіям та пристроям IoT, що регулярно з'являються на ринку. Надаючи дані в режимі реального часу, автоматизацію та дистанційне керування пристроями, IoT може сприяти підвищенню ефективності операцій, покращенню процесу прийняття рішень та розробці нових продуктів і послуг.

Інтернет речей, або IoT, — це мережа взаємопов'язаних пристроїв, які підключаються та обмінюються даними з іншими пристроями IoT і хмарними сховищами. Пристрої IoT зазвичай оснащені технологіями, такими як датчики та програмне забезпечення, і можуть включати механічні та цифрові машини.

Ці пристрої охоплюють все, від повсякденних побутових предметів до складних промислових інструментів. Все частіше організації в різних галузях використовують IoT для більш ефективної роботи, надання покращеного обслуговування клієнтів, вдосконаленого прийняття рішень та підвищення вартості бізнесу. За допомогою IoT дані можна передавати через мережу без необхідності взаємодії між людьми або між людиною та комп'ютером.

Річчю в Інтернеті речей може бути людина з імплантованим кардіомонітором, сільськогосподарська тварина з біочіп-транспондером, автомобіль із вбудованими датчиками, що попереджають водія про низький тиск у шинах, або будь-який інший природний чи штучний об'єкт, якому можна присвоїти IP-адресу та який може передавати дані через мережу.

Для функціонування екосистеми IoT необхідні наступні чотири елементи:

- Апаратне забезпечення (АЗ): воно призначене для конкретної мети, наприклад, для використання датчиків обміну даних або контролю температури. Існує три поширені типи АЗ IoT: виконавчі пристрої, датчики та шлюзи. Датчики можуть виявляти та вимірювати зміни в навколишньому середовищі (наприклад,

вологість та освітлення). Їх можна використовувати в таких сферах, як промисловий моніторинг та медицина. Виконавчі пристрої дистанційно керуються для виконання конкретних дій, таких як відкриття дверей або керування вентилем. Вони часто використовуються в домашній автоматизації та робототехніці. Шлюзи діють як ворота для підключення та маршрутизації даних між хмарним сховищем та IoT пристроями. Вони включають таке апаратне забезпечення, як процесори та модулі IoT, які дозволяють пристроям спілкуватися за допомогою стільникового зв'язку, Bluetooth та Wi-Fi.

- Програмне забезпечення: набір програм, які допомагають виконувати такі завдання, як збір, обробка, зберігання даних та аналіз команд на основі цих даних. Деякими прикладами з до цієї категорії є операційні системи, прошивка, додатки, проміжне програмне забезпечення. Збір даних охоплює зчитування даних, їх фільтрування, вимірювання, агрегування та, під кінець, управління їх безпекою. Збір даних здійснюється з різних джерел, розподіляється між пристроями, а потім надходить до центрального сховища. Інтеграція пристроїв — це процес зв'язування інтелектуальних пристроїв, додатків, баз даних і систем для полегшення обміну даними та забезпечення автоматизації потоків робіт. Цей процес керує всіма обмеженнями, протоколами та додатками, які обробляються належним чином для забезпечення зв'язку між пристроями. Над зібраними та обробленими даними можуть виконуватися автоматизовані завдання, які аналізують ці дані та виявляють певні закономірності.

- Комунікації: хоча підключення до Інтернету речей є технологією, яка забезпечує його функціонування, саме комунікація IoT пристроїв з Інтернетом дозволяє рішенням генерувати вартість. Обмін даних між шлюзами і пристроями IoT і далі в хмару, дозволяє здійснювати їх обробку, аналіз і зберігання. IoT об'єднує телекомунікації та протоколи IT разом з кількома IoT-специфічних протоколів, які допомагають оптимізувати та стандартизувати процеси комунікації;

- Платформа: вона є програмною інфраструктурою, яка з'єднує, управляє та координує мережу IoT пристроїв, створюючи цілісну екосистему. Ці платформи

полегшують комунікацію між пристроями через Інтернет і, як правило, інтегруються з існуючими системами, включаючи додатки та озера даних. Потім вони компілюють, аналізують та обмінюються даними з цих пристроїв і таким чином автоматизують завдання та генерують аналітичну інформацію.

- IoT допомагає людям приймати розумніші рішення в житті і роботі. Споживачі, наприклад, можуть використовувати пристрої з вбудованим IoT, такі як автомобілі, смарт-годинники або термостати, щоб поліпшити своє життя. Наприклад, коли людина приїжджає додому, її автомобіль може зв'язатися з гаражем, щоб відкрити двері, термостат може налаштуватися на задану температуру, а освітлення може бути встановлено на меншу інтенсивність і колір. Разом з автоматизацією будинків за допомогою розумних пристроїв, IoT є важливою частиною бізнесу. Він надає організаціям погляд на роботу їхніх систем в режимі реального часу, надаючи інформацію про все, від продуктивності обладнання до ланцюгів постачання та логістики.

- Пристрої IoT можуть підвищити ефективність та якість обслуговування пацієнтів при інтеграції у вертикальний ринок, як охорона здоров'я. Це поєднання відоме, як Інтернет медичних речей або IoMT.

IoT дозволяє машинам виконувати монотонні завдання без людського втручання. Компанії можуть автоматизувати процеси, зменшити ціни на працю, скоротити відходи та поліпшити якість обслуговування. За допомогою Інтернету речей можливо здешевити виробництво та доставку товарів, а також забезпечує прозорість транзакцій клієнтів. IoT продовжує розвиватися, оскільки все більше підприємств усвідомлюють потенціал під’єднаних пристроїв для збереження своєї конкурентоздатності.

Далі наведені типові приклади використання Інтернету речей:

- Аграрне виробництво: IoT може покращити фермерську справу, полегшуючи їхню роботу. Наприклад, за допомогою датчиків можливо збирати дані про температуру, вологість та кількість опадів, склад ґрунту, а також автоматизувати технології сільського господарства. Крім того, пристрої IoT можна використовувати для контролю стану здоров'я худоби, моніторингу

обладнання та оптимізації постачальних ланцюгів;

- Будівництво: Інтернет Речей дозволяє контролювати операції, пов'язані з інфраструктурою. Датчики можуть контролювати події або зміни в будівельних спорудах, мостах та іншій інфраструктурі, які можуть становити потенційні загрози безпеці. Це забезпечує такі переваги, як поліпшення реагування на надзвичайні ситуації, зниження операційних витрат та поліпшення якості обслуговування;
- Домашня автоматизація: Інтернет Речей можна застосовувати у сфері домашньої автоматизації для спостереження та управління електричними системами будівель. Власники житла також можуть дистанційно контролювати та автоматизувати своє домашнє середовище за допомогою пристроїв IoT, включаючи інтелектуальні термостати, системи освітлення, камери безпеки та голосові помічники, такі як Alexa та Siri, для підвищення комфорту та енергетичної ефективності;
- Розумні будинки та Розумні міста: вони можуть допомогти громадянам зменшити кількість відходів та споживання енергії. У цьому випадку датчики IoT можуть зменшити витрати на енергію, визначаючи кількість людей у приміщенні та вмикаючи кондиціонер, якщо вони виявляють, що конференц-зал заповнений, або зменшуючи опалення, коли офіс порожній;
- Системи міського управління: технології IoT також можуть керувати та спостерігати за технологіями міського управління, таким як світлофори, паркомати, мережі громадського транспорту та системи управління відходами;
- Моніторинг стану здоров’я: такі розумні пристрої, як системи дистанційного моніторингу пацієнтів, розумні медичні пристрої та трекери ліків, дозволяють медичним працівникам контролювати стан здоров'я пацієнтів, контролювати хронічні захворювання та вчасно проводити медичне втручання. IoT дає лікарям можливість детальніше спостерігати за пацієнтами. Лікарні також часто використовують системи IoT для виконання таких завдань, як управління медичними запасами та інструментами;
- Роздрібна торгівля: за допомогою датчиків та маячків IoT у

роздрібних магазинах можуть відстежувати переміщення клієнтів, аналізувати закономірності покупок, керувати інвентарем та персоналізувати рекламні повідомлення. Це покращує досвід покупців та оптимізує складські операції;

- Транспорт: прилади Інтернету Речей допомагають транспортній галузі за допомогою моніторингу ефективності автомобілів, оптимізації маршрутів та відстеження поставок. Приміром, ефективність палива під'єднаних автомобілів можливо відстежувати, щоб підвищити сталість довкілля та зменшити витрати на паливо. Ці пристрої можуть також відслідковувати стан вантажу, завдяки чому він досягає місця призначення в найкращому стані;
- Носимі пристрої: такі пристрої з датчиками та програмним забезпеченням можуть збирати та аналізувати дані користувачів, надсилаючи повідомлення іншим технологіям, щоб зробити їхнє життя простішим та комфортнішим. Носимі пристрої також використовуються для захисту громадської безпеки: наприклад, шляхом скорочення часу реагування служб екстреної допомоги під час надзвичайних ситуацій шляхом надання оптимізованих маршрутів до місця події або відстеження життєвих показників будівельників чи пожежників у небезпечному середовищі;
- Енергетичний менеджмент: інтелектуальні мережі, інтелектуальні лічильники та системи енергетичного менеджменту на базі Інтернету речей дають змогу комунальним підприємствам і споживачам контролювати та оптимізувати використання енергії, керувати програмами реагування на попит та ефективніше інтегрувати відновлювані енергоносії. Приміром, дані, зібрані датчиками та пристроями, допомагають виявляти закономірності, пікові періоди використання та області неефективності.

Повний перелік застосувань IoT зображено на рис 1.1.

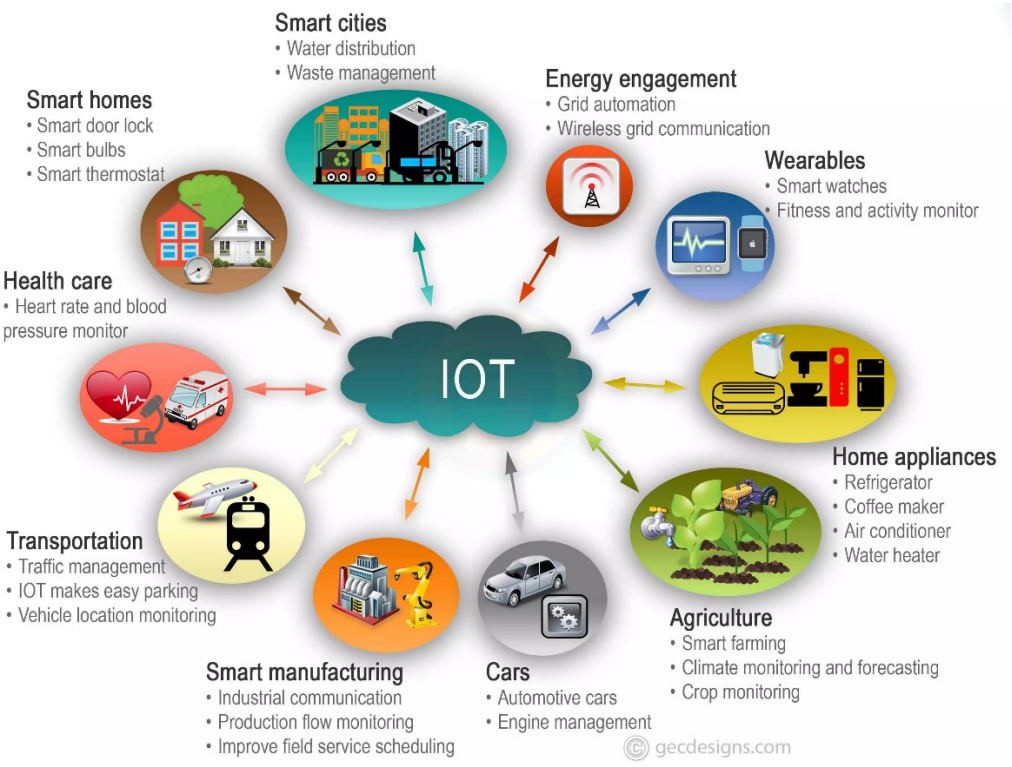


Рис. 1.1 Приклади застосування IoT [1]

1.2 Архітектура та інфраструктура IoT

Чим автоматизований пристрій, такий як вимикач світла, що активується датчиком, відрізняється від під'єднаного до Інтернету речей пристрою, який виконує ту ж річ? Одним словом: даними. У пристрої, під'єднаному до Інтернету речей, коли датчик виявляє рух і актуатор вмикає світло, ці дії фіксуються як дані і надсилаються до хмари або центру обробки даних для запису та аналізу. А там, де є дані, має бути архітектура Інтернету речей, яка вказує, куди надсилати дані, який формат використовувати, як їх отримати і які дії вживати на їх підставі. Процеси архітектури IoT надсилають дані в іншому напрямку теж у вигляді команд або інструкцій, що вказують актуатору або іншому фізично підключеному пристрою прийняти певні дії для контролю над фізичними процесами. Актуатор може виконувати такі прості дії, як увімкнення світла, або такі серйозні, як зупинка конвеєрної лінії, якщо виявлено загрозу відмови.

В архітектурі системи IoT часто описується у чотирьох етапах, як показано на рис. 1.2, де дані надходять від датчиків, приєднаних до «речей», через мережу

і, зрештою, до корпоративного дата-центру або хмари для обробки, аналізу та зберігання:

1) Датчики та актуатори: вони є критично важливими компонентами багатьох сучасних технологій, включаючи пристрої Інтернету речей, промислову автоматизацію, робототехніку, аналізатори і багато іншого. Розумний датчик — це пристрій, який приймає вхідні дані з фізичного середовища, такі як потік або тиск, і використовує свої вбудовані обчислювальні ресурси для виконання заздалегідь визначених функцій після виявлення конкретних вхідних даних, а потім обробляє дані перед їх передачею. Розумні актуатори за своїми можливостями схожі на розумні датчики. Використовуючи подібні конструкції цифрових комунікацій та мікропроцесорні системи збору та аналізу, ці пристрої інтегрують додаткові можливості, такі як алгоритми управління та інтерфейси комунікації. Датчики та актуатори відіграють важливу роль в автоматизації, оскільки їхні розширені можливості обробки дозволяють датчику зберігати власні параметри конфігурації, масштабувати вхідні дані до заданого діапазону або рівня сигналу, генерувати сигнали тривоги, визначати свій стан за допомогою діагностичних процедур та надавати обчислені значення, такі як сумарний потік або середня температура;

2) Інтернет-шлюзи та системи збору даних: цей етап функціонує в безпосередній близькості до датчиків та актуаторів, але залишається окремим рівнем, що вимагає власного огляду. Шлюзи перетворюють дані, зібрані датчиками, у формати, зрозумілі решті системи. У великих розгортаннях, що можуть включати мільйон датчиків або більше, цей шар знаходиться під тиском, щоб агрегувати, відбирати та транспортувати великі обсяги інформації, що ймовірно, продовжать зростати, оскільки системи Інтернету речей стають все більш зв'язаними. Шлюзи мають центральне значення для безпеки тому, що вони управляють інформаційними потоками в обидві сторони, як портали від окремого датчика до системи, що з застосуванням відповідних засобів шифрування та безпеки можуть допомогти запобігти як витоку даних із хмари, так і атакам на IoT девайси;

3) Попередня обробка: обробка даних може відбуватися на сервері або на кордоні і включає в себе такі операції з даними:

- Фільтрування даних — це моніторинг даних пристрою та прийняття або відхилення всього повідомлення або його частини на основі заздалегідь визначених показників. Наприклад, додавання та видалення полів із застарілих профілів даних для їх стандартизації з новими форматами;
- Перетворення даних — це операції трансформації та маніпулювання даними, щоб їх стандартизувати та поліпшити зрозумілість. Наприклад, розширення літери «C» в полі температури до «Celsius»;
- Збагачення даних — це додавання контекстних даних до повідомлень пристроїв. Наприклад, додавання ідентифікатора клієнта до поточного повідомлення на основі ID пристрою;
- Аналіз даних займається такими завданнями, як отримання висновків з даних у реальному часі та взаємодія з моделями машинного навчання. Це, мабуть, найважливіший компонент архітектури IoT, орієнтованої на дані. Наприклад, отримання ключового показника ефективності (KPI) на основі даних пристроїв IoT для розуміння ефективності обладнання або застосування моделі машинного навчання з профілактичного обслуговування для усунення пошкоджень до того, як вони настануть;

4) Детальний аналіз у хмарі або дата-центрі: хмарні обчислення в Інтернеті речей представляють собою використання хмарної інфраструктури для підтримки IoT екосистем. Поки пристрої IoT генерують величезні обсяги даних, хмарні платформи централізовано зберігають, обробляють і аналізують ці дані, забезпечуючи можливість отримання оперативних даних та прийняття рішень. На відміну від звичайних локальних рішень, хмарні системи усувають необхідність у дорогих фізичних серверах і дозволяють підприємствам без зусиль масштабувати операції. Поки окремі пристрої збирають дані та виконують певні дії, хмара забезпечує централізоване зберігання та обробку даних, розширені аналітичні можливості та інтеграцію між різними пристроями та системами.

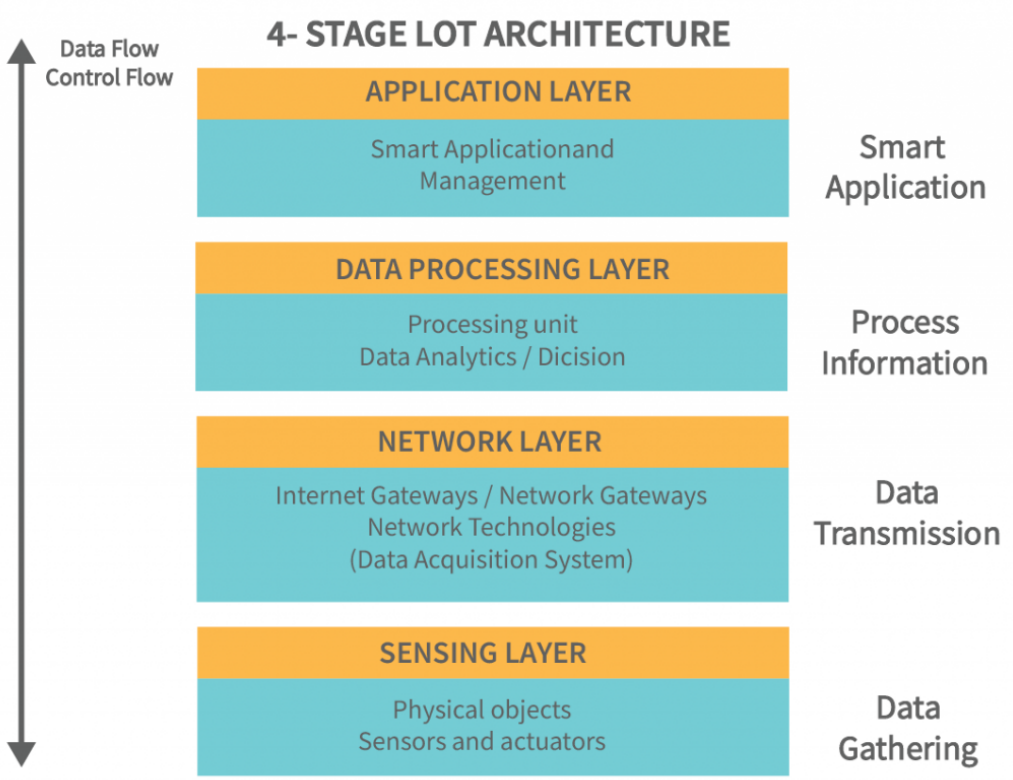


Рис. 1.2 Етапи архітектури IoT[2]

Основне питання, що задають багато інженерів під час підготовки до проектування мереж: «Яка топологія найкраще підійде для моєї реалізації?» Серед варіантів є протоколи мереж типу mesh, такі як Zigbee, а також протоколи «точка-точка» або «точка-мультиточка». У деяких випадках на основі раніше поставлених питань стає зрозуміло, яка топологія підходить найкраще. В інших випадках потрібні додаткові випробування та дослідження.

