

Хмельницький національний університет
Факультет інформаційних технологій
Кафедра комп'ютерної інженерії та інформаційних систем

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

Галузь знань 12 – Інформаційні технології

Спеціальність 123 – Комп'ютерна інженерія

на тему «Кіберфізична система виявлення дефектів медичних виробів»

КвРКІП.170164.21.16.05 ПЗ

Виконав: студент 2 курсу, група КІ2м-21-1


Керівник доктор техн. наук, професор
Науковий ступінь, вчене звання



Підпис

Дунець А.С.
Ініціали, прізвище

Яцків В.В.
Ініціали, прізвище

До захисту допускаю:
Зав. кафедри КІС, д.т.н., проф.
Т.О. Говорушенко
18 05 2023 р. 

Хмельницький, 2023

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

Освітній рівень МАГІСТР

Галузь знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Спеціальність 123 КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

Освітня програма ОСВІТНЬО-НАУКОВА ПРОГРАМА «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ ТА ПРОГРАМУВАННЯ»

ЗАТВЕРДЖУЮ

Зав. кафедри Т.О.Говорущенко

“ 01 ” 09 2022 р.

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ МАГІСТРА

Дунцо Артему Сергійовичу

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Кіберфізична система виявлення дефектів медичних виробів
Керівник проекту (роботи) Яцків В.В., д.т.н., професор

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 09.01.2023 р. № 1

2. Строк подання студентом проекту (роботи) на кафедру 01.05.2023 р.

3. Вихідні дані до проекту (роботи) Завдання на дипломне проектування

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити) _____

Аналіз відомих методів існуючих апаратних та програмних засобів, що використовуються в кіберфізичних системах виявлення дефектів медичних виробів





Моделювання процесу виявлення дефектів медичних виробів

Метод виявлення дефектів медичних виробів

Кіберфізична система виявлення дефектів медичних виробів

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень) _____

6. Консультанти розділів кваліфікаційної роботи магістра

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Лисенко С.М., професор кафедри КПС		
Антиплагіат	Нічепорук А.О., доцент кафедри КПС		

7. Дата видачі завдання « 06 » 09 2022р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) кваліфікаційної роботи магістра	Термін виконання етапів проекту (роботи)	Примітка
1	Вибір напрямку дослідження та узгодження тематики КвРМ з керівником	05.09.2022	ВИКОНАНО
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	05.10.2022	ВИКОНАНО
3	Робота над розділом 1 – аналіз відомих моделей, методів за темою; постановка задачі	05.11.2022	ВИКОНАНО
4	Робота над розділом 2 – розробка моделей для вирішення поставленої задачі	05.12.2022	ВИКОНАНО
5	Робота над науковою статтею	05.01.2023	ВИКОНАНО
6	Робота над розділом 3 – розробка методів для вирішення поставленої задачі	15.02.2022	ВИКОНАНО
7	Робота над розділом 4 – проектування та розробка ПЗ для вирішення поставленої задачі, експериментальна частина	05.04.2023	ВИКОНАНО
8	Оформлення пояснювальної записки згідно вимог	15.04.2023	ВИКОНАНО
9	Попередній захист ДРМ	18.04.2023	ВИКОНАНО
10	Захист ДРМ на засіданні ЕК	До 10.05.2023	

Студент

Керівник роботи


Підпис


Підпис

А.С. Дунець
Ініціали, прізвище

В.В. Яцків
Ініціали, прізвище

РЕФЕРАТ

Тема кваліфікаційної роботи магістра: Кіберфізична система виявлення дефектів медичних виробів

Автор роботи: Дунець А.С.

Керівник роботи: Яцків В.В.

Пояснювальна записка: 71 с., 6 рис., 2 табл., 2 дод., 80 джерел.

ПЕРЕЛІК КЛЮЧОВИХ СЛІВ: КІБЕРФІЗИЧНА СИСТЕМА, ДЕФЕКТИ, МЕДИЧНІ ВИРОБИ, ДАТЧИКИ.

Об'єктом дослідження є процес виявлення дефектів медичних виробів в режимі реального часу.

Предметом дослідження є кіберфізична система виявлення дефектів медичних виробів.

Метою кваліфікаційної роботи магістра є підвищення безпеки пацієнтів за рахунок виявлення та класифікація дефектів медичних виробів за допомогою кіберфізичної системи виявлення дефектів медичних виробів.

На основі проведених досліджень набув подальшого розвитку метод виявлення та класифікації дефектів медичних виробів за рахунок введених критеріїв, що характеризують ступінь ризику дефекту для пацієнта. Також набула подальшого розвитку архітектура кіберфізичної системи виявлення дефектів медичних виробів, в частині додавання підсистеми виявлення та аналізу дефектів.

Практична значимість отриманих результатів полягає у можливості забезпечення високої якості та безпеки медичного обладнання, покращенні точності та ефективності діагностики та лікування, зменшенні ризику для пацієнтів, економії ресурсів та часу медичного персоналу, а також відкритті нових можливостей для медичної діагностики та досліджень.

За результатами проведених досліджень подані тези на XVII міжнародну наукову конференцію «ОЛЬВІЙСЬКИЙ ФОРУМ-2023: СТРАТЕГІЇ КРАЇН ПРИЧОРНОМОРСЬКОГО РЕГІОНУ В ГЕОПОЛІТИЧНОМУ ПРОСТОРІ», СЕКЦІЯ КОМП'ЮТЕРНА ІНЖЕНЕРІЯ.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ	5
ВСТУП.....	6
1 АНАЛІЗ ВІДОМИХ РІШЕНЬ ДЛЯ ВИЯВЛЕННЯ ДЕФЕКТІВ МЕДИЧНИХ ВИРОБІВ	9
1.1 Аналіз існуючих підходів у використанні медичних кіберфізичних систем	9
1.2 Класифікація дефектів та несправностей медичних виробів	13
1.3 Огляд відомих кіберфізичних систем виявлення дефектів медичних виробів.....	18
1.4 Постановка задачі. Висновки	22
2 ВИЯВЛЕННЯ ДЕФЕКТІВ МЕДИЧНИХ ВИРОБІВ ЗА ДОПОМОГОЮ КІБЕРФІЗИЧНОЇ СИСТЕМИ.....	25
2.1 Моделювання процесу виявлення дефектів медичних виробів.....	25
2.2 Методи аналізу даних при використанні кіберфізичної системи виявлення дефектів медичних виробів	28
2.3 Метод виявлення та класифікації дефектів медичних виробів	35
2.4 Висновки.....	41
3 АРХІТЕКТУРА КІБЕРФІЗИЧНОЇ СИСТЕМИ ВИЯВЛЕННЯ ДЕФЕКТІВ МЕДИЧНИХ ВИРОБІВ	43
3.1 Проектування кіберфізичної системи виявлення дефектів медичних виробів.....	43
3.2 Виявлення дефектів медичних виробів за допомогою кіберфізичної системи	51
3.3 Результати аналізу даних про дефекти медичних виробів в кіберфізичній системі виявлення дефектів медичних виробів	55

3.4 Висновки.....	59
4 КІБЕРФІЗИЧНА СИСТЕМА ВІЯВЛЕННЯ ДЕФЕКТІВ МЕДИЧНИХ ВИРОБІВ.....	60
4.1 Розроблення кіберфізичної системи виявлення дефектів медичних виробів	60
4.2 Функціонування кіберфізичної системи виявлення дефектів медичних виробів.....	70
4.3 Висновки	75
ВИСНОВКИ	77
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ	78
ДОДАТОК А Копія тез	87
ДОДАТОК Б Презентація	91

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

БД - база даних

БПР - блок прийняття рішень

КФС – кіберфізична система

ПЗ - програмне забезпечення

FMEA - Failure Mode Analysis (аналіз видів і наслідків відмов)

FTA – Fault Tree Analysis (аналіз дерева відмов)

ВСТУП

Успіхи в обчислювальній техніці, мережах і сенсорних технологіях призвели до повсюдного розгортання кіберфізичних систем у критично важливих для безпеки середовищах, таких як аерокосмічна сфера, енергетика, транспорт і охорона здоров'я. Зокрема, існує значне розгортання медичних кіберфізичних систем у різних клінічних та персоналізованих умовах, починаючи від крихітних кардіостимуляторів і дефібриляторів, які можна імплантувати, до переносних пристроїв моніторингу стану здоров'я, складних моніторів пацієнтів у відділеннях інтенсивної терапії і дорогих систем для променевої терапії та роботизованої хірургії.

Зростання складності медичних систем, тісний зв'язок між їхніми кібернетичними та фізичними компонентами, а також неминуче залучення людей-операторів до нагляду та контролю призвели до серйозних проблем із забезпеченням надійності та безпеки системи. Наприклад, в США протягом останніх п'яти років до управління з контролю за продуктами й ліками надійшли повідомлення про понад 6,8 тисячі відкликань медичних виробів і 2,4 мільйона побічних подій (це включаючи 923 тисячі травм і 49 тисяч смертей). Майже 24% відкликань було спричинено пов'язаними з комп'ютером збоями в програмному та апаратному забезпеченні, батареях або системних інтерфейсах, які вплинули на понад 18 мільйонів медичних пристроїв на ринку, несучи від середнього до високого ризику серйозних наслідків для здоров'я пацієнтів і значних витрат для виробників і осіб, які доглядають за ними [1 – 3].

Незважаючи на те, що найсучасніші медичні системи часто розроблені з механізмами безпеки, які намагаються виявити збої та перевести систему в безпечний стан, на практиці вони мають обмежені можливості виявлення в реальному часі та автоматичного відновлення після загроз безпеці. Багато медичних пристроїв відкликано через проєктні потоки, у яких відсутній комплексний аналіз небезпеки та оцінка ризику, або через використання механізмів безпеки, які не були ретельно перевірені на стійкість. Механізми

відновлення часто обмежуються рекомендаціями щодо ручних дій, які повинні виконуватися операторами пристроїв, або дорогим ремонтом чи заміною пристроїв виробниками [2].

Актуальність роботи полягає в розробці кіберфізичної системи виявлення дефектів медичних приладів, яка дозволяють підвищити безпеку пацієнтів, внаслідок виявлення потенційних дефектів або несправностей в медичних приладах на ранніх стадіях. Це дозволяє запобігати можливим небезпекам та забезпечує безпеку пацієнтів. Також такі системи покращують якість медичних послуг завдяки вчасному виявленню дефектів у медичних приладах, що допомагає уникнути збоїв у їхній роботі та забезпечує належну функціональність.

Метою кваліфікаційної роботи магістра є виявлення та класифікація дефектів медичних приладів за допомогою кіберфізичної системи виявлення дефектів медичних приладів.

Для досягнення поставленої мети необхідно розв'язати такі основні задачі:

- 1) провести аналіз існуючих апаратних та програмних засобів, що використовуються в кіберфізичних системах виявлення дефектів медичних приладів;
- 2) провести огляд існуючих моделей та методів виявлення дефектів медичних приладів;
- 3) розробити метод виявлення дефектів медичних приладів кіберфізичною системою;
- 4) запропонувати архітектуру кіберфізичної системи виявлення дефектів медичних приладів.

Об'єктом дослідження є процес виявлення дефектів медичних приладів в режимі реального часу.

Предметом дослідження є кіберфізична система виявлення дефектів медичних приладів.

1. Набув подальшого розвитку метод виявлення та класифікації дефектів медичних приладів за рахунок введених критеріїв, що характеризують ступінь ризику дефекту для пацієнта.

2. Набула подальшого розвитку архітектура кіберфізичної системи виявлення дефектів медичних приладів, в частині додавання підсистеми виявлення та аналізу дефектів.

Практична цінність отриманих результатів у можливості підвищення якості та безпеки медичного обладнання, зменшенні ризику для пацієнтів, економії ресурсів та часу медичного персоналу.

За результатами проведених досліджень подані тези на XVII міжнародну наукову конференцію «ОЛЬВІЙСЬКИЙ ФОРУМ-2023: СТРАТЕГІЇ КРАЇН ПРИЧОРНОМОРСЬКОГО РЕГІОНУ В ГЕОПОЛІТИЧНОМУ ПРОСТОРІ», СЕКЦІЯ КОМП'ЮТЕРНА ІНЖЕНЕРІЯ.

1 АНАЛІЗ ВІДОМИХ РІШЕНЬ ДЛЯ ВИЯВЛЕННЯ ДЕФЕКТІВ МЕДИЧНИХ ВИРОБІВ

1.1 Аналіз існуючих підходів у використанні медичних кіберфізичних систем

На сьогоднішній день для виявлення дефектів медичних пристроїв і приладів використовуються різні методи і технології. Розглянемо декілька з них:

1. Візуальний огляд і перевірка функціональності. Цей метод є одним з найбільш поширених для виявлення дефектів медичних пристроїв. При цьому оглядач перевіряє пристрій на наявність видимих дефектів, таких як тріщини, розірвання, знос, корозію і т.д. Прилад також перевіряється на наявність функціональних дефектів, таких як нерівномірна робота, несправність кнопок, показників тощо.

2. Електричні вимірювання. Цей метод зрозуміло використовується для виявлення електричних дефектів. При цьому пристрій підключається до вимірювального приладу, який перевіряє роботу кожного елемента в пристрої, щоб визначити наявність електричних дефектів.

3. Рентгенівська томографія. Вона використовується для виявлення дефектів внутрішньої структури медичних пристроїв. При цьому пристрій піддається рентгенівському випромінюванню, а отримані зображення аналізуються на наявність дефектів, таких як тріщини, розірвання, знос тощо.

4. Акустичні вимірювання. Цей метод використовується для виявлення дефектів, пов'язаних з звуком. При цьому використовується спеціальний вимірювальний прилад, який використовує високочастотні звукові хвилі для дослідження внутрішньої структури медичного пристрою.

5. Інфрачервона термографія. При застосуванні цього методу вимірюється температура медичних пристроїв, щоб виявити наявність дефектів. Наприклад, якщо температура на деяких ділянках пристрою є нерівномірною, це може бути ознакою наявності дефектів в медичному приладі.

6. *Non destructive testing*. Цей метод використовується для виявлення дефектів медичних пристроїв, які не можуть бути виявлені за допомогою візуального огляду. Це може бути випробуванням пристрою на міцність, довговічність і т.д. за допомогою спеціального обладнання. Наприклад, пристрій може бути підданий випробуванням на згинання, розтягування, стиснення, щоб виявити його міцність і стійкість.

7. Вібраційні вимірювання. Використовуються для виявлення дефектів, пов'язаних з вібраціями. Якщо пристрій нестійкий під час роботи і видає зайві вібрації, це може бути ознакою наявності дефектів.

8. Фотоелектричні вимірювання. Використовується для виявлення дефектів, пов'язаних з оптикою і світлом. При цьому пристрій піддається світловому випромінюванню, а спеціальний фотодатчик перевіряє роботу кожного елемента в пристрої, щоб визначити наявність дефектів.

Слід зазначити, що ці методи і технології можуть використовуватися як окремо так і в поєднанні між собою для виявлення дефектів медичних приладів та пристроїв.

Медичний прилад та медичний пристрій – це дві різні назви для того ж самого об'єкта, який використовується для медичних досліджень, діагностики, лікування або контролю за станом пацієнтів.

Термін «медичний прилад» частіше використовується в контексті менших портативних пристроїв, таких як термометри, тонометри, глюкометри тощо, а також більш великих пристроїв, таких як рентгенапарати та УЗД-сканери.

Термін «медичний пристрій» частіше використовується в контексті більш складних систем, які можуть містити кілька компонентів та функцій, таких як комп'ютерні томографи, електрокардіографи, системи штучної вентиляції легенів та інші.

Взагалі кажучи, терміни «медичний прилад» та «медичний пристрій» використовуються взаємозамінно та можуть описувати будь-яке медичне обладнання, яке використовується для медичної діагностики, лікування або контролю за станом пацієнтів.

Медичні кіберфізичні системи містять взаємопов'язані електронні компоненти та модулі програмного забезпечення, які взаємодіють із механічними/фізичними компонентами, декількома операторами та пацієнтами за суворих часових обмежень. В умовах різноманітності внутрішніх і зовнішніх збурень і змін у динаміці пацієнтів і навколишнього середовища комплексна оцінка безпеки системи в цілому є складним завданням.

Стандартні методи аналізу небезпеки та оцінки безпеки, рекомендовані та застосовувані виробниками медичних пристроїв (наприклад, аналіз дерева відмов (FTA) [6] та аналіз режиму та наслідків відмови (FMEA) [7]), зосереджені насамперед на відмовах окремих компонентів або людські помилки в системі. Інші важливі фактори, які сприяють безпеці системи, такі як складні помилки програмного забезпечення, небезпечні взаємодії компонентів і контекстуальні фактори (стани системи та умови, за яких виконуються дії), часто не враховуються ретельно під час типового аналізу небезпек [6, 7]. Таким чином, багато інцидентів виникають через те, що загрози безпеці та вразливі місця не були виявлені та усунені під час процесу проектування, або через те, що стійкість механізмів виявлення та пом'якшення не підтверджена належним чином. Крім того, зі збільшенням розміру та складності програмного забезпечення, навіть якщо використовуються найсуворіші процеси аналізу ризиків і перевірки, деякі залишкові збої проявляються як непередбачувані небезпеки під час роботи пристрою.

Хоча медичні системи часто оснащені механізмами безпеки, які виявляють збої та переводять систему в безпечний стан, на практиці своєчасне виявлення та ефективно пом'якшення загроз безпеці (спричинених випадковими збоями або зловмисними атаками) є дуже складним завданням. Це пояснюється складним характером інцидентів, складністю точного моделювання причинно-наслідкових зв'язків і невизначеністю в діях оператора та стані здоров'я пацієнта.

Зменшення загроз безпеці вимагає завчасного виявлення несприятливих наслідків команд і розуміння семантики взаємодії між операторами, кібернетичними та фізичними компонентами на різних рівнях системи.

Існуючі механізми виявлення та відновлення розроблені в основному на основі включення перевірок надмірності та узгодженості або моніторингу програмного забезпечення та фізичних компонентів системи окремо один від одного. Взаємодія між операторами, програмними модулями та фізичними компонентами, динаміка фізичної системи та стан пацієнта часто не враховуються при розробці цих механізмів, здебільшого через обмеження вартості та реального часу.

Наприклад, управління з контролю за продуктами й ліками США (FDA) регулює медичні пристрої, що продаються в Сполучених Штатах, вимагаючи від виробників дотримання низки регуляторних заходів до та після виходу на ринок. FDA класифікує медичні пристрої за 5853 різними типами та 19 медичними спеціальностями, такими як анестезіологія, серцево-судинні захворювання, клінічна хімія, загальні лікарні, загальна хірургія та радіологія, із зазначенням їх нормативного класу та маркетингових вимог [8]. Усі пристрої мають відповідати загальним вимогам контролю, таким як реєстрація, перелік, система якості та маркування, але класи пристроїв потребують додаткового спеціального контролю.

Такі пристрої, як зарядні пристрої для кардіостимуляторів, ліжка для пацієнтів або крісла, які не становлять дуже серйозного ризику для здоров'я пацієнтів, звільняються від спеціального регуляторного контролю. Більшість пристроїв із середнім рівнем ризику, таких як монітори пацієнта, роботизовані пристрої та діагностичне програмне забезпечення вимагають спеціального набору засобів контролю, включаючи подання передпродажного повідомлення 510(k) до FDA. Попереднє сповіщення 510(k) має продемонструвати, що пристрій, по суті, еквівалентний пристрою, який законно комерційно розповсюджується в Сполучених Штатах. Такі пристрої, як кардіостимулятори, обладнання для променевої терапії та інфузійні насоси, які становлять значний ризик захворювання або травмування пацієнтів, повинні пройти процес попереднього схвалення, під час якого претензії щодо їх функціональності мають підтверджуватися поданням клінічних даних [12]. Після того, як медичний пристрій розповсюджується на ринку, FDA збирає та відстежує звіти про

несприятливі події та інші проблеми з пристроями, а також попереджає медичних працівників і громадськість шляхом відкликання або сповіщень про безпеку, щоб забезпечити належне використання пристроїв і пацієнтів.

В Україні вимоги до медичних виробів (пристроїв, приладів) складені на основі Керівного документу Європейської Комісії MEDDEV 2.4/1, редакція 9, та не є юридично обов'язковими, а також наказу міністерства охорони здоров'я від 22.01.2020 № 142 [4]. Можливе відступлення від правил класифікації в рамках технічного прогресу або інформації, отриманої після виходу виробу на ринок.

Дані про відкликання медичних приладів і побічні ефекти медичних приладів дають цінну інформацію про минулі несправності медичних приладів і про те, як їх розробку можна було б покращити в майбутньому. Однак автоматичний аналіз цих звітів є складним завданням, яке потребує семантики інтерпретація тексту природною мовою та врахування всіх потенційних причин і контекстуальних факторів, включаючи несправні компоненти, людські помилки та стани системи.

Враховуючи, що Україна не веде базу стосовно наявних несправностей медичних приладів, для проведення дослідження скористаємось загальнодоступною базою даних під назвою «База даних, що містить доклади клініцистів про виникнені ускладнення, що пов'язані з медичними процедурами» (MAUDE).

В ній містяться добровільно надані звіти починаючи з червня 1993 року, відгуки пацієнтів (починаючи з 1991 року), звіти дистриб'юторів (починаючи з 1996 року), а також звіти виробників (починаючи з 1996 року). Дана база є доступною для загального користування [9].

1.2 Класифікація дефектів та несправностей медичних виробів

В загальному існують декілька класифікацій дефектів, несправностей та видів збоїв медичних приладів [3, 4]. На нашу думку, загалом, найкраще

класифікувати відкликання приладів за трьома класами спираючись на відносний ступень небезпеки для здоров'я, який представляє прилад. Розглянемо цю класифікацію. Пропонується дефекти та несправності за цією ознакою ділити на три класи.

Дефект класу I свідчить про достатню ймовірність того, що використання приладу спричинить серйозні несприятливі проблеми зі здоров'ям або смерть. Прикладами дефектів та несправностей приладів цього класу є дефібрилятори/монітори, апарати для наркозу та системи доставки ліків.

Дефекти класу II вказують на прилади, які можуть спричинити тимчасові або оборотні несприятливі наслідки для здоров'я або створювати віддалену ймовірність серйозних проблем зі здоров'ям. Монітори рівня глюкози та багатопараметричні монітори пацієнта є прикладами приладів, відкликаних у цьому класі.

Клас III вказує на прилади, які порушують закони FDA, але, ймовірно, не спричинять негативних наслідків для здоров'я, наприклад програматори для пацієнтів і програмне забезпечення ультразвукової системи.

Кожен запис, поданий до бази даних відкликаних FDA, містить структуровану інформацію, таку як унікальний номер відкликання; клас відкликання; дата публікації в FDA, а також неструктуровані описи, що описують назву продукту (тобто назву пристрою та опис його функціональних можливостей), фірму/виробника, що відкликає, кількість у продажу (тобто кількість пристроїв, що розповсюджуються на ринку), і важливі інформацію про питання безпеки пристрою та причину відкликання.

Згідно Закону України від 28.03.2013 № 2648 Стаття 5. Класифікація медичних виробів, медичні вироби поділяються на наступні класи: I, IIa, IIb та III. Розподіл медичних виробів за такими класами зумовлений вразливістю людського організму, при застосуванні або впливі медичного виробу, з урахуванням потенційних ризиків, що пов'язані з розробленням, виготовленням та впровадженням таких виробів. Слід зазначити, що в українському законодавстві, що стосується медичних виробів, медичним виробом вважаються –

апаратура, інструменти, різноманітні пристрої та прилади, в тому числі програмне забезпечення, матеріали, будь-які вироби, включаючи інвазивні. А також вироби, які можна використовувати як окремо так і з різними комплектуючими, які необхідні для правильного використання, враховуючи програмне забезпечення цих виробів. Слід зазначити, що згідно визначень описаних у Законі, класифікацію медичних виробів покладено на виробника [3, 4].

