ДОДАТОК А

Графічний матеріал кваліфікаційної роботи

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ
КАФЕДРА ЕОМ

МЕТОДИ ТА МОДЕЛЬ ПІДВИЩЕННЯ НАДІЙНОСТІ ІНФРАСТРУКТУРИ ІНТЕРНЕТУ РЕЧЕЙ

КВАЛІФІКАЦІЙНА РОБОТА

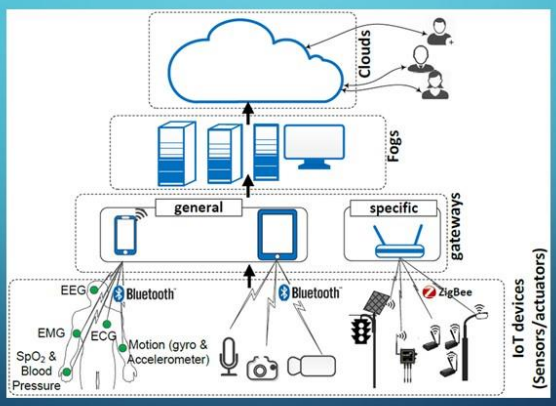
Виконав: ст. гр. СПм-23-5 Дяченко М.С.

Керівник: проф. Торба А.А.

МЕТА І ЗАДАЧІ РОБОТИ

- Мета: розробка та дослідження методів і моделі підвищення надійності інфраструктури IoT шляхом інтеграції засобів безпеки, резервування, самовідновлення та інтелектуального моніторингу.
- Задачі:
  - проаналізувати сучасний стан досліджень проблеми надійності IoT-систем;
  - систематизувати методи підвищення надійності з урахуванням особливостей IoT-інфраструктур;
  - запропонувати модель підвищення надійності на основі формальних математичних підходів;
  - реалізувати експериментальне дослідження моделі та оцінити ефективність запропонованих методів;
  - розробити практичні рекомендації щодо впровадження результатів у прикладних IoT-сценаріях.

СХЕМА ІНФРАСТРУКТУРИ IOT



3

ФОРМАЛІЗОВАНІ ВИМОГИ ДО НАДІЙНОСТІ IOT-СИСТЕМ

№	Вимога	Опис
1	MTTF (Mean Time to Failure)	Середній час безвідмовної роботи системи до першої відмови
2	MTTR (Mean Time to Repair)	Середній час, необхідний для відновлення після відмови
3	Availability (A = MTTF / (MTTF+MTTR))	Частка часу, у яку система працює коректно
4	Redundancy	Рівень дублювання апаратних чи програмних ресурсів
5	Resilience	Здатність до адаптації та відновлення при зовнішніх впливах

4

ПОРІВНЯННЯ МОДЕЛЕЙ ОЦІНЮВАННЯ НАДІЙНОСТІ IOT-СИСТЕМ

Модель / Метод	Ключові характеристики	Переваги	Обмеження
Марковські моделі	Станова модель з імовірнісними переходами	Чітка математична база; аналіз MTTF/MTTR	Не масштабуються для великих мереж
Стохастичні мережі Петрі (SPN)	Подання станів і подій у вигляді позицій і транзицій	Підтримка паралелізму; детальний аналіз	Потребує складного моделювання
Нечіткі мережі Петрі	Враховують невизначеність у параметрах системи	Підходить для адаптивного аналізу	Низька стандартизація; обмежена кількість інструментів
Reliability Block Diagram (RBD)	Блокова модель логічного з'єднання компонентів системи	Простота реалізації; візуалізація	Лише структурна модель; без урахування поведінкових змін
Цифрові двійники (Digital Twins)	Віртуальне віддзеркалення фізичних пристроїв IoT у реальному часі	Динамічна візуалізація; сценарії "що, якщо"	Висока складність впровадження; потреба в реальних даних
Моделі довіри та репутації	Обчислення показників на основі поведінки пристроїв і взаємодій	Врахування поведінкових характеристик; AI-адаптивність	Потребують даних для навчання; високий рівень обчислень
High-level Petri Nets (HLPN)	Моделювання конфліктів, правил і сценаріїв високого рівня у складних середовищах	Гнучкість у політиках; можливість формалізації сервісної логіки	Потребують спеціалізованих засобів розробки

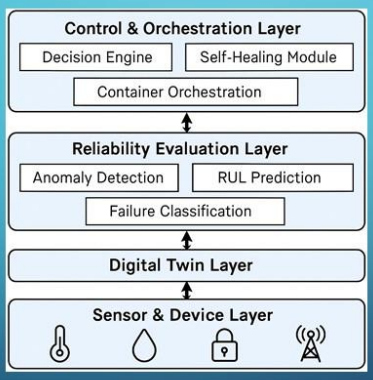
5

БЕЗПЕЧНІ ПРОТОКОЛИ ЗВ'ЯЗКУ

Протокол	Шар OSI	Характеристики	Захист
MQTT	Application	Легкий, push-based, для обмежених пристроїв	TLS, JWT, ACL
CoAP	Application	REST-подібний, UDP-базований	DTLS, OSCORE
LoRaWAN	MAC	Наддалека передача з низькою швидкістю	AES-128, Network/App Keys
HTTPS	Application	HTTP через TLS	Сертифікати, шифрування