Mesh-мережа.

Мережеві інженери часто мають досвід роботи з певною топологією і можуть припустити, що її можна використовувати в будь-яких умовах, але іноді для різних сценаріїв використання більш оптимальним буде інший вибір. Щоб визначити, чи є mesh-топологія хорошим вибором для певного застосування, важливо розуміти переваги та недоліки цієї стратегії. Критичним фактором, який необхідно проаналізувати, є часові вимоги системи. Mesh-топології маршрутизують дані від вузла до вузла по мережі, яка побудована у вигляді сітки. Тому необхідно враховувати кількість «стрибків» через додану затримку.

Остаточне рішення належить інженеру мережі, але наявність варіантів для різних топологій може мати критичне значення для успіху бездротового розгортання.

Особливості mesh-мережі:

- Mesh-мережа має перевагу у вигляді підтримки великої кількості вузлів у мережі — у деяких випадках до тисячі, залежно від архітектури.
- Дані знаходять шлях від вузла до вузла до шлюзу;
- Якщо вузол зникає в мережі, мережа знову знаходить новий шлях, щоб забезпечити передачу даних у шлюз;
- При додаванні вузлу до мережі та його виявлення мережа може маршрутизувати дані через цей вузол;
- Mesh-мережа забезпечує резервування, дозволяючи використовувати кілька шляхів від вузла або пристрою до шлюзу, і має змогу адаптуватися до змін умов;
- Можливе створення підмереж для відокремлення даних від сусідніх мереж. Це надзвичайно корисна функція для щільної мережі з тисячами вузлів, наприклад сонячної електростанції або системи розумного освітлення, де затримка не створює проблем.

Точка-точка або точка-мультиточка.

Бездротові мережі точка-точка (PTP) і точка-мультиточка (PTMP) — це топології, що використовуються для з'єднання в широкому діапазоні застосувань, наприклад у випадках, коли потрібно замінити кабелі бездротовим з'єднанням. Вони забезпечують зв'язок між двома пристроями (точка-точка) або від одного пристрою до багатьох (точка-мультиточка). Є кілька факторів, які слід враховувати, таких як відстань, час і заряд батареї, які можуть вказувати на те, чи потрібна PTP мережа, а не mesh.

Ось деякі основні особливості протоколів PTP і PTMP:

- Якщо потрібне бездротове з'єднання для декількох пристроїв, які знаходяться на відстані однієї-двох миль, і є пряма видимість, PTP може бути найпростішим рішенням;
- PTP або PTMP можуть бути ефективними для пристроїв, що працюють

від батарей. Дані можна надсилати за потреби, а потім увімкнути режим сну залежно від потреб зв'язку. Не є рідкістю, коли батареї в пристроях типу PTP/PTMP працюють декілька років;

- На противагу, mesh-мережа збільшує затримку і споживає більше енергії, оскільки для її роботи потрібен маршрутизатор або ретранслятор, що живиться від електромережі.

Тому, якщо мережа досить невелика і діапазон чіткий, PTP/PTMP має багато переваг над mesh-мережею. Ще одна перевага мереж PTP і PTMP полягає в тому, що вони дуже прості і швидкі в налаштуванні. Вони добре працюють з протоколами, що мають жорсткі вимоги до синхронізації, як Modbus.

Пряме підключення до стільникового зв'язку, Bluetooth та Wi-Fi.

На додаток до IoT архітектур, які були обговорені, можливо безпосередньо підключати пристрої до хмари через стільниковий зв'язок та Wi-Fi, якщо це виправдовують обставини.

Найпоширенішим протоколом є Wi-Fi. Однак важливо враховувати доступність Інтернету на сайті клієнта, а також його політику безпеки. Отримання дозволу на підключення пристроїв IoT до чужої мережі Wi-Fi не завжди є швидким процесом. Це може вимагати додаткової перевірки безпеки, а в деяких випадках буде просто неможливим через корпоративну політику клієнта.

Важливі міркування щодо стільникових застосувань:

- При підключенні за допомогою мобільних радіостанцій необхідно переконатися, що є доступ до стільникової мережі, яка зазвичай доступна в більшості міських районів, але може бути проблемою в сільських районах;
- Необхідно враховувати швидкість передачі даних. Протоколи LTE-M і LTE Cat-1 ідеально підходять для більшості додатків IoT, які надсилають дані з датчиків до хмари;
- Також необхідно брати до уваги активації, тарифні плани, управління SIM-картами та віддалене управління пристроями, оскільки для підтримки стільникового з'єднання для пристроїв IoT потрібно більше

рухомих частин.

Мережа Drop-in.

Підключення віддалених датчиків або пристроїв через бездротовий канал до інтелектуального шлюзу, який має опції для передачі даних через стільниковий зв'язок, Wi-Fi або Ethernet, є перевіреним методом. Дані збираються з віддаленого пристрою або датчика, а потім надсилаються через бездротовий канал на розумний шлюз. Потім шлюз передає дані до хмари для аналізу або контролю.

У середовищі SCADA або телеметрії впроваджується шлюз, який має можливість передачі даних, а також здатність підключатися до віддалених радіочастотних вузлів для передачі туди й назад.

У деяких застосуваннях мереж drop-in все, що потрібно, — це стільниковий маршрутизатор, підключений до пристроїв. Одним прикладом є кіоск або POS-термінал у роздрібному магазині, який використовує стільниковий зв'язок для обробки транзакцій.

Ще однією перевагою drop-in мережі є те, що не потрібно покладатися на існуючу мережу або отримувати дозвіл на приєднання. Часто отримання дозволу на приєднання до мережі Wi-Fi клієнта може зайняти більше часу, ніж проектування та розгортання власної. Створення drop-in мережі дає гнучкість для вирішення, яка топологія працює найкраще: point-to-point, point-to-multipoint або mesh, а також контролювати всі аспекти мережі.

Mesh мережі з тисячами вузлів, які часто зв'язуються з шлюзом, чудово підходять для таких застосувань, як вуличне освітлення та сонячні поля. Використання радіостанції з великим радіусом дії 900 МГц у застосуванні PTP або PTMP з топологією мережі Drop-in може допомогти охопити пристрої, які розташовані на великих відстанях, наприклад на нафтовому родовищі або в сільському господарстві.

1.3 Технічні аспекти та підходи до запобігання аварій

Коли люди думають про технології на робочому місці, вони зазвичай мають на увазі лише ті, що підвищують продуктивність праці або сприяють розвитку IT-

стратегій. Однак на робочому місці існує багато типів технологій. Компанії починають приділяти більше уваги їх використанню для забезпечення здоров'я та безпеки на робочому місці, щоб відповідати новим законам і стандартам. Технології вже багато років запобігають смертності та травмам працівників, але нові передові інструменти пропонують вдосконалення охорони праці.

Носимі пристрої.

Засоби індивідуального захисту (ЗІЗ) є невід'ємною частиною захисного вбрання працівників. Ці засоби слугують першою лінією захисту в разі нещасного випадку. Інновації в області носимих технологій, та мініатюризація датчиків дозволили стартапам і масштабним компаніям, що займаються технологіями безпеки, перетворити ЗІЗ на розумні пристрої. Ці розумні ЗІЗ здатні контролювати стан як працівника, так і його оточення. Вони також оснащені кнопкою тривоги, яка спрацьовує вручну або автоматично при виявленні падіння або нещасного випадку. Інші інновації в області носимих пристроїв привели до розробки екзоскелетів, які допомагають працівникам у виконанні завдань. Окрім цих промислових рішень, деякі стартапи також зосереджуються на носимих рішеннях для офісних середовищ, які стежать за життєвими показниками працівників. Таким чином, ця тенденція в галузі охорони праці надає організаціям інформацію про здоров'я та безпеку працівників, які працюють у режимі реального часу у різних місцях.

Носимі технології поділяються на чотири категорії:

- Фізіологічний моніторинг — пристрої, що відстежують температуру тіла, частоту серцебиття, дихання та інші фізіологічні показники, можуть допомогти визначити, коли працівник відчуває втому або стрес і, отже, піддається більшому ризику;
- Моніторинг навколишнього середовища — ці носимі пристрої можуть попереджати співробітників про небезпечну якість повітря або температурні умови, які можуть спричинити травми;
- Сенсори наближення- цей тип носимих пристроїв, які можуть бути вбудовані в засоби індивідуального захисту (ЗІЗ), такі як каски, можуть

допомогти запобігти потраплянню співробітників у небезпечні зони або надто близькому наближенню до устаткування;

- Екзоскелети та екзокостюми — надаючи допоміжну силу для фізичних завдань, таких як підйом важких предметів або тривале стояння, ці носимі пристрої можуть допомогти запобігти травмам і дозволити співробітникам швидше продовжити роботу.

Американський стартап Verve Motion розробляє носимі роботизовані пристрої для працівників, які займаються підйомом і переміщенням вантажів. SafeLift Suit — це м'який і легкий екзокостюм, який носять як рюкзак. Він забезпечує до 240 ньютонів сили підйому, знімаючи 40% навантаження з працівника при кожному підйомі. Він також оснащений передовою системою аналізу рухів з бездротовим підключенням та інтуїтивно зрозумілою системою управління, що дозволяє налаштовувати роботу під користувача та трудову діяльність. Це рішення безпосередньо знижує рівень травм, покращує досвід працівників та забезпечує їх утримання на робочому місці.

Канадський стартап SolusGuard пропонує носимі тривожні кнопки для працівників, які працюють наодинці. Швидке натискання кнопки запускає мобільний додаток SolusGuard, який сповіщає мережу контактів для екстрених ситуацій. Це позбавляє працівників необхідності розблоковувати телефони, відкривати додаток або дзвонити в небезпечних ситуаціях. Крім того, запатентована технологія SolusGuard, що захищає від збоїв, запускає екстрені дзвінки, навіть якщо телефон працівника вимкнений або недоступний. Це дає перевагу над іншими кнопками тривоги, сприяючи швидшому реагуванню до загострення ситуації.

Програмне забезпечення для звітування про робочу безпеку.

Комунікація дуже важлива для ефективного функціонування системи управління безпекою. Традиційні методи, що передбачають використання паперу та електронних таблиць, призводять до повторюваних і рутинних завдань навіть для звітування про незначні порушення безпеки. Більше того, відсутність динамічної панелі інструментів, що самостійно оновлюється, може призвести до

пропущення певних даних, які неможливо відновити з документів, заповнених вручну. Цифрові інновації, зумовлені новими технологіями хмарних обчислень та розробкою API, призвели до появи програмного забезпечення для звітування з питань безпеки, яке автоматизує завдання з керування безпекою. Веб-програмне забезпечення та мобільні додатки допомагають в управлінні дозволами на роботу, інцидентами, дотриманням вимог безпеки, ризиками для працівників та аудитом. Плавне виконання цих заходів підвищує прозорість питань. Крім того, це сприяє отриманню практичних висновків щодо її процесів.

Американський стартап Resilienci пропонує платформу безпеки на робочому місці, яка контролює та стежить за стійкістю підприємства на рівні персоналу, робочих місць, ланцюгів постачання та об'єктів. Roamwell — це платформа, яка пропонує мобільні рішення та програмне забезпечення як послугу (SaaS) для забезпечення розумного та безпечного пересування робочої сили. Платформа присвоює кожному співробітнику особистий індекс ризику, що базується на його переміщеннях. Ці індекси надають керівництву та операційній команді рекомендації щодо управління ризиками збоїв в бізнесі. Платформа також підтримує динамічну інформаційну панель для візуалізації операційних загроз та уникнення порушення найважливіших функцій.

Американський стартап Odin пропонує повністю інтегроване програмне рішення, яке управляє ризиками для персоналу на будівельних майданчиках промислового рівня. Платформа стартапу автоматизує дотримання нормативних вимог і ведення бухгалтерського обліку, оцифровує записи про працівників і підрядників, а також переводить звітність про інциденти в електронний вигляд. Функція автоматичного дотримання нормативних вимог гарантує, що на будівельному майданчику працюють тільки кваліфіковані працівники, що знижує ризики для безпеки. Це економить час, дозволяючи уникнути рутинних завдань, і дає можливість керівникам майданчиків зосередитися на завданнях, що додають вартість до бізнесу.

Імерсивні технології.

Сьогодні багато постачальників технологій вже пропонують програми

навчання з безпеки у форматі віртуальної реальності (VR), які дозволяють співробітникам практикуватися у використанні обладнання та моделювати робочі середовища, що становлять потенційний ризик. VR також можна використовувати для навчань, таких як пожежна евакуація. У майбутньому технології віртуальної реальності та доповненої реальності (AR) можуть все частіше використовуватися для моделювання завдань з метою оцінки та зменшення ризиків до того, як працівник приступить до справжньої роботи.

Чеський стартап WeBoard розробляє навчальну екосистему, яка покращує якість та ефективність роботи співробітників за допомогою імерсивних цифрових мультимедійних матеріалів. Стартап створює навчальні сесії, поєднуючи віртуальну реальність передові моделі машинного навчання та. Симульована реальність робочого середовища дозволяє працівникам виконувати конкретні робочі процедури з дотриманням норм безпеки. WeDash — це хмарна платформа стартапу, яка відстежує результати навчання кожного співробітника в реальному часі. Це рішення не тільки робить навчання співробітників більш цікавим, але й допомагає організаціям самостійно досягати своїх цілей.

Польський стартап AIDAR пропонує платформу на базі VR та AR, яка сприяє ефективному навчанню співробітників і дозволяє передавати компетенції в віддалені місця. Платформа створює цифровий двійник навчальної станції і переносить виробничі процеси у віртуальну реальність. Співробітник виконує завдання безпечно і без фізичного ризику, а потім отримує оцінку та зворотний зв'язок. Таким чином, це рішення ефективно і безпечно розвиває компетенції співробітників.

Дрони та роботи.

Виробничі роботи, які виконують повторювані та підйомні завдання, вже давно дозволяють підприємствам зменшити кількість травм на робочому місці. Тепер підприємство може ще більше підвищити безпеку на робочому місці, доручаючи завдання з підвищеним ризиком складним, високомобільним роботам і дронам. Дрони, або безпілотні літальні апарати (UAS), можуть використовуватися будівельними компаніями та виробниками для мінімізації ризику падіння та

інших ризиків для співробітників шляхом інспектування об'єктів та відстеження операцій. Подібним чином, роботи можуть діставатися до небезпечних, важкодоступних місць, таких як тунелі та резервуари, для проведення інспекцій та відбору проб.

Шведський стартап FieldRobotix пропонує повністю автономні дрони для точного та надійного збору даних. Дизайн стартапу використовує модульний підхід, що дозволяє встановлювати комбінації датчиків відповідно до вимог. Ці дрони також не потребують фіксованої інфраструктури, радіозв'язку або попереднього досвіду пілотування. Вони корисні для інспекції таких робочих місць, як підземні шахти та об'єкти важкої промисловості. Це рішення дозволяє подолати недоліки ручних інспекцій та оцінок, надаючи точну картину обмежених зон та замкнутих просторів. Це скорочує час простою, час інспекції та ризики для співробітників.

Іспанський стартап Dronomy пропонує автономні дрони, що полегшують інспекції в приміщенні та на відкритому повітрі. Запатентована технологія позиціонування стартапу забезпечує сантиметрову точність як у приміщенні, так і на відкритому повітрі, безперебійно виконуючи польоти за допомогою GPS, візуальних маркерів або радіомаяків. Дрон легко інтегрується з камерами видимого/інфрачервоного діапазону та іншими сенсорними навантаженнями для виконання автономних інспекцій на великих висотах та в складних, забруднених і небезпечних середовищах. Це сприяє дистанційній інспекції активів та інфраструктури без нараження співробітників на небезпечні умови.

Колаборативні роботи.

Найкращим заходом безпеки є уникання небезпечних дій, які можуть призвести до негайних травм або довгострокових захворювань. Колаборативний робот — це інновація на робочому місці, яка дозволяє працівникам мінімізувати свої зусилля під час виконання ризикованих операцій з підйому вантажів та інших операцій з переміщення матеріалів. Роботи допомагають працівникам, виконуючи важчу або ризиковану підйомну діяльність. Це запобігає травмам спини та іншим видам нещасних випадків. Це також дозволяє уникнути присутності людей у

небезпечних зонах з пилом, хімічними речовинами та сильною спекою. Окрім застосування у виробництві та на складах, коботи корисні в медичних закладах для підйому пацієнтів або для переміщення вантажу в готелях. Таким чином, тенденція до підвищення безпеки на робочому місці зменшує ергономічні ризики за рахунок скорочення монотонних завдань.

Американський стартап WorkFar Robotics створює Avatar Robots, дистанційно керовану робототехнічну систему для небезпечних промислових середовищ. Ці роботи інтегрують штучний інтелект, машинне навчання та комп'ютерний зір для прогнозування та оптимізації своїх рухів і траєкторій. Наприклад, Avatar Robot замінює людських водіїв у сценаріях випробувань автомобілів на зіткнення та дозволяє дистанційно виконувати завдання в печах, електростанціях, лабораторіях та інших складних умовах.

Корейський стартап Safetics пропонує платформу для спільного проектування та аналізу робочих процесів, яка гарантує безпечну роботу коботів з людьми. Платформа стартапу дозволяє дизайнерам та інженерам оптимізувати функцію уникнення зіткнень робота за використовуючи штучний інтелект. Веб-інтерфейс Safetics дозволяє користувачам впроваджувати процеси без встановлення додаткового ПЗ.

Штучний інтелект.

Кожна аварія є результатом ланцюжка подій, що завершується пошкодженням інфраструктури, травмами або навіть смертю. Завдяки цифровізації робочих місць організації мають доступ до великої кількості даних, які відображають стан робочого середовища в будь-який момент часу. Ці дані включають дані датчиків навколишнього середовища, журнали співробітників, датчиків обладнання і зображення з камер відеоспостереження. Розвиток штучного інтелекту надає рішення, які дозволяють отримати з цих наборів даних інформацію, що покращує безпеку праці. Ці рішення використовують алгоритми машинного навчання на історичних даних для розпізнавання закономірностей, які слугують орієнтиром для виявлення аномалій, що можуть призвести до аварій. Таким чином, тенденція до підвищення безпеки на робочому місці сприяє

ранньому виявленню загроз безпеці, а також дозволяє прогнозувати катастрофічні відмови, що дає можливість менеджерам з технічного обслуговування вживати проактивних заходів, таких як превентивне обслуговування.

Ірландський стартап Protex AI створює платформу, яка допомагає командам з охорони навколишнього середовища, здоров'я та безпеки (EHS) підприємств приймати проактивні рішення з безпеки. Стартап пропонує пристрій для обробки зображень, який підключається до камер відеоспостереження для фіксації небезпечних подій у конкретному робочому середовищі. Платформа дозволяє користувачам визначати небезпечні події та налаштовувати фактори ризику та небезпеки на своєму підприємстві. Крім того, функціональність сценарію Protex дозволяє командам EHS співпрацювати, щоб вчитися на подіях, пов'язаних з безпекою, та вживати коригувальних заходів.

Ізраїльський стартап ArmourSense розробляє програмне забезпечення для аналізу відео, яке використовує існуючі відеокамери та штучний інтелект для моніторингу безпеки. Він прогнозує та зменшує ризики для безпеки людей, підвищує ефективність роботи та зменшує витрати часу простою. Рішення ідентифікує та прогнозує небезпечні ситуації та попереджає про них, захищаючи працівників та запобігаючи нещасним випадкам. Програмне забезпечення здатне виявляти небезпечні дії, пов'язані з рухом навантажувачів, роботою виробничої лінії та дотриманням вимог щодо ЗІЗ.

