

УНИВЕРЗИТЕТ У БЕОГРАДУ  
ФАКУЛТЕТ ОРГАНИЗАЦИОНИХ НАУКА

РАСТКО Д. МАРТАЋ

Примена *IoT* модела и сервиса у управљању  
и одржавању брана

докторска дисертација

Београд, 2020. године

UNIVERSITY OF BELGRADE  
FACULTY OF ORGANIZATIONAL SCIENCES

RASTKO D. MARTAĆ

Application of IoT models and services in the  
management and maintenance of dams

Doctoral Dissertation

Belgrade, Serbia, 2020

**Ментор:**

**Проф. др Душан Бараћ**

Ванредни професор, Универзитет у Београду,

Факултет организационих наука

**Чланови комисије:**

**Проф. др Божидар Раденковић**

Редовни професор, Универзитет у Београду,

Факултет организационих наука

**Проф. др Маријана Деспотовић-Зракић**

Редовни професор, Универзитет у Београду,

Факултет организационих наука

**Проф. др Саша Лазаревић**

Ванредни професор, Универзитет у Београду,

Факултет организационих наука

**Проф. др Бобан Стојановић**

Ванредни професор, Универзитет у Крагујевцу,

Природно-математички факултет

Датум одбране:

## **Примена *IoT* модела и сервиса у управљању и одржавању брана**

### **Сажетак:**

Предмет истраживања дисертације јесте развој модела техничког осматрања брана, заснован на концептима и технологијама интернета интелигентних уређаја. Главни проблем који се разматра у дисертацији је могућност примене интернета интелигентних уређаја, *RFID* технологије и *cloud computing*-а на постојећем систему осматрања брана.

У мануелном техничком осматрању неопходно је присуство човека. Код традиционалног модела техничког осматрања, неопходно је да осматрачи обилазе сваки од уређаја појединачно, читавају податке и записују их на папир. Након извршеног осматрања резултати са папира уносе се у рачунар. У читавом процесу осматрања могуће је случајно направити више грешака. Циљ новог модела је да се употребом *RFID* и *Bluetooth* технологија елиминише фактор људске грешке и унапреди процес осматрања.

У раду је развијен модел техничког осматрања брана, заснован на концептима и технологијама интернета интелигентних уређаја. Модел обухвата елементе инфраструктуре и архитектуре техничког осматрања бране и *RFID* технологију која ће бити коришћена у имплементацији модела инфраструктуре система техничког осматрања. Биће детаљно представљена *RFID* технологија која унапређује и убрзава процес мануелног техничког осматрања и смањује могућност људске грешке.

Предложени модел могуће је интегрисати на постојећу инфраструктуру и систем техничког осматрања брана. У оквиру евалуације модела, у докторској дисертацији реализовано је тестирање и мерење релевантних параметара који утичу на ефикасност предложеног модела. Развијени модел техничког осматрања имплементиран је на брани ХЕ „Ђердап 1” у Кладову, Република Србија.

**Кључне речи:** Интернет интелигентних уређаја, *RFID*, *Cloud computing*, Систем управљања безбедношћу брана, Мониторинг брана, Мануелно техничко осматрање.

**Научна област:** Информациони системи и технологије

**Ужа научна област:** Електронско пословање

**УДК број:**

# **Application of IoT models and services in the management and maintenance of dams**

## **Abstract:**

The subject of the doctoral dissertation research is the development of the model of technical monitoring of dams, based on the concepts and technologies of Internet of Things. This dissertation studies the effectiveness of using Internet of Things, RFID technology, and cloud computing on the existing dam monitoring system.

In the traditional model of technical monitoring, a human observer needs to visit each device individually, read the data and write them down on paper. After the monitoring, the observer enters the results from the paper into the computer.

During this process, it is possible to make numerous inadvertent mistakes. Advances in computer systems and wireless technology can alleviate or eliminate human errors and improve the efficiency of the monitoring process.

This dissertation develops a novel model of technical monitoring of dams based on the concepts and technologies of the Internet of Things. The model encompasses elements of the infrastructure and architecture of the technical monitoring of the dam as well as RFID technology that will be used in the implementation of the infrastructure model of the technical monitoring system. This dissertation shows how RFID technology enhances the technical monitoring process, in particular speeding up the process of manual technical monitoring and reducing the possibility of human error.

The model can be integrated in the existing infrastructure and systems for technical monitoring of dams. The author implemented the proposed model for technical monitoring at the dam HPP Iron Gate 1 in Kladovo, Republic of Serbia. The dissertation presents the evaluation of the model using testing and measurement of relevant parameters that influence the model's effectiveness.

**Key words:** Internet of Things, RFID, Cloud computing, Dam safety management system, Dam Monitoring, Manual technical monitoring

**Scientific field:** Information Systems and Technology

**Scientific subfield:** E-business

**UDK number:**

## САДРЖАЈ

1.	Увод	1
1.1	Дефинисање предмета и циљева дисертације	1
1.2	Циљеви истраживања	4
1.3	Полазне хипотезе	5
1.4	Методе истраживања	5
2.	Паметно управљање бранама	7
2.1	Концепт паметних брана	7
2.2	Анализа литературе	10
3.	Технологије за развој решења	19
3.1	Интернет интелигентних уређаја	19
3.1.1	Паметни уређаји	20
3.1.2	Бежичне сензорске мреже	23
3.1.3	Мрежни протоколи интернета интелигентних уређаја	24
3.1.4	<i>Machine-To-Machine</i> комуникација	27
3.1.5	Софтверски дефинисане мреже	28
3.1.6	Протоколи апликативног слоја интернета интелигентних уређаја	28
3.2	<i>RFID</i>	30
3.2.1	Концепт <i>RFID</i> технологије у индустрији	30
3.2.2	Примена <i>RFID</i> технологије	36
3.3	<i>Bluetooth</i>	41
3.3.1	<i>Beacons</i>	42
3.4	Мобилне технологије	46
3.5	<i>Cloud computing</i> технологије	49
3.6	<i>IoT Edge (Edge computing)</i>	52
3.7	Технологије за управљање подацима	54
3.7.1	Нерелационе базе података	54
3.7.2	Релационе базе података	55
3.7.3	Технологије за чување и пренос података	56
4.	Развој модела за паметно управљање/осматрање бранама	58
4.1	Анализа постојећих модела	58
4.2	Модел осматрања брана у Србији	60
4.3	Модел система за управљање безбедношћу брана у Србији	64
4.3.1	Слојеви у моделу система за управљање безбедношћу брана	70
4.3.2	Интеграција <i>IoT</i> -а у мануелном техничком осматрању брана	72
4.3.3	Управљање процесима у СУБ-у	74

5.	Имплементација и примена развијеног модела	76
5.1	Пројектни задатак	76
5.2	Хардверско-софтверска архитектура	76
5.3	Имплементација развијеног СУБ модела	77
6.	Евалуација модела	82
6.1	Контрола квалитета мерених техничких података	82
6.2	Процена квалитета података	83
6.3	Модел прихватања <i>RFID</i> технологије у осматрању	88
7.	Научни и стручни доприноси	93
8.	Будућа истраживања	95
9.	Закључак	96
10.	Литература	97
11.	Списак слика	107
12.	Списак табела	110

# 1. УВОД

## 1.1 Дефинисање предмета и циљева дисертације

Праћење и прикупљање података је процес од великог значаја за управљање браном. Прикупљени подаци се користе за предвиђања понашања бране, што је важно за управљање њиховом безбедношћу.

Безбедност брана и поузданост инструмената (уређаја) утичу на цео екосистем у области бране, а и шире. Опасност од оштећења бране расте са годинама, па је неопходно да се стално унапређује систем за праћење и сигурност бране, како би се избегле нежељене катастрофе.

Бране су инфраструктурни објекти, који по својој природи представљају одређени ризик, потенцијалну опасност за околно подручје. Ризик се никада не може елиминисати, али се може знатно умањити [1]. Питање сигурности брана, као и сигурност припадајућих објеката, од великог је значаја, посебно у случају великих индустријских брана. Сигурност бране обухвата њену заштиту, формирање акумулационог језера, са којим се могу обављати све предвиђене функционалности, без последица по људе, околину или физичке објекте.

С обзиром на то да бране задржавају велику количину воде у акумулационом језеру, која има велику разорну моћ, неопходно је да се брана и припадајући објекти перманентно одржавају на одговарајући начин, како не би дошло до пуцања бране које може изазвати озбиљне последице [1].

Одржавање бране обухвата низ активности различитих субјеката. Активности се предузимају са циљем систематског праћења стања (виталности) бране и припадајућих објеката у целини. Одговарајућим активностима могуће је на време идентификовати и предузети све мере које су потребне ради обезбеђења сигурности и функционалности објеката. Циљ свих мера одржавања бране је да се она дуготрајно одржи у добром стању, тј. да може да испуни све своје пројектоване функције, а да при томе постоји пуна сигурност самог објекта и околине.

Добар пројекат и квалитетно извођење радова су неопходни за постизање сигурности бране [1]. С обзиром на то да су бране физички објекти великих димензија, пројектом није могуће обухватити све факторе који могу утицати на саму сигурност бране, па самим тим не може се ни очекивати да бране издрже све непознате факторе. Посебно је тешко предвидети понашање брана у случају земљотреса, великих вода и сл. Ризик који носе бране не може никада бити елиминисан, па је питање сигурности брана увек актуелно.

Циљ одржавања брана је предупредивање свих потенцијалних проблема у раду и санирање кварова. У оквиру одржавања, предузимају се потребни радови обнове, поправке или реконструкције. Вредновање стања сигурности бране требало би да је редовна мера у одржавању бране. Сигурност бране се мора посматрати као незаобилазан фактор, паралелно са свим осталим функцијама које брана и остали објекти треба да испуне [1].

Питање одржавања великих брана је комплексно, јер обухвата различите чиниоце везане за саме објекте: конструкције, природне факторе, факторе средине и деловање људи. Различити организационо-хијерархијски нивои требало би да учествују у одржавању и функционисању брана. Кључни учесници требало би да буду власник, корисник, локална заједница и држава.

Престанак задржавања воде у акумулацији или неконтролисано испуштање воде из акумулације, може се дефинисати као рушење бране, тј. престанак њеног нормалног функционисања [1]. Са аспекта рушења бране, сигурност бране се може дефинисати као мера отпора против неконтролисаног испуштања воде из акумулационог језера.

Слично другим конструкцијама, и бране имају век трајања [2]. Бране треба редовно одржавати и, ако је потребно, правовремено реаговати како би се спречила могућност оштећења,



урушавања или неконтролисаног испуштања воде. Међутим, услови хидроенергетске производње постепено мењају карактеристике материјала који се користе за изградњу бране. Карактеристике геотехничког окружења такође су подложне променама. Осим тога, током времена мењају се професионални и социјални фактори, као и критеријуми сигурности и ризика (хидролошки, сеизмичко-тектонски итд.) праћени повременим променама стандарда и законских норми. Без обзира на све поменуте променљиве елементе, неопходно је управљати сигурношћу бране током читавог периода експлоатације.

Техничко осматрање брана је део процеса управљања и осматрања брана. Укључује аутоматизоване инструменте у процес осматрања, као и додатне инструменте где је неопходан људски фактор. Мануелно техничко осматрање је део техничког осматрања брана који укључује људски фактор, па је вероватноћа да се деси грешка велика. Процес мониторинга (надгледања), прикупљања и управљања подацима о системима је од велике важности за инжењерске пројекте и структуре, као што су бране [3]. Прикупљени подаци користе се за предвиђање понашања бране и за адекватно управљање њеном сигурношћу (СУБ). Сигурност бране и поузданост различитих уређаја за мерење параметара утичу на читав екосистем бране [4], [5]. С обзиром на то да ризик од прогресивне штете на брани постаје већи са сваком новом штетом, потребно је континуирано унапређивати систем праћења сигурности брана. Током изградње, на одабраним мерним местима у и око бране уграђени су уређаји за мониторинг. Током периода експлоатације, велики број уређаја је замењен новим уређајима који су засновани на новим технологијама. Пошто се одређени уграђени уређаји не могу заменити (екстензометар у бетону, напонска ћелија, бетонски термометар, итд.), присуство оператера (људи) у процесу мониторинга и прикупљања података на брани је неизбежно приликом коришћења ових уређаја. У таквом процесу читања и бележења података могућа је људска грешка.

Увођење нових технологија, попут радиофреквентне идентификационе технологије (*RFID*), донело је нове могућности за поузданије прикупљање података на бранама, избегавајући скупу инсталацију нових сложених уређаја. Примена *RFID* технологије може повећати ефикасност процеса прикупљања података по приступачним ценама [6]. У [7], [8] аутори наводе да осим повратног финансијског улагања (*return of investments – ROI*), коришћење *RFID* технологије у процесу аутоматизованог праћења може елиминисати људску грешку. Додатне предности у даљинском надгледању бране могу се постићи коришћењем технологије интернета интелигентних уређаја (*Internet of Things – IoT*), разним сензорима и актуаторима.

Анализа литературе показује да се радови који се баве управљањем сигурношћу брана углавном заснивају на унапређењу софтвера ([9], [10], [11]). Кључна идеја у овој дисертацији је побољшање систем мониторинга брана коришћењем *RFID* и *Bluetooth* технологија на конкретном примеру велике бране хидроелектране (ХЕ) „Ђердап 1” на Дунаву. Ова дисертација је фокусирана на унапређење система за мануелни технички мониторинг, прикупљање података и трансформацију постојећег система у паметни аутоматизовани систем користећи доступне *IoT* технологије. Главна идеја овог решења је коришћење *RFID* технологије, која би требало да замени ручно прикупљање података и на тај начин побољша систем за мониторинг брана и унапреди сигурност екосистема. Додатно, решење се заснива на *Bluetooth* технологији, која омогућава аутоматизовани процес прикупљања података на брани, и на тај начин елиминише фактор људске грешке.

Модел је имплементиран на брани ХЕ „Ђердап 1”. Ова брана је највећа хидротехничка грађевина на Дунаву, половином управља Република Србија, а другом половином Република Румунија.

Предмет истраживања дисертације је развој модела и сервиса интернета интелигентних уређаја у систему управљања и одржавања брана. Централни проблем који се разматра у дисертацији је испитивање могућности примене концепата *IoT*-а и рачунарства у облаку (*cloud computing*) у систему за техничко осматрање брана.

Бране су комплексни објекти који перманентно представљају одређени ризик и потенцијалну опасност за подручје и екосистем који их окружују. Истраживања су показала да је питање сигурности бране, као и припадајућих објеката, од велике важности. Овај проблем је посебно значајан за високе бране (више од 15 метара). Под сигурношћу бране подразумева се да се она увек налази у стању у коме може да испуњава све своје пројектоване функције, без неповољних последица по људе, околину или имовину.

Бране, као и остали грађевински објекти, имају одређени век трајања. Током времена, расте и потреба да се стање брана ажурно прати и по потреби реагује да би се спречила могућност оштећења, рушења и неконтролисаног испуштања воде. Неопходно је пратити кључне параметре за функционисање брана. Мануелно техничко осматрање брана је проблематичније од аутоматског и полуаутоматског осматрања, јер у овом случају треба узети у обзир и људски фактор (могуће случајне грешке). Да би се минимизовале грешке и подаци мерења били поуздани, неопходно је смањити могућност људске грешке приликом читавања и уписивања измерене вредности на минималан ниво. Примена *IoT* инфраструктуре и сервиса, и *cloud computing*-а, подиже техничко осматрање на виши ниво, где се могућност људске грешке своди на минимум, а подаци постају поузданији.

За изградњу стабилног система осматрања неопходно је поседовање одговарајуће инфраструктуре. Инфраструктура треба да буде поуздана, дистрибуирана и скалабилна, да би могла да подржи раст броја сензора, чиме се повећава и број измерених података. *Cloud computing* се издваја као добро решење са аспекта скалабилности и трошкова. *Cloud computing* представља високо-скалабилну и апстраховану инфраструктуру, са виртуелизованим ресурсима.

За праћења стања објеката неопходно је да постоји добро пројектован систем техничког осматрања, са знатним бројем разноврсних инструмената и мерења. Сврха техничког осматрања је мерење низа релевантних величина, које могу да покажу да ли је стварно стање бране у експлоатацији у сагласности са предвиђеним функционисањем. Циљ прикупљања података је да се обезбеде информације на основу којих се може извршити идентификација и благовремена детекција процеса који могу да угрозе сигурност објекта.

Систем управљања безбедношћу обухвата обједињавање и стандардизацију прикупљања, аквизиције, архивирања, обраде и коришћења података о техничком осматрању [12]. Циљ СУБ-а је да омогући континуирано одржавање постојеће сигурности бране ХЕ „Ђердап 1”, а у случају потребе унапређивање и правовремено спречавање угрожавања сигурности.

СУБ треба да обезбеди континуирано праћење свих важних информација и ефикасно спровођење свих поступака стручне службе, везаних за сигурност бране. Затим, да омогући надлежним институцијама правовремено доношење одлука у вези са сигурношћу бране. Ово се спроводи формирањем јединственог информационог система за управљање подацима.

Концепт управљања сигурношћу брана обухвата низ поступака који имају за циљ да се направи физички систем са одговарајућом софтверском подршком. Систем треба да обезбеди сабирање свих података који су значајни за сигурност бране, анализу података и инжењерску интерпретацију. Интерпретација се одвија кроз математичке моделе релевантних процеса, контролу сигурности бране и доношење одговарајућих закључака у погледу мера које је потребно предузимати ради реализације сигурности. Основне функције система су обезбеђивање података који су значајни за сигурност бране (валидација, аквизиција, архивирање, одређивање техничког квалитета података и унифицирани приступ), као и праћење сигурности бране употребом математичких модела, са циљем континуалног праћења резултата мерења и провере сигурности бране. Процедуре и поступци управљања безбедношћу брана морају се непрекидно унапређивати у области техничког осматрања, у начину управљања подацима, као и у начинима коришћења података у поступцима

утврђивања сигурности објеката, а тиме и одређивања оптималног начина њиховог одржавања.

Систем за контролу квалитета мерених техничких података (ККМТП) представља важан део СУБ информационих система, а резултати овог слоја информационог система су у директној вези са поузданошћу спроведених анализа на основу измерених података [13]. Систем за контролу квалитета се састоји од два дела: валидације података и контроле квалитета мерених техничких података. Мерењем хидротехничких и осталих величина од користи за СУБ, формира се мерени технички податак, који осим вредности величине има и атрибуте који укључују запис о условима под којима је обављено мерење, време када је обављено мерење, информације о мерном инструменту, информације о стању мерне опреме и остале релевантне информације. Један од важнијих атрибута представља и информација о квалитету самог податка. Тај атрибут се додаје податку при уписивању у централну базу података, а израчунава се у процесу ККМТП.

Модел који је развијен у дисертацији обухвата инфраструктуру система за техничко осматрање брана, са фокусом на мануелно техничко осматрање, применом интернета интелигентних уређаја. Развијени модел се може користити за боље и прецизније предвиђање понашања брана, уз смањење људске грешке на минималан ниво да би се повећала тачност и поузданост података и унапредила сигурност на бранама.

Примена интелигентних уређаја у комбинацији са *cloud computing*-ом омогућиће прикупљање прецизнијих и поузданијих података. С обзиром на то да се прикупљени подаци користе за предвиђање понашања брана, унапређени систем техничког осматрања унапредиће сигурност брана и животног окружења.

Прикупљени подаци са брана не смеју бити доступни јавности, јер се могу злоупотребити. У постојећим системима могуће је приступити подацима искључиво преко апликације за преглед и анализу података, која захтева логовање корисника. Администрација корисника реализује се преко администраторског алата за управљање корисницима.

## 1.2 Циљеви истраживања

Примарни циљ истраживања у дисертацији је унапређење управљања и осматрања брана применом интернета интелигентних уређаја. Циљ дисертације се реализује кроз дефинисање модела и имплементацију технологија и концепата примене интернета интелигентних уређаја, чиме се креира савремена инфраструктура за техничко осматрање брана. Циљеви које треба постићи имплементацијом су:

- адаптација постојећег система техничког осматрања брана применом савремених интелигентних сензора;
- смањење људске грешке на минимални ниво при ручном прикупљању података применом технологија интернета интелигентних уређаја;
- унапређење система уноса података кроз развој савремених софтвера ради смањења људске грешке;
- унапређење квалитета података техничког осматрања;
- квалитетнија комуникација између оператера и сензора, и
- интеграција унапређеног модела техничког осматрања на постојећим инфраструктурама.

Савремени модел и сервис за техничко осматрање на бранама допринеће унапређењу система осматрања и безбеднијем функционисању бране. У основном облику, модел је општи, и биће имплементиран и тестиран у систему за управљање и осматрање бране ХЕ „Ђердап 1”. У општијем смислу, имплементација ће пружити основ за даљи развој модела и примену на другим бранама у Србији, а и шире, где год постоји потреба за техничким осматрањем.

### 1.3 Полазне хипотезе

Главна хипотеза која је тестирана у дисертацији гласи:

Применом унапређеног модела и сервиса за управљање и осматрање брана, заснованих на интернету интелигентних уређаја, унапређује се техничко осматрање, смањује се фактор људске грешке, повећава поузданост и тачност података, прецизније се предвиђа понашање бране и побољшава сигурност објекта.

На основу дефинисаног предмета истраживања, могу се издвојити неколико посебних хипотеза. Даљим прецизирањем наведених посебних хипотеза, формулишу се појединачне које се односе на елементарне чиниоце предмета истраживања.

X1. Могуће је унапредити управљање и осматрање брана развојем модела мануелног техничког осматрања заснованог на интернету интелигентних уређаја.

X2. Увођењем интернета интелигентних уређаја у процесе управљања и осматрања брана, омогућава се развој напредних метода контроле квалитета мерених техничких података.

X3. Примена интернета интелигентних уређаја у управљању и осматрању брана доприноси бољем увиду у стање објекта и ствара услове за њихово оптимално одржавање.

Даљим прецизирањем наведених посебних хипотеза, формулишу се појединачне које се односе на елементарне чиниоце предмета истраживања.

X1.1. Могуће је развити систем заснован на *IoT*-у за мерење виталних параметара и параметара окружења.

X1.2. Развијени модел је могуће прилагодити потребама осматрања конкретних брана.

X1.3. Доступност података у моделу техничког осматрања заснованом на *IoT*-у могуће је унапредити применом *cloud computing*-а.

X2.1. Применом техничког осматрања заснованог на *IoT*-у могуће је редуковати грешке изазване људским фактором.

X2.2. Поузданост података повећава се применом нових метода контроле квалитета мерених техничких података.

X3.1. Развијене методе контроле квалитета мерених техничких података, засноване на *IoT*-у, могу се инкорпорирати у постојеће системе за управљање безбедношћу брана, чиме се постиже поузданија оцена стања и сигурности брана.

X3.2. Примена развијеног модела доприноси вишем степену сигурности брана, безбедности становништва и екосистема.

### 1.4 Методе истраживања

Методологија истраживања у дисертацији обухватиће сложен и организован поступак, полазећи од логичких начела и принципа по утврђеним фазама. У сврху израде дисертације, од општих научних метода коришћене су методе прикупљања и анализе постојећих научних резултата и достигнућа, моделирање, аналитичко-дедуктивна и статистичка метода. Моделирање се користи приликом израде модела инфраструктуре ручног прикупљања и уноса података, заснованог на примени интелигентних сензора. Аналитичко-дедуктивне методе користе се за анализу података о постојећим решењима, као и о технологијама, приступима и библиотекама за развој софтверских компонената. Мерење релевантних параметара и анализа добијених резултата биће обављени помоћу стандардних статистичких метода.

У експерименталном делу биће евалуиран развијени модел. Добијени резултати експеримента треба да потврде главну хипотезу о унапређењу система за осматрање брана и побољшању коначних резултата у процесу сигурности брана.

Ово истраживање се може класификовати по општости као појединачно (обухвата само једну компоненту појаве, процеса и односа у строго одређеној јединици времена и простора), по критеријуму својства предмета, као комплексно (уједначено учешће теоријског и емпиријског), по критеријуму времена једне појаве, као трансверзално (пресек појаве у једном временском одсечку), по припадности науци, као интердисциплинарно, по актуелности предмета као актуелно, по сврси и циљевима, иновационо-хеуристичко (усмерено на откривање непознатих неоткривених чинилаца, својстава и односа предмета истраживања), а по функцији у развоју науке припада акционом истраживању (решава конкретан актуелни проблем на основу изграђеног научног сазнања).

Резултати истраживања биће презентовани текстуално, описивањем, и приказани у више табела, слика и дијаграма са упоредним резултатима. Синтеза, апстракција, генерализација и класификација, као и остале методе научног објашњења, биће примењене у закључивању на основу индукције и дедукције.

## 2. ПАМЕТНО УПРАВЉАЊЕ БРАНАМА

### 2.1 Концепт паметних брана

Бране пружају широк спектар друштвених, економских и еколошких користи, помажући у контроли протока воде, стварању хидроелектрана, контроли поплава, управљању отпадом, навигационим сврхама, и делују као станишта за водени живот [14].

У последњој деценији било је могуће видети све више штете и кварова на бранама услед старења, земљотреса и климатских промена. Из тих разлога, безбедност брана свакодневно постаје све важнија у смислу управљања катастрофама на националном нивоу. У свету постоје бројне организације које су одговорне за безбедност брана, а неке од њих су: Међународна комисија за велике бране (*International Commission on Large Dams - ICOLD*), Удружење за безбедност бране (*Association of State Dam Safety Officials - ASDSO*), Међуресорни одбор за безбедност бране (*Interagency Committee on Dam Safety - ICODS*), Национални одбор за безбедност бране (*National Dam Safety Review Board*) и Интересна група за безбедност брана (*Dam Safety Interest Group - DSIG*).

Кварови на брани могу бити:

- структурални;
- хидраулички; или
- механички.

#### Структурални кварови

Кварови темеља, укључујући нестабилност насеља и падина (клизишта), или штете проузроковане земљотресима, разлог су око 30 процената свих кварова на бранама у Америци [15]. Приликом пројектовања конструкција бране, планира се да оне трају више деценија. Према *ASDSO*, тренутна просечна старост брана у Америци је 56 година, што представља знатан број година у односу на пројектовани живот бране. Због тога је неопходно да власници редовно врше свеобухватне инспекције структура бране, како би верификовали њену стабилност и идентификовали и реаговали на ране индикације о компромитујућем структуралном понашању, попут пукотина, слегања или померања подземне површине.

Иако није могуће уградити трајне сензоре на сваком квадратном метру бране, инспектори за сигурност имају више могућности од једноставног препознавања развојних рањивости и прописивања програмских визуелних прегледа. Интелигентне и повезане сензорске технологије могу да прате структурне перформансе са много бољом прецизношћу него што их може ручно обављати особље за мониторинг, а трошкови су знатно мањи него икад раније.

#### Хидраулички кварови

Преливање бране је чест узрок њихове пропасти [15]. Америчка национална статистика показује да долази до преливања услед неадекватног пројектовања прелива, блокаде преливног канала, процуривања или слегања круне бране, што представља око 34 процената свих отказа брана у Америци.

Догађаји као што су падавине, главни су покретач хидрауличких кварова. Кише, топљење снега и други фактори животне средине, могу довести до прекомерног прилива површинске воде у акумулацију. Током прилива велике количине воде неопходно је активно управљање протоком воде и нивоима. У многим случајевима, службе осматрања не само да треба да обраћају пажњу на осмотрене метеоролошке карактеристике у непосредној близини већ морају да прате њихов утицај на целокупни слив и да координирају са доносиоцима одлука у сливу да би се правилно управљало водним ресурсима слива. У појединим регионима то је додатно закомпликовано прописима, који захтевају прописане сезонске одливе воде за одржавање станишта риба. Ови оперативни проблеми, климатске промене које изазивају

погоршане временске догађаје и дуже суше, велики су изазов за оператере на бранама у Америци и у свету.

Такође, вода може бити један од фактора који прави највећу ерозију, посебно када је реч о стени, металу и бетону. Иако вода преовлађује на целој брани, постоје одређена подручја у којима вода не би требало да постоји. Због тога, ако се уочи капљање или процуривање неопходна је хитна акција да би се спречиле потенцијалне катастрофе.

Мреже фиксираних сензора за мерење метеоролошких величина, за које нису потребна велика одржавања, могу се финансијски исплативо распоредити на великим површинама користећи *IoT* технологије. Повећања енергетске ефикасности смањила су величину и трошкове електроенергетских система. Флексибилни уређаји повезивања (бежични, мобилни и сателитски) повећали су поузданост система. *Edge computing*, ефикаснија комуникација и протоколи за управљање учинили су сензорске мреже динамичнијим и ефикаснијим током критичних догађаја.

Сензорске мреже које прате влагу земљишта, подземне воде и процуривање, постављене у стратешким областима у и око бране, могу ефикасно да препознају промене у свакодневним перформансама конструкције.

### **Механички кварови**

Неисправне уставе и затварачнице, водови или вентили, могу проузроковати квар бране или поплаву и узводно и низводно од ње, и представљају око 36 процената свих кварова на бранама у Америци [15]. Преливне и излазне структуре кључни су елемент сваке бране. Правилно управљање преливним и излазним структурама омогућава оператерима да управљају нивоом воде у акумулацији и спречавају преливање. Међутим, с временом улаз или излаз на ове конструкције може бити препречен или запушен, што представља знатну претњу за безбедност бране. Уобичајене препреке су нагомилавање седимената и смеће из околине. Ако прелив не ради исправно, или садржи стајаћу воду у дужем периоду, може брже да оштети инфраструктуру, што доводи до даљег ризика од квара. Стога је неопходно да се блокаде уклоне што је брже могуће.

Осим тога, инфраструктура брана наставља да стари, због тога јој је неопходна стална инспекција, која ће постајати све тежа и критичнија да се спроведе. Удаљена локација многих објеката додатно отежава овај проблем и смањује ефикасност радне снаге која има задатак да управља тим средствима.

Могућност даљинског снимања и анализирања података, који се састоје од даљинског испитивања и мрежа уграђених сензора на различитим тачкама бране и око ње, омогућава радницима да изврше виртуелне инспекције онолико често колико је прописано или потребно да реагују на било коју идентификовану потребу. Све ово је могуће без размештања радне снаге за извршавање задатка. Поред значајних уштеда трошкова, које то подразумева, додатна корист правремене идентификације проблема драстично смањује ризик од већих оштећења грађевине и може знатно да продужи ефикасан живот водене инфраструктуре.

Начин могућег рушења бране зависи и од врсте бране [1]. Бране се граде помоћу различитих система конструкције и материјала. Према материјалу и конструктивном систему, бране се могу поделити на:

- насуте бране;
- бетонске бране;
- зидане бране;
- остале бране.

**Насуте бране** могу бити: земљане, од каменог набачаја са вертикалним или косим глиненим језгром, од каменог набачаја са узводним екраном од бетона, асфалта или другог материјала и

од каменог набачаја са дијафрагмом. **Бетонске бране** деле се на: гравитационе, олакшане гравитационе, контрафорне са равним, или залученим екраном и лучне бране

Најбржи лом се дешава на лучним бранама, док је релативно спор на насутим и гравитационим бетонским [1]. Процена лома бране мора препознати све значајне потенцијалне облике лома и спровести одговарајуће анализе да би се гарантовала сигурност бране. Брана се сматра сигурном ако не дође до клизања, прекорачења чврстоће конструкције или темеља, испирања материјала, или било ког другог облика лома. Уколико се на време не уочи или идентификује потенцијални тип лома, онда и најпрефињеније методе прорачуна не могу помоћи са великом тачношћу. Ломови брана који су се десили у прошлости, не гарантују да су препознати сви облици ломова брана, јер већина тих ломова није технички документована на адекватан начин и комбинација је више фактора који су утицали на лом бране.

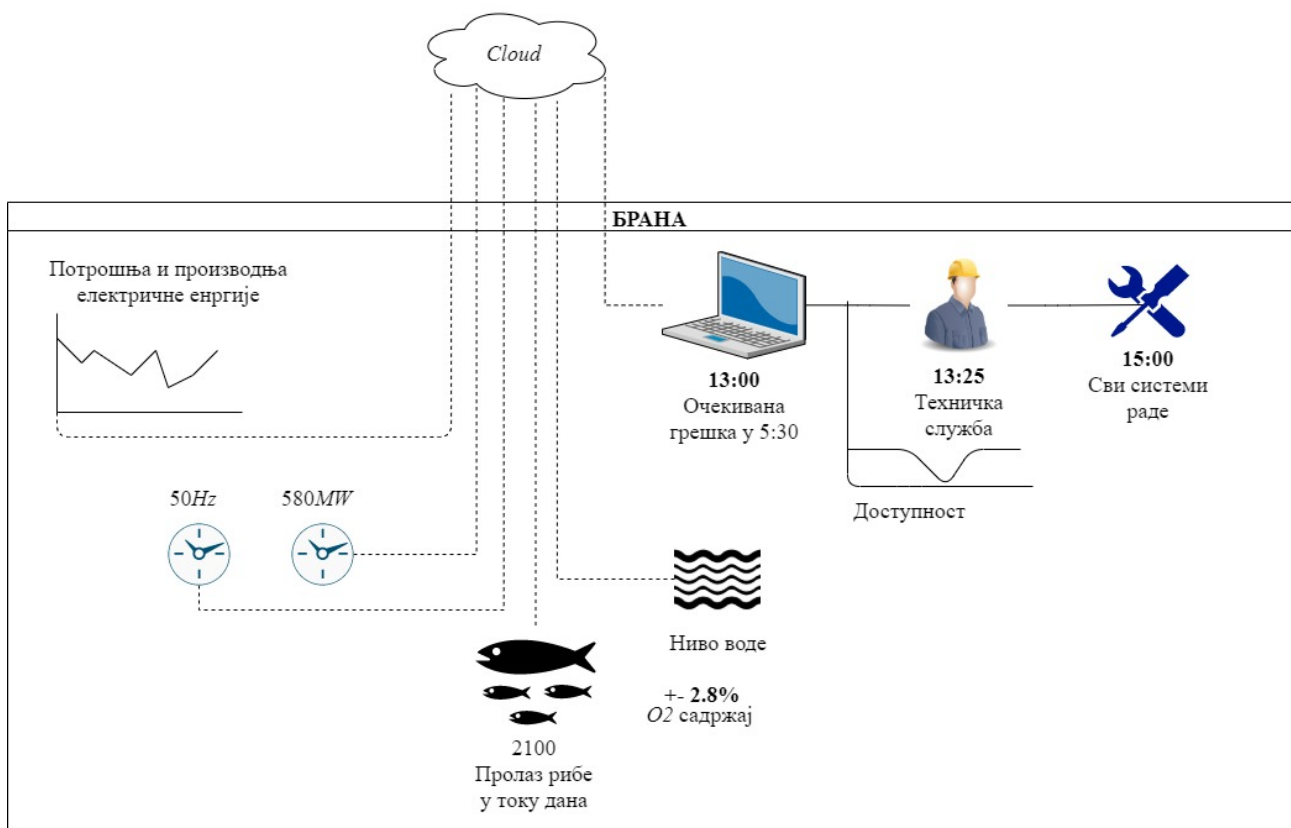
Могући узроци рушења брана су [1]:

- екстремни природни утицаји (изузетне поплаве и преливање воде из акумулације, земљотрес, појава нетектонских померања, дејство таласа из акумулације изазваним појавом великих клизишта на падинама акумулације);
- деградација материјала бране или темеља (дуготрајне промене физичких, хемијских и механичких карактеристика материјала у телу и темељу бране под дејством спољних утицаја – воде, мраза, високих температура итд.);
- квар опреме (квар затварача на евакуационим органима, квар опреме задужене за нормално функционисање дренажног система, и сл.);
- екстремни антропогени утицаји (експлозије и сл.).

Иако је у већини случајева узрок рушења брана нека природна појава, одговорност је на човеку, јер их је лоше направио или одржавао. Са ове тачке гледишта, узроци рушења могу се класификовати на: грешке у пројектовању и/или извођењу радова, грешке у управљању и одржавању бране и ратна дејства и терористички напади.

У [16] аутори су објаснили шта је паметна брана. Паметна брана је нови концепт који се базира на дигиталним бранама усвајањем информационих технологија нове генерације, као што су *IoT*, *cloud computing-a*, *Big data* и друге паметне технологије (Слика 1). Овај концепт такође значи специфичан интелигентни систем управљања и рада бране, који је динамичан, префињен и препознатљив у анализи и контроли. Осим тога, паметна брана често има специфичне карактеристике, као што су интегритет, интероперабилност, могућност фузије, аутономија и робусност [16].



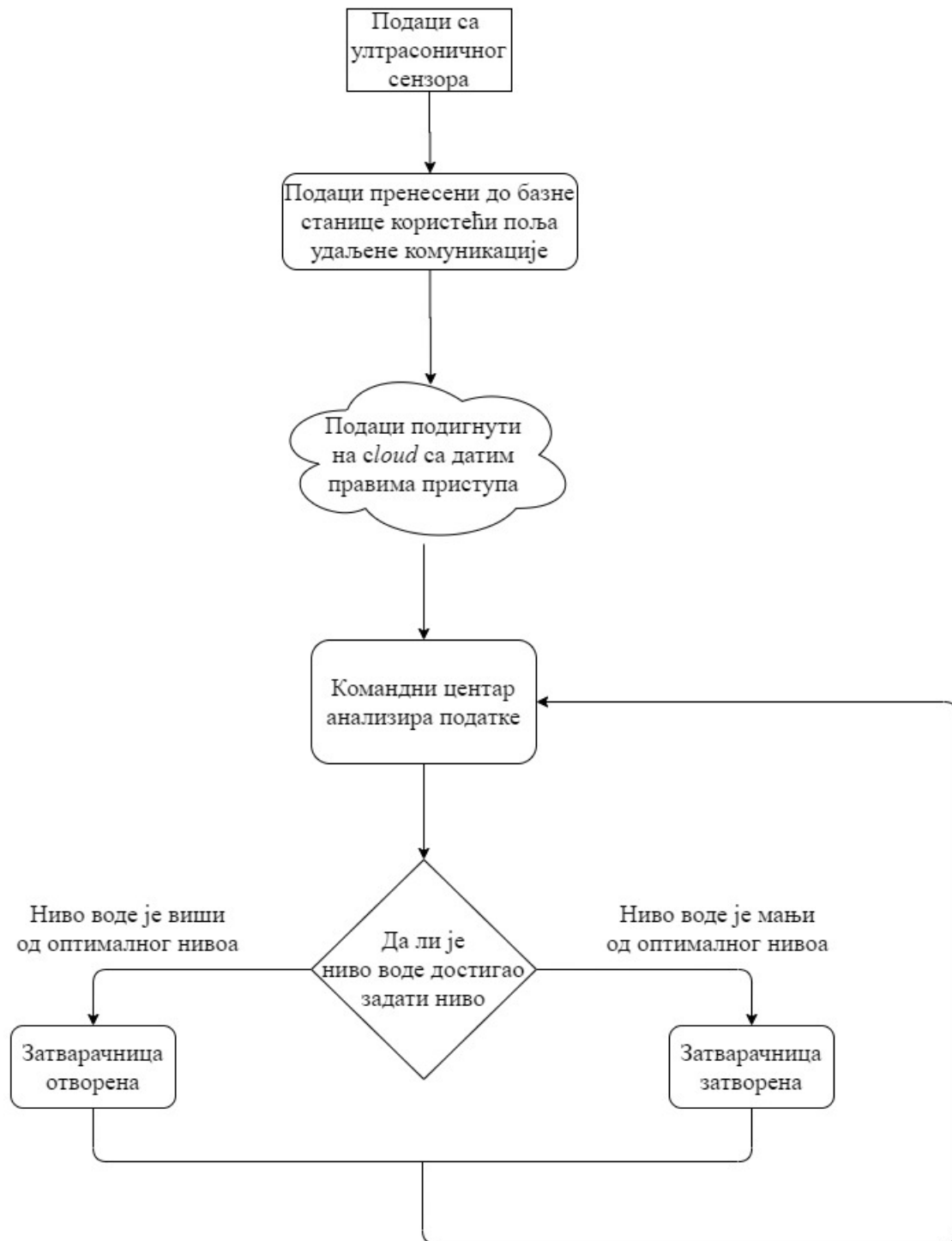


Слика 1. Концепт паметне бране (хидроелектране) [17]

## 2.2 Анализа литературе

Осматрање брана једна је од важних мера за осигурање њихове безбедности. Ово је важна активност у раду и управљању браном [18]. Рачунарски софтвер има кључну улогу у праћењу безбедности брана. Бројни власници брана развили су и имплементирали информационе системе за надзор и управљање сигурношћу бране да би олакшали управљање и анализу података. У [19], *Bao* и други аутори описују пример компаније *Fujian Electric Power Company*, која у источној Кини управља са 27 различитих брана: бетонске, земљане, лучне и насуте бране. Све бране су размештене у удаљеним руралним подручјима, услед чега је било тешко управљати сигурносним информацијама за све бране. Због тога је компанији *Fujian Electric Power* било важно да развије и унапреди информациони систем за даљинско управљање системом надзора, сакупљања и преноса података о безбедности брана, тако да се све те информације могу обрађивати, анализирати и вредновати како би се ефектно донела одлука о статусу безбедности брана. Информациони систем примењен је на скупу брана којима управља *Fujian Electric Power Company*, где се може користити систем за анализу и процену података. У [18] аутори приказују систем управљања безбедношћу бране „Првонек” у Врању, Република Србија. Развијени софтвер помаже запосленима у мониторингу и процени стања бране. Систем се састоји од неколико софтвера који су задужени за безбедност бране.