Враховуючи, що в Україні немає загальної бази, яка містить єдиний перелік всіх дефектів та несправностей виявлених в процесі експлуатації медичних приладів, для проведення нашого дослідження скористаємось відомостями наявними в загальнодоступній базі MAUDE.

База даних MAUDE – це загальнодоступна колекція звітів про ймовірні побічні ефекти, пов'язані з медичними пристроями, які обов'язково (користувачі, виробники та дистриб'ютори) і добровільно (медичні працівники, пацієнти та клієнти) звітують до FDA. Правила FDA вимагають від фірм, які отримують скарги, повідомляти FDA про випадки, пов'язані з використанням медичних пристроїв, у тому числі про несправності пристроїв, серйозні травми та смерті, пов'язані з пристроями. Не всі зареєстровані побічні ефекти призводять до відкликання; виробники та FDA регулярно відстежують несприятливі події, щоб вчасно виявити та усунути проблеми.

Класифікація дефектів та несправностей медичних приладів може відрізнитися залежно від конкретного приладу, його призначення та специфікацій. Однак, загалом, можна виділити наступні типи дефектів та несправностей медичних приладів:

1. Механічні пошкодження: це може бути пошкодження елементів конструкції медичного приладу, наприклад, тріщини на корпусі, зімкнення контактів, зношеність деталей тощо.

2. Електричні несправності: це може бути пов'язано з проблемами живлення, зімкненням проводів, перебоїв в електромережі, несправністю електронних компонентів тощо.

3. Програмні несправності: це може бути пов'язано з помилками в програмному забезпеченні медичного приладу, невірними налаштуваннями, багами тощо.

4. Несправності, пов'язані з сенсорами: це може бути пов'язано зі збоєм в роботі датчиків, їхньою некоректною калібруванням, перевантаженням тощо.

5. Несправності, пов'язані зі зносом та експлуатаційними проблемами: це може бути пов'язано зі зносом деталей приладу, необхідністю заміни деяких компонентів, неякісним збором приладу, технічними несправностями тощо.

Класифікація дефектів та несправностей медичних приладів може допомогти відрізнити різні причини несправностей та забезпечити ефективне їхнє виявлення та усунення. Це дозволяє підвищити безпеку пацієнтів та забезпечити надійну та ефективну роботу медичних приладів.

Для того, щоб дослідити виникнення дефектів та несправностей, що виникають при експлуатації медичних приладів, спочатку було проаналізовано написані людьми описи відкликаних і звітів про побічні події, отримані з баз даних FDA. Будемо визначати пов'язану з комп'ютером несправність як будь-яку подію, яка спричиняє неправильне функціонування комп'ютерного медичного приладу або завдає шкоди пацієнтам/користувачам через збої в будь-якому з наступних компонентів пристрою: програмне забезпечення, апаратне забезпечення, введення/виведення або акумулятор. Інші несправності комп'ютерних пристроїв, які не можна легко віднести до цих чотирьох класів, класифікуються в іншій категорії. Описані комп'ютерні збої можна класифікувати наступним чином: на основі класу несправності, режиму відмови, категорії дій відновлення, кількості відкликаних приладів та категорії приладу. Розглянемо їх більш детально:

1. Клас несправності – дефектні компоненти, які призвели до поломки або виходу з ладу приладу.
2. Режим відмови – вплив збоїв на безпечне функціонування приладу.
3. Категорія дії відновлення – тип дій, які виробник вжив для вирішення проблеми відкликання.

4. Кількість відкликаних приладів – кількість відкликаних приладів, розповсюджених на ринку.

5. Категорія приладу – категорії та типи відкликаних приладів.

В даній роботі використовувалась загальна кількість пристроїв, на які впливає кожне відкликання, як показник для вимірювання впливу збоїв. Слід звернути увагу на критично важливих для безпеки відкликаннях, які включають:

1. Відкликання, класифіковане FDA як клас I, представляє високу ймовірність серйозних травм або смерті пацієнтів.

2. Відкликання, для яких у полі «Причина відкликання» конкретно зазначено проблему безпеки пацієнта, наприклад травму або смерть.

3. Відкликання, для яких у полі «Причина відкликання» чітко вказано потенціал викриття пацієнтів/користувачів до негайної «фізичної загрози безпеці», такої як «передозування», «надмірне опромінення», «ураження електричним струмом», «опік» і «пожежа».

Критичні для безпеки відкликання були використані як основа для пошуку категорій і типів критично важливих для безпеки медичних пристроїв, збоїв в яких, швидше за все, призведуть до критичних для життя наслідків для пацієнтів. Аналіз повідомлень про несприятливі події дозволяє виміряти вплив несправностей пристрою з точки зору фактичних несприятливих наслідків (наприклад, серйозних травм або смерті), про які повідомляється FDA.

Нарешті, ґрунтуючись на конкретних питаннях безпеки, визначених для життєво важливих медичних пристроїв, необхідно вирішувати проблеми, пов'язані з розробкою медичних пристроїв нового покоління.

В таблиці 1.1 наведені приклади дефектів медичних виробів пов'язаних із комп'ютером.

Таблиця 1.1 – Приклади дефектів медичних виробів, пов'язаних із комп'ютером

Вид дефекту	Клас дефекту	Проблема	Опис	Наслідок дефекту/ режим відмови
Програмне забезпечення	II	Виріб має проблеми з програмним інтерфейсом	При підключенні до основної системи це не дозволить системі розпізнати прилад нефункціональним на всіх сайтах	Збій в роботі пристрою
Апаратне забезпечення	I	Нездатність приладу здійснити шоківий імпульс (розряд)	Несправний конденсатор може спричинити затримку або відсутність розряду дефібрилятора, що може призвести до неможливості реанімації пацієнта	Переривання лікування/ невдача терапії
Інше	I	Пристрій вмикається, а потім вмикається самостійно або не вмикається	Пристрій або сам вмикається або вмикає оператор, або пристрій не вмикається зовсім	Збій в роботі пристрою
Батарея	I	Ненавмисне перезавантаження	Насос демонструє періодичну втрату живлення через періодичну втрату контакту між чашкою та контейнером акумулятора, що призводить до скидання пристрою	Переривання лікування/ невдача терапії
Вхід/вихід	II	Динаміки на моніторі пацієнта вийшли з ладу	Відсутність звукової сигналізації та затримка лікування пацієнта	Помилка повідомлення тривоги

1.3 Огляд відомих кіберфізичних систем виявлення дефектів медичних виробів

Кіберфізичні системи виявлення дефектів медичних виробів є важливим інструментом для забезпечення безпеки пацієнтів та ефективної роботи медичного обладнання. Вони поєднують в собі технології програмного

забезпечення та апаратного забезпечення з метою виявлення дефектів та моніторингу роботи медичних пристроїв.

Основна мета кіберфізичних систем виявлення дефектів медичних приладів полягає в тому, щоб забезпечити надійність та безпеку роботи медичного обладнання. Вони дозволяють виявляти неполадки та дефекти медичних приладів, які можуть призвести до неправильної діагностики та лікування, зниження якості медичної допомоги та можуть стати причиною травм та інших небезпек для пацієнтів та медичного персоналу.

Крім того, кіберфізичні системи виявлення дефектів медичних приладів дозволяють зменшити час, необхідний для виявлення та усунення дефектів, що дозволяє забезпечити швидке та ефективне лікування пацієнтів. Вони також допомагають зменшити ризик виникнення дефектів медичних приладів шляхом моніторингу їх роботи та вчасного виявлення неполадок.

Отже, кіберфізичні системи виявлення дефектів медичних приладів є важливим інструментом для забезпечення безпеки пацієнтів та ефективної роботи медичного обладнання. Вони дозволяють виявляти та усувати дефекти медичних приладів, що забезпечує безпечне та ефективне лікування пацієнтів.

Нижче наведено огляд деяких відомих кіберфізичних систем виявлення дефектів медичних приладів.

В роботі [15] автори запропонували підхід та система, який використовується для виявлення дефектів медичних приладів. System for Prediction and Identification of Defects (SPID) – це система, яка використовує нейромережеві алгоритми для виявлення дефектів в медичних приладах. Система збирає дані про роботу приладу та використовує їх для навчання моделі, яка може прогнозувати вірогідність виникнення дефектів та несправностей. SPID використовується в багатьох лікарнях та медичних центрах. Недоліком є те, що ця система потребує достатньо великих обсягів даних для навчання моделі, що у випадку дефектів рідкісних медичних приладів може бути проблемою.

Автори [16] запропонували підхід, з використанням якого розроблена система eXtended IoT Platform for Healthcare (XIP-H). Це система, яка поєднує в

собі різноманітні датчики та моніторингові пристрої для збору даних про роботу медичних приладів. Дані збираються та аналізуються в режимі реального часу, що дозволяє виявляти дефекти та несправності майже миттєво. ХІР-Н також має вбудований інтерфейс користувача, який дозволяє медичному персоналу відслідковувати стан медичного приладу та приймати рішення щодо його утримання. Недоліком може бути те, що ця система потребує встановлення долаткових медичних датчиків та моніторингових приладів, що може бути складним при використанні застарілих медичних приладів.

В роботі [17] використовується штучний інтелект для аналізу даних про роботу медичних приладів та виявлення дефектів та несправностей. Розроблена на основі цього підходу кіберфізична система Medical Device Safety System забезпечує автоматичне виявлення та повідомлення про дефекти, що дозволяє медичному персоналу швидко приймати рішення щодо їх усунення. Система також забезпечує збереження даних про стан медичного приладу та його ремонт.

Автори [18] пропонують Health Monitoring System for Medical Devices (HMS-MD) – це система, яка використовує бездротові мережі та різноманітні датчики для збору даних про роботу медичних приладів.

Система MMS (Medical Monitoring System) відслідковує функціональні параметри медичних приладів, такі як пульс, тиск, температура, та надсилає повідомлення адміністратору, якщо якість даних не задовільна або пристрій потребує ремонту [19].

MMDAS (Medical Device Detection and Analysis System) – ця система використовує методи машинного навчання для виявлення аномальної поведінки медичних приладів. Вона визначає нормальні шаблони поведінки приладу та сповіщає адміністратора, якщо з'являються відхилення [20].

MIPAS (Medical Instrument Performance Analysis System) – ця система відстежує ефективність медичних приладів, вимірює їх точність та надійність та генерує звіти про їх стан [21].

MDCS (Medical Device Control System) – ця система забезпечує контроль за доступом до медичних приладів та їх належним використанням, дозволяючи

адміністраторам встановлювати різні рівні доступу до різних функцій приладу та вимагати від користувачів дотримання встановлених правил [22].

Кіберфізична система «SoftWear» – ця система використовує навчальні моделі машинного навчання для розпізнавання та виявлення дефектів в електронних компонентах медичних приладів. Вона працює на основі аналізу електричних сигналів, що генеруються приладами, та забезпечує високу точність виявлення дефектів [23].

Кіберфізична система «MediScan» – ця система використовує технології машинного навчання та обробки зображень для виявлення дефектів медичних приладів, що використовуються в медичних зображеннях, наприклад, в рентгенівських апаратах. Вона може автоматично виявляти дефекти, такі як дірки, плями або шум, та допомагати операторам знизити кількість недостовірних діагнозів [24].

Кіберфізична система «MedMon» – ця система використовує технології IoT (Internet of Things) для моніторингу та виявлення дефектів медичних приладів у реальному часі. Вона може забезпечити віддалений моніторинг роботи приладів та повідомляти про будь-які несправності або дефекти [25].

Кіберфізична система «HealthWatch» – ця система використовує навчальні моделі машинного навчання для виявлення дефектів медичних пристроїв, що використовуються для моніторингу стану пацієнтів, наприклад, пристроїв для вимірювання пульсу або тиску. Вона може виявляти різні типи дефектів, такі як неправильні вимірювання, зламані екрани або несправні сенсори [26].

«Proactive Detection» – ця система від компанії "Baxter" розроблена для виявлення дефектів в інфузійних помпах. Вона включає сенсори, які зчитують дані щодо роботи насоса і передають їх до хмарного сховища даних, де аналізуються за допомогою алгоритмів машинного навчання. Ці алгоритми здатні виявляти незначні зміни у поведінці насоса, які можуть вказувати на наявність дефектів, наприклад, засмічення трубок або зменшення потужності насоса [27].

Компанія «Royal Philips» [28], розробила та представила систему «HealthPAS», яка виявляє дефекти в медичних приладах за допомогою датчиків і

алгоритмів аналізу даних. Вона дозволяє виявляти дефекти в режимі реального часу, що дозволяє швидко реагувати на них і забезпечувати безпеку пацієнтів. Система HealthPAS може бути використана для виявлення дефектів в різних медичних приладах, таких як монітори пацієнта, електрокардіографи, інфузійні помпи та інші.

«Virtual Medical Assistant» – це система, розроблена компанією "IBM", яка використовує штучний інтелект для виявлення дефектів в медичних приладах та забезпечення їх підтримки. Система може взаємодіяти зі співробітниками служби технічної підтримки за допомогою текстових повідомлень або голосових інтерфейсів. Вона також може надавати підтримку пацієнтам, допомагаючи їм користуватися медичними приладами [29].

Sysmex XN-Series Hematology Analyzers – ці системи використовуються для автоматизованого аналізу крові, що дозволяє виявляти дефекти в роботі аналізаторів, такі як помилки при нанесенні зразка крові, неправильні результати аналізу та інші проблеми. Система відстежує якість аналізу та сповіщає оператора про будь-які виявлені дефекти [30].

Кіберфізична система Welch Allyn Spot Vital Signs Monitor – це портативний прилад, що вимірює основні показники здоров'я, такі як артеріальний тиск, пульс, температуру тіла та інші. Система має вбудований алгоритм для виявлення дефектів у вимірюваннях, таких як помилки при надходженні даних від сенсорів, помилки у розрахунках та інші [31].

Також на сьогоднішній день широкого поширення набуло використання медичних роботів для виконання різноманітних процедур та операцій. Багато медичних роботів мають вбудовані системи виявлення дефектів, які дозволяють контролювати рухи робота та виявляти будь-які неправильності у роботі [32].

1.4 Постановка задачі. Висновки

Огляд літературних джерел показав, що на даний момент актуальність використання кіберфізичних систем в медичній галузі зростає. Кіберфізичні

системи виявлення дефектів медичних приладів дозволяють підвищити безпеку пацієнтів, внаслідок виявлення потенційних дефектів або несправностей в медичних приладах на ранніх стадіях. Це дозволяє запобігати можливим небезпекам та забезпечує безпеку пацієнтів. Також такі системи покращують якість медичних послуг завдяки вчасному виявленню дефектів у медичних приладах, що допомагає уникнути збоїв у їхній роботі та забезпечує належну функціональність. Кіберфізичні системи можуть автоматизувати процес виявлення дефектів та неполадок в медичних приладах. Це дозволяє ефективно спрямовувати зусилля технічного персоналу на ремонт або заміну пристроїв, що зменшує час і витрати на обслуговування. Кіберфізичні системи забезпечують постійний моніторинг медичних приладів, що дозволяє виявляти потенційні проблеми на ранніх етапах. Це сприяє швидкому реагуванню та запобіганню серйозним відхиленням у роботі приладів. Кіберфізичні системи також можуть збирати дані про роботу медичних приладів, що дозволяє аналізувати їхню продуктивність та прогнозувати потенційні дефекти.

Разом з тим, наявні певні недоліки у використанні таких систем. Кіберфізичні системи не здатні виявити всі можливі дефекти або неполадки в медичних приладах, особливо в умовах реального часу. Деякі проблеми можуть залишатися непоміченими, що може призвести до потенційних небезпек для пацієнтів. Впровадження та підтримка таких кіберфізичних систем можуть вимагати значних фінансових витрат. Вони можуть бути дорогими для медичних закладів, особливо для менших установ, які мають обмежений бюджет. Інтеграція кіберфізичних систем з існуючими медичними пристроями та інфраструктурою може бути складною задачею. Це може вимагати спеціалізованих знань та технічної експертизи для належної настройки та забезпечення сумісності.

Кіберфізичні системи виявлення дефектів медичних приладів можуть стати об'єктом кібератак або вразливостей в захисті даних. Це може призвести до ризику втрати конфіденційної медичної інформації або недоступності приладів для нормального функціонування. Кіберфізичні системи виявлення дефектів медичних приладів потребують наявності та належного функціонування певних

технологій, таких як мережі зв'язку, датчики, програмне забезпечення тощо. В разі відмови або неполадок в цих технологічних компонентах може виникнути ризик недостатнього моніторингу та виявлення дефектів.

Отже, метою даного дослідження є дослідження процесу виявлення дефектів медичних приладів в умовах реального часу та мінімізація ризиків для пацієнта за допомогою кіберфізичної системи виявлення дефектів медичних приладів.

Отже, для розроблення кіберфізичної системи виявлення дефектів медичних приладів необхідним є розв'язання таких задач:

- 1) провести аналіз існуючих апаратних та програмних засобів, що використовуються в кіберфізичних системах виявлення дефектів медичних виробів;
- 2) провести огляд існуючих моделей та методів виявлення дефектів медичних виробів;
- 3) розробити метод виявлення дефектів медичних виробів кіберфізичною системою;
- 4) запропонувати архітектуру кіберфізичної системи виявлення дефектів медичних виробів.

2 ВИЯВЛЕННЯ ДЕФЕКТІВ МЕДИЧНИХ ВИРОБІВ ЗА ДОПОМОГОЮ КІБЕРФІЗИЧНОЇ СИСТЕМИ

2.1 Моделювання процесу виявлення дефектів медичних виробів

В процесі використання в медичних закладах є така категорія медичних приладів, до яких ставляться підвищені вимоги до надійності, оскільки наслідки збоїв, дефектів та несправностей можуть бути критичними для пацієнта. У наш час безпека медичного обладнання та пов'язані з ним небезпеки їх використання є одним із критичних питань для охорони здоров'я організації по всьому світу.

Медичні прилади – це інструменти або машини, які використовуються для діагностики, моніторингу, лікування або запобігання захворюванням чи іншим станам. Зниження продуктивності критично важливих медичних приладів і неналежного обслуговування медичного обладнання створює неприйнятний ризик травмування пацієнта. Крім того, існують ризики травмування клінічного персоналу від простих, прямих небезпек, наприклад, випадковий контакт з електрифікованими частинами або від механічних несправностей всередині пристрою [3], наприклад дефекти в ультразвукових апаратах, несправні штучні клапани серця, витік інсулінових pomp [4], а також велика кількість помилок під час комп'ютерної томографії в деяких випадках призводить до того, що пацієнти отримують дозу опромінення, яка в 10 разів перевищує призначену.

Враховуючи представлену в розділі 1 класифікацію дефектів медичних приладів, для процесу моделювання опишемо класи дефектів медичних приладів наступним кортежем:

$$Kd = \langle D1, D2, D3 \rangle, \quad (2.1)$$

де $D1$ – дефекти класу I, що є критичними та можуть призвести до серйозних проблем зі здоров'ям пацієнта або спричинити смерть;

D2 – дефекти класу II, що можуть спричинити несприятливі наслідки для здоров'я пацієнта;

D3 – дефекти класу III, не є критичними, не призводять до суттєвих несприятливих наслідків для здоров'я, але разом з тим спричиняють неякісне надання медичних послуг.

Типи дефектів медичних приладів представимо кортежем виду 2.2:

$$Td = \langle M, El, P, S, Ek, In \rangle, \quad (2.2)$$

де *M* – механічні пошкодження приладу;

El – електричні несправності;

P – дефекти програмного забезпечення;

S – дефекти сенсорів;

Ek – дефекти пов'язані з експлуатаційними проблемами.

У 1996 році Американське товариство інженерів охорони здоров'я (ASHE) [42] представили класифікаційну схему для ранжування медичного обладнання за п'ятьма критеріями. Загальний бал (*T*) розраховується для кожного компонента за допомогою наступного рівняння:

$$T = E + A + \left(\frac{P + F + Y}{3} \right), \quad (2.3)$$

де *E* – функція обладнання;

A – клінічне застосування;

P – вимоги до профілактичного обслуговування;

F – ймовірність виходу з ладу обладнання;

Y – екологічне використання.

На основі кортежа 2.1 та формули 2.3 введемо три стани кіберфізичної системи виявлення дефектів – виникнення дефектів (*V*), виявлення дефектів (*W*) та можливість усунення дефектів в реальному режимі (*U*). Також додатково до

цих станів опишемо критерії, які дозволять виявляти критичність стану. Зокрема пропонуємо застосовувати наступні два критерії, що стосується виникнення – серйозність S та складність C . Опис критерію серйозність представлений формулою 2.4:

$$S = \langle Sh, Sm, Sl \rangle, \quad (2.4)$$

де Sh – висока серйозність дефекта, що виник,

Sm – середня серйозність дефекта, що виник,

Sl – низька серйозність дефекта, що виник.

Опис критерію складність представлений формулою 2.5:

$$C = \langle Ch, Cm, Cl \rangle, \quad (2.5)$$

де Ch – висока складність дефекта, що виник,

Cm – середня складність дефекта, що виник,

Cl – низька складність дефекта, що виник.

Для стану виявлення дефектів можливі два стани – виявлено або невиявлено.

Для стану можливість усунення пропонуємо наступні критерії – можливість усунення в реальному режимі (висока, середня, низька), тип дефекту (програмне забезпечення, апаратне забезпечення, електрика, інше).

В загальному, процес виявлення дефектів медичних приладів кіберфізичною системою представимо у вигляді наступних кроків:

1. Збір даних з медичних приладів, що включає часові ряди даних, що відображають різні параметри приладів. Ці дані можуть бути зібрані з датчиків, що встановлюються на приладі або з систем, що використовуються для моніторингу та контролю роботи приладів.

2. Попередня обробка даних. Дані можуть бути передані до системи попередньої обробки даних, де вони можуть бути очищені від шумів та інших аномалій. Додатково можуть бути використані методи, такі як фільтрація даних, нормалізація даних, віднімання фону тощо.

3. Аналіз даних. Дані можуть бути проаналізовані за допомогою методів машинного навчання, таких як класифікація, кластеризація, аналіз часових рядів тощо, щоб виявити можливі дефекти в медичному приладі.

4. Виявлення дефектів. Після аналізу даних можуть бути виявлені можливі дефекти в медичному приладі. Наприклад, можуть бути виявлені аномалії в параметрах приладу, що вказують на можливу несправність або необхідність ремонту.

5. Результати та управління. Результати аналізу можуть бути відображені на інтерфейсі користувача та передані до систем управління для прийняття рішень. Якщо виявлено дефект, система може надавати можливість для віддаленого управління медичним приладом або надіслання повідомлень медичному персоналу про необхідність проведення ремонту.

2.2 Методи аналізу даних при використанні кіберфізичної системи виявлення дефектів медичних виробів

Один з методів класифікації, що може бути використаний для виявлення можливих дефектів медичного приладу за допомогою кіберфізичної системи – це метод машинного навчання, зокрема, навчання з учителем.

Процес використання методу класифікації включає наступні кроки:

1. Збір даних. Збирання даних з медичного приладу, які описують його стан та функціонування. Це можуть бути дані з сенсорів, показники роботи приладу, параметри виконання тощо.

2. Підготовка даних. Перед обробкою дані потрібно підготувати, включаючи очищення від шуму, видалення відсутніх значень, нормалізацію або стандартизацію.

3. Вибір ознак. Вибір важливих ознак (параметрів) зі зібраних даних, які будуть використовуватись для класифікації. Ці ознаки повинні мати значущий вплив на виявлення дефектів.

4. Розбиття на навчальний та тестовий набори. Дані розділяються на дві частини: навчальний набір, на якому модель буде навчатись, та тестовий набір, який буде використовуватись для оцінки ефективності моделі.

5. Вибір моделі. Вибір відповідної моделі класифікації, яка найкраще підходить для конкретної задачі. Це можуть бути моделі, такі як логістична регресія, дерева рішень, випадковий ліс, метод опорних векторів, нейронні мережі тощо.

6. Тренування моделі. Модель навчається на навчальному наборі даних, де вона вивчає залежності між вхідними ознаками та вихідними класами (дефект або нормальний стан приладу).