Моніторинг безпеки співробітників, навчання, звітність та компенсація працівникам – це лише кілька прикладів того, як технології покращують безпеку на робочому місці для співробітників. Технології також дозволяють співробітникам краще усвідомлювати оточення на робочому місці та небезпеки. Вони забезпечують високошвидкісний зв'язок для підвищення робочої безпеки. Дистанційна робота відкриває двері для багатьох нових ризикованих ситуацій, але технології, що дозволяють працівникам спілкуватися в режимі реального часу, зменшують його. Існує багато нових технологій, що роблять робоче середовище безпечнішим як для працівників, так і для роботодавців.

Компанії поєднують технології та 3D-візуалізації. Ця програма дозволяє

співробітникам краще усвідомлювати оточення на робочому місці та небезпеки, з якими вони можуть зіткнутися. Програмне забезпечення генерує реалістичні зображення, використовуючи два кути записаного зображення. Це програмне забезпечення дає величезні переваги для навчання співробітників у будь-якому місці. Можна відтворити нові робочі місця та середовища, що дозволяє співробітникам дізнатися про потенційні небезпеки та ризики, перш ніж вони потраплять на нові робочі місця. Високошвидкісний зв'язок та технологія передачі даних у реальному часі дозволяють віддаленим співробітникам бути в більшій безпеці під час роботи. Багато компаній вимагають від своїх співробітників подорожувати та працювати віддалено, що створює нові ризики для роботи. Для роботодавця важливо забезпечити безпеку своїх співробітників, і високошвидкісний зв'язок допомагає це реалізувати. Програмне забезпечення для управління поїздками — ще інструмент, який роботодавці використовують для охорони безпеки своїх співробітників під час дистанційної праці. Під час відряджень співробітники наражаються на багато ризиків, тому програмне забезпечення, яке дозволяє роботодавцям дізнаватися, коли співробітники не зареєструвалися в запланований час, є дуже корисним.

1.4 Інтеграція IoT та запобігання аварій

Моніторинг безпеки на таких великих робочих місцях, як фабрики чи шахти, є викликом. Навіть на невеликих робочих місцях, таких як офіси, ручний моніторинг небезпечних умов не є ідеальним рішенням. Інновації в галузі промислового Інтернету речей (IIoT) привели до створення таких рішень, як інтелектуальні датчики та пристрої, здатні безперервно контролювати навколишнє середовище та інфраструктуру. До цих пристроїв належать датчики небезпечних матеріалів, які оцінюють рівні токсичних газів, та пристрої моніторингу обладнання, які фіксують різні параметри машин, що вказують на стан обладнання. Ця тенденція надає дані в режимі реального часу, що дозволяє інженерам та менеджерам швидко виявляти будь-які проблеми, які можуть призвести до потенційної загрози.

Організації, які вирішили інтегрувати рішення IoT з метою створення згуртованого колективу, отримують значні та стабільні вигоди. Використання рішень IoT для охорони праці та безпеки створює ефект доміно, який поширюється на всі рівні організації, тим самим формуючи культуру та середовище, в яких безпека та успіх стоять понад усе.

Під покровом управління безпекою відстеження активів та обладнання дає такі переваги:

- Автоматизація за допомогою Інтернету речей (IoT): Інтернет Речей змінив роботу офісів. Багато розумних датчиків на робочому місці можуть вчитися на щоденних зразках поведінки та самостійно налаштовуватися, тобто все працює без втручання людини. Інтернет речей використовується для автоматизації освітлення, що допомагає зменшити витрати на енергію, визначаючи, коли приміщення зайняте, а також налаштовуючи освітлення відповідно до природного світла, що надходить через вікна протягом дня. Датчики IoT в ліфтах дозволяють здійснювати профілактичне обслуговування, що допомагає запобігти простою та підвищити безпеку і надійність. Системи HVAC використовують датчики для вимірювання температури та циклу роботи, що не тільки економить енергію, але й допомагає продовжити їх термін експлуатації. У рамках завдань співробітників він може допомогти командам, надаючи дані та інформацію, які допомагають їм приймати більш обґрунтовані рішення там, де необхідне втручання людини, заощаджуючи час і гроші;
- Продуктивність через IoT: датчики збирають дані, що дозволяє заощадити незліченні години роботи, які б пішли на ручне накопичення інформації. Замість того, щоб вручну отримувати інформацію з різних джерел, датчики можуть передавати її в додатки, які збирають, обробляють і аналізують дані за вас. Така продуктивність характерна не тільки для офісних робочих місць, але й для таких приміщень, як роздрібні магазини. IoT у роздрібній торгівлі використовується в

розумних полицях, які оснащені датчиками ваги для визначення обсягів запасів. Співробітники можуть отримувати сповіщення, коли запас товару закінчується і його потрібно поповнити. Теги радіочастотної ідентифікації (RFID) також можуть допомогти в управлінні запасами та відстежувати активи, щоб знати їх місцезнаходження в ланцюжку поставок до того, як вони надійдуть до магазину, і в магазині, що допомагає контролювати крадіжки;

- Зменшення витрат: технологія IoT дозволяє підприємствам заощаджувати кошти. Згадані переваги не тільки підвищують ефективність і продуктивність, але й запобігають втратам і катастрофічним збоям. Датчики IoT збирають дані, щоб надати більш повне уявлення про бізнес, що дозволяє здійснювати більш обґрунтовані операції, аналіз і планування. Ці заощадження швидко накопичуються, що полегшує підприємствам скорочення витрат. IoT допомагає усунути витрати часу і зусиль на рутинні завдання, щоб заощадити час і гроші. Існує багато способів інтегрувати IoT у бізнес. Багато постачальників і провайдерів додатків, послуг та інших технологій вже інтегрували IoT у свої пропозиції;
- Покращення дотримання вимог безпеки: роботодавці повинні створити програми навчання для своїх співробітників, щоб вони могли легко виявляти потенційні загрози їхній безпеці. Технологія IoT може бути використана для моніторингу та підтримання безпечного робочого середовища, особливо за допомогою ефективного управління документами. У цьому конкретному випадку перевіряються записи про навчання з дотримання вимог, і керівництво переконується, що всі співробітники пройшли його;
- Прискорення та підвищення ефективності рятувальних робіт: IoT у сфері робочої безпеки також може покращити функцію моніторингу обладнання. В результаті всі підключені пристрої зможуть ефективно працювати для виявлення можливої аварії. У разі нещасного випадку

можна швидко розпочати рятувальні роботи та відновити безпечне середовище.

1.5 Існуючі рішення у сфері запобігання аварій на основі сенсорів IoT

Промислові підприємства знаходяться під тиском, щоб підтримувати виробництво, усунути незаплановані простої та досягти більшої ефективності за допомогою невеликих команд технічного обслуговування. Більшість підприємств зараз експлуатують від 50 до 500 критично важливих машин на кожному об'єкті, багато з яких працюють 24 години на добу, де одна несподівана поломка може коштувати сотні тисяч втрат виробництва.

Датчики моніторингу стану стали незамінними, оскільки вони забезпечують раннє виявлення проблем з обладнанням, особливо в галузях з безперервним процесом виробництва, таких як хімічна, нафтова і газова, целюлозно-паперова, гірничодобувна та харчова промисловість, де доступність є головною метрикою. Для великих дискретних виробників, які зосереджені на загальній ефективності обладнання (OEE), вони допомагають підтримувати продуктивність і якість, одночасно зменшуючи мікрозупинки і запобігаючи браку.

Tractian Smart Trac Ultra.

Найкраще підходить для: промислових підприємств із внутрішнім технічним обслуговуванням, які потребують надійного обладнання, вбудованої діагностики та повного циклу надійності.

Smart Trac Ultra — це бездротовий датчик вібрації, призначений для важких промислових умов. Він стежить за вібрацією, температурою, часом роботи та обертами на хвилину для понад 100 категорій активів, включаючи машини зі змінною швидкістю та ті, що працюють з перервами. Відмінною рисою Tractian є система технічного обслуговування за станом в замкнутому циклі. Датчик виявляє проблеми на ранній стадії: платформа діагностує режим відмови, а потім автоматично генерує структуровані інспекції та покрокові стандартні операційні процедури за допомогою штучного інтелекту. Для заводів, які ставлять на перше місце доступність, хочуть передбачуваного виконання та експлуатують критично

важливі активи 24 години на добу, Smart Trac Ultra пропонує найповніше комплексне рішення.

Основні особливості:

- Asset GPT підвищує надійність програм, пояснюючи аномалії простими словами, показуючи, чому була виявлена проблема, і допомагаючи командам приймати швидші та більш впевнені рішення щодо технічного обслуговування;
- Створений для надійності, датчик має ступінь захисту IP69K і сертифікований для використання в небезпечних місцях, що дозволяє йому надійно працювати в зонах миття, зонах з високою температурою, запилених приміщеннях і вибухонебезпечному середовищі;
- Функція «Temperature Seasonality» виявляє природні сезонні зміни температури і фільтрує їх, допомагаючи командам уникнути помилкового тлумачення нормальних змін навколишнього середовища як ознак несправності устаткування;
- Функція «Always Listening» для періодичної роботи та точного фіксування вібрації під час руху машин;
- Датчик обертів, визначає швидкість обертання безпосередньо з сигналів вібрації, навіть на об'єктах із змінною швидкістю;
- Бібліотека підшипників із понад 75 000 моделей несправностей для автоматичного виявлення частоти;
- Індикатори стану обладнання та порівняльний аналіз між об'єктами, майданчиками та історичними часовими шкалами.

AssetWatch.

Найкраще підходить для: команд, які потребують віддаленої служби моніторингу, де зовнішні аналітики інтерпретують дані датчиків.

AssetWatch надає бездротові датчики та хмарну платформу, що підтримується аналітиками, які дистанційно контролюють стан обладнання. Ця модель корисна для об'єктів, які не мають власних експертів з вібрації. Однак значна залежність від зовнішніх аналітиків може обмежувати розвиток

внутрішніх вмінь команд. Оповіщення також можливо зберігати в окремому порталі, якщо не створено інтеграції, що може затримати дії на заводах, які потребують швидкого виконання робіт технічними фахівцями. Масштабування на різнопрофільні операції може спричинити вузькі місця, оскільки все проходить через сервісний рівень постачальника.

Основні особливості:

- Бездротові датчики вібрації та температури, призначені для безперервного моніторингу обладнання;
- Проста модель розгортання, призначена для заводів, які не мають власних фахівців з вібрації;
- Аналітики з дистанційного моніторингу стану, які інтерпретують дані датчиків і надають рекомендації.

Augury.

Найкраще підходить для: організацій, які хочуть поєднати виявлення аномалій на основі штучного інтелекту з віддаленими експертними послугами.

Augury використовує дані про вібрацію, температуру та магнітне поле, проаналізовані за допомогою власних AI моделей. Їхня пропозиція включає рекомендовані коригувальні дії, розроблені на основі поєднання машинного навчання та досвіду фахівців Augury. Недоліком є характер діагностики, що нагадує «чорний ящик». Фахівці з надійності часто хочуть бачити прозорі частоти несправностей та чітке обґрунтування попереджень. Впровадження зазвичай вимагає підтримки IT, OT та мережі, що може уповільнити розгортання. Моделі, що вимагають значних витрат на обслуговування, важко виправдати в довгостроковій перспективі для заводів, які віддають перевагу внутрішнім методам управління надійністю.

Основні особливості:

- Багатосигнальне вимірювання вібрації, температури, магнітних сигнатур та контексту процесу;
- Загальні панелі моніторингу ризиків, розроблені для надійності на декількох об'єктах;

- Управління послугами моніторингу, що орієнтовані на промислові активи з високим рівнем критичності.

Waites.

Найкраще підходить для: підприємств, які шукають економічний стартовий пакет для моніторингу стану з можливістю додаткової експертної оцінки.

Waites пропонує доступні бездротові датчики та хмарний портал для даних про вібрацію та температуру. Він добре підходить для об'єктів, які переходять від ручного збору даних до безперервного моніторингу. Недоліком є те, що налаштування сповіщень та вибірка даних повинні ретельно контролюватися, інакше команди можуть отримувати надмірну кількість повідомлень. Інтеграція з CMMS та корпоративними інструментами обмежена, що додає ручні кроки, які уповільнюють реалізацію. Для великих заводів, на яких працює сотні критично важливих машин, це може перевантажити команди з ощадливого технічного обслуговування.

Основні особливості:

- Бездротові трьохосьові датчики вібрації та температури для двигунів, редукторів, насосів і конвеєрів;
- Хмарний портал із відображенням спектрів, графіками історичних тенденцій і налаштовуваними сигналами тривоги;
- Доступне обладнання, придатне для великих флотів обладнання середньої критичності.

Relay.

Найкраще підходить для: команд, які шукають легкі, компактні датчики з базовим виявленням аномалій.

Relay пропонує компактні датчики IIoT з моніторингом температури та вібрації. Рішення просте та швидке у впровадженні, що зацікавить підприємства, які вперше розглядають можливість моніторингу. Для великих промислових об'єктів платформа може не пропонувати глибину діагностики, сертифікати небезпечності або інтеграцію робочих процесів технічного обслуговування, необхідні для впровадження на всьому підприємстві. Масштабування на

багатолінійні або розподілені операції часто вимагає більш просунутих можливостей, ніж ті, що наразі підтримує Relay.

Основні особливості:

- Полегшена хмарна платформа для базових сповіщень про аномалії та візуалізації тенденцій;
- Економічно ефективний шлях для заводів, які прагнуть цифровізувати зусилля моніторингу на ранній стадії;
- Легко інтегрується з меншими периферійними шлюзами та мережами IoT.

Perceptive Sensor Technologies.

Ультразвуковий моніторинг стану обладнання вирішує проблеми як управління технічним обслуговуванням обладнання, та скорочення промислової робочої сили на основі швидко розгортаємих систем, які не вимагають великої участі робочої сили. Вони використовують гетеродинування для захоплення і перетворення коротких хвиль, які не чутні для людини, і локалізації їх точного місця розташування в надзвичайно шумних середовищах. Perceptive Sensor Technologies розробляє FluID — рішення для ультразвукового моніторингу стану резервуарів та обладнання для зберігання рідин. Датчики залишаються на зовнішній частині контейнерів, але чітко реєструють швидкість, імпеданс та щільність матеріалу всередині них на основі запатентованих алгоритмів ультразвукового «відбитку пальців».

Основні особливості:

- Хмарна перевірка в режимі реального часу квитанцій матеріалів та їх перевезень незалежною сторонньою інспекційною компанією;
- Зменшення ризику переповнення, забруднення продукції та потенційно шкідливого впливу на навколишнє середовище;
- Неінтрузивні методи перевірки та моніторингу зменшують час простою та мінімізують втрати продуктивності.

2 ДОСЛІДЖЕННЯ ПРИНЦИПІВ РОБОТИ СЕНСОРНОГО АНАЛІЗУ

2.1 Основи роботи моніторингу стану

У виробництві та інших промислових умовах моніторинг стану (Condition monitoring, CM) є процесом відстеження продуктивності обладнання в режимі реального часу для розуміння поточного стану активу. Зазвичай це досягається за допомогою дротових або бездротових датчиків, які збирають критичні дані про обладнання та передають їх на програмну платформу для аналізу. Отримані дані можуть бути використані реактивно (наприклад, для спрацьовування тривоги при наближенні несправності) або проактивно (наприклад, для інформування про стратегію оптимізації стану обладнання з метою запобігання майбутнім проблемам).

Впровадження моніторингу стану в стратегію управління продуктивністю активів є проривом. Це дає можливість в режимі реального часу отримувати інформацію про стан активів, що дозволяє робити розумніші рішення, зменшувати ризики та забезпечувати безперебійну роботу.

Крім того, існують деякі додаткові переваги впровадження цієї технології:

- Мінімізація дорогих простоїв: випередження проблем з обладнанням означає менше несподіваних зупинок виробництва. Це означає менше пропущених термінів, нижчі витрати на понаднормову роботу та меншу потребу в екстрених викликах служби технічного обслуговування.
- Запобігання ланцюговим несправностям: коли одна машина виходить з ладу, це може спричинити вихід з ладу інших, але не в тому випадку, коли проблема вчасно виявлена. Моніторинг стану допомагає захистити сусідні системи та уникнути дорогих побічних збитків.
- Зменшення витрат на непотрібне технічне обслуговування: замість того, щоб дотримуватися жорстких графіків, можливо використовувати конкретні дані як основу для зусиль з технічного обслуговування. Це економить час, подовжує термін експлуатації активів і дає більшу вартість від кожної машини.

- Оптимізація зусиль з технічного обслуговування: точне знання місця несправності означає менше часу на пошуки і більше часу на усунення справжньої проблеми. Це призводить до швидшого ремонту та більш ефективного використання часу технічної команди.
- Підвищення безпеки на робочому місці: виявлення та усунення проблем з обладнанням до їх загострення допомагає захистити команду. Це проактивний спосіб створення більш безпечного та контрольованого робочого місця.
- Покращення продуктивності обладнання: відстеження тенденцій продуктивності дозволяє точно налаштувати неефективні компоненти.

Моніторинг стану обладнання підтримує зусилля з профілактичного обслуговування, перетворюючи необроблені дані про обладнання на цінну інформацію. Це простий процес, який забезпечує визначення проблем на ранніх етапах і зберігає безперебійну роботу. Впроваджені в рамках програми профілактичного обслуговування, методи моніторингу стану обладнання дозволяють на ранній стадії виявляти відхилення від нормальних умов експлуатації. Це дає можливість команді з технічного обслуговування планувати інспекції та ремонтні роботи в час, зручний для виробництва, а також запобігати аваріям.

Моніторинг стану обладнання включає три основні етапи:

1) Встановлення параметрів моніторингу: процес починається з визначення, які частини обладнання потребують уваги, зазвичай — критично важливі компоненти. Датчики встановлюються в ключових місцях для відстеження конкретних показників, створюючи основу для ефективного профілактичного технічного обслуговування.
2) Збір та аналіз даних: після встановлення датчиків вони безперервно збирають дані про продуктивність та стан в режимі реального часу або за розкладом. Ці дані аналізуються за допомогою розумних інструментів, які порівнюють поточні показники з історичними тенденціями для виявлення невідповідностей.

3) Реєстрація та реагування на сповіщення: коли щось виглядає не так, система автоматично надсилає сповіщення електронною поштою, SMS або через програмне забезпечення для моніторингу, щоб повідомити команду з обслуговування. Ці сповіщення викликають своєчасну реакцію, тому команди можуть вжити заходів, перш ніж незначні проблеми перетворяться на дорогі несправності.

Для ефективного виявлення несправностей надзвичайно важливо вибрати та впровадити методи моніторингу стану, спеціально розроблені для конкретних критично важливих активів.