Употреба *IoT*-а у осматрању брана још увек није често заступљена у пракси, али *IoT* постепено доживљава експанзију у мониторингу. У [20], [21] аутори спомињу употребу *IoT*-а у осматрању брана и слање података у реалном времену. *Siddula* и други аутори предлажу иновативно решење за прикупљање и размену података о нивоу воде, између сензора и ауторизованог центра, у реалном времену. На основу тога центар одлучује да ли треба отворити или затворити затварачнице на брани. Алгоритам за отварање или затварање затварачница приказан је на следећој слици (Слика 2).

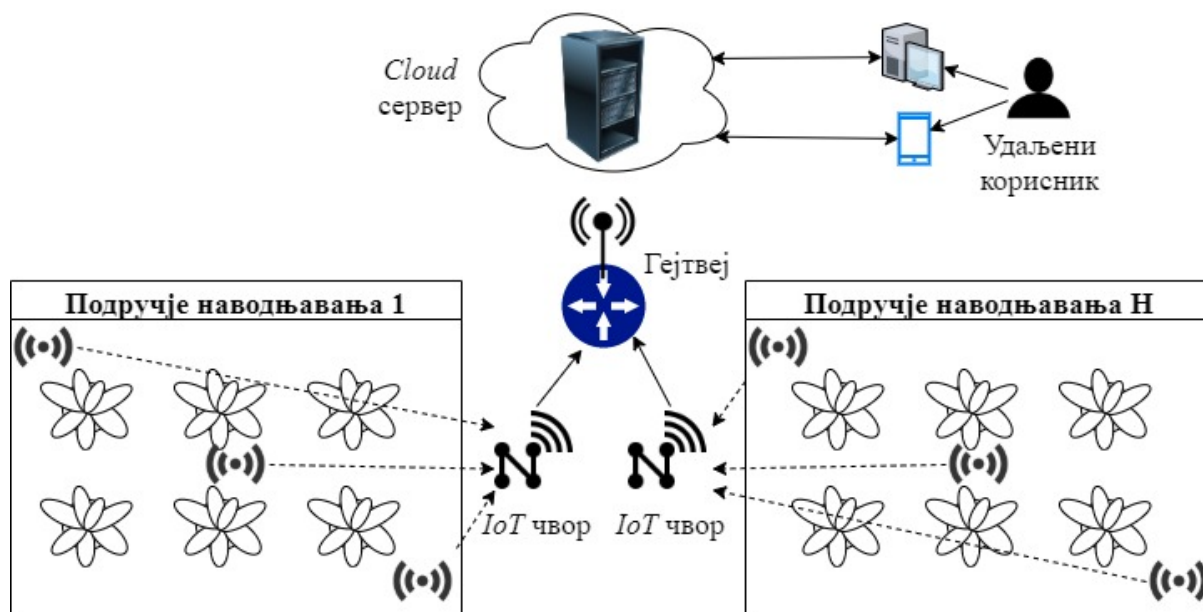


Слика 2. Алгоритам за отварање или затварање затварачница на брани [20]

*Varghese* и други аутори за сличну проблематику предлажу мехатронички систем за отварање и затварање затварачница. Систем се састоји од сензорских чворова, паметног контролера и комуникационог система. Систем може да ради као ауто-пилот или мануелно [21].

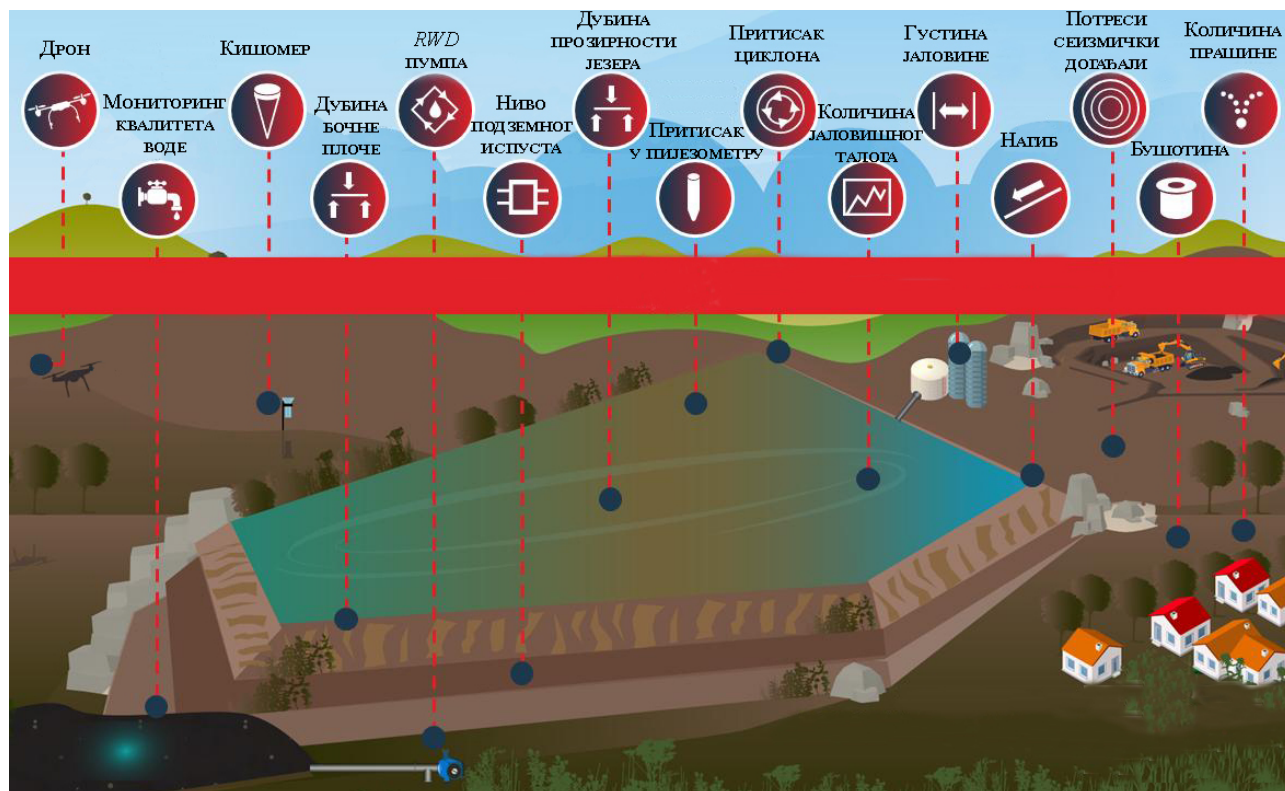
У [22] аутори су показали спој управљања браном, *IoT*-а и наводњавања (Слика 3). Аутори су представили систем под називом *IoT-DWM (Internet of Things based Dam Water Management system)* који се бави смањењем губитка воде. Систем се састоји од три секције: поље сензора, *IoT* мреже и контроле бране. Параметри (подаци) могу се проматрати кроз различите сензоре постављене у пољопривредном подручју. Сви очитани подаци шаљу се у *cloud*. Оператер на брани прима ажурне податке са одређеног подручја и процењује потребу за водом. Потреба за водом варира зависно од усева који се узгајају у том подручју. Док процењује потребу за

водом, оператер разматра различите параметре, као што су врста усева у том подручју, температура, влага и брзина ветра.



Слика 3. IoT-DWM [22]

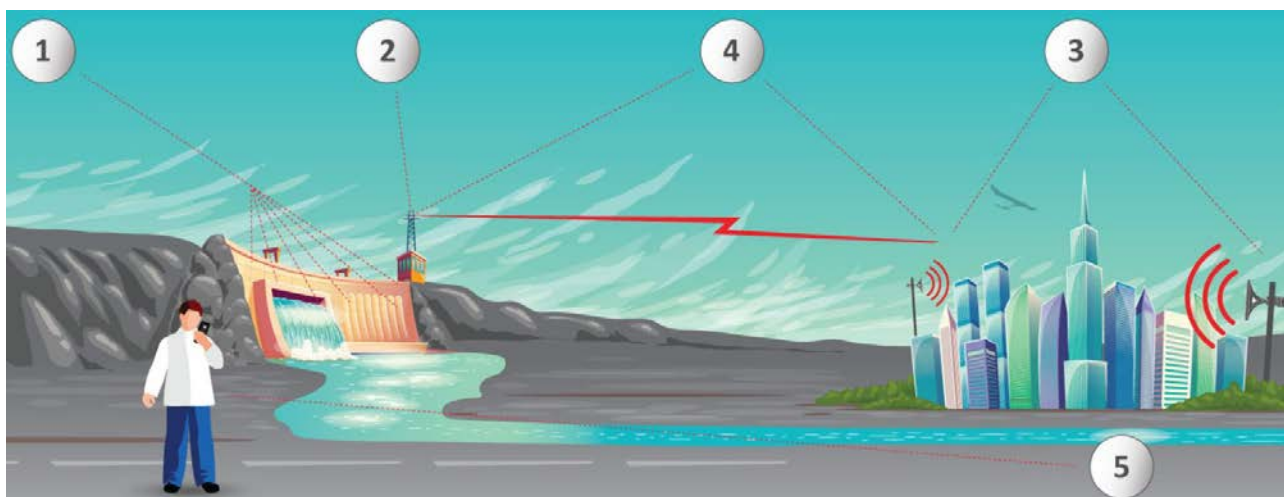
Raptor решење, које су развиле компаније IsoMetrix и IoT.nxt, а које се користи за управљање јаловишним бранама, приказано је на слици која следи (Слика 4). На слици је могуће видети више сензора који се користе на јаловишним бранама.



Слика 4. Управљање јаловишним бранама [23], [24]

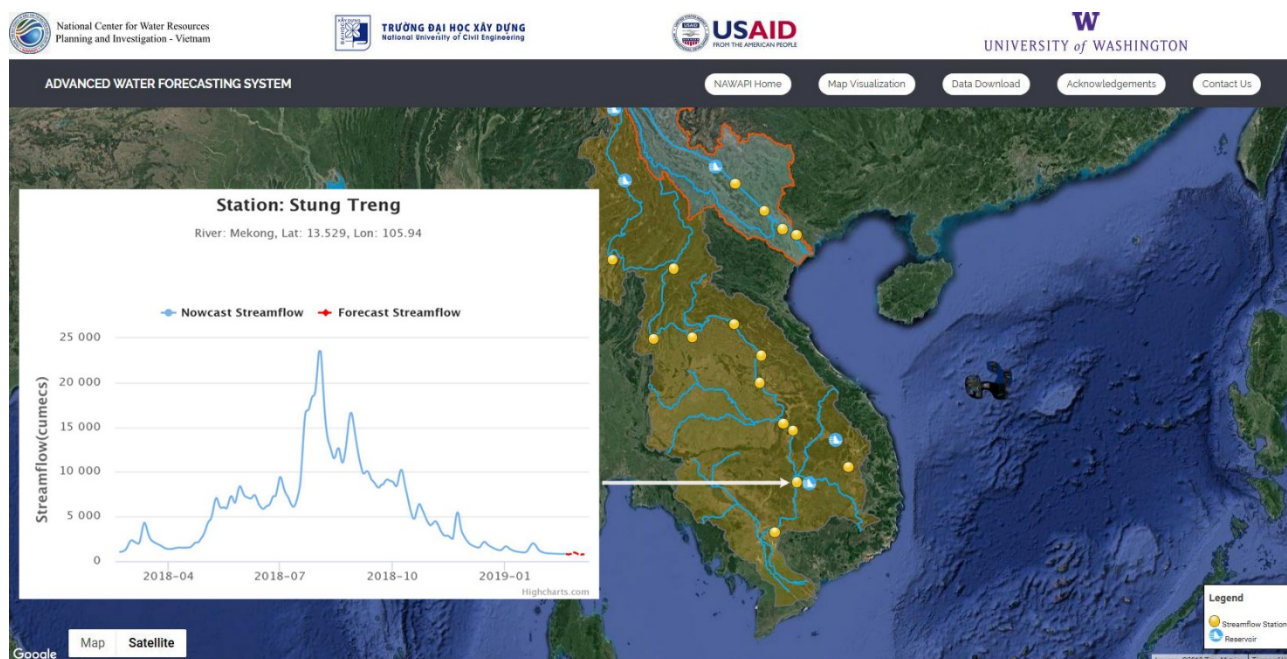
Компанија Telegrafija направила је софтверски систем за упозоравање на бранама и акумулацијама (Слика 5). Систем се састоји од осматрања, упозоравања и нотификација. Саставни део система су: мониторинг и сензорска мрежа (1); контролни центар (2); интерне и

екстерне сирене (3); комуникациона инфраструктура (4); и одговорне особе/особе које се обавештавају (5).



Слика 5. Систем упозоравања на бранама и акумулацијама [25]

Вијетнамски и амерички истраживачи учествовали су у развоју сателитског приступа систему за надгледање и управљање прекограничним поплавама [26]. Тимови из Вијетнамског националног центра за планирање и истраживање водних ресурса (NAWAPI) и Универзитета у Вашингтону заједно су развили и применили напредни систем за прогнозирање кретања и нивоа воде. У Вијетнаму је покренут сателитски систем који има за циљ да побољша правовремени приступ информацијама о акумулацијама узводно у прекограничним речним сливовима Црвене и Меконг реке. Прекривање облацима током сезоне монсуна и ограничен приступ интернету, показали су се као изазов за земље у развоју у Јужној Азији. Истраживачи предлажу решење коришћењем рачунарских сервиса заснованих на *cloud*-у и синтетичким радарским инструментима који стварају слике високе резолуције, који се монтирају на ваздушне или свемирске летелице. Софтверски систем сателитског предвиђања кретања и нивоа воде приказан је на слици 6.

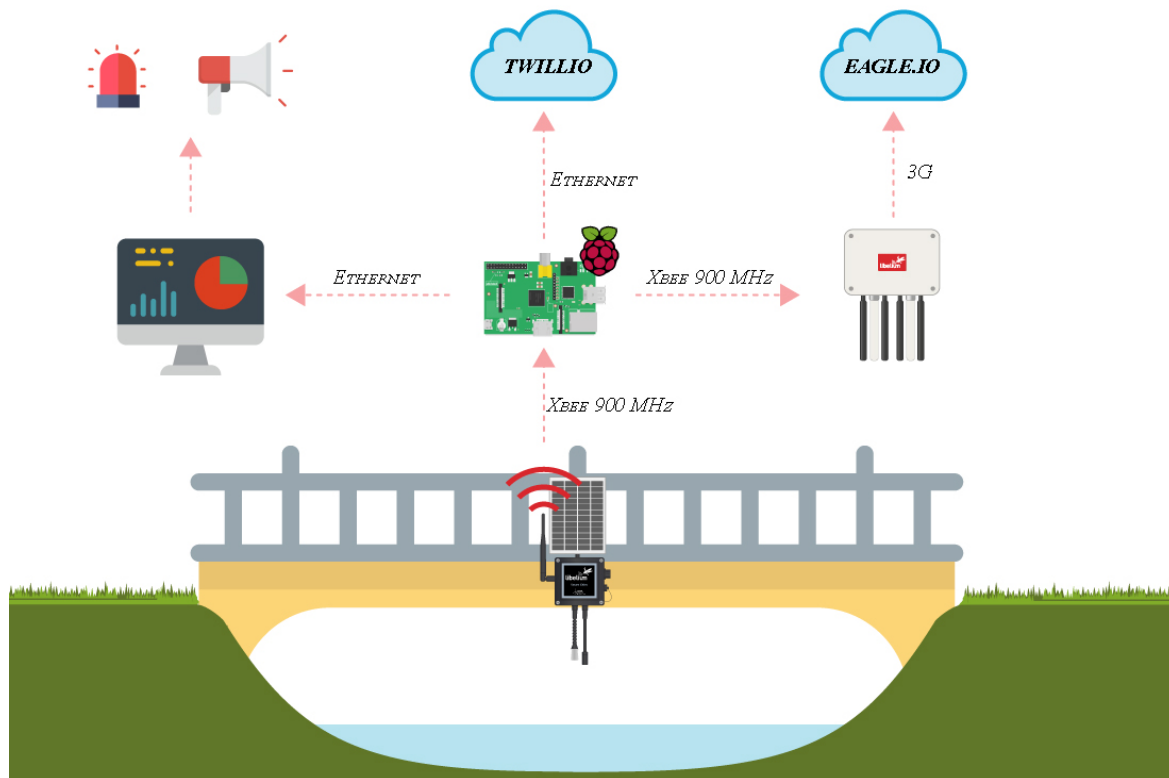


Слика 6. Систем за предвиђање кретања и нивоа вода [26]

Колумбијска компанија *Federmán Comunicaciones*, направила је решење за рану најаву поплава у Колумбији [27]. Систем је развијен на три реке: Либоријана, Клара и Барозо.

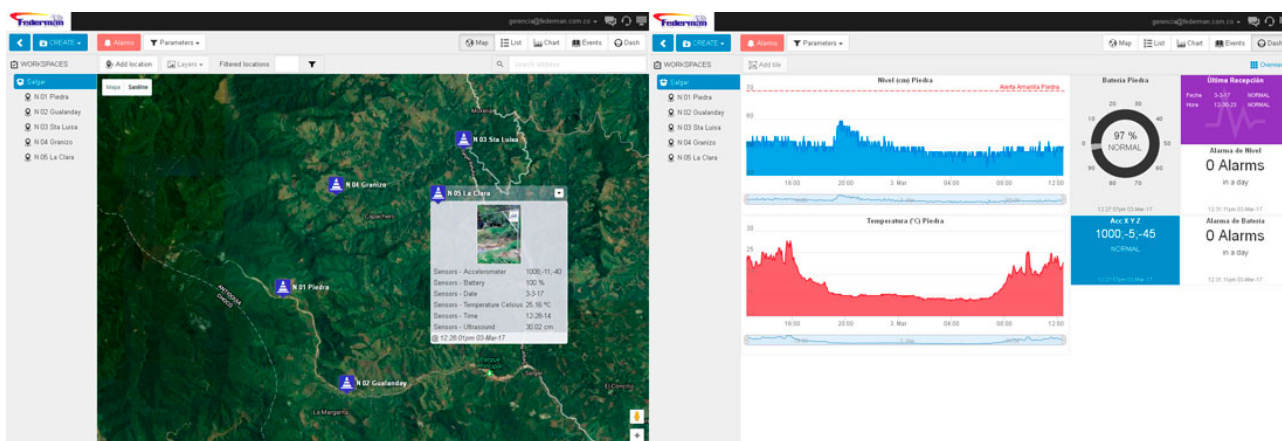


Бежична сензорска мрежа *Waspote* континуирано прати нивое река и температуру ваздуха како би упозорила заједницу у случају потенцијалне поплаве или клизишта. Сирене су постављене у општинама и у поплавном подручју. У *Salgar* пројекту су коришћени *Raspberry Pi 3B* и *cloud computing* технологија (Слика 7).



Слика 7. Комуникациони дијаграм у *Salgar* пројекту [27]

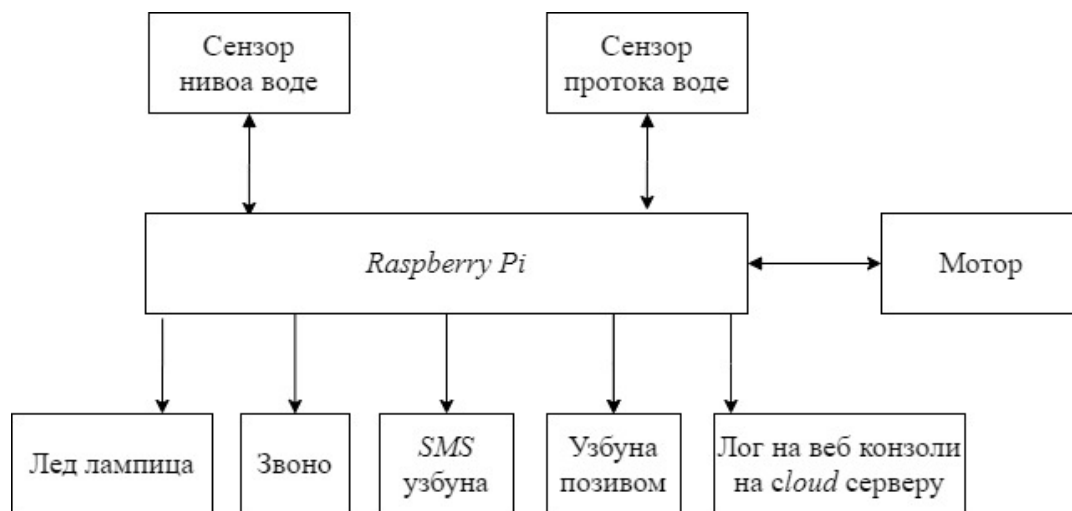
Главни циљ пројекта је контрола понашања речних сливова и прибављање информација у реалном времену ради генерисања упозорења уколико су ограничења прекорачена. У случају узбуне, и ако је потребно, контролна јединица мора да активира сирене и систем јавних адреса за људе који се евакуишу из подручја ризика. Ова јавна инвестиција има за крајњи циљ пружање сигурности и заштиту заједнице од природних катастрофа. На следећој слици (Слика 8) приказан је изглед софтвера који се користи у *Salgar* пројекту.



Слика 8. Софтвер који се користи у *Salgar* пројекту [27]

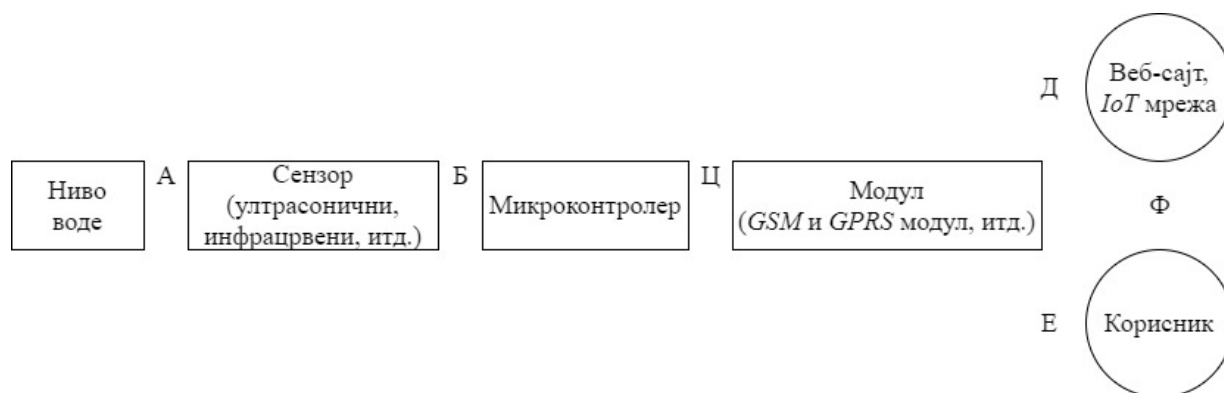
Помоћу савремених јефтених технологија, као што је *Arduino* (микроконтролер), могуће је управљати системима који мере ниво воде [28]. У споменутом раду аутори користе *Arduino* и сензоре (спадају у јефтину технологију), који мере ниво воде да би укључили или искључили пумпу која доводи воду до акумулације. *Lambrou* и други аутори баве се сензорима који су

јефтине, лагани за примену и обезбеђују поуздан и дуготрајан рад [29]. Сензори мере квалитет воде у цевима. Експериментални резултати су показали да је овај јефтини систем способан да детектује састојке који су штетни (контаминирани) у прилично ниским концентрацијама. У [30] аутори су користили *Arduino* и јефтине сензоре, док у [31] аутори су испитивали квалитет воде коришћењем *Raspberry Pi B+* (микрорачунар). Систем се састоји од више сензора који се користе за мерење физичких и хемијских параметара воде. Мерени параметри су температура, *pH*, замућеност и проток воде. Аутори у [32] објашњавају важност брана у наводњавању, контроли поплава и генерисању електричне енергије. Аутори се баве бранама у Индији, којих има око 4.200 (високих и ниских). У раду се користе сензори повезани на *Raspberry Pi 3* који помоћу *IoT* технологије прослеђују податке на веб-сајт. Велике количине воде, тј. поплаве, међу опаснијим су елементарним непогодама, јер могу да униште многе животе и животно окружење [33]. Поплаве се углавном јављају због обилних киша и преливања кроз евакуационе органе брана. Због тога је од кључног значаја развити систем раног откривања поплава, који у друштву шири свест о утицају пораста нивоа вода на регионе који су подложни поплавама. Аутори предлажу коришћење *Raspberry Pi*, различитих сензора и *Way2SMS API*-ја који служе за слање порука упозорења уколико закаже интернет конекција (Слика 9). У систему је развијена опција за позивање људи у току ноћи уколико дође до поплава.



Слика 9. Систем за узбуну у случају поплава [33]

У [34] аутори предлажу употребу *Arduino* и ултрасоничног сензора који очитава податке и шаље у *cloud*. У систему ране детекције поплава (*Flood Early Warning Detection System – FEWDS*) сензор мери ниво воде и помоћу *GSM* и *GPRS* модула прослеђује податке (Слика 10).



Слика 10. Унапређени систем *FEWDS* [34]

Да би предупредили могућност поплава и направили систем раног узбуњивања, аутори у [35] предлажу употребу *IoT*-а и микроелектромеханичког система (*microelectromechanical systems – MEMS*), који би радио мониторинг у близини бране. Комбинација ове две технологије

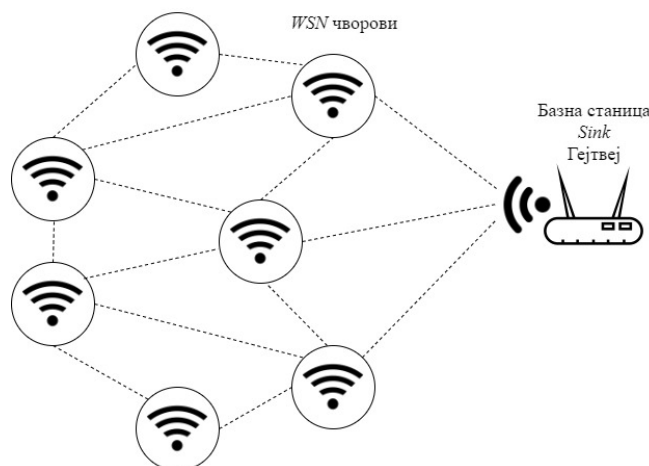
омогућава мерење нивоа воде, температуре и влажности. У [36] аутори такође предлажу употребу *IoT*-а са циљем спречавања поплава у Малезији. Аутори су развили систем праћења поплава и систем раног упозоравања у реалном времену, користећи бежични сензорски чвор на подручју подложном поплавама. У основи, сензорски чвор се састоји од ултразвучног сензора и сензора за кишу којим управља *NodeMCU*, као микроконтролер система, који се поставља на идентификовано поплавно подручје. Подаци о нивоу поплаве шаљу се на *e-mail*, што може помоћи разним организацијама у даљем унапређивању система и предвиђању поплава.

Неопходно је периодично пратити квалитет и ниво воде у акумулацији и временске услове да би се предвидео улазни проток воде у акумулацију [37]. Аутори предлажу употребу системске архитектуре састављене од два *cloud*-а: *cloud* сензора, и *UAV (unmanned aerial vehicle) cloud*, пројектованих за мониторинг бране. Први *cloud* пружа податке сензора, док их други прикупља и доставља центру за мониторинг бране. Систем је заснован на *Blockchain* технологији, која омогућава аутентификацију, складиштење, интегритет података, итд. У [14] аутори су предложили и имплементирали нову идеју, базирану на *IoT*-у, о аутоматизацији процеса у управљању бранама и прикупљању података о водостају да би контролисали рад бране. Ово решење поједностављује контролу брана у Индији и смањује радну снагу за одржавање брана.

У [38] аутори предлажу употребу бежичних сензорских мрежа (*Wireless Sensor Network – WSN*) и *Zigbee* технологију у надзору наводњавања. Параметри који су укључени у контролу резерве воде су ниво воде и кретање мотора уставе, који контролише проток воде. Подаци сензора мере се у реалном времену и шаљу у базу станицу или контролну/надзорну собу. Развијена платформа је исплатива и омогућава лако прилагођавање. *Thekkil* и други аутори објашњавају битност бележења у реалном времену достигнуте висине воде и процуривање воде кроз зидове брана [39]. Ови подаци су битни да би се избегле поплаве, а самим тим и људске жртве. Аутори предлажу употребу *WSN*-а у реалном времену за рано откривање поплава и систем мониторинга у реалном времену. Систем користи *Zigbee* и *GSM* мрежу за пренос података.

На грађевинским објектима попут брана, мостова, зграда, битно је током времена пратити стање структуре грађевине (*Structural Health Monitoring – SHM*). *SHM* се користи за континуирано мерење кључних параметара, структуралних и еколошких услова у реалном времену [40]. Намена *SHM* је откривање оштећења конструкције, безбедност, ублажавање катастрофа итд. На мостовима и бранама бежични сензори мере убрзање, нагиб стуба моста и ниво воде.

Бежичне сензорске мреже користе се у индустрији, праћењу урбаних терена и надзору цивилних структура, сигурности и надзора, паметним зградама итд. *WSN* се састоји од бројних чворова и једне или више базних станица (Слика 11).



Слика 11. *WSN* мрежа [41]

У [40] аутори су користили на мосту *WSN*, сензоре акцелерометра и ултразвучни сензор. Изградња брана и насипа, наводњавање и антропогене активности утичу на квалитет воде [42]. Праћење квалитета воде захтева прикупљање великог броја узорака и одређени период чекања док резултати не буду доступни. Аутори предлажу *WSN* и систем праћења, који се контролише помоћу *online* доступног интерфејса који омогућава даљинско надгледање путем интернета. Систем је примењен у Киркларели, Турска. [41] такође предлажу употребу *WSN*-а у осматрању квалитета вода.

Вештачка интелигенција (*Artificial Intelligence - AI*), роботика и *IoT* привлаче велику пажњу и очекује се да ће ове технологије променити друштво у будућности [43]. Ове иновативне технологије имају потенцијал за изградњу: (1) комуникационог друштва без граница; (2) симбиозе између људи и робота; и (3) сигурног и умреженог друштва. Аутор је представио специфична решења компаније *Panasonic*: (1) решење за аутоматско превођење; (2) роботизовано решење за испитивање сигурности бране; и (3) безбедносно решење великог капацитета. Сва ова решења треба да су повезана са *cloud*-ом и евалуирају у напреднији систем.

У табели која следи (Табела 1) приказани су издвојени пројекти из области мониторинга са називом и описом пројекта. Пројекат СУБ, који је реализован у Србији, основа је развијеног модела мануелног техничког осматрања брана, презентованог у дисертацији.

Табела 1. Пројекти мониторинга брана и речних сливова

Назив пројекта	Опис
<b>СУБ</b> [18]	<ul style="list-style-type: none"> <li>• Институт за водопривреду „Јарослав Черни“</li> <li>• скуп софтвера за мониторинг бране</li> <li>• брана ХЕ „Ђердап 1“ (Кладово), ХЕ „Ђердап 2“ (Неготин), „Првонек“ (Врање), ХЕ „Власина“ (Сурдулица)</li> <li>• Србија</li> </ul>
<b>KDSMS</b> [44]	<ul style="list-style-type: none"> <li>• <i>Kwater</i></li> <li>• управљање 30 великих брана</li> <li>• систем за управљање безбедношћу брана</li> <li>• Кореја</li> </ul>
<b>DSMMIS</b> [45]	<ul style="list-style-type: none"> <li>• <i>Browser/Server</i> архитектура</li> <li>• брана БиКоу</li> </ul>
<b>IEWSDS</b> [46]	<ul style="list-style-type: none"> <li>• брана се посматра као витални и интелигентни систем</li> <li>• интелигентни системи раног упозоравања</li> </ul>
<b>TDMPAS</b> [47]	<ul style="list-style-type: none"> <li>• употреба <i>IoT</i>-а и <i>cloud computing</i>-а</li> <li>• јаловишна брана</li> </ul>
<b>FEWDS</b> [34]	<ul style="list-style-type: none"> <li>• систем ране детекције поплава</li> <li>• употреба <i>Arduino</i> и ултрасоничног сензора</li> <li>• употреба <i>GSM</i> и <i>GPRS</i> модула</li> </ul>
<b>MEMS</b> [35]	<ul style="list-style-type: none"> <li>• систем раног узбуђивања</li> <li>• употреба <i>IoT</i>-а и микроелектромеханичког система</li> </ul>



Назив пројекта	Опис
<b><i>IoT-DWM</i></b> [22]	<ul style="list-style-type: none"> <li>• управљање сигурношћу брана</li> <li>• наводњавање</li> <li>• употреба <i>IoT</i>-а</li> </ul>
<b><i>DAM WARNING SYSTEMS</i></b> [25]	<ul style="list-style-type: none"> <li>• <i>Telegrafia</i></li> <li>• систем за упозоравање на бранама и акумулацијама</li> </ul>
<b><i>NAWAPI</i></b> [26]	<ul style="list-style-type: none"> <li>• сателитско праћење кретања и нивоа вода</li> <li>• прекограничне поплаве</li> <li>• Вијетнам</li> </ul>
<b><i>SALGAR</i></b> [27]	<ul style="list-style-type: none"> <li>• <i>Federmán Comunicaciones</i></li> <li>• рана најава поплава</li> <li>• контрола речних токова (три реке)</li> <li>• Колумбија</li> </ul>

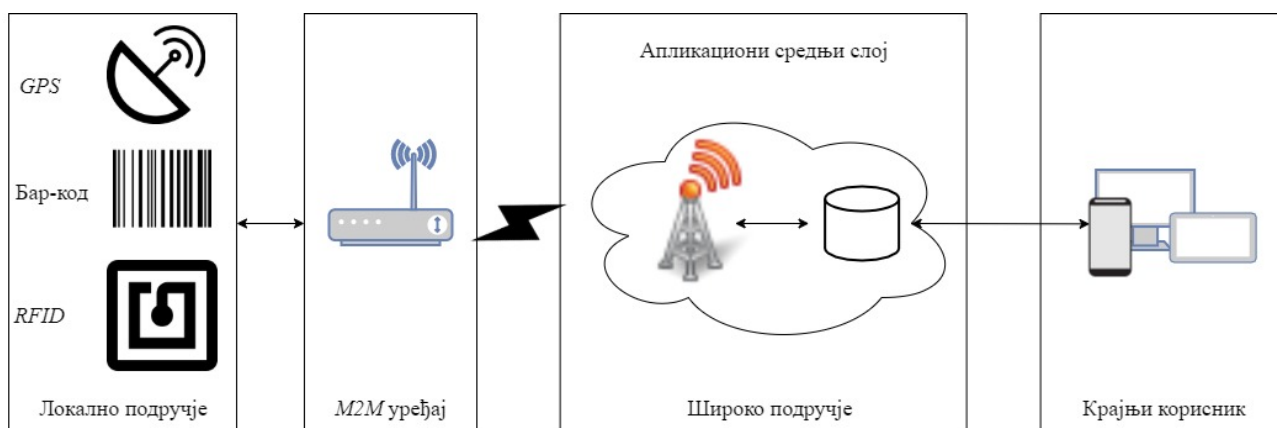
### 3. ТЕХНОЛОГИЈЕ ЗА РАЗВОЈ РЕШЕЊА

#### 3.1 Интернет интелигентних уређаја

Развој интернет технологија, *IPv6* протокола, и нова достигнућа у нано технологијама омогућили су пројектовање, производњу, постављање и умрежавање бројних уређаја опремљених сензорима и актуаторима [48]. Овим уређајима може се приступати и управљати путем интернета у реалном времену.

Структура *IoT*-а може се поделити на три слоја: апликације и сервиси, инфраструктура и хардвер. Намена хардвера је физичко повезивање уређаја. Међусобно повезани уређаји једино могу да размењују податке. Инфраструктура омогућава *IoT* уређајима повезивање на рачунарску мрежу, а апликације и сервиси представљају део *IoT* структуре за прибављање података са уређаја, обраду и испоруку.

Реч ствар (*thing*) у концепту *IoT*-а, или реч машина (*machine*) у *M2M*, представља физички објекат чија идентификација или стање може да се преноси кроз инфраструктуру која је повезана на интернет [49]. *IoT* омогућава да објекти буду опажени и контролисани даљински, помоћу постојеће мрежне инфраструктуре (Слика 12). Интернет интелигентних уређаја пружа могућност за директну интеграцију животног окружења и рачунарских система. Сваку ствар (објекат) је могуће јединствено идентификовати кроз уграђен рачунарски систем, и свака ствар треба да буде интероперабилна у оквиру постојеће интернет инфраструктуре.



Слика 12. *IoT* структура

За повезивање интелигентних уређаја посредно или непосредно на неку мрежу, неопходно је да уређаји поседују одговарајући интерфејс и да подржавају одговарајуће мрежне технологије и комуникационе протоколе [50]. Интелигентни уређаји користе *HTTP* и *TCP/IP* бежичне протоколе у које спадају *RFID*, *Bluetooth*, *ZigBee* и стандарде за бежичну комуникацију *802.15.4e*, *6LoWPAN*, *RPL CoAP*.

Интернет интелигентних уређаја је међусобно повезана мрежа физичких објеката (уређаја) који комуницирају са људима или другим физичким објектима и системима, где се комуникација међу машинама може обављати без људске интеракције/надзора [51].

Интернет интелигентних уређаја представља мрежу физичких уређаја састављених од сензора, актуатора, микроконтролера и микрорачунара, повезаних на интернет, који имају способност да сакупљају и деле податке и на основу њих извршавају акције [52]. Повезивање различитих објеката и додавање сензора на тим уређајима даје ниво дигиталне интелигенције који иначе нису „паметни”, омогућавајући им да комуницирају у реалном времену, без укључивања човека. *IoT* доприноси да окружење буде паметније и одговорније, спајајући дигитални и физички свет.

Сензори су део уређаја који прикупљају или дистрибуирају информације о локацији, висини, брзини, температури, осветљењу, кретању, и слично, и конвертују их у електричне величине које могу да користе други електронски уређаји.