В свою чергу тренування моделі включає наступні кроки:

1. Налаштування параметрів моделі. Вибір оптимальних параметрів моделі, які впливають на її точність та ефективність. Це може включати вибір функції втрат, оптимізатора, регуляризацію та інші параметри моделі.

2. Навчання моделі. Застосування навчального алгоритму для навчання моделі на навчальному наборі даних. Під час навчання модель встановлює залежності між вхідними ознаками та вихідними класами шляхом адаптації своїх внутрішніх параметрів.

3. Оцінка моделі. Використання тестового набору даних для оцінки точності та ефективності моделі. Це може включати обчислення метрик класифікації, таких як точність, відновлення, F-міра, або матриці плутанини.

4. Застосування моделі. Після успішного тренування та оцінки модель може бути застосована для класифікації нових даних, що надходять в реальному часі. Це дозволяє виявляти можливі дефекти медичного приладу на основі його

вхідних ознак та приймати відповідні заходи. Важливо зазначити, що успішність класифікації залежить від якості та репрезентативності навчального набору даних, вибору відповідної моделі та налагодження її параметрів.

Алгоритми обробки даних про дефекти медичних приладів можуть варіюватися залежно від конкретної кіберфізичної системи виявлення дефектів. Однак, деякі загальні алгоритми можуть бути використані для аналізу та класифікації дефектів:

1. Аналіз статистичних даних. Даний алгоритм використовує статистичні методи для аналізу отриманих даних про дефекти. За допомогою статистичного аналізу можна виявити шаблони у даних та визначити типи дефектів, які найчастіше відбуваються.

2. Машинне навчання. Кіберфізичні системи виявлення дефектів можуть використовувати алгоритми машинного навчання для класифікації дефектів. За допомогою цих алгоритмів можна навчити систему відрізняти різні типи дефектів та автоматично виявляти їх у майбутньому.

3. Аналіз вібрації. Кіберфізичні системи можуть використовувати датчики вібрації для аналізу роботи медичних приладів. За допомогою аналізу вібрації можна виявити дефекти, пов'язані з нестабільною роботою механічних деталей.

4. Аналіз електричних сигналів. Кіберфізичні системи можуть використовувати аналіз електричних сигналів для виявлення дефектів медичних приладів. Наприклад, за допомогою аналізу електричних сигналів можна виявити переривання електричних контактів або нестабільну роботу електронних компонентів.

5. Аналіз зображень. Деякі кіберфізичні системи можуть використовувати Аналіз зображень може бути використаний в кіберфізичних системах для виявлення дефектів медичних приладів, які мають оптичні частини або використовують зображення для діагностики. Алгоритми обробки зображень можуть використовувати методи комп'ютерного зору, щоб автоматично визначати розмір, форму та кількість дефектів на зображеннях.

Наприклад, цей підхід може бути використаний для виявлення дефектів на рентгенівських знімках, мамографічних зображеннях або зображеннях ультразвукової діагностики. Алгоритми обробки зображень можуть використовувати нейронні мережі для автоматичного виявлення аномалій на зображеннях та повідомлення оператора про потенційні дефекти.

Також, кіберфізичні системи можуть використовувати терміновий аналіз зображень для виявлення дефектів, які можуть призвести до аварії медичного приладу. Наприклад, терміновий аналіз зображень може бути використаний для виявлення проблем з терморегулюванням відповідних компонентів приладу, таких як датчики температури.

Проведений аналіз даних, щодо 1000 дефектів пов'язаних із різними медичними приладами різної критичності виявив, що 937 (93,7%) виявлених дефектів стосуються несправностей пристроїв і інструментів. Ці події мали значний негативний вплив на пацієнтів, іноді призводячи до смертей і травм або викликаючи переривання процедури для усунення системних проблем. Незважаючи на те, що найсучасніші медичні прилади та системи розроблені з механізмами безпеки, які намагаються виявити ці збої та дефекти та перевести прилади та системи в безпечний стан, щоб запобігти ризиків для пацієнтів, на практиці ці механізми недосконалі. Зокрема, із 536 розглянутих системних помилок, виявлених під час процедур, 488 (91%) призвели до перерви в ході операції, що змусило хірургічні бригади вручну перезавантажити систему (43% з 488), конвертувати процедуру (61,5%), або переносити його на більш пізній термін (24,8%). У деяких випадках після кількох перезавантажень системи процедуру було перетворено або переплановано.

Діагностичні механізми медичних приладів та систем наразі недостатньо повні, щоб правильно визначити причини несправностей і системних помилок під час операції, тобто в режимі реального часу. Таким чином, інформація про тип системного дефекту (наприклад, у стані помилки, яку можна відновити або не підлягає відновленню) і відповідні процедури усунення несправностей можуть бути неадекватними або неправильно передані медичному персоналу. Основні

причини часто визначаються лише постфактум, коли інженери з обслуговування на місцях проводять додаткові дослідження та повторюють сценарії збою. Наприклад, про несправність кодера або датчика було повідомлено як про виправну системну помилку під час процедури, коли її не можна було відновити та можна було виправити лише заміною компонента після процедури [9].

Системні оператори (включно з лікарями, асистентами лікарів та інженерами обслуговування) часто недостатньо навчені правильно тлумачити причини спостережуваних системних помилок і вибирати ефективні дії з усунення дефектів для відновлення після надзвичайних ситуацій. Наприклад, в одному випадку було повідомлено, що хірургічна бригада витратила значну кількість часу на усунення невивірної системної помилки, коли пацієнт перебував під анестезією більше однієї години [9].

Ці результати показують важливість розробки надійних функцій безпеки та перевірки ефективності механізмів виявлення та відновлення медичних приладів, щоб допомогти медичному персоналу прогнозувати та запобігати критичним подіям та виконувати ефективні процедури усунення несправностей. Крім того, слід покращити підготовку системних операторів, щоб зробити усунення несправностей і обробку несприятливих подій центральною частиною навчання. Насправді в інших галузях, що мають важливе значення для безпеки (наприклад, комерційна авіація), багато зусиль витрачається на постійне вдосконалення практики безпеки шляхом ретельного розслідування аварій, детального аналізу небезпек і передового дизайну безпеки в поєднанні з комплексним навчанням на основі симуляції, яке включає роботу в наявність критичних для безпеки відмов [47].

Міжнародні стандарти безпеки (наприклад, ISO 14971 для медичних пристроїв [20] та ISO 26262 для автомобілів [48]) рекомендують ідентифікувати потенційні загрози безпеці та визначати вимоги безпеки для впровадження механізмів, які можуть виявляти та пом'якшувати небезпеки. Стандарти (наприклад, Керівництво з безпеки програмного забезпечення NASA [49]) також наголошують на важливості перевірки введення несправностей як засобу

перевірки надійності механізмів безпеки за наявності несправностей і ненормальних умов [50].

Як показують дослідження, традиційні методи аналізу небезпеки, які використовуються для медичних пристроїв, зосереджені насамперед на відмовах окремих компонентів або людських помилках у системі. Інші потенційні причинні фактори, такі як складні помилки програмного забезпечення та небезпечні взаємодії компонентів, часто не враховуються ретельно під час аналізу. Теоретико-системні методи аналізу небезпек, такі як STPA (системно-теоретичний аналіз процесів) [12], долають це обмеження шляхом моделювання аварій як складних динамічних процесів, що є результатом неадекватних механізмів контролю, які порушують обмеження безпеки. Показано, що STPA може ідентифікувати додаткові причини аварій, які не виявляються методами FTA та FMEA [12], [56].

Програмно-реалізована ін'єкція помилок (SWIFI) [51, 52] є поширеною технікою перевірки ефективності механізмів відмовостійкості шляхом вивчення поведінки системи за наявності помилок. Наслідки програмних чи апаратних збоїв емулюються випадковим чином.

База даних FDA Recalls містить секретні відкликання медичних пристроїв з 1 листопада 2002 року. Відкликання – це добровільна дія, яку вживає виробник, дистриб'ютор або інша відповідальна сторона, щоб виправити або видалити з ринку будь-який медичний пристрій, який порушує закони FDA. Відкликання ініціюється, щоб захистити здоров'я та благополуччя населення від пристроїв, які є дефектними або становлять ризики для здоров'я, такі як захворювання, травми або смерть. У рідкісних випадках, якщо компанія не в змозі добровільно відкликати пристрій, який представляє ризик для здоров'я, FDA може видати наказ про відкликання виробнику.

FDA класифікує відкликання на три класи на основі відносного ступеня небезпеки для здоров'я, який представляє пристрій. Відкликання класу I свідчить про достатню ймовірність того, що використання пристрою спричинить серйозні несприятливі проблеми зі здоров'ям або смерть. Прикладами відкликаних

пристроїв цього класу є дефібрилятори/монітори, апарати для наркозу та системи доставки ліків. Клас II вказує на пристрої, які можуть спричинити тимчасові або оборотні несприятливі наслідки для здоров'я або створювати віддалену ймовірність серйозних проблем зі здоров'ям. Монітори рівня глюкози та багатопараметричні монітори пацієнта є прикладами пристроїв, відкликаних у цьому класі. Клас III вказує на пристрої, які порушують закони FDA, але, ймовірно, не спричинять негативних наслідків для здоров'я, наприклад програматори для пацієнтів і програмне забезпечення ультразвукової системи.

Кожен запис, поданий до бази даних відкликаних FDA, містить структуровану інформацію, таку як унікальний номер відкликання; клас відкликання; Дата публікації в FDA, а також неструктуровані описи, що описують назву продукту (тобто назву пристрою та опис його функціональних можливостей), фірму/виробника, що відкликає, кількість у продажу (тобто кількість пристроїв, що розповсюджуються на ринку), і важливі інформацію про питання безпеки пристрою, причину відкликання.

З досліджених дефектів, тих, що пов'язані з комп'ютером становить близько 50%, що, в свою чергу призвели до 398 смертей та 182 поранення. Але можна припустити, що в базі даних MAUDE є неточності та заниження даних, а також невідповідності.

Як приклад невідповідності можна навести, що хоча критичні для безпеки комп'ютерні дефекти вплинули на значну кількість пристроїв, що використовуються в радіології, дуже мало серйозних побічних ефектів через комп'ютерні проблеми можна було ідентифікувати для цих пристроїв у базі даних MAUDE. Тим не менш, імплантовані кардіостимулятори, дефібрилятори та інфузійні насоси переважають серед комп'ютерних несправностей (35 відкликаних) і смертельних випадків (392 смерті).

Це спостереження можна пояснити великою кількістю цих пристроїв, які використовуються для лікування критичних станів, таких як раптова зупинка серця.

2.3 Метод виявлення та класифікації дефектів медичних виробів

Для опису методу виявлення та класифікації дефектів медичних приладів в кіберфізичній системі виявлення дефектів скористаємось розробленими формулами 2.1 – 2.4.

Перший крок полягає у застосуванні методу для визначення індексу ризику для досліджуваних приладів, формула 2.5:

$$R = \langle R1, R2, R3 \rangle, \quad (2.5)$$

де $R1$ – індекс ризику високий;

$R2$ – індекс ризику середній;

$R3$ – індекс ризику низький.

На другому кроці ці критерії застосовуються для різних виробів, щоб врахувати інші аспекти небезпек.

Використавши класифікації ризиків запропоновані Інститутом ризику (ECRI) [46] шляхом присвоєння оцінки 5 високому ризику (H), оцінка 4 — середній ризик (M) і оцінка 1 – низький ризик (L). Оцінки технічного обслуговування однакові з Fennigkoh і Сміт [50] критерій обслуговування. Ван і Райс [53] запропонували два методи відбору проб для включення частини медичного обладнання в технічне обслуговування; спрощена версія градієнтного ризику вибірка (GRS) і вибірка атрибутів. Ridgway [53] обговорює, що хоча профілактичне обслуговування запобігає виходу з ладу деяких пристроїв, справа в тому, що це корисно для відносно небагато пристроїв, і його не можна використовувати для всіх несправностей пристроїв. Він також надає вказівки для МЕМР і знайомить з деякими інструментами, які успішно використовуються в різних галузях промисловості, наприклад технічне обслуговування, орієнтоване на надійність (RCM). Юсеф та ін. [54] запропонував модель класифікації медичних виробів на основі їх складності. Їхня модель складається з двох етапів: технічної складності та використання складності. Технічна складність включає

чотири критерії, що стосуються технічної перспективи, таку як ремонтпридатність обладнання під час використання, складність складається з дев'яти критеріїв щодо складності на рівні експлуатації медичного обладнання, наприклад введення даних, процесу налаштування.

Деякі автори [54-57] обговорювали, що хоча ризик це важливий критерій у класифікації медичного обладнання, також слід враховувати такі критерії, як рівень використання обладнання, наявність ідентичних пристроїв, критичність місії, повідомлення про небезпеку та історія відкликань. Щоб подолати цю проблему, Тагіпур та ін. [57] представили багатокритеріальне прийняття рішень з використанням аналітичного ієрархічного процесу для встановлення пріоритетів медичного обладнання на основі їх критичності. Їх запропонований метод складається з шести критеріїв «ризик», «вік», «функція обладнання», «важливість місії», «відкликання» та «вимоги до технічного обслуговування». Однак цей метод багато хто критикував через такі певні питання як необхідність великої кількості суб'єктивних попарних порівнянь, невизначеність експертів та через суб'єктивність у процесі порівняння, тощо.

Нещодавно Corciova та ін. [48] надав деякі рекомендації створити та керувати програмою забезпечення якості медичного обладнання, а також представити деякі процедури перевірки, обслуговування, оцінка та перевірка продуктивності медичних пристроїв. Вони розглянули п'ять критеріїв ризику у своїй системі оцінки щодо пацієнтів і співробітників. Тавфік та ін. [7] розробили нечітку модель класифікації медичного обладнання. Вони використовували чотири критерії (статус критичності місії, функціонування обладнання, обслуговування вимоги та фізичні ризики), щоб обчислити ризик бали для кожного пристрою. Їх результати показують, що в деяких випадках той самий тип обладнання може мати різні оцінки ризику. Крім того, вони порівняли свою класифікаційну схему порівняно з іншими схемами. Це порівняння ілюструє, що в деяких випадків, коли медичне обладнання може отримати різні оцінки ризику.

Незважаючи на всі ці зусилля, деякі важливі моменти залишаються поза увагою і, потребують вдосконалення. Серед них слід звернути увагу на наступні аспекти:

1) оскільки пріоритезація та класифікація медичного обладнання є, то слід розглядати оцінки різних експертів, а не визначати пріоритети на основі оцінки одного експерта;

2) деякі критерії, що широко використовуються в різних літературних джерелах та дослідженнях, потребують переоцінки та перегляду;

3) деякі нові критерії повинні бути додані до переоцінених критеріїв;

4) критерії та таблиці, які використовуються в процесі встановлення пріоритетів, повинні бути визначено більш простим і реалістичним способом, щоб бути зрозумілим для всіх клінічних експертів.

Підхід до медичного пристрою на основі нечіткого визначення пріоритетів.

Відповідно до традиційних принципів FMEA та RBM, мета запропонованого підходу полягає в забезпеченні високої доступності для критичних медичних приладів. Коротше кажучи, цей підхід може віддати пріоритет медицині приладів виходячи з їх критичності з урахуванням різних критеріїв та розмірів. Крім того, запропонована модель здатна вибрати найкращу стратегію обслуговування для кожного медичного пристрою.

Запропонований підхід складається з трьох наступних кроків.

Перший крок базується на моделі FFMEA, яка об'єднує три критерії (D, O і S) і вісім підкритеріїв. У традиційному FMEA методі, пріоритети ризику режимів відмови отримують за допомогою число пріоритету ризику (RPN), яке є добутком трьох факторів ($RPN = O \times S \times D$). Цей метод простий, але багато авторів його критикують. Деякі з цих критичних зауважень включають:

1. Різні набори O, S і D можуть створювати ідентичні RPN.
2. Не враховується відносна важливість між O, S і D.
3. Метод, який використовується традиційним FMEA для розрахунку ризику бали невдач.
4. Фактори витрат і прибутковості ігноруються.

5. Ігноруються думки різних експертів,

6. Шкали для S, O і D є порядковими.

Щоб подолати традиційні недоліки FMEA, найкраще використовувати нечіткий підхід для обчислення RPN. При цьому ми застосовуємо модифіковану версію FFMEA на першому кроці моделі шляхом призначення лінгвістичних змінних факторам RPN, щоб врахувати невизначеності в ідеї експертів. Крім того, були призначені певні ваги до ідей експертів, а також факторів RPN. Крім того, додалися вісім підкритеріїв до основних критеріїв (S, O та D) методу RPN, щоб розглянути різні аспекти невдач у кожному медичном виробі. Слід підкреслити, що запропонована модель FFMEA має здатність розглядати численні відмови.

Критерій виявлення (D). Цей критерій відноситься до ймовірності виявлення потенційної несправності до її виникнення. У цьому дослідженні виявленість включає два наступні підкритерії; ймовірність виявлення та метод виявлення збоїв.

Ймовірність виявлення (D1). Цей підкритерій оцінює швидкість виявлення несправностей пристрою за допомогою таблиці 1.

За даними Sharma et al. [19], «ймовірність виявлення пов'язане з різними факторами, включаючи здатність обслуговування персонал для виявлення несправності шляхом періодичного огляду або голіоко або за допомогою машинних діагностичних засобів, наприклад автоматичних засоби керування, сигналізації та датчики». Нечіткі оцінки визначені згідно з досвідом авторів, думкою обслуговуючого персоналу та з використанням дослідження Брагліа [20]. Зверніть увагу, що оцінки для цього критерію були розглянуті у зворотному масштабі, оскільки ми маємо справу з ймовірністю «виявлення». Це видно, що чим менше видима несправність пристрою, тим менше зростає ймовірність її виявлення. Виявлення другого елемента через засоби автоматичної діагностики відноситься до програм автоматичного аналізу або встановлені датчики для виявлення деяких дефектів пристрою. Кожен експерт слід враховувати всі ці чотири елементи, щоб мати можливість оцінити підкритерій D1. На рисунку 2.1 показана нечітка функція належності цей підкритерій.

Усі типи несправностей та пов'язана з ними частота, наслідки, і виявленість можна оцінити за допомогою обслуговування пристрою історії [17].

Метод виявлення відмови (D2). Вид методу, який використовується для виявлення збоїв є ще одним важливим показником можливість виявлення ремонтпридатних пристроїв. Зокрема, цей підкритерій вимірює ступінь автоматизації процесу перевірки медичний прилад. Слід зазначити, що для решти функціонує нечітка належність підкритеріїв (O1, O2, O3, C1, C2, C3 і C4). Критерій поява (O) оцінки частоти відмов або ймовірності їх виникнення частота потенційних збоїв або ризиків для даного пристрою.

Для більш точного розрахунку цієї ймовірності потрібно щоб деякі підкритерії були додані до критерію появи залежно від пристрою чи системи. Тоді пропонується три наступні підкритерії, які потрібно додати до критерію появи; частота або середній час між відмовами (O1), повторюваність (O2) і видимість (O3). Ці підкритерії представлені нижче.

Середній час напрацювання на відмову (O1). Середній час між відмов (MTBF) є одним із часто використовуваних основних заходів у розробці надійності ремонтпридатних пристроїв або компонентів [21]. MTBF повідомляє очікуваний час між двома відмовами для ремонтпридатна система. Можна отримати необхідні дані щодо MTBF від комп'ютеризованих систем управління технічним обслуговуванням (CMMS). фірм/організацій, і вони повинні бути інтегровані з досвідом експертів з технічного обслуговування. У цьому дослідженні MTBF визначається як ймовірність відмови протягом періоду часу, як показано в таблиці 3.

Повторюваність (O2). Повторюваність є ще одним важливим фактором з точки зору появи, який слід враховувати при оцінці ймовірність виникнення. Geumet al.[22] визначити «повторюваність» як «поняття, що відрізняється від частоти, що представляє частота виникнення несправностей через те саме джерело в межах визначений час». У цій роботі повторюваність визначається як «те саме збій пристрою чи компонента, який стався протягом певного періоду часу».

При одній і тій же несправності, що відбувається протягом короткого періоду (наприклад, 3 місяці), його рейтинг повторюваності становить дуже високий, тоді як коли один і той же збій відбувається протягом тривалого періоду часу (наприклад, 10 років), рейтинг повторюваності дуже низький.

Критерій видимість (O3). Помітність невдач є третім важливим критерієм.

Фактор вимірювання ймовірності появи відмов спеціально прихованих відмов. Він показує, чи є збій видимим для експертами з обслуговування чи ні.

На першому етапі нечіткий аналіз режимів відмови та наслідків. Представлення критеріїв у вигляді функцій належності представлено на рисунку 2.1.

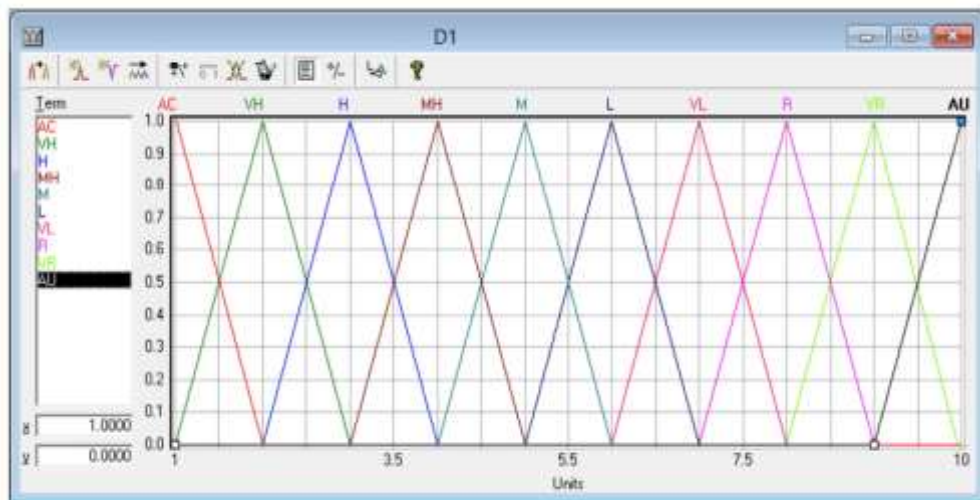


Рисунок 2.1 – Представлення критеріїв у вигляді функцій належності

Метод застосовується з урахуванням кількох факторів оцінки ризику. На другому кроці такі параметри, як небезпеки, пов'язані з використанням, вік і використання медичних приладів, застосовуються для врахування всіх аспектів небезпек та ризику у визначенні пріоритетів медичних виробів.

За допомогою методу, представленого в роботі, медичний персонал може легко класифікувати медичні пристрої для технічного обслуговування відповідно до їх балів критичності. Впровадження цієї структури може збільшити доступність машини високого ризику в галузях охорони здоров'я. Крім того, цю

структуру можна застосовувати в інших критичних галузях, шляхом зміни деяких критеріїв і розмірів.

Покладаючись на складне програмне забезпечення, складне апаратне забезпечення, батареї, датчики та мережевий зв'язок, медичні вироби стикаються з кількома проблемами щодо надійності, безпеки та безпеки.

Збільшення складності підвищує ймовірність нещасних випадків взаємодії компонентів; портативність робить пристрої більш уразливими до відключень електроенергії; а взаємозв'язок збільшує ймовірність поширення помилки і ймовірність зіткнутися зі штормовими збоями, з якими пристрої не зможуть впоратися безвідмовно.

Крім того, медичні пристрої схильні до серйозних уразливостей у безпеці та конфіденційності, таких як несанкціоноване керування сенсорними та комунікаційними функціями пристроїв і доступ до особистих даних пацієнтів. Незважаючи на важливість проблем, пов'язаних із безпекою та конфіденційністю, у базах даних FDA ці проблеми значно занижені.