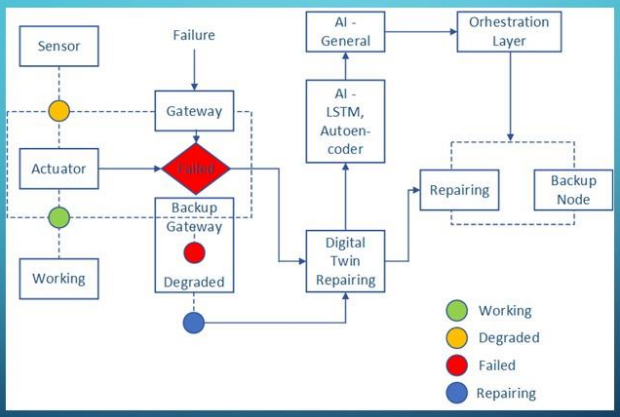
6

КОНЦЕПТУАЛЬНА МОДЕЛЬ R-SHIELD



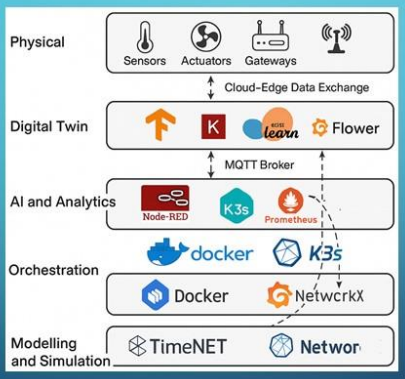
7

МОДЕЛЬ ІНФРАСТРУКТУРИ IOT



8

ПРОГРАМНІ ЗАСОБИ ДЛЯ ІНФРАСТРУКТУРИ IOT



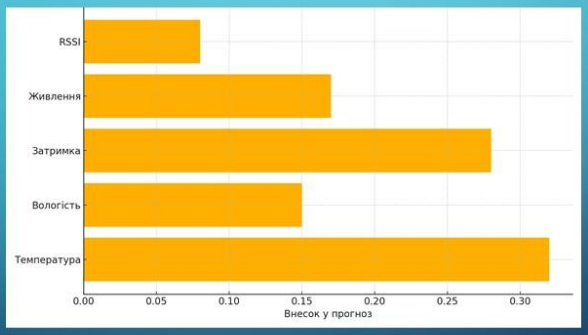
9

ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ

- Етап 1. Створення моделі віртуальної IoT-інфраструктури.
- Етап 2. Інтеграція машинного навчання.
- Етап 3. Формалізоване моделювання через SPN.
- Етап 4. Симуляція відмов і реакція системи.
- Етап 5. Реакція цифрових двійників та самооновлення.

10

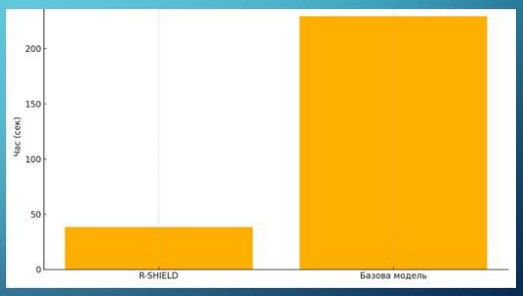
ДІАГРАМА ЗНАЧУЩОСТІ ПАРАМЕТРІВ ДЛЯ AUTOENCODER



11

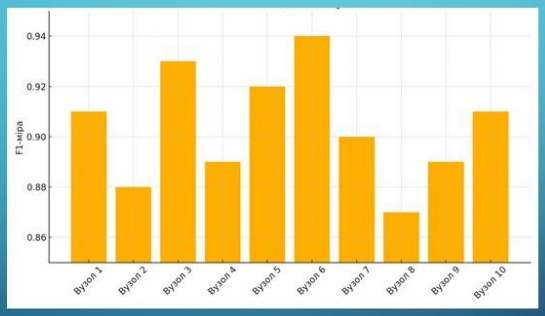
РЕЗУЛЬТАТИ ДЛЯ МОДЕЛІ R-SHIELD

Метрика	R SHIELD	Базова модель
MTTR, с	38,2	229,4
MTTF, с	17933	15100
Availability	0,978	0,938
Середній час реагування, с	6,7	44,1
Втрата даних під час інцидентів, %	0,8	5,4
F1-score для виявлення аномалій	0,92	–
Успішність перемикання на резерв, %	100	48