Актуатори су уређаји који претварају неку врсту складиштене енергије у покрет. Сачувана енергија је обично у облику компримованог ваздуха (пнеуматски притисак), електричног потенцијала или течног (хидрауличког) притиска [53]. Код интернета интелигентних уређаја, актуатори се користе кад год постоји потреба да се укључи/искључи неки други уређај или делује на неки предмет применом силе (помери, подигне, окрене и сл.). Актуатори често имају функцију прекидача и управљача [52].

Микрорачунари су рачунари на штампаној плочи, са компонентама које има сваки рачунар – процесор, оперативна меморија, меморија за складиштење података, мрежни интерфејс и периферија. Архитектура коју користе микрорачунари је углавном *ARM* или *RISC*. За разлику од правих рачунара, микрорачунари троше мање енергије и могу да се напајају помоћу батерије. Због ограничености ресурса микроконтролера, на већини уређаја инсталиран је *Linux* оперативни систем.

Микроконтролер је компактно интегрисано коло, направљено тако да управља специфичним операцијама у интегрисаним системима. Микроконтролер обично садржи процесор, меморију, улазно/излазне (*I/O*) периферије на једном чипу. Микроконтролери немају оперативни систем, већ садрже *firmware*. Хардверски је слабији од микрорачунара, а пренос апликације се врши помоћу развојног окружења.

Интернет интелигентних уређаја примењује се у разним областима [50]:

- личне и пословне сврхе (аутоматизација кућа, зграда, станова и канцеларија);
- градско окружење (аутоматизација градова, тј. улица, паркинга, осветљења итд.);
- образовање (паметне учионице, аутоматизација факултета, библиотека...);
- здравство (аутоматизација болница, мониторинг пацијената и спортиста, *wearable* уређаји и сл.);
- логистика (аутоматизација транспорта, праћење испорука робе, праћење доставних возила);
- индустрија (аутоматизација фабрика, надгледање рада машина и алата...);
- окружење (праћење временских прилика, загађености ваздуха, буке, пожара...);
- енергетски системи (паметне електроенергетске мреже и системи обновљиве енергије);
- пољопривреда (аутоматизација система наводњавања и контрола стаклених башта); и
- роботика (паметни роботи).

Интернет интелигентних уређаја омогућава развој и примену нових технологија повећавајући сигурност грађевинских објеката. Са циљем смањења броја несрећа на бранама, све више пажње се посвећује унапређењу сигурности. Значајан број истраживања покушава да унапреди сигурност на бранама применом *IoT*-а у области осматрања брана. Применом *IoT*-а у техничком осматрању, подаци прикупљени сензорима могу се користити ради повећања сигурности брана, као и при ефикасном предвиђању понашања брана.

### 3.1.1 Паметни уређаји

Паметни уређаји имају уграђену памет или интелигенцију, идентификацију, аутоматизацију, надгледање и контролу [54]. Паметни уређај је електронски уређај, који је углавном повезан са другим уређајима или мрежама путем различитих протокола, као што су *Bluetooth*, *NFC*, *WiFi*, мобилне мреже (*3G*, *4G* или *5G*) итд., који могу у одређеној мери да делују интерактивно и аутономно.

## Паметне куће

У паметну кућу (*Smart Home*) уграђени су различите врсте сензора. Сензори су повезани са паметним уређајима у домаћинству. Корисник може да управља системом на различите начине, а све у складу са потребама и навикама. Пример сервиса паметне куће је када се врата гараже сама отварају при доласку аута (камера препознаје таблице), осветљење које се укључује при уласку у кућу, или се пали у одређеним терминима, а клима уређај се активира пре доласка људи са посла, или уколико температура опадне или порасте изван дефинисаног температурног оквира, чиме добијамо да је у свако доба дана температура у просторијама потпуно пријатна.

Појам паметна кућа описује аутоматизацију грађевина (приватних кућа), у којима су појединачне компоненте (сензори и актуатори) међусобно умрежени, са циљем формирања интелигентног система [55]. Паметна кућа је стамбени додатак аутоматизацији зграда и укључује контролу и аутоматизацију свих њених уграђених технологија [56]. Саставни део паметних кућа су уређаји који контролишу осветљење, грејање, хлађење, климатизацију, телевизоре, рачунаре, мултимедијалне системе и велике кућне апарате, као што су фрижидери, замрзивачи, машине за прање и сушење, системи за безбедност и камере, који су међусобно повезани и комуницирају.

Важна карактеристика система је могућност прилагођавања корисниковим навикама, активностима, његовом расположењу или животном стилу (могућност система да „научи” навике људи). Како систем паметне куће рационално троши енергију и уопште смањује потребу за производњом електричне енергије, он активно доприноси очувању околине. Такође, систем паметне куће омогућава једноставно управљање повезаним уређајима, односно целокупним системом, а самим тим олакшава живот и аутоматизује одређене активности и радње о којима свакодневно бринемо.

Неке од предности које доносе паметне куће су:

- управљање свим кућним уређајима са једног места (нпр. мобилни уређај);
- максимална безбедност дома (мониторинг камерама и могућност прегледа на мобилном телефону);
- даљинско управљање кућним уређајима (укључивање или искључивање уређаја);
- побољшана функционалност уређаја; или
- повећана енергетска ефикасност.

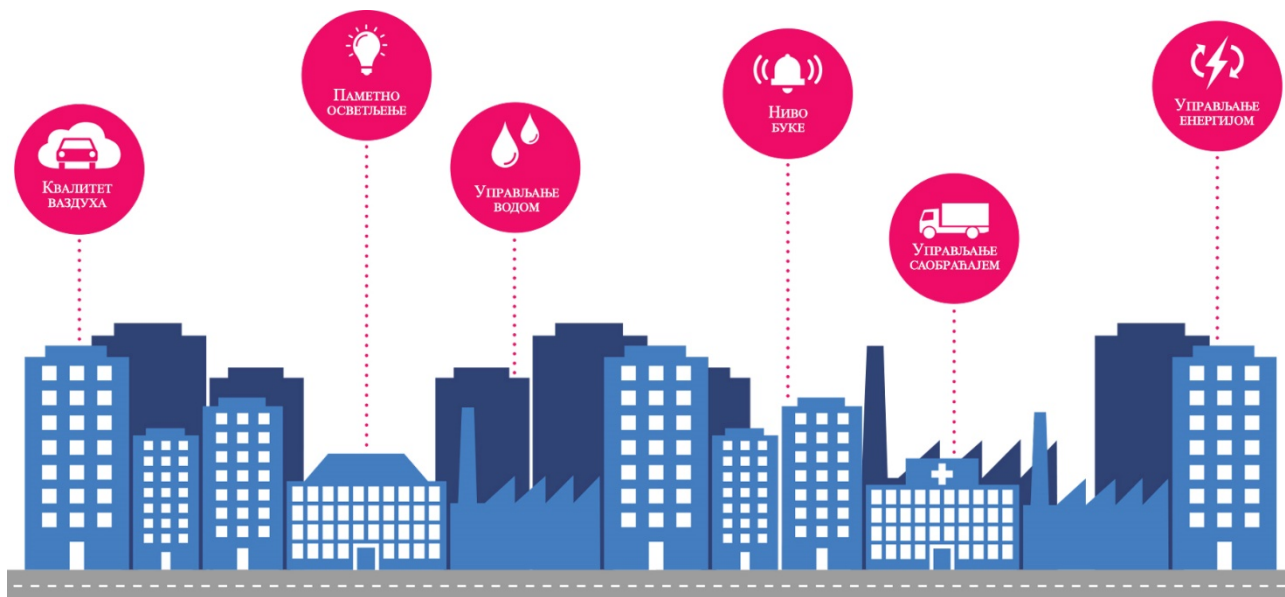
## Паметни градови

Паметни градови су дефинисани као функционална урбана подручја артикулисана коришћењем информационих и комуникационих технологија (ИКТ) и модерне инфраструктуре за решавање градских проблема на ефикасан и одржив начин [57]. Унутар ИКТ-а, системи препорука су снажни алати који филтрирају релевантне информације, надограђујући односе између интересних група у политици и цивилном друштву и помажу при доношењу одлука кроз технолошке платформе.

Иако постоји више дефиниција шта је паметни град, општа идеја паметног града је оптимизација функција града и покретање економског раста, уз истовремено побољшање квалитета живота његових грађана, користећи паметну технологију и анализу података. Вредност паметног града оцењује се на основу ефикасности и ефективности примењене технологије, а не само на основу количине технологије коју град поседује. Неке од карактеристика које утичу на вредност, тј. одређивање колико је неки град паметан су:

- технолошки заснована инфраструктура;
- еколошке иницијативе;
- систем високог функционисања јавног превоза;
- самоуверени осећај урбаног планирања;

- људи који живе и раде у граду, и користе његове ресурсе.



Слика 13. Паметан град [58]

Параметри који се могу мерити и пратити у паметним градовима приказани су на слици 13. Успех паметног града зависи од снажног однос између владе, укључујући њену бирократију и прописе, и приватног сектора. Ова веза је неопходна јер се већински део посла на стварању и одржавању дигиталног окружења, које се заснива на подацима, врши изван владе.

У Београду, на општини Врачар, имплементиран је паметни систем паркинга, где возачи могу видети колико слободних паркинг места има у којој улици.

### ***Wearables***

*Wearables* су уређаји који се користе свакодневно за мерење одређених параметара, било да су од виталног значаја за човека или параметара окружења. Велику примену нашли су у медицини и спорту. Медицински параметри могу бити притисак, откуцаји срца, температура и сл. У спорту се користе нпр. за мерење пролазног времена при трчању, откуцаја срца, пређену километражу итд., а у фудбалу се мери и прати кретање фудбалера током утакмице. Присуство паметних телефона није неопходно, јер је након неког времена могуће извршити синхронизацију података. Коришћење *Wearables* у свакодневном животу приказано је на наредној слици (Слика 14).



Слика 14. *Wearables* [59]

Паметне носиве ствари могу се користити и у контексту управљања бранама, када је потребно измерити одређене параметре везане за околину или оператере. Измерени подаци могу се користити за утврђивање степена тежине посла који обављају запослени у служби осматрања, или за информације о тренутном стању одређених параметара на брани. Такође, помоћу паметних уређаја могуће је пратити кретање оператера и време проведено у телу бране.

### 3.1.2 Бежичне сензорске мреже

Бежичне сензорске мреже могу се дефинисати као самоконфигурисане и бежичне мреже, које немају инфраструктуру, и чији је циљ надгледање физичких или услова окружења, као што су температура, звук, вибрације, притисак, кретање или загађивачи и да заједнички прослеђују своје податке кроз мрежу главној локацији (*sink*), где се подаци могу посматрати и анализирати [60]. *Sink*, или базна станица, делују попут интерфејса између корисника и мреже. Бежичне сензорске мреже могу садржати стотине хиљада сензорских чворова. Сензорски чворови могу међусобно комуницирати користећи радио-сигнале. Бежични сензорски чвор опремљен је: сензорским и рачунарским уређајима, радио примопредајницима и компонентама напајања.

Појединачни чворови у бежичној сензорској мрежи имају ограничене ресурсе: ограничену брзину обраде, капацитет складиштења и опсег комуникације. Након распоређивања сензорских чворова, они су одговорни за самоорганизацију одговарајуће мрежне инфраструктуре, често уз вишеструку комуникацију са њима. *Onboard* сензори тада почињу да сакупљају потребне податке. Бежични сензорски уређаји такође одговарају на упите послате са „контролног места” да би извршили одређена упутства или пружили узорке сензора. Начин рада сензорских чворова може бити континуиран или се покретати неким догађајима. Глобални систем за позиционирање (*Global Positioning System - GPS*) и локални алгоритми за позиционирање могу се користити за добијање информација о локацији и позиционирању. Бежични сензорски уређаји могу бити опремљени актуаторима да би „деловали” под одређеним условима.

У даљем развоју система осматрања брана могућа је имплементација *WSN*. *WSN* уређаји истовремено могу да мере разне параметре у окружењу бране и комуницирају међусобно. Уколико дође до отказа неког уређаја, особље у контролно-командном центру може добити поруку о квару уређаја у реалном времену и на време реаговати на прави начин, како не би било угрожено подручје око бране.

### 3.1.3 Мрежни протоколи интернета интелигентних уређаја

Интернет интелигентних уређаја представља мрежу физичких објеката или уређаја са уграђеном електроником, софтвером и сензорима, који прикупљају податке из окружења и размењују их с другим уређајима и системима [50]. Постојећа мрежна инфраструктура омогућава овим уређајима даљински приступ и комуникацију са окружењем. Мрежна инфраструктура мора да обезбеди свим *IoT* уређајима несметан и безбедан приступ интернету.

У последње време, у области комуникација популарна је интеграција *M2M* система и бежичних сензорских мрежа са интернет сервисима [50]. Интернет сервиси користе постојеће *TCP/IP* протоколе. Интеграција омогућава интелигентним уређајима конективност преко *TCP/IP* стека и веб-сервиса. Интелигентним уређајима се такође омогућавају агрегација, визуелизација и анализа података добијених из паметних уређаја.

Протоколи за комуникацију с паметним уређајима су једноставни, али њихова сложеност зависи од хардверских и софтверских могућности самих *IoT* уређаја.

**Ethernet** је породица мрежних технологија, која је у почетку развијена за имплементацију жичаних *LAN* (*Local Area Network*) мрежа. *Ethernet* је мрежна технологија која покрива прва два слоја *OSI* (*Open Systems Interconnection*) референтног модела. Главне карактеристике *Ethernet* заснивају се на ниским трошковима, лакој конфигурацији и распоређивању опреме [61]. *Ethernet* је протокол дефинисан *IEEE 802.3* стандардима за комуникацију на физичком слоју и слоју везе *OSI* референтног модела, и представља једну од најчешће коришћених више-медијумских технологија у *LAN* и *WAN* (*Wide area network*) мрежама [50]. Сваки уређај у *Ethernet* мрежи има хардверски део, картицу за интерфејс са *MAC* адресом (48 бита). *MAC* адреса (*Media Access Control Address*) на јединствен начин идентификује уређај са кога је послат и коме је фрејм намењен.

**WiFi** (*Wireless Fidelity*) је заснован на *IEEE 802.11* породици стандарда и првенствено је технологија локалног умрежавања (*LAN*), дизајнирана да омогући уградњу широкопојасне покривености [62]. *WiFi* се често користи у *IoT* комуникацијама. *WiFi* представља технологије за локалне бежичне мреже, засноване на групи *IEEE 802.11* стандарда. Најчешће се користи опсег фреквенција од 2,4–2,4835GHz, осим код *802.11a* стандарда који захтева опсег од 5,725–5,850GHz [50].

**WiMAX** (*Worldwide Interoperability for Microwave Access*) технологија је бежична широкопојасна комуникациона технологија заснована на *IEEE 802.16* стандарду, који пружа велике брзине података на широком подручју [63]. *WiMAX* технологија може да задовољи потребе великог броја корисника наручио оних у развијеним земљама, који желе да инсталирају нову мрежу велике брзине података јефтино, без трошкова и времена потребног за инсталирање жичане мреже, до оних у руралним областима којима је потребан брз приступ, где жичана решења можда неће бити одржива због растојања и трошкова. Осим тога, користи се за мобилне апликације, пружајући податке о брзини корисницима у покрету.

У складу са захтевима мобилности, примена *WiMAX* може бити подељена у четири групе [50]:

- фиксни приступ;
- номадски приступ;
- мобилни приступ;
- потпуна мобилност.

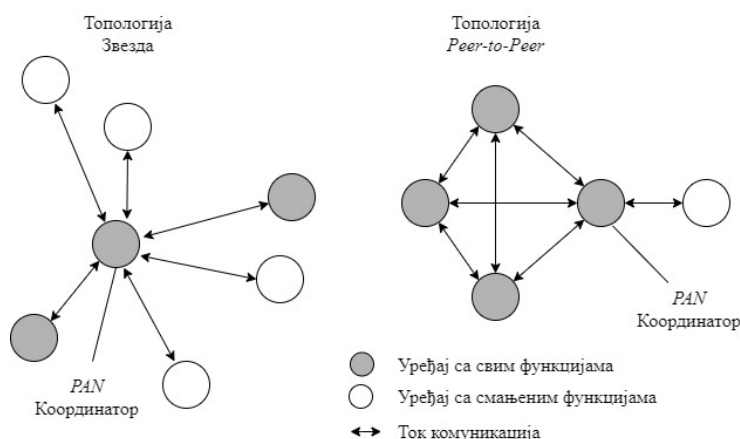


**Bluetooth** представља пример бежичне технологије умрежавања великог броја уређаја. Карактеристично за *Bluetooth* технологију је мала потрошња енергије и јефтине бежичне комуникације засноване на радио-таласима. Детаљнији опис *Bluetooth* технологији биће дат у следећим поглављима.

Породица стандарда **IEEE 802** подељена је у бројне групе, укључујући 802.3 (*Ethernet*) и 802.11 (*WiFi*), као и 802.15 (бежични *Professional Associate Network – PAN*) [64]. Конкретно, **IEEE 802.15.4** (15.4) је у надлежности радне групе 4, која је одговорна за различите карактеристике протокола, укључујући *RF* (радио-фреквенцијски) спектар и физичке слојеве. Стандард 15.4 је проширен и укључује *PHY* (физичке слојеве) за радио-фреквенцијску идентификацију, ултраширокопојасне (*Ultra-wideband - UWB*) *PHY*, а такође разматра се и као могуће решење за комуникацију између два аутомобила, и од аутомобила до ивичњака.

802.15.4 односи се само на физички и слој контроле приступа медијуму (*MAC*) – у моделу *OSI* мреже, слојеви један и два. Горње слојеве оставља имплементатору. На трећем и вишем слоју, налази се више могућности, укључујући *ZigBee*, *Z-Wave* и *6LoWPAN*. Свака од њих имплементира остатак модела протокола *OSI* за испоруку услуга, као што су усмеравање и откривање, као и *API*-је за корисничке апликације.

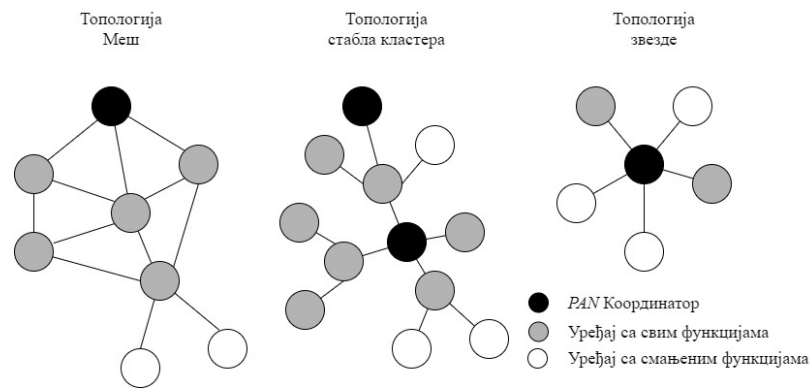
**IEEE 802.15.4** је стандард који је дефинисала **IEEE 802.15** радна група, а односи се на физички слој и контролу приступа медијуму за *LR-WPAN* (*Low-Rate Wireless Personal Area Networks*) мреже малих брзина преноса података [50]. Зависно од захтева апликација, **IEEE 802.15.4** *LR-WPAN* мреже могу бити са топологијом звезде или *peer-to-peer* топологијом. У топологији звезде комуникација се успоставља између уређаја и централног контролера који се назива *PAN* координатор (*Personal Area Network Coordinator*).



Слика 15. Топологије *LR-WPAN* мрежа

**ZigBee** је протокол за бежичну комуникацију, изграђен на **IEEE 802.15.4** стандарду [50]. *ZigBee* омогућава контролу и управљање паметним уређајима у оквиру *IoT* система и *M2M* комуникације. *ZigBee* мрежни слој подржава следеће три мрежне топологије: звезда, кластер стабло и генеричка меш-мрежа.





Слика 16. ZigBee мрежне топологије

ZigBee је спецификација за бежичну локалну мрежу (*Wireless Local Area Network – WLAN*) мале потрошње, која је дизајнирана тако да обезбеђује малу количину података користећи мало енергије, јер је на већини повезаних уређаја извор напајања батерија [65]. Због тога је овај отворени стандард повезан са комуникацијом *M2M* и индустријским *IoT*-ом. ZigBee се не фокусира на *point-to-point* комуникације, као *Bluetooth*, где један уређај са јаким напоном шаље податке другом уређају са јаким напоном у кратком распону, и ставља га у меш-мрежу, због чега је одличан за паметне куће.

ZigBee ради на неколико фреквенција [66]:

- 2,4GHz
- 868MHz
- 90MHz

Брзина преноса ZigBee везе је 250Kbps, што је знатно ниже од WiFi везе, али у зависности од потреба корисник бира одређену технологију. Сензорима је потребан мали опсег, па је због тога ZigBee одговарајући протокол. У случајевима где су дуг животни век и сигурност битни, а брзина преноса мање битна, ZigBee је погодно решење.

Постоје три различита типа ZigBee уређаја [67]:

- ZigBee координатор – уређај који представља корен стабла мреже и служи за спајање са другим мрежама. Свака мрежа има само један координатор, који је у стању да складишти информације о мрежи;
- ZigBee рутер;
- ZigBee End Device – садржи управо онолико функција колико му је довољно да комуницира са матичним чвором (било координатором или рутером). Омогућава да чвор „спава” и на тај начин штеди батерију. Захтева малу количину енергије и стога је и јефтинији од координатора и рутера.

**LoRaWAN** је мрежни протокол широког подручја мале потрошње (*Low Power Wide Area – LPWA*) пројектован да бежично повезује уређаје на интернет, којима је извор напајања батерија, у регионалну, националну или глобалну мрежу, и кључни захтев интернета интелигентних уређаја двосмерна комуникација, *end-to-end* заштита, мобилност и локализација услуга [68].

LoRaWAN мрежна архитектура распоређена је у топологију звезда, у којој гејтвеји преносе поруке између крајњих уређаја и централног мрежног сервера. Гејтвеји су повезани на мрежни сервер путем стандардних IP веза и делују као транспарентан мост, једноставно претварају RF пакете у IP пакете и обрнуто.

LoRaWAN има три различите класе крајњих уређаја за решавање различитих потреба које се одражавају у широком спектру примена:

- Класа А – најмања снага, двосмерни крајњи уређаји;
- Класа В – двосмерни крајњи уређаји са детерминистичком *downlink* латенцијом;
- Класа С – најмања кашњења, двосмерни крајњи уређаји.

Сигурност је главна брига за свако масовно постављање *IoT*-а. *LoRaWAN* спецификација дефинише два слоја криптографије:

- јединствени 128-битни мрежни кључ сесије, који се дели између крајњег уређаја и мрежног сервера;
- јединствени 128-битни кључ сесије апликација (*APIsKey*) дели крајњи крај на нивоу апликације.

*AES* алгоритми се користе за аутентификацију и интегритет пакета мрежном серверу и *end-to-end* енкрипцију апликативном серверу. Обезбеђивањем ова два нивоа, могуће је имплементирати „*multi-tenant*” дељене мреже, а да мрежни оператер нема увид о корисничком оптерећењу подацима.

### 3.1.4 *Machine-To-Machine* комуникација

*Machine-To-Machine* је технологија која се све брже развија због своје намене [69]. Ова технологија представља жичани и/или бежични пренос, анализу и процесирање података између различитих уређаја преко комуникационих мрежа. *M2M* представља повезивање индустријске опреме, возила, банкомата, продајних места, и сл. који аутоматски међусобно комуницирају путем интернета. *M2M* технологија представља аутоматску размену података између машина и уређаја. Улога *M2M* је да успостави услове који омогућавају уређајима (двосмерну) размену информације са пословном апликацијом путем комуникационе мреже, тако да уређај и/или апликација могу да послуже као основа за ову размену информација [70].

*M2M* технологија је прво усвојена у производним и индустријским гранама, где су друге технологије, као што су *SCADA* (*Supervisory Control And Data Acquisition*) и даљински мониторинг, помогле даљинском управљању и контроли података измерених мерним уређајима. *M2M* је након тога примењен у другим областима, као што су здравство, пословање, осигурање итд. *M2M* је основа и за *IoT*.

Главна сврха технологије *M2M* је коришћење података сензора и њихово прослеђивање у мрежу. За разлику од *SCADA* или других алата за даљинско праћење, *M2M* системи често користе јавне мреже и методе приступа због исплативости (мобилни или *Ethernet*).

Главне компоненте *M2M* система укључују сензоре, *RFID*, *WiFi*, или мобилну комуникациону везу и софтвер за аутономно рачунање, који је програмиран да помогне мрежном уређају да интерпретира податке и доноси одлуке. *M2M* апликације преводe податке, што може покренути унапред програмиране и аутоматизоване акције. Једна од познатијих врста комуникације *M2M* је телеметрија, која се користи од почетка прошлог века за пренос оперативних података. Пионири у телеметрији прво су користили телефонске линије, а касније и радио-таласе за пренос мерења перформанси, прикупљених помоћу инструмената за мониторинг на удаљеним локацијама.

Кључне карактеристике *M2M* технологије укључују:

- мала потрошња енергије, у настојању да се побољша способност система да ефикасно сервисира *M2M* апликације;
- мрежни оператер који пружа услугу преноса пакета;
- надгледање способности које пружају функцију за откривање догађаја;
- временска толеранција, што значи да се пренос података може одложити;
- временска контрола, што значи да се подаци могу слати или примати само у унапред одређеним периодима;

- локацијски специфични окидачи који упозоравају или пробуде уређаје када уђу у одређене области; и
- могућност сталног слања и примања малих количина података.

*M2M* комуникација је веома битна на бранама, јер се на бранама користе разни мерни уређаји, који су повезани или међусобно комуницирају и прикупљају податке који се могу користити за процену сигурности бране.

### 3.1.5 Софтверски дефинисане мреже

Софтверски дефинисане мреже (*Software Defined Networking – SDN*) је појам који обухвата више врста мрежних технологија ради креирања мреже која треба да буде више агилна и флексибилна и подржи виртуелни сервер и складиштење инфраструктуре модерног дата центра (*data center*) [71]. *SDN* технологија омогућава мрежним администраторима да ефикасно и флексибилно управљају мрежном опремом кроз стандардне интерфејсе [72]. Циљ успешне имплементације *SDN*-а је стицање оперативних и економских користи кроз мрежу која нема ограничења произвођача, или није ограничена карактеристикама наслеђених система. Кључне *SDN* технологије су функционално раздвајање, виртуелизација мреже и аутоматизација кроз програмабилност [73].

Основне карактеристике на којима се заснивају *SDN* су логичка централизација интелигенције, програмабилност и апстракција [50]. Логичка централизација интелигенције представља управљање мрежом, које је раздвојено од прослеђивања саобраћаја. Програмабилност значи да се мрежама управља путем софтвера (динамички). Коришћењем *API*-ја, отвореног стандарда, могуће је имплементирати апликације тако да се зависно од самих потреба, мрежни ресурси динамички (аутоматски) додељују, без обзира на произвођаче самог хардвера. Апстракција представља раздвајање корисничких апликација и мрежних елемената, који су апстраховани у односу на управљачки слој. На тај начин апликације не сагледавају мрежну инфраструктуру која се налази у слоју испод.

*SDN* се користе у систему осматрања брана у инфраструктури дата центра.

### 3.1.6 Протоколи апликативног слоја интернета интелигентних уређаја

Апликативни слој налази се на врху *IoT* протокол стека и кључан је за испоруку апликација корисницима [50]. Избор протокола на апликативном слоју није једноставан, јер динамика промена и потребе корисника воде ка дефинисању нових циљева и развоју савршенијих и унапређивању постојећих *IoT* апликација.

При избору протокола, у апликативном слоју узима се у обзир већи број захтева, а основни се односе на:

- механизам размене порука;
- безбедност података;
- интероперабилност уређаја; и
- скалабилност *IoT* система.

Најзначајнији протоколи апликативног слоја *IoT*-а су: *HTTP*, *REST*, *COAP*, *WebSocket*, *MQTT*, *XMPP*, *DDS* и *AMQ*.

*HTTP* (*Hypertext Transfer Protocol*) је протокол апликационог слоја, који се користи за комуникацију и размену података на вебу [50]. Најзаступљенија је верзија *HTTP1.1*, а последња верзија је *HTTP/2* из 2015. године. Функционише по методу захтев-одговор (*request-response*) и омогућује размену хипертекста. Клијент шаље *HTTP* захтев (поруку), а сервер одговара *HTTP* одговором. *HTTP* је протокол помоћу којег клијент повлачи информације са сервера, уместо да сервер гура информацију ка клијенту. Основни елементи *HTTP* захтева су: линија захтева, заглавље, празан ред и порука. Осам метода које дефинише *HTTP* протокол помоћу којих се реализују одређене акције су: *HEAD*, *GET*, *POST*, *PUT*,

*DELETE, TRACE, OPTIONS, CONNECT. HTTP* је протокол без стања (*stateless protocol*), јер пошиљалац и прималац нису упућени у претходне захтеве, и нема гаранције да ће поруке бити испоручене.

**REST** (*REpresentational State Transfer*) представља модел архитектуре који се заснива на постојећим широко прихваћеним и коришћеним технологијама и протоколима [50]. Главна имплементација ове архитектуре је *HTTP* протокол у комбинацији са *URI* (*Uniform Resource Identifier*, другим речима, вебом). Садржи пет обавезних и једно опционо ограничење:

- униформни интерфејс;
- клијент-сервер;
- без стања;
- могућност кеширања (*cache*);
- слојевит систем; и
- код на упит (опционо).

**CoAP** (*Constrained Application Protocol*) протокол представља реализацију *REST* архитектуре у форми погодној за ограничене уређаје и мреже (*constrained*) [50]. *Constrained* мреже имају ограничења која се односе на брзину преноса, висок ниво губитака пакета, променљиве величине пакета, недостатак напредних сервиса, као што је *IP multicast*, ограничену величину пакета, ограничену доступност уређаја у мрежи итд. *6LoWPAN* мрежа је представник *CoAP* протокола.

Циљ *CoAP* протокола јесте да смањи оптерећење саобраћаја у мрежи и тиме ограничи потребу за фрагментацијом у мрежном слоју. *CoAP* захтев сличан је *HTTP* захтеву: клијент шаље захтев серверу да изврши акцију на одређеном ресурсу, а сервер након обављеног задатка враћа одговор са кодом одговора.

Модел размене порука у *CoAP* заснован је на *UDP* протоколу (*User Datagram Protocol*): свака порука садржи свој *MessageID*, који се користи за откривање дупликата.

**Веб-сокет** (*WebSocket*) је двосмерни комуникациони протокол [50]. Настао је у оквиру *HTML 5* спецификације. Протокол омогућује *full-duplex* комуникацију преко једне *TCP* конекције између клијента и сервера. Када се успостави конекција, поруке путују од сервера ка браузеру. Комуникација је поједностављена, јер не постоји потреба за комплексном двосмерном разменом (клијент повлачи податке са сервера).

Веб-сокет је дефинисан за апликације које се користе преко веб-претраживача. Намењен је за комуникацију у реалном времену, а карактеришу га поузданост и минимизација оптерећења. Веб-сокет је ефикасан систем за размену порука између сервера и *IoT* уређаја.

**MQTT** (*Message Queue Telemetry Transport*) је *publish-subscribe* протокол, дизајниран за *M2M* комуникације [50]. *MQTT* је отворени стандард и има циљ да омогући ефикасну размену података и смањи потрошњу енергије. Базиран је на клијент-сервер моделу размене порука, где је сензор клијент повезан са сервером (брокером) преко *TCP* везе. Кључни елемент у комуникацији је *MQTT* брокер, који је задужен за управљање и распоређивање свих порука између пошиљача и одговарајућих прималаца. Главна предност *MQTT* протокола у односу на *HTTP* јесте што клијент не мора да захтева информације које су му потребне, него их брокер гура ка клијенту у случају промена у подацима. *MQTT* омогућује размену порука у реалном времену уз минималну потрошњу енергије.

**XMPP** (*Extensible Messaging and Presence Protocol*) је протокол намењен размени текстуалних порука, заснован на захтев-одговор парадигми (*request-response*) [50]. *XMPP* протокол користи *XML* формат и ради преко *TCP* везе. Архитектура *XMPP* протокола подразумева да два клијента комуницирају један са другим преко сервера задуженог за рутирање (усмеравање) порука.

*DDS (Data Distribution Service)* је први отворени стандард у средњем слоју, који се заснива на *publish-subscribe* моделу [50]. *DDS* протокол је оријентисан ка подацима, а не ка порукама, што је случај код других протокола. Фокус поменутог протокола је на подацима које је дефинисао корисник. Јединица размене јесте вредност податка. Протоколи засновани на подацима једноставнији су за одржавање и проширивање, омогућују корисницима да се фокусирају на развој пословне логике, а не само на писање порука. *DDS* може истовремено да достави милионе порука у секунди, великом броју прималаца, а притом омогућује висок ниво *QoS (Quality of Service)* контроле, *multicast*, свеприсутну редундантност и поузданост.

*LWM2M (Lightweight Machine to Machine)* протокол дефинише низ стандардних интерфејса и модела података да би се обезбедила интероперабилност између *CoAP* уређаја и локалних или удаљених сервиса [50]. *LWM2M* дефинише једноставан објектни модел користећи *CoAP REST API* архитектуру за управљање уређајима, коришћењем *REST* објеката и системске функционалности, укључујући контролу асинхроних нотификација.

Од поменутих протокола, у тренутном систему осматрања брана користе се: *HTTP*, *REST*, *CoAP*, *WebSocket* и *MQTT*.

## 3.2 RFID

### 3.2.1 Концепт *RFID* технологије у индустрији

*IoT* је прихваћен као технолошка архитектура која се користи у многим информационим технологијама. Са циљем бољег схватања *IoT*-а и његових технологија, *Zhang* и други аутори у [74] описују *IoT* архитектуру са шест слојева, примарно базирану на мрежној хијерархијској структури. Затим, аутори разматрају кључне технологије које се користе у сваком слоју *IoT*-а, као што су *RFID*, бежичне сензорске мреже, интернет, *SOA (Service-Oriented Architecture)*, *cloud computing*, веб-сервиса и сл. Аутоматски систем препознавања објеката на основу тага направљен је интегрисањем *RFID*-а и *WSN*-а, и направљена је и стратегија интеграцијом *RFID*-а и веб-сервиса.

*IoT* систем захтева да се информације прикупљају од било које физичке ствари или уређаја, било кад и било где. Ради постизања поменутог, потребни су бежични уређаји следећих карактеристика: (1) имају способност аутоматског прикупљања података; (2) мале су величине; (3) имају дуг животни век; и (4) имају могућност комуницирања између великих раздаљина. Да би обезбедили поменуте захтеве, *Katayama Minoru* и други аутори у [75] предлажу употребу активног *RFID* система. Активни *RFID* има више предности у односу на пасивни *RFID* и омогућава боље перформансе читања података на великим раздаљинама. У овом раду аутори анализирају активне *RFID* системе, услуге које тренутно могу да пруже, сличне техничке проблеме ових услуга и смер у ком треба да иде даље истраживање. Аутори такође описују резултате *EPCglobal (Electronic Product Code – EPC)* пилот тестова спроведених на глобалној логистици за праћење прекоокеанског транспорта, користећи активне *RFID* системе за које су аутори развили нове типове активних *RFID* тагова. Полуактивни *RFID* тагови, као и активни тагови, захтевају батерију која ограничава њихове примене у многим областима. Због поменутог ограничења, *Chu* и други аутори у [76] свој фокус су усмерили на изворе енергије за *RFID* тагове. Аутори дају нацрт за самостално напајајући *RFID* таг с акустичним резонантним пијезо-електричним напајањем (*PPS*) танког филма, који се може користити као преносни даљински надзор за температуру. Тај систем се скраћено назива *PPS-RFID*. Аутори су у раду посветили пажњу дизајну и симулацији *PPS*. Резултати истраживања су показали да интегрисани *PPS* може пружити довољну снагу за дизајнирани *PPS-RFID* таг. *PPS-RFID* таг може се широко користити за надзор температуре током мобилног транспорта кварљивих ствари, као што су лекови или храна. Код пасивних радио фреквенција, *UHF* технологија препознавања брзо се развила од једноставног означавања физичких ствари, до бежичних сензора. Велики број научних радова показује да се физичка својства, начелно, могу пратити и надзирати током читавог животног циклуса.

*Occhiuzzi* и други аутори у [77] представљају јединствен преглед новог питања везаног за таг као сензор. Посебну пажњу посвећују формализацији мерног показатеља и односу комуникације и читавања, с циљем пружања прве базе знања за суочавање с великим бројем нових апликација за опажање.

*RFID* има могућност да подржи аутоматско праћење информација и управљање током процеса у многим областима. Типична област где се употребљава *RFID* је управљање модерним складиштима. Производи су обележени таговима, а са инвентаром (производима) се управља преузимањем *ID*-а тагова. Многе практичне примене захтевају претрагу групе тагова да би се одредило да ли су у систему или не. Постојеће студије о претраживању тагова углавном се фокусирају на унапређење временске ефикасности, а запостављају енергетску ефикасност која је битна за активне тагове, који се напајају путем батерије. Да би превазишли овај проблем, *Zhang* и други аутори у свом раду [78] баве се испитивањем претраге са становишта енергетске ефикасности. Аутори предлажу енергетски ефикасан протокол за претрагу тагова у системима са више *RFID* читача, под називом *ESiM*, који гура потрошњу по тагу до лимита, како би сваки таг разменио један бит података са читачем. Аутори су развили унапређену временски ефикаснију верзију *ESiM*, названу *TESiM*, која драстично може да смањи време извршења, док се оптерећење незнатно повећава. У већини разматраних сценарија, *TESiM* смањује време извршења за више од 50 процената.

Бројна истраживања су посвећена сигурности и приватности *RFID*-а. Већина студија су спроведене под претпоставком да се *RFID* систем састоји од: *RFID* тагова, читача, и *back-end* сервера. У [79] *Erguler* наводи да ће велики број *RFID* читача бити распоређен и повезан на систем путем интернета. Такође, аутор наводи да окружење са више *RFID* читача, где читачи могу бити мобилни уређаји, као мобилни телефон, треба да се укључи у анализу безбедности *RFID*-а. *Erguler* указује да је *RFID* аутентификационом протоколу и *IoT*-у потребан нови безбедносни механизам који разматра непоуздане *RFID* објекте, компромитоване читаче или небезбедан комуникациони канал између читача и *back-end* сервера. Традиционалне *RFID* безбедносне шеме, пројектоване за затворене системе, не могу да испуне захтеве за безбедност и приватност, уколико су директно прилагођени *IoT* окружењу. Да би нагласио разлику, аутор овог рада приказује како затворени *RFID* систем може да угрози безбедносни систем у овом новом *RFID* концепту. Да би заштитио систем од нежељених напада, аутор је надоградио протокол, тако да он задржи своја безбедносна својства.

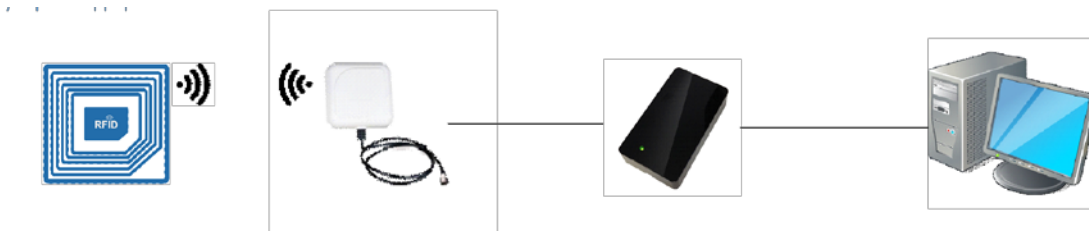
Паметне технологије су нашле примену у разним областима, као што су логистика, индустријски објекти, велике конструкције, енергетски сектор итд. Пример добре употребе паметних технологија је примена *RFID*-а у мониторингу. *RFID* је техника препознавања и локализације објеката из даљине [80]. *Pursula* и други аутори у свом раду описују развој пасивних *HF* и *UHF RFID*, који се баве мониторингом влажности и температуре [81]. Пројекат је коришћен у бетонским одливцима. У [76] аутори приказују дизајн за самонапајајуће *RFID* тагове који користе пијезо-електрично напајање (*PPS*). Решење представља преносиво даљинско надгледање температуре. У [82], [83] *RFID* технологија се користи у мониторингу саобраћаја и инфраструктуре. У мостовима се користе пасивни тагови, а читач има могућност да открије неисправан таг и количину одступања. У саобраћају, *RFID* технологија је примењена у надгледању возила на путевима и тунелима. Постоје два сценарија надгледања саобраћаја: систем за читање на бази прага и читач на путу.