2.4 Висновки

Пропонується класифікацію діяльності з технічного обслуговування медичних пристроїв за допомогою графічного рішення. Розгляд аспектів вартості шляхом віднесення економічних збитків до наслідків відмови кожного медичного пристрою через витрати на технічне обслуговування (МС), втрати від затримки лікування (DL) та лінгвістичні терміни. У запропонованій структурі кілька міждисциплінарних експертів можуть оцінювати як важливість критеріїв, так і оцінку альтернатив. Насправді мультидисциплінарна команда забезпечує врахування різних думок. Запропонована структура здатна враховувати як якісні, так і кількісні критерії/підкритерії.

Двома основними внесками цього дослідження є: розробка основи для встановлення пріоритетів критичних медичних пристроїв та пропозиція методу вибору найкращої стратегії обслуговування для кожного пристрою. Пріоритезація

медичних пристроїв на основі ризиків є важливою для організацій охорони здоров'я при визначенні пріоритетів технічного обслуговування та виділенні бюджетних коштів на роботи з технічного обслуговування. Крім того, результати цього дослідження є дуже корисними як для академічних наук, так і для інших критичних галузей, таких як авіація, нафтова промисловість і тощо, модифікувавши деякі критерії та параметри.

3 АРХІТЕКТУРА КІБЕРФІЗИЧНОЇ СИСТЕМИ ВИЯВЛЕННЯ ДЕФЕКТІВ МЕДИЧНИХ ВИРОБІВ

3.1 Проєктування кіберфізичної системи виявлення дефектів медичних виробів

Кіберфізичні системи є інтеграцією реальних фізичних процесів та віртуальних обчислювальних процесів. Вони є складними інженерними системами, які спираються на інтеграцію фізичних обчислень та комунікаційних процесів [1]. Кіберфізичні системи, які взаємодіють з фізичним світом ніколи не будуть працювати в контрольованому середовищі, отже вони мають бути готовими до несподіваних умов і бути адаптованим до будь-яких збоїв системи або підсистем [17].

Постійно зростаючий попит різного призначення на системи управління інформацією призводить до оптимізації методів проєктування обчислювальних засобів. Переважна більшість сучасних систем – це системи управління інформацією, які є вбудованими системами і мережами. Вони тісно пов'язані з контрольними або об'єктами управління.

Вбудовані системи за сферою використання поділяються на:

- 1) системи автоматичного керування;
- 2) вимірювальні системи та системи, що зчитують інформацію від датчиків;
- 3) інформаційні системи «питання-відповідь» в режимі реального часу;
- 4) цифрові системи передачі даних;
- 5) складні системи реального часу;
- 6) системи управління рухомими об'єктами;
- 7) підсистеми комп'ютерної системи загального призначення;
- 8) мультимедійні системи.

Теперішніми вимогами є підвищення рівня інтеграції та безпеки вбудованих систем, а також можливість поєднувати їх у керовані мережі. Зниження цін на елементи вбудованих систем та збільшення зв'язку з фізичними об'єктами управління призвело до появи кіберфізичних систем. Кіберфізичні системи – це

спеціалізовані обчислювальні системи, які дають змогу програмному додатку взаємодіяти з предметами та подіями у фізичному світі. У вбудованих системах основна увага приділяється обчислювальним елементам, але в кіберфізичних системах - зв'язку обчислювальних розрахунків з фізичними елементами. Кіберфізичні системи використовуються в таких сферах, як медицина, управління дорожнім рухом, промисловий і технологічний контроль, екологічний моніторинг, промислові роботи та захист систем. Для широкого використання кіберфізичних систем у медицині та медичних інституціях, вони повинні бути адаптивними, масштабованими та економічно ефективними, а також забезпечувати безпеку та ефективність для всіх процесів. Бездротові сенсорні мережі можуть стати важливою частиною кіберфізичних систем через високу здатність чутливості, що є одним із основних рушійних факторів кіберфізичного розподілу системних додатків. Швидкий розвиток бездротових сенсорних мереж в медичних датчиках та системи хмарних обчислень роблять кіберфізичні системи перспективними для використання та вдосконалення стаціонарної та амбулаторної медичної допомоги [3].

Процес розвитку кіберфізичної системи не може бути реалізовано без залучення іншого сектора професіоналів, які можуть налаштувати можливості системи відповідно до необхідного рівня для сфери використання. Знання комп'ютерів, програмне забезпечення, мережі та фізичні процеси, які будуть інтегровані в систему, потрібні для розробки кіберфізичної системи [18].

Кіберфізична система, як і будь-яка вбудована система процес проектування включає управління вимогами, проект план управління, тестування та безпеки.

Операційні системи реального часу керують вбудованими системами згідно нормативних документів. Розвиток кіберфізичних систем, які тісно взаємодіють з фізичними процесами, вимагає технічно складного низькорівневого дизайну. Розробники медичних кіберфізичних систем змушені справлятися з контролерами переривання, архітектурою пам'яті, процесами планування, програмування на рівні асемблера, мережевих інтерфейсів проектування та встановлення драйверів. Проте було б краще зосередитися на функціональності системи та визначенні

поведінки. Кіберфізичні системи, які використовуються в галузі охорони здоров'я, повинні підтримувати широкий спектр стандартів обміну інформацією, які використовуються у більшості існуючих медичних приладів, що отримують та задалегідь обробляють інформацію про стан здоров'я пацієнта.

Зберігати інформацію про показники стану здоров'я пацієнта, система необхідно розрізняти джерело інформації та рівень довіри джерела можуть бути оцінені експертами, що дозволить системі вимірювати достовірність даних і приймати рішення щодо подальше використання інформації [18].

Архітектурне проектування кіберфізичної системи виявлення дефектів медичних приладів має базуватися на загальному моделюванні поведінки систем та обладнання, програмного забезпечення, єдиного дизайну мережі та фізичних процесів [13].

Процес проектування – це ітеративний процес, який складається з трьох фаз: моделювання, проектування та аналізу (рисунок 3.1). Щоб розробити системи, які зможуть працювати в реальному світі та режимі, спочатку слід виконати аналіз реального світу, а також визначити фізичні процеси, які будуть взаємодіяти з кіберфізичною системою.

Наступний крок – почати розробку абстракції процесів реального світу. Модельний дизайн дозволяє подолати деякі фундаментальні проблеми в проектуванні кіберфізичних систем, таких як безпека, детермінізм і час.

Кожна система розроблена для вирішення конкретної проблеми або виконання конкретного завдання. Системні вимоги можна описати простою мовою, офіційно або за моделями. Формальний опис зменшує кількість можливих помилок, але моделювання служить для ілюстрації динаміки системи.

Процес розробки кіберфізичної системи виявлення дефектів медичних виробів може включати наступні етапи:

1. Аналіз вимог та потреб користувачів. На цьому етапі проводиться дослідження потреб користувачів і визначається, які вимоги повинна задовольняти кіберфізична система.

2. Проєктування архітектури системи. Цей етап присвячений розробці загальної архітектури системи, включаючи визначення компонентів системи, їх функцій та інтерфейсів.

3. Розробка програмного забезпечення. На цьому етапі проводиться розробка програмного забезпечення для збору даних, обробки даних та виявлення дефектів.

4. Розробка апаратної складової. На цьому етапі проводиться розробка апаратної складової, включаючи сенсори, пристрої збору даних та інтерфейси з медичними приладами.

5. Тестування та налагодження. Тут проводиться тестування та налагодження системи, включаючи випробування на реальних медичних приладах та відповідну настройку алгоритмів виявлення дефектів.

6. Впровадження. Після успішного тестування та налагодження система готова до впровадження в роботу. На цьому етапі проводиться навчання персоналу, інтеграція системи з медичними приладами та її повний запуск у роботу.

7. Підтримка та розвиток. Після того, як відбудеться впровадження кіберфізичної системи, проводиться її підтримка та розвиток, включаючи відслідковування нових потреб користувачів, вдосконалення алгоритмів виявлення дефектів та розширення функцій за потреби.

У процесі аналізу визначається ступінь, в якому система відповідає вимогам специфікації. Набір правил і стандартів поширюється на всі медичні системи, що вказує на те, що система електрично, фізично, біологічно та хімічно безпечна для кінцевого споживача.

Датчики кіберфізичної системи генерують конфіденційні дані, які мають бути захищені та доступні лише безпечним способом.

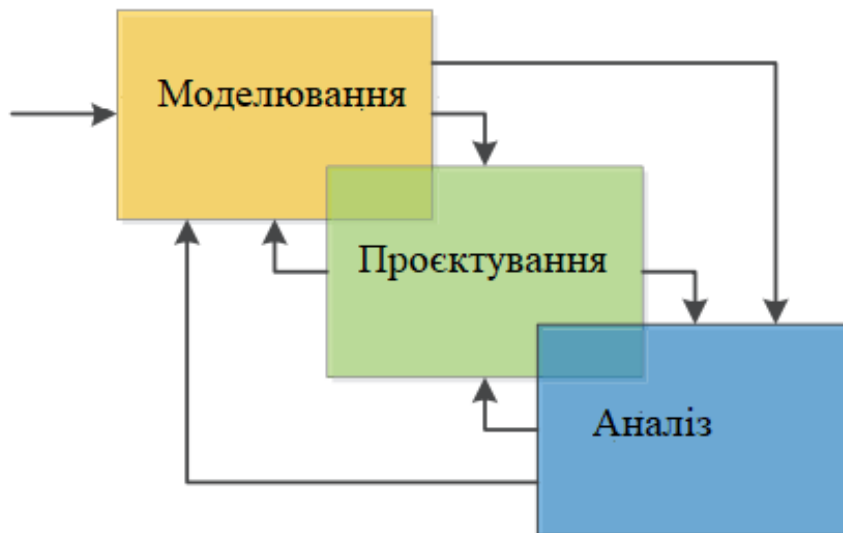


Рисунок 3.1 – Процес розробки кіберфізичної системи

На даний момент немає стандартів і правил, які застосовуються безпосередньо до кіберфізичних систем охорони здоров'я [6, 12]. Однак, перед розробленням кіберфізичної системи в медичній галузі варто ознайомитися з медичними стандартами, що застосовуються до медичного обладнання, з правилами та клінічними стандартами. Правила, що застосовуються для медичного обладнання аналогічні б багатьох країнах світу, але вони не ідентичні. Це означає, що той самий медичний виріб може бути визнаний безпечним для використання в медичних закладах країн Євросоюзу або інших країнах, але не в Сполучених Штатах. Європейський Союз використовує маркування CE для сертифікації виробу, який повинен відповідати нормам ЄС. Подібні стандарти є і в США, наприклад FDA (Управління з контролю за продуктами й ліками США), що вказує на відповідність медичного обладнання нормам та стандартам США. В Україні розроблені стандарти на основі документації Європейського Союзу, але маркування CE для використання медичних приладів недостатньо, необхідна ще українська сертифікація [36]. Країни, які не розробили і не прийняли жодного Положення щодо медичного обладнання в першу чергу використовують стандарти ВООЗ (Всесвітня організація охорони здоров'я). У той час як стандарти охорони здоров'я кіберфізичних систем є ще не розбудовані, ряд промислових,

комунікацій (наприклад, Bluetooth - IEEE 802.15.1, Wi-Fi - IEEE 802.11), якості (ISO 9001, ISO 13845, ISO 14971), медобладнання (ISO/IEEE 11073, HL7 – рівень здоров'я 7, DICOM – Цифрові зображення та комунікації в медицині) і до них можна застосувати клінічні стандарти [18].

ISO/IEEE 11073 – це набір стандартів для особистої медичної допомоги пристроїв. Загальним контекстом цього є передача даних і інтерфейс між агентом і менеджером. Рівень здоров'я 7 – це група стандартів для обміну, інтеграція, обмін та пошук електронної інформації про здоров'я інформації. HL7 визначає багато адаптованих стандартів, керівних принципів і методологій, які забезпечують комунікацію різні комп'ютерні системи в лікарнях і різних закладах охорони здоров'я провайдерів [18].

Стандарти на медичне обладнання встановлюються для забезпечення безпеки та ефективності його використання. Основні стандарти, які використовуються в галузі медичного обладнання, включають:

1. ISO 13485: Системи управління якістю для медичного обладнання - вимоги до розробки та виробництва [37].
2. IEC 60601: Електричне обладнання медичне - Частина 1-11: Загальні вимоги до безпеки, включаючи основні вимоги до безпеки та ефективності [38].
3. IEC 62304: Медичне програмне забезпечення - Життєвий цикл програмного забезпечення [39].
4. IEC 62366: Ергономіка медичних пристроїв - Застосування людських факторів до проектування та оцінки безпеки медичних пристроїв [40].
5. IEC 60601-1-2: Електричне обладнання медичне - Частина 1-2: Загальні вимоги до безпеки - Електромагнітна сумісність [38].
6. ISO 14971: Цей стандарт визначає вимоги до управління ризиками медичних пристроїв, включаючи процеси оцінки та керування ризиками [41].

Ці стандарти встановлюють вимоги до безпеки, ефективності та якості медичного обладнання та програмного забезпечення, що використовуються в галузі медицини. Вони є обов'язковими для дотримання виробниками медичного

обладнання та програмного забезпечення, що використовується в галузі медицини.

Розроблені стандарти на медичне обладнання дозволяють покращити якість, безпеку, електричну безпеку, електромагнітну сумісність, управління ризиками та інші аспекти медичного обладнання. Вони сприяють забезпеченню безпеки пацієнтів та високої якості медичних пристроїв.

Варто підкреслити, що в охороні здоров'я на об'єктах повинні використовуватися лише сертифіковані кіберфізичні системи.

Отже, враховуючи вищевикладене, архітектура кіберфізичної системи виявлення дефектів медичних приладів складається з трьох рівнів та представлена на рисунку 3.2.

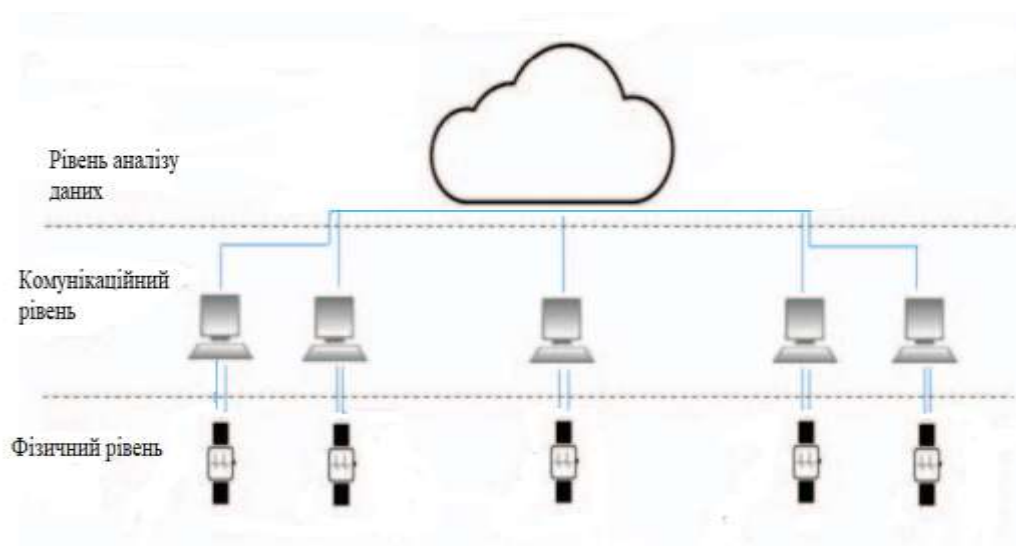


Рисунок 3.2 – Архітектура кіберфізичної системи виявлення дефектів медичних виробів

Розглянемо ці рівні детальніше. Фізичний рівень призначений для датчиків, які взаємодіють з медичними приладами та отримують інформацію про стан медичних приладів.

Після цього інформація про стан медичних приладів передається на комунікаційний рівень. Все пристрої повинні бути приєднані до комп'ютера

безпечним способом стосовно обміну даними, щоб виключити можливість обміну даними з пристроями або комп'ютером, які не належать до системи.

На рівні аналізу даних є можливість обробляти всю отриману інформацію (крім приватної інформації) з комунікаційного рівня обслуговування та надсилати відповідь запитувачу, включаючи інформацію про можливі несправності та рішення для запобігання або усуненні цих несправностей. Основна роль шару полягає в зборі інформації з різних датчиків та приладів та використовувати всю отриману інформацію для подальшого аналізу даних.

Кіберфізична система виявлення дефектів медичних приладів – це система, яка поєднує фізичні технології і програмне забезпечення для виявлення дефектів в медичних приладах. Ця система може бути використана для автоматичного моніторингу медичних приладів, що дозволяє забезпечити їх безперебійну роботу і запобігти можливим нещасним випадкам, пов'язаним з несправністю обладнання.

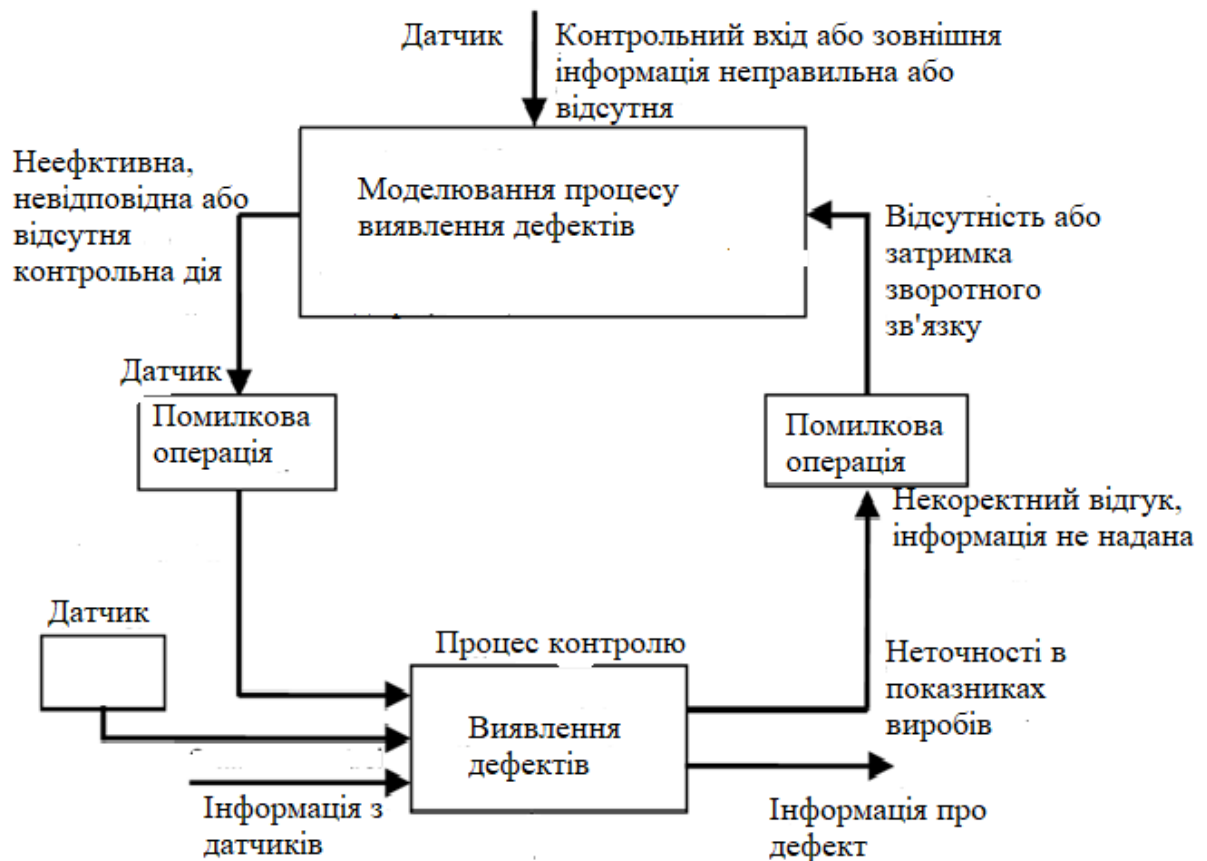


Рисунок 3.3 – Система виявлення та аналізу дефектів

3.2 Виявлення дефектів медичних виробів за допомогою кіберфізичної системи

Метод виявлення дефектів медичних приладів за допомогою кіберфізичної системи може включати наступні кроки:

1. Збір даних з медичних приладів за допомогою датчиків, що встановлюються на приладах. Дані можуть включати різні параметри, такі як температура, вологість, тиск, рівень заряду батареї та інші параметри, що відповідають за роботу медичного приладу.

2. Аналіз даних за допомогою програмного забезпечення з аналітикою даних. Програмне забезпечення може використовувати різні алгоритми та методи, такі як аналіз часових рядів, класифікація та кластеризація, щоб виявити можливі дефекти медичного приладу.

3. Виявлення дефектів медичного приладу та інформування про них. Якщо програмне забезпечення виявить можливий дефект, воно повідомляє про це систему моніторингу та управління. Система моніторингу та управління може надавати можливість для віддаленого управління медичним приладом або надіслання повідомлень медичному персоналу про необхідність проведення ремонту.

4. Моніторинг стану медичного приладу та зберігання даних про нього. Кіберфізична система може зберігати дані про стан медичного приладу та його ремонт, що може бути корисно для підтримки його ефективної роботи та попередження можливих проблем у майбутньому.

Цей метод виявлення дефектів медичних приладів за допомогою кіберфізичної системи може допомогти забезпечити ефективне та безпечне використання медичних приладів у медичних закладах. В даній роботі використовуємо метод класифікації.

В ході дослідження виявлено, що незважаючи на те, що збої програмного забезпечення залишаються основною причиною (64,3%) відкликаних комп'ютерних медичних пристроїв, апаратне забезпечення, батарея та

введення/виведення також вносять значний внесок у збої, які можуть призвести до потенційно критичних небезпек для життя.

Незважаючи на те, що збої програмного забезпечення залишаються основною причиною (64,3%) відкликаних комп'ютерних медичних пристроїв, апаратне забезпечення, батарея та введення/виведення також вносять значний внесок у збої, які можуть призвести до потенційно критичних небезпек для життя.

Збої апаратного забезпечення, батареї та вводу-виводу мали більший вплив (вплинули на 6,5 мільйонів, 54% відкликаних пристроїв на ринку) з точки зору кількості пристроїв, які постраждали від відкликаних (майже втричі) та вартості видалення пристроїв /ремонт.

З усіх критично важливих для безпеки відкликаних 80,7% стосувалися пристроїв, що використовуються в радіології (наприклад, лінійні прискорювачі), серцево-судинних (наприклад, автоматичні зовнішні дефібрилятори), загальних лікарнях (наприклад, інфузійні насоси), анестезіології (наприклад, вентилятори) та загальна хірургія (наприклад, електрохірургічні аксесуари). Що ще важливіше, 73,8% відкликаних класу I стосувалися серцево-судинних та загальних лікарняних пристроїв, таких як дефібрилятори, монітори пацієнта та інфузійні насоси, для яких також повідомляється про найбільшу кількість летальних випадків, пов'язаних із пристроями.

У багатьох випадках ланцюжок подій, що призводять до збоїв, неможливо визначити на основі обмеженої інформації, наданої в описах відкликаних. Однак, розглядаючи приклади важливих для безпеки збоїв (наприклад, апаратний дефект, який може призвести до впорскування гарячої рідини в тіло пацієнта) можна бачити, що багато відкликаних пристроїв були або розроблені без виявлення та вирішення проблем безпеки, або механізми безпеки були розроблені/впроваджені неправильно.

Деякі залишкові несправності/помилки можуть уникнути навіть найсуворішого аналізу ризиків, проектування та процесів перевірки та проявлятися у вигляді збоїв і непередбачених небезпек під час роботи пристрою. Наприклад, якщо розглянути дефект інтегральної плати, який може призвести до

впорскування гарячої рідини в тіло пацієнта. Такі катастрофічні збої, ймовірно, викликані кутовими випадками, які важко перевірити, і їх можна запобігти за допомогою перевірки на основі впровадження помилок і формального моделювання ключових режимів збою системи. У [26] показано, що символічне впровадження помилок є успішним у виявленні кутових випадків, які можуть уникнути виявлення помилок у критичному для безпеки програмному забезпеченні управління повітряним рухом.