Існує багато способів моніторингу стану обладнання, кожен з яких має своє унікальне призначення. Нижче наведені деякі з найбільш поширених видів моніторингу стану:

- Моніторинг вібрації: обертове обладнання має характерні вібраційні сигнали, які відображають такі параметри, як стан балансу та стан підшипників. Пошкодження спричиняє різку зміну частоти та/або амплітуди, тоді як знос підшипників і шийок проявляється у вигляді поступового збільшення амплітуди. Аналіз вібрації є одним із найстаріших видів моніторингу стану і є ефективним для виявлення пошкоджень інструментів або несправностей підшипників. Він застосовується до насосів, двигунів, редукторів, компресорів та будь-яких інших пристроїв, вібраційні характеристики яких залишаються стабільними під час нормальної експлуатації;

- Моніторинг температури: точне вимірювання температури дозволяє здійснювати один з найважливіших видів технічного обслуговування на основі стану. Багато машин працюють найефективніше в межах вузького діапазону температур. Вихід за межі цього діапазону може вказувати на питання, які можуть спричинити проблеми з якістю, прискорити знос або збільшити споживання енергії. Промислові датчики температури забезпечують безперервний моніторинг в режимі реального часу місця, в якому вони встановлені. Прикладами можуть бути корпуси двигунів, підшипникові шийки та електричні шафи;

- Моніторинг тиску: безліч промислових процесів залежать від утримання

та подачі рідин під певним тиском. Інші використовують вакуум. У обох випадках промислові датчики тиску можуть забезпечувати безперервний моніторинг у реальному часі та запустити сигнал тривоги при виникненні аномальних станів або подій. Це підвищує безпеку та надає можливість точного контролю процесу, одночасно захищаючи обладнання від пошкодження та втрати продукції;

- Моніторинг вологості: Вологість може мати значний вплив на якість певних продуктів, включаючи їжу, фармацевтичні препарати та медичні вироби. Вона також може завдати шкоди цінному обладнанню через корозію та іржу. Впровадження датчиків вологості на виробничих та переробних площах дозволяє промисловим підприємствам відстежувати кількість вологи в повітрі, що сприяє контролю якості, профілактичному обслуговуванню та іншим процесам;

- Ультразвуковий моніторинг: Ультразвук — це звук з частотою, що значно перевищує діапазон чутності людини. Він використовується для моніторингу стану двома способами: для виявлення витоків та для пошуку дефектів або недоліків всередині конструкції. Ультразвукове виявлення витоків схоже на звук свистка чайника, що закипає. Коли газ під тиском виходить, він видає високочастотний звук, який вловлюють детектори витоків. Ультразвук для виявлення внутрішніх дефектів передбачає надсилання високочастотного звуку в тверду структуру, таку як вилив, і вимірювання того, як він передається, відбивається і заломлюється. Аномалії виявляються, коли звукові хвилі проходять несподіваним шляхом.

- Моніторинг двигунів: Двигуни є повсюдними в промислових і виробничих умовах, і їх несправність або неефективна робота можуть дорого коштувати. Моніторинг стану двигуна — це сукупність методів, що використовуються для виявлення аномальної роботи. Головним серед них є аналіз ланцюга двигуна (Motor Circuit Analysis, MCA). У цій техніці (двигун необхідно на короткий час вивести з експлуатації) в двигун подаються сигнали змінного струму, а відповідь вказує на характеристики опору, ємності та індукції.

- Електричний моніторинг: Електричні несправності можуть становити серйозну загрозу безпеці та спричиняти перегрів і пожежі. Електричний

моніторинг, одним із видів якого є згаданий раніше МСА, охоплює цілу низку методів вимірювання, включаючи тестування імпедансу, опору та поширення. Крім того, споживання енергії є цінним показником для моніторингу роботи машини. Воно може сигналізувати про те, що умови роботи є неоптимальними, та надавати дані про стан обладнання для автоматичного розрахунку загальної ефективності обладнання.

- Аналіз масла: Масло накопичує мікроскопічні частинки сміття, коли змащує та охолоджує редуктори, повзунки та інші механізми. Під впливом тепла та тиску воно також окислюється та змінює в'язкість, що знижує його здатність виконувати свою функцію. Аналіз масла передбачає вимірювання складових та ключових параметрів для оцінки стану масла та визначення, які компоненти машини зазнають зносу. Датчики можна встановити в системі змащення для постійного моніторингу стану масла, але для більш ретельного дослідження необхідний лабораторний аналіз.

- Термографічне тестування: Термографія — це безконтактний метод вимірювання температури на певній ділянці. Він виконується за допомогою камери, здатної виявляти інфрачервоне теплове випромінювання. Термографія є надзвичайно цінною в профілактичному технічному обслуговуванні, оскільки вона може забезпечити раннє попередження про нові проблеми. Воно також може виявляти витоки, оскільки вони можуть виглядати гарячішими або холоднішими, ніж навколишній простір. Термографічне тестування може виконуватися вручну за допомогою портативного пристрою або автоматично за допомогою датчиків фіксованого положення, а аналіз зображення може бути кількісним або якісним.

- Електромагнітне вимірювання: Ця техніка передбачає використання магнітних полів для виявлення аномальних умов. Вихрострумові датчики широко використовуються для виявлення тріщин, і це одне із застосувань моніторингу стану, але інші — це вимірювання корозії та зносу.

- Лазерна інтерферометрія: Ця техніка моніторингу стану використовує когерентне лазерне світло для виявлення поверхневих і підповерхневих дефектів шляхом вимірювання змін в інтерференційних закономірностей. Вона також може

виявляти деформацію в деяких матеріалах.

Основним обмеженням регламентного обслуговування є те, що роботи можуть виконуватися частіше, ніж це необхідно. Якщо вони не виконуються достатньо часто, ризик поломок підвищується. Предиктивне технічне обслуговування вирішує цю проблему за допомогою даних про стан обладнання, що дозволяють виявити ранні ознаки наближення проблем. Це дає команді технічного обслуговування час для планування, коли вони спричинять найменші незручності для виробництва і коли доступне спеціалізоване обладнання. Це також дозволяє застосовувати більш економічно ефективні політики закупівлі запасних частин та зберігання. Існує багато типів технологій моніторингу стану, деякі вимагають моніторингу на місці, а інші можуть бути зроблені віддалено. Вибір найбільш підходящої технології для конкретного застосування вимагає детального розуміння варіантів та ознайомлення з їх застосуванням.

2.2 Предиктивне обслуговування за допомогою моніторингу стану

Предиктивне технічне обслуговування (PdM) — це технічне обслуговування, яке відстежує продуктивність та стан обладнання під час нормальної роботи з метою зменшення ймовірності виходу з ладу. Його мета спочатку передбачити, коли може статися вихід з ладу обладнання (на основі певних факторів), а потім запобігти цьому за допомогою регулярного планового та коригувального технічного обслуговування.

Предиктивне технічне обслуговування не може існувати без моніторингу стану. Існує три види моніторингу стану: онлайн, періодичний та дистанційний. Онлайн-моніторинг стану визначається як безперервний моніторинг машин або виробничих процесів із збором даних про критичні швидкості та зміну положень.

Періодичний моніторинг стану, який здійснюється за допомогою аналізу вібрації, дає розуміння про зміну поведінки вібрації установок за допомогою аналізу тенденцій. Нарешті, дистанційний моніторинг стану, як випливає з його назви, дозволяє контролювати обладнання з віддаленого місця, передаючи дані для аналізу.

Існує кілька відмінностей між предиктивним та превентивним технічним обслуговуванням. Превентивне технічне обслуговування передбачає перевірку та обслуговування обладнання незалежно від того, чи потребує воно обслуговування. Графік такого обслуговування базується на інтенсивності використання або часових інтервалах. Наприклад, опалювальне обладнання обслуговується щороку перед зимою.

Крім того, превентивне обслуговування не вимагає компонента моніторингу стану, як це робить предиктивне обслуговування. Не вимагаючи моніторингу стану, програма превентивного обслуговування не передбачає великих капіталовкладень у технології та навчання. Нарешті, багато програм превентивного обслуговування потребують ручного збору та аналізу.

Якщо превентивне технічне обслуговування визначається на основі середнього терміну експлуатації активу, то предиктивне технічне обслуговування визначається на основі заздалегідь встановлених і визначених умов конкретного обладнання з використанням різних технологій. Предиктивне технічне обслуговування також вимагає більших інвестицій у персонал, навчання та обладнання, ніж превентивне технічне обслуговування, але в довгостроковій перспективі економія часу та коштів буде більшою.

Предиктивне технічне обслуговування має кілька переваг:

- Зниження витрат: предиктивне технічне обслуговування може знизити витрати. Це особливо важливо, коли організації мають інвестувати в заробітні плати, технічне обслуговування, запасні частини, інструменти та обладнання, необхідні в разі серйозних несправностей;
- Скорочення кількості несправностей обладнання: існує багато досліджень щодо зменшення кількості відмов машин. Регулярний моніторинг машин і систем може знизити ймовірність несподіваних, масштабних збоїв. Після двох років впровадження програми предиктивного технічного обслуговування частота і характер поломок обладнання часто зменшуються;
- Зниження часу простою: завдяки предиктивному технічному обслуговуванню ремонт обладнання займає менше часу. Регулярний моніторинг і аналіз стану

обладнання допомагає технічному персоналу швидко знаходити несправні компоненти на всіх машинах і вирішувати проблеми. Це скорочує час простою і, в багатьох випадках, повністю запобігає йому;

- Зменшення обсягів запасів: часто компанії мають справу з великими інвестиціями в запаси різних деталей, що може заморожувати капітал. Якщо деталі не використовуються досить швидко, їхня якість погіршується і вони можуть зіпсуватися. Замість того, щоб утримувати великі запаси деталей на випадок потреби, замовлення деталей тільки тоді, коли вони потрібні, може зменшити витрати на зберігання;

- Збільшення термін служби обладнання: виявлення проблем з обладнанням до того, як вони перетворяться на катастрофічні несправності може збільшити термін експлуатації обладнання. Наявність програми предиктивного технічного обслуговування на основі стану обладнання гарантує, що обладнання ніколи не досягне стадії серйозного пошкодження. Більший термін експлуатації обладнання забезпечує кращу рентабельність інвестицій;

- Оцінка середнього наробітку між відмовами: додатковою перевагою профілактичного технічного обслуговування є можливість оцінити середній наробіток між відмовами (MTBF). Це означає найбільш економічно вигідний термін для заміни обладнання. Деякі компанії схильні використовувати обладнання з усіма його недоліками та численними ремонтами, помилково вважаючи, що нове обладнання є дорогим вкладенням. Можливість заміни обладнання в кінці його терміну експлуатації дозволяє уникнути високих витрат на технічне обслуговування зношеного обладнання;

- Збільшення виробництва: програми предиктивного технічного обслуговування за станом потребує підтримки з боку надійних технологічних систем, що збільшує її ефективність. Комплексна програма прогнозного технічного обслуговування, що включає моніторинг параметрів, може підвищити ефективність роботи і, в свою чергу, збільшити обсяги виробництва;

- Підвищення безпеки операторів: за допомогою предиктивного технічного обслуговування можна встановити сигнали раннього попередження, щоб

запобігти травмам від несправностей в обладнанні. Багато страхових компаній визнають і пропонують пільги виробникам, які використовують програму предиктивного технічного обслуговування на основі стану. Впровадження цієї програми може знизити витрати на страхування без шкоди для страхового покриття;

- Перевірка ремонтів: під час усунення однієї проблеми ремонт може пошкодити інші частини машини. За допомогою аналізу вібрації команда технічного обслуговування може виявити будь-які відхилення від норми після ремонту. Завдяки профілактичному технічному обслуговуванню компанії можуть аналізувати дані для планування та організації планових зупинок на технічне обслуговування, максимально ефективно використовуючи час простою машини;
- Збільшення прибутку: предиктивне технічне обслуговування покращує виробничі операції та роботу переробних заводів. Система управління на основі стану коштує більше, ніж вартість програми. За допомогою методів предиктивного технічного обслуговування компанії можуть знизити щорічні експлуатаційні витрати та зменшити ризики.

2.3 SCADA

Диспетчерське управління і збір даних (Supervisory control and data acquisition, SCADA) — це архітектура, яка дозволяє промисловим організаціям відстежувати та керувати процесами, машинами та цехами.

Системи SCADA використовують комп'ютери, мережі та графічні інтерфейси для забезпечення високого рівня управління та нагляду за виробничими процесами. Мережі SCADA мають вирішальне значення для промислових операцій, але складаються з апаратного та програмного забезпечення, яке може легко стати жертвою хакерів, що робить безпеку SCADA все більш важливою.

Концепція систем диспетчерського контролю та збору даних з'явилася в 1960-х роках, коли тодішні комп'ютерні системи почали завойовувати ринки, зосередившись на автоматизації виробництва. Більшість ранніх систем

використовували централізовані мейнфрейми для збору даних та контролю. З удосконаленням технологій програмовані логічні контролери та віддалені пристрої зв’язку знайшли своє місце в системах SCADA. З того часу вони продовжували розвиватися, перетворюючись на ще більш досконалі та розподілені системи. Трохи пізніше, у 1980-х і 1990-х роках, мережеві та веб-орієнтовані системи SCADA стали відомі завдяки набагато більшій гнучкості та доступності. Це програмне забезпечення SCADA продовжило розвиватися завдяки сучасним технологіям, поєднуючись із хмарними обчисленнями та розширеною аналітикою.

SCADA — це автоматизована система управління (ICS), яка відстежує та керує інфраструктурними процесами. Системи SCADA взаємодіють із пристроями та промисловим обладнанням у рамках технологічних процесів систем управління. Вони збирають дані, записують та реєструють їх, а також представляють інформацію через людино-машинний інтерфейс (HMI).

Автоматизоване управління промисловими процесами та машинами.

Більшість дій з управління в системі SCADA виконуються автоматично віддаленими терміналами (RTU) або програмованими логічними контролерами (PLC) системи. Системи SCADA дозволяють організаціям автоматизувати управління промисловими процесами та машинами, що було б занадто складним або комплексним для ручного керування. Системи використовують вимірювальні прилади та датчики для автоматичного виявлення тривог та ненормальної поведінки і реагують за допомогою запрограмованих функцій управління. Наприклад, якщо тривога спрацювала внаслідок надмірного тиску в промисловій лінії, система SCADA видасть команду відкрити клапан і відновити нормальний рівень.

Збирання та аналіз даних.

SCADA часто використовується як термін, що визначає збір, аналіз та представлення даних. Система SCADA приймає аналогові дані та представляє їх у вигляді графіків. Вона також збирає цифрові дані, які можуть містити сигнали тривоги, що можуть бути активовані, та накопичує імпульсні дані, що зазвичай

передбачає підрахунок обертів лічильника. Ці процеси збору та аналізу даних допомагають SCADA контролювати інфраструктурні процеси критично важливих об'єктів та утиліт. Однак SCADA зазвичай координує процеси в режимі реального часу, а не контролює.

Моніторинг систем.

Системи SCADA можуть використовуватися для моніторингу промислового обладнання, машин, систем або будівель, таких як електростанції. Цей процес може бути автоматичним або ініціюватися за допомогою команд оператора.

Повідомлення про події та тривоги.

Більшість систем SCADA включають функцію спостереження та управління тривогами, яка підтримує програмне забезпечення в системі. Важливо, щоб вона була налаштована таким чином, щоб нею керувала сама система SCADA або вона спрацьовувала за ініціативою користувачів.

Звітність.

Системи SCADA інтегруються з вимірювальними пристроями, такими як датчики, в інфраструктурі промислових і виробничих організацій. Вони збирають дані в аналоговій або цифровій формі, а потім надсилають їх до RTU або PLC, щоб їх можна було перетворити на корисну та придатну для використання інформацію. Потім ця інформація надсилається до HMI або інших дисплеїв, що дозволяє операторам аналізувати дані та взаємодіяти з ними.

Системи SCADA зазвичай використовуються організаціями, що займаються постачанням електроенергії, природного газу, контролем відходів, водопостачанням та іншими необхідними комунальними послугами. Тому мережі SCADA є дуже цінними, але й дуже вразливими. Державні органи та приватні компанії, відповідальні за управління цими послугами, повинні гарантувати безпеку SCADA щоб захистити їх.

Апаратне забезпечення відповідає за збір і передачу даних на комп'ютер, на якому встановлено програмне забезпечення SCADA. Комп'ютер обробляє дані, а потім записує та реєструє події у файлі, що зберігається на жорсткому диску, або надсилає їх на принтер. Додаток SCADA також видає попередження або звуковий

сигнал, коли умови стають небезпечними.

Системи SCADA складаються з декількох компонентів, апаратного та програмного забезпечення, що забезпечують збір та передачу даних, необхідних для контролю та моніторингу промислових процесів (рис. 2.1). До цих ключових компонентів належать:

- Віддалені термінали (RTU): збирають і зберігають інформацію з датчиків, а потім надсилають її до головного терміналу (MTU), який складається з комп'ютера, PLC і мережевого сервера, що утворюють ядро системи SCADA. RTU збирає і зберігає дані, поки не отримає відповідну команду від MTU, а потім їх передає. Після цього MTU може спілкуватися з операторами та обмінюватися даними з іншими системами;

- Людино-машинний інтерфейс (HMI) SCADA: користувацький інтерфейс або панель управління, що дозволяє людині підключатися до пристрою, машини або системи. Це дає можливість операторам контролювати вхідні та вихідні дані машини, стежити за ключовими показниками ефективності (KPI), відстежувати час виробництва та тенденції, а також візуально відображати дані. HMI використовуються більшістю промислових організацій для взаємодії з машинами та оптимізації їх процесів. Вони можуть мати вигляд комп'ютерних моніторів, планшетів та екранів, вбудованих у машини, які надають інформацію про продуктивність та хід роботи механічної системи. Наприклад, оператор на першому поверсі промислового підприємства може використовувати HMI для контролю та моніторингу температури резервуара для води або продуктивності насоса;

- Комунікаційна інфраструктура: зв'язок між RTU та MTU, який забезпечує передачу даних між цими пристроями. Цей бездротовий канал зв'язку є двонаправленим і використовується для мережевих цілей разом з іншими комунікаційними процесами та обладнанням, такими як волоконно-оптичні кабелі та кручені пари;

- Входи: SCADA покладаються на входи, які зчитуються і записуються PLC для реєстрації та зберігання даних. PLC (Programmable logic controller) — це

міні-комп'ютер, який знаходиться в мережі SCADA і збирає дані входів та виходів від пристроїв в системі. PLC контролює стан входів, таких як швидкість і продуктивність двигуна, а потім використовує цю інформацію для виведення сигналів, таких як його зупинка або уповільнення.

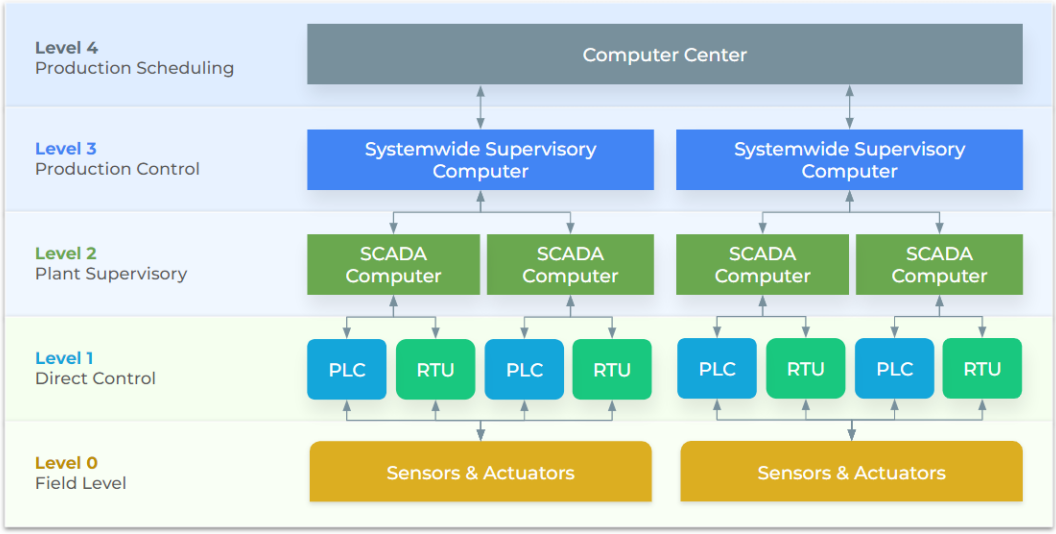


Рис. 2.1 Схема роботи SCADA[19]

SCADA дозволяє організаціям контролювати промислові процеси; збирати, відстежувати та обробляти дані в режимі реального часу; взаємодіяти з критично важливими пристроями, такими як двигуни, насоси, датчики та клапани; а також записувати події в лоґ-файли.