*RFID* технологија се користи и за праћење грејања. У [84] аутори представљају *demand-driven HVAC* операције и *RFID* у системима за откривање заузећа у грејању, вентилацији и климатизацији.

Зависно од фреквенције, тагови се деле на нискофреквентне (*low frequency - LF*) са распоном до 10cm, тагови високе фреквенције (*high frequency - HF*) са распоном од 10cm до 1m и тагови ултрависоке фреквенције (*ultra high frequency - UHF*) са распоном до 12m. У овом пројекту

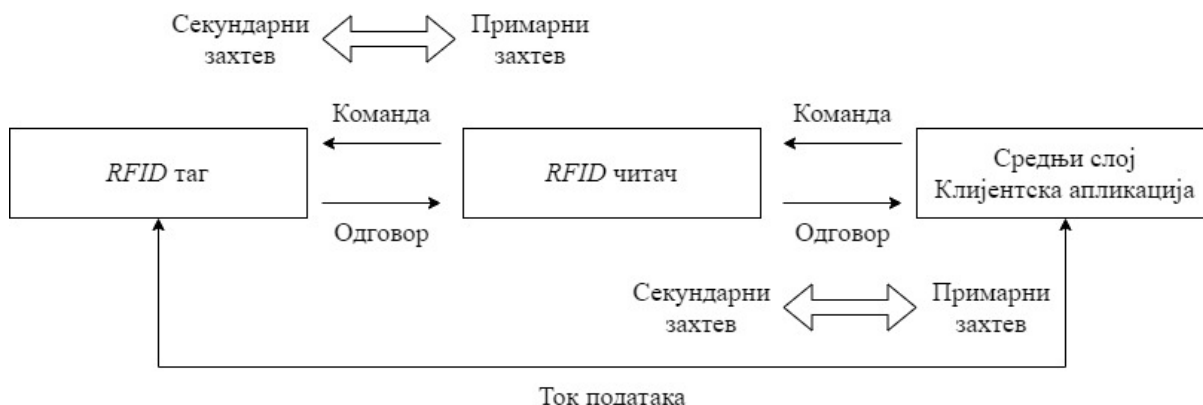
употребљени су *UHF* тагови, јер је требало да трају што је дуже могуће (без промене батерије) и због доступности терена (распон) [85].

*RFID* (*Radio-Frequency IDentification*) представља мале електронске уређаје који се састоје од малог чипа и антене. *RFID* систем се састоји од тага, читача који комуницира са тагом на одређеној фреквенцији, и рачунара на који је читач прикључен, а који обично садржи базу података. На слици 17 приказане су основне компоненте *RFID* система.



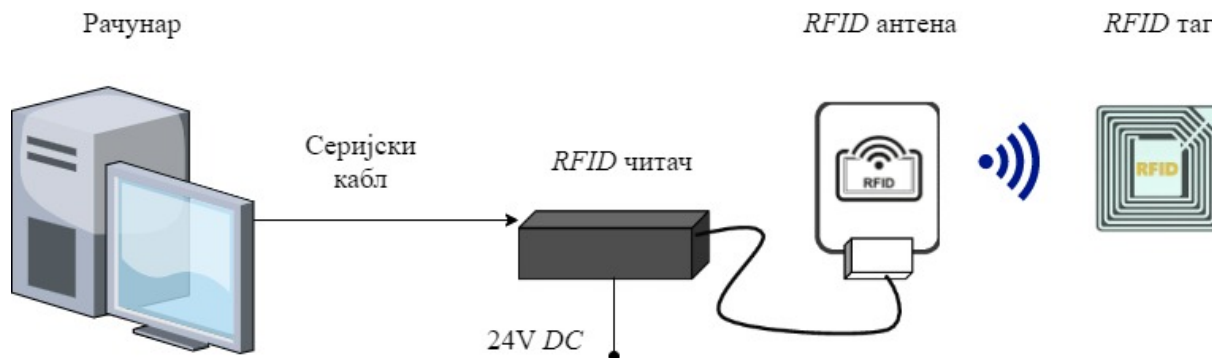
Слика 17. Основне компоненте *RFID* система

*RFID* уређај има исту намену као бар-код или магнетна трака на полеђини кредитне картице или *ATM* картице (јединствени идентификатор за тај објекат). Бар-код или магнетна трака морају бити скенирани да би добили информације које су записане. *RFID* такође мора бити скениран да би се преузели идентификациони подаци [86]. Ток података у *RFID* систему приказан је на следећој слици (Слика 18).



Слика 18. *RFID* ток података [87]

Битна карактеристика *RFID* технологије је позиционирање, јер *RFID* уређај не треба да се позиционира испред скенера да би био прочитан, за разлику од бар-код технологије. *RFID* уређаји ће радити и на већој удаљености од скенера (зависно од фреквенције). *RFID* хардвер приказан је на слици која следи (Слика 19).



Слика 19. Схематски приказ *RFID* хардвера [88]



У оквиру *RFID* технологије постоје три типа система: активни, полуактивни и пасивни. Активни системи су они који имају сопствени извор напајања. Полуактивни системи су системи који имају малу помоћ батерије. Пасивни системи су системи који немају свој извор напајања (батерију) и користе сигнале читача као вид напајања.

*RFID* системи се могу поделити према фреквенцији подручја у три групе:

- Ниска фреквенција (*LF*) – 100–500kHz, а најчешће 125kHz, најкраћег су домета сигнала и најмање брзине читавања и преноса. Домет до 10cm.
- Висока фреквенција (*HF*) – 10–15MHz, а најчешће 13,56MHz, кратког до средњег су домета сигнала, средње брзине читавања и преноса. Постоји и систем стандардизације: *ISO 15693* представља стандард за чипове и читаче који раде на фреквенцији од 13,56MHz. Домет до 30cm.
- Ултрависока фреквенција (*UHF*) – ради у распону од 433– 915MHz, и 2,45GHz, највећег су домета сигнала (под *FCC* регулативом) и веће брзине преноса. Овај тип *RFID*-а је специфичан јер не сме бити ометања, тј. препрека између читача и транспондера. *UHF* радио-талас не продире тако добро кроз материјале и захтева више енергије за трансмисију у датом опсегу него талас ниже фреквенције. Три су најчешће фреквенције (као представници ових група) 125kHz, 13,56MHz и 2,45GHz. Већина земаља користи 125kHz или 134kHz подручје за системе ниске фреквенције, и 13,56MHz за системе високе фреквенције. Домет до 100m.

***RFID* читачи** су уређаји који могу да емитују и примају радио-таласе, а користе се за прикупљање информација од *RFID* тагова. *RFID* читачи су кључни део система и неопходни су за функционисање било ког система. Постоје два типа читача:

1. Фиксни
2. Преносиви
  - *RFID Computer*
  - *RFID Handheld*

Фиксни читач, *RFID Computer*, и *RFID Handheld*, приказани су на сликама 20, 21 и 22.



Слика 20. Фиксни *RFID* читач [89]

*RFID Computer* је преносиви уређај, који у себи има *RFID* модул. *RFID Computer* поседује оперативни систем *Windows CE* који је углавном за индустријске уређаје (није исти *Windows* као за *desktop* рачунаре), *Android* или неки други.





Слика 21. *RFID Handheld Juno T41R* [90]

*RFID Handheld* је уређај налик пиштољу, на који се каче таблет или мобилни уређај, и може да подржи различите оперативне системе.



Слика 22. *RFID Handheld* [91]

Активни *RFID* системи се састоје од три кључна дела:

1. читач или испитивач;
2. антена;
3. таг.

**Активни *RFID* тагови** поседују сопствени извор напајања, који омогућава таговима да могу бити прочитани са велике удаљености. Такође, напајање им омогућава и велико складиште меморије. Батерија активних *RFID* тагова уобичајено траје од 3–5 година. Кад се истроши батерија, неопходно је заменити активни таг. Функционалност система потпуно зависи од одабраног типа тага. Постоје два типа активних тагова: *Transponders* (трансподери) и *Beacons* [92],[93], [94].

У системима који користе активни трансподер таг, читач (као пасивни део система) први ће послати сигнал, а затим ће активни трансподер послати назад сигнал са релевантним информацијама. Трансподер тагови су ефикасни, јер продужавају животни век батерије (штеде енергију) када је таг ван домета читача. Активни *RFID* тагови се углавном користе за сигурносне контроле приступа или за системе наплате путарине.

У системима који користе *Beacon* таг, таг не чека сигнал читача. Таг шаље специфичне информације сваких 3–5 секунди. *Beacon* тагови често се употребљавају у индустрији нафте и гаса, рудницима и праћењу товара. Активни таг *Beacon* може да се прочита са раздаљине од

неколико стотина метара, али да би се сачувао животни век батерије, обично су подешени на мању снагу емитовања (раздаљина до 100m).

Предности активних *RFID* тагова су: читање тагова са екстремно велике удаљености, велика издржљивост тагова и већа могућност повезивања тагова са партнерским (сличним) технологијама.

Пасивни *RFID* тагови се састоје од две компоненте:

1. антена;
2. микрочип или интегрално коло (*IC*).

**Пасивни *RFID* таг** чека сигнал од *RFID* читача. *RFID* читач шаље енергију коју прима антена *RFID* тага и енергију претвара у *RF* талас који се прослеђује у зону читања. Након читања записа у тагу, чип генерише енергију и враћа сигнал преко антене до *RFID* читача. Сваки таг се састоји од четири врсте меморије: резервисана меморија, *EPC* меморија, *TID* меморија и корисничка меморија. Резервисана меморија се користи за закључавање или откључавање могућности писања на таг. У *EPC* меморију се снима, тј. садржи *EPC* код (*Electronic Product Code*). *TID* (*Tag Identifier*) меморију једино користи произвођач да унесе јединствени број свог производа. Уколико није довољна *EPC* меморија, користи се проширена корисничка меморија, која може бити величине 4kB или 8kB.

**Тагови** се по тврдоћи деле на уметнуте (штампане) и тврде. Тврди тагови су дуготрајнији и направљени су од пластике, метала, керамике, чак и од гуме. Постоји неколико типова тагова, зависно од њихове намене ([95]):

- *high temperature* – отпоран на високе температуре;
- *rugged* – нераван (отпоран на лед, снег, кишу);
- *embeddable* – уградив (у пукотине и премазан неком смесом);
- *dry inlays* – закачени на материјал или подлогу звану *Web*;
- *wet inlays* – лепе се на објекат (*PET* или *PVT* амбалаже);
- *paper face tags* – штампани на папиру.

Могуће је да тагови имају и додатна својства, као што су анти-метал и водоотпорност. Анти-метал тагови су специфично дизајнирани да се изборе са проблемима који настају када метал омета *UHF* таласе. Постоје различити нивои водоотпорности тагова, зависно од тога у којој мери могу доћи у додир са водом (*IP67*, *IP68*...). На слици 23 приказани су тагови који су коришћени у имплементацији развијеног модела техничког осматрања на брани ХЕ „Бердап 1”.



Слика 23. *RFID UHF* анти-метал и водоотпорни таг [96]

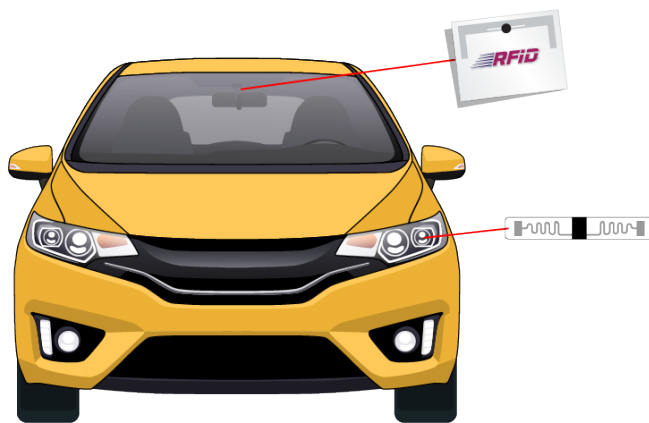
Предности пасивних *RFID* тагова су: мала величина, јефтинији су од активних, танки су и флексибилни, разноврсни, могу да трају читавог живота без батерије (зависно од хабања).

### 3.2.2 Примена *RFID* технологије

*RFID* се примењује у разним друштвеним сферама: у трговини, транспорту и логистици, системима заштите, наплатама путарина, малопродајним објектима итд.

Индустрија малопродаје је међу првим индустријама које су прихватиле *IoT* технологију. Канал продаје нуди две примарне функције: достављање информација и производа купцима. *IoT* има улогу у интеграцији канала, јер омогућава компанијама да уравнотежују понуду и потражњу [97]. Обједињавањем појмова *IoT*-а и малопродаје креира се појам паметна малопродаја ствари (*Retail of Things – RoT*). Паметна малопродаја ствари обједињује хардвер и софтвер прилагођен примени у малопродајном окружењу, тј. малопродајним објектима. *RoT* значи да ће унутрашње и спољашње дигиталне ознаке, ормарићи са екраном, сензори, паметни тагови производа, *wearables*, паметни телефони и други уређаји надгледати, пратити, анализирати, извештавати, сугерисати и саветовати [98]. Хиперконективност ће омогућити да производи, уређаји и справе формирају вишедимензионалне слојеве, поједноставити пословање продавница и побољшати корисничко искуство. Кључна компонента овог појма је технологија. Под технологијом се подразумевају уређаји и компоненте које малопродајним објектима утврђују и поспешују везу са купцима. Технологија омогућава и прикупљање података чијом анализом је могуће оптимизовати пословне циљеве и смањити трошкове пословања. Употреба *RFID* технологије (*Beacon*-а) омогућава продавницама праћење локације производа у целокупном ланцу продаје. Могућност праћења кретања инвентара у реалном времену омогућава трговцима и да боље управљају ресурсима у логистици, набавци сировина итд. Све претходно наведено помаже у оптимизацији трошкова.

*RFID* електронски систем плаћања путарине је систем коришћења налепница да би се прошла наплата рамп (Слика 24) [99]. *RFID* налепница или *RFID* таг је јединствена на сваком возилу, опремљена је радио-чипом, а налепљена је или на фару аутомобила, или на шофершајбни. *RFID* таг је повезан са *Touch 'n Go* електронским новчаником (*eWallet*) са ког ће се новчани износ скинути. Оваква врста наплате путарине користи се у Малезији. Слично читавање путарина је заступљено и у Србији. У Србији се користи таг на који се уплаћује новац. Приликом приласка возила рампи, читач лоциран на рампи препознаје таг и отвара рампу уколико има довољно новца на тагу.



Слика 24. Електронска наплата путарина [99]

*RFID* технологија се примењује и у ормарићима за остављање одређених персоналних ствари на краћи период. Могућа је употреба у спортским објектима, за ормариће за пресвлачење. С обзиром на то да су наруквице гумене, то значи да су водоотпорне, па их је могуће примењивати и на базенима (Слика 25).



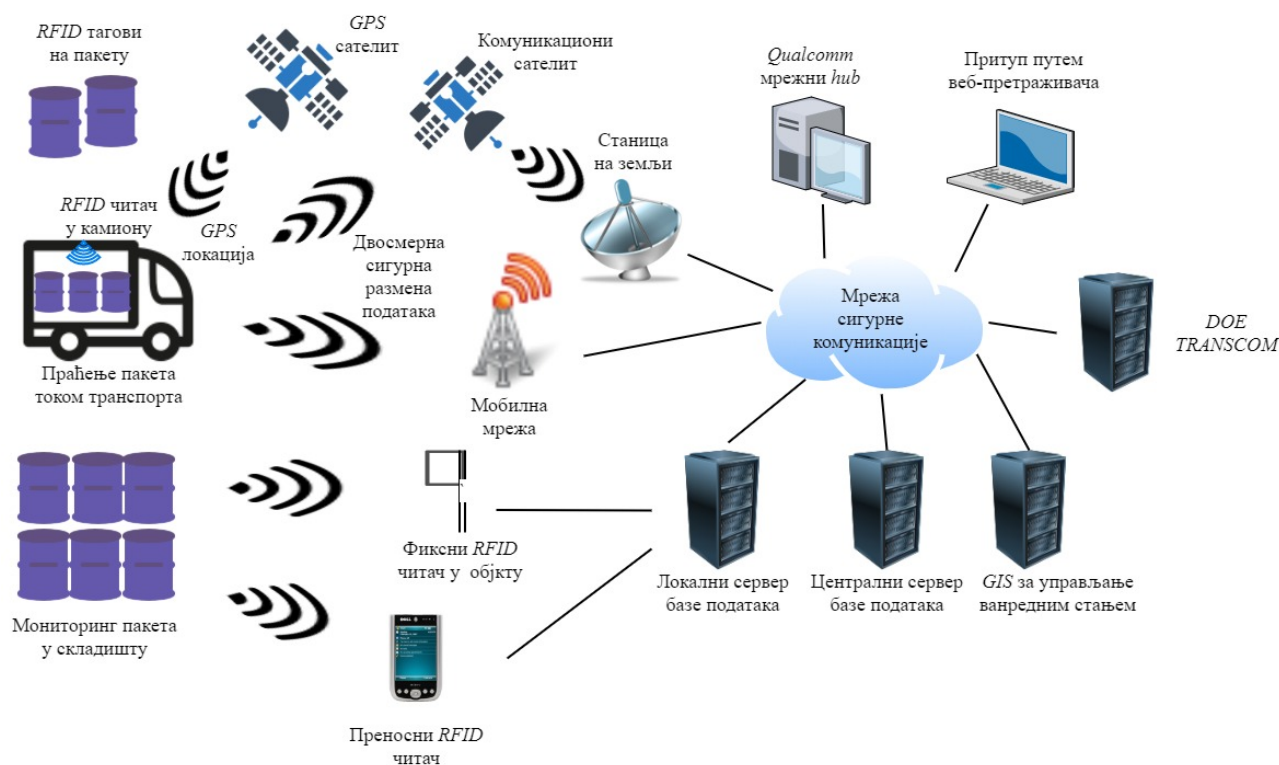
Слика 25. *RFID* наруквица [100]

*RFID* тагови се користе и за контролу приступа. У данашње време, ти привесци често се могу видети на кључевима, јер тагови омогућавају улаз у стамбену зграду или неку просторију (Слика 26).



Слика 26. *RFID* привезак за кључ [101]

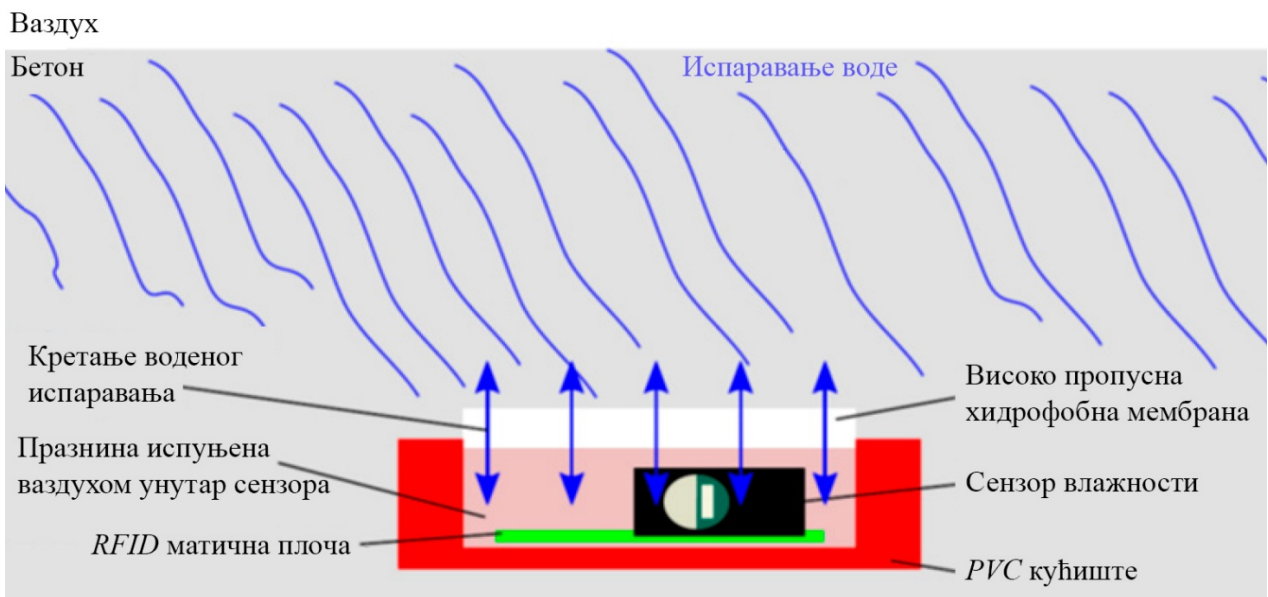
У литератури и на интернету, често повезивани појмови за примену *RFID* тагова су логистика и транспорт. Примена *RFID* тагова у транспорту приказана је на следећој слици (Слика 27). Могуће је пратити стање на залихама, пакет током транспорта, колико робе је ушло у магацин итд.



Слика 27. Примена *RFID* у логистици [102]

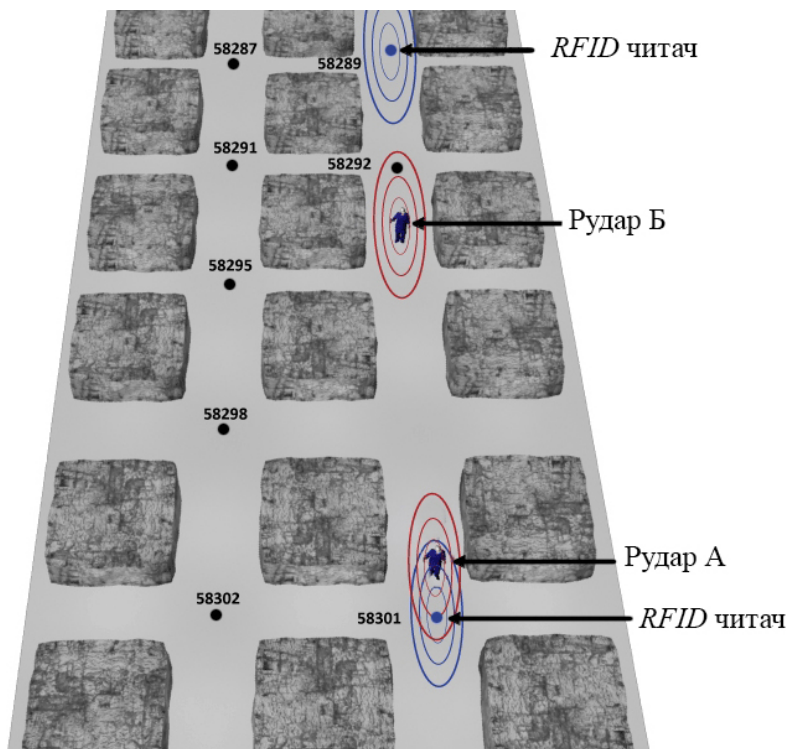
Анализом литературе могуће је видети масовну примену *RFID* технологије у индустрији и логистици, али постоје и друге области где се примењује. Прегледом бројних научних радова, аутор дисертације није наишао на употребу *RFID* технологије у осматрању брана. Већина радова који се баве сигурношћу бране фокусира се на побољшања или иновације софтвера, употребу микрорачунара и микроконтролера и њихову примену у комбинацији са системима раног узбуњивања ([9], [11], [34], [103]).

Многе конструкције у грађевинарству направљене су од армираног бетона [104]. Већина процеса разградње релевантних за овај материјал, нпр. корозија, односи се на повећан ниво влаге материјала. Стога се праћење влаге у армираном бетону сматра кључном методом надзора исправности структура. У [104] студији, у бетон су уграђени сензори засновани на пасивној *RFID* технологији. Сензори су погодни за дуготрајан рад током деценија и добро су заштићени од тешких услова околине. За снабдевање енергијом и пренос података сензора влажности, задужена је *RFID* технологија. Аутори су пратили влажност цемента и показали у експерименту да су уграђени пасивни сензори засновани на *RFID*-у изузетно погодни за дугорочно надгледање структура у грађевини. Схематски приказ система за мерење влажности бетона приказан је на слици 28.



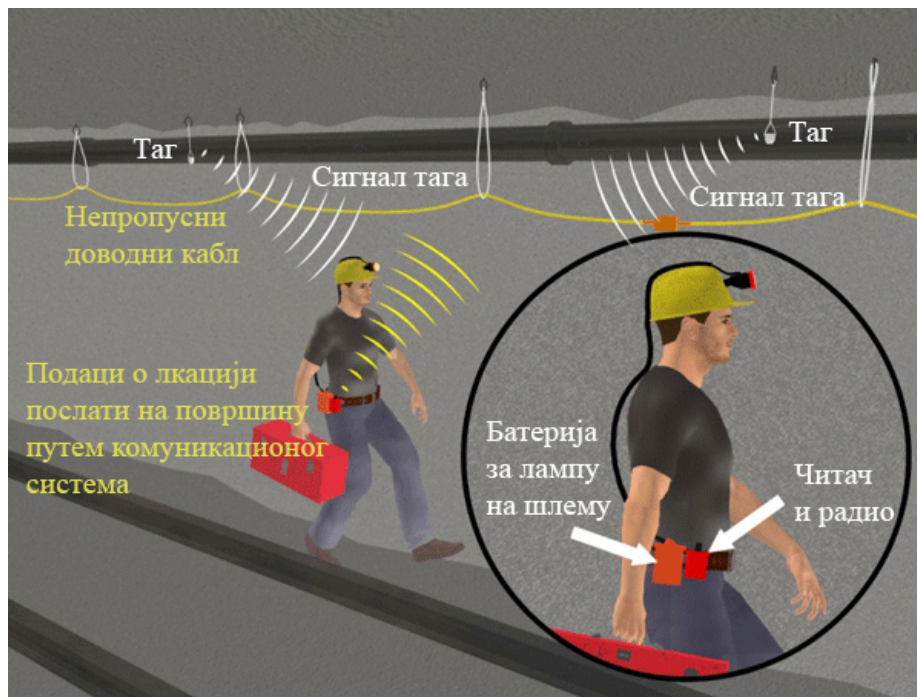
Слика 28. Систем за мерење одговарајуће релативне влажности са уграђеним сензором базираним на пасивној *RFID* технологији [104]

*RFID* технологија је пронашла своју примену и у области рударства. *RFID* читачи постављени су по зонама, тако да могу да прате кретање рудара, што је веома битно када дође до несреће да би се знало колико је рудара у опасности. Зонско праћење рудара приказано је на следеће две слике (Слика 29 и Слика 30).



Слика 29. *RFID* праћење по зонама [105]





Слика 30. *RFID* праћење рудара [105]

*RF Link* је бежични активни *RFID GPS* систем за праћење, интегрисан са *GPS* праћењем, надзором температуре и телематиком. Решење се састоји од активних *RFID* тагова монтираних на контејнере, (расхладне) приколице или било које средство, чиме се обезбеђује тачна, скалабилна и изузетно поуздана видљивост и контрола за било коју промену величине, чак и у отежаним и удаљеним окружењима. Ови *RFID* тагови комуницирају са *Piccolo Plus GPS* јединицом телематике, инсталираном на камиону (делује као *RF* гејтвеј), која пружа решење за управљање возним парком, укључујући понашање возача и дијагностику мотора. Ова два система заједно чине квалитетан и свеобухватан *RFID GPS* систем за праћење за све потребе управљања возним парком и надгледање.

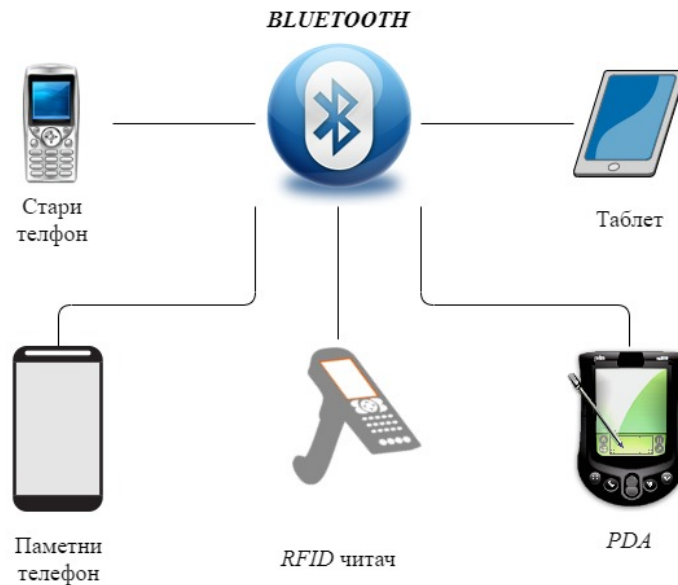


Слика 31. *RFID GPS* систем за праћење возила [105]

*RFID* технологија представља основу унапређеног модела техничког осматрања брана развијеног у дисертацији, и веома је значајна у процесима обележавања битних места (*points of interest – POI*) и праћењу људи и објеката. *RFID* технологија у дисертацији има круцијалну улогу у обележавању мерних места и препознавању мерних уређаја.

### 3.3 Bluetooth

*Bluetooth* је бежична технологија која постоји на већини мобилних уређаја. Примена ове технологије је свестрана и користи се за размену података. Широки спектар комуникације *Bluetooth* технологије са мобилним уређајима приказан је на наредној слици (Слика 32).



Слика 32. *Bluetooth* веза са мобилним уређајима

*Bluetooth* технологија прошла је кроз одређене фазе развоја (Табела 2).

Табела 2. Развој *Bluetooth* технологије [106]

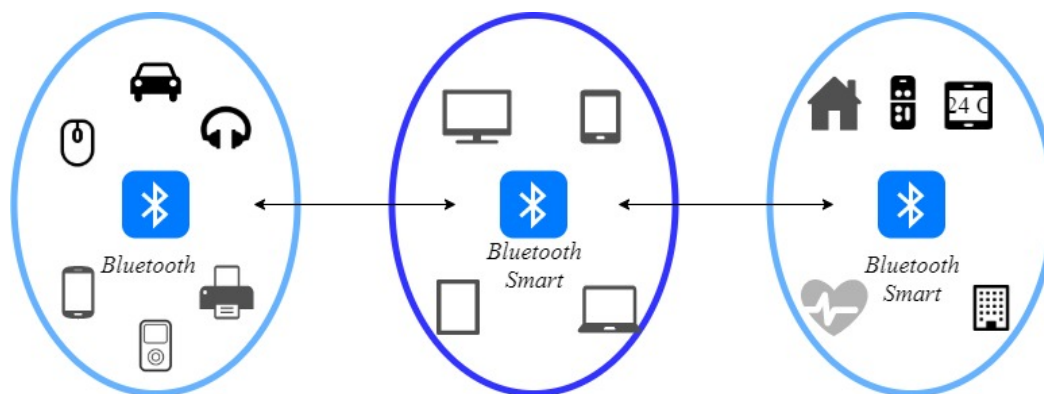
<b>Bluetooth верзија</b>	<b>Спецификација</b>
<b>Bluetooth v1.0 до v1.08</b>	Обавезан <i>Bluetooth</i> хардверски уређај и адреса
<b>Bluetooth v1.1</b>	<i>IEEE</i> стандард 802.15.1 – 2002
<b>Bluetooth v1.2</b>	Бржа конекција
<b>Bluetooth v2.0+EDR</b>	Побољшана брзина протока података
<b>Bluetooth v2.1</b>	Осигурано једноставно упаривање
<b>Bluetooth v3.0</b>	Пренос података велике брзине
<b>Bluetooth v4.0</b>	Мала потрошња енергије
<b>Bluetooth v5.0</b>	Дупли бржи пренос података и четири пута већи домет у односу на <i>Bluetooth v4.0</i>

Постоје две врсте *Bluetooth* технологије које се разликују по потрошњи електричне енергије: *Bluetooth Low Energy (BLE)* и *Bluetooth Classic*. *BLE* се углавном користи за сензоре или за уређаје који имају малу потрошњу енергије. Постоје три класе, зависно од домета: класа 1 распона 100m, класе 2 домета 10m, и класе 3, домета мањег од 10m. Најчешће се употребљава класа 2. Пример употребе класе 2 могуће је видети у раду [107]. *Bluetooth* функционише на опсегу од 2,4GHz *ISM (Industrial, Scientific и Medical)* и базиран је на нискобуџетном радио-линку кратког домета, омогућавајући једноставну комуникацију са стационарним и мобилним окружењем [108]. *Shorey* и други аутори у свом раду објашњавају које су предности



и мане *Bluetooth* технологије и представљају проблеме са којима се корисници *Bluetooth*-а могу сresti у будућности. У [109] аутори су приказали упоредну анализу између *BLE*-а и стандардног *Bluetooth*-а што може користити људима који се баве сензорима. *BLE* проширује *Bluetooth* технологију на уређаје са малим комуникационим захтевима и већим ограничењима у погледу меморијских могућности и аутономије напајања. Тиме *BLE* омогућава бежични пренос информација са паметних објеката, као што су носиви клинички уређаји, амбијентални сензори и актуатори. Ови паметни објекти почињу да буду уређаји који омогућавају интернет, достижући тако интернет интелигентних уређаја. *Zapata* и други аутори користе *FieldVisits* апликацију за дигитално прикупљање података током мерења и пратећих тура на мобилним уређајима, као што су *notebook*-ови, таблети или паметни телефони [110]. *Field* протоколи се могу унети у поље, и ако су повезани путем *GPS*-а, *GPRS*-а, *Bluetooth*-а или *WLAN*-а, могу се директно обрадити, похранити и учинити доступним свим корисницима у систему надзора зграде. као што је *WISKI*. Енергетска компанија *Vorarlberger Illwerke AG* одлучила се за *FieldVisits* као решење за добијање података мерења у реалном времену. *FieldVisits* се тренутно користи и за надгледање брана и за хидрологију. У [111] аутори приказују употребу *BLE* технологија у бежичној сензорској мрежи. *WSN* се понаша као систем за рано обавештавање.

Разноврсна употреба *Bluetooth* технологије приказана је на слици 33.



Слика 33. Разноврсност примене *Bluetooth* технологије [112]

Први круг представља бежичне уређаје, дељење разноврсног садржаја, као што су видео или аудио. Трећи круг представља уређаје са сензорима који шаљу мале пакете података, са малом потрошњом енергије. У средини се налазе уређаји који су повезани са првим и трећим кругом, тј. *Bluetooth* центар.

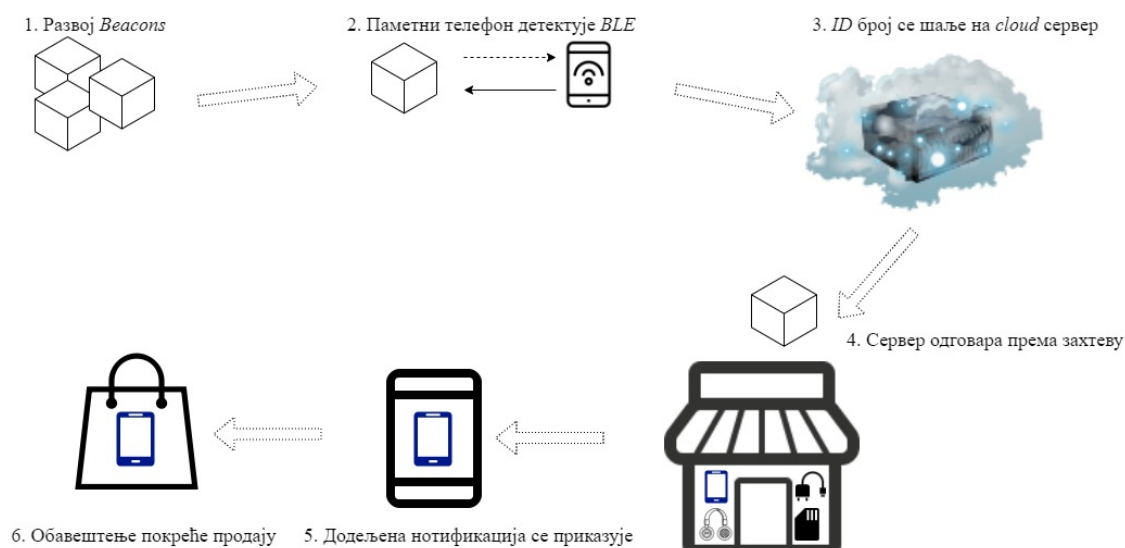
Мерни уређаји на брани који прикупљају податке немају у себи интегрисан *Bluetooth*. Коришћењем екстерног *Bluetooth* модула, омогућена је размена података између мерних уређаја и мобилног преносног уређаја. Ово је битно, јер је интеграцијом *Bluetooth* технологије делимично искључен људски фактор, чиме је елиминисана могућност људске грешке која се може појавити у процесу осматрања бране.

### 3.3.1 *Beacons*

*Beacon* је мали бежични уређај, са напајањем из батерије, који користи *Bluetooth* технологију ниске енергије (*Bluetooth Low Energy*) за оглашавање свог присуства и услуга [113]. *Beacon* константно емитује или оглашава идентификатор сигнала ка компатибилним паметним телефонима или таблетима у непосредној близини. Паметни телефони или таблети затим могу да користе информације *Beacon*-а да би одредили његову локацију и услуге, и у складу са тим делују.

*Beacon* се обично користе у *proximity-aware* апликација (машине које комуницирају са оближњим машинама, и често се заснивају на аутоматизованом локалном умрежавању са малом потрошњом енергије и ограниченим дометом). Мониторингом *Beacon*-а, уређај може да открије када је неко ушао у одређено подручје или изашао из њега, а затим те информације

искористи за стварање интерактивних искустава у смислу шта се налази у близини. Начин функционисања *Beacon*-а приказан је на следећој слици (Слика 34).



Слика 34. Функционисање *Beacon*-а [114]

Сваки *Beacon* уређај садржи процесор (*CPU*), радио и батерије. *Beacon* емитује више пута свој идентификатор. Овај идентификатор прихвата уређај у близини, обично мобилни, и означава важно место у окружењу. Идентификатор је јединствени матични број који паметни телефон препознаје као јединствен за *Beacon*. Једном када буде повезан, *Beacon* ће вршити било коју функцију која је била програмирана да је обавља.

*Beacon* је први пут употребљен у 254 *Apple* продавнице децембра 2013. године, а након тога у *McDonalds* продавницама. Употреба *Beacon*-а у наведеним продавницама имала је за циљ да обавештава купце о тренутним акцијама у продавницама. У данашње време честа је употреба *Beacon*-а у продавницама технике, одеће и обуће, јер су ту акцијски попусти чести.

Не постоји званични стандард *Bluetooth Special Interest Group (SIG)* за *Beacon*. Уместо тога, постоје разни *Beacon* псеудостандарди из конзорцијума компанија или великих провајдера оперативних система. Сваки псеудостандард користи неку од предности *BLE* и широку доступност самог *Bluetooth*-а. Постоји неколико протокола за *Beacon* технологију. Најпознатији протоколи су:

1. *AltBeacon (Radius Networks)*;
2. *GeoBeacon (Tecno-World)*;
3. *iBeacon (Apple)*;
4. *Eddystone (Google)*.