Крім того, збої можна виявити під час виконання, перш ніж призвести до небезпечних ситуацій, використовуючи такі методи, як твердження під час виконання, сторожові таймери, механізми самоперевірки та періодичні перевірки системи (наприклад, для критичних частин, таких як батареї, датчики, процесор і пам'ять). Дослідження, описане в [27], демонструє використання статичного програмного аналізу для розробки специфічних для програми тверджень часу виконання для виявлення помилок даних, що призводять до збоїв із високим охопленням за дуже низькою ціною.

Повне видалення пристрою може бути неприйнятним варіантом усунення несправностей пристрою через високу вартість для виробників, засобів користувача та пацієнтів. У сучасних обчислювальних системах використовуються багато добре зрозумілих механізмів захисту від відмов і методів відновлення після збоїв, які можна використовувати в медичних пристроях, щоб управляти відмовами з меншими витратами. Наприклад, збої акумулятора або апаратного забезпечення, що призводять до втрати живлення та неочікуваних завершень роботи можна керувати шляхом вимкнення живлення невикористовуваних компонентів системи та підтримки живлення критичних частин, щоб уникнути раптових відключень електроенергії (наприклад, сплячі режими використовуються в сучасних вбудованих системах, таких як мобільні телефони).

Також такі методи, як локалізація несправностей (використовуються в аерокосмічних і комерційних системах), можуть бути використані для ізоляції несправних блоків або компонентів (наприклад, пошкоджених батарей) і

переведення системи в безвідмовний режим, не завдаючи шкоди пацієнтам/користувачам. Можна застосувати інтелектуальну стратегію реконфігурації для перемикавання на резервні батареї або резервні апаратні блоки у разі збою. Наприклад, неконтрольований рух пристрою не можна було зупинити навіть ручним відключенням живлення, оскільки пристрій автоматично перемикався на резервний акумулятор.

У цьому випадку визначення типу несправності та причини втрати живлення (навмисної чи випадкової) до прийняття рішення про перемикавання на резервну батарею може зупинити ненавмисне переміщення та потенційне травмування пацієнта.

Слід зазначити, що на сьогоднішній день діагностичні механізми недостатньо повні, щоб правильно визначити причини несправностей і системних помилок під час операції. Таким чином, інформація про тип системної помилки (наприклад, у стані помилки, яку можна відновити або не підлягає відновленню) і відповідні процедури усунення несправностей можуть бути неадекватними або неправильно передані хірургічній групі. Основні причини часто визначаються лише постфактум, коли інженери з обслуговування на місцях проводять додаткові дослідження та повторюють сценарії збою. Наприклад, про несправність кодера або датчика було повідомлено як про виправну системну помилку під час процедури, коли її не можна було відновити та можна було виправити лише заміною компонента після процедури (наприклад, звіт MAUDE 3035720).

Системні оператори (включно з хірургами, асистентами хірургів та інженерами польового обслуговування) часто недостатньо навчені правильно тлумачити причини спостережуваних системних помилок і вибирати ефективні дії з усунення несправностей для відновлення після надзвичайних ситуацій. Наприклад, в одному випадку було повідомлено, що хірургічна бригада витратила значну кількість часу на усунення невіправної системної помилки, коли пацієнт перебував під анестезією більше однієї години.

3.3 Результати аналізу даних про дефекти медичних виробів в кіберфізичній системі виявлення дефектів медичних виробів

Збої апаратного забезпечення, батареї та вводу-виводу мали більший вплив (вплинули на 6,5 мільйонів, 54% відкликаних пристроїв на ринку) з точки зору кількості пристроїв, які постраждали від відкликань (майже втричі) та вартості видалення пристроїв /ремонт. З усіх критично важливих для безпеки відкликань 80,7% стосувалися пристроїв, що використовуються в радіології (наприклад, лінійні прискорювачі), серцево-судинних (наприклад, автоматичні зовнішні дефібрилятори), загальних лікарнях (наприклад, інфузійні насоси), анестезіології (наприклад, вентилятори) та загальна хірургія (наприклад, електрохірургічні аксесуари). Що ще важливіше, 73,8% відкликань класу I стосувалися серцево-судинних та загальних лікарняних пристроїв, таких як дефібрилятори, монітори пацієнта та інфузійні насоси, для яких також повідомляється про найбільшу кількість летальних випадків, пов'язаних із пристроями. У багатьох випадках ланцюжок подій, що призводять до збоїв, неможливо визначити на основі обмеженої інформації, наданої в описах відкликань. Однак, розглядаючи приклади важливих для безпеки збоїв, досліджених тут (наприклад, апаратний дефект, який може призвести до впорскування гарячої рідини в тіло пацієнта, ми бачимо, що багато відкликаних пристроїв були або розроблені без виявлення та вирішення проблем безпеки, або механізми безпеки були розроблені/впроваджені неправильно.

Однак традиційні методи аналізу безпеки, рекомендовані FDA [23] і зазвичай використовуються в промисловості (включаючи аналіз дерева відмов (FTA) [10], аналіз дерева подій [24], дослідження небезпеки та працездатності (HAZOP) [25]) і методи аналізу надійності (наприклад, аналіз режиму та наслідків відмови (FMEA) [11]), здебільшого зосереджені на надійності окремих компонентів у системі або виконанні імовірнісної оцінки ризику. Ці методи мають обмежені можливості щодо виявлення інших факторів, що сприяють безпеці системи, таких як складні помилки програмного забезпечення, збої взаємодії

компонентів, людські помилки, складне прийняття рішень людиною та недосконале управління в проекті [12]. Наприклад, перший відклик було спричинено збоєм взаємодії між пристроєм та інструментом, через що інструмент не працював і становив ризик ускладнень під час операції. Це можна вважати небезпечною ситуацією, яка не була передбачена на етапі аналізу безпеки.

У [12] пропонується нова техніка аналізу небезпек, яка називається системним теоретичним аналізом процесів (STPA), для безпечного проектування складних програмно-інтенсивних систем. Цей метод розглядає процес проектування як проблему оптимізації управління, а не як проблему відмови компонента. Небезпечні ситуації запобігаються/пом'якшуються шляхом створення обмежень безпеки на основі виявлення потенційно небезпечних дій керування в системі та модифікації конструкції для усунення впливу недоліків керування.

З розглянутих тут прикладів відкликань стає зрозуміло, що деякі залишкові несправності/помилки можуть уникнути навіть найсуворішого аналізу ризиків, проектування та процесів перевірки та проявлятися у вигляді збоїв і непередбачених небезпек під час роботи пристрою. Наприклад, розглянемо дефект інтегральної плати, який може призвести до впрорскування гарячої рідини в тіло пацієнта. Такі катастрофічні збої, ймовірно, викликані кутовими випадками, які важко перевірити, і їх можна запобігти за допомогою перевірки на основі впровадження помилок і формального моделювання ключових режимів збою системи. У [26] показано, що символічне впровадження помилок є успішним у виявленні кутових випадків, які можуть уникнути виявлення помилок у критичному для безпеки програмному забезпеченні управління повітряним рухом.

Повне видалення пристрою може бути неприйнятним варіантом усунення несправностей пристрою через високу вартість для виробників, засобів користувача та пацієнтів. У сучасних обчислювальних системах використовуються багато добре зрозумілих механізмів захисту від відмов і методів відновлення після збоїв, які можна використовувати в медичних пристроях, щоб управляти відмовами з меншими витратами. Наприклад, збої

акумулятора або апаратного забезпечення, що призводять до втрати живлення та неочікуваних завершень роботи можна керувати шляхом вимкнення живлення невикористовуваних компонентів системи та підтримки живлення критичних частин, щоб уникнути раптових відключень електроенергії (наприклад, сплячі режими використовуються в сучасних вбудованих системах, таких як мобільні телефони).

Також такі методи, як локалізація несправностей (використовуються в аерокосмічних і комерційних системах), можуть бути використані для ізоляції несправних блоків або компонентів (наприклад, пошкоджених батарей) і переведення системи в безвідмовний режим, не завдаючи шкоди пацієнтам/користувачам. Можна застосувати інтелектуальну стратегію реконфігурації для перемикавання на резервні батареї або резервні апаратні блоки у разі збою. Наприклад, неконтрольований рух пристрою не можна було зупинити навіть ручним відключенням живлення, оскільки пристрій автоматично перемикався на резервний акумулятор. У цьому випадку визначення типу несправності та причини втрати живлення (навмисної чи випадкової) до прийняття рішення про перемикавання на резервну батарею може зупинити ненавмисне переміщення та потенційне травмування пацієнта.

Механізми FDA для звітування про відкликання та несприятливі події виробниками можуть допомогти запобігти майбутнім несприятливим подіям завдяки урокам, отриманим із попередніх проблем. Однак поточні бази даних FDA для звітів про відкликання та несприятливі події страждають від заниження, неточностей і невідповідностей, що у багатьох випадках ускладнює визначення причин несправностей та їх впливу на пацієнтів, щоб визначити, як можна покращити дизайн майбутніх пристроїв. Нижче наведено рекомендації, засновані на дослідженні щодо того, як можна покращити механізми звітності:

1. Надання надійних і систематичних інтерфейсів для звітування про відкликання та несприятливі події, щоб більш точна та повна інформація (наприклад, *Назва пристрою, код продукту, і Проблема з продуктом*) вноситься до звітів.

2. Список ключових слів, що представляють різні *Проблеми з продуктом* в базі даних MAUDE [1] точніше відображає причини збоїв пристроїв, особливо пов'язаних з комп'ютером.

3. Створення інтегрованих баз даних про відкликання та несприятливі події, щоб: *Назва продукту* і *Причина відкликання* поля кожного запису про відкликання відповідають стандарту назви пристроїв, коди продуктів і категорії пристроїв, визначені FDA. Записи про відкликання можна перехресно посилати на відповідні звіти про несприятливі події в MAUDE бази даних.

Аналіз даних про несприятливі події дає цінну інформацію про можливі небезпеки системи та може бути використаний для підвищення безпеки системи з метою запобігання майбутнім інцидентам, спричиненим несправністю медичних пристроїв. Проте традиційні методи моделювання та аналізу нещасних випадків (наприклад, аналіз першопричини, який зазвичай використовується в медицині), як правило, зосереджені на прямих причинно-наслідкових зв'язках між подіями, що призвели до нещасного випадку (на основі ланцюжків подій або моделей швейцарського сиру [51]) і часто роблять висновок: суб'єктивний акцент на одній (основній) причині, наприклад, збої фізичних пристроїв або людські помилки. Інші причинно-наслідкові та контекстуальні фактори та основні умови, які опосередковано сприяють несприятливим подіям, у таких аналізах не враховуються ретельно; наприклад, небезпечна взаємодія між компонентами системи та людьми-операторами; неточні оператори ментальні моделі системи; або обставини (стани системи), за яких здійснюються дії або приймаються рішення [12]. Тому цих підходів часто недостатньо для розуміння всіх причин, що сприяють нещасним випадкам у сучасних складних медичних системах [52] – [54], а рекомендації, зроблені на основі такого аналізу, часто не підвищують безпеку, і подібні нещасні випадки повторюються.

Теоретико-системні моделі причинно-наслідкових зв'язків аварій, такі як STAMP (теоретико-системна модель аварій і процеси) [12], долають це обмеження шляхом моделювання аварій як складних динамічних процесів, що є результатом неадекватних механізмів контролю, які порушують обмеження

безпеки. Керуючись концепціями систем і теорій управління, STAMP забезпечує структуру моделювання для аналізу небезпек і розслідування нещасних випадків і застосовується в кількох критично важливих для безпеки сферах, таких як авіація [55], медичне обладнання [56], [57], автомобільна [58] , [59] та транспорт [60], [61].

Можна використати структуру моделювання STAMP для аналізу несприятливих подій у критично важливих для безпеки медичних пристроях. Щоб полегшити теоретико-системний аналіз великих наборів звітів про несприятливі події, ми пропонуємо нову онтологічну модель, засновану на структурах управління людиною в циклі, щоб керувати.

3.4 Висновки

Охарактеризувавши причини комп'ютерних збоїв та їхній вплив на пацієнтів, а також визначити найпоширеніші типи критично важливих для безпеки комп'ютерних медичних пристроїв, які були задіяні в життєво важливих інцидентах. Незважаючи на те, що значна частина нашого аналізу включала ручний перегляд даних про відкриття та несприятливі події, отримані комп'ютерні відкриття можна використовувати як навчальний набір для автоматизації аналізу нових даних, поданих до баз даних FDA.

4 КІБЕРФІЗИЧНА СИСТЕМА ВИЯВЛЕННЯ ДЕФЕКТІВ МЕДИЧНИХ ВИРОБІВ

4.1 Розроблення кіберфізичної системи виявлення дефектів медичних виробів

Кіберфізична система виявлення дефектів медичних виробів – це система, яка використовується для моніторингу та контролю якості роботи медичних приладів. Вона складається з апаратного та програмного забезпечення, що дозволяє автоматично виявляти дефекти та відхилення у роботі медичних приладів.

Основна ідея полягає в тому, що система стежить за параметрами роботи медичного приладу, зчитує дані з його датчиків та аналізує їх, щоб виявити будь-які аномалії та відхилення у роботі. Якщо система виявляє якісь проблеми, то вона може надіслати сповіщення або запустити автоматичний процес відновлення роботи приладу.

Основні компоненти кіберфізичної системи виявлення дефектів медичних приладів можуть включати в себе:

Датчики, які вимірюють різні параметри медичних приладів, такі як температура, тиск, вологість і т.д.

Програмне забезпечення, яке аналізує дані з датчиків і виявляє можливі дефекти.

Комунікаційні пристрої, що забезпечують зв'язок між системою виявлення дефектів і медичним приладом, включаючи мережі Інтернет вещей (IoT).

Інтерфейс користувача, який дозволяє медичному персоналу отримувати інформацію про стан медичного приладу і при необхідності приймати відповідні заходи.

Кіберфізична система виявлення дефектів медичних приладів може бути використана в різних медичних закладах, таких як лікарні, клініки, стоматологічні кабінети тощо. Вона дозволяє підтримувати медичні прилади у відповідному стані і запобігати можливим проблемам з їх функціонуванням.

Архітектура кіберфізичної системи виявлення дефектів медичних приладів може включати наступні компоненти:

Датчики та інструменти збору даних: Цей компонент відповідає за збір фізичних даних з медичних приладів, таких як температура, вологість, тиск тощо. Ці дані збираються за допомогою датчиків, що встановлюються на медичних приладах.

Програмне забезпечення з аналітикою даних: Цей компонент відповідає за аналіз даних, отриманих від датчиків, з метою виявлення можливих дефектів медичного приладу. Програмне забезпечення може використовувати аналітичні алгоритми та інтелектуальні методи для аналізу даних.

Модуль комунікації: Цей компонент відповідає за забезпечення зв'язку між датчиками, програмним забезпеченням та іншими системами. Він може використовувати бездротові технології, такі як Bluetooth або Wi-Fi, для передачі даних.

Система моніторингу та управління: Цей компонент відповідає за моніторинг стану медичного приладу і виявлення можливих дефектів. Він також може надавати можливість для віддаленого управління медичним приладом. Інтерфейс користувача: Цей компонент відповідає за взаємодію з користувачем, наприклад, з медичним персоналом. Він може включати в себе веб-інтерфейси, мобільні додатки та інші засоби відображення даних та керування медичними приладами.

Усі компоненти кіберфізичної системи виявлення дефектів медичних приладів мають взаємодіяти між собою.

У загальному розумінні, функціонування кіберфізичної системи виявлення дефектів медичних приладів можна умовно поділити на наступні кроки:

1. Збір та аналіз даних про параметри роботи медичного приладу за допомогою датчиків та інших вимірювальних пристроїв.
2. Обробка та аналіз отриманих даних за допомогою програмного забезпечення системи.

3. Виявлення аномалій та відхилень у роботі медичного приладу, порівняння отриманих даних з заданими нормами роботи приладу.

4. Вирішення проблем шляхом запуску автоматичного процесу відновлення роботи приладу або надіслання сповіщення користувачеві про необхідність його ремонту або заміни.

5. Моніторинг та контроль якості роботи медичного приладу в режимі реального часу.

Застосування кіберфізичної системи виявлення дефектів медичних приладів може допомогти зменшити кількість некоректної роботи медичних приладів і тим самим покращити якість медичних послуг. Наприклад, система може виявити ранні ознаки проблем з медичним приладом, що дозволить вчасно провести ремонт або заміну. Також, система може допомогти у виявленні проблем з електронними компонентами медичних приладів, що може запобігти їх перегріванню та випадковому відключенню, що може призвести до серйозних наслідків для пацієнтів. В цілому, застосування кіберфізичних систем виявлення дефектів медичних приладів допомагає забезпечити безпеку та ефективність медичної техніки.

Розглянемо більш детально описані кроки функціонування кіберфізичної системи виявлення дефектів медичних приладів.

Збір та аналіз даних про параметри роботи медичного приладу є ключовим етапом у функціонуванні кіберфізичної системи виявлення дефектів медичних приладів. Для збору даних про роботу медичного приладу використовуються датчики, які вимірюють різні параметри, такі як тиск, температура, швидкість потоку, вібрації, рівень шуму та інші.

Зібрані дані передаються до кіберфізичної системи виявлення дефектів медичних приладів для подальшого аналізу. Для аналізу використовуються алгоритми машинного навчання та інші методи аналізу даних. За допомогою цих методів можна виявити аномальні поведінки приладу та потенційні проблеми, що можуть призвести до відмови приладу.

Крім того, аналіз даних може допомогти виявити шаблони роботи приладу, що можуть бути корисними для розробки алгоритмів виявлення дефектів та покращення ефективності медичного приладу.

Отже, збір та аналіз даних про параметри роботи медичного приладу є важливим етапом у функціонуванні кіберфізичної системи виявлення дефектів медичних приладів, який допомагає вчасно виявляти можливі проблеми та покращувати ефективність приладу.

Обробка та аналіз отриманих даних є важливим етапом у функціонуванні кіберфізичної системи виявлення дефектів медичних приладів. Дані, що збираються з датчиків та інших вимірювальних пристроїв, потрібно обробляти, аналізувати та інтерпретувати, щоб виявити можливі дефекти або проблеми у роботі медичного приладу.

Програмне забезпечення кіберфізичної системи виявлення дефектів медичних приладів може мати різноманітні алгоритми для обробки даних. Наприклад, можна використовувати алгоритми статистичного аналізу, машинного навчання, штучного інтелекту, аналізу спектру частот або кореляційного аналізу. Кожен з цих методів може допомогти виявити різні типи дефектів або проблем у роботі медичного приладу.

Після обробки та аналізу даних програмне забезпечення може виконувати різні дії, залежно від виявлених дефектів або проблем. Наприклад, система може автоматично відключити медичний прилад, щоб уникнути можливих небезпек для пацієнтів. Або ж система може надіслати повідомлення технічному персоналу про необхідність виконати ремонт або заміну деталей. Крім того, дані, що збираються та аналізуються системою виявлення дефектів, можуть бути використані для вдосконалення самого медичного приладу. Наприклад, на основі отриманих даних можуть бути внесені зміни в дизайн медичного приладу або в технології його виробництва для запобігання дефектів та поліпшення якості роботи приладу.

Виявлення аномалій та відхилень у роботі медичного приладу є однією з основних функцій кіберфізичної системи виявлення дефектів медичних приладів. Після збору та обробки даних за допомогою датчиків та інших вимірювальних

пристроїв, програмне забезпечення кіберфізичної системи проводить аналіз отриманих даних та порівнює їх з заданими нормами роботи приладу.

Якщо виявлено аномалії або відхилення від заданих норм, кіберфізична система виявлення дефектів медичних приладів генерує спеціальний сигнал або повідомлення, що попереджає оператора про можливі проблеми з роботою приладу. Далі оператор може провести додаткову діагностику та ремонт медичного приладу. Цей процес автоматизованої діагностики та контролю допомагає запобігти некоректній роботі медичних приладів та забезпечити їх безперебійну роботу в умовах реального застосування.

Так, кіберфізична система виявлення дефектів медичних приладів може автоматично вирішувати проблеми, які виявляються під час моніторингу роботи приладу. Якщо система виявляє відхилення від нормальної роботи приладу, вона може запустити автоматичний процес відновлення його роботи, який може включати в себе різні дії, наприклад перезавантаження приладу або відновлення заводських налаштувань. У випадку, якщо проблема не може бути вирішена автоматично, кіберфізична система може надіслати повідомлення користувачеві про необхідність ремонту або заміни приладу. Це дозволить запобігти небезпеці для пацієнтів і зменшити час, необхідний для усунення проблеми.

Моніторинг та контроль якості роботи медичного приладу в режимі реального часу є важливим етапом в процесі функціонування кіберфізичної системи виявлення дефектів медичних приладів. Цей процес дозволяє виявляти можливі проблеми з роботою приладу в ранніх стадіях, що дозволяє швидко вжити необхідних заходів для їх усунення.

Для моніторингу та контролю якості роботи медичного приладу в режимі реального часу в кіберфізичній системі використовуються спеціальні датчики та вимірювальні пристрої, які забезпечують збір даних про параметри роботи приладу. Отримані дані аналізуються за допомогою спеціального програмного забезпечення, що дозволяє виявляти можливі проблеми з роботою приладу в режимі реального часу.

У разі виявлення аномалій чи відхилень від заданих норм роботи приладу, система автоматично запускає процес відновлення роботи приладу або надсилає сповіщення користувачеві про необхідність його ремонту або заміни. Такий моніторинг та контроль якості роботи медичного приладу дозволяє забезпечити безперебійну та надійну роботу приладу, а також збільшити термін його експлуатації.

Програмне забезпечення кіберфізичної системи виявлення дефектів медичних приладів складається з наступних компонентів:

1. Драйвери пристроїв: програмні засоби, що забезпечують зв'язок з фізичними датчиками та вимірювальними приладами для збору даних про параметри роботи медичного приладу.

2. База даних: це компонент, що забезпечує збереження зібраних даних про параметри роботи медичного приладу та інформації про норми роботи приладу.

3. Алгоритми обробки даних: це компонент, що забезпечує обробку зібраних даних та порівняння їх з заданими нормами роботи медичного приладу.

4. Модуль аналізу даних: це компонент, що забезпечує виявлення аномалій та відхилень у роботі медичного приладу, порівняння отриманих даних з заданими нормами роботи приладу.

5. Модуль управління: це компонент, що забезпечує автоматичний процес відновлення роботи приладу або надсилання сповіщення користувачеві про необхідність його ремонту або заміни у разі виявлення дефектів або відхилень в роботі медичного приладу.

6. Модуль моніторингу та контролю якості: це компонент, що забезпечує моніторинг та контроль якості роботи медичного приладу в режимі реального часу.

Загалом, програмне забезпечення кіберфізичної системи виявлення дефектів медичних приладів повинно забезпечувати надійний та ефективний збір та аналіз даних про параметри роботи медичного приладу, виявлення аномалій та

відхилень у роботі приладу, та автоматичне вирішення проблем з роботою приладів.

Драйвери пристроїв, які використовуються в кіберфізичних системах виявлення дефектів медичних приладів, залежать від конкретного медичного приладу та його виробника. Зазвичай виробники медичних приладів надають драйвери для своїх пристроїв, які можна використовувати у кіберфізичних системах. Однак, також можуть використовуватися стандартні драйвери, які підтримують загальноживані комунікаційні протоколи, такі як USB, Bluetooth, Wi-Fi та інші. Залежно від конкретної кіберфізичної системи та її функціональних можливостей, можуть використовуватися різні драйвери та комунікаційні протоколи.

Алгоритми обробки даних про дефекти медичних приладів можуть варіюватися залежно від конкретної кіберфізичної системи виявлення дефектів. Однак, деякі загальні алгоритми можуть бути використані для аналізу та класифікації дефектів:

1. Аналіз статистичних даних. Даний алгоритм використовує статистичні методи для аналізу отриманих даних про дефекти. За допомогою статистичного аналізу можна виявити шаблони у даних та визначити типи дефектів, які найчастіше відбуваються.