Системи SCADA контролюють і моніторять промислові процеси та машини в широкому спектрі галузей. До них входять:

- Обробка харчових продуктів: системи SCADA мають вирішальне значення для компаній, що займаються обробкою харчових продуктів, у поліпшенні їх якості та кількості. SCADA також забезпечує зниження витрат і мінімізацію втрат;

- Фармацевтика/біотехнології: фармацевтичні та біотехнологічні компанії використовують системи SCADA для забезпечення оптимальної роботи обладнання та зменшення витрат на технічне обслуговування. Вони також покладаються на SCADA для максимізації своїх виробничих процесів;

- Управління водопостачанням: компанії з управління водопостачанням використовують системи SCADA для забезпечення ефективної роботи своїх заводів та моніторингу роботи резервуарів для зберігання, насосних станцій, очисних споруд та іншого обладнання. SCADA має вирішальне значення для запобігання кібератакам та забезпечення відповідних заходів безпеки на водоочисних станціях;

- Управління системами опалення, вентиляції та кондиціонування повітря (HVAC) та комерційними будівлями: ці системи мають вирішальне значення для регулювання роботи систем опалення, вентиляції та кондиціонування повітря, а також систем освітлення та введення даних у цих будівлях;

- Енергопостачання та комунальні послуги: Робота більшості енергопроводів автоматизована, але іноді може знадобитися ручне втручання. Системи SCADA забезпечують процеси моніторингу та сигналізації, що дозволяють енергетичним компаніям втручатися, якщо діяльність заводу відхиляється від норми. Системи SCADA також допомагають комунальним підприємствам забезпечувати надійність та безперервний моніторинг продуктивності, щоб мінімізувати людські помилки;

- Переробка морепродуктів: системи SCADA дозволяють підприємствам з переробки морепродуктів поліпшити стабільність і гарантувати їх якість. Вони також допомагають максимізувати продуктивність обладнання на заводах для скорочення витрат;

- Сортування та виконання замовлень: сортувальні підприємства можуть відстежувати та керувати продуктивністю обладнання. Це гарантує відсутність помилок і високий рівень ефективності.

3 РОЗРОБКА IOT-РІШЕННЯ ДЛЯ ЗАПОБІГАННЯ АВАРІЙ

3.1 Засоби розробки

Інструменти для розробки IoT можуть включати апаратне забезпечення, таке як плати розробки та екрани, інструменти для створення програм, що запускають системи IoT, та платформи, що використовуються для управління приладами. Наприклад, якщо потрібна програма, яка контролює камери безпеки навколо будинку та сповіщає про будь-які зміни, ця програма має бути розроблена кимось на платформі з певним типом кодування.

Пристрої IoT часто мають обмежену обчислювальну потужність і можливості підключення, тому програми не можуть розраховувати на велику ємність пам'яті на периферії або можливість в будь-який час встановлювати патчі та оновлення, як з додатком на телефоні. А архітектура IoT має ряд місць, де потрібні додатки.

У роботі використовувалися наступні інструменти:

Wokwi.

WOKWI — це популярний онлайн-симулятор електронних проектів. Цей симулятор включає в свою платформу популярні набори для розробки та інтегральні схеми, такі як Arduino UNO, MEGA, ATtiny85, серія ESP32, плати STM32 та інші. Крім того, він також включає необхідні будівельні блоки для формування електронних схем, такі як резистори, світлодіоди, датчики, вхідні перемикачі та пристрої, модулі дисплея, двигуни, логічні IC, макетні плати та інші.

Середовище використовує формат обміну даними JSON і зберігає їх у файлі під назвою diagram.json. Цей файл містить перелік усіх необхідних атрибутів компонентів та взаємозв'язків для завершення візуальної схеми.

Тут можливо не тільки створювати повні електронні схеми, але й використовувати повністю функціональне середовище кодування. Підтримується кодування Arduino, включаючи реалізацію вихідних файлів C і файлів заголовків, бібліотек Arduino та послідовного порту.

На додаток до послідовного порту, реалізовано логічний аналізатор для спостереження за поведінкою цифрових сигналів. Можливо інтерпретувати послідовні дані (такі як I2C, SPI та UART), зберігаючи їх у форматі VCD (Value Change Dump). Цей формат розпізнається в програмному забезпеченні з відкритим кодом для аналізу сигналів PulseView (sigrok).

HiveMQ.

HiveMQ — це платформа MQTT для підприємств, яка зберігає високу надійність навіть у стресових умовах, таких як нестабільність мережі та високе навантаження через великі обсяги передачі та прийому даних та має можливість швидкої та ефективної передачі даних між пристроями IoT.

Основні особливості брокера HiveMQ MQTT:

- Масштабований брокер MQTT: екземпляри брокера HiveMQ MQTT масштабуються разом з базовим обладнанням. Неблокуючий і багатопотоковий підхід дозволяє підключати до 10 000 000 пристроїв одночасно, зберігаючи надзвичайно високу пропускну здатність і мінімальну затримку;

- Надійна доставка даних: доставка даних через ненадійні мережі може бути складним завданням. HiveMQ реалізує всі рівні якості обслуговування MQTT, включаючи доставку щонайбільше раз, не щонайменше раз і рівно один раз. Підтримка розширених політик збереження повідомлень і черги повідомлень в автономному режимі є необхідною для компенсації затримки мережі;

- Еластичне кластеризування: HiveMQ побудовано на основі справді розподіленої архітектури кластерів без головного сервера, що означає відсутність єдиної точки відмови та можливість розширення і скорочення кластера під час роботи без втрати даних або доступності. Підтримка Kubernetes, OpenShift і DC/OS дає змогу автоматично масштабувати HiveMQ відповідно до вимог програми IoT;

- Безпека корпоративного рівня: HiveMQ розроблений для захисту даних IoT від пристроїв до корпоративних систем. Передача даних захищена галузевими стандартами, такими як TLS 1.3, безпечні веб-сокети і найсучасніші набори шифрів. Підтримка автентифікації та авторизації включає сертифікати X.509, ім'я

користувача/пароль, автентифікацію на основі IP та API, що дозволяє використовувати власні логіки автентифікації, авторизації та дозволів, такі як інтеграція OAuth 2.0;

- Стовідсоткова сумісність з MQTT: брокер MQTT від HiveMQ на 100% сумісний зі специфікаціями MQTT 3.1, MQTT 3.1.1 та MQTT 5. Клієнти, що працюють з MQTT 3 та MQTT 5 також можуть спілкуватися з HiveMQ одночасно. Усі розширені функції, такі як символи-замінники тем, постійні сесії з чергою в автономному режимі, збереження повідомлень та всі рівні якості обслуговування, доступні в будь-якому масштабі;

- Розгортання будь-де: HiveMQ можна розгорнути в приватній, гібридній та публічній хмарі. Готові образи можна розгорнути в приватних хмарах за допомогою Kubernetes, OpenShift та DC/OS. Підтримувані публічні хмарні платформи включають AWS та MS Azure. HiveMQ також може працювати в нативному режимі на Linux, Windows та OS X;

- Ефективне використання мережі: на відміну від HTTP, HiveMQ і MQTT базуються на архітектурі pub-sub, тому загальний трафік мережі зменшується, оскільки немає опитування клієнтів. Розмір повідомлень MQTT також значно менший, ніж у HTTP, тому обсяг даних, що проходять через мережу, знижується;

- Інтеграція корпоративних даних у великому масштабі: інтеграція корпоративних даних досягається за допомогою двонаправленої передачі даних між брокером HiveMQ MQTT і корпоративною системою, яка виступає в ролі клієнта. Використовуючи протокол MQTT pub-sub, клієнт кожної корпоративної системи підписується на потрібні дані. Реалізація MQTT Shared Subscription від HiveMQ дозволяє горизонтально масштабувати клієнти, завдяки чому інтеграція підприємства є масштабованою та надійною;

- Моніторинг даних у реальному часі: адміністратори можуть використовувати панель управління HiveMQ для моніторингу даних, що проходять через брокер MQTT та клієнти MQTT, підключені до програми IoT, у режимі реального часу. Для кожного клієнта MQTT адміністратор може бачити повний огляд стану клієнта, відключити клієнта, видалити сесію MQTT та

додати/видалити підписки. Для розширеного усунення несправностей HiveMQ дозволяє створювати записи, які можна використовувати для виявлення проблем та вузьких місць у розгорнутих додатках IoT. Загальна інформаційна панель надає операційній команді повний огляд кластера брокерів та загального стану системи в режимі реального часу;

- Фреймворк розширень та ринок: відкритий API та гнучке розширення дозволяють інтегрувати HiveMQ та дані IoT в існуючі корпоративні системи. Фреймворк дозволяє розробникам швидко створювати розширення для обробки даних, автентифікації пристроїв та механізмів авторизації. HiveMQ також надає ринок готових розширень для Kafka, Oracle DB, MongoDB та інших;

- Клієнтські бібліотеки MQTT: з HiveMQ можна використовувати будь-яку клієнтську бібліотеку, сумісну з MQTT. HiveMQ надає власну бібліотеку Java, але також можливо використовувати бібліотеки Eclipse Paho, C/C++, у Python або JavaScript. Деякі споживачі також створюють власних клієнтів. Різні варіанти клієнтів MQTT означають, що компанії не прив'язані до одного постачальника;

- Повністю керована хмарна служба MQTT: HiveMQ Cloud — це хмарна служба обміну повідомленнями для Інтернету речей, яка спрощує розгортання та управління платформами MQTT. Вона створює масштабовані та надійні кластери хмарних брокерів MQTT, призначені для виробництва, всього за кілька кліків.[28]

Node-RED.

Node-RED — це зручний візуальний інструмент, який дозволяє створювати програми або API безпосередньо у браузері. В першу чергу, це візуальний інструмент, розроблений для Інтернету речей, але його також можна використовувати для інших додатків, щоб дуже швидко зібрати потоки різних сервісів.

Воно має відкритий вихідний код і його створила організація IBM Emerging Technology. Воно входить до складу стартового пакету додатків IBM Bluemix (Platform-as-a-Service або PaaS). Node-RED також можна розгорнути окремо за допомогою додатка Node.js. Наразі Node-RED є проектом JS Foundation.

Node-RED дозволяє користувачам об'єднувати веб-сервіси та апаратне

забезпечення, замінюючи типові завдання низькорівневого кодування (наприклад, простий сервіс, що спілкується з послідовним портом), і це можна зробити за допомогою візуального інтерфейсу з функцією drag-and-drop. Різні компоненти в Node-RED з'єднуються між собою для створення потоку. Більшість необхідного коду створюється автоматично.

Основні функції Node-RED перелічені далі:

- Воно підтримує браузерне редагування потоку;

- Оскільки воно побудоване на Node.js, воно підтримує легке середовище виконання разом із подійно-орієнтованою та неблокуючою моделлю;

- Різні потоки Node-RED, можна зберегти за допомогою JSON, який легко завантажити для обміну даними;

- Його можна запускати локально (за допомогою Docker тощо);

- Він легко підходить для найбільш поширених пристроїв, таких як Raspberry Pi, BeagleBone Black, Arduino, пристрої Android тощо;

- Воно може працювати в хмарному середовищі, такому як Bluemix, AWS, MS-Azure тощо.

Grafana.

Grafana — це рішення з відкритим кодом для аналізу даних за допомогою метрик, які дають уявлення про складну інфраструктуру та величезний обсяг даних, з якими працюють сервіси, за допомогою налаштовуваних інформаційних панелей.

Grafana підключається до всіх можливих джерел даних, таких як Graphite, Prometheus, Influx DB, ElasticSearch, PostgreSQL, MySQL тощо. Відкритий характер рішення допомагає писати власні плагіни для підключення до будь-якого джерела даних.

Цей інструмент допомагає вивчати, аналізувати та відстежувати дані протягом певного періоду часу, що технічно називається аналітикою часових рядів. Він допомагає відстежувати поведінку користувачів, поведінку додатків, частоту помилок, що виникають у виробничому, попередньо виробничому або будь-якому іншому середовищі, тип помилок та контекстні сценарії, надаючи

відповідні дані.

Великою перевагою проєкту є те, що його можуть розгорнути на місці організації, які з міркувань безпеки не хочуть, щоб їхні дані передавалися до хмарного сховища постачальника. З часом ця платформа набула великої популярності в галузі і використовується такими гігантами, як PayPal, eBay, Intel та багато інших.

Grafana має безліч функцій, які надають вартість відразу після встановлення. Ці функції є причиною того, що Grafana, безперечно, є одним з найпопулярніших програмних засобів візуалізації, доступних для моніторингу метрик, завдяки їхній простоті у використанні:

- Візуалізація: Grafana має величезну кількість опцій візуалізації, які допоможуть легко переглядати та розуміти дані. Ці опції розділені на панелі, які потім використовуються для створення графічного інтерфейсу Grafana. Панель є найдетальнішим елементом візуалізації в Grafana. Вона використовується для відображення даних, які були отримані з джерела, пов'язаного з нею;
- Оповіщення: під час моніторингу додатків дуже важливо отримувати повідомлення, як тільки щось йде не так. Це має критичне значення для підтримання роботи систем і зменшення часу простою. Grafana має інтегровану підтримку величезного числа каналів повідомлень, залежно від того, що найбільше підходить. Щоб створити сповіщення, потрібно спочатку налаштувати правило. Це правило слугує тригером для сповіщення, так що кожного разу, коли воно порушується, сповіщення надсилається через канал зв’язку, який був налаштований;
- Анотації: Grafana дозволяє робити анотації, або, простіше кажучи, залишати нотатки безпосередньо на графіках. Ця проста, але потужна функція дозволяє легко позначати важливі точки. Це служить нагадуванням про подальші дії в майбутньому, надає контекст для нового члена команди або просто позначає особливу подію;
- Відкритий код: Grafana має відкритий код і підтримується активною спільнотою. Це надає користувачам величезні переваги, такі як гнучкість у

розробці та публікації власних плагінів або використанні плагінів, розроблених іншими. Їх легко встановити, завантаживши вихідний код і запустивши його вручну. Однак відкритий код має і деякі недоліки. Наприклад, доведеться самостійно обслуговувати свій екземпляр Grafana, виконувати оновлення тощо.

3.2 Апаратне забезпечення

Існує п'ять основних апаратних компонентів, які забезпечують роботу системи.

Датчики та виконавчі механізми.

Датчики вимірюють фізичні параметри, такі як температура, тиск, швидкість потоку, рівень та близькість, і перетворюють їх у сигнали, зрозумілі для комп'ютерів. До поширених промислових датчиків належать термометри опору, термопари, тензорезистори, рівнеміри та оптичні інфрачервоні пристрої. Виконавчі механізми отримують сигнали управління від контролерів і виконують такі дії, як відкриття клапанів, запуск двигунів та підняття заслінок для керування польовим обладнанням.

Датчик температури та вологості.

Датчик температури та вологості DHT22 (рис. 3.1) — це універсальний та економічний датчик, що вимірює температуру та вологість. Він базується на цифровому виході сигналу, забезпечуючи високу точність вимірювань з роздільною здатністю температури 0,1 градуса Цельсія та вологості 0,1%. Датчик використовує ємнісний елемент для вимірювання вологості та терморезистор для вимірювання температури. Датчик DHT22 також має відносно низьке енергоспоживання і може працювати в діапазоні напруги від 3,3 В до 5 В, що робить його придатним для проектів, що працюють від батарей. Крім того, він забезпечує довгострокову стабільність і високу надійність, що робить його ідеальним вибором для різних застосувань, включаючи системи опалення, вентиляції та кондиціонування повітря, метеостанції та системи моніторингу якості повітря.

Датчик DHT22 містить терморезистор NTC і сенсорний модуль. Елемент,

що вимірює вологість, складається з підкладки, що поглинає вологу, розміщеної поміж двох електродів. Коли вона поглинає вологу, опір зменшується. Зміна опору вимірюється вбудованим АЦП мікроконтролера і використовується для обчислення відносної вологості.

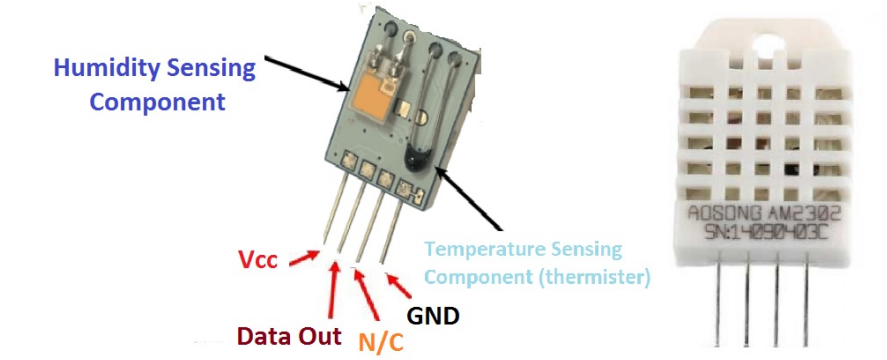


Рис. 3.1 Будова датчика DHT22[29]

Датчик вібрації.

MPU6050 — це невеликий, але потужний модуль, що поєднує в собі гіроскоп і акселерометр в одному чіпі. Таке поєднання дозволяє вимірювати обертання вздовж усіх трьох осей (X, Y і Z), статичне прискорення, спричинене гравітацією, та динамічне прискорення, спричинене рухом, ударами або вібраціями.

Акселерометр працює за принципом п'єзоелектричного ефекту, тобто здатності певних матеріалів генерувати електричний заряд у відповідь на механічне навантаження. Уявіть собі кубічну коробку, всередині якої знаходиться маленька кулька, як на рис. 3.2. Стінки цієї коробки виготовлені з п'єзоелектричних кристалів. Кожного разу, коли коробка нахиляється, кулька під дією сили тяжіння змушена рухатися в напрямку нахилу. Стінка, з якою стикається кулька, створює крихітні п'єзоелектричні струми. У кубі є три пари протилежних стінок. Кожна пара відповідає осі в 3D-просторі: осям X, Y і Z. Залежно від струму, що генерується п'єзоелектричними стінками, можна визначити напрямок нахилу і його величину.

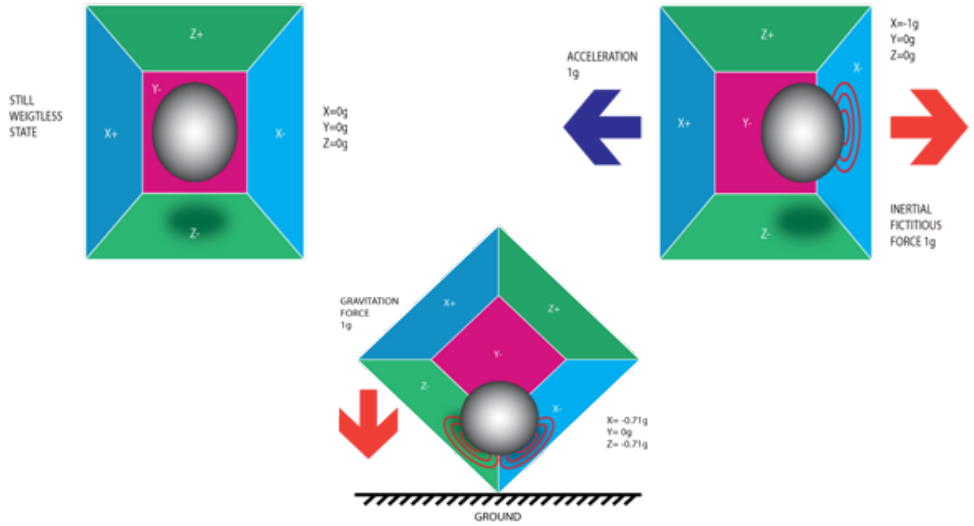


Рис. 3.2 Принцип роботи MPU6050[30]

Віддалені термінали.