12

ТОЧНІСТЬ МОДЕЛІ ПО ВУЗЛАХ IOT

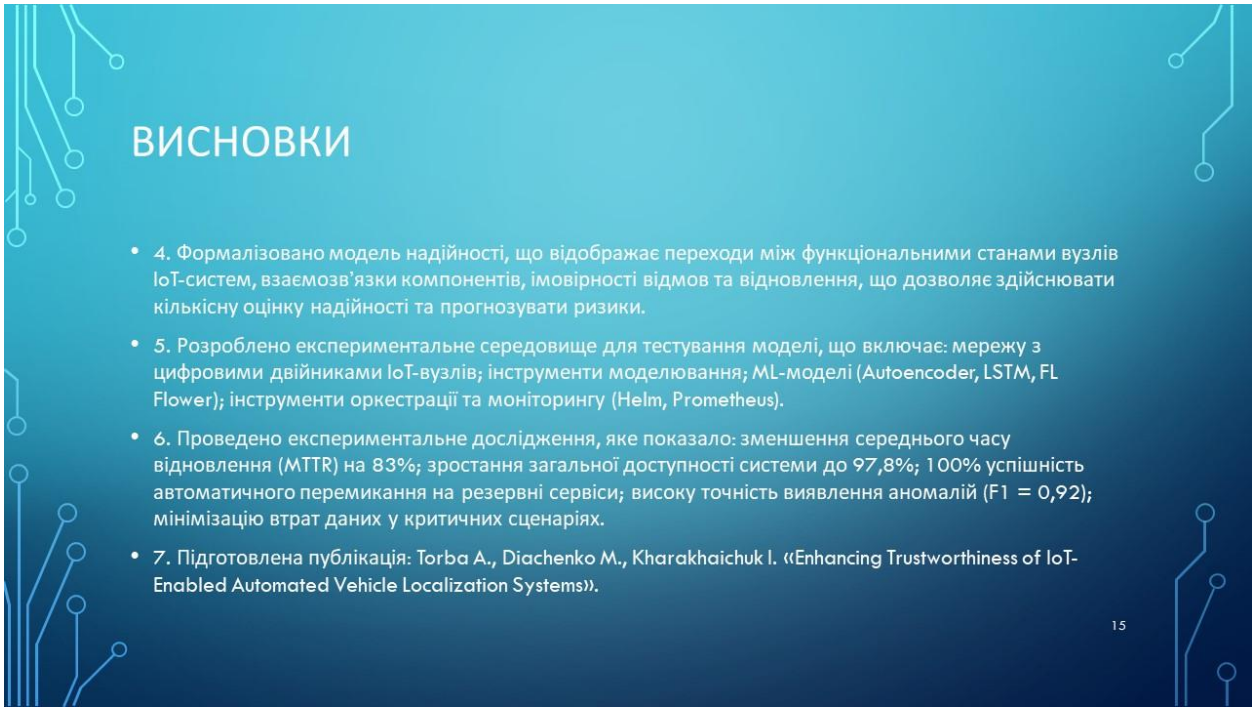


13

ВИСНОВКИ

- 1. Проаналізовано сучасний стан проблеми забезпечення надійності IoT-інфраструктури. Окреслено ключові виклики, вимоги до надійності, ризики та вразливості. Проведено порівняльний аналіз підходів: від класичних методів резервування до сучасних ML-базованих систем виявлення аномалій.
- 2. Сформульовано та систематизовано методи підвищення надійності, які охоплюють: безпеку як основу надійної роботи (криптографія, контроль доступу, захищені протоколи); відмовостійкість (контейнери, балансування, резервування); моніторинг та прогнозування збоїв; самоорганізацію та самовідновлення в IoT-мережах.
- 3. Запропоновано концептуальну модель підвищення надійності інфраструктури IoT R-SHIELD, яка є багаторівневою архітектурою з інтеграцією: цифрових двійників вузлів; машинного навчання для виявлення аномалій та прогнозування RUL; стохастичних мереж Петрі (SPN) як формального апарату для моделювання відмов та реконфігурації; графових моделей залежностей; технологій оркестрації та контейнеризації.

14


ВИСНОВКИ
• 4. Формалізовано модель надійності, що відображає переходи між функціональними станами вузлів IoT-систем, взаємозв'язки компонентів, імовірності відмов та відновлення, що дозволяє здійснювати кількісну оцінку надійності та прогнозувати ризики.
• 5. Розроблено експериментальне середовище для тестування моделі, що включає: мережу з цифровими двійниками IoT-вузлів; інструменти моделювання; ML-моделі (Autoencoder, LSTM, FL Flower); інструменти оркестрації та моніторингу (Helm, Prometheus).
• 6. Проведено експериментальне дослідження, яке показало: зменшення середнього часу відновлення (MTTR) на 83%; зростання загальної доступності системи до 97,8%; 100% успішність автоматичного перемикання на резервні сервіси; високу точність виявлення аномалій (F1 = 0,92); мінімізацію втрат даних у критичних сценаріях.
• 7. Підготовлена публікація: Torba A., Diachenko M., Kharakhaichuk I. «Enhancing Trustworthiness of IoT-Enabled Automated Vehicle Localization Systems».
15