*AltBeacon* спецификација дефинише формат поруке за оглашавање коју *Beacon* емитује блиским уређајима помоћу *BLE*-а [115]. Намена *AltBeacon*-а је да створи отворено и конкурентно тржиште за имплементацију *Beacon*-а. Спецификација *AltBeacon*-а је бесплатна за све имплементације и без икакве накнаде. Примери употребе *AltBeacon*-а су [116]:

- обавештавање корисника о посебним понудама док посећују просторе у робној кући;
- представљање могућности да посетилац у музеју може да добије додатне информација о експонату; или
- аутоматско пријављивање у систему резервација ресторана по доласку госта.

Основна намена *GeoBeacon*-а је иста као и *AltBeacon*-а. Предност *GeoBeacon*-а у односу на претходни тип *Beacon*-а је што користи *NAC (Natural Area Coding System)* формат за адресирање [117]. Главни разлог употребе *NAC*-а је што је обједињује концепт геодетских

тачака, пресека линија, подручја и тродимензионалних региона. Примери употребе *GeoBeacon*-а су:

- обавештавање корисника да су стигли на тачно место;
- слање корисницима нових координата за следеће место које треба да посете, или следећа ствар коју треба да ураде; или
- корисницима се шаљу посебни подаци, тј. поруке, савети итд.

С обзиром на то да су *iBeacon* и *Eddystone* најзаступљенији због својих произвођача, у наредној табели (Табела 3) биће приказана упоредна анализа ова два стандарда.

Табела 3. Упоредна анализа *iBeacon* и *Eddystone* [118]

	<i>Apple's iBeacon</i>	<i>Google's Eddystone</i>
<b>Технологија</b>	<i>iBeacon</i> технологија је <i>beacon</i> протокол. који је уграђен у <i>Apple iOS 7</i> и новије верзије оперативних система, који омогућава <i>iPhone</i> и <i>iPads</i> уређајима да константно скенирају <i>Bluetooth</i> уређаје који су у близини. <i>Beacons</i> користе <i>Bluetooth Low Energy</i> који је део <i>Bluetooth 4.0</i> спецификације.	<i>Google's Eddystone</i> , некада се звао <i>UriBeacon</i> , јесте <i>open-source</i> (отвореног кода) <i>Beacon</i> протокол, који може било које предузеће произвести по приступачној цени.
<b>Компатибилност</b>	<i>iBeacon</i> је компатибилан са <i>Android</i> и <i>iOS</i> , али нативан је само за <i>iOS</i> .	<i>Google's Eddystone</i> је компатибилан са <i>Android</i> и <i>iOS</i> . У суштини, то је <i>cross-platform</i> и као такав компатибилан је са било којом платформом која подржава <i>BLE Beacons</i> .
<b>Профил</b>	Власнички је софтвер. Спецификацију контролише <i>Apple</i> .	Отвореног је кода. Спецификација је доступна на <i>GitHub</i> сајту, под <i>open-source Apache v2.0</i> лиценцом, тако да предузећа и програмери могу да јој приступе и развијају је.
<b>Лакоћа употребе</b>	Једноставан је за имплементацију.	Флексибилна је, али захтева више компликованог програмирања када дође до интеграције, с обзиром на то да шаље више пакета од <i>iBeacon</i> -а.

	<i>Apple's iBeacon</i>	<i>Google's Eddystone</i>
<b>Пакети емитовања</b>	<p>Сваки <i>Beacon</i> емитује информације које су идентификоване као пакети. <i>iBeacon</i> емитује само један рекламни пакет, који има јединствени <i>ID</i> број који се састоји од три дела <i>UUID</i>, <i>Major</i> и <i>Minor</i>.</p>	<p><i>Eddystone</i> емитује три различита пакета:</p> <p>(1) јединствени <i>ID</i> број (<i>Eddystone-UID</i>) – у основи је идентичан као у <i>iBeacon</i>-у. Сви <i>Beacons</i>-и које емитује <i>Eddystone-UID</i> регистровани су у <i>Google</i> бази података.</p> <p>(2) <i>URL</i> адреса (<i>Eddystone-URL</i>) – обавештава паметне уређаје да треба да отворе <i>URL</i> адресу. На тај начин, није потребно да се унапред инсталира апликација одређеног програмера.</p> <p>(3) телеметрија сензора (<i>Eddystone-TLM</i>) – шаље податке сензора. Ово је корисно за компаније које морају да управљају великом количином <i>Beacon</i>-а, јер ова врста оквира шаље дијагностичке податке и здравствену статистику <i>Beacon</i>-а.</p>
<b>Употреба</b>	<p><i>UUIDs</i>, једна од компоненти рекламног пакета, у основи је повезана са програмерским сервером. Када се пошаље на паметни телефон, уређају ће бити потребна посебна апликација да изврши одређени задатак са примљеним информацијама. Због тога је неопходна мобилна апликација за примање порука путем <i>iBeacon</i>-а.</p>	<p><i>Eddystone</i>, шаље <i>URL</i> уместо <i>UUID</i>, који се може једноставно отворити у претраживачу без потребе за специфичном апликацијом. За <i>iOS</i> уређаје, подржан је од стране <i>Chrome</i>-а са укљученом 'Today' нотификацијом, док је за <i>Android</i> уређаје, подржан од 'Physical Web' претраживача.</p>
<b>Сигурност и приватност</b>	<p>Нема неке посебне опције као што је <i>Ephemeral Identifiers (EIDs)</i> у <i>iBeacon</i>-у. Сигнал који емитује <i>Beacon</i> је јавни сигнал и може бити детектован било којим <i>iOS</i> и <i>Android</i> уређајем са одговарајућом спецификацијом.</p>	<p><i>Eddystone</i> има уграђену опцију <i>EIDs</i> која константно мења и дозвољава <i>Beacon</i>-у да емитује сигнал који је доступан само ауторизованим корисницима.</p>

	<i>Apple's iBeacon</i>	<i>Google's Eddystone</i>
<b>API</b>	<i>Apple</i> нема <i>API</i> направљен за управљање <i>iBeacon</i> флотом. <i>Application Program Interface (API)</i> је скуп рутина, протокола, и алата за прављење софтвера. Описује како компоненте треба да се повезују међусобно.	<i>Eddystone</i> има предност, с обзиром на то да је <i>Google</i> објавио <i>API (Nearby API and Proximity Beacon API)</i> , што чини <i>Eddystone Beacons</i> -е моћнијим. Ови <i>API</i> -ји омогућавају много лакше управљање <i>Beacon</i> флотом.

Употреба *RFID* технологије омогућила је унапређење застарелог начина осматрања и прикупљања података са уређаја где је неопходно присуство људског фактора. Осим што је омогућено дигитално препознавање мерног места, употреба *Beacon*-а омогућиће прикупљање података о окружењу у коме човек борави, што се може искористити за оцену квалитета мерених техничких података.

### 3.4 Мобилне технологије

Иницијалне мобилне мреже настале средином 1980-их година двадесетог века, које се називају **мрежама прве генерације (1G)**, биле су засноване на аналогној комуникацији [119]. Ове мреже су имале ограничен регионални опсег, и углавном су биле ограничене на државне границе. Карактеристично за *1G* мрежу су аналогни телефонски позиви, слаба спектрална ефикасност и бројни сигурносни проблеми.

**Друга генерација (2G)** мобилне мреже први пут је представљена 1992. године [120]. Карактеристично за *2G* мрежу је употреба дигиталне енкрипције разговора. Заснована је на *CDMA (Code-Division Multiple Access)*, *GSM (Global System For Mobile Communications)* и *TDMA (Time-Division Multiple Access)* технологијама. Ова мобилна мрежа користи дигиталну технологију. Дигитална технологија омогућила је дигиталне телефонске позиве и слање *SMS (Short Message Service)* текстуалних порука, уз повећану безбедност, али ограничене брзине слања (до *200Kbps*).

**Трећа генерација (3G)** базирана је на *EVDO (Evolution-Data Optimized)*, *HSPA (High Speed Packet Access)* и *UMTS (Universal Mobile Telecommunications System)* технологијама [121]. Главне карактеристике *3G* мреже су пружање мобилних мултимедијалних услуга при брзини преноса од *144Kbps* при великој брзини, *384Kbps* у нормалном раду и *2Mbps* у затвореном простору.

**Четврта генерација (4G)** је унапредила проблем кашњења пакета. Базирана је на *WiMax (Worldwide Interoperability For Microwave Access)* и *LTE (Long-Term Evolution)* технологијама, које омогућавају брзине и до *1Gbps*. Циљ увођења *4G* мобилних комуникационих технологија је остваривање бежичне комуникације са истом брзином података као што је омогућено коришћењем оптичких преносних система који су данас доступни [122]. Четврта генерација (*4G*) мобилне мреже није свуда подједнако заступљена. У неким земљама тек почиње масовно да се примењује.

Од 2012. године, формулисан је низ иницијатива за покретање и дефинисање *5G* мобилних мрежа. Источна Азија и Северна Америка су предњачиле у жељи за још бржом и квалитетнијом мрежом, док је у Европи све то текло знатно спорије. *ITU-R (Интернационална телекомуникациона унија је одговорна за радио-комуникације, која управља фреквенцијама и сателитским орбитама)*, 2012. године је покренула пројект *IMT-2020* [123]. Покретањем поменутог пројекта званично је отпочео развој мобилних система пете генерације.

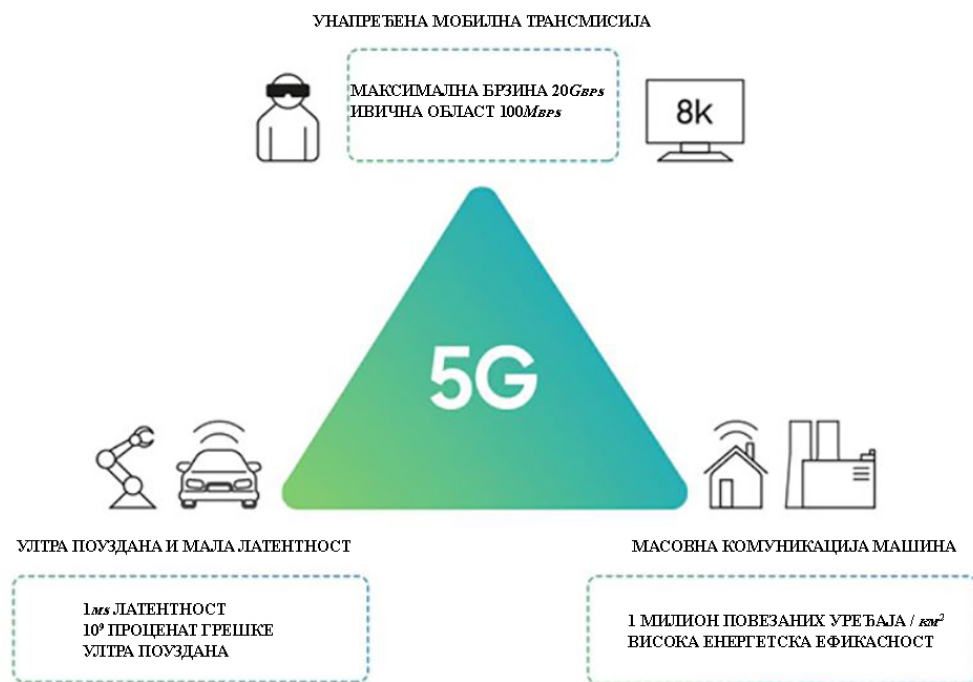
**Пета генерација (5G)**, мобилна мрежа последње генерације користи ћелијску структуру. Ова структура омогућава велики број динамичних корисника, ефикасну употребу *RF* спектра, високу покривеност и адаптивност условима. 5G мрежу чини скуп малих ћелија (фемто ћелије), као што су кућни рутери [124]. Претходне генерације одликовале су велике базне станице. Нова структура мреже омогућава мањим ћелијама (на ивицама мреже) већу аутономију (*Edge Intelligence*). Нову структуру мреже карактерише употреба високих фреквенција, много ефикасније коришћење пропусног опсега, али и повећање капацитета мреже (већи број уређаја на мрежи). Капацитет мреже последње генерације је четири пута већи у поређењу са 4G мрежом.

5G технологија користи нове формате модулације: *GFDM (Generalised Frequency Division Multiplexing)*, *FBMC (Filter Bank Multi-Carrier)*, *UFMC (Universal Filtered Multi-Carrier)*, и управљање са више шема приступања [125]. Системи са више носилаца (*multicarrier systems*) омогућавају већу флексибилност мреже. Употреба микроталасних фреквенција отвара могућност коришћења десетина антена (такозваних паметних антена) на истој опреми. Паметне антене омогућују промену смера таласа, више директних комуникација и повећан капацитет ћелија.

Главне предности које доноси 5G технологија налазе се у технологијама које ће произаћи из принципа рада *SDN* и виртуелизације мрежних функција *NFV (Network Functions Virtualization)*. 5G мрежа се користи за повезивања три главне услуге, побољшане мобилне широкопојасне мреже, есенцијалне комуникације и многобројни *IoT* [51]. 5G мобилна технологија може подстакнути нова имерзивна искуства, као што су *VR (Virtual Reality)* и *AR (Augmented Reality)* са бржим, уједначенијим протоцима података, мањим кашњењем и мањим трошковима по биту. 5G може омогућити нове услуге које могу трансформисати индустрије помоћу ултрапоузданих и доступних веза са малом латенцијом, попут даљинског управљања критичним инфраструктурама, возилима и медицинским процедурама. 5G је намењен неприметном повезивању већег броја уграђених сензора, кроз могућност смањења брзине преноса података, снаге и мобилности, на тај начин пружајући једноставна и јефтина решења за повезивање.

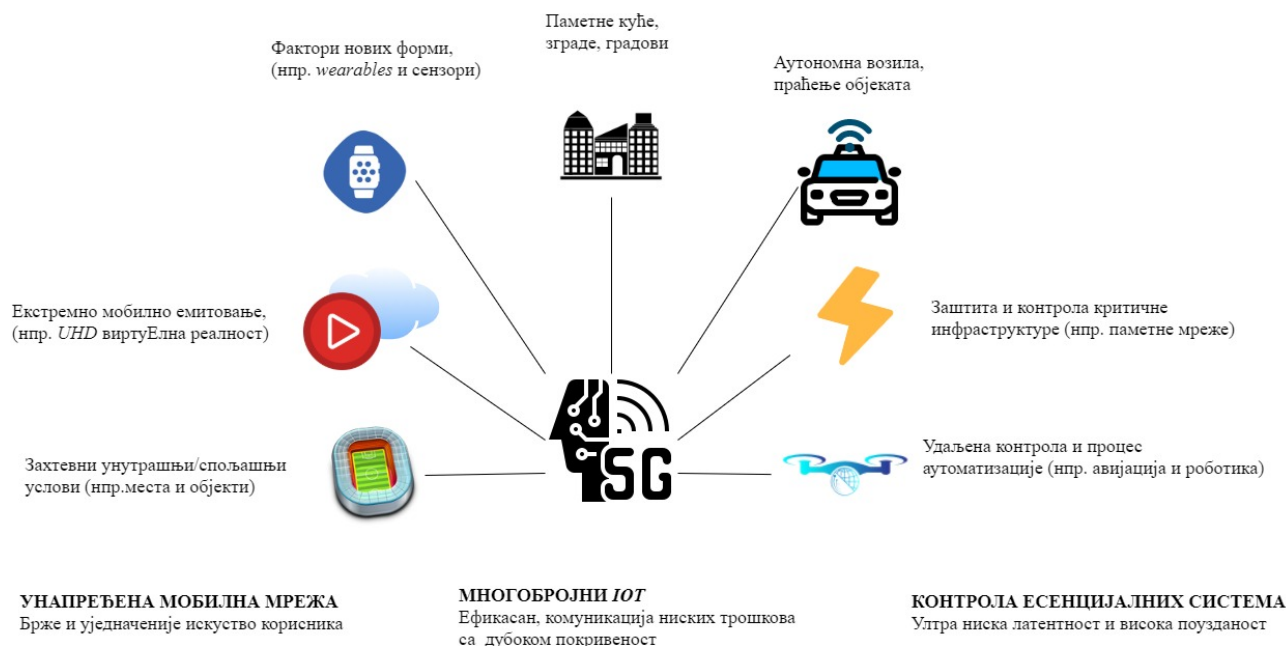
Увођење 5G омогућава корист у три главне области, познате и као „5G троугао” (Слика 35) [126]:

- *uRLLC*: ултрапоуздани примери употребе комуникације са малим кашњењем;
- *mMTC*: случајеви употребе масовне машинске комуникације (*IoT*);
- *eMBB*: побољшана мобилна широкопојасна мрежа – случајеви употребе велике брзине.



Слика 35. 5G троугао [127]

Аутономна возила, 5G IoT у инфраструктури паметних градова и управљању саобраћајем, 5G IoT апликације у индустријској аутоматизацији, проширена и виртуелна реалност, 5G IoT примена код дрoнова само су нека од поља где се 5G може примењивати (Слика 36).



Слика 36. Употреба 5G мреже [128]

Мобилни оператори започели су увођење почетком 2019. године. Очекује се да ће 5G мобилне мреже бити доступне у већини земаља током 2020. године. Такође, сви већи произвођачи Android телефона комерцијализују 5G телефоне. Потрошачи очекују веће брзине мобилног интернета са малим кашњењем. Иако је тешко предвидети када ће сви корисници имати приступ 5G, приметна је велика заинтересованост за покретање 5G мреже. Неке од земаља које



су до сада увеле 5G су: Аустралија, Аустрија, Бахреин, Немачка, Кина, Италија, Јапан, Кина, Америка, Швајцарска, Шпанија итд.

5G је прилагодљив и омогућава многе нове примене које са претходном технологијом нису биле могуће, посебно у урбаним областима и градовима. Случајеви употребе 5G неће бити ограничени на одређене учеснике: потрошачи, предузећа, индустрије, па и градови, имаће користи од једне или више димензија „5G троугла”.

Употребом мобилних технологија, а у овој дисертацији *Trimble* мобилног уређаја, омогућено је оператерима који врше мониторинг да унапреде своје пословање, убрзавајући читавање података и смањујући могућност за грешком. Употребом новијих генерација мобилне мреже (4G и 5G), пренос података при аутоматизованом читавању података убрзаће процес преношења података од мерног инструмента до сервера, а недостаци који су пратили претходне генерације мобилних мрежа биће елиминисани или унапређени. У блиској будућности може се размотрити увођење WSN-а у комбинацији са 5G мрежом.

### 3.5 *Cloud computing* технологије

*Cloud computing* је апстрактна, скалабилна и контролисана рачунарска инфраструктура која хостује (чува) апликације за крајње кориснике [129]. *Cloud computing* је област рачунарства која путем интернета пружа клијентима високоскалабилни ИТ простор (капацитет) као услугу. *Cloud computing* је модел који омогућава општеприсутан, прилагодљив, „по захтеву” приступ мрежи заједничке групе подесивих рачунарских ресурса (нпр. мреже, сервери, складиштења, апликације и услуге), које могу брзо снабдевати кориснике уз минималан напор управљања или интеракција са провајдером услуге.

Организације употребљавају *cloud computing* да би смањиле трошкове који се односе на *e-mail*, ИТ инфраструктуру, дата центре, складишта и пословне апликација [130]. *Cloud computing* је модел који омогућава свеприсутан, практични приступ мрежи, базиран на корисничком захтеву, дељеном складишту подесивих рачунарских ресурса (нпр. мреже, сервери, складишта, апликације и услуге), који се могу брзо обезбедити и објавити уз минималне напоре управљања или интеракцију провајдера.

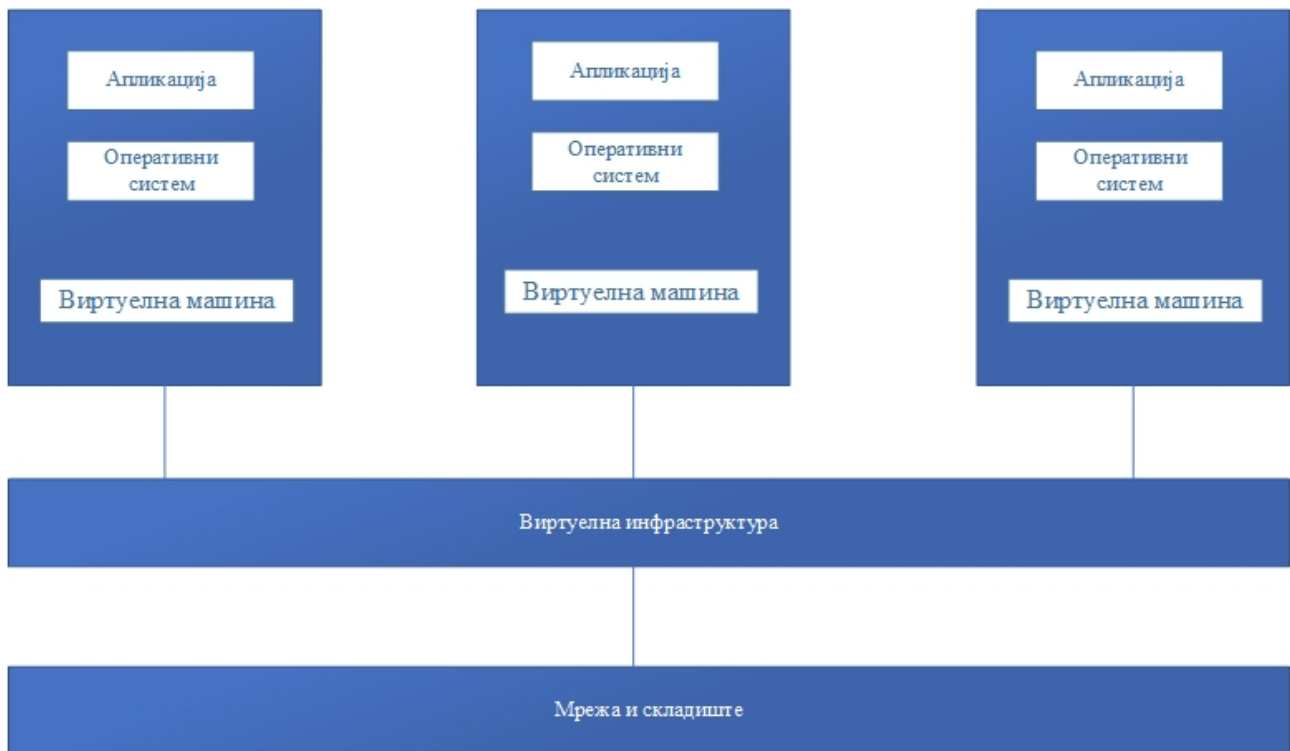
Глобално, по начину употребе и власништву, *cloud* се може поделити на јавни и приватни *cloud* [131]. Јавни *cloud*-ови су у власништву провајдера и њима управљају провајдери. Супротно моделу јавног *cloud*-а, приватни модел омогућава образовним установама потпуну контролу управљања идентитетом, услугама, сигурношћу података, апликацијама и ресурсима који се пружају њиховим корисницима.

Постоје одређене технологије које раде иза *cloud computing* платформи и чине *cloud computing* флексибилним, поузданим и употребљивим [132]. Ове технологије су: виртуелизација, сервисно оријентисана архитектура, *Grid computing*, *Utility computing*.

#### **Виртуелизација**

Виртуелизација је рачунарска техника, која омогућава поделу једне физичке инстанце, апликације или ресурса између више организација или корисника. То функционише додељивањем логичког имена физичком ресурсу и обезбеђивањем показивача на тај ресурс када је то захтевано. Концепт виртуелизације приказан је на слици 37.





Слика 37. Концепт виртуелизације [132]

### Виртуелизација мрежних функција

Виртуелизација мрежних функција (*NFV*) је концепт мрежне архитектуре који омогућава одвајање софтвера од хардвера. Одвајање је омогућено због повећања перформанси комерцијално доступних платформи. *NFV* је начин за виртуелизацију мрежних сервиса, попут рутера, *firewall*-а и балансера учитавања, који се традиционално изводе на власничком хардверу [133]. Ове услуге су упаковане као виртуелне машине (*virtual machine*) на хардверу, што омогућава провајдерима услуга да покрећу своју мрежу на стандардним серверима уместо на власничким. Уз *NFV*, није обавезно имати наменски хардвер за сваку мрежну функцију. *NFV* побољшава скалабилност и агилност омогућавајући пружаоцима услуга испоруку нових мрежних услуга и апликација на захтев, без потребе за додатним хардверским ресурсима.

### Сервисно оријентисана архитектура

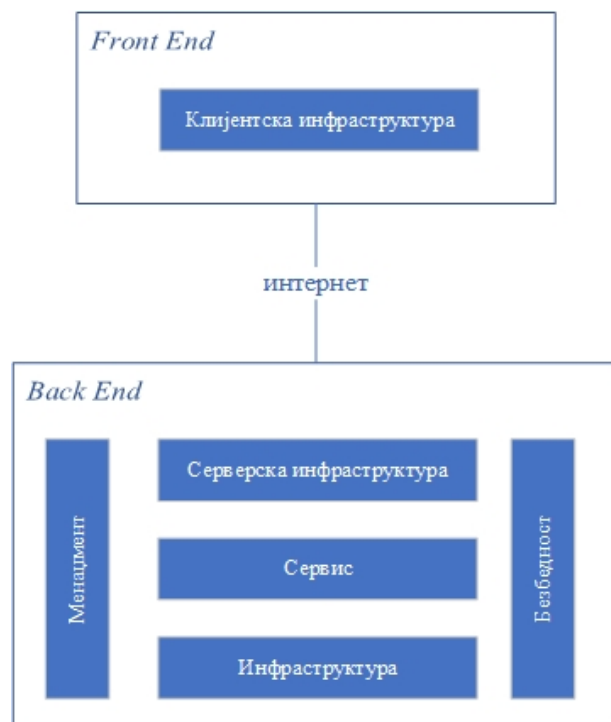
Сервисно оријентисана архитектура (*SOA*) омогућава да се апликације користе као сервиси за друге апликације, без обзира на произвођача, производ или технологију. То омогућава размену информација између апликација различитих произвођача без додатног програмирања или измене услуга.

### *Grid Computing*

*Grid Computing* се односи на дистрибуирано рачунарство у којем је група рачунара са различитих локација међусобно повезана ради постизања заједничког циља. Рачунарски ресурси су хетерогени и географски распршени. *Grid Computing* дели комплексне задатке на мање делове, који се дистрибуирају до процесора који се налазе унутар мреже.

### *Cloud computing*

*Cloud computing* архитектура се састоји од много *cloud* компоненти које су слободно повезане [132]. Архитектуру облака могуће је поделити на *Front End* и *Back End*. Оба краја су повезана преко мреже, углавном преко интернета. На следећој слици (Слика 38) могуће је видети архитектуру *cloud computing*-а.



Слика 38. *Cloud computing* архитектура [132]

*Front End* се односи на клијентски део *cloud computing* система. Састоји се од интерфејса и апликација које су потребне за приступ *cloud computing* платформама (веб-претраживач). *Back End* се односи на сам *cloud*. Обухвата ресурсе који су неопходни системима *cloud computing*-а. Састоји се од великог складишта података, виртуелних машина, механизма заштите, сервиса, сервера итд.

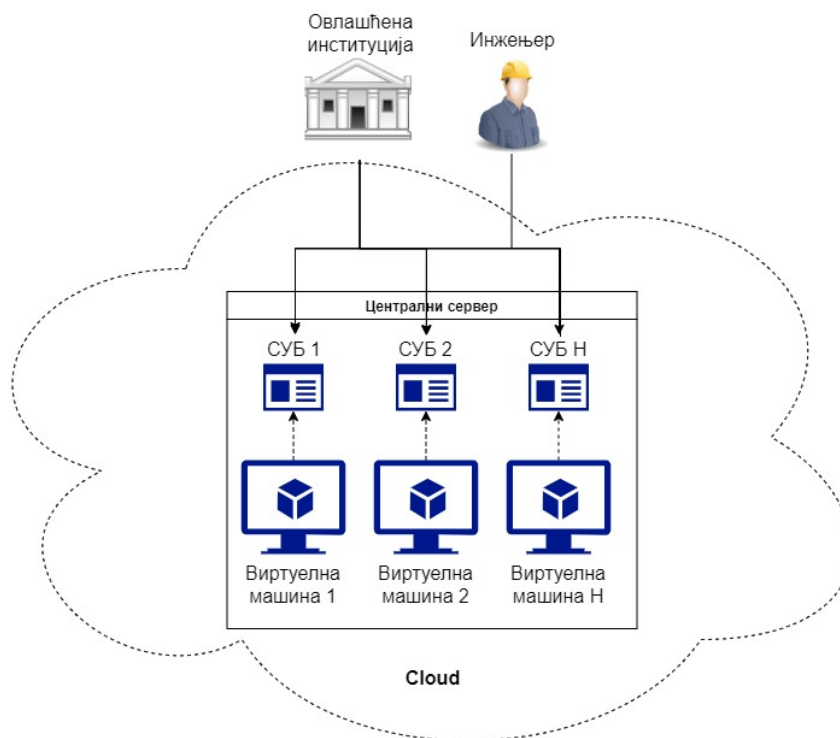
Постоје три типа *cloud computing*-а [134], [135]: *Software as a Service (SaaS)*, *Platform as a Service (PaaS)* и *Infrastructure as a Service (IaaS)*.

*SaaS* је популарна и често коришћена форма рачунарства у облаку. Пружа све функције сложене традиционалне апликације. Уместо коришћења локално инсталираних апликација, ове функције се пружају путем веб-претраживача.

*PaaS* обезбеђује виртуелизоване сервере, где корисници могу да покрећу постојеће апликације или да развијају нове, без бриге око одржавања оперативних система, хардвера сервера, капацитета рачунара или оптерећења.

*IaaS* обезбеђује виртуелизоване сервере, мреже, складиште и софтверске системе направљене тако да додају или мењају функције целог дата центра.

*Cloud computing* је битна технологија у овој дисертацији, јер се свим подацима, који су на удаљеном серверу, приступа преко интернета, тј. веб-апликација (Слика 39). Употребом *cloud computing*-а омогућава се еластичност и скабилност система. Систем користи онолико ресурса колико је потребно у том тренутку, што значи уколико се повећавају активности, повећавају се и ресурси, и обрнуто у случају смањивања. Централни сервер се налази у *cloud*-у. На централном серверу су подигнуте виртуелне машине у којима се налазе софтвери који се користе за управљање сигурношћу брана. Свака виртуелна машина је везана за одређену брану. Веб-апликације омогућавају корисницима да прате историјске податке у реалном времену и на основу тога да праве прорачуне и моделирају бране, такође могуће је сагледати мерне инструменте, мерна места, и остале податке који се тичу самих брана. Апликације користе различите групе корисника овлашћене институције, инжењери, службе осматрања итд.



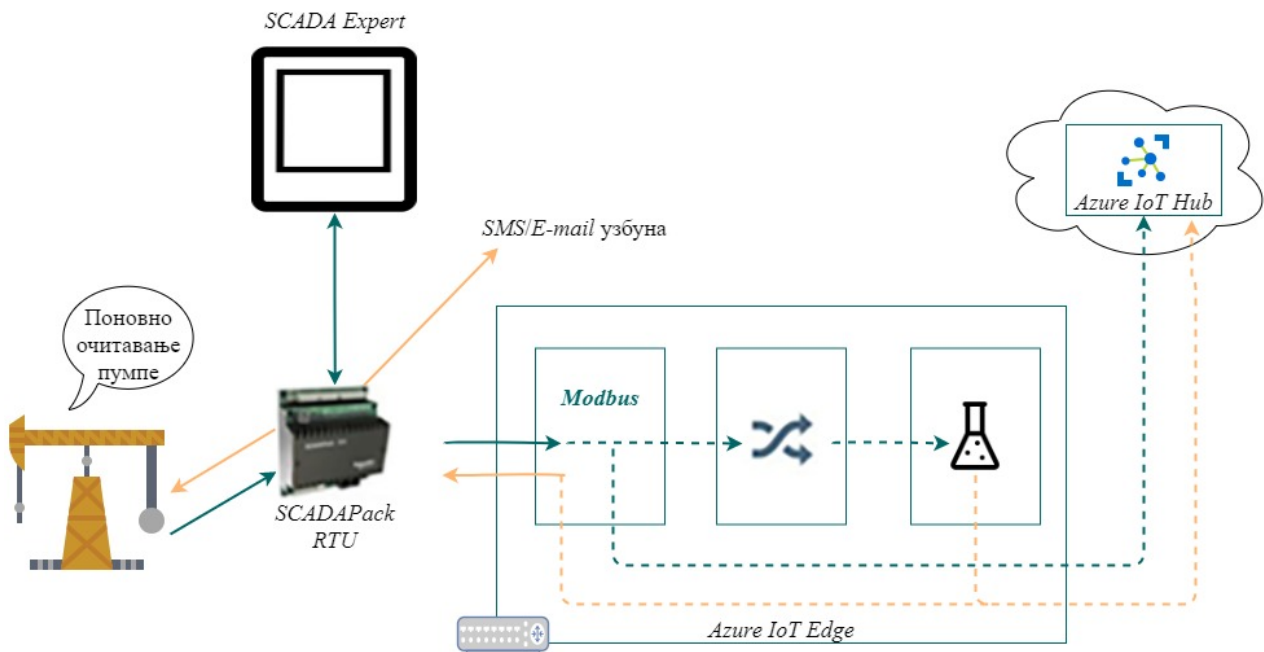
Слика 39. Концепт виртуелизације и *cloud computing*-а

### 3.6 *IoT Edge (Edge computing)*

*IoT Edge* трансформише начин на који се управља подацима, обрађује и преноси (испоручује) са милиона уређаја широм света [136]. Раст броја *IoT* уређаја, заједно са новим апликацијама којима је потребна рачунска снага у реалном времену захтевају употребу *Edge computing* система. Брже технологије умрежавања, попут *5G* бежичне везе, омогућавају модерним рачунарским системима да убрзају стварање или подршку апликацијама у реалном времену, као што су видео-обрада и аналитика, аутономни аутомобили, вештачка интелигенција и роботика.

*Edge computing* је филозофија умрежавања која је фокусирана на приближавање рачунара извору података, ради смањења кашњења испоруке података и употребе пропусне ширине (*bandwidth*) [137]. *Edge computing* омогућава веће рачунарске прорачуне и мрежне захтеве од крајњих уређаја ка паметним стварима. Представља смањење процеса који се одвијају у облаку и премештање тих процеса на локална места (мерна места), попут рачунара корисника, *IoT* уређаја или рубног сервера. Довођење процесног рачунања до ивице мреже минимизује количину комуникације на даљину, која се мора догодити између клијента и сервера.

За уређаје повезане на интернет, мрежна ивица је место на којем уређај или локална мрежа, која садржи уређај, комуницира с интернетом. Ивица је помало неодређен појам, јер нпр. корисников рачунар или процесор унутар *IoT* камере могу се сматрати мрежном ивицом, али и корисников рутер, *ISP (Internet service provider)* или локални ивични сервер се такође сматрају ивицом. Важно је да је ивица мреже географски близу уређаја, за разлику од матичних сервера и сервера у облаку, који могу бити доста удаљени од уређаја са којима комуницирају. На следећој слици (Слика 40) приказано је решење компаније *Schneider Electric*. Приказан је систем пумпи за вештачко дизање, који користе *Azure Machine Learning* и *Azure IoT*, да би довели предиктивну аналитику на ивицу.



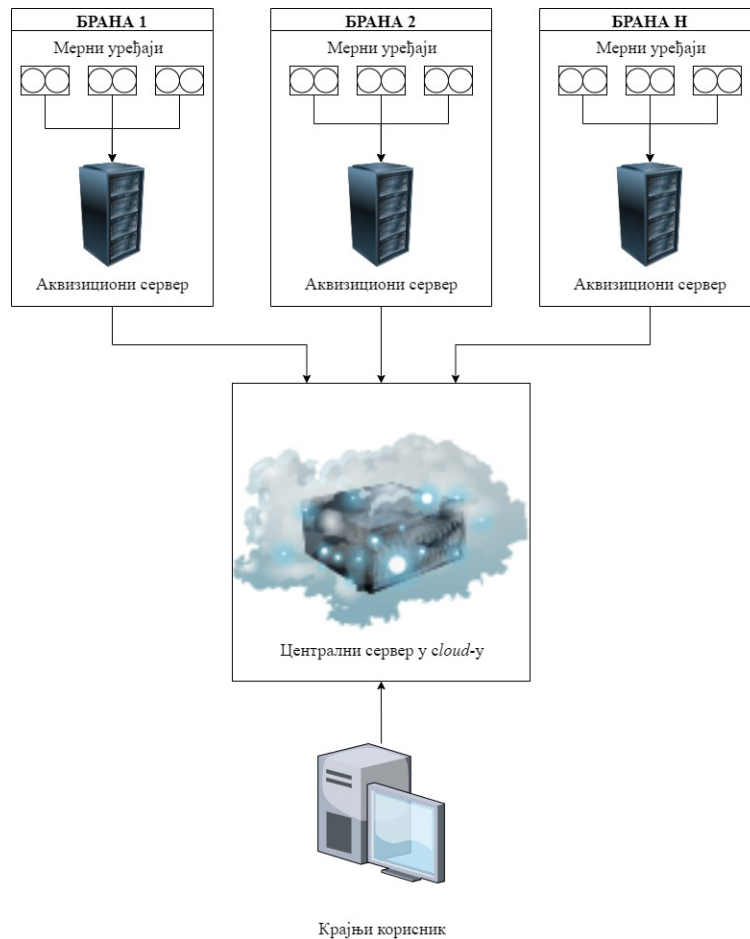
Слика 40. Schneider Electric систем пумпи [138]

Кључне предности *Edge computing*-а су:

- смањена латенција;
- смањење коришћења пропусне ширине и повезаних трошкова;
- смањење ресурса сервера и повезаних трошкова; и
- додатна функционалност.

Један од недостатака *Edge computing*-а је што може да повећа векторе напада. Уз додавање више паметних уређаја у микс, попут рубних сервера и *IoT* уређаја који имају робусне уграђене рачунаре, отварају се нове могућности злоупотребе ових уређаја.

Још један недостатак *Edge computing*-а је то што захтева више локалног хардвера. На пример, док је *IoT* камери потребан уграђени рачунар да би послао своје необрађене видео-податке на веб-сервер, потребан јој је много софистициранији рачунар са више процесорске снаге да би могао покренути своје алгоритме за откривање покрета. Смањење трошкова хардвера омогућава јефтинију опцију за изградњу паметнијих уређаја.



Слика 41. *Edge computing* на брани

На основу претходне слике (Слика 41), може се рећи да је идеја *Edge computing*-а делимично заступљена на брани. Аквизициони сервери, који су близу мерних уређаја, користе се за обраду и валидацију података, који се касније прослеђују централном серверу. Крајњи корисник приступа подацима на централном серверу путем разних апликација.

## 3.7 Технологије за управљање подацима

### 3.7.1 Нерелационе базе података

**Нерелациона база података** не користи табеларну схему редова и колона који се налазе у већини традиционалних система база података [139]. Нерелационе базе података користе модел складиштења који је оптимизован за специфичне захтеве, прилагођене врсти података који се чувају. На пример, подаци се могу чувати као једноставни парови кључа/вредности, као *JSON* документи или као графикон. Нерелационе базе података су све више прихваћене и примењене, јер су дизајниране да превазиђу ограничења релационих база података и решавају проблем *Big data* [140]. Иако се нерелационе (*NoSQL*) технологије веома разликују, ове базе података су обично скалабилније и флексибилније од релационе базе података.

Нерелационе базе података еволуирале су из релационих технологија због:

- Модели података: за разлику од релационих модела који захтевају унапред дефинисану шему, *NoSQL* базе података нуде флексибилну схему пројектовања, која олакшава надоградњу базе података, како би се изашло у сусрет променљивим захтевима апликација.