Віддалений термінал (RTU) — це мікропроцесорний польовий контролер, який безпосередньо взаємодіє з датчиками та виконавчими механізмами в полі. RTU отримують телеметричні дані від датчиків і передають їх через комунікаційні мережі на центральний сервер SCADA. Вони також можуть отримувати команди управління від головної системи для керування підключеними виконавчими механізмами.

ESP32.

Чіп ESP32 зарекомендував себе як один з найпопулярніших і найуніверсальніших чіпів на ринку. Він використовується для різних застосувань Інтернету речей, бездротового зв'язку, робототехніки, домашньої автоматизації та обробки аудіо/відео. Крім того, що він має досить низьку вартість порівняно з конкурентами, а також має функції наднизького споживання енергії.

ESP32 — це універсальний і широко використовуваний мікроконтролер та система на кристалі (SoC) Wi-Fi/Bluetooth, вироблена Espressif Systems. SoC — це, по суті, інтегральна схема, яка використовує єдину платформу та інтегрує на ній всю електронну систему для конкретного застосування. На відміну від простого мікроконтролера (наприклад, Atmega324p Arduino Uno), який пропонує кілька периферійних пристроїв загального призначення замість конкретного набору

інструментів для одного застосування. У випадку з ESP32, він був розроблений як IoT SoC з уже інтегрованими Wifi, Bluetooth та криптографічним апаратним прискоренням, щоб дозволити користувачеві отримати доступ до Інтернету.

Крім того, ESP32 має вбудовану флеш-пам'ять об'ємом 4 Мб і близько 500 Кб оперативної пам'яті. Це є фундаментальним для підтримки стеку IP і TLS, а також усіх технологій, пов'язаних з інтернет-комунікацією, які споживають занадто багато ресурсів. Навіть використовуючи Wi-Fi або Bluetooth, все одно залишається додаткова оперативна пам'ять для решти коду. А в найгіршому випадку завжди можна придбати чіпи з кращими характеристиками, інтегрованою PSRAM 8 Мб і 32 Мб Flash.

Найголовніше, що якщо потрібно перейти на більший обсяг пам'яті, ми все одно можемо використовувати той самий код з декількома простими налаштуваннями. Без необхідності підключення або проектування нової друкованої плати, як у більшості мікроконтролерів на ринку.

Переваги використання ESP32 включають:

- Вартість: використання ESP32 знижує вартість обладнання. Зазвичай вартість готової до використання плати розробки ESP32 на ринку становить близько 6 доларів США, що значно дешевше для двоядерного чіпа з вбудованим Wi-Fi та Bluetooth. Інші альтернативи, такі як NRF, в середньому коштують 20 доларів США;

- Фреймворки: завдяки специфікаціям ESP32, він підтримується на багатьох платформах, що використовують різні SDK та мови програмування. Ось деякі з них:

Arduino (C/C++);

IDF, ADF (переважно C);

Platform (C/C++);

MicroPython (Python);

Mongoose OS (JavaScript/C);

espruino (JavaScript).

Це дозволяє мати різні варіанти при розробці прошивки та економити час,

використовуючи вже існуючі бібліотеки для конкретних додатків; можна отримати велику перевагу, наймаючи професійні компанії з розробки вбудованої прошивки. Тільки на офіційному веб-сайті виробника можна знайти спеціалізовані SDK для IoT, такі як IDF, аудіо ADF, бездротове з'єднання ESP-Mesh та ESP-Matter. Ці SDK також містять загальні рішення для продукту або прототипу, такі як управління сховищем, генерація командної консолі, OTA та забезпечення WIFI;

- Апаратне забезпечення: Espressif постійно випускає на ринок нові, більш потужні та спеціалізовані мікросхеми. Це стосується нової лінійки мікросхем ESP32-S, ESP32-C та ESP32-H. Підтримка різних бездротових протоколів та екосистем, таких як:

Wifi;

Bluetooth Classic;

Bluetooth BLE;

Thread;

Matter;

Zigbee;

EspNow;

Головний термінал (MTU).

MTU є центральним сервером системи SCADA. Промислові комп'ютери, встановлені в стійках, такі як розподілені системи управління (DCS) або системи на базі PLC, є надійними та надлишковим. MTU агрегує телеметрію від польових пристроїв, обробляє та архівує її з позначкою часу, виконує аналіз даних, розміщує програмне забезпечення для візуалізації людино-машинного інтерфейсу (HMI) та сприяє розподілу даних по мережі. Він також видає команди нагляду RTU на основі логіки або дій оператора. MTU забезпечує централізовану координацію розподілених об'єктів.

Підключення датчиків до ESP32.

Щоб отримати вимірювання на ESP32, використовуючи датчик температури і вологості DHT22, потрібно підключити його. DHT22 має чотири контакти, але

ми будемо використовувати тільки три з них:

1) DHT22 контакт 1 (VCC): цей контакт треба підключити до 3,3 В ESP32;
2) Контакт 2 DHT22 (дані): до GPIO 19 ESP32;
3) Контакт 4 DHT22 (GND): до GND ESP32.

Інтерфейс з DHT22 досить простий, оскільки він використовує однопровідний протокол, тобто нам потрібно лише підключити його до одного GPIO мікроконтролера.

Він працює з напругою живлення в діапазоні від 3,3 В до 5,5 В, тому його можна легко використовувати з ESP32.

Помістимо датчик на макетну плату поруч з ESP32. Підключимо контакт VCC датчика до контакту 3,3 В ESP32, а заземлення — до заземлення. Підключимо контакт даних датчика до контакту 19 ESP32.

MPU6050 спілкується з ESP32 через протокол I2C, тому нам потрібно лише два дроти для з'єднання ESP32 і MPU6050. Контакти SCL і SDA MPU6050 підключені до контактів D22 і D21 ESP32, а контакти VCC і GND MPU6050 підключені до 3,3 В і GND ESP32.

3.3 MQTT

MQTT — це протокол комунікації між машинами (M2M) для Інтернету речей, розроблений як легкий інструмент для публікації/підписки на повідомлення. MQTT корисний для з'єднань, де потрібна невелика кількість ресурсів або пропускна здатність мережі є обмеженою. MQTT був створений доктором Енді Стенфорд-Кларком з IBM та Арленом Ніппером з Arcom у 1999 році. На той час IBM співпрацювала з нафтогазовою компанією, якій потрібно було отримувати дані з нафтопроводів у віддалених районах, що вимагало нового протоколу, який би відповідав цим вимогам. Результатом стала розробка MQTT.

MQTT використовувався внутрішньо в IBM, поки в 2010 році не була випущена специфікація MQTT 3.1, що дозволило іншим створювати власні реалізації MQTT. Розробники швидко усвідомили цінність MQTT для випадків використання, пов'язаних з IoT, і його застосування швидко поширилося,

з'явилися численні брокери з відкритим кодом і клієнтські бібліотеки.

MQTT — це універсальний мережевий протокол, який ідеально підходить для будь-яких ситуацій, коли мережа може бути ненадійною, потрібно мінімізувати споживання пропускної здатності, є апаратне забезпечення з низьким енергоспоживанням або архітектура, в якій багато клієнтських пристроїв потребують доступу до одних і тих самих даних майже в режимі реального часу.

Протокол MQTT дозволяє системі SCADA отримувати доступ до даних IIoT. MQTT надає багато потужних переваг для робочого процесу:

- Більш ефективне розповсюдження інформації;
- Підвищення масштабованості;
- Значне зменшення споживання пропускної здатності мережі;
- Зменшення частоти оновлення до секунд;
- Дуже добре підходить для дистанційного зондування та контролю;
- Максимізація доступної пропускної здатності;
- Надзвичайно легка навантаження;
- Високий рівень безпеки завдяки системі дозволів;
- Використовується нафтогазовою промисловістю, Amazon, Facebook та іншими великими компаніями;
- Економія часу на розробку;
- Протокол публікації/підписки збирає більше даних з меншою пропускною здатністю в порівнянні з протоколами опитування.

MQTT використовує модель повідомлень публікації/підписки, що означає, що клієнтські пристрої підключаються до брокера, який виступає посередником між ними. Пристрої, підключені до брокера, можуть публікувати повідомлення, які будуть пересилатися іншим підключеним пристроям через брокера. Кожне повідомлення повинно мати тему, і брокер буде передавати повідомлення тільки тим пристроям, які явно підписалися на тему.

За допомогою MQTT будь-який підключений клієнтський пристрій може надсилати або отримувати повідомлення після підключення до брокера MQTT. Кожен пристрій також має можливість просто публікувати повідомлення без

підписки на теми або підписуватися тільки на теми і ніколи не публікувати жодних повідомлень.

Деякі з ключових понять, які потрібно знати, для роботи з MQTT, включають:

Брокер MQTT.

Брокери MQTT працюють, передаючи повідомлення між підключеними пристроями. Кожен пристрій, замість того, щоб зв'язуватися з іншими, що було б надзвичайно складним і ресурсоємним, має лише створити одне з'єднання з брокером, і він зможе отримувати дані від будь-якого іншого пристрою.

Брокери MQTT можуть обробляти мільйони підключених клієнтів і надавати ряд функцій, які будуть розглянуті далі в цьому розділі. Брокер робить ці функції можливими, і саме тому MQTT настільки популярний серед розробників IoT.

Клієнт MQTT.

Клієнт MQTT — це будь-який пристрій, на якому працює програмне забезпечення MQTT, що дозволяє йому підключатися до брокера. Клієнти MQTT можуть публікувати повідомлення, а також підписуватися на теми для їх отримання. Клієнт MQTT — це будь-що, що здатне запускати реалізацію бібліотеки клієнта і підключатися до брокера.

Деталі протоколу MQTT.

В основі MQTT лежить мережевий стек TCP/IP. Хоча він дещо менш продуктивний і легкий у порівнянні з UDP, TCP забезпечує гарантовану доставку, що є життєво важливим для багатьох випадків використання IoT. Ще однією перевагою використання TCP є те, що MQTT може шифрувати дані за допомогою SSL/TLS.

Теми.

Теми є основним способом, за допомогою якого MQTT організовує повідомлення, що надсилаються до брокера. Кожне повідомлення, що надсилається, вимагає визначеної теми, а підключені пристрої можуть підписуватися на теми, щоб отримувати повідомлення, коли вони надсилаються.

Теми є рядками UTF-8, які розділяються за допомогою косих рисок. Ось приклад базової теми MQTT: «top/middle/bottom»

Ці повідомлення можуть бути будь-якими, але в ідеалі вони матимуть базову структуру, щоб зробити ієрархію тем логічною і зрозумілою для розробників, оскільки програма з часом розростається і додається все більше тем. Теми не потрібно заздалегідь визначати перед публікацією повідомлень або перед тим, як клієнти підпишуться на тему, їх можна додавати нові теми на ходу, не турбуючись про це.

Окрім основних статичних текстових рядків, таких як вищезазначені теми, MQTT підтримує динамічні теми за допомогою операторів-замінників, використовуючи знак + між косими рисками. Знак плюс забезпечує лише однорівневе узгодження замінників. Якщо потрібна багаторівнева підтримка замінників, можна використовувати хештег, і тема буде відповідати будь-чому після хештега. Наприклад, якщо потрібно підписатися на всі повідомлення, які генерує розумний дім, треба використовувати таку тему: «home/#» .

Ці оператори-замінники дуже корисні, але їх слід використовувати обережно, бо надмірне використання замінників, коли вони не потрібні, призведе до погіршення продуктивності брокера, оскільки він використовує ресурси для надсилання повідомлень на пристрої, які їх не потребують. Потрібно переконатися, що пристрій потребує підписки на тему MQTT, якщо ні, буде марнуватися пропускна здатність і обчислювальна потужність, доставляючи повідомлення MQTT, які не потрібні клієнтам, що їх отримують.

Сесії.

Сесія MQTT — це все, що відбувається з моменту, коли клієнтський пристрій надсилає запит на підключення до брокера MQTT, до моменту переривання з'єднання. Виходячи з цього, сесія може бути лише невдалим початковим запитом на підключення або тривалою з великою кількістю повідомлень, що публікуються та отримуються клієнтом.

Сесії важливі, оскільки вони мають пов'язаний стан залежно від рівня якості обслуговування (QoS), встановленого для відповідних повідомлень. Брокер

повинен мати можливість визначити, чи були певним клієнтським пристроям доставлені необхідні повідомлення, а клієнт у деяких випадках повинен відповісти, щоб підтвердити, що вони були доставлені.

Термін дії повідомлення.

MQTT дозволяє клієнтам встановлювати термін дії опублікованих повідомлень. Він встановлюється в секундах і вказує брокеру, як довго зберігати повідомлення перед його видаленням. Якщо термін дії повідомлення закінчується, коли клієнт не підключений, він не отримає повідомлення.

Функція Keep Alive.

MQTT забезпечує спосіб перевірки, чи встановлене з'єднання між брокером і клієнтом все ще активне, шляхом встановлення інтервалу для підтвердження з'єднання. Це відоме як функція Keep Alive, і частоту її використання може визначити розробник, який використовує MQTT. Якщо клієнт не надіслав або не отримав повідомлення від брокера протягом встановленого інтервалу, брокер надсилає клієнту запит ping і очікує на відповідь. Якщо клієнт не відповість, брокер зареєструє пристрій як відключений.

Збережені повідомлення.

Збережені повідомлення — це звичайні повідомлення MQTT, які були позначені, щоб їх зберігав брокер. Використовуючи збережені повідомлення, будь-який клієнт, який підписався на тему, отримає найновіше збережене повідомлення, щоб клієнт міг отримати найновіше оновлення, а не чекати на надсилання повідомлення.

Якість обслуговування.

Якість обслуговування (QoS) — це спосіб, яким MQTT контролює гарантії доставки повідомлень. MQTT QoS — це, по суті, угода між відправником і одержувачем повідомлення про те, як визначити, що потрібно, щоб вважати повідомлення «доставленим». В MQTT доступні три рівні QoS:

- Щонайбільше раз (0) - Мінімальний рівень QoS, який вважається доставкою «з максимальним зусиллям». Немає гарантії, що повідомлення досягне підписників, і підтвердження не надсилається до пристрою, що публікує. Брокер

просто підтверджує, що підписник підключений, і надсилає йому повідомлення;

- Щонайменше раз (1) - Рівень QoS 1 гарантує доставку повідомлення, але може призвести до того, що повідомлення буде надіслано або навіть доставлено кілька разів. Наявність декількох копій одного і того ж повідомлення може призвести до проблем, якщо це не враховано у програмі;
- Рівно один раз (2) - Рівень QoS 2 є найвищим рівнем обслуговування, що надається MQTT. Він не тільки гарантує доставку підписаним клієнтам, але й гарантує, що вони отримають повідомлення тільки один раз. MQTT робить це, вимагаючи 4-частинного рукостискання, щоб спочатку підтвердити, що клієнт отримав повідомлення, а потім ще один запит і відповідь з використанням прапорця, щоб переконатися, що не було отримано дублікатів повідомлень.

Під час доставки повідомлення є дві частини, пов'язані з доставкою повідомлення до місця призначення. Спочатку повідомлення створюється і публікується клієнтом і надсилається до брокера MQTT, а потім брокер повинен доставити це повідомлення клієнтам, які підписалися.

QoS є однією з найважливіших функцій, що надаються MQTT, оскільки вона дозволяє розробникам встановлювати певні гарантії залежно від важливості їхніх даних. Це означає, що навіть у ненадійних мережах MQTT можна покладатися на доставку даних. Водночас це надає розробникам гнучкість; якщо певні дані не є важливими, MQTT може дозволити втрату цих повідомлень і не витрачати пропускну здатність у певних ситуаціях.

LWT (Last Will and Testament).

LWT — це функція, що надається MQTT, яка дозволяє клієнтам вказати повідомлення, яке буде надіслано іншим клієнтським пристроям, якщо воно припинить з'єднання через непередбачену помилку. Коли клієнтський пристрій підключається до брокера MQTT, LWT надсилаються і зберігаються на брокері. Повідомлення буде надіслано, коли брокер виявить, що клієнт відключився, не надіславши стандартне повідомлення DISCONNECT, яке використовується для звичайних відключень.

3.4 Програмне забезпечення

Датчики.

Код для зчитування даних з датчиків за допомогою ESP32 наведено нижче.

```
#include <Arduino.h>
#include <ArduinoJson.h>
#include "DHTesp.h"
#include <WiFi.h>
#include <WiFiClientSecure.h>
#include <PubSubClient.h>
#include <Adafruit_MPU6050.h>
#include <Adafruit_Sensor.h>
#include <Wire.h>

const char* ssid = "Wokwi-GUEST";
const char* password = "";

const char* mqtt_broker = "952bab3d263548bbaba6f6dc215e99f5.s1.eu.hivemq.cloud";
const int mqtt_port = 8883;
const char* mqtt_username = "admin";
const char* mqtt_password = "Sergbond9325";

const char* topic_publish = "esp32/sensor_data";


const int temp_and_hum_sensor_pin = 19;

DHTesp dhtSensor;
WiFiClientSecure wifiClient;
PubSubClient mqttClient(wifiClient);

Adafruit_MPU6050 mpu;

long previous_time = 0;

void setupMQTT() {
  mqttClient.setServer(mqtt_broker, mqtt_port);
}

void reconnect() {
  Serial.println("Connecting to MQTT Broker...");
  while (!mqttClient.connected()) {
    Serial.println("Reconnecting to MQTT Broker...");
    String clientId = "ESP32Client-";
    clientId += String(random(0xffff), HEX);

    if (mqttClient.connect(clientId.c_str(), mqtt_username, mqtt_password)) {
      Serial.println("Connected to MQTT Broker.");
```

```
    } else {
      Serial.print("Failed, rc=");
      Serial.print(mqttClient.state());
      Serial.println(" try again in 5 seconds");
      delay(5000);
    }
  }
}

void setup() {
  Serial.begin(115200);

  WiFi.begin(ssid, password);
  while (WiFi.status() != WL_CONNECTED) {
    delay(500);
    Serial.print(".");
  }
  Serial.println("");
  Serial.println("Connected to Wi-Fi");

  wifiClient.setInsecure();

  setupMQTT();

  if (!mpu.begin()) {
    Serial.println("Failed to find MPU6050 chip");
    while (1) {
      delay(10);
    }
  }
  Serial.println("MPU6050 Found!");

  mpu.setAccelerometerRange(MPU6050_RANGE_8_G);
  Serial.print("Accelerometer range set to: ");
  switch (mpu.getAccelerometerRange()) {
  case MPU6050_RANGE_2_G:
    Serial.println("+-2G");
    break;
  case MPU6050_RANGE_4_G:
    Serial.println("+-4G");
    break;
  case MPU6050_RANGE_8_G:
    Serial.println("+-8G");
    break;
  case MPU6050_RANGE_16_G:
    Serial.println("+-16G");
    break;
  }

  mpu.setFilterBandwidth(MPU6050_BAND_5_HZ);
```

```
  Serial.print("Filter bandwidth set to: ");
  switch (mpu.getFilterBandwidth()) {
  case MPU6050_BAND_260_HZ:
    Serial.println("260 Hz");
    break;
  case MPU6050_BAND_184_HZ:
    Serial.println("184 Hz");
    break;
  case MPU6050_BAND_94_HZ:
    Serial.println("94 Hz");
    break;
  case MPU6050_BAND_44_HZ:
    Serial.println("44 Hz");
    break;
  case MPU6050_BAND_21_HZ:
    Serial.println("21 Hz");
    break;
  case MPU6050_BAND_10_HZ:
    Serial.println("10 Hz");
    break;
  case MPU6050_BAND_5_HZ:
    Serial.println("5 Hz");
    break;
  }


  pinMode(temp_and_hum_sensor_pin, INPUT); // Set IR sensor pin as input
  dhtSensor.setup(temp_and_hum_sensor_pin, DHTesp::DHT22);
}

void loop() {
  if (!mqttClient.connected()) {
    reconnect();
  }
  mqttClient.loop();

  TempAndHumidity  data = dhtSensor.getTempAndHumidity();

  sensors_event_t a, g, temp;
  mpu.getEvent(&a, &g, &temp);

  JsonDocument JSONbuffer;
  JsonObject JSONencoder = JSONbuffer.to<JsonObject>();

  JSONencoder["equipment"] = "Turbine";
  JSONencoder["location"] = "Kyiv";
  JsonArray values = JSONencoder["values"].to<JsonArray>();


  values.add(data.temperature);
```

```
  values.add(data.humidity);
  values.add(a.acceleration.x);

  char JSONmessageBuffer[100];

  serializeJson(JSONbuffer, JSONmessageBuffer);
  long now = millis();
  if (now - previous_time > 1000) { // Publish every 10 seconds
    previous_time = now;

    Serial.print("Sensor Value: ");
    Serial.println(String(data.temperature, 2) + " " + String(data.humidity, 1) + " "
+ String(a.acceleration.x));
    mqttClient.publish(topic_publish, JSONmessageBuffer);
  }
}
```