2. Машинне навчання: Деякі кіберфізичні системи виявлення дефектів можуть використовувати алгоритми машинного навчання для класифікації дефектів. За допомогою цих алгоритмів можна навчити систему відрізняти різні типи дефектів та автоматично виявляти їх у майбутньому.

3. Аналіз вібрації. Деякі кіберфізичні системи можуть використовувати датчики вібрації для аналізу роботи медичних приладів. За допомогою аналізу вібрації можна виявити дефекти, пов'язані з нестабільною роботою механічних деталей.

4. Аналіз електричних сигналів. Деякі кіберфізичні системи можуть використовувати аналіз електричних сигналів для виявлення дефектів медичних приладів. Наприклад, за допомогою аналізу електричних сигналів можна виявити

переривання електричних контактів або нестабільну роботу електронних компонентів.

5. Аналіз зображень. Деякі кіберфізичні системи можуть використовувати аналіз зображень для виявлення дефектів медичних приладів, які мають оптичні частини або використовують зображення для діагностики. Алгоритми обробки зображень можуть використовувати методи комп'ютерного зору, щоб автоматично визначати розмір, форму та кількість дефектів на зображеннях.

Наприклад, цей підхід може бути використаний для виявлення дефектів на рентгенівських знімках, мамографічних зображеннях або зображеннях ультразвукової діагностики. Алгоритми обробки зображень можуть використовувати нейронні мережі для автоматичного виявлення аномалій на зображеннях та повідомлення оператора про потенційні дефекти.

Також, кіберфізичні системи можуть використовувати терміновий аналіз зображень для виявлення дефектів, які можуть призвести до аварії медичного приладу. Наприклад, терміновий аналіз зображень може бути використаний для виявлення проблем з терморегулюванням відповідних компонентів приладу, таких як датчики температури.

Архітектура підсистеми керування кіберфізичною системою виявлення дефектів медичних виробів буде реалізовано з набором датчиків, які отримують зворотний зв'язок/дані про навколишнє середовище від закладу охорони здоров'я. Аналізовані дані подаються в механізм керування, щоб визначити, наскільки показання відхиляються від очікуваних значень.

Коригування потім можуть бути подані на відповідні приводи для внесення коригувань у фізичне середовище перед тим, як відбулися додаткові показання датчика. На рисунку 4.1 представлена архітектура підсистеми керування кіберфізичною системою виявлення дефектів медичних виробів.

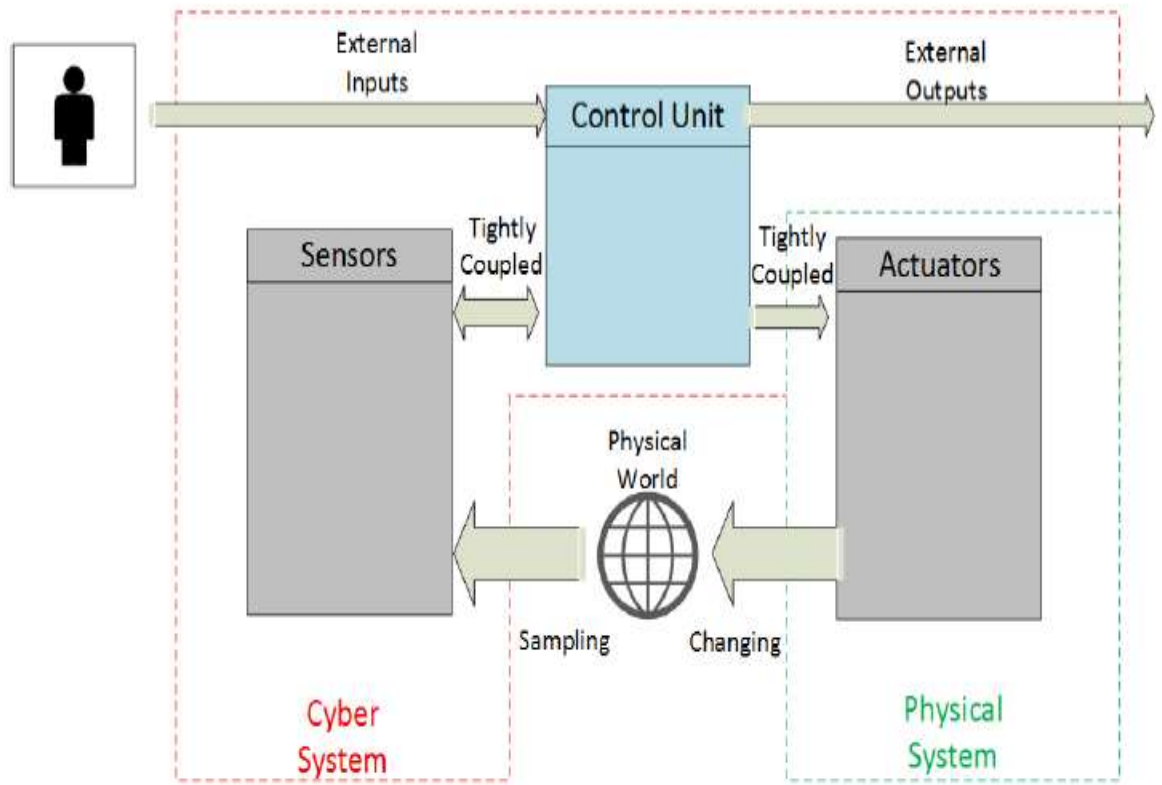


Рисунок 4.1 – Архітектура підсистеми керування кіберфізичною системою виявлення дефектів медичних виробів

В літературі така багаторівнева архітектура описана на двох різних рівнях. Перший з них починається з фізичного рівня та просувається до датчиків, вузлів-приймачів, які збирають цю групу пов'язані зчитування датчиків і контрольні вузли, які збирають і групують події з вузлів-приймачів. Другий Опис розглядається на більш високому рівні, зазвичай описуючи більшу частину інфраструктури датчиків як одну рівень, створення локальних подій як другий рівень, а також хмарна інфраструктура та програми, які взаємодіють з це як один або декілька вищих рівнів.

На рисунку 4.2 показаний один із запропонованих варіантів багаторівневої архітектури кіберфізичної системи виявлення дефектів медичних приладів.

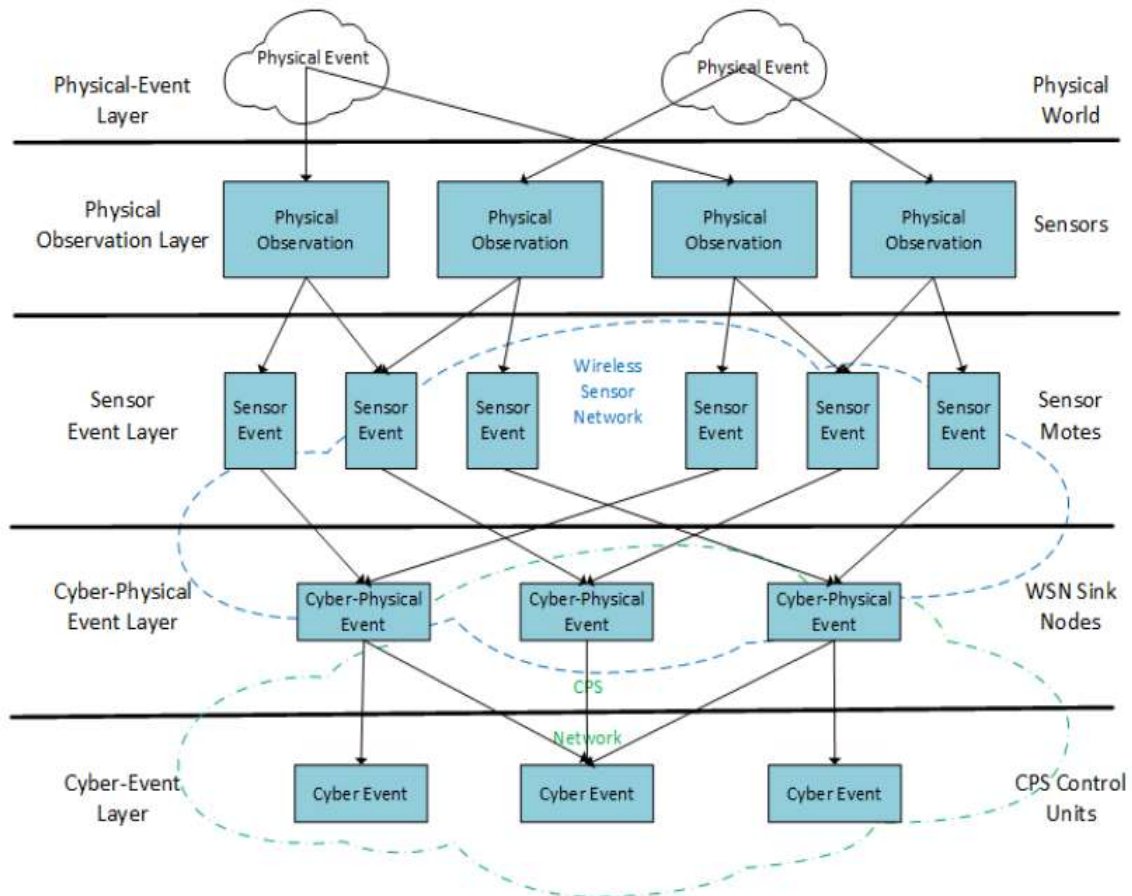


Рисунок 4.2 – Структурна схема рівнів кіберфізичної системи виявлення дефектів медичних виробів

Надлишкові вузли на нижчому рівні можуть повідомляти дані, які потім можна спільно аналізувати для покращення рівня достовірності виявлених показань. Потім ці надлишки можуть бути видалені. Реактивність є одним з головних недоліків багаторівневих підходів, коли своєчасність може бути проблемою. Така архітектура мало що надає для визначення того, що буде зроблено для врахування таких дій і що має бути виконано в результаті події. Можна припустити, що запит на дію високого рівня може бути відправлений на рівень нижче для повторного розкладання. Те саме можна сказати про події, які вимагають негайної дії, але мають бути передані ще кілька рівнів, перш ніж ініціюється фактична відповідь. Багатошарова архітектура буде боротися з мобільністю вузлів. Поєднання спостережень перед відправленням на вищі рівні стає складною задачею, оскільки датчики рухаються в середовищі. Щоб це

працювало належним чином, об'єднання показань датчиків може бути дозволено перенести між рівнями архітектури або тягар обробки в основному локальних подій може проводитися на глобальному рівні, фактично усуваючи будь-які переваги багаторівневої архітектури. Зазвичай спостерігається поєднання спостережень на нижчих рівнях перед відправленням на вищі рівні у багаторівневій архітектурі пропонує механізм для створення надійності в архітектурі. Зайві вузли нижчого рівня можуть повідомляти дані, які потім можна спільно аналізувати для підвищення довіри.

4.2 Функціонування кіберфізичної системи виявлення дефектів медичних виробів

Існує безліч програмних платформ, які можуть бути використані для розробки кіберфізичних систем виявлення дефектів медичних приладів. Ось декілька прикладів:

LabVIEW – це програмна платформа для розробки систем збору даних та контролю процесів, що використовується в багатьох галузях, включаючи медицину. LabVIEW надає інструменти для розробки кіберфізичних систем виявлення дефектів медичних приладів.

MATLAB – це програмна платформа для наукових обчислень та аналізу даних, яка також може бути використана для розробки кіберфізичних систем виявлення дефектів медичних приладів. MATLAB надає багато інструментів для роботи з сигналами та даними, які можуть бути корисні для аналізу даних з медичних приладів.

Python – це популярна мова програмування, яка часто використовується для розробки кіберфізичних систем. Python має багато бібліотек для аналізу даних та машинного навчання, які можуть бути корисні для розробки систем виявлення дефектів медичних приладів.

R – це інша мова програмування для аналізу даних та статистики, яка може бути використана для розробки кіберфізичних систем виявлення дефектів

медичних приладів. R має багато бібліотек для аналізу даних та візуалізації результатів, що може бути корисно для аналізу даних з медичних приладів. Ці програмні платформи не є єдиними варіантами для розробки кіберфізичних систем виявлення дефектів медичних приладів, проте вони є досить популярними та мають багато інструментів та бібліотек.

Кіберфізичні системи виявлення дефектів медичних приладів можуть стати об'єктом кібератак або вразливостей в захисті даних.

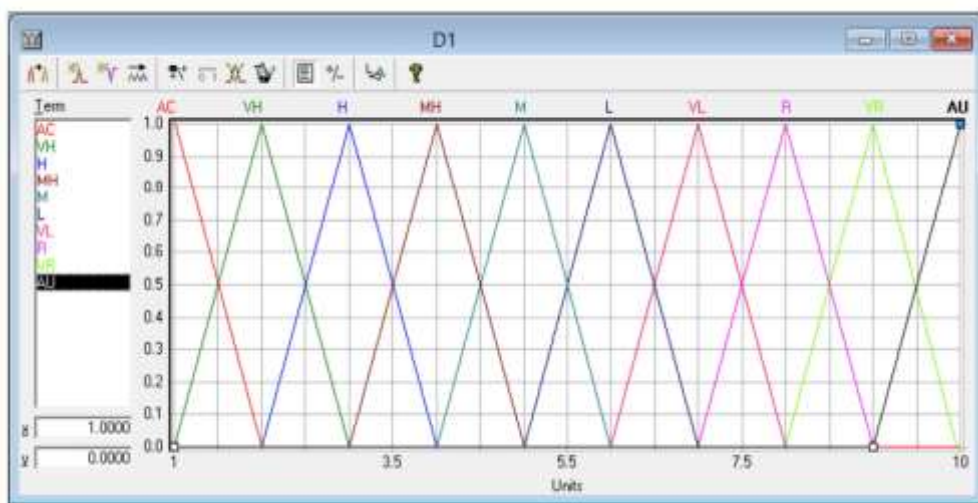


Рисунок 4.3 – Функції належності для опису дефектів медичних приладів

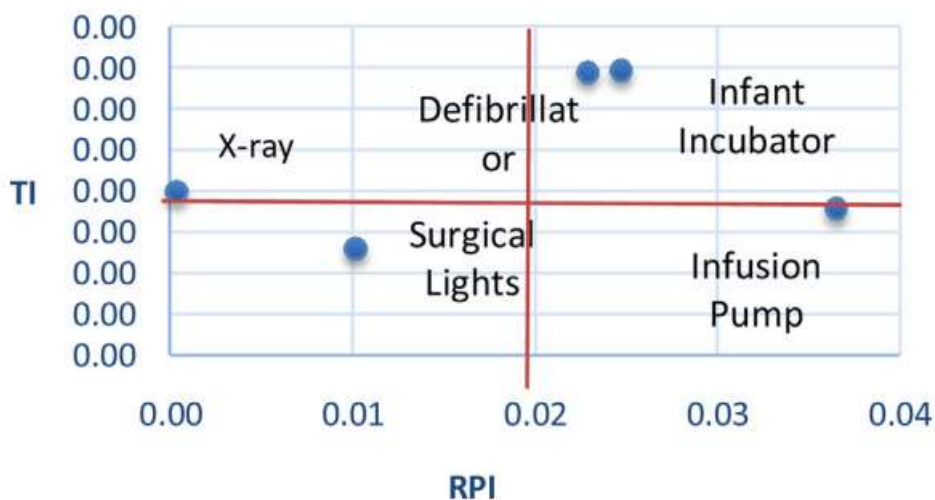


Рисунок 4.4 – Діаграма опису дефектів медичних приладів

У наших експериментах визначені сценарії загрози безпеці (небезпечні керуючі дії та причинні фактори) з аналізу небезпек STPA використовувалися в поєднанні зі знаннями про структуру програмного коду для розробки стратегій ін'єкції помилок. Зокрема, ми зіставили ідентифіковані причинні фактори в кожному циклі структури керування системою з відповідними програмними модулями та функціями, які повинні бути націлені на впровадження помилок. Щоб підвищити ймовірність активації загроз безпеці в системі, ми вручну визначили змінні в кожній програмній функції, на яку потрібно націлити, значення для введення та умови для запуску ін'єкцій. Ми виконали обмежені випадкові ін'єкції до змінних, що відповідають керуючій дії, зворотному зв'язку, моделі процесу та алгоритмам у кожному контурі керування.

Було змодельовано загалом 45 сценаріїв шляхом введення несправностей у 25 місць у межах 13 програмних функцій мережі та потоків керування робота RAVEN II під час виконання попередньо зібраної траєкторії хірургічного руху.

Показує приклади сценаріїв, коли помилки виявлялися в системі. Загалом ми провели 2146 експериментів з ін'єкцією помилок на роботі RAVEN. Однак більшість помилок (наприклад, введені значення в межах діапазону змінних) не проявлялися в системі, або їх вплив не було повністю зареєстровано процесом збору даних через зависання/збої системи (наприклад, апаратне забезпечення «E- STOP»), спричинених несправностями. Для кожного сценарію ми провели кілька прогонів (загалом 368 ін'єкцій помилок), щоб отримати впевненість у відтворюваності проявленої/спостережуваної поведінки системи, і вручну зібрали результати (див. Таблицю 4.2). У кожному випадку ми аналізували поведінку системи як під час процесу приведення (яка система ініціалізується, а маніпуляції користувачем ще не почалися), так і після переведення. Третій стовпець у таблиці показує кількість експериментів, проведених для кожного сценарію, а останній стовпець відповідає ідентифікатору сценарію. Повний список причинно-наслідкових сценаріїв доступний за адресою [59].

Наростаюча складність підключення медичних кіберфізичних систем, їх швидке розгортання в лікарнях і широке використання в різноманітних

клінічних умовах роблять їх стійкість (тобто їх здатність підтримувати прийнятний рівень безпечної роботи), незважаючи як на випадкові збої, так і на зловмисні атаки. складне завдання. Багато нещодавніх звітів свідчать про існування вразливостей у конфігурації лікарняних мереж сторонніх мереж (наприклад, лабораторій і аптек) пристроїв, якими користуються працівники лікарні (охорона здоров'я). професіонали та технічні спеціалісти) та медичні пристрої без латок, які можуть дозволити зловмисникам проникнути в мережі лікарень і потенційно отримати несанкціонований доступ до критично важливих для безпеки медичних пристроїв.

В медичних кіберфізичних системах відмовостійкість найкраще досягається за допомогою:

1. Широкомасштабний аналіз минулих інцидентів, щоб покращити наше розуміння багатовимірних причин, пов'язаних з інцидентами, і отримати статистично достовірні показники їх впливу.

2. Експериментальна перевірка механізмів безпеки та захисту за наявності реалістичних сценаріїв загрози безпеки та атаки на безпеку.

3. Розробка механізмів для безперервного моніторингу людей-операторів, кібер- і фізичних станів системи, стану пацієнта та швидкого виявлення подій, які можуть призвести до порушень безпеки.

Відмовостійкість кіберфізичних систем виявлення дефектів медичних виробів є важливою проблемою, оскільки від цих систем залежить безпека і ефективність медичної діагностики та лікування. Ці системи використовуються для контролю якості та виявлення дефектів у медичних виробках, таких як медична апаратура, інструменти, протези, імплантати тощо.

Щоб забезпечити високу відмовостійкість кіберфізичних систем виявлення дефектів медичних виробів, необхідно вживати наступні заходи:

1. Надійна апаратна база. Кіберфізичні системи повинні мати надійну апаратну основу зі зменшеним ризиком відмов. Це означає використання якісних компонентів, резервних апаратних засобів та механізмів відновлення.

2. Захист від кібератак. Медичні вироби можуть стати метою кібератак, які можуть спотворити або перешкодити роботі системи виявлення дефектів. Важливо застосовувати заходи з кібербезпеки, такі як шифрування даних, аутентифікація користувачів та захист від несанкціонованого доступу.

3. Перевірка та калібрування. Кіберфізичні системи повинні проходити регулярну перевірку та калібрування для забезпечення їх правильної роботи. Це допомагає виявити можливі проблеми або відхилення у роботі системи та прийняти відповідні заходи.

4. Резервне копіювання та відновлення даних. Важливо регулярно резервувати дані, зібрані системою виявлення дефектів, і мати механізм відновлення даних в разі виникнення відмови. Це допомагає уникнути втрати даних та забезпечує безперебійну роботу системи.

5. Моніторинг та тривоги. Кіберфізичні системи повинні бути обладнані механізмами моніторингу, які дозволяють виявляти відхилення у роботі системи або показників виробів. Також варто встановлювати систему тривоги, яка негайно повідомлятиме про відмови або небажані події.

6. Навчання та підтримка персоналу. Важливо надати належне навчання персоналу, що використовує кіберфізичні системи виявлення дефектів. Це допоможе їм розуміти принципи роботи системи та правильно реагувати на відмови або небажані ситуації.

7. Стандарти та регуляторні вимоги. Враховуйте відповідні стандарти та регуляторні вимоги, що стосуються відмовостійкості медичних виробів.

8. Постійне оновлення: Слід постійно вдосконалювати кіберфізичні системи та враховувати нові технології, що допоможуть покращити їх відмовостійкість. Системи повинні бути гнучкими та готовими до змін для відповіді на зростаючі вимоги та загрози.

Дотримання цих вимог допомагає забезпечити високу якість та безпеку системи.

Загалом, відмовостійкість кіберфізичних систем виявлення дефектів медичних виробів є незворотною умовою для забезпечення безпеки та ефективності медичної практики.

Моніторинг стану медичних приладів: Кіберфізична система може постійно відслідковувати різні параметри роботи медичних приладів, такі як температура, тиск, електрична потужність тощо. В разі виявлення аномалій або виходу параметрів за допустимі межі, система може автоматично сповістити операторів або виконати певні заходи для запобігання можливим дефектам або аваріям.

Діагностика та аналіз даних: Кіберфізична система може збирати, аналізувати та інтерпретувати дані, що отримані з медичних приладів. Застосовуючи методи машинного навчання та штучного інтелекту, система може виявляти відхилення в роботі приладів, розпізнавати патологічні зміни в сигналах, виявляти потенційні дефекти та прогнозувати можливі проблеми.

Автоматичне управління: Кіберфізична система може мати можливість автоматично коригувати роботу медичних приладів на основі зібраних даних. Наприклад, якщо система виявляє, що певний параметр підвищує ризик дефекту, вона може змінювати налаштування приладу або запускати процедури самодіагностики та відновлення роботи.

Прогнозування та попередження: Кіберфізична система може використовувати аналітичні моделі та алгоритми для прогнозування можливих дефектів медичних приладів. На основі зібраних даних та знань про попередні випадки дефектів, система може виявляти ризикові ситуації та сповіщати про них, дозволяючи прийняти вчасні заходи для усунення проблем.

4.3 Висновки

Розглянуті приклади демонструють різноманітні можливості кіберфізичної системи виявлення дефектів медичних приладів. Її функціонування може включати контроль якісних характеристик виробу, виявлення зносу та відхилень в

роботі, ідентифікацію потенційних проблем з елементами конструкції, аналіз великого обсягу даних для виявлення взаємозв'язків та закономірностей, а також підтримку процесу прийняття рішень щодо ремонту, заміни або покращення медичних приладів.

ВИСНОВКИ

У роботі за результатами виконаних теоретичних та практичних досліджень розроблено кіберфізичну систему виявлення дефектів медичних виробів.

Отримані результати свідчать про ефективність системи у виявленні різноманітних дефектів, що сприяє поліпшенню безпеки та надійності медичного обладнання. Розроблена система має потенціал для використання у медичних закладах та сприяє покращенню якості надання медичних послуг. Кіберфізичні системи виявлення дефектів медичних приладів призначені для забезпечення надійності та безпеки використання медичної техніки. Вони дозволяють виявляти та діагностувати дефекти, несправності або зміни в роботі приладів, що можуть впливати на їх функціонування та результати медичних процедур. Це дозволяє оперативно реагувати на проблеми, попереджати виникнення аварійних ситуацій, підтримувати високу якість та ефективність медичних приладів, а також забезпечувати безпеку пацієнтів та медичного персоналу.