- Структура података: нерелационе базе података дизајниране су за обраду неструктурисаних података који се не уклапају исправно у редове и колоне. Ово је важно јер је већина данас генерисаних података неструктурисана.
- Скалирање: систем је могуће хоризонтално скалирати користећи предности јефтиних сервера.
- Развојни модел: *NoSQL* базе података су обично отвореног кода, што значи да се унапред не плаћа накнада за лиценцирање софтвера.

**Big data** су подаци великог обима, које тешко могу обрадити традиционални протоколи база података попут *SQL*-а [141]. Обим, разноликост и брзина доступних информација експоненцијално повећавају сложеност информација којима компаније треба да управљају. Системи који обрађују и складиште *Big data* постали су уобичајена компонента архитектуре управљања подацима у организацијама. *Big data* често карактеришу три ствари: велика количина података у многим окружењима, велика разноликост врсте података похрањених у великим системима података, и брзина којом се подаци генеришу, прикупљају и обрађују. Ове карактеристике је први идентификовао *Doug Laney*, тада аналитичар у *Meta Group Inc.*, 2001. године [142]. У новије време, неколико других карактеристика је додато различитим описима *Big data*, укључујући истинитост, вредност и променљивост.

Код појма *Big data* није битна количина података, већ како и за шта се ти подаци користе [143]. Подаци могу бити прикупљени и анализирани из било ког извора да би се добили одговори који омогућавају: 1) смањење трошкова; 2) смањење времена обраде података; 3) развој нових производа и оптимизована понуда; и 4) паметно доношење одлука. Комбиновањем *Big data* и напредне аналитике, могуће је извршити пословне задатке, као што су:

- утврђивање узрока кварова, проблема и недостатака у такорећи реалном времену;
- генерисање купона на продајном месту на основу навика купца;
- прерачунавање целокупног портфолија ризика у минутима; или
- откривање лажног понашања пре него што се одрази на предузеће.

Појам *Big data* је поменут као технологија коју је могуће користити у блиској будућности и помоћу које ће моћи да се врши предиктивна аналитика, и брзо претражују историјска стања брана. У блиској будућности, са све већом употребом *GIS (Geographic Information System)* података, може доћи до потребе за имплементацијом *Big data* концепта у контексту осматрања брана. У [144] аутори користе *IoT* и *Big data* аналитику за управљање квалитетом воде. За управљање водом аутори користе паметне водомере који бележе и пријављују квалитет и потрошњу воде, упозоравају на цурење воде или потенцијално загађење. Подаци се бележе у нерелационим базама података. *Big data* и *Machine Learning* показали су велики потенцијал за примену при доношењу одлука заснованих на подацима, научним открићима и оптимизацији процеса [145]. Овај технолошки напредак може се у великој мери користити у управљању водама и животном средином (*Environment and Water Management – EWM*), посебно зато што многе *EWM* апликације (нпр. рано упозорење од поплава) захтевају могућност за самостално и у реалном времену извлачење корисних информација из велике количине података.

### 3.7.2 Релационе базе података

*SQL* је стандард релационих упитних језика, и далеко је заступљенији у релационим системима од осталих стандарда, због чега је његово детаљно познавање неопходно за ефикасно коришћење тих система [146]. Постоји неколико врста *SQL*-а. *Oracle* база података користи своју верзију *PL/SQL*, а *SQL* сервер компаније *Microsoft* користи *Transact-SQL* [147]. Све варијације се заснивају на индустријском стандарду *ANSI SQL*.

У досадашњем функционисању мониторинга брана у Србији користиле су се релационе базе података и *SQL*. Тренутна поставка система омогућава крајњем кориснику да захтева податке из *SQL* базе путем веб-апликација. Подаци који се прикупљају различитог су типа и формата.



Прикупљени подаци се преносе у *JSON* или *XML* формату. У централној бази података налазе се подаци о временским серијама, подаци о осматрањима, документа и подаци о функционалности централног сервера (Слика 42). Подаци о функционалности, који се налазе у централној бази података, односе се на графичке подлоге, временске дијаграме и корисничке налоге. Сви подаци су временски референцирани, па је могуће пратити историју измена у току коришћења система. Коришћење база података је битно због претраге историјских података. Историјски подаци су битни приликом одређивања контроле квалитета мерених података. У Србији је могуће анализирати податке још из 60-их година 20. века. У бази података такође се повезују мерна места са мерним уређајима, како би се знало који мерни уређај се налази на ком мерном месту.



Слика 42. Централна база података [13]

### 3.7.3 Технологије за чување и пренос података

*JSON* (*JavaScript Object Notation*) је синтакса која се користи за чување и размену података [148]. *JSON* је текст који је писан са *JavaScript* нотацијом објеката. *JSON* формат је само текст, и њим се лако може управљати, тј. може се једноставно послати на сервер и са сервера, а користи се као формат података у било ком програмском језику. *JSON* формат је колекција података, читљива за људско око, којој се може логички приступати.

*XML* (*eXtensible Markup Language*) је језик означавања (*markup*), који је пројектован за чување и размену података [149]. Пројектован је тако да сам себе описује. Састоји се од тагова, који нису предефинисани. Осетљив је на велика и мала слова. *XML* дозвољава дефинисање *markup* елемената и генерисање прилагођеног (*customized*) *markup* језика.

Главна разлика између два формата приказана је у табели која следи.

Табела 4. Разлика између *XML* и *JSON* формата [150].

<i>JSON</i>	<i>XML</i>
<i>JSON</i> објекат има тип.	<i>XML</i> подаци су без типа.
<i>JSON</i> типови: <i>string</i> , <i>number</i> , <i>array</i> , <i>Boolean</i> .	Сви <i>XML</i> подаци требало би да буду типа <i>string</i> .
Подаци су лако доступни као <i>JSON</i> објекти.	<i>XML</i> податке треба парсирати.
<i>JSON</i> подржава већина претраживача.	Парсирање <i>XML</i> -а између претраживача може бити тешко.
<i>JSON</i> нема могућности приказа.	<i>XML</i> нуди могућност приказа података јер је то <i>markup</i> језик.

<b>JSON</b>	<b>XML</b>
<i>JSON</i> подржава само текстуалне и бројчане типове података.	<i>XML</i> подржава разне типове података, као што су бројеви, текст, слике, графици, графови, итд. Такође нуди опције за пренос структуре или формата података са актуелним подацима.
Извлачење вредности је једноставно.	Извлачење вредности је тешко.
Потпуно аутоматизовани начин десеријализације/серијализације <i>JavaScript</i> .	Програмери морају да пишу <i>JavaScript</i> код за десеријализацију/серијализацију <i>XML</i> -а.
Уграђена подршка за објекте.	Објекат мора бити изражен конвенцијама – углавном је промашена употреба атрибута и елемената.
Подржава само <i>UTF-8</i> .	Подржава разне типове енкодирања.
Не подржава коментаре.	Подржава коментаре.
<i>JSON</i> документи су читљивији од <i>XML</i> .	<i>XML</i> документи су тежи за читање и интерпретирање.
Нема подршку за <i>namespaces</i> .	Подржава <i>namespaces</i> .
Мање је безбедан.	Безбеднији је од <i>JSON</i> -а.

*JSON* и *XML* су подржани формати за пренос и чување података који се користе на бранама. Помоћу поменутих формата врши се пренос података од мерног уређаја до базе података.

У зависности од имплементације система за управљање браном, односно дела везаног за управљање подацима, користе се једна или комбинација више технологија описаних у овом потпоглављу.

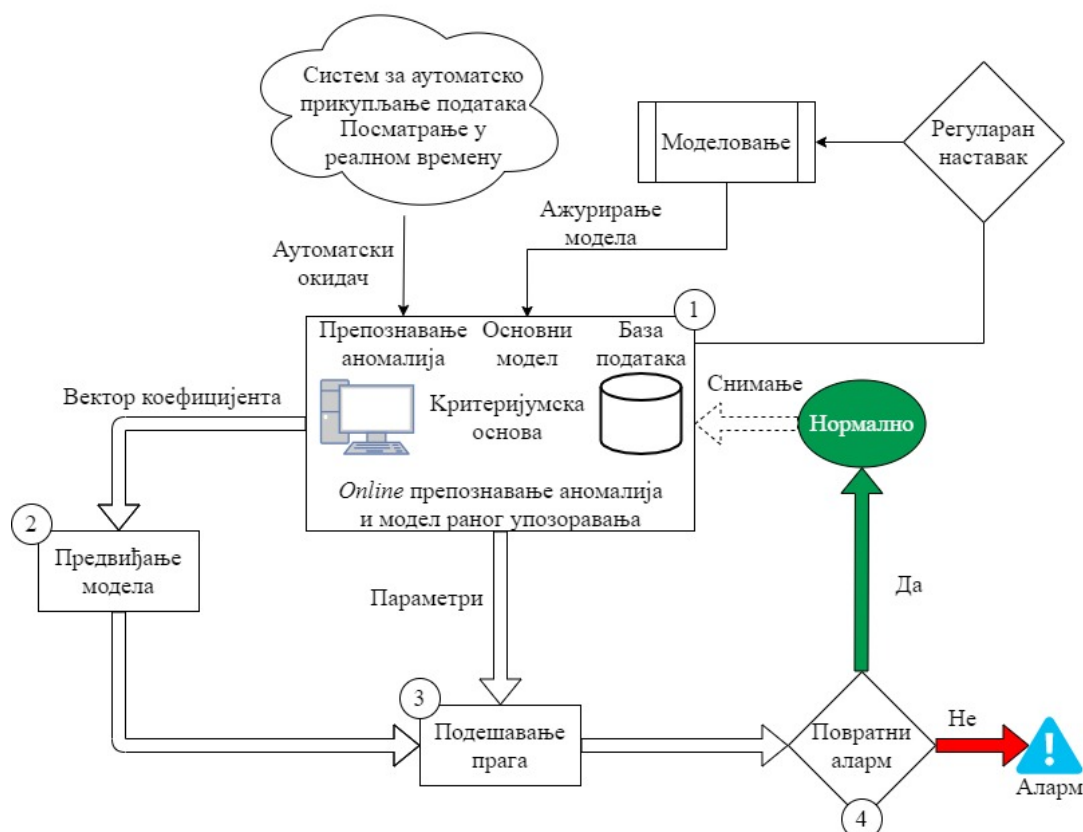


## 4. РАЗВОЈ МОДЕЛА ЗА ПАМЕТНО УПРАВЉАЊЕ/ОСМАТРАЊЕ БРАНАМА

### 4.1 Анализа постојећих модела

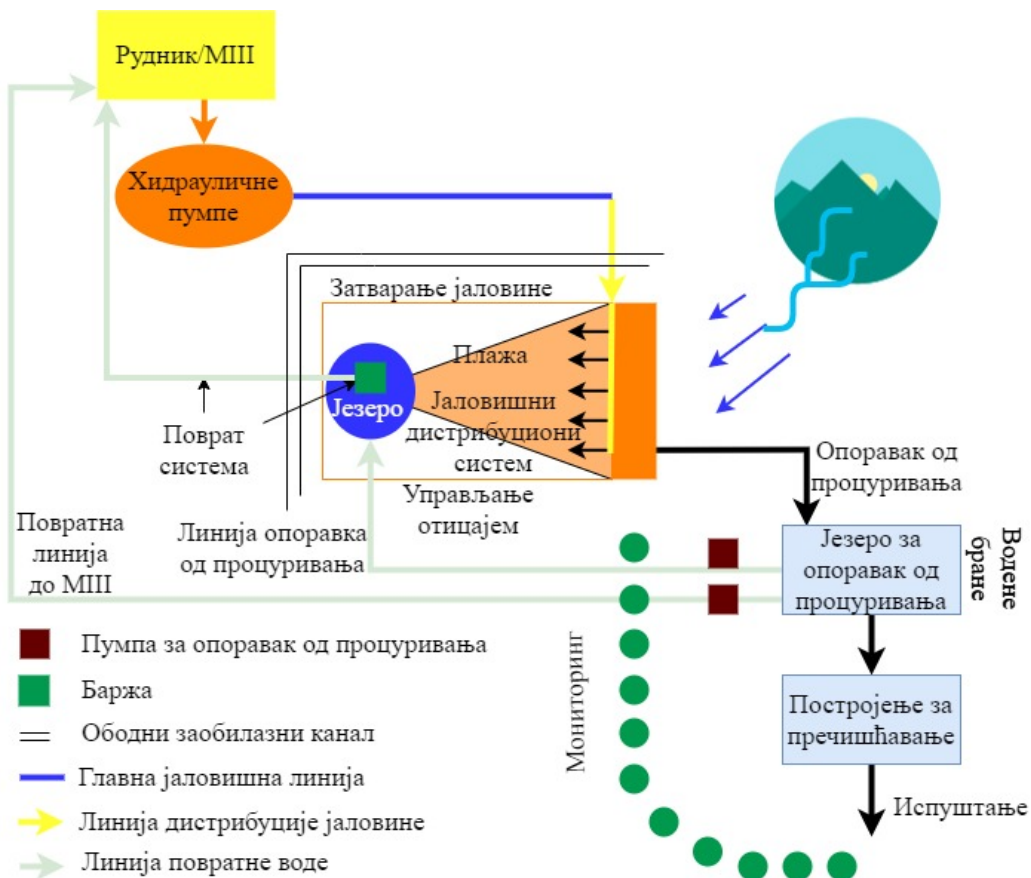
Мониторинг брана је битан у функционисању брана. Мониторинг брана примењен је на разне начине и презентован у бројним пројектима. Већина пројеката реализована је унапређењем софтверског система или употребом *IoT* технологија (*Raspberry Pi* или *Arduino*). Битан елемент мониторинга брана је пред аларм, тј. систем раног упозоравања (*pre alarm, early warning*).

У [9] аутори предлажу *online* pametno препознавање аномалија помоћу робусне регресије (део робусне статистике) и модел базиран на раном упозоравању (*online Robust Recognition and Early Warning model – RREW model*). Модел је приказан на слици која следи (Слика 43). Модел је примењен на насутуј и бетонској брани.



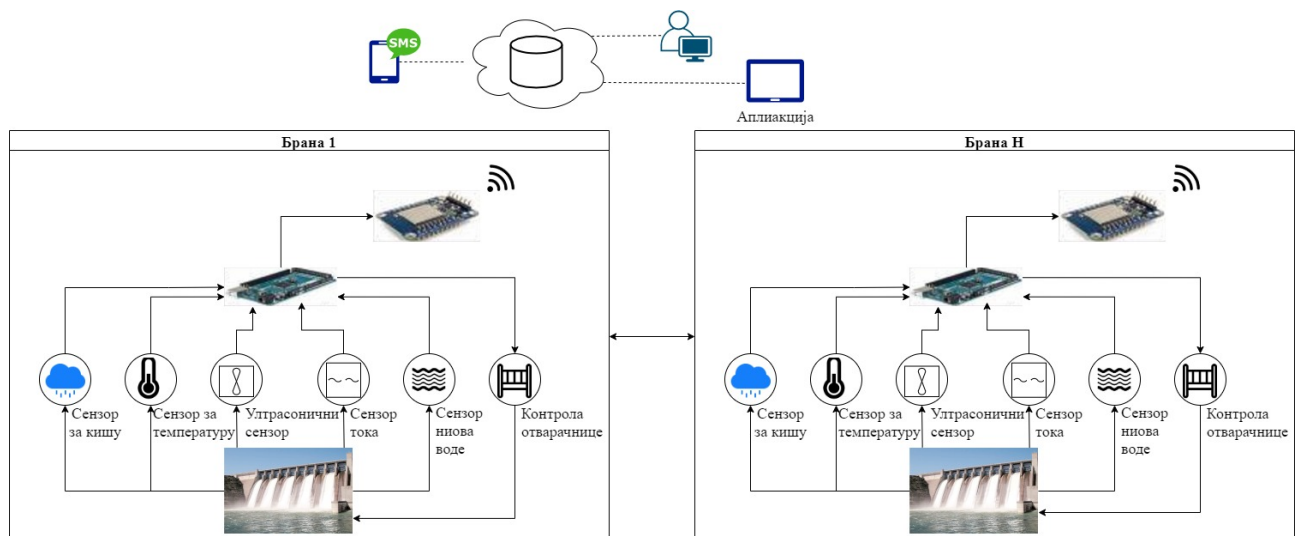
Слика 43. Дијаграм предложеног *RREW* модела [9]

*Sun* и други аутори, развили су систем за мониторинг и рано упозоравање на јаловишним бранама (у рудницима) под називом *Tailings Dam Monitoring and Pre-Alarm System (TDMPAS)* (Слика 44) [47]. *TDMPAS* је базиран на *IoT* технологијама и *cloud computing*-у. Систем има могућност праћења линије сатурације, загађеног водостаја и деформације бране.



Слика 44. TDMPAS систем [47]

У Индији се тренутно бране надгледају и контролишу мануелно [21]. Људски фактор може да повећа вероватноћу грешке, што резултира временским кашњењем у доношењу одлука. Varghese и други аутори предлажу увођење система који функционише у реалном времену, за надгледање и управљање катастрофама насипа базираног на IoT технологијама (*IoT based Disaster Monitoring and Management System for Dams – IDMMSD*). Систем се бави надгледањем нивоа воде који може да варира, зависно од промене водостаја река и језера, или због прекомерних падавина у речном сливу. Систем на основу измерених података управља евакуационим органима (уставе и темељни испусти) бране (отварање/затварање) и користи SMS за обавештавање становништва и државних институција. IDMMSD систем је приказан на следећој слици (Слика 45).



Слика 45. IoT модел осматрања бране [21]

*The Korea Water Resource Corporation (Kwater)* тренутно управља и одржава 30 брана у Кореји. *Jeon* и други аутори развили су систем за управљање сигурношћу брана (*Kwater's Dam Safety Management System – KDSMS*) [44]. KDSMS се састоји од података о бранама и акумулацијама, хидролошком информационом систему, картама терена и систему управљања подацима, мерним уређајима и мониторингу система (Слика 46). Мониторинг укључује мониторинг земљотреса, испитивање терена, процену безбедности и обједињени информациони систем.



Слика 46. KDSMS систем мониторинга брана [44]

Након бројних несрећа на бранама у последњих неколико година (*Way Ela* [151], *Zhouqu* [152], *SE Brazil* [153], итд.), људи су постали свесни колико је битан систем за управљање и мониторинг брана и да је потребно константно унапређивати га. Бројни су научни радови које се баве тематиком мониторинга. Унапређења која се односе на систем мониторинга базирана су или на софтверском унапређењу или применом неке иновативне технологије попут *IoT*-а. Велики број научника са истока користи јефтине хардверске компоненте (микроконтролере и микрорачунаре) у комбинацији са сензорима и труде се да их имплементирају и прилагоде постојећим системима, како би сачували екосистем и окружење које трпи велике последице због климатских промена.

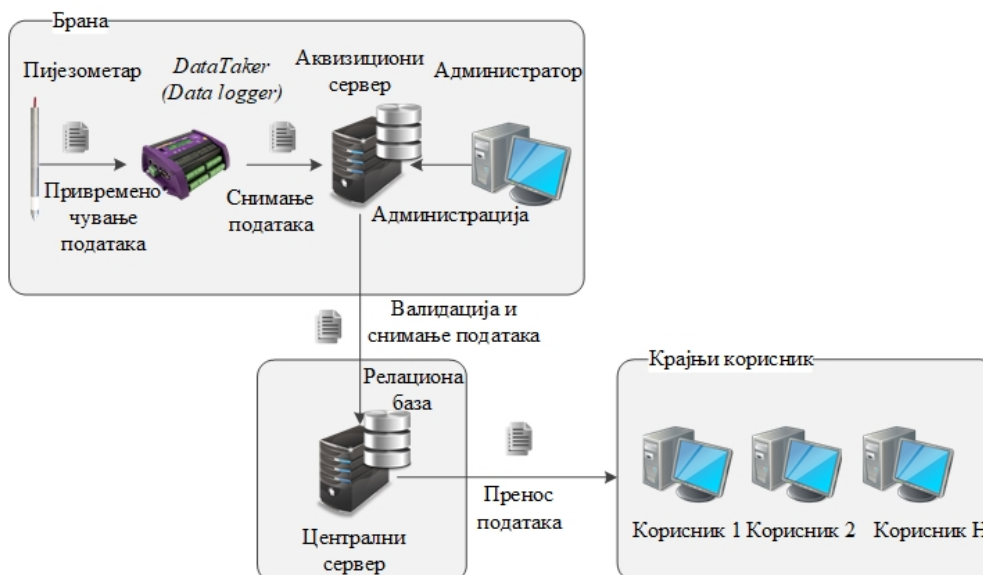
## 4.2 Модел осматрања брана у Србији

Надгледање бране укључује бројне типове мерних уређаја који врше различита мерења и чувају их у бази података [154]. Обрада података је такође значајна када су у питању кварови на бранама. Обрада података омогућава симулационим моделима да прогнозирају понашање бране, што у великој мери помаже процесу управљања бранама. Одређен број мерних уређаја, који се користе за мониторинг брана у Србији и њихова сврха, приказани су табеларно (Табела 5) [155].

Табела 5. Мерни уређаји

<b>Мерење</b>	<b>Уређај</b>
<b>Притисак подземних вода</b>	Пијезометар са манометром
	Даљински пијезометар
<b>Релативно померање бране</b>	Координометар
	Даљински координометар
<b>Промена нагиба бране</b>	Клинометар са вертикалном базом
	Клинометар са хоризонталном базом
	Даљински климометар
<b>Рад дилатационих спојница</b>	Деформетар
	Дилатометар
	Компаратер
<b>Температура ваздуха</b>	Термометар за ваздух
<b>Дилатација бетона</b>	Екстензометар
<b>Температура бетона</b>	Термометар за бетон
<b>Ниво воде</b>	Водомерна летва

У Србији постоје три начина прикупљања података на бранама: аутоматско, полуаутоматско и ручно. Аутоматско прикупљање података је организовано тако да измерени податак пролази цео процес аутоматизовано, од мерења, до складиштења у базу. Полуаутоматско прикупљање података користи се за проверу аутоматског прикупљања података, где је мерење аутоматизовано, а читавање мануелно. Ручно прикупљање података захтева присуство човека, јер се и мерење и читавање врши мануелно.

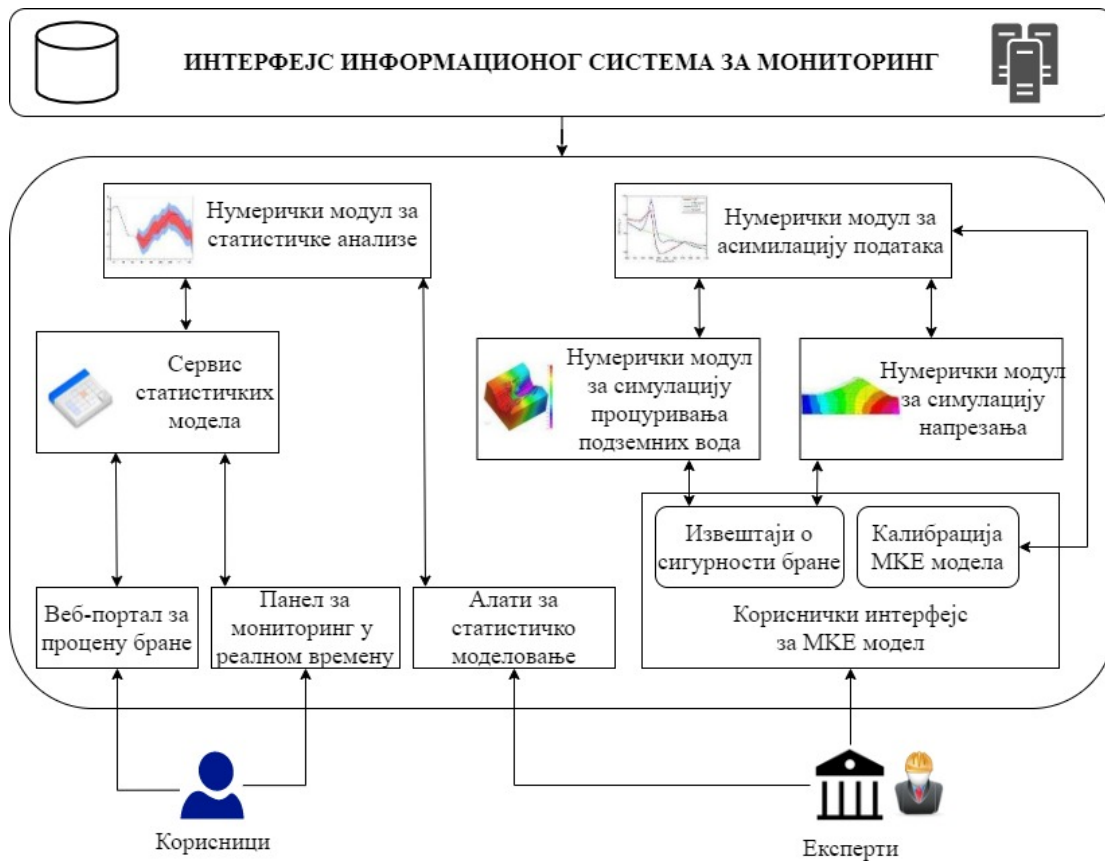


Слика 47. Дијаграм система за аутоматско прикупљање података

На претходној слици (Слика 47) приказана је функција пијезометра у аутоматском процесу прикупљања података. Пијезометар је уређај који мери ниво подземне воде, тј. притисак пијезометра. *Data logger* аутоматски прикупља податке користећи уграђени софтвер. Сервис аквизиције је компонента сачињена од хардвера и софтвера, чији је циљ прикупљање, валидација и припрема података. Након што су подаци преузети и валидирани од стране сервера за преузимање (аквизициони), централни сервер преузима валидиране податке и смешта их у базу података. Централни сервер је хардверско-софтверска компонента, чији је циљ координација, дистрибуција, синхронизација и чување података, као и управљање приступом подацима и сервисима. Информационо-комуникациони систем садржи централни сервер и на њега су повезани сви други елементи система. СУБ садржи само један централни сервер. Друга два модела прикупљања података биће приказана у даљем делу текста, јер су основа за развијени модел у дисертацији.

Архитектура информационог система за управљање сигурношћу брана, чији је саставни део развијени модел за мануелно техничко осматрање брана, приказана је на следећој слици (Слика 48). Софтвер за безбедност брана се састоји од следећих компоненти [18]:

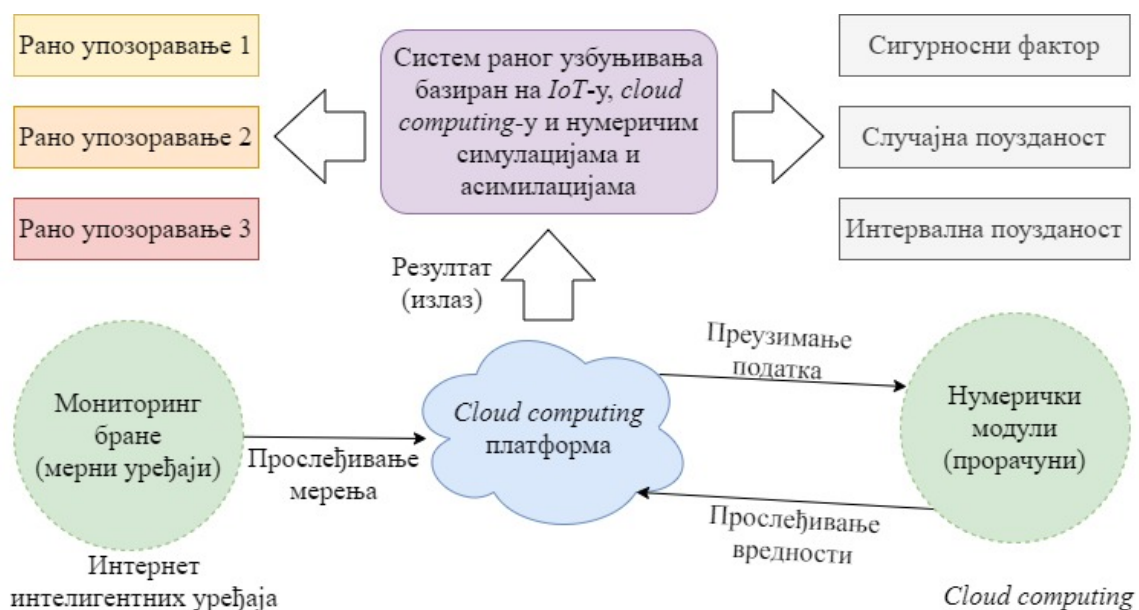
- интерфејс техничког мониторинга;
- нумерички модул за статистичке анализе;
- нумерички модул за симулацију процуривања подземних вода;
- нумерички модул за симулацију напрезања/истезања; и
- нумерички модул за асимилацију података и апликације.



Слика 48. Архитектура информационог система за управљање безбедношћу брана [18]

Апликације у информационом систему за управљање сигурношћу бране пројектоване су тако да омогуће корисницима визуелизацију података о мрежама у реалном времену и процену стања бране.

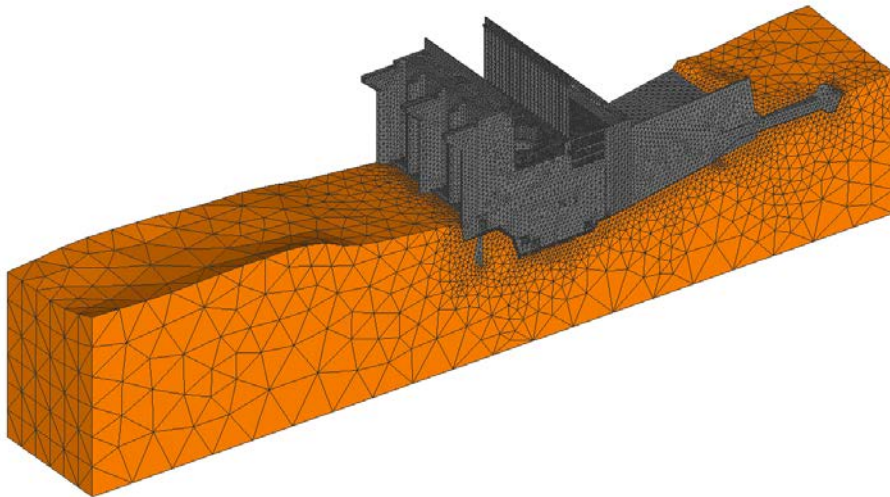
Општи систем раног узбуђивања у процесу осматрања брана, базиран на *cloud computing*-у и *IoT* технологијама, приказан је на слици 49. Систем тренутно није у потпуности развијен у Србији, већ се прилагођава одговарајућим проблемима. Тренутно се развија аутоматизовани систем, који ће бити могуће применити на различите случајеве кварова на брани.



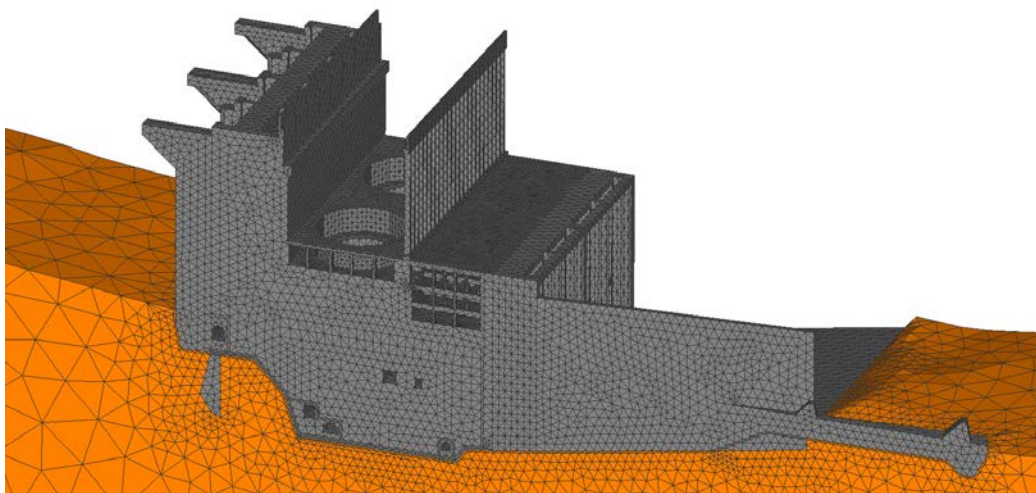
Слика 49. Систем раног узбуђивања базиран на *cloud computing*-у и *IoT*-у [156]



Мрежа коначних елемената (МКЕ) секције I бране ХЕ „Ђердап 1”, која је развијена у [157], приказана је на следеће две слике (Слика 50 и Слика 51). МКЕ је нумеричка метода за решавање диференцијалних једначина којом се описују физички феномени у различитим областима инжењерства (машинство, грађевинарство, електротехника, итд.) [158]. Модел коначних елемената формиран је на основу тродимензионалног геометријског модела бране и омогућава израчунавање напона и деформације у било којој тачки бране. Ови модели се користе да би се проверила сигурност бране у одређеним тачкама мреже.



Слика 50. МКЕ мрежа секције I бране ХЕ „Ђердап 1” [157]



Слика 51. МКЕ мрежа секције I бране ХЕ „Ђердап 1” [157]

### 4.3 Модел система за управљање безбедношћу брана у Србији

Модел система за управљање безбедношћу брана обухвата: структуру модела СУБ-а, систем техничког мониторинга, процес мануелне аквизиције, модел података, дијаграм класа, слојеви архитектуре СУБ-а заснованог на *IoT*-у, вишеслојни модел структуре СУБ-а, концептуални модел интеграције мануелног техничког осматрања брана са *IoT*-ом, дијаграм система мануелног техничког осматрања, систем валидације података.

За потребе пројекта унапређења мониторинга брана, развијена је инфраструктура модела техничког осматрања брана заснованог на *IoT* технологијама.

Архитектура система за управљање безбедношћу брана се састоји од [12]:

- система за мерење и прикупљање података;
- аквизиционог сервера;
- централног сервера базе података;
- корисничког подсистема за анализу података и управљање прорачунима;
- централног прорачунског сервера и администраторских алата.

Систем за мерење и прикупљање података састоји се од: опреме и уређаја за мерење и аквизицију, службе осматрања, и опреме и софтвера за привремено складиштење. Саставни делови аквизиционог сервера су: слој за пријем и валидацију података, *ETL (Extract, Transform, Load)* и слој са подацима. У централном серверу базе података налази се слој са подацима. Кориснички подсистем за анализу података и управљање прорачунима задужен је за корисничке алате. Софтверски систем за анализу сигурности главни је елемент централног прорачунског сервера.

Модел система за управљање безбедношћу брана приказан је на следећој слици (Слика 52).



Слика 52. Структура модела система за управљање безбедношћу брана [159]

Систем за мерење и прикупљање података омогућава физичку реализацију осматрања бране, што подразумева мерење и прикупљање низа релевантних података (показатеља), који могу да покажу да ли је стварно стање бране у експлоатацији у сагласности са предвиђеним понашањем бране у експлоатацији.





Слика 53. Систем техничког мониторинга [1]

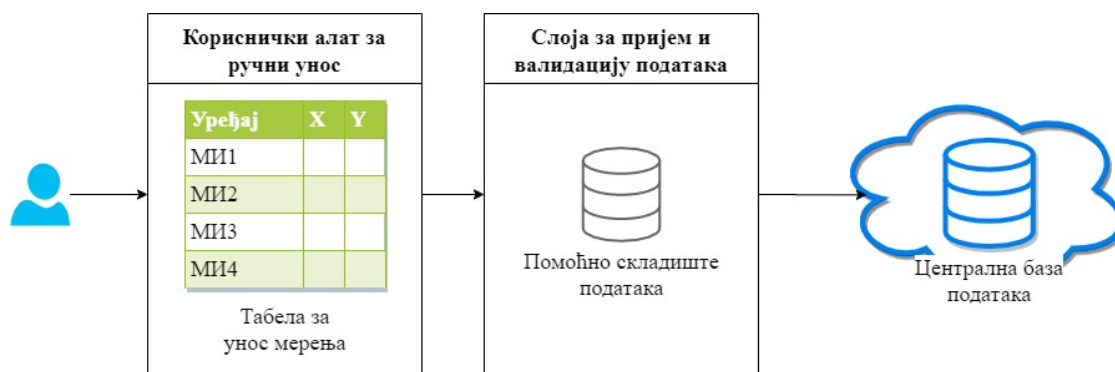
Процес техничког мониторинга на брани, који је саставни део процеса управљања браном, приказан је на претходној слици (Слика 53). Циљ мониторинга је да се омогући да се на једном месту прикупе различити подаци из целокупног система техничког осматрања, поседовање оцена поузданости тих података, као и да пристап свим подацима буде једноставан, интерактиван и брз.

Систем за мерење и прикупљање се састоји од опреме и уређаја за мерење и аквизицију, као и опреме и софтвера за привремено складиштење података. Опрему и уређаје за мерење и аквизицију представљају различити типови мерних инструмената, од инструмената са потпуно аутоматизованим поступком мерења, читавања и преноса података, до инструмената са мануелним читавањем који захтевају накнадни ручни унос података мерења. Мануелни технички мониторинг је саставни део система за мерење и прикупљање података, и бави се мануелним прикупљањем података.

Опрема и уређаји за мерење и аквизицију се састоје од:

- мерних инструмената за аутоматска мерења и аутоматску аквизицију;
- опреме и уређаја за аутоматски пренос;
- мерних инструмената за аутоматска мерења и мануелну аквизицију;
- мерних инструмената за мануелна мерења и мануелну аквизицију;
- преносних уређаја за мануелну аквизицију;
- *RFID* таг;
- *Bluetooth* модул.

Процес мануелне аквизиције података од стране особља задуженог за мониторинг на брани, приказан је на слици испод (Слика 54).



Слика 54. Процес мануелног прикупљања података (мануелна аквизиција) [13]

У даљем тексту описани су елементи СУБ-а, који су детаљно приказани у литератури [159].

Опрема и софтвери за привремено складиштење имају задатак да прихвате све податке мерења, како оне који потичу из аутоматског процеса аквизиције, тако и оне који су ручно забележени.

Аквизициони сервер се састоји од хардверских и софтверских делова повезаних у једну целину. Циљ аквизиционог сервера је да податке који се привремено складиште у систему за мерење и прикупљање података преузме, валидује и припреми за слање на централни сервер базе података СУБ-а. Састоји се од слоја за пријем и валидацију података и слоја са подацима.

Централни сервер се састоји од хардверских и софтверских компоненти повезаних у јединствену целину. Циљ је да се омогући управљање и приступ подацима и сервисима корисницима. Централни сервер представља главни елемент информационо-комуникационе инфраструктуре система. Сви други елементи система су повезани и комуницирају са централним сервером.

Централни прорачунски сервер се састоји од хардверских и софтверских елемената ради обезбеђивања инфраструктуре потребне за коришћење математичких модела у процесу праћења и анализе сигурности објеката бране.

Кориснички алати су саставни део корисничког подсистема за анализу података. Ови алати користе се за претрагу, преузимање и анализу историјских података и података у реалном времену.

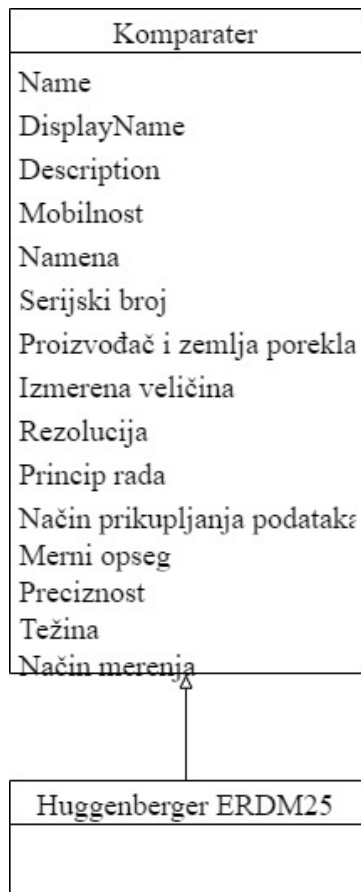
Администраторски алати користе се за потребе одржавања базе података и управљање радом система. Приступ овим подацима омогућен је корисницима система са администраторским правима.