Перше, що нам потрібно зробити, це підключити бібліотеки, щоб отримати доступ до функцій, необхідних для вимірювання.

```
#include <Arduino.h>
#include <ArduinoJson.h>
#include "DHTesp.h"
#include <WiFi.h>
#include <WiFiClientSecure.h>
#include <PubSubClient.h>
#include <Adafruit_MPU6050.h>
#include <Adafruit_Sensor.h>
#include <Wire.h>
```

Підключимося до Wi-Fi, вказавши SSID і пароль мережі.

```
const char* ssid = "Wokwi-GUEST";
const char* password = "";
```

Тепер нам потрібно використовувати метод setServer, для якого потрібна адреса і порт брокера.

```
void setupMQTT() {
    mqttClient.setServer(mqtt_broker, mqtt_port);
}
```

Використаємо PubSubClient для встановлення з'єднання з брокером MQTT.

```
void reconnect() {
  Serial.println("Connecting to MQTT Broker...");
  while (!mqttClient.connected()) {
    Serial.println("Reconnecting to MQTT Broker...");
    String clientId = "ESP32Client-";
    clientId += String(random(0xffff), HEX);

    if (mqttClient.connect(clientId.c_str(), mqtt_username, mqtt_password)) {
      Serial.println("Connected to MQTT Broker.");
    } else {
      Serial.print("Failed, rc=");
      Serial.print(mqttClient.state());
      Serial.println(" try again in 5 seconds");
      delay(5000);
    }
  }
}
```

Функція setAccelerometerRange() визначає, яке прискорення може виміряти датчик.

```
  mpu.setAccelerometerRange(MPU6050_RANGE_8_G);
  Serial.print("Accelerometer range set to: ");
  switch (mpu.getAccelerometerRange()) {
  case MPU6050_RANGE_2_G:
    Serial.println("+-2G");
    break;
  case MPU6050_RANGE_4_G:
    Serial.println("+-4G");
    break;
  case MPU6050_RANGE_8_G:
    Serial.println("+-8G");
```

```
  break;
 case MPU6050_RANGE_16_G:
  Serial.println("+-16G");
  break;
 }
```

Функція setFilterBandwidth() встановлює пропускну здатність цифрового фільтра нижніх частот, що допомагає згладити сигнал, позбавившись від високочастотних шумів.

```
 mpu.setFilterBandwidth(MPU6050_BAND_5_HZ);
 Serial.print("Filter bandwidth set to: ");
 switch (mpu.getFilterBandwidth()) {
 case MPU6050_BAND_260_HZ:
  Serial.println("260 Hz");
  break;
 case MPU6050_BAND_184_HZ:
  Serial.println("184 Hz");
  break;
 case MPU6050_BAND_94_HZ:
  Serial.println("94 Hz");
  break;
 case MPU6050_BAND_44_HZ:
  Serial.println("44 Hz");
  break;
 case MPU6050_BAND_21_HZ:
  Serial.println("21 Hz");
  break;
 case MPU6050_BAND_10_HZ:
  Serial.println("10 Hz");
  break;
 case MPU6050_BAND_5_HZ:
```

```
  Serial.println("5 Hz");
  break;
 }
```

Переходячи до функції головного циклу, ми будемо періодично отримувати поточну температуру, викликаючи метод getTemperature на нашому раніше ініціалізованому об'єкті DHTesp.

```
  TempAndHumidity  data = dhtSensor.getTempAndHumidity();
```

Ми будемо зчитувати прискорення, обертання і температуру і відображати їх на послідовному моніторі. Спочатку створимо об'єкт sensors_event_t для зберігання результатів. sensors_event_t — це визначений користувачем тип даних (структури в C), який містить дані з датчика mpu в певний момент часу.

```
  sensors_event_t a, g, temp;
```

Функція getEvent() використовується для зчитування нового набору значень з датчика mpu, перетворення їх у відповідні одиниці SI та масштаб, а потім присвоєння результатів об'єкту датчика mpu.

```
 mpu.getEvent(&a, &g, &temp);
```

Тепер у функції головного циклу ми оголошуємо об'єкт класу JsonDocument, який буде використовуватися для створення повідомлення JSON, що надсилається через MQTT.

```
  JsonDocument JSONbuffer;
  JsonObject JSONencoder = JSONbuffer.to<JsonObject>();
```

Далі додаємо значення до нашого JsonObject.

```
  JSONencoder["equipment"] = "Turbine";
  JSONencoder["location"] = "Kyiv";
  JsonArray values = JSONencoder["values"].to<JsonArray>();

  values.add(data.temperature);
  values.add(data.humidity);
  values.add(a.acceleration.x);
```

Тепер ми надрукуємо повідомлення JSON у буфер символів за допомогою

функції serializeJson.

```
char JSONmessageBuffer[100];
serializeJson(JSONbuffer, JSONmessageBuffer);
```

Після успішного встановлення з'єднання з брокером MQTT, ESP32 опублікує повідомлення у відповідну тему.

```
mqttClient.publish(topic_publish, JSONmessageBuffer);
```

Моделювання бази даних.

Спочатку перетягнемо вузол MQTT (рис. 3.3) на сторінку в меню зліва. Після подвійного клацання на вузлі праворуч з'явиться сторінка конфігурації для редагування вузла MQTT, потім ми створимо нову інформацію про з'єднання відповідно до інструкцій, заповнимо іншу інформацію про з'єднання MQTT і натиснимо кнопку «Готово», щоб зберегти інформацію про вузол.

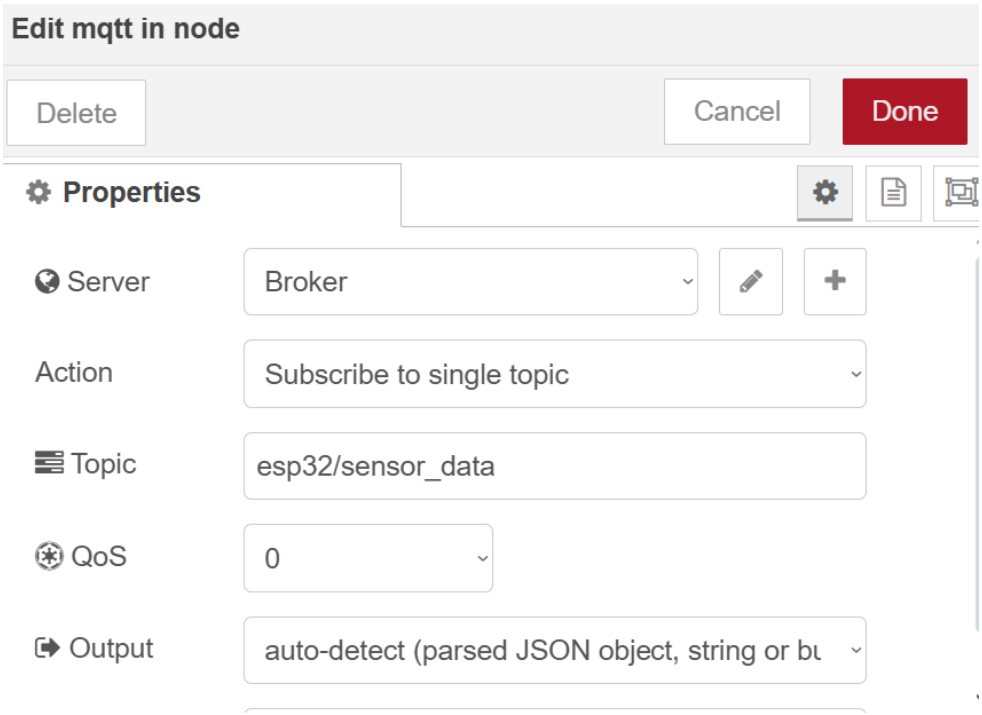


Рис. 3.3 Вузол MQTT

Після додання вузлу JSON на сторінку, ми зможемо налаштувати дію (рис. 3.4) на сторінці конфігурації. Потім ми встановлюємо його як «Завжди конвертувати в об'єкт Javascript». Оскільки ми не можемо бути впевнені, чи отримані дані є даними у форматі JSON або рядком JSON, першим кроком є

виконання конвертації для отриманих повідомлень. Після конфігурації ми підключаємо цей вузол до вузла MQTT.

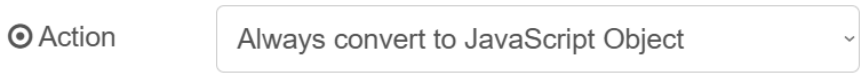


Рис 3.4 Дія вузлу JSON

Дані, закодовані в JSON, також є текстовим рядком, тому їх можна зберігати безпосередньо в базі даних, але частіше за все потрібно витягти частини даних для використання як ключі бази даних (імена стовпців).

Процес такий:

1) Витягнення елементів даних із вхідних даних;
2) Створення команди SQL;
3) Передача команди до коннектора бази даних.

Наступний фрагмент коду показує, як ми це робимо:

```
var temperature = msg.payload.values[0];
var vibration = msg.payload.values[2];
var humidity = msg.payload.values[1];
var equipment = msg.payload.equipment;
var location = msg.payload.location;
var faulty;
if (temperature > 85 || humidity > 60 || humidity < 40) {
    faulty = true;
  } else {
    faulty = false;
  }

msg.topic = "INSERT INTO `equipment_anomaly_data`(`temperature`, `vibration`,
`humidity`, `equipment`, `location`, `faulty`)" +
"VALUES ("+temperature+", "+vibration+", "+humidity+", "+equipment+", "+location+",
"+faulty+")";

return msg;
```

Перетягнемо вузол MySQL на полотно, а потім натиснемо кнопку «+», розташовану поруч із полем «База даних». Введемо змінні середовища, додані для хоста, порту, користувача, пароля та бази даних, у відповідні поля. Залишимо набір символів за замовчуванням, оскільки він встановлений на «UTF8», який є широко сумісним і підтримує різні мови та символи. Натиснемо «Додати», щоб

зберегти конфігурацію.

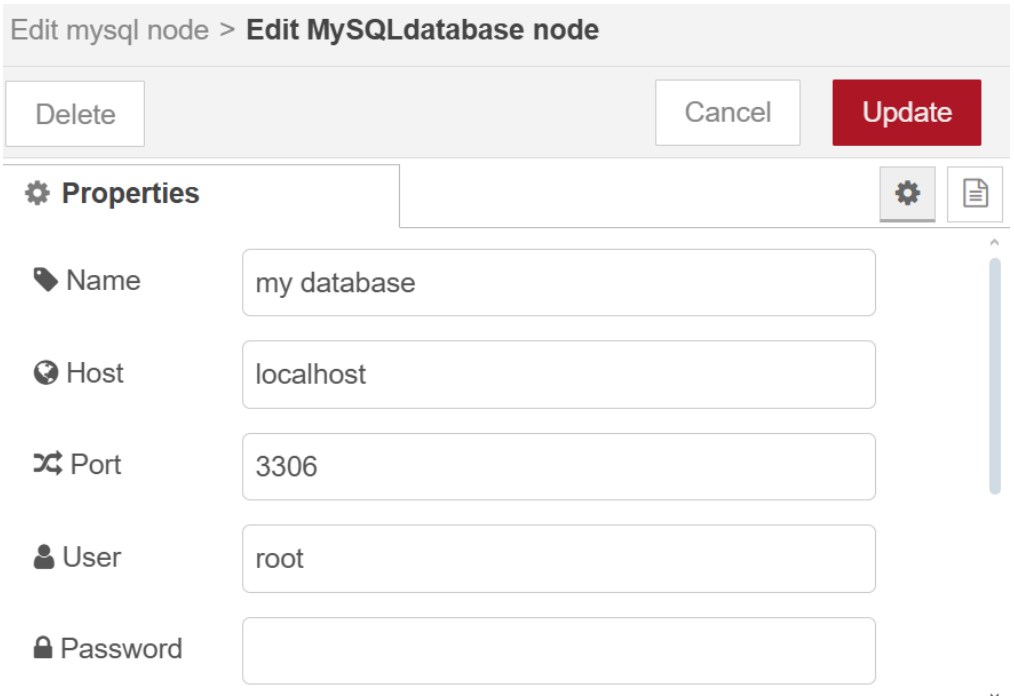


Рис. 3.5 Вузол MySQL

Створення панелі спостереженя.

У меню навігації натисніть Джерела > Додати нове з'єднання. На цій сторінці ми можемо знайти MySQL Server і вибрати його як джерело даних.

Після цього будуть запропоновані необхідні параметри конфігурації для з'єднання з даними MySQL (рис. 3.5). Ось що потрібно заповнити:

- Хост: IP-адреса або доменне ім'я хостингового сервера MySQL, а також порт, який використовується для сервера бази даних. Зверніть увагу, що якщо налаштоване з'єднання з localhost:3306, яке є заданим значенням за замовчуванням, потрібно натиснути на поле і ввести його, інакше з'єднання не буде працювати;
- База даних: база даних, яка буде використовуватися як джерело;
- Користувач;
- Пароль.

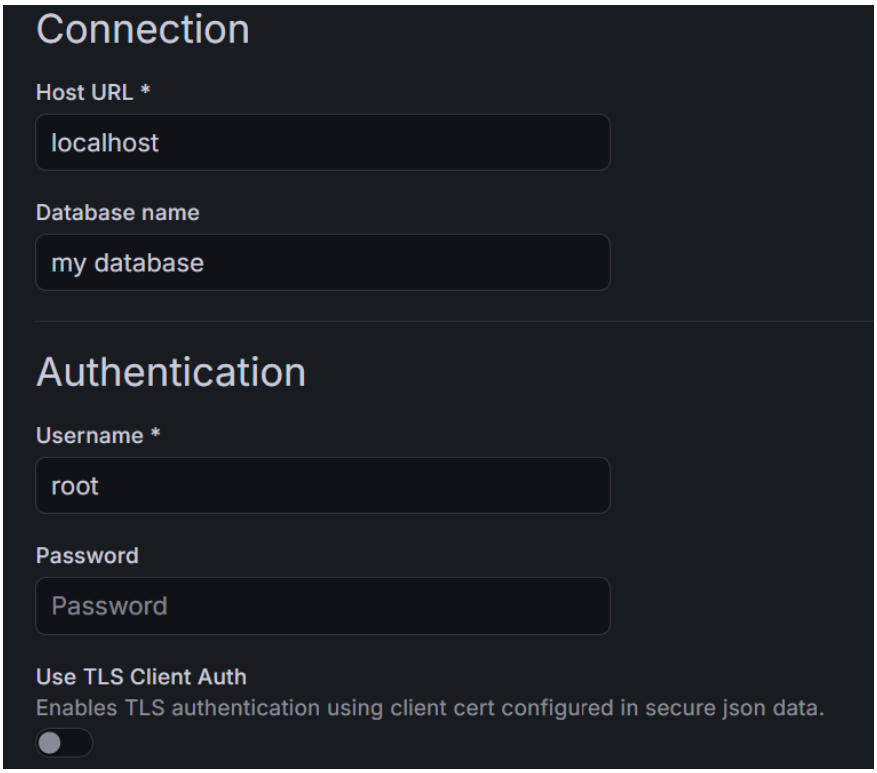


Рис. 3.5 Параметри з'єднання MySQL

Можливо, також доведеться увімкнути опцію «Пропустити перевірку TLS». Варто вказати ім'я для цього з'єднання, особливо якщо потрібно мати кілька з'єднань MySQL з Grafana.

Налаштуємо ці параметри та натиснемо «Зберегти та перевірити». Зрештою ми побачите повідомлення «З'єднання з базою даних успішне».

Після створення джерела даних для MySQL можна почати створювати інформаційні панелі на основі даних MySQL. Почнемо з меню навігації та натиснемо «Інформаційні панелі». На сторінці «Інформаційні панелі» натиснемо «+ Створити інформаційну панель», а потім «+ Додати візуалізацію». Відкриється вікно «Вибрати джерело даних», де треба вибрати створене з'єднання. Потім натиснемо «Виконати запит», щоб виконати згенерований запит. Після виконання запиту отримані дані заповнюються над редактором запитів. Тут можете вибрати візуалізацію, яку потрібно використовувати для представлення даних на інформаційній панелі.

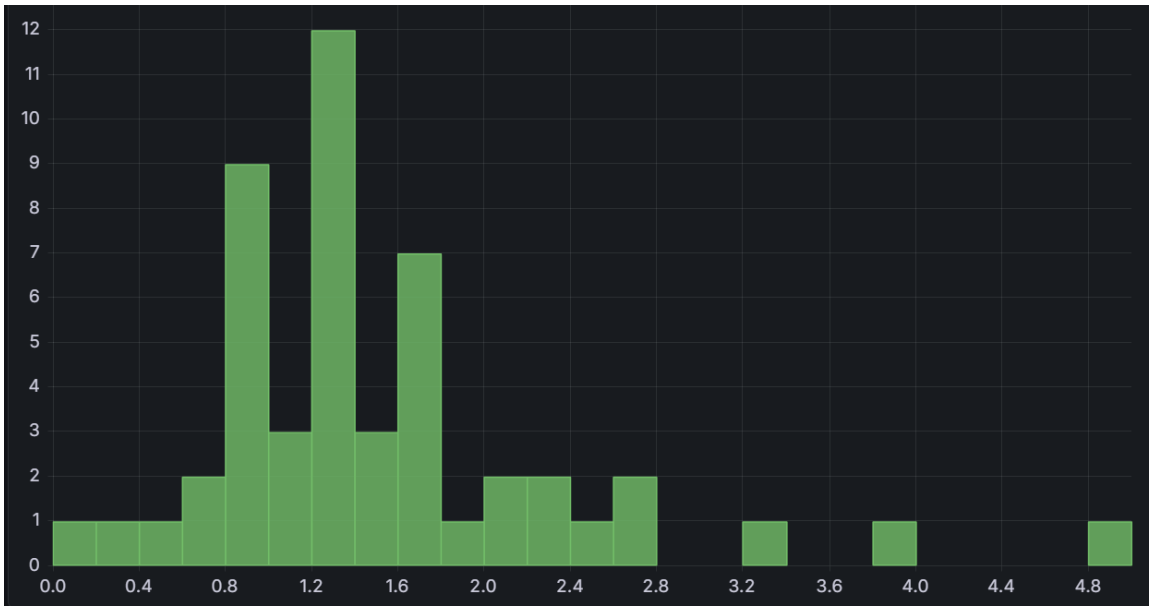


Рис. 3.6 Приклад візуалізації Grafana

3.5 Тестування розробленої IoT-системи

Після завантаження коду в ESP32 відкриємо послідовний порт Arduino IDE (рис. 3.7) і встановимо швидкість передачі даних 115200. Нарешті, ми можемо побачити показання MPU-6050 на послідовному порту Arduino.

```
Gyro range set to: +- 500 deg/s
Filter bandwidth set to: 5 Hz
Connecting to MQTT Broker...
Reconnecting to MQTT Broker...
Connected to MQTT Broker.
Sensor Value: 24.00 40.0 0.00
```

Рис. 3.7 Послідовний порт

Після розгортання потоку можна протестувати кожну операцію. Для налагодження додайте до потоку вузли налагодження.

id 1	temperature	vibration	equipment	humidity	location	faulty
7675	24	0	Turbine	40	Kyiv	0

Рис. 3.8 Додання нового запису в базу даних

Після налаштування джерела даних MySQL ми можемо почати створювати

інформаційні панелі та візуалізації.