У першому розділі проведено огляд кіберфізичних систем, що використовуються в медичній галузі та існуючих рішень для виявлення дефектів медичних приладів, а також приведена класифікація дефектів медичних виробів.

У другому розділі представлено моделювання процесу виявлення дефектів медичних виробів, а також

У третьому розділі проведений аналіз даних процесу виявлення дефектів медичних приладів.

У четвертому розділі розглянуті приклади демонструють різноманітні можливості кіберфізичної системи виявлення дефектів медичних приладів. Її функціонування може включати контроль якісних характеристик виробу, виявлення зносу та відхилень в роботі, ідентифікацію потенційних проблем з елементами конструкції, аналіз великого обсягу даних для виявлення взаємозв'язків та закономірностей, а також підтримку процесу прийняття рішень щодо ремонту, заміни або покращення медичних приладів.

За темою кваліфікаційної роботи магістра опубліковані тези доповіді.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Abd Rahman N.H, Ibrahim A.K, Hasikin K, Abd Razak N.A. Critical Device Reliability Assessment in Healthcare Services. *J Healthc Eng.* 2023. Feb 20. 3136511. doi: 10.1155/2023/3136511. PMID: 36860328; PMCID: PMC9970731.
2. El Biyaali A., El Barkany A., Mahfoud H. Medical maintenance performance monitoring: a roadmap to efficient improvement. *International Journal of Productivity and Quality Management*. 2017. Vol. 22(1). P. 117. doi: 10.1504/IJPQM.2017.10006242.
3. Про затвердження методичних рекомендацій із застосування Технічного регламенту щодо медичних виробів, затвердженого постановою Кабінету Міністрів України від 02 жовтня 2013 року № 753: »: Наказ Міністерства охорони здоров'я України 22.01.2020 р. № 142.
4. Методичні рекомендації «Класифікація медичних виробів»: Наказ Міністерства охорони здоров'я України 22.01.2020 р. № 142.
5. Лікарські засоби управління ризиками для якості (ICH Q9) СТ-Н МОЗУ 42-4.2:2011: Настанови, Міністерство охорони здоров'я України. Київ. 2011.
6. Peter Feiler and Julien Delange. Automated Fault Tree Analysis from AADL Models. *ACM SIGAda Ada Letters*. Volume 36. Issue 2. 2017. Pp 39–46. <https://doi.org/10.1145/3092893.3092900>.
7. K. Batbayar, M. Takács and M. Kozlovsky Medical device software risk assessment using FMEA and fuzzy linguistic approach: Case study. *2016 IEEE 11th International Symposium on Applied Computational Intelligence and Informatics (SACI)*, Timisoara, Romania. 2016. Pp. 197-202, doi: 10.1109/SACI.2016.7507369.
8. FDA. Medical Devices. URL: <https://www.fda.gov/medical-devices> (дата звернення: 10.02.2023).
9. MAUDE – Manufacturer and User Facility Device Experience. URL: <https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfmaude/search.cfm> (дата звернення: 07.02.2023).

10. U.S. Food and Drug Administration, “Pulse Oximeters - Premarket Notification Submissions [510(k)s] - Guidance for Industry and FDA Staff,” Mar. 2013. [URL: http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm341718.htm](http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm341718.htm) (дата звернення: 07.02.2023).
11. Sametinger Johannes, et al. Security challenges for medical devices. *Communications of the ACM* 58.4. 2015. Pp. 74-82.
12. Neuman M. R., Baura G. D., Meldrum S., Soykan O., Valentinuzzi M. E., Leder, R. S., Zhang, Y. T. Advances in medical devices and medical electronics. *Proceedings of the IEEE, 100*(Special Centennial Issue). 2012. Pp. 1537-1550.
13. Bitkina Olga VI, Hyun K. Kim, and Jaehyun Park Usability and user experience of medical devices: An overview of the current state, analysis methodologies, and future challenges. *International Journal of Industrial Ergonomics* 76 (2020): 102932.
14. M. Kohani and M. Pecht, Malfunctions of Medical Devices Due to Electrostatic Occurrences Big Data Analysis of 10 Years of the FDA’s Reports, in *IEEE Access*, vol. 6, pp. 5805-5811, 2018, doi: 10.1109/ACCESS.2017.2782088.
15. Knisely Benjamin M., et al. An analysis of FDA adverse event reporting data for trends in medical device use error. *Proceedings of the International Symposium on Human Factors and Ergonomics in Health Care*. 2020. Vol. 9. No. 1. Sage CA: Los Angeles, CA: SAGE Publications.
16. Jalaj Pachouly, Swati Ahirrao, Ketan Kotecha, Ganeshsree Selvachandran, Ajith Abraham. A systematic literature review on software defect prediction using artificial intelligence. *Datasets, Data Validation Methods, Approaches, and Tools, Engineering Applications of Artificial Intelligence*. 2022. Vol. 111. 104773. ISSN 0952-1976. <https://doi.org/10.1016/j.engappai.2022.104773>.
17. CORCIOVĂ Călin; ANDRIȚOI Doru; LUCA Cătălina. A modern approach for maintenance prioritization of medical equipment. *Oper Manag-Emerg Trend Digit Era*, 2020.

18. Sangpetch O., Sangpetch A. Security Context Framework for Distributed Healthcare IoT Platform. In: Ahmed M., Begum S., Raad W. (eds) *Internet of Things Technologies for HealthCare. HealthyIoT*. 2016. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 2016. Vol 187. Springer, Cham. https://doi.org/10.1007/978-3-319-51234-1_11.
19. Miclăuș T., Valla V., Koukoura A. et al. Impact of Design on Medical Device Safety. *Ther Innov Regul Sci* 54. 2020. Pp. 839–849. <https://doi.org/10.1007/s43441-019-00022-4>.
20. Mshali, Haider, Lemlouma, Tayeb Moloney, Maria Magoni Damien. A Survey on Health Monitoring Systems for Health Smart Homes. *International Journal of Industrial Ergonomics*. 2018. Vol. 66. 10.1016/j.ergon.2018.02.002.
21. MMS Full Form in Medical. URL: <https://www.doctorsfinder.in/full-form/mms-full-form-in-medical/> (дата звернення: 12.02.2023).
22. Sezdi, Mana. Performance Analysis for Medical Devices. *Biomedical Engineering Research*. 2013. Vol. 2. Pp. 139-146. 10.5963/BER0203003.
23. J. Giraldo, E. Sarkar, A. A. Cardenas M. Maniatakos and M. Kantarcioglu, Security and Privacy in Cyber-Physical Systems: A Survey of Surveys, in *IEEE Design & Test*, vol. 34, no. 4, pp. 7-17, Aug. 2017, doi: 10.1109/MDAT.2017.2709310.
24. A. Gatouillat, Y. Badr, B. Massot and E. Sejdić, Internet of Medical Things: A Review of Recent Contributions Dealing With Cyber-Physical Systems in Medicine, in *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3810-3822, Oct. 2018, doi: 10.1109/JIOT.2018.2849014.
25. Z. Jiang, M. Pajic and R. Mangharam, Cyber-Physical Modeling of Implantable Cardiac Medical Devices in *Proceedings of the IEEE*, vol. 100, no. 1, pp. 122-137, Jan. 2012, doi: 10.1109/JPROC.2011.2161241.
26. R. Mitchell and I. -R. Chen, Behavior Rule Specification-Based Intrusion Detection for Safety Critical Medical Cyber Physical Systems, in *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 1, pp. 16-30, 1 Jan.-Feb. 2015, doi: 10.1109/TDSC.2014.2312327.

27. HealthSuite. Powering the next generation of connected Cloud health applications. URL: <https://www.usa.philips.com/healthcare/innovation/about-health-suite> (дата звернення: 10.02.2023).
28. Dey N., Ashour A.S., Shi F. et al. Medical cyber-physical systems: A survey. *J Med Syst* 42, 74 (2018). <https://doi.org/10.1007/s10916-018-0921-x>.
29. G. Grispos, W. B. Glisson and K. -K. R. Choo, Medical Cyber-Physical Systems Development: A Forensics-Driven Approach, *2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)*, Philadelphia, PA, USA. 2017. pp. 108-113, doi: 10.1109/CHASE.2017.68.
30. Zhihao Jiang, Houssam Abbas, Pieter J. Mosterman, and Rahul Mangharam Technical Report: Abstr t: Abstraction-Tree For Closed-loop Model or Closed-loop Model Checking of Medical Devices. *Computer Engineering | Electrical and Computer Engineering*. 2015. P.21.
31. Chen G., Jiang Z. Environment modeling during model checking of cyberphysical systems. *Computer*. Vol. 54(9). 2021. Pp. 49-58.
32. B. Hannaford, et al., Raven-II: An open platform for surgical robotics research, *IEEE Transactions on Biomedical Engineering*, vol. 60, no. 4, pp. 954-959, 2013.
33. CX. Zhai and S. Massung. Text Data Analysis and Management: A Practical Introduction to Text Mining and Information Retrieval. Association for Computing Machinery and Morgan & Claypool Publishers. 2015. New York, NY.
34. AlZubi A.A., Al-Maitah, M. Alarifi A. Cyber-attack detection in healthcare using cyber-physical system and machine learning techniques. *Soft Computing*. Vol.25. 2021. Pp.12319–12332. <https://doi.org/10.1007/s00500-021-05926-8>.
35. Abdali-Mohammadi F, Meqdad MN, Kadry S Development of an IoT-based and cloud-based disease prediction and diagnosis system for healthcare using machine learning algorithms. *Int J ArtifIntell*. 2020. ISSN 2252(8938):8938.
36. Оцінка відповідності медичних виробів. URL: <https://cratia.ua/uk/conformity-assessment-medical-devices> (дата звернення: 15.04.2023).

37. ISO 13485:2016: Medical devices — Quality management systems — Requirements for regulatory purposes. URL: <https://www.iso.org/standard/59752.html> (дата звернення: 16.04.2023).

38. IEC 60601-2-38: Medical Electrical Equipment - Part 2-38: Particular Requirements for the Safety of Electrically Operated Hospital Beds. URL: <https://standards.globalspec.com/std/761412/IEC%2060601-2-38> (дата звернення: 16.04.2023).

39. IEC/TR 80002-3:2014: Medical device software — Part 3: Process reference model of medical device software life cycle processes (IEC 62304). URL: <https://www.iso.org/standard/65624.html> (дата звернення: 16.04.2023).

40. ДСТУ EN 62366-1:2019 Прилади медичні. Частина 1. Застосування інженерних технологій до медичних виробів (EN 62366-1:2015, IDT; IEC 62366-1:2015, IDT).

41. ISO 14971:2019: Medical devices — Application of risk management to medical devices. URL: <https://www.iso.org/standard/72704.html> (дата звернення: 16.04.2023).

42. Jeon, M., Yoo, S., & Kim, S. W. A contactless PCBA defect detection method: Convolutional neural networks with thermographic images. *IEEE Transactions on Components, Packaging and Manufacturing Technology*. 2022. Vol. 12(3). pp. 489-501.

43. Dhingra, G., Kumar, V., Joshi, H. D. A novel computer vision based neutrosophic approach for leaf disease identification and classification. *Measurement*. 2019. Vol. 135. Pp.782-794.

44. Chen H., Zhang Z., Zhao C., Liu J., Yin W., Li Y., Lin Z. Depth classification of defects based on neural architecture search. *IEEE Access*, 9.2021. Pp. 73424-73432.

45. Koçak H. M., Naskali A. T., Mitard, J. (2021, December). Detecting Transistor Defects in Medical Systems Using a Multi Model Ensemble of Convolutional Neural Networks. *In 2021 IEEE International Conference on Big Data (Big Data)*. Pp. 4731-4737. IEEE.

46. Psarommatis F., Kiritsis D. A hybrid Decision Support System for automating decision making in the event of defects in the era of Zero Defect Manufacturing. *Journal of Industrial Information Integration*. Vol.26. 2022. 100263.
47. Feiler P., Delange J. Automated fault tree analysis from aadl models. *ACM SIGAda Ada Letters*, 36(2). 2017. Pp. 39-46.
48. Procter S., Hatcliff, J. An architecturally-integrated, systems-based hazard analysis for medical applications. *The 12th ACM/IEEE Conference on Formal Methods and Models for Codesign (MEMOCODE)*. 2014. Pp. 124-133. IEEE.
49. Hunte J., Neil M., Fenton N. A hybrid Bayesian network for medical device risk assessment and management. 2022. arXiv preprint arXiv:2209.03352.
50. AlTawy R., Youssef A. M. Security tradeoffs in cyber physical systems: A case study survey on implantable medical devices. *IEEE Access*. 2016. Vol. 4. Pp. 959-979.
51. Gatouillat A., Badr Y., Massot B., Sejdić E. Internet of medical things: A review of recent contributions dealing with cyber-physical systems in medicine. *IEEE internet of things journal*. 2018. Vol. 5(5). Pp. 3810-3822.
52. Konstantinou, C., Maniatakos, M., Saqib, F., Hu, S., Plusquellic, J., & Jin, Y. (2015, May). *Cyber-physical systems: A security perspective*. In 2015 20th IEEE European Test Symposium (ETS) (pp. 1-8). IEEE.
53. AlZubi A. A., Al-Maitah M., Alarifi A. Cyber-attack detection in healthcare using cyber-physical system and machine learning techniques. *Soft Computing*. 2021. Vol. 25(18). Pp. 12319-12332.
54. Dogaru, D. I., Dumitrache I. Cyber-physical systems in healthcare networks. *In 2015 E-Health and Bioengineering Conference (EHB)*. 2015. pp. 1-4. IEEE.
55. Gatouillat A., Badr, Y., Massot B., Sejdić E. Internet of medical things: A review of recent contributions dealing with cyber-physical systems in medicine. *IEEE internet of things journal*. 2018. Vol. 5(5). Pp. 3810-3822.
56. Jantunen E., Zurutuza U., Ferreira L. L., Varga P. Optimising maintenance: What are the expectations for Cyber Physical Systems. *The 3rd International Workshop*

on *Emerging Ideas and Trends in Engineering of Cyber-Physical Systems (EITEC)*. 2016. pp. 53-58. IEEE.

57. Balas V. E., Solanki V. K., Kumar R., Ahad M. A. R. (Eds.). A handbook of internet of things in biomedical and cyber physical system. 2020. (No. 172554). Berlin/Heidelberg, Germany: Springer.

58. Pankratova N. D. Creation of Physical Models for Cyber-Physical Systems. *Cyber-Physical Systems and Control*. 2020. Pp. 55-63. Springer International Publishing.

59. Chen F., Tang, Y., Wang C., Huang J., Huang C., Xie, D., Zhao, C. art. *IEEE Transactions on Computational Social Systems*. 2021. Vol. 9(5). Pp. 1359-1386.

60. Silva L. C., Almeida, H. O., Perkusich A., Perkusich M. A model-based approach to support validation of medical cyber-physical systems. *Sensors*, Vol. 15(11). 2015. Pp. 27625-27670.

61. Sayed-Mouchaweh M. (Ed.). Diagnosability, security and safety of hybrid dynamic and cyber-physical systems. Cham: Springer. 2018.

62. Wolf M., Serpanos D. Safety and security in cyber-physical systems and internet-of-things systems. *Proceedings of the IEEE*. 2017. Vol. 106(1). Pp. 9-20.

63. Dowdeswell B., Sinha R., MacDonell S. G. Finding faults: A scoping study of fault diagnostics for Industrial Cyber-Physical Systems. *Journal of systems and software*. 2020. Vol. 168 (110638).

64. Zanero S. Cyber-physical systems. *Computer* Vol. 50(4). 2017. Pp. 14-16.

65. Liu Y., Peng, Y., Wang B., Yao S., Liu, Z. Review on cyber-physical systems. *IEEE/CAA Journal of Automatica Sinica*. Vol. 4(1). 2017. Pp. 27-40.

66. Schneble W., Thamilarasu G. Attack detection using federated learning in medical cyber-physical systems. *28th International conference on computer communications and networks (ISSNN)*. 2018. pp. 1-8.

67. Costanzo A., Faro A., Giordano D., Pino, C. Mobile cyber physical systems for health care: Functions, ambient ontology and e-diagnostics. *The 13th IEEE Annual*

Consumer Communications & Networking Conference (CCNC). 2016. Pp. 972-975).
IEEE.

68. Li T., Cao J., Liang J., Zheng, J. Towards context-aware medical cyber-physical systems: design methodology and a case study. *Cyber-Physical Systems*, Vol. 1(1). 2015. Pp. 5-23.

69. Celdrán A. H., Pérez M. G., Clemente F. J. G., Pérez G. M. Sustainable securing of medical cyber-physical systems for the healthcare of the future. *Sustainable Computing: Informatics and Systems*, Vol. 19. 2018. Pp. 138-146.

70. Liu Y., Peng Y., Wang B., Yao S., Liu, Z. Review on cyber-physical systems. *IEEE/CAA Journal of Automatica Sinica*, Vol. 4(1). 2017. Pp. 27-40.

71. Rajkumar R., De Niz D., Klein M. Cyber-physical systems. Addison-Wesley Professional. 2016. P.548.

72. Lv Z., Chen, D., Lou R., Alazab A. Artificial intelligence for securing industrial-based cyber-physical systems. *Future generation computer systems*, Vol. 117. Pp. 291-298.

73. Sverstiuk A. Математичне моделювання кібер-фізичних біосенсорних та імуносенсорних систем. *COMPUTER-INTEGRATED TECHNOLOGIES: EDUCATION, SCIENCE, PRODUCTION*. Vol 34. 2019. Pp. 5-18.

74. Korotunov S. U., Tabunshchuk G. V. АНАЛІЗ ПІДХОДІВ ДО МОДЕЛЮВАННЯ ТА ВЕРИФІКАЦІЇ КІБЕРФІЗИЧНИХ СИСТЕМ. *Radio Electronics, Computer Science, Control*. Vol. (3). Pp. 57-68.

75. Головатенко І., Писаренко, А. Методи моделювання кібер-фізичних систем. *Адаптивні системи автоматичного управління*, Вип. 2(39). 2021. Pp. 74-83.

76. Sverstiuk, A., Bagriy-Zayats, O., Horkunenko, A., Mayhruk, Z., & Gaida, V. (2019). Кіберфізичні системи для визначення рівня глюкози. *COMPUTER-INTEGRATED TECHNOLOGIES: EDUCATION, SCIENCE, PRODUCTION*. Vol. (36). Pp. 69-76.

77. І. Ш. Невлюдов, В. В. Євсєєв, А. О. Андрусевич, С. С. Максимова
Моделі та методи кіберфізичних виробничих систем в концепції Industry 4.0 :
монографія. Oktan Print – Prague. 2023. 321 с.

78. Свєрстюк А. С., Багрій-Заяць О. А., Горкуненко, А. Б., Майхрук З. В.,
Мойсеєнко О. В. Розробка кіберфізичних біосенсорних систем для медико-
біологічних досліджень. 2019. Вісник Хмельницького національного
університету. с. 252-257.

79. Kocabas O., Soyata T., Aktas M. K. Emerging security mechanisms for
medical cyber physical systems. *IEEE/ACM transactions on computational biology and
bioinformatics*. Vol.13(3). 2016. Pp. 401-416.

80. Priyadarshini I., Kumar R., Tuan L. M., Son L. H., Long H. V., Sharma R.,
Rai S. A new enhanced cyber security framework for medical cyber physical
systems. *SICS Software-Intensive Cyber-Physical Systems*. 2021. Pp.1-25.

ДОДАТОК А
(обов'язковий)

ТЕЗИ ДОПОВІДІ НА XVII МІЖНАРОДНУ НАУКОВУ КОНФЕРЕНЦІЮ
«ОЛЬВІЙСЬКИЙ ФОРУМ-2023: СТРАТЕГІЇ КРАЇН ПРИЧОРНОМОРСЬКОГО
РЕГІОНУ В ГЕОПОЛІТИЧНОМУ ПРОСТОРІ», СЕКЦІЯ КОМП'ЮТЕРНА
ІНЖЕНЕРІЯ

(<https://drive.google.com/drive/folders/1elqkg0f9zqxmrjc9xqxowvjemn4cbwtj>)

СЕКЦІЯ: ТЕХНІЧНІ НАУКИ

ПІДСЕКЦІЯ: Комп'ютерна інженерія

Дунець А.С. Кіберфізична система виявлення дефектів медичних виробів

Магістр кафедри комп'ютерної інженерії та інформаційних систем
Хмельницький національний університет, м. Хмельницький, Україна

КІБЕРФІЗИЧНА СИСТЕМА ВИЯВЛЕННЯ ДЕФЕКТІВ МЕДИЧНИХ ВИРОБІВ

Розвиток обчислювальної техніки, мереж та сенсорних технологій призвів до повсюдного розгортання кіберфізичних систем у критично важливих для безпеки середовищах, таких як аерокосмічна сфера, енергетика, транспорт і охорона здоров'я. Зокрема, існує значне розгортання медичних кіберфізичних систем у різних клінічних та персоналізованих умовах, починаючи від крихітних кардіостимуляторів і дефібриляторів, які можна імплантувати, до переносних пристроїв моніторингу стану здоров'я, складних моніторів пацієнтів у відділеннях інтенсивної терапії і дорогих систем для променевої терапії та роботизованої хірургії.

Кіберфізична система виявлення дефектів медичних приладів – це інтегрована система, що поєднує фізичну складову (медичні прилади) та кібернетичну складову (системи аналітики даних та обробки інформації) для виявлення та діагностики дефектів у медичних приладах. Основна мета такої системи - покращення якості та безпеки медичних приладів шляхом раннього виявлення можливих проблем.

На даний момент немає стандартів і правил, які застосовуються безпосередньо до кіберфізичних систем охорони здоров'я. Однак, перед розробленням кіберфізичної системи в медичній галузі варто ознайомитися з медичними стандартами, що застосовуються до медичного обладнання, з правилами та клінічними стандартами. Правила, що застосовуються для медичного обладнання аналогічні б багатьох країнах світу, але вони не ідентичні. Це означає, що той самий медичний виріб може бути визнаний безпечним для використання в медичних закладах країн Євросоюзу або інших країнах, але не в Сполучених Штатах. Європейський Союз використовує маркування CE для сертифікації виробу, який повинен відповідати нормам ЄС. Подібні стандарти є і в США, наприклад FDA (Управління з контролю за продуктами й ліками США), що вказує на відповідність медичного обладнання нормам та стандартам США. В Україні розроблені стандарти на основі документації Європейського Союзу, але маркування CE для використання медичних приладів недостатньо, необхідна ще українська сертифікація. Країни, які не розробили і не прийняли жодного Положення щодо медичного обладнання в першу чергу використовують стандарти ВООЗ (Всесвітня організація охорони здоров'я). У той час як стандарти охорони здоров'я кіберфізичних систем є ще не розбудовані, ряд промислових, комунікацій (наприклад, Bluetooth - IEEE 802.15.1, Wi-Fi - IEEE 802.11), якості (ISO 9001, ISO 13845, ISO 14971), медобладнання (ISO/IEEE 11073, HL7 – рівень здоров'я 7, DICOM – Цифрові зображення та комунікації в медицині) і до них можна застосувати клінічні стандарти.

ISO/IEEE 11073 – це набір стандартів для особистої медичної допомоги пристроїв. Загальним контекстом цього є передача даних і інтерфейс між агентом і менеджером. Рівень здоров'я 7 – це група стандартів для обміну, інтеграція, обмін та пошук електронної інформації про здоров'я інформації. HL7 визначає багато адаптованих стандартів, керівних принципів і методологій, які забезпечують комунікацію різні комп'ютерні системи в лікарнях і різних закладах охорони здоров'я провайдерів.