У даљем тексту приказани су табеларно поједностављени модел података и дијаграм класа за два мерна уређаја. Опширнији приказ неће бити презентован у дисертацији због компанијске политике заштите података. Модели података за мерне уређаје, компаратер и механички дилатометар, приказани су табеларно (Табела 6 и Табела 7). Дијаграми класа за поменуте мерне уређаје приказани су на следеће две слике (Слика 55 и Слика 56).

Табела 6. Модел компаратер

Назив	Тип података	Ограничење	Подразумевана вредност
<i>Name</i>	<i>String</i>		
<i>DisplayName</i>	<i>String</i>		
<i>Description</i>	<i>String</i>		

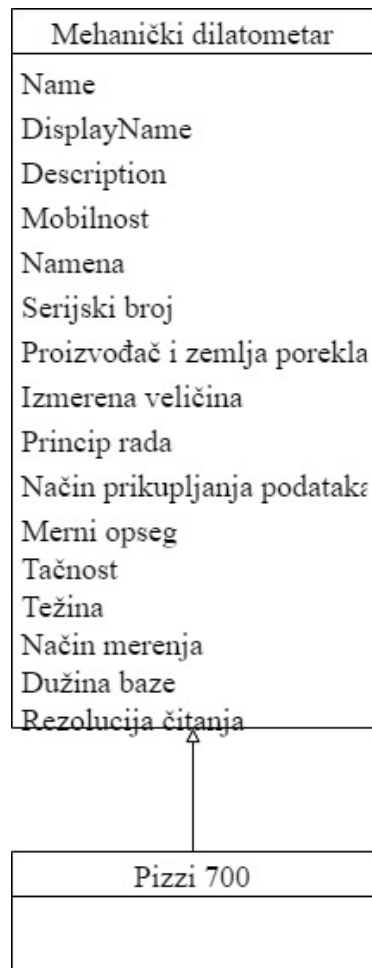
Назив	Тип података	Ограничење	Подразумевана вредност
Mobilnost	SingleSelect	Rečnik	Prenosni
Namena	String		Praćenje rada dilatacionih spojnica ili prslina
Serijski broj	String		
Proizvođač i zemlja porekla	SingleSelect	Rečnik	Huggenberger – Švajcarska
Izmerena veličina	String		Rastojanje para repera uz dilatacionu spojnicu ili prslinu
Rezolucija	Double		0,01
Princip rada	MultiSelect	Rečnik	Mehanički
Način prikupljanja podataka	MultiSelect	Rečnik	Manuelno
Merni opseg	Interval		[0;25]
Preciznost	Double		0,02
Težina	Double		0,4
Način merenja	MultiSelect	Rečnik	Manuelno



Слика 55. Дијаграм класа за модел компаратер

Табела 7. Модел механички дилатометар

Назив	Тип података	Ограничење	Подразумевана вредност
<i>Name</i>	<i>String</i>		
<i>DisplayName</i>	<i>String</i>		
<i>Description</i>	<i>String</i>		
<b>Mobilnost</b>	<i>SingleSelect</i>	Rečnik	Prenosni
<b>Namena</b>	<i>String</i>		Praćenje rada dilatacionih spojnicu ili prslina
<b>Serijski broj</b>	<i>String</i>		
<b>Proizvođač i zemlja porekla</b>	<i>SingleSelect</i>	Rečnik	Pizzi – Italija
<b>Izmerena veličina</b>	<i>String</i>		Rastojanje para repera uz dilatacionu spojnicu ili prslinu
<b>Princip rada</b>	<i>MultiSelect</i>	Rečnik	Mehanički
<b>Način prikupljanja podataka</b>	<i>MultiSelect</i>	Rečnik	Manuelno
<b>Merni opseg</b>	Interval		(0;5)
<b>Tačnost</b>	<i>Double</i>		0,002
<b>Težina</b>	<i>Double</i>		3,1
<b>Način merenja</b>	<i>MultiSelect</i>	Rečnik	Manuelno
<b>Dužina baze</b>	<i>Double</i>		700
<b>Rezolucija čitanja</b>	<i>Double</i>		0,01



Слика 56. Дијаграм класа за модел механички дилатометар

#### 4.3.1 Слојеви у моделу система за управљање безбедношћу брана

Инфраструктура система за управљање сигурношћу брана, заснована на примени *IoT* технологије, обухвата шест слојева: слој уређаја, гејтвеј, платформа аквизиционог сервера, платформа централног сервера, слој сервиса и апликативни слој.

Слојеви архитектуре система за управљање безбедношћу брана приказани су на следећој слици (Слика 57). Слој уређаја чине: мерни уређаји (пијезометар са манометром, даљински пијезометар, координометар, даљински координометар, клинометар, итд.), *RFID* тагови и *Bluetooth* модули. Слој уређаја је полазна тачка система, одакле потичу мерни подаци. Подаци се складиште у локалним складиштима (*data logger*) привезаним за мерне уређаје или их оператер повлачи на *RFID* мобилни уређај (*PDA*). *RFID* омогућава прикупљање и дистрибуцију података са мерних уређаја.



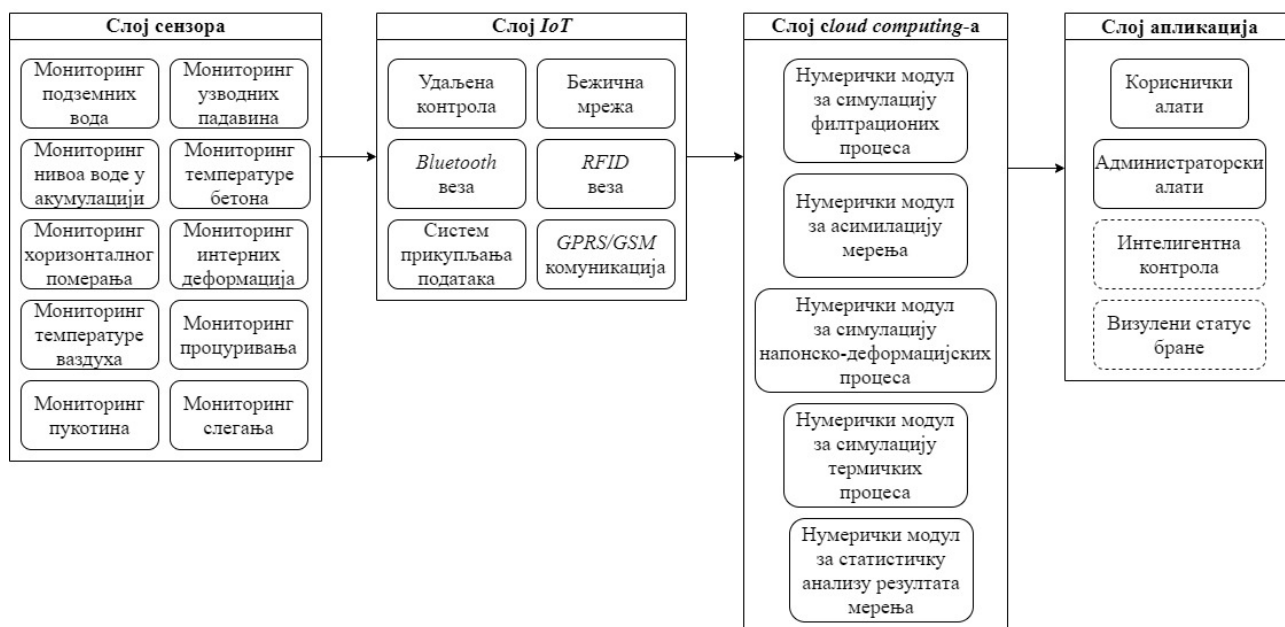
Слика 57. Слојеви у архитектури система за управљање безбедношћу брана, заснованог на *IoT*-у

Подаци се путем гејтвеја прослеђују до платформе (аквизиционог сервера), која за циљ има валидацију и привремено складиштење података, одакле се путем интернет везе врши пренос података до следеће платформе (централног сервера).

Инфраструктура *cloud computing*-а обезбеђује рачунарске ресурсе неопходне за развој и извршавање сервиса и складиштење података. Оваква инфраструктура омогућава доступност, скалабилност, поузданост и брз приступ сервисима.

Апликативни слој се налази на врху вишеслојне архитектуре. Апликативни слој представљају апликације (администраторски и кориснички алати), што представља интерфејс корисника. Интерфејсу приступају стручњаци који се баве сигурношћу брана и овлашћене институције. Наведени корисници различито су ауторизовани, па немају иста права приступа апликацијама. Корисници су подељени у две групе: корисници који имају права прегледа и анализирања података и администратори апликација који формирају базу и мењају садржај података апликације.

Вишеслојни модел инфраструктуре СУБ-а приказан је на следећој слици (Слика 58). Структура се састоји од четири слоја: слој сензора, слој *IoT*-а, слој *cloud computing*-а и слој апликација. У слоју *cloud computing*-а се налазе разни модули који врше прорачуне за бране на основу којих се одређује сигурност бране.

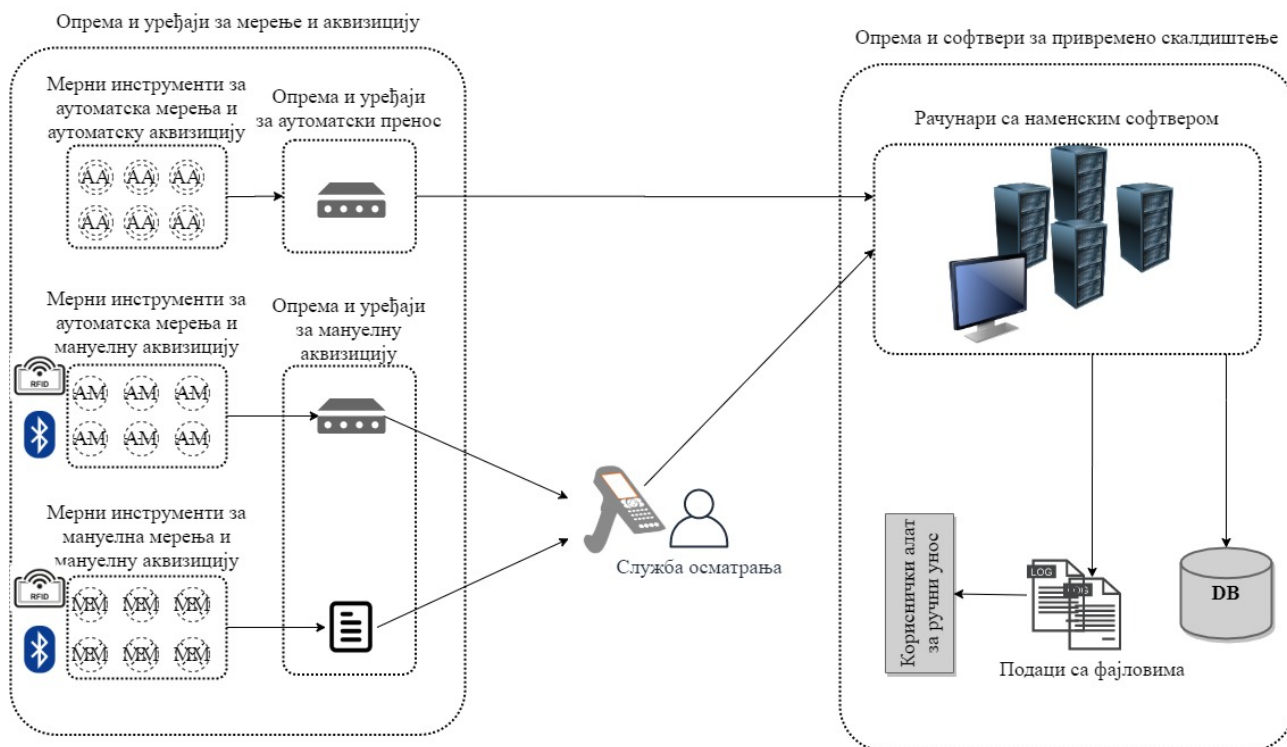


Слика 58. Вишеслојни модел инфраструктуре система за управљање безбедношћу брана, заснованог на *IoT*-у [156]

#### 4.3.2 Интеграција *IoT*-а у мануелном техничком осматрању брана

Имплементација *RFID* и *Bluetooth* технологија у процесу мануелног техничког осматрања брана омогућила је смањења фактора људске грешке. Нове технологије омогућиле су аутоматизована читавања и бележења података са мерног инструмента. На следећој слици (Слика 59) приказан је концептуални модел техничког осматрања бране.





Слика 59. Концептуални модел интеграције система мануелног техничког осматрања брана са *IoT* технологијом [13]

Предложени концептуални модел комуникације између мерних уређаја и *RFID* и *Bluetooth* технологија је интероперабилан. Концептуални модел се може применити на било које мануелно техничко осматрање, и на било који мерни уређај осматрања, уколико је изводљиво на самом уређају повезивање са *Bluetooth* модулом, тј. уколико постоји комуникациони порт. Уколико мерни уређај већ поседује у себи *Bluetooth* порт, довољно је модификовати (прилагодити) табеле за прикупљање података одговарајућем уређају, тј. формирати табелу према параметрима које мерни уређај мери. *ID RFID* таг је записан у бази и повезан са *ID*-ем мерног места. Због тога је једноставним изменама *ID*-ева и назива мерног места у бази могуће прилагодити базу новој ситуацији. Неке од могућих примена развијеног модела техничког осматрања су мостови, зграде, речна корита итд. На мостовима се користе дилатационе спојнице, као и на бранама, па су промене мале. На грађевинама се мери нагиб неког објекта, што је случај и са бранама, па су промене такође минималне. На речним токовима могуће је користити модел за мерење нивоа воде, јер се ниво воде осматра и на речним токовима и на акумулацијама на бранама.

Комуникација *RFID* читача са мерним уређајем одвија се преко екстерног *Bluetooth* модула који је са мерним уређајем повезан преко комуникационог порта (Слика 60). *RFID* читач садржи *Bluetooth* у свом хардверу. Повезивањем две стране путем *Bluetooth* везе омогућава се трансфер података са мерног уређаја у привремену меморију *RFID* читача.

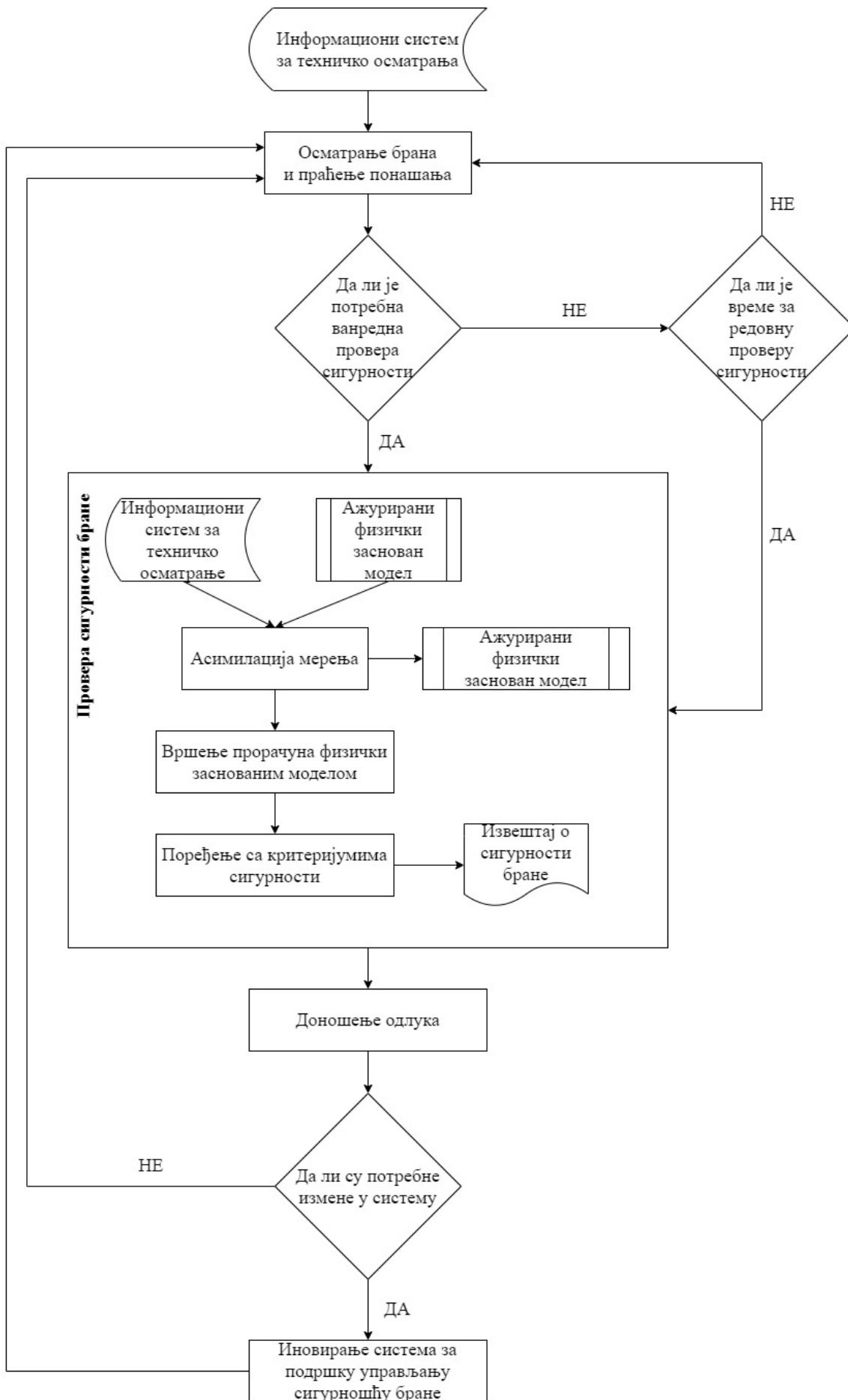


Слика 60. Концептуални модел комуникације између мерних уређаја и *RFID* технологије

#### 4.3.3 Управљање процесима у СУБ-у

Провера сигурности брана у СУБ-у врши се периодично (годишње) или по потреби [1]. Редовна годишња контрола бране је обавезна, док се периодична врши у екстремним ситуацијама, када постоји могућност нарушавања бране (нпр. поплаве, земљотреси). Циљ осматрања и праћења понашања бране је утврђивање потребе да се преиспита стање система уколико нека мерења почну битно да одступају од очекиваних. Узрок одступања може бити и у систему техничког осматрања. Поступак се ослања на успостављене статистичке моделе, који на основу мерених улаза могу дати очекивану вредност неке величине.

Дијаграм одлучивања о сигурности бране приказан је на слици која следи (Слика 61).



Слика 61. Контрола сигурности бране [1]

## 5. ИМПЛЕМЕНТАЦИЈА И ПРИМЕНА РАЗВИЈЕНОГ МОДЕЛА

### 5.1 Пројектни задатак

Са циљем унапређења техничког осматрања на брани, неопходно је имплементирати *IoT* систем и пројектовати софтвер који ће олакшати мануелно техничко осматрање.

За мерна места на којима се врше мерења помоћу мануелних клинометара (за праћење промене нагиба) и компаратера (за праћење рада спојница и прслина) потребно је извршити набавку и уградњу *RFID* тагова.

Потребно је набавити одговарајуће *RFID* читаче и преносне уређаје (таблет или преносни рачунар) на којима ће се извршавати кориснички алат за ручни унос система за управљање безбедношћу бране ХЕ „Бердап 1”. Потребно је дефинисати јасне процедуре коришћења нове опреме.

Потребно је израдити функционалне маске (шаблоне) за ручни унос:

- очитаних вредности мерења помоћу мануелних клинометара са хоризонталном и вертикалном базом (за праћење промене нагиба); и
- очитаних вредности мерења помоћу компаратера (за праћење рада спојница и прслина).

Тамо где је потребно, маске прилагодити раду на преносним уређајима у условима без постојања сталне везе или интернет везе са аквизиционим сервером.

### 5.2 Хардверско-софтверска архитектура

Управљање сигурношћу брана реализује се успостављањем, одржавањем и коришћењем система за управљање безбедношћу, који чине следећи елементи: систем за мерење и прикупљање података, аквизициони сервер, централни сервер базе података, централни прорачунски сервер, кориснички подсистем за анализу података и управљање прорачунима, и администраторски алати [12].

Систему за управљање безбедношћу брана, а ради коришћења и одржавања, може приступити шири круг обученог и стручног особља. Систем предвиђа управљање правима приступа на нивоу улога, као и на нивоу појединачних корисника. Основне улоге у СУБ-у су [12]:

- корисник (анализира мерене податке);
- служба осматрања (мануелно прикупља податке);
- овлашћена институција (прати и анализира сигурност брана и припадајућих објеката);
- администратор (ажурира садржај базе података и управља правима приступа).

Прикупљање података на бранама врши се помоћу мерних инструментима за аутоматска мерења и аутоматску аквизицију, мерних инструмената за аутоматска мерења и мануелну аквизицију, и мерних инструмената за мануелно прикупљање података и мануелну аквизицију.

Први тип мерења и аквизиције је потпуно аутоматизован и измерени податак се смешта у базу без учешћа човека. Мерење са мерним инструментима за аутоматска мерења и мануелну аквизицију представља проверу мерења са мерним инструментима за аутоматска мерења и аутоматску аквизицију. Осматрач излази на терен и мануелно сакупља податке. Након тога, осматрач одлази у командно-контролни центар и забележене податке уноси у софтвер, где се врши упоређивање података и могућа одступања у мерењима.

У првом начину мерења аутоматски се пребацују подаци са инструмента до рачунара помоћу опреме за аутоматски пренос података, док за други и трећи начин мерења осматрач мора бити присутан.

У дисертацији је описан развијени унапређени модел прикупљања података, који се врши помоћу мерних инструмената за мануелно осматрање и мануелну аквизицију.

Употреба *cloud computing*-а у техничком осматрању брана и процес синхронизације података између аквизиционог сервера, који се налази на брани, и централног сервера, који се налази ван бране у *cloud*-у, приказани су на следећој слици (Слика 62). *Cloud* омогућава крајњим корисницима употребу ресурса сервера за анализирање података, који је много веће процесорске моћи и ресурса од корисничких рачунара. Овај приступ омогућава крајњим корисницима приступ апликацијама које се извршавају на централном серверу било кад, и било где. Апликације које се извршавају на централном серверу покрећу се у оквиру виртуелних машина.



Слика 62. Употреба *cloud computing*-а на брани

### 5.3 Имплементација развијеног СУБ модела

Мануелно техничко осматрање брана један је од главних начина мониторинга, у који је потребно укључити људе. Мењање мерних уређаја којима људи ручно управљају је скупо. Такође, на неким местима немогуће је заменити мануелни аутоматским уређајем, јер је неопходна визуелна провера. Да би експерт разумео резултате мерења, треба да има увид у место мерења, јер резултат који показује мерни уређај није довољан. Досадашњи уређаји показали су се поузданим, а мерења прецизна, због чега се уређаји неће мењати у скорије време. Осим финансијских ограничења, постоје и ограничења која се односе на окружење у коме се врше мерења – влаге, температуре, светла, итд. Због тога је неопходно да уређаји буду отпорни, поуздани и јефтине. У пројекту је одабрана *RFID* технологија јер има широку примену у индустрији, где је потребно означавање, робусна је, модерна, брза и може да удовољи захтевима по прихватљивим ценама.

Када се врши мануелно техничко осматрање бране, неопходно је да запослени изађе на терен, чита вредности на уређају и забележи ове податке. Подаци се касније снимају у базу података, јер на брани нема интернета. Пре имплементације развијеног модела техничког осматрања бране базираног на *RFID* технологији, запослени су читавали податке и бележили мерења на папиру на коме су одштампане табеле са називима мерних места и уређаја. Када запослени чита сва мерења на различитим уређајима, одлази у канцеларију и уноси податке у апликацију која је повезана на интернет.

На следећој слици (Слика 63) приказано је мануелно техничко осматрање бране. При таквом осматрању могу се јавити следеће грешке: нечитљива етикета на месту мерења, погрешно изабран папир за унос података, погрешно поље за уписивање података, погрешно читавање података, нетачан унос и снимање података у апликацију.



Слика 63. Дијаграм систем мануелног техничког осматрања брана

Имплементација развијеног модела за техничко осматрање састоји се од три фазе. Прва фаза је имплементација *RFID* технологије (препознавање уређаја), друга фаза је имплементација *Bluetooth*-а (пренос података), а трећа фаза је примена *Beacon*-а, као посебне врсте *RFID* активних тагова (са сензором за прикупљање података из окружења). Прве две фазе су успешно изведене и користе се на брани ХЕ „Ђердап 1”. У току је имплементација развијеног модела мануелног техничког осматрања на брани ХЕ „Ђердап 2”. На следеће две слике приказане су прва (Слика 64) и друга фаза (Слика 65) примене унапређеног модела система мануелног техничког осматрања (имплементирано решење на брани ХЕ „Ђердап 1”). На мерном месту поред сваког уређаја инсталиран је пасивни *RFID* таг. Свака ознака има свој јединствени *ID*. Веза између мерног места и ознаке записана је у бази података. Пошто мерни уређај који се користи нема *Bluetooth*, поред уређаја је инсталиран спољни *Bluetooth* модул који је повезан са мерним уређајем. Модул и мерни уређај комуницирају преко *RS485* порта.



Слика 64. Дијаграм систем мануелног техничког осматрања брана (фаза 1)





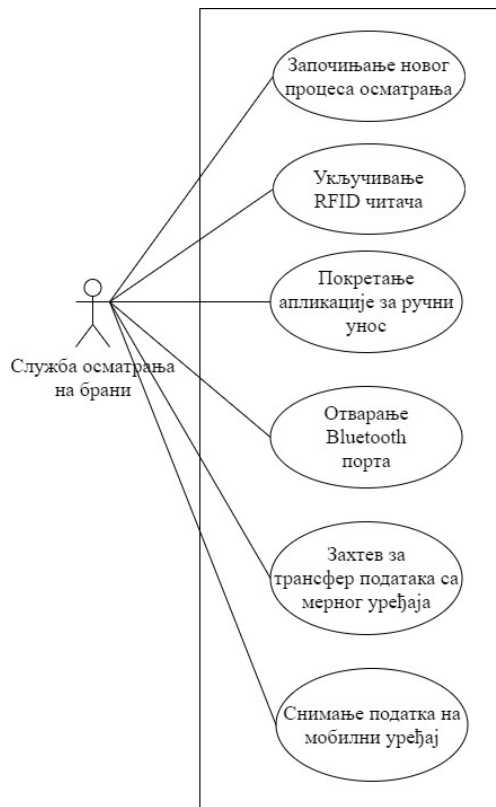
Слика 65. Унапређени модел система осматрања брана (фаза 2)

Након очитавања тага, *RFID* читач (*PDA*) покреће апликацију са маском (табела) за унос података [160]. Кликот на дугме корисник у апликацији покреће захтев за пренос података са препознатог мерног уређаја. Након тога се отвара *Bluetooth* порт и почиње пренос података са мерног уређаја на *PDA*. Након престанка преноса података, унете вредности привремено се чувају у меморији *RFID* читача. Поступак преузимања података са мерног уређаја приказан је на следеће две слике помоћу дијаграма случајева коришћења (Слика 66) и дијаграма секвенци (Слика 67).

Након мониторинга свих мерних уређаја, корисник одлази у контролно-командни центар (ККЦ) где повезује *RFID* читач са радном станицом администратора (кабл или *WiFi*). *Windows Mobile Device Centre* [161] омогућава кориснику да инсталира управљачке програме уређаја и преноси податке са *RFID* читача на рачунар. Након преноса података врши се синхронизација између рачунара и аквизиционог сервера. У овој фази имплементације, развијени модел је реализован само за *Windows* уређаје, што се може сматрати недостатком овог пројекта.

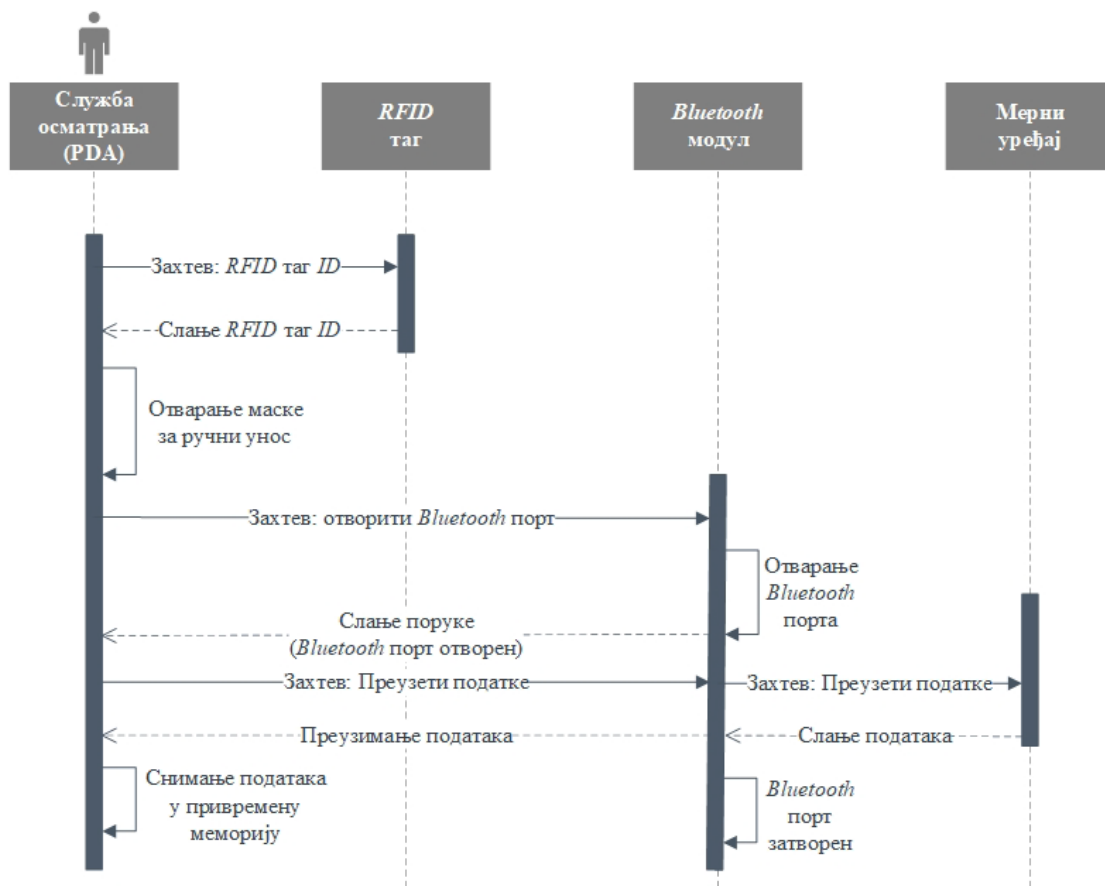
На следећој слици (Слика 66) приказан је дијаграм случајева коришћења (*use-case diagram*). Случајеви коришћења, који представљају главну функционалност осматрача су: започињање новог процеса осматрања, укључивање *RFID* читача, покретање апликације за ручни унос, отварање *Bluetooth* порта, захтев за трансфер података са мерног уређаја, снимање података на мобилни уређај.





Слика 66. Дијаграм случајева коришћења службе осматрања

На следећој слици (Слика 67) представљен је дијаграм секвенци развијеног модела мануелног техничког осматрања, заснован на *RFID* и *Bluetooth* технологијама.



Слика 67. Дијаграм секвенци мануелног техничког осматрања, заснован на *RFID* и *Bluetooth* технологијама

Интеграција прве и друге фазе елиминише могућност људске грешке, чинећи грешку у читању података минималном. Посматрач на мерном месту више не пише податке на папир. Такође, оператер у ККЦ-у не прекуцава записане податке на рачунар. Ово решење чини податке аутентичнијим и процес мануелног техничког осматрања бржим. Може се рећи да нема простора за грешке људског фактора. Овом надоградњом подаци постају поузданији, јер једина грешка која се може догодити, јесте квар уређаја. Ова врста грешке и уклањање нетачних података биће детаљно објашњено у наредним поглављима.

## 6. ЕВАЛУАЦИЈА МОДЕЛА

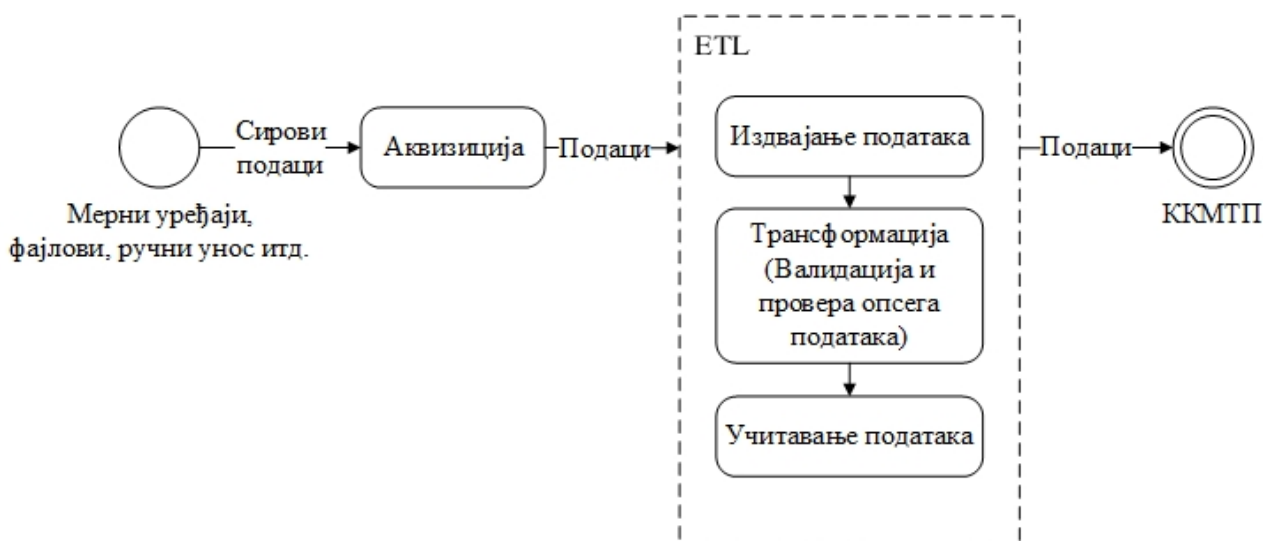
Реализацијом развијеног решења на једној великој брани у Србији, ова дисертација покушава да реши следећа истраживачка питања:

1. Да ли употреба *RFID*-а и *Bluetooth*-а у процесу мануелног техничког осматрања побољшава процес праћења брана?
2. Да ли *RFID* и *Bluetooth* у процесу праћења брана пружају поузданије податке од мануелног читања података?
3. Које информације, прикупљене *RFID*-ом и *Bluetooth*-ом, могу да се користе за контролу квалитета мерених техничких података?
4. Како употреба *RFID*-а и *Bluetooth*-а утиче на ефикасност и продуктивност запослених на брани?

Евалуација развијеног модела укључује два кључна дела: тестирање успешности имплементације *RFID* технологије и анкете запослених. Провера успеха примене *RFID* технологије огледа се у анализи серија измерених података. Серије које се анализирају су оне пре и после уградње *RFID* технологије и добијају оцену квалитета. Упоредна анализа броја грешака утврђује да ли је побољшани модел ефикаснији од претходног. Анкетирање запослених врши се коришћењем специјализованих модела истраживања који омогућавају боље разумевање утицаја *RFID* технологија на рад запослених.

### 6.1 Контрола квалитета мерених техничких података

Систем контроле квалитета мерених техничких података је важан део целокупног информационог система за управљање бранама. ККМТП директно доприноси поузданости извршених анализа на основу измерених података [13]. ККМТП се састоји од два дела: валидације података и контроле квалитета мерених техничких података (Слика 68). ККМТП је базиран на више претпоставки, а битније су дате у наставку: сваки податак састоји се од измерене вредности и придружених атрибута (мерење, мерно место и мерни уређај), након примене ККМТП, подацима се додељује оцена квалитета од 0 до 1, ККМТП систем се формира за сваку серију појединачно коришћењем математичко-статистичких модела, математичко-статистички модели ККМТП оцењују један аспект квалитета података и коначна оцена квалитета података формулише се обједињавањем више аспеката квалитета података.



Слика 68. Систем валидације података [13]

ККМТП процес може се покренути и *online* и *offline* аутоматски, или га покреће стручњак. Контрола квалитета мерених техничких података врши се на два начина: евалуацијом података

из аквизиције (*Online quality control of measured technical data*) и евалуацијом архивских података (*Offline quality control of measured technical data*).

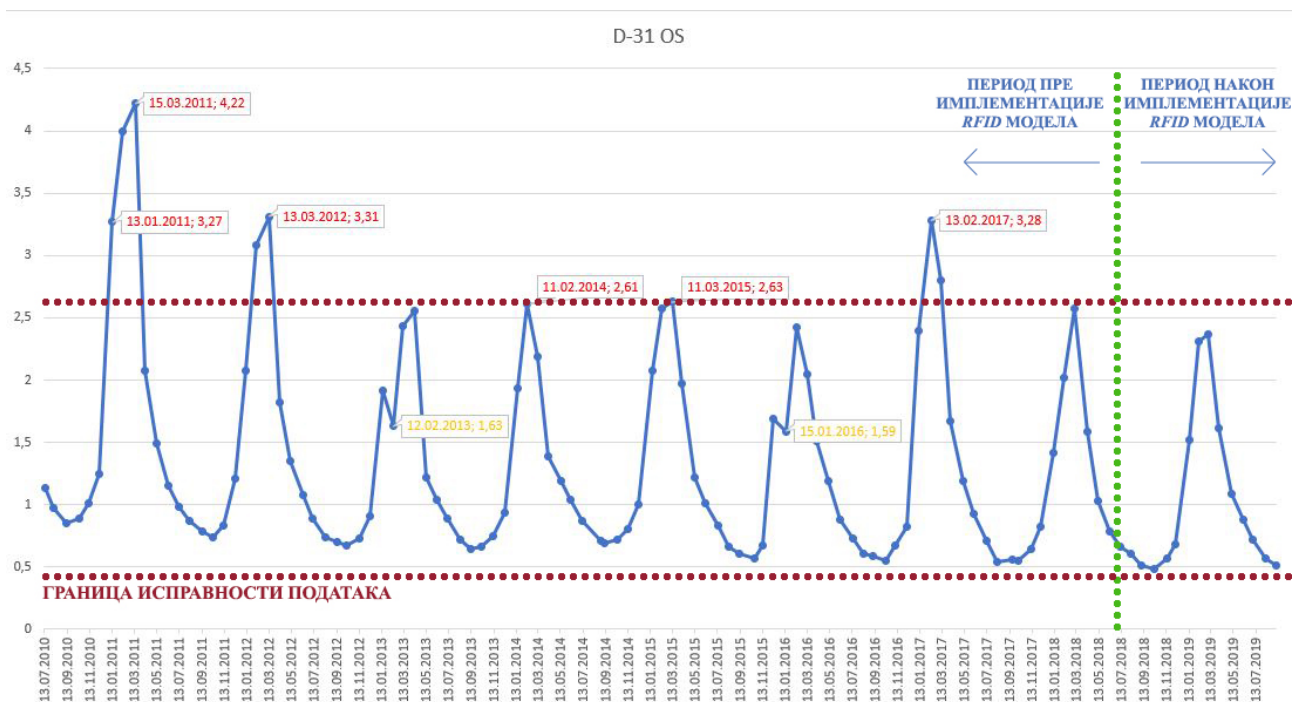
*Online* контрола квалитета мерених техничких података врши се након процеса прикупљања података (и система валидације), а пре уноса података у централну базу података са свим придодатим атрибутима. За разлику од *online* процене, приликом процене архивских података доступни су и сви остали историјски подаци. Ова чињеница знатно повећава могућности процене квалитета података, јер се подаци могу упоредити са једним или више мерења, како из прошлости, тако и из будућности, чинећи процену поузданијом.