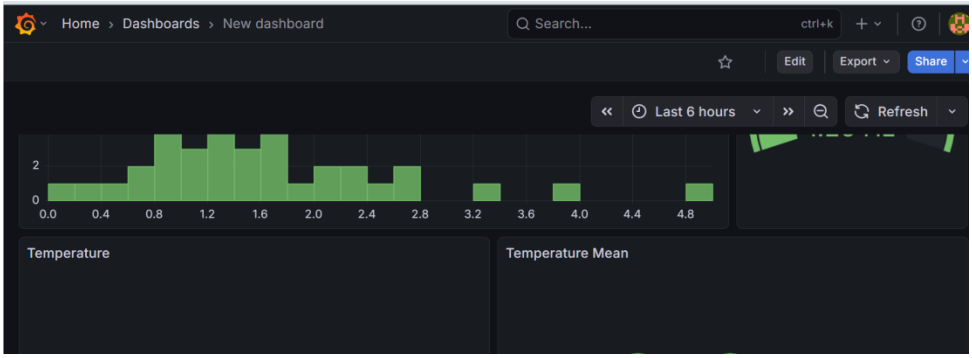


Рис. 3.9 Приклад інформаційної панелі Grafana

Ми бачимо проблему до того, як вона стане критичною. Можна вивантажити PDF-звіт для клієнта або керівництва про те, що всі бекапи за місяць пройшли успішно.

ВИСНОВКИ

При виконанні кваліфікаційної роботи було розроблено IoT-рішення для запобігання аварій у промислових системах за допомогою аналізу сенсорних даних.

У першому розділі було проведено огляд архітектури та існуючих рішень у сфері IoT. Як він показав Інтернет Речей має потенціал докорінно змінити сферу технічного обслуговування індустріальних машин з допомогою технологій предиктивного обслуговування та моніторингу стану. Було розглянуто ряд перспективних рішень та стартапів IoT, що показали його користь в сучасній індустрії.

У другому розділі було детально вивчено принципи роботи технології SCADA і встановлено її перспективи використання. Можливість отримувати дані будь-де з великою швидкістю та дистанційно керувати технічним обладнанням у разі несправності робить цю технологію великим проривом у сфері запобігання аварій.

Третій розділ складається з вибору інструментів розробки та фізичних компонентів. Розроблене рішення включає апаратну архітектуру на основі ESP32 і сучасних сенсорів та програмне забезпечення, що працює через MQTT та Grafana. Датчики DHT22 та MPU6050 передають дані на ESP32, що у свою чергу під’єднується до Wi-Fi мережі та публікує їх на MQTT брокер. Брокер надсилає дані далі на сервер, що зберігає їх у базі даних MySQL. Користувацький інтерфейс потім використовує ці дані для створення візуалізації.

ПЕРЕЛІК ПОСИЛАНЬ

1. Role Of Iot In Digital Marketing [Електронний ресурс] // GEC Designs. – Режим доступу: https://gecdesigns.com/blog/role-of-iot-in-digital-marketing. – Назва з екрана.
2. IoT Architecture - Detailed Explanation [Електронний ресурс] // InterviewBit. – Режим доступу: https://www.interviewbit.com/blog/iot-architecture/. – Назва з екрана.
3. What Is the Internet of Things? [Електронний ресурс] // Oracle. – Режим доступу: https://www.oracle.com/internet-of-things/. – Назва з екрана.
4. Components of IOT and relation with Cloud Computing - GeeksforGeeks [Електронний ресурс] // GeeksforGeeks. – Режим доступу: https://www.geeksforgeeks.org/blogs/components-of-iot-and-relation-with-cloud-computing/. – Назва з екрана.
5. Gokhale P. Introduction to IOT [Електронний ресурс] / Pradyumna Gokhale, Omkar Bhat, Sagar Bhat // International Advanced Research Journal in Science, Engineering and Technology. – 2018. – Т. 5, № 1. – Режим доступу: https://www.researchgate.net/publication/330114646_Introduction_to_IOT. – Назва з екрана.
6. Devi Kotha H. IoT Application, A Survey [Електронний ресурс] / Harika Devi Kotha, V. Mnssvkr Gupta // International Journal of Engineering & Technology. – 2018. – Т. 7, № 2.7. – С. 891. – Режим доступу: https://doi.org/10.14419/ijet.v7i2.7.11089. – Назва з екрана.
7. An overview of IoT architectures, technologies, and existing open-source projects [Електронний ресурс] / Tomás Domínguez-Bolaño [та ін.] // Internet of Things. – 2022. – С. 100626. – Режим доступу: https://doi.org/10.1016/j.iot.2022.100626. – Назва з екрана.
8. De Masi G. The impact of topology on Internet of Things: A multidisciplinary review [Електронний ресурс] / Giulia De Masi // 2018 Advances in Science and Engineering Technology International Conferences (ASET), Abu Dhabi, 6 лют. – 5

квіт. 2018 р. – [Б. м.], 2018. – Режим доступу: https://doi.org/10.1109/icaset.2018.8376837. – Назва з екрана.

9. MacLachlan K. IoT in the workplace: Benefits & applications [Електронний ресурс] / Kristan MacLachlan // AT&T Business. – Режим доступу: https://www.business.att.com/learn/articles/iot-in-the-workplace.html. – Назва з екрана.
10. Elangovan M. Monitoring of Workplace Safety Using IoT [Електронний ресурс] / Muniyandy Elangovan, D. Surrya Prakash, P. Sasidharan // Journal of Physics: Conference Series. – 2021. – Т. 2115, № 1. – С. 012014. – Режим доступу: https://doi.org/10.1088/1742-6596/2115/1/012014. – Назва з екрана.
11. IBM. What is a Condition Monitoring (CM)? | IBM [Електронний ресурс] / IBM // IBM. – Режим доступу: https://www.ibm.com/think/topics/condition-monitoring. – Назва з екрана.
12. Condition Monitoring: A Decade of Proposed Techniques [Електронний ресурс] / Yvan Avenas [та ін.] // IEEE Industrial Electronics Magazine. – 2015. – Т. 9, № 4. – С. 22–36. – Режим доступу: https://doi.org/10.1109/mie.2015.2481564. – Назва з екрана.
13. Importance of condition monitoring in mechanical domain [Електронний ресурс] / S. K. Nithin [та ін.] // Materials Today: Proceedings. – 2021. – Режим доступу: https://doi.org/10.1016/j.matpr.2021.08.299. – Назва з екрана.
14. On Predictive Maintenance in Industry 4.0: Overview, Models, and Challenges [Електронний ресурс] / Mounia Achouch [та ін.] // Applied Sciences. – 2022. – Т. 12, № 16. – С. 8081. – Режим доступу: https://doi.org/10.3390/app12168081. – Назва з екрана.
15. A Survey of Predictive Maintenance: Systems, Purposes and Approaches [Електронний ресурс] / Tianwen Zhu Zhu [та ін.] // IEEE Communications Surveys and Tutorials. – 2019. – Режим доступу: https://doi.org/10.48550/arXiv.1912.07383. – Назва з екрана.
16. What is SCADA? Supervisory Control and Data Acquisition [Електронний ресурс] // PTC. – Режим доступу: https://www.ptc.com/en/technologies/iiot/industrial-

automation/scada. – Назва з екрана.

17. Two decades of SCADA exploitation: A brief history [Електронний ресурс] / Simon Duque Anton [та ін.] // 2017 IEEE Conference on Application, Information and Network Security (AINS), Miri, 13–14 листоп. 2017 р. – [Б. м.], 2017. – Режим доступу: https://doi.org/10.1109/ains.2017.8270432. – Назва з екрана.
18. A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics [Електронний ресурс] / Dimitrios Pliatsios [та ін.] // IEEE Communications Surveys & Tutorials. – 2020. – Т. 22, № 3. – С. 1942–1976. – Режим доступу: https://doi.org/10.1109/comst.2020.2987688. – Назва з екрана.
19. SCADA (Supervisory Control and Data Acquisition) [Електронний ресурс] // VKS. – Режим доступу: https://vksapp.com/dictionary/scada-supervisory-control-and-data-acquisition. – Назва з екрана.
20. User Guide : Node-RED [Електронний ресурс] // Low-code programming for event-driven applications : Node-RED. – Режим доступу: https://nodered.org/docs/user-guide/. – Назва з екрана.
21. HiveMQ Documentation [Електронний ресурс] // HiveMQ Platform. – Режим доступу: https://docs.hivemq.com/hivemq/latest/user-guide/index.html. – Назва з екрана.
22. Technical documentation [Електронний ресурс] // Grafana Labs. – Режим доступу: https://grafana.com/docs/. – Назва з екрана.
23. ESP Test Tools and Guidelines - ESP32 [Електронний ресурс] // Technical Documents | Espressif Systems. – Режим доступу: https://docs.espressif.com/projects/esp-test-tools/en/latest/esp32/index.html. – Назва з екрана.
24. Digital-output relative humidity & temperature sensor/module DHT22 (DHT22 also named as AM2302) [Електронний ресурс] // SparkFun Electronics. – Режим доступу: https://cdn.sparkfun.com/assets/f/7/d/9/c/DHT22.pdf. – Назва з екрана.
25. Siepert B. MPU6050 6-DoF Accelerometer and Gyro [Електронний ресурс] / Bryan Siepert, Isaac Wellish // Adafruit Learning System. – Режим доступу: https://learn.adafruit.com/mpu6050-6-dof-accelerometer-and-gyro. – Назва з

екрана.

26. MQTT Version 5.0 [Електронний ресурс] // OASIS Open. – Режим доступу: https://docs.oasis-open.org/mqtt/mqtt/v5.0/os/mqtt-v5.0-os.pdf. – Назва з екрана.
27. Introduction of Message Queue Telemetry Transport Protocol (MQTT) [Електронний ресурс] / GeeksforGeeks. – Режим доступу: https://www.geeksforgeeks.org/computer-networks/introduction-of-message-queue-telemetry-transport-protocol-mqtt/. – Назва з екрана.
28. HiveMQ Data Sheet [Електронний ресурс] // HANNOVER MESSE. – Режим доступу: https://www.hannovermesse.de/apollo/hannover_messe_2023/obs/Binary/A1228930/HiveMQ-Data-Sheet.pdf. – Назва з екрана.
29. Introduction to DHT22 [Електронний ресурс] // The Engineering Projects. – Режим доступу: http://www.theengineeringprojects.com/2019/02/introduction-to-dht22.html. – Назва з екрана.
30. Sanjeev A. How to Interface Arduino and the MPU 6050 Sensor [Електронний ресурс] / Arvind Sanjeev // Maker Pro. – Режим доступу: https://maker.pro/arduino/tutorial/how-to-interface-arduino-and-the-mpu-6050-sensor. – Назва з екрана.

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ

IoT-система для запобігання аварій у промислових системах на основі аналізу сенсорних даних

Виконав: Бондаренко Сергій Юрійович
Керівник: Срібна Ірина Миколаївна

на здобуття освітнього ступеня магістра
зі спеціальності 126 Інформаційні системи та технології

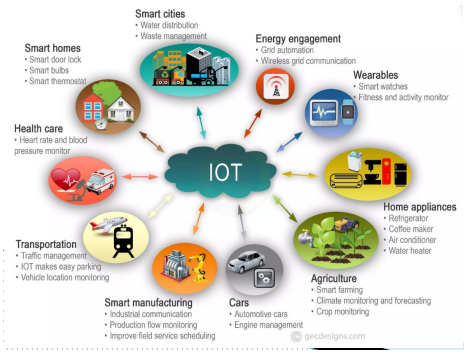
Київ-2025

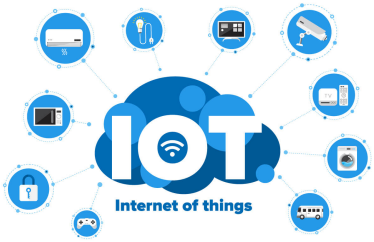
- **Об'єкт дослідження** – процес виявлення та запобігання аварій у промислових системах.
- **Предмет дослідження** – методи та алгоритми аналізу сенсорних даних.
- **Метою роботи** є розробка апаратного модуля та програмного забезпечення IoT-рішення для запобігання аварій у промислових системах із застосуванням аналізу сенсорних даних.

- *Актуальність теми.* Розвиток промисловості передбачає зростання потреби у сучасних заходах безпеки. З удосконаленням технологій Інтернет речей (IoT) став рушійною силою у підвищенні безпеки на робочому місці. Інтеграція IoT рішень дозволяє компаніям ефективніше управляти заходами безпеки. Ця тенденція простежується у різних секторах, від охорони здоров'я до виробництва. Через неї організації усвідомлюють, як потенціал IoT допомагає створити безпечніші робочі середовища. Традиційні методи безпеки включають паперову документацію, ручні перевірки та реактивні заходи у випадку появи інцидентів. Завдяки IoT ця динаміка змінюється, а безпека на робочому місці стає оперативною та динамічною системою а не статичним набором правил.

Інтернет речей

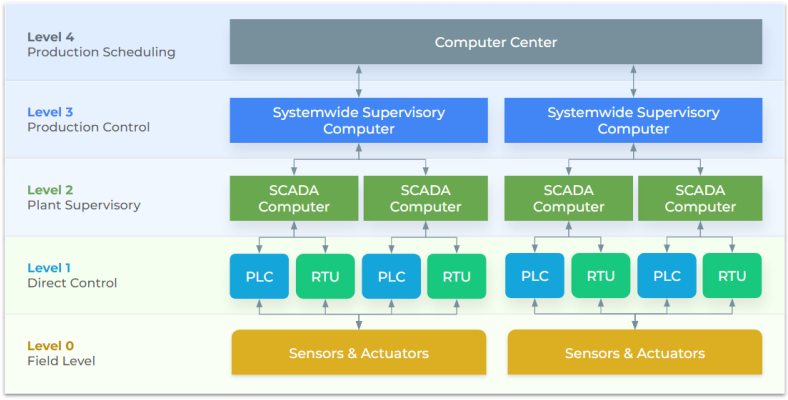
- Інтернет речей, або IoT, — це мережа взаємопов'язаних пристроїв, які підключаються та обмінюються даними з іншими пристроями IoT і хмарними сховищами. Пристрої IoT зазвичай оснащені технологіями, такими як датчики та програмне забезпечення, і можуть включати механічні та цифрові машини.
- Ці пристрої охоплюють все, від повсякденних побутових предметів до складних промислових інструментів. Все частіше організації в різних галузях використовують IoT для більш ефективної роботи, надання покращеного обслуговування клієнтів, вдосконаленого прийняття рішень та підвищення вартості бізнесу. За допомогою IoT дані можна передавати через мережу без необхідності взаємодії між людьми або між людиною та комп'ютером.





SCADA

- Диспетчерське управління і збір даних (Supervisory control and data acquisition, SCADA) — це архітектура, яка дозволяє промисловим організаціям відстежувати та керувати процесами, машинами та цехами.



SCADA

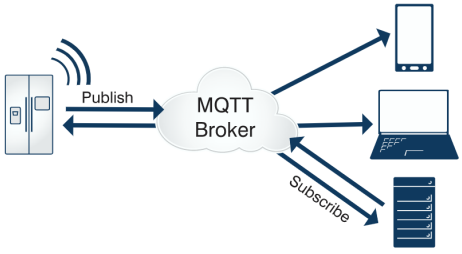
- Диспетчерське управління і збір даних (Supervisory control and data acquisition, SCADA) — це архітектура, яка дозволяє промисловим організаціям відстежувати та керувати процесами, машинами та цехами.
- Системи SCADA можуть використовуватися для моніторингу промислового обладнання, машин, систем або будівель, таких як електростанції. Цей процес може бути автоматичним або ініціюватися за допомогою команд оператора.

SCADA

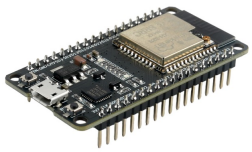
- Системи SCADA інтегруються з вимірювальними пристроями, такими як датчики, в інфраструктурі промислових і виробничих організацій. Вони збирають дані в аналоговій або цифровій формі, а потім надсилають їх до RTU або PLC, щоб їх можна було перетворити на корисну та придатну для використання інформацію. Потім ця інформація надсилається до HMI або інших дисплеїв, що дозволяє операторам аналізувати дані та взаємодіяти з ними.

MQTT

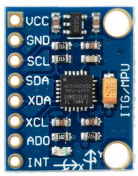
- MQTT — це протокол комунікації між машинами (M2M) для Інтернету речей, розроблений як легкий інструмент для публікації/підписки на повідомлення. MQTT корисний для з'єднань, де потрібна невелика кількість ресурсів аб пропускна здатність мережі є обмеженою. MQTT був створений доктором Енді Стенфорд-Кларком з IBI та Арленом Ніппером з Arcom у 1999 році. На той час IBM співпрацювала з нафтогазовою компанією, якій потрібно було отримувати дані з нафтопроводів віддалених районах, що вимагало нової протоколу, який би відповідав цим вимогам.



Вибір обладнання



Мікроконтролер



Датчик вібрацій

Датчик температури та вологості

Підключення датчиків

Інтерфейс з DHT22 досить простий, оскільки він використовує однопровідний протокол, тобто нам потрібно лише підключити його до одного GPIO мікроконтролера.
Він працює з напругою живлення в діапазоні від 3,3 В до 5,5 В, тому його можна легко використовувати з ESP32.
Помістимо датчик на макетну плату поруч з ESP32. Підключимо контакт VCC датчика до контакту 3,3 В ESP32, а заземлення — до заземлення. Підключимо контакт даних датчика до контакту 19 ESP32.
MPU6050 спілкується з ESP32 через протокол I2C, тому нам потрібно лише два дроти для з'єднання ESP32 і MPU6050. Контакти SCL і SDA MPU6050 підключені до контактів D22 і D21 ESP32, а контакти VCC і GND MPU6050 підключені до 3,3 В і GND ESP32.

Висновки

- Інтернет Речей має потенціал докорінно змінити сферу технічного обслуговування індустріальних машин з допомогою технологій предиктивного обслуговування та моніторингу стану.
- Можливість отримувати дані будь-де з великою швидкістю та дистанційно керувати технічним обладнанням у разі несправності робить технологію SCADA великим проривом у сфері запобігання аварій.