Стандарти на медичне обладнання встановлюються для забезпечення безпеки та ефективності його використання. Основні стандарти, які використовуються в галузі медичного обладнання, включають:

1. ISO 13485: Системи управління якістю для медичного обладнання - вимоги до розробки та виробництва.
2. IEC 60601: Електричне обладнання медичне - Частина 1-11: Загальні вимоги до безпеки, включаючи основні вимоги до безпеки та ефективності.
3. IEC 62304: Медичне програмне забезпечення - Життєвий цикл програмного забезпечення.
4. IEC 62366: Ергономіка медичних пристроїв - Застосування людських факторів до проектування та оцінки безпеки медичних пристроїв.
5. IEC 60601-1-2: Електричне обладнання медичне - Частина 1-2: Загальні вимоги до безпеки - Електромагнітна сумісність.
6. ISO 14971: Цей стандарт визначає вимоги до управління ризиками медичних пристроїв, включаючи процеси оцінки та керування ризиками.

Ці стандарти встановлюють вимоги до безпеки, ефективності та якості медичного обладнання та програмного забезпечення, що використовуються в галузі медицини. Вони є обов'язковими для дотримання виробниками медичного обладнання та програмного забезпечення, що використовується в галузі медицини.

Розроблені стандарти на медичне обладнання дозволяють покращити якість, безпеку, електричну безпеку, електромагнітну сумісність, управління ризиками та інші аспекти медичного обладнання. Вони сприяють забезпеченню безпеки пацієнтів та високої якості медичних пристроїв.

Варто підкреслити, що в охороні здоров'я на об'єктах повинні використовуватися лише сертифіковані кіберфізичні системи.

Отже, враховуючи вищевикладене, архітектура кіберфізичної системи виявлення дефектів медичних приладів складається з трьох рівнів та представлена на рисунку 1.

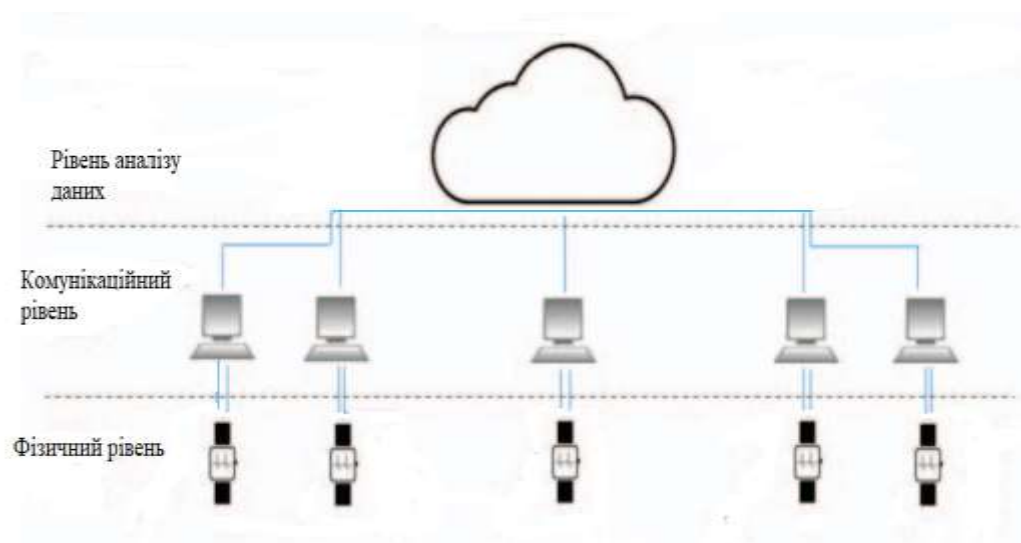


Рисунок 1 – Архітектура кіберфізичної системи виявлення дефектів медичних виробів

Розглянемо ці рівні детальніше. Фізичний рівень призначений для датчиків, які взаємодіють з медичними приладами та отримують інформацію про стан медичних приладів.

Після цього інформація про стан медичних приладів передається на комунікаційний рівень. Все пристрої повинні бути приєднані до комп'ютера безпечним способом стосовно обміну даними, щоб виключити можливість обміну даними з пристроями або комп'ютером, які не належать до системи.

На рівні аналізу даних є можливість обробляти всю отриману інформацію (крім приватної інформації) з комунікаційного рівня обслуговування та надсилати відповідь запитувачу, включаючи інформацію про можливі несправності та рішення для запобігання або

усуненні цих несправностей. Основна роль шару полягає в зборі інформації з різних датчиків та приладів та використовувати всю отриману інформацію для подальшого аналізу даних.

Кіберфізична система виявлення дефектів медичних приладів – це система, яка поєднує фізичні технології і програмне забезпечення для виявлення дефектів в медичних приладах. Ця система може бути використана для автоматичного моніторингу медичних приладів, що дозволяє забезпечити їх безперебійну роботу і запобігти можливим нещасним випадкам, пов'язаним з несправністю

ДОДАТОК Б
(обов'язковий)

ПРЕЗЕНТАЦІЯ

Кіберфізична система виявлення
дефектів медичних виробів

Виконав: магістр гр.КІ2м-21-1 Донець
А.С.

Керівник: д.т.н., професор Яцків В.В.

Актуальність

- Кіберфізичні системи виявлення дефектів медичних виробів є важливим інструментом для забезпечення безпеки пацієнтів та ефективної роботи медичного обладнання. Вони поєднують в собі технології програмного забезпечення та апаратного забезпечення з метою виявлення дефектів та моніторингу роботи медичних пристроїв.
 - Основна мета кіберфізичних систем виявлення дефектів медичних виробів полягає в тому, щоб забезпечити надійність та безпеку роботи медичного обладнання. Вони дозволяють виявляти неполадки та дефекти медичних виробів, які можуть призвести до неправильної діагностики та лікування, зниження якості медичної допомоги та можуть стати причиною травм та інших небезпек для пацієнтів та медичного персоналу.
 - Крім того, кіберфізичні системи виявлення дефектів медичних виробів дозволяють зменшити час, необхідний для виявлення та усунення дефектів, що дозволяє забезпечити швидке та ефективне лікування пацієнтів. Вони також допомагають зменшити ризик виникнення дефектів медичних приладів шляхом моніторингу їх роботи та вчасного виявлення неполадок.
-
- Мета дослідження: мінімізація ризиків для пацієнта за допомогою кіберфізичної системи виявлення дефектів медичних виробів.
 - Об'єкт дослідження: процес виявлення дефектів медичних виробів в режимі реального часу.
 - Предмет дослідження: кіберфізична система виявлення дефектів медичних виробів.

Задачі дослідження

- 1) провести аналіз існуючих апаратних та програмних засобів, що використовуються в кіберфізичних системах виявлення дефектів медичних виробів;
- 2) провести огляд існуючих моделей та методів виявлення дефектів медичних виробів;
- 3) розробити метод виявлення дефектів медичних виробів кіберфізичною системою;
- 4) запропонувати архітектуру кіберфізичної системи виявлення дефектів медичних виробів.

Наукова новизна

1. Набув подальшого розвитку метод виявлення дефектів медичних виробів за рахунок введених критеріїв, що характеризують ступінь ризику дефекту для пацієнта.
2. Набула подальшого розвитку архітектура кіберфізичної системи виявлення дефектів медичних виробів, в частині додавання підсистеми виявлення та аналізу дефектів.

Практична цінність отриманих результатів у можливості підвищення якості та безпеки медичного обладнання, зменшенні ризику для пацієнтів, економії ресурсів та часу медичного персоналу.

- Огляд літературних джерел показав, що на даний момент актуальність використання кіберфізичних систем в медичній галузі зростає.
- Застосування кіберфізичних систем виявлення дефектів медичних виробів дозволяє підвищити безпеку пацієнтів, внаслідок виявлення потенційних дефектів або несправностей в медичних виробках на ранніх стадіях. Це дозволяє запобігати можливим небезпекам та забезпечує безпеку пацієнтів. Також такі системи покращують якість медичних послуг завдяки вчасному виявленню дефектів у медичних виробках, що допомагає уникнути збоїв у їхній роботі та забезпечує належну функціональність.
- В процесі використання в медичних закладах є така категорія медичних виробів, до яких ставляться підвищенні вимоги до надійності, оскільки наслідки збоїв, дефектів та несправностей можуть бути критичними для пацієнта. У наш час безпека медичного обладнання та пов'язані з ним небезпеки їх використання є одним із критичних питань для охорони здоров'я організації по всьому світу.
- Як показують дослідження, традиційні методи аналізу небезпеки, які використовуються для медичних виробів, зосереджені насамперед на відмовах окремих компонентів або людських помилках у системі. Інші потенційні причинні фактори, такі як складні помилки програмного забезпечення та небезпечні взаємодії компонентів, часто не враховуються ретельно під час аналізу.

Таблиця 1.1 – Приклади дефектів медичних виробів, пов'язаних із комп'ютером

Вид дефекту	Клас дефекту	Проблема	Опис	Наслідок дефекту/ режим відмови
Програмне забезпечення	II	Виріб має проблеми з програмним інтерфейсом	При підключенні до основної системи це не дозволить системі розпізнати прилад нефункціональним на всіх сайтах	Збій в роботі пристрою
Апаратне забезпечення	I	Нездатність приладу здійснити шоківий імпульс (розряд)	Несправний конденсатор може спричинити затримку або відсутність розряду дефібрилятора, що може призвести до неможливості реанімації пацієнта	Переривання лікування/ невдача терапії
Інше	I	Пристрій вмикається, а потім вмикається самостійно або не вмикається	Пристрій або сам вмикається або вмикає оператор, або пристрій не вмикається зовсім	Збій в роботі пристрою
Батарея	I	Ненавмисне перезавантаження	Насос демонструє періодичну втрату живлення через періодичну втрату контакту між чашкою та контейнером акумулятора, що призводить до скидання пристрою	Переривання лікування/ невдача терапії
Вхід/вихід	II	Динаміки на моніторі пацієнта вийшли з ладу	Відсутність звукової сигналізації та затримка лікування пацієнта	Помилка Активності повідомлення тривоги "Падає"

Моделювання процесу виявлення дефектів медичних виробів кіберфізичною системою

Введемо три критерії оцінки стану кіберфізичної системи виявлення дефектів

- виникнення дефектів (V)
- виявлення дефектів (W)
- можливість усунення дефектів в реальному режимі (U).

Також додатково до цих критеріїв опишемо критерії, які дозволять виявляти критичність стану. Зокрема пропонуємо застосовувати наступні два критерії, що стосується виникнення – серйозність S та складність C . Опис критерію серйозність представлений формулою 1:

$$S = \langle Sh, Sm, Sl \rangle, \quad (1)$$

-
- де Sh – висока серйозність дефекта, що виник,
- Sm – середня серйозність дефекта, що виник,
- Sl – низька серйозність дефекта, що виник.

Моделювання процесу виявлення дефектів медичних виробів кіберфізичною системою

Опис критерію складність представлений формулою 2:

$$C = \langle Ch, Cm, Cl \rangle, \quad (2)$$

де Ch – висока складність дефекта, що виник,
 Cm – середня складність дефекта, що виник,
 Cl – низька складність дефекта, що виник.

Для критерію виявлення дефектів можливі два додаткових критерія – виявлення або невиявлення.

Для опису критерію можливість усунення пропонуємо наступні критерії – можливість усунення в реальному режимі (висока, середня, низька), тип дефекту (програмне забезпечення, апаратне забезпечення, електрика, інше).

Метод виявлення дефектів медичних виробів за допомогою кіберфізичної системи:

1. Збір даних з медичних виробів за допомогою датчиків, що встановлюються на приладах. Дані можуть включати різні параметри, такі як температура, вологість, тиск, рівень заряду батареї та інші параметри, що відповідають за роботу медичного приладу.
2. Аналіз даних за допомогою програмного забезпечення з аналітикою даних. Програмне забезпечення може використовувати різні алгоритми та методи, такі як аналіз часових рядів, класифікація та кластеризація, щоб виявити можливі дефекти медичного приладу.

Метод виявлення дефектів медичних виробів за допомогою кіберфізичної системи:

3. Виявлення дефектів медичного виробу та інформування про них (В цьому пункті метод виявлення помилок вдосконалено за рахунок введення критеріїв, описаних на слайді 8 та 9). Оцінюється критичність стану медичного виробу і таким чином це дає змогу мінімізувати ризик для пацієнтів, оскільки оператор має можливість оперативно реагувати на стан медичного виробу.

Метод виявлення дефектів медичних виробів за допомогою кіберфізичної системи:

4. Якщо програмне забезпечення виявить можливий дефект, воно повідомляє про це систему моніторингу та управління. Система моніторингу та управління може надавати можливість для віддаленого управління медичним приладом або надіслання повідомлень медичному персоналу про необхідність проведення ремонту.

5. Моніторинг стану медичного виробу та зберігання даних про нього. Кіберфізична система може зберігати дані про стан медичного приладу та його ремонт, що може бути корисно для підтримки його ефективної роботи та попередження можливих проблем у майбутньому.

- Кіберфізична система виявлення дефектів медичних виробів – це система, яка поєднує фізичні технології і програмне забезпечення для виявлення дефектів в медичних приладах. Ця система може бути використана для автоматичного моніторингу медичних приладів, що дозволяє забезпечити їх безперебійну роботу і запобігти можливим нещасним випадкам, пов'язаним з несправністю обладнання.

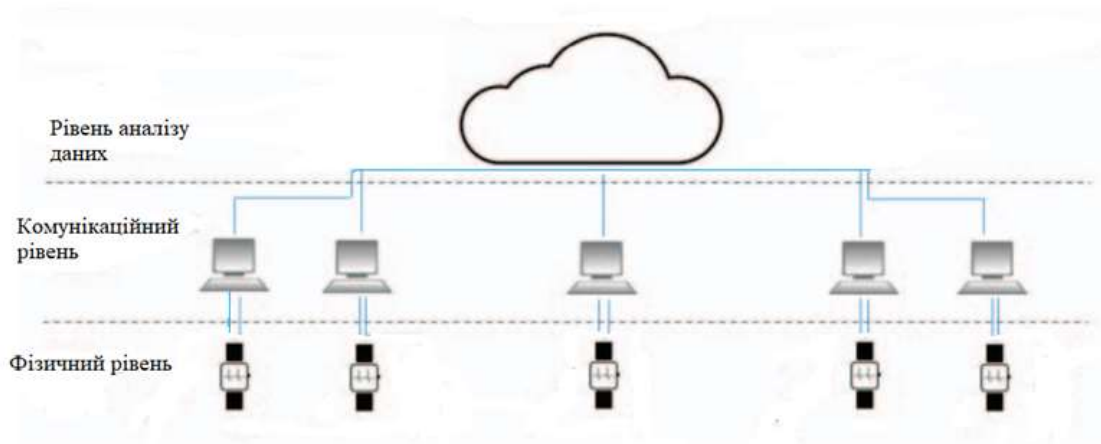


Рисунок 1 – Архітектура кіберфізичної системи виявлення дефектів медичних виробів

Основні компоненти кіберфізичної системи виявлення дефектів медичних виробів включають в себе:

- 1) Датчики, які вимірюють різні параметри медичних приладів, такі як температура, тиск, вологість і т.д.
- 2) Програмне забезпечення, яке аналізує дані з датчиків і виявляє можливі дефекти.
- 3) Комунікаційні пристрої, що забезпечують зв'язок між системою виявлення дефектів і медичним приладом, включаючи мережі Інтернет речей (IoT).
- 4) Інтерфейс користувача, який дозволяє медичному персоналу отримувати інформацію про стан медичного приладу і при необхідності приймати відповідні заходи.

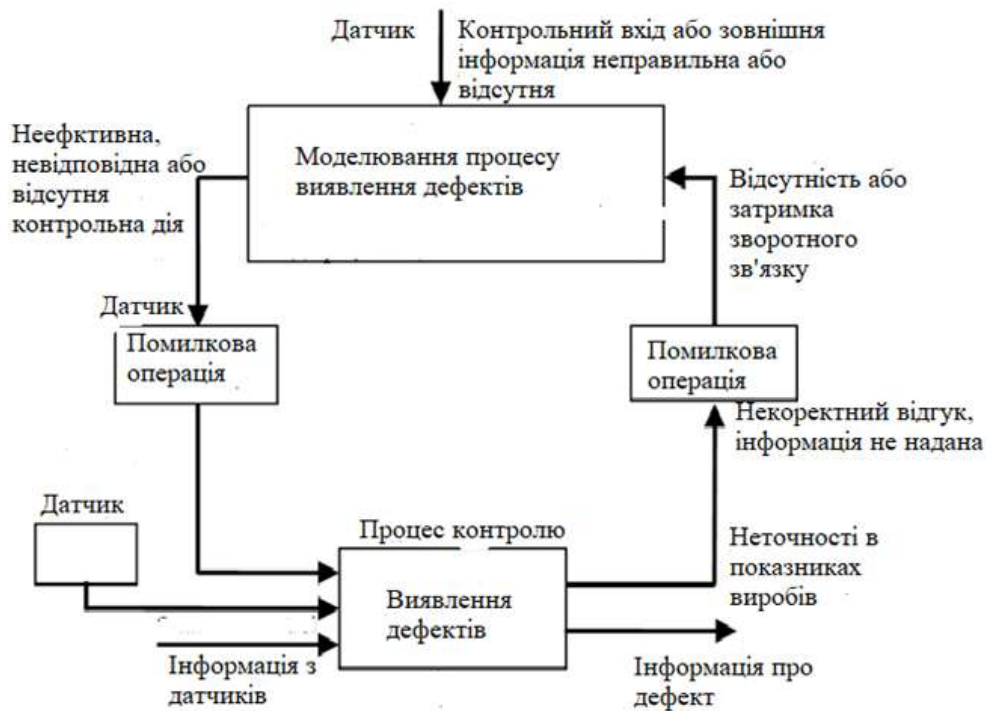


Рисунок 2 – Підсистема виявлення та аналізу дефектів

Висновки

- Застосування кіберфізичної системи виявлення дефектів медичних виробів допомагає зменшити кількість некоректної роботи медичних виробів і тим самим покращити якість медичних послуг. Наприклад, система може виявити ранні ознаки проблем з медичним виробом, що дозволить вчасно провести ремонт або заміну. Також, система допомагає у виявленні проблем з електронними компонентами медичних виробів, що може запобігти їх перегріванню та випадковому відключенню, що може призвести до серйозних наслідків для пацієнтів. В цілому, застосування кіберфізичної системи виявлення дефектів медичних виробів допомагає забезпечити безпеку та ефективність медичної техніки.

Висновки

- 1) проведено аналіз існуючих апаратних та програмних засобів, що використовуються в кіберфізичних системах виявлення дефектів медичних виробів;
- 2) проведено огляд існуючих моделей та методів виявлення дефектів медичних виробів;
- 3) набув подальшого розвитку метод виявлення дефектів медичних виробів за рахунок введених критеріїв, що характеризують ступінь ризику дефекту для пацієнта.
- 4) набула подальшого розвитку архітектура кіберфізичної системи виявлення дефектів медичних виробів, в частині додавання підсистеми виявлення та аналізу дефектів.

Дякую за увагу!



Ім'я користувача:
Кафедра КІ

Дата перевірки:
15.05.2023 14:46:59 EEST

Дата звіту:
15.05.2023 14:49:34 EEST

ID перевірки:
1015088284

Тип перевірки:
Doc vs Internet + Library

ID користувача:
100005591

Назва документа: Дунець_Кіберфізична система виявлення дефектів медичних приладів

Кількість сторінок: 78 Кількість слів: 16809 Кількість символів: 133386 Розмір файлу: 912.36 KB ID файлу: 1014772978

0.86% Схожість

Найбільша схожість: 0.6% з джерелом з Бібліотеки (ID файлу: 1014424613)

0.43% Джерела з Інтернету 67 Сторінка 80

0.75% Джерела з Бібліотеки 68 Сторінка 80

0% Цитат

Цитати 5 Сторінка 81

Посилання 1 Сторінка 81

0% Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи 4

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 1.0%

Словник перевірки: en_US, ru_RU, uk_UA. Пошук в документах: 9%

ID: 113368 Назва: БКР Кіберфізична система виявлення дефектів водних приставів Додано в БД: 2023-05-15 Автор: Дунець А.С. Керівник: Яків В.В. Консультант: Опонент:	Документ		Сумарний збіг по Бюї Даних	
	Словот	Лексем	Словот	Лексем
	118279	863	932 (1%)	10 (1%)

Джерело плагіату

ID	Опис	Навність плагіату в документі	
		Словот	Лексем

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дипломник: Дунець Артем Сергійович

Тема: Кіберфізична система виявлення дефектів медичних виробів

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг кваліфікаційної роботи:

Кількість листів креслень _____ Кількість сторінок записки 91

1. Короткий зміст роботи та прийнятих рішень: в результаті виконаного дослідження набув подальшого розвитку метод виявлення дефектів медичних виробів за рахунок введених критеріїв, що характеризують ступінь ризику дефекту для пацієнта та набула подальшого розвитку архітектура кіберфізичної системи виявлення дефектів медичних виробів, в частині додавання підсистеми виявлення та аналізу дефектів.
2. Висновок про відповідність роботи дипломному завданню: Магістерська робота відповідає поставленому завданню
3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У першому розділі магістерської роботи проведено огляд відомих апаратних та програмних засобів, що використовуються в кіберфізичних системах виявлення дефектів медичних виробів. Застосування кіберфізичних систем виявлення дефектів медичних виробів дозволяє підвищити безпеку пацієнтів, внаслідок виявлення потенційних дефектів або несправностей в медичних виробках на ранніх стадіях. Це дозволяє запобігати можливим небезпекам та забезпечує безпеку пацієнтів. Також такі системи покращують якість медичних послуг завдяки вчасному виявленню дефектів у медичних виробках, що допомагає уникнути збоїв у їхній роботі та забезпечує належну функціональність. В другому розділі описаний огляд існуючих моделей та методів виявлення дефектів медичних виробів; процес моделювання процесу виявлення дефектів медичних виробів. В третьому розділі запропоновано метод виявлення дефектів медичних виробів кіберфізичною системою за рахунок введених критеріїв, що характеризують ступінь ризику дефекту для пацієнта. У четвертому

розділі архітектура кіберфізичної системи виявлення дефектів медичних виробів, в частині додавання підсистеми виявлення та аналізу дефектів.

4. Позитивні сторони роботи: Позитивною стороною роботи є ґрунтовний аналіз даних про виявлення дефекти медичних виробів.

5. Негативні сторони роботи: _____

6. Оцінка графічного оформлення та пояснювальної записки роботи: _____

7. Відгук про роботу в цілому: Робота виконана на достатньому науково-технічному рівні

8. Інші зауваження: _____

9. Оцінка дипломної роботи: Розглянувши представлену роботу, вважаю, що
 робота _____ заслуговує _____ оцінки _____ задовільно _____ D
 (3.5)

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) Бедратюк
Олексій Петрович, д. ф-м. наук, професор, зав. кафедри
"Технологія програмного забезпечення"

"18" травня 2023 р.

 (підпис)

Завідувачу кафедри КНС
д-р.техн.наук, проф. Говорущенко Т. О.

Душня Артема Сергійовича

ПІБ здобувача вищої освіти

ФІЛ, 2 курсу, групи КІ2М-21-1

ЗАЯВА

З правилами чинного Положення «Про дотримання академічної доброчесності в Хмельницькому національному університеті» від 26.09.2020 (зі змінами від 26.11.2020), згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат повідомлений (а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.



18.05.2023

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ
КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ
ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованою системою виявлення текстових збігів/ідентичності/схожості:

Назва: Киберфізична система виявлення дефектів медичних виробів

Автор: Дунець Артем Сергійович

Спеціальність: 123 – Компютерна інженерія

Освітня програма: освітньо-наукова

Науковий керівник: Яцків Василь Васильович

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи. Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

- 1) запозичення розміщені в розділах аналізу існуючих аналогів та прототипів, які не описують безпосередньо авторське дослідження і не стосуються результатів роботи;
- 2) усі запозичення фрагментарні, або мають належним чином оформленні посилання;
- 3) окремі виявлені збіги є загальноживаними фразами або виразами, про що свідчить посилання системи на збіг з 2-5 джерелами на один фрагмент речення;
- 4) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ідентичності/схожості, складає 0.86% і адресується до 68 першоджерела, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи

Гарант ОП

Завідувач кафедри КПС





В.В. Яцків

О. С. Савенко

Т. О. Говорущенко