## 6.2 Процена квалитета података

Мерење деформација високих грађевина, брана и хидроелектрана, врши се ради обезбеђивања могућих изненадних и непредвидивих појава (оштећења), са циљем заштите животне средине и низводног подручја од катастрофа. Прикупљање потребних података врши се геодетско-техничким надгледањем најпрецизнијих геодетских мерења, ради рационалног одржавања високих грађевина [162].

Геодетска мерења померања обухватају сва мерења за утврђивање промене облика грађевине или тла под утицајем спољних или унутрашњих сила. Објекат се идеализује одређеним бројем тачака, при чему се положај одређује у односу на референтну или основну геодетску базу изван подручја могућих помака [163].

На брани ХЕ „Ђердап 1”, развијени модел са *RFID* и *Bluetooth* технологијама примењен је на неколико врста мерних уређаја: деформетри, дилатометри, координометри, клинометри, манометри и пијезометри. Резултати дилатометара (компаратера) су приказани у дисертацији. Неопходно је да прикупљене податке обради стручњак да би открио и обележио погрешне податке, уклонио их и заменио интерполираним подацима. Генерално, први корак у откривању погрешних података са аномалијама назива се процена квалитета или валидација података [164]. У следећим примерима подаци су процењени ручно (*offline*) на основу историјских података, посматрајући период од 10 година и више. Посматрани период у коме су подаци анализирани и упоређивани је период од 12 месеци (од 1. јула), пошто су *RFID* и *Bluetooth* технологије инсталиране у јулу 2018. Подаци, који су измерени дилатометром (компаратером) *D-31*, на брани ХЕ „Ђердап 1” приказани су на следећој слици (Слика 69). Подаци су мерени на отворима спојница, од јула 2010. године, до јула 2019. Дилатометри (Слика 70) мере померање спојница на брани у три смера: горе-доле, напред-назад и лево-десно. Рад спојнице се односи на период од почетка осматрања спојница, у почетку дилатометром *Pizzi*, а касније компаратером *Huggenberger* (Слика 71). Компаратер са дигиталним дисплејом користи се за праћење рада дилатационих спојница или прлина. Мерење се обавља постављањем инструмента на одговарајуће ослонце. Мерна величина је рад спојнице (отварање/затварање – *OS*), а мерна јединица *mm*.



Слика 69. Историјски подаци дилатометра *D-31* пре и после имплементације новог модела осматрања

Постоје три врсте података који се уносе у базу података: исправни, прихватљиви и неважећи подаци. Исправни подаци су они који улазе у предвиђени опсег мерења уређаја. Прихватљиви подаци улазе у предвиђени опсег мерења уређаја, уз мање грешке приликом читања или снимања вредности (нпр. пермутација броја), тако да дијаграм има мали скок или пад. Неважећи или неприхватљиви подаци појављују се изван предвиђеног распона мерења (нпр. неисправни уређај). Неважећи подаци се неће користити у анализи. На претходној слици (Слика 69) приказан је период пре и после примене *RFID*-а и *Bluetooth*-а. Након примене *RFID*-а и *Bluetooth*-а, није било података који су регистровани као мања грешка. Такође, могуће је видети да је могућност људске грешке сведена на минимум.

У следећој табели (Табела 8) приказан је укупан број мерења 6 дилатометара груписаних по години. Такође, у табели су приказани број и проценат података са мањом грешком.

$$\text{Процент грешке} = \frac{\text{Број мањих грешака}}{\text{Број мерења за 6 уређаја}} * 100$$

Табела 8. Процент тачности

Период од 12 месеци (од 1. јула)				
Уређај	Период мерења	Мерења за 6 уређаја	Мање грешке	Процент грешке (%)
Дилатометар (компаратер)	2014–2015	214	8	3,7
	2015–2016	208	10	4,8
	2016–2017	210	9	4,3
	2017–2018	214	6	2,8
	2018–2019	214	1	0,47

На претходној табели приказано је да је након употребе *RFID*-а и *Bluetooth*-а проценат људских грешака (мањих грешака) знатно смањен. У посматраном периоду од 2014. до 2018. године, процентуална грешка износила је око 4%, док је од 2018, применом *RFID*-а и *Bluetooth*-а, тај проценат анулиран (0,4%). Употреба *RFID*-а и *Bluetooth*-а смањила је могућност људске грешке на низак ниво, јер је процес читања и снимања података побољшан.



Слика 70. Дилатометар *Pizzi 700* [165]





Слика 71. Компаратер *Huggenberger ERDM25* [165]

На следеће три слике приказана је имплементација *RFID* тагова на мерним местима где се користе мерни уређаји: дилатометар, клинометар и компаратер.



Слика 72. Дилатометар на мерном месту *D-20-H* [165]





Слика 73. Клинометар на мерном месту *CL-42R-H* [165]



Слика 74. Компаратер на мерном месту *DP-20* [165]

### 6.3 Модел прихватања *RFID* технологије у осматрању

Истраживање је спроведено на запосленима који свакодневно користе *RFID* и *Bluetooth* технологије. Резултати анкете су доказ задовољних радника и успешне примене технологије у оквиру техничког осматрања. Да би модел био прихваћен, морају га прихватити професионалци који врше мерења (техничари). За ову студију је коришћена модификована верзија модела прихватања технологије (*Technology Acceptance Model 2 – TAM2*) како би се структурирао истраживачки процес и помогло да се побољша разумевање прихватања и коришћења *RFID*-а и *Bluetooth*-а у мониторингу [166]. Модификовани модел *TAM2* користи технолошке аспекте, али искључује социолошке аспекте. Модел мери пет различитих аспеката потенцијалне употребе нових технолошки напредних производа који долазе из искуства корисника [167]: употребљивост (*Perceived usefulness – PU*), лакоћа употребе (*Perceived ease of use – PEOU*), контрола понашања уређаја (*Perceived behavioral control – PBC*), добровољно коришћење (*Perceived voluntariness – PV*), намера даљег коришћења (*Scale for behavioral intention – PBI*). Прикупљање података спроведено је анкетом која је садржала свих пет аспеката. То је специфичан систем који користи мали број стручњака (десет запослених). Истраживање је спроведено над свим професионалцима (стручњацима) који су укључени у прикупљање и обраду података. Анкету су попунили запослени из одељења за надгледање бране (два запослена), обраде података (три запослена) и одељења за анализу података (два запослена), као и одељења за предвиђање понашања бране (три запослена). Одељење за мониторинг бране и одељење за предвиђање понашања бране налазе се у Кладову, одељење за обраду података налази се у Крагујевцу, а одељење за анализу података налази се у Београду.

Просечна вредност и стандардно одступање за свако питање у анкети приказани су у следећој табели (Табела 9). Такође је могуће видети просечне вредности и стандардна одступања за сваки аспект истраживања. Просечна оцена већине питања прелази оцену 4, што показује да су *RFID* и *Bluetooth* корисници задовољни побољшањем процеса праћења на брани.

Табела 9. Примена *TAM2* у евалуацији *RFID* технологије у техничком осматрању бране

Аспект	Питање	Просек	Станд. девијација	Просек	Девијација
Употребљивост	<i>RFID</i> и <i>Bluetooth</i> омогућују ми да брже испуним задатке.	4,800	0,422		
	<i>RFID</i> и <i>Bluetooth</i> побољшали су мој квалитет рада.	4,400	0,516		
	<i>RFID</i> и <i>Bluetooth</i> олакшавају мој посао.	4,500	0,527	4,350	0,685
	<i>RFID</i> и <i>Bluetooth</i> побољшали су моју продуктивност.	4,300	0,675		
	<i>RFID</i> и <i>Bluetooth</i> дају ми већу контролу над мојим послом.	3,900	0,994		
	<i>RFID</i> и <i>Bluetooth</i> побољшавају моју ефикасност у послу.	4,200	0,632		



Аспект	Питање	Просек	Станд. девијација	Просек	Девијација
Лакоћа употребе	Моја интеракција са <i>RFID</i> -ем и <i>Bluetooth</i> -ом била је јасна и разумљива.	4,400	0,699	4,283	0,804
	<i>RFID</i> и <i>Bluetooth</i> су једноставни за употребу.	4,500	0,527		
	Учење да користим <i>RFID</i> и <i>Bluetooth</i> било ми је лако.	4,300	0,675		
	Ретко се збуним када користим <i>RFID</i> и <i>Bluetooth</i> .	3,900	1,101		
	Ретко правим грешке када користим <i>RFID</i> и <i>Bluetooth</i> .	4,500	0,707		
	Ретко сам фрустриран када користим <i>RFID</i> и <i>Bluetooth</i> .	4,100	0,994		
Контрола понашања уређаја	Могу поуздано да користим <i>RFID</i> и <i>Bluetooth</i> .	4,700	0,483	4,460	0,646
	Знам да користим <i>RFID</i> и <i>Bluetooth</i> .	4,500	0,527		
	Имам ресурсе за коришћење <i>RFID</i> -а и <i>Bluetooth</i> -а.	4,700	0,483		
	Могу да користим <i>RFID</i> и <i>Bluetooth</i> .	4,400	0,699		
	Имам контролу над коришћењем <i>RFID</i> -а и <i>Bluetooth</i> -а.	4,000	0,816		
Добровољно коришћење	Моја употреба <i>RFID</i> -а и <i>Bluetooth</i> -а је добровољна.	3,900	0,994	3,209	1,163
	Мој надређени захтева од мене да користим <i>RFID</i> и <i>Bluetooth</i> .	2,900	0,994		
	Иако би могло бити од користи, коришћење <i>RFID</i> -а и <i>Bluetooth</i> -а није обавезно у мом послу.	3,400	1,350		
Намера даљег коришћења	Намеравам да наставим да користим <i>RFID</i> и <i>Bluetooth</i> за обављање свог посла.	4,300	0,675	4,050	0,887
	Намеравам често да користим <i>RFID</i> и <i>Bluetooth</i> за обављање свог посла.	3,800	1,033		

Отворена питања и одговори запослених, који се баве осматрањем брана, приказани су у следећој табели (Табела 10).

Табела 10. Сугестије и примедбе добијене из отворених питања

Питање	Одговор
<p><b>П1:</b> Зашто <i>RFID</i> и <i>Bluetooth</i> олакшавају ваше пословање?</p>	<p>Већина одговора запослених на ово питање је да <i>RFID</i> и <i>Bluetooth</i> смањују могућност грешке.</p> <p>A1.1: Смањује могућност грешке, мања је вероватноћа да ћу погрешити.</p> <p>A1.2: Мања могућност грешке.</p> <p>A1.3: Употреба <i>RFID</i>-а и <i>Bluetooth</i>-а олакшава извршавање свакодневних задатака, јер убрзава активност тако што аутоматизује идентификацију мерних места и смањује могућност грешке.</p> <p>A1.4: Олакшава читање и унос података.</p> <p>A1.5: Контрола грешака приликом мерења. Лакше је прикупљање података.</p>
<p><b>П2:</b> Шта би вам олакшало посао?</p>	<p>Већина одговора запослених на ово питање је да аутоматизација може да олакша посао.</p> <p>A2.1: Уколико би постојало више опција за аутоматизацију, нпр. аутоматско читавање мерног уређаја, итд.</p> <p>A2.2: Примена <i>RFID</i>-а и <i>Bluetooth</i>-а на више мерних места.</p>
<p><b>П3:</b> Шта треба побољшати да би прикупљање података било ефикасније?</p>	<p>Према одговорима запослених, већа аутоматизација је нешто што може да побољша прикупљање података.</p> <p>A3.1: Већа аутоматизација.</p> <p>A3.2: Аутоматска идентификација мерног уређаја, аутоматско читавање, итд.</p> <p>A3.3: Увести дигитално прикупљање података и смањити појаву грешке у мерењу.</p>

Бране су веома осетљиве на минимална померања, тако да минимизовање људске грешке при посматрању има велики утицај на могуће неповољне догађаје [168]. Неке од брана на којима су се десили кварови су *Way Ela* [151], *Zhouqu* [152], *SE Brazil* [153], итд. У [169] аутори описују ситуацију у Калифорнији, где је већина брана старија од 50 година. Резултати показују да ће се вероватноћа кварова повећати за већину брана у Калифорнији до 2100. Због тога је потребно стално побољшавати систем осматрања и повећавати сигурност брана. У Србији је побољшање сигурности брана ХЕ „Ђердап 1” и ХЕ „Ђердап 2” од великог значаја због многих насеља која се налазе у сливу доњег Дунава. Осим тога, ХЕ „Ђердап 1” има велики значај за енергетски систем Србије и региона са годишњом производњом електричне енергије од 6,4GWh [170].

Кључни допринос дисертације је детаљан опис примене *RFID*-а и *Bluetooth*-а у процесу мануелног техничког осматрања брана. Спроведено је истраживање међу запосленима који користе *RFID* и *Bluetooth* користећи *TAM2* методу. Такође, извршена је анализа података са циљем поређења грешака у мониторингу података пре и после примене *RFID*-а и *Bluetooth*-а.

Резултати показују да се употребом *RFID*-а и *Bluetooth*-а у процесу мануелног техничког осматрања побољшава свеукупни процес праћења, подаци постају поузданији, процес ручног прикупљања података је бржи, а запослени су задовољнији јер проводе мање времена у телу бране и осећају мањи притисак због могуће грешке у осматрању. Коришћењем *RFID*-а и *Bluetooth*-а, подаци постају веродостојнији јер се проценат грешке коју изазива људски фактор своди на ниску стопу (Табела 8). Смањењем броја грешака, модел предвиђања оштећења ће дати тачнију слику стања бране [171].

Резултати анкете показују да употреба *RFID*-а и *Bluetooth*-а убрзава процес мануелног техничког осматрања. Убрзавањем процеса мануелног техничког осматрања запослени проводе мање времена у телу бране, тј. у собама са влагом и slabим осветљењем. Такође, употреба *RFID*-а и *Bluetooth*-а смањује притисак на запослене да могу да погреше у читању или писању података и решава проблем осветљења и погрешног читања мерења, јер се то врши аутоматски. Све наведено утиче на радне услове запослених и повећава њихово задовољство. Идеја о коришћењу *RFID*-а и *Bluetooth*-а може се реализовати у било којем другом објекту где се врши мануелно техничко осматрања (зграде, мостови итд.), јер је принцип осматрања сличан. Листа главних импликација и практичних препорука за различите групе заинтересованих страна приказана је табеларно (Табела 11).

Табела 11. Кључне импликације за главне интересне групе

Интересне групе	Импликације (истраживачка питања)
<b>Корисници</b>	<p>Употреба <i>RFID</i>-а и <i>Bluetooth</i>-а делимично је аутоматизовала и дигитализовала процес мануелног техничког осматрања, што убрзава осматрање и смањује вероватноћу људске грешке. Све то чини запосленог задовољнијим, јер има мање стреса и брже завршава своје задатке. (ИП4)</p> <p>Процена модела показује да се <i>RFID</i> и <i>Bluetooth</i> могу користити у процесу осматрања када је потребан експерт за прикупљање и анализу података.</p>
<b>Власници брана</b>	<p>Употреба <i>RFID</i>-а и <i>Bluetooth</i>-а побољшава процес мониторинга брана, минимизујући људске грешке, што податке чини поузданијим. Поузданији подаци осигуравају боље одржавање бране. (ИП2)</p> <p>Препоручује се коришћење што већег броја пасивних <i>RFID</i> тагова, због унификације и финансијских ограничења [85], као и због ефикасне замене у случају квара.</p>
<b>Влада</b>	<p>Поуздани подаци омогућавају нормално одржавање бране, што утиче на сигурност објекта, и у директној је вези са заштитом екосистема који се налази у близини бране. (ИП1)</p> <p>Примена <i>RFID</i>-а и <i>Bluetooth</i>-а има добрих ефеката, нпр. очување друштвеног окружења, смањење трошкова пројеката које финансира влада, аутоматизацију процеса итд. [172]. Резултати истраживања указују да би <i>RFID</i> и <i>Bluetooth</i> требало у великој мери користити приликом пројектовања и имплементације огромних <i>IT</i> екосистема или инфраструктурних пројеката.</p>

Интересне групе	Импликације (истраживачка питања)
<b>Истраживачи</b>	<p>Време проведено поред уређаја, осветљење, влага, температура итд., могу утицати на перцепцију запослених. Такви подаци могу се прикупити помоћу <i>Beacons</i>-а, који се даље могу користити за контролу квалитета мерених техничких података. Поузданији подаци прикупљени <i>RFID</i>-ем и <i>Bluetooth</i>-ом који се користе за моделирање брана омогућавају прецизнију слику стања бране. Прикупљени подаци мерења могу се користити за успостављање базе поузданости уређаја. (ИПЗ)</p> <p>Истраживачи би у великој мери требало да користе <i>RFID</i> и <i>Bluetooth</i> и омогуће прикупљање онолико података колико <i>IoT</i> произведе [173]. Даље, додатне напоре би требало уложити у надоградњу постојећих модела опсежним технологијама (<i>RFID</i>, <i>Beacons</i>, <i>AI</i>, итд.)</p>

Главни допринос дисертације огледа се у побољшању система мониторинга брана, користећи издржљиву и јефтину *RFID* технологију, што доводи до смањења фактора људске грешке и директно утиче на поузданост података, резултирајући реалнијим стањем брана. Дисертација доноси нову вредност постојећој литератури кроз оригинални приступ. У дисертацији је могуће видети приступ побољшању сигурности бране са техничке стране, тј. употребу *RFID*-а и *Bluetooth*-а, који омогућавају поузданије податке и олакшавају посао запосленима који се баве мануелним техничким мониторингом. Развијени модел мануелног техничког мониторинга који користе *RFID* и *Bluetooth*, пројектован је за специфичне услове окружења (у затвореном простору, влага итд.) које диктирају високе бране. Модел није тестиран у условима као што су мониторинг зграда или мостова, па једно од ограничења могу бити другачији временски услови окружења на другим типовима грађевина.

Следећа фаза примене унапређеног модела техничког осматрања је побољшање процене квалитета података. Развијена је идеја о употреби *Beacons*-а у прикупљању података о животној средини (влага ваздуха, температура...), који се могу користити као улазни параметри у функцијама за процену података. Формуле са новим улазним параметрима надоградиће постојеће формуле које се користе за процену квалитета мерених техничких података и пружаће бољу процену података. Једна од следећих фаза побољшања техничког осматрања и процене квалитета је употреба предиктивне аналитике. На основу постојећих примера и историјских података, могуће је створити базу података са случајевима коришћења.

## 7. НАУЧНИ И СТРУЧНИ ДОПРИНОСИ

Најзначајнији допринос дисертације је унапређени модел инфраструктуре система за техничко осматрање брана, намењеног повећању сигурности објеката.

Финални резултати дисертације су развијени модел, инфраструктура и сервиси система за ручно прикупљање и унос података. Овај развијени модел представља основу за имплементацију модела на брани ХЕ „Бердап 1” током рада на докторској дисертацији.

Кључни научни доприноси дисертације огледају се у:

- формалном опису развијеног модела и сервиса управљања и одржавања брана заснованог на интернету интелигентних уређаја;
- детаљном опису развијеног модела система за мануелно техничко осматрање брана заснованог на примени *IoT*-а;
- унапређењу модела архитектуре и инфраструктуре система за мануелно техничко осматрање на бранама заснованог на *IoT*-у;
- опису методолошког поступка за примену интернета интелигентних уређаја у систему управљања и осматрања брана; и
- анализи предложеног модела са аспекта користи и задовољавања потреба.

Рад на дисертацији резултује и низом стручних доприноса, од којих су најважнији:

- анализа примене интернета интелигентних уређаја и *cloud computing*-а у адаптацији модела и сервиса за управљање и одржавање брана;
- преглед и анализа технологија потребних за имплементацију модела за мануелно техничко осматрање брана, заснованог на *IoT*-у;
- анализа могућности примене савремених технолошких концепата, као што су *RFID*, *NFC*, *Beacons* и *cloud computing* у контексту осматрања и одржавања брана;
- анализа и валидација ефикасности примене *IoT*-а у функционисању брана; и
- могућности интеграције инфраструктуре система за мануелно техничко осматрање брана са постојећим системом за техничко осматрање.

Истраживање проблематике увођења концепата и технологија интернета интелигентних уређаја и *cloud computing*-а у систему за техничко осматрање објеката, са становишта друштвене корисности може имати вишеструке импликације:

- резултати истраживања помоћи ће да се минимизују људске грешке;
- резултати истраживања помоћи ће да се побољша поузданост и прецизност прикупљених података;
- резултати истраживања помоћи ће да се унапреди сигурност брана;
- резултате истраживања могу користити друге бране, где се користи техничко осматрање; и
- развијени модел техничког осматрања на бранама погодан је да се користи и на другим грађевинским објектима где има потребе за техничким осматрањем.



Радови који су проистекли из дисертације:

### **Списак радова проистеклих из дисертације**

Током досадашњег рада, Растко Мартаћ је објавио више радова у земљи и иностранству, и учествовао на више међународних и домаћих скупова и конференција.

#### **Радови у зборницима међународних часописа (M23):**

Martać R., Milivojević N., Despotović-Zrakić M., Bogdanović Z. и Barać D., „*Enhancing Large Dam Safety Using IoT Technologies: A Case of a Smart Dam*”, у *Journal of Universal Computer Science (J.UCS)*, ISSN 0948-695X, том 26, изд. 5, стр. 583–603, 2020.

#### **Радови у зборницима међународних часописа (M24):**

Martać R., Milivojević N., Milivojević V., Ćirović V. и Barać D., „*Using IoT in monitoring and management of dams in Serbia*”, у *Facta Universitatis*, ISSN: 0353-3670, том 29, изд. 3, стр. 419–435, 2016, DOI: 10.2298/FUEE1603419M.

#### **Радови у зборницима међународних конференција (M33):**

Martać R., Novarlić M. и Barać D., „*Using Big data on Large dams*”, у *15th International Symposium – Symorg 2016*, ISBN 978-86-7680-326-2, стр. 432–438, Златибор, 2016.

Martać R., Barać D. и Vujin V., „*Application of the Internet of Things in hydrology*”, у *14th International Symposium – Symorg 2014*, ISBN: 978-86-7680-295-1, стр. 426–433, Златибор, 2014.

## 8. БУДУЋА ИСТРАЖИВАЊА

Имплементирани модел техничког осматрања брана, заснован на *IoT* технологијама, може се успешно применити у процесу осматрања брана. Позитивни резултати и решења унапређеног модела осматрања брана, проистекли из дисертације, отварају могућност за даља истраживања и у области грађевине (мониторинга) и у даљем усавршавању мониторинга брана.

С обзиром на то да се мониторинг врши на разноликим грађевинским објектима, а не само бранама, развијени модел је могуће применити и на мостовима и на зградама, а затим тестирати и анализирати успешност модела у другачијим условима окружења где се врши мониторинг.

У дисертацији је имплементиран модел мануелног техничког осматрања брана са применом *RFID* и *Bluetooth* технологија. Евалуација описаног развијеног модела мануелног техничког осматрања је развијена кроз две фазе и приказала је бројна унапређења система мониторинга брана. Потребно је додатно усавршити систем контроле квалитета мерених техничких података. Могуће је извршити надоградњу развијеног модела мониторинга брана применом *Beacons* тагова, који имају додатне могућности у односу на обичне *RFID* тагове. Концептуални модел примене *Beacons*-а, у развијеном моделу мануелног техничког осматрања брана, приказан је на слици испод (Слика 75).



Слика 75, Будућа истраживања – употреба *Beacons*-а

Трећа фаза процеса унапређења мануелног техничког осматрања концентрисана је на побољшање процене квалитета измерених података. У трећој фази планирана је инсталација *Beacons*-а. *Beacons* су активни *RFID* тагови, који могу да читају различите параметре окружења. Параметри околине, као што су температура ваздуха, влажност, ниво светлости итд., у великој мери могу да утичу на повећање фактора људске грешке. Такође, осим фактора окружења, *Beacons* могу да измере време проведено на одређеном мерном месту, јер неки мерни уређаји захтевају да након повезивања читача са уређајем треба сачекати неко време да би се уређај стабилизовао и започело са мерењима параметара бране. Све измерене вредности, тј. метаподаци, биће снимљени у бази података. Добијене измерене вредности прошле би кроз одређене формуле и пружиле процену квалитета података. У даљем развоју постоји и могућност употребе *AI* у управљању бранама за анализу и процену квалитета података, коришћењем аутоматског машинског учења (*AutoML*) [174].

У складу са постављеним циљевима у дисертацији и ограничењима у истраживању (финансијска и немогућност замене одређених мерних инструмената), будућа истраживања, поред наведеног, могу да обухвате: 1) примену модела мануелног техничког осматрања заснованог на *IoT* технологијама на већем броју мерних уређаја; 2) имплементацију *Beacons* тагова ради унапређења ККМТП и; 3) употребу *AI* у управљању брана за анализу и процену квалитета података.

## 9. ЗАКЉУЧАК

У дисертацији је истакнут значај брана у савременом начину живота, с обзиром на то да бране утичу на снабдевање водом, штите од поплава, омогућавају наводњавање и производњу струје.

У дисертацији су анализирани главни изазови мануелног техничког мониторинга брана, који је битан аспект мониторинга брана. Мониторинг брана је битан за функционисање и управљање бранама. Предложено је решење система мануелног техничког мониторинга брана заснованог на савременим *IoT* технологијама. У дисертацији су изложене теоријске основе мониторинга брана, *IoT*-а, *RFID* и *Bluetooth* технологија, које су примењене у мониторингу на конкретном примеру бране ХЕ „Ђердап 1”. Приказани су модели постојећег осматрања брана и примене савремених технологија *IoT*-а, *RFID*-а и *Bluetooth*-а у индустрији и водопривреди. Дефинисан је нови модел мануелног техничког осматрања брана, заснованог на *IoT* технологијама и представљене су кључне карактеристике развијеног модела и практично решење које може помоћи у елиминацији фактора људске грешке.

У експерименталном делу пројектован је и имплементиран модел мануелног техничког осматрања на брани ХЕ „Ђердап 1”. Спроведени су тестирање и мерење релевантних параметара система на конкретном примеру у свакодневном функционисању бране. Анкетирани су запослени, стручњаци који се баве мониторингом брана.

Решење техничког осматрања брана заснованог на *IoT* технологијама, може се успешно применити у процесу осматрања брана. У истраживању које је спроведено показано је да коришћење *RFID* и *Bluetooth* технологија минимизује фактор људске грешке, што утиче на то да подаци који се користе за предвиђање понашања брана буду релевантнији. Вредности добијене током истраживања показале су видно унапређење процеса мануелног техничког осматрања брана. На основу спроведене анкете, утврђено је да имплементирање савремених технологија убрзава процес осматрања запосленима, смањује стрес, јер су могућности за грешку минималне, а услови рада се побољшавају јер запослени проводе мање времена у слабо осветљеним и влажним просторијама (тело бране).

Експериментални део који је реализован на брани ХЕ „Ђердап 1”, из разних аспеката, донео је видна побољшања у мониторингу брана. Тренутно се врши имплементација развијеног модела мануелног техничког мониторинга на брани ХЕ „Ђердап 2”.

Развијени модел унапређеног система мануелног техничког осматрања саставни је део система за управљање безбедношћу бране ХЕ „Ђердап 1”. Спровођење овог истраживања је подржао Институт за водопривреду „Јарослав Черни”, а захвалност дугујем свим члановима тима који су учествовали у реализацији СУБ-а ХЕ „Ђердап 1”.

## 10. ЛИТЕРАТУРА

- [1] Д. Дивац и други аутори, „Студија - Одржавање великих брана у Републици Србији“, Београд, 2011.
- [2] T. S. Titova, A. Longobardi, R. G. Akhtyamov, и E. S. Nasyrova, „Lifetime of earth dams“, *Mag. Civ. Eng.*, том 69, изд. 1, стр. 34–43, 2017.
- [3] H. Wang, L. Li, Y.-Y. Jiao, X.-R. Ge, и S.-C. Li, „A relationship-based and object-oriented software for monitoring management during geotechnical excavation“, *Adv. Eng. Softw.*, том 71, стр. 34–45, Мај 2014.
- [4] B. Sander-Kessels и K.-H. Strasser, „Implementation of a Dam Safety Management System Experiences in the Rollout“, *Wasserwirtschaft*, том 106, изд. 6, стр. 116–119, 2017.
- [5] R. Martać, N. Milivojević, V. Milivojević, V. Ćirović, и D. Barać, „Using internet of things in monitoring and management of dams in Serbia“, *Facta Univ. - Ser. Electron. Energ.*, том 29, изд. 3, стр. 419–435, 2016.
- [6] С.-Н. Ко, „RFID-based building maintenance system“, *Autom. Constr.*, том 18, изд. 3, стр. 275–284, Мај 2009.
- [7] K. O. Schnock, B. Biggs, A. Fladger, D. W. Bates, и R. Rozenblum, „Evaluating the Impact of Radio Frequency Identification Retained Surgical Instruments Tracking on Patient Safety“, *J. Patient Saf.*, стр. 1, Феб. 2017.
- [8] „Using RFID technology to reduce medication errors - Hospital News“. [На Интернету]. Доступно на: <https://hospitalnews.com/using-rfid-technology-to-reduce-medication-errors/>. [Приступљено: 15-Јули-2019].
- [9] X. Li, Y. Li, X. Lu, Y. Wang, H. Zhang, и P. Zhang, „An online anomaly recognition and early warning model for dam safety monitoring data“, *Struct. Heal. Monit.*, стр. 147592171986426, Јули 2019.
- [10] X. Zhang, X. Chen, и J. Li, „Improving Dam Seepage Prediction Using Back-Propagation Neural Network and Genetic Algorithm“, *Math. Probl. Eng. 2020*, том 11, стр. 1–8, Апр. 2020.
- [11] S. Li, L. Yuan, H. Yang, H. An, и G. Wang, „Tailings dam safety monitoring and early warning based on spatial evolution process of mud-sand flow“, *Saf. Sci.*, том 124, стр. 104579, Апр. 2020.
- [12] „Синтезни извештај - Модернизација техничког осматрања бране ХЕ ,Ђердап 1‘ у 2019. години“, 2019.
- [13] Д. Дивац и други аутори, „Књига 10 - Извештај о теоријским основама и алгоритмима контроле квалитета и статистичког моделирања мерених техничких података“, Институт за водопривреду „Јарослав Черни“, Београд, 2016.
- [14] S. S. Siddula, P. C. Jain, и M. D. Upadhyay, „Real Time Monitoring and Controlling of Water Level in Dams using IoT“, у *Proceedings of the 8th International Advance Computing Conference, IACC 2018*, 2018, стр. 14–19.
- [15] „Dam Safety in the Digital Age: How IoT is Transforming Dam Safety | sensemetrics Blog“, 2019. [На Интернету]. Доступно на: <https://sensemetrics.com/blog/dam-safety-in-the-digital-age-how-iot-is-transforming-dam-safety/>. [Приступљено: 14-Мај-2020].
- [16] D. Zhong, F. Wang, B. Wu, B. Cui, и Y. Liu, „From digital dam toward smart dam“, *Shuili Fadian Xuebao/Journal Hydroelectr. Eng.*, том 34, изд. 10, стр. 1–13, Окт. 2015.
- [17] „IIoT and the Future of Hydropower“. [На Интернету]. Доступно на:



- [33] S. Murali, K. R. Jothi, R. Lokeshkumar, S. Anto, и G. Ravikumar, „A Low-Cost Cloud based Smart Flood Detection and Alert System“, *Biosci. Biotechnol. Res. Commun. Spec. ISSUE*, том 12, изд. 498, стр. 50–55, 2019.
- [34] J. Simatupang Welman, „Flood Early Warning Detection System Prototype Based on IoT Network“, *Internetworking Indones. J.*, том 11, изд. 1, стр. 17–22, Май 2019.
- [35] N. V. S. S. Varma, E. E. Preethi, M. R. Kumar, и R. Kumar Tenali, „Internet of Things Based Smart Flood Monitoring & detecting system“, *Int. J. Recent Technol. Eng.*, том 7, изд. 6, стр. 2277–3878, Март 2019.
- [36] M. S. Mohd Sabre, S. S. Abdullah, и A. Faruq, „Flood Warning and Monitoring System Utilizing Internet of Things Technology“, *Kinet. Game Technol. Inf. Syst. Comput. Network, Comput. Electron. Control*, том 4, изд. 4, стр. 287–296, Окт. 2019.
- [37] S. B. H. Youssef, S. Rekhis, и N. Boudriga, „A Blockchain based Secure IoT Solution for the Dam Surveillance“, у *IEEE Wireless Communications and Networking Conference, WCNC*, 2019, том 2019-April.
- [38] Z. Rasin, H. Hamzah, и M. S. Mohd Aras, „Application and evaluation of high power Zigbee based wireless sensor network in water irrigation control monitoring system“, у *2009 IEEE Symposium on Industrial Electronics and Applications, ISIEA 2009 - Proceedings*, 2009, том 2, стр. 548–551.
- [39] T. M. Thekkil и N. Prabakaran, „Real-time WSN based early flood detection and control monitoring system“, у *2017 International Conference on Intelligent Computing, Instrumentation and Control Technologies, ICICICT 2017*, 2018, том 2018-January, стр. 1709–1713.
- [40] P. K. Patil и S. R. Patil, „Structural health monitoring system using WSN for bridges“, у *Proceedings of the 2017 International Conference on Intelligent Computing and Control Systems, ICICCS 2017*, 2017, том 2018-Janua, стр. 371–375.
- [41] M. Pule, A. Yahya, и J. Chuma, „Wireless sensor networks: A survey on monitoring water quality“, *J. Appl. Res. Technol.*, том 15, изд. 6, стр. 562–570, Дек. 2017.
- [42] G. Tuna, B. Nefzi, O. Arkoc, и S. Potirakis M, „Wireless Sensor Network-Based Water Quality Monitoring System“, *Key Eng. Mater.*, том 605, стр. 47–50, 2014.
- [43] T. Yukitake, „Innovative solutions toward future society with AI, Robotics, and IoT“, у *IEEE Symposium on VLSI Circuits, Digest of Technical Papers*, 2017, стр. C16–C19.
- [44] J. Jeon, J. Lee, D. Shin, и H. Park, „Development of dam safety management system“, *Adv. Eng. Softw.*, том 40, изд. 8, стр. 554–563, Авг. 2009.
- [45] J. Yang, T. Bao, D. Liang, Y. Mi, и L. Yang, „Management Information System for Dam Safety Monitoring Based on B/S Structure“, у *2009 First International Conference on Information Science and Engineering*, 2009, стр. 2332–2335.
- [46] S. Huai-Zhi и W. Zhi-Ping, „Intelligent early-warning system of dam safety“, у *2005 International Conference on Machine Learning and Cybernetics*, 2005, стр. 1868-1877 Vol. 3.
- [47] E. Sun, X. Zhang, и Z. Li, „The internet of things (IOT) and cloud computing (CC) based tailings dam monitoring and pre-alarm system in mines“, *Saf. Sci.*, том 50, изд. 4, стр. 811–815, Апр. 2012.
- [48] J. Gómez, J. F. Huete, O. Hoyos, L. Perez, и D. Grigori, „Interaction system based on Internet of things as support for education“, у *Procedia Computer Science*, 2013, том 21, стр. 132–139.

- [49] R. Martać, D. Varać, и V. Vujin, „Application of the internet of things in hydrology“, у *Symorg 2014*, 2014, стр. 426–433.
- [50] B. Radenković, M. Despotović-Zrakić, Z. Bogdanović, D. Varać, A. Labus, и Ž. Vojojić, *Internet inteligentnih uređaja*. Beograd: Fakultet organizacionih nauka, 2017.
- [51] S. Ahmadi, *5G NR: Architecture, technology, implementation, and operation of 3GPP new radio standards*. Elsevier, 2019.
- [52] K. M. Симић, „Модел инфраструктуре е-образовања базиран на Интернету интелигентних уређаја“, Факултет Организационих Наука, Београд, 2017.
- [53] A. Rayes и S. Salam, „The Things in IoT: Sensors and Actuators“, у *Internet of Things From Hype to Reality*, Springer International Publishing, 2017, стр. 57–77.
- [54] C. Wilson, T. Hargreaves, и R. Hauxwell-Baldwin, „Benefits and risks of smart home technologies“, *Energy Policy*, том 103, стр. 72–83, Апр. 2017.
- [55] „EnOcean - Technology“. [На Интернету]. Доступно на: <https://www.enocean.com/en/technology/>. [Приступљено: 06-Апр-2020].
- [56] M. Domb, „Smart Home Systems Based on Internet of Things“, у *IoT and Smart Home Automation [Working Title]*, IntechOpen, 2019.
- [57] L. Quijano-Sánchez, I. Cantador, M. E. Cortés-Cediel, и O. Gil, „Recommender systems for smart cities“, *Inf. Syst.*, том 92, Сеп. 2020.
- [58] „Smart City“. [На Интернету]. Доступно на: <https://www.paessler.com/iot/smart-city>. [Приступљено: 04-Мај-2020].
- [59] „Wearable tech and their impact on health | Instant Healthy Life“. [На Интернету]. Доступно на: <https://instanthealthylife.com/en/wearable-tech-and-their-impact-on-health/>. [Приступљено: 04-Мај-2020].
- [60] H. Modares, A. Moravejsharieh, R. Salleh, и J. Lloret, „Security overview of wireless sensor network“, *Life Sci. J.*, том 10, изд. 2, стр. 1627–1632, Сеп. 2013.
- [61] D. Valencic, V. Lebinac, и A. Skendzic, „Developments and current trends in Ethernet technology“, у *2013 36th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2013 - Proceedings*, 2013, стр. 431–436.
- [62] R. Zhang и други аутору, „A new environmental monitoring system based on WiFi technology“, у *Procedia CIRP*, 2019, том 83, стр. 394–397.
- [63] F. Alecu, „The WiMAX Technology“, Bucharest, 2010.
- [64] „Networking the IoT with IEEE 802.15.4/6LoWPAN - Tech Briefs“. [На Интернету]. Доступно на: <https://www.techbriefs.com/component/content/article/tb/supplements/st/features/articles/27510>. [Приступљено: 06-Апр-2020].
- [65] D. Gislason, *Zigbee Wireless Networking*. Elsevier Ltd, 2008.
- [66] S. Farahani, *ZigBee Wireless Networks and Transceivers*. Elsevier Ltd, 2008.
- [67] „ZigBee wireless standard“. [На Интернету]. Доступно на: <https://www.automatika.rs/baza-znanja/obrada-signal/zigbee-wireless-standard.html>. [Приступљено: 06-Апр-2020].
- [68] „About LoRaWAN® | LoRa Alliance®“. [На Интернету]. Доступно на: <https://loralliance.org/about-lorawan>. [Приступљено: 14-Мај-2020].
- [69] „M2M Tehnologija :: Geneko“. [На Интернету]. Доступно на:



<https://www.geneko.rs/sr/m2m-tehnologija>. [Пристапљено: 18-Мај-2020].

- [70] D. Boswarthick, O. Elloumi, и O. Hersent, *M2M Communications: A Systems Approach*. Chichester, UK: wiley, 2011.
- [71] A. Paunović, „Softverski definisane mreže (SDN) i virtualizacija mrežnih funkcija (NFV): Definicija i osnovne tehnologije u 5G mrežama“, Fakultet tehničkih nauka, Čačak, 2016.
- [72] J. Šuh, Ž. Bojović, M. Despotović-Zrakić, Z. Bogdanović, и A. Labus, „Designing a course and infrastructure for teaching software-defined networking“, *Comput. Appl. Eng. Educ.*, том 25, изд. 4, стр. 554–567, Јули 2017.
- [73] Z. Yan, P. Zhang, и A. V. Vasilakos, „A security and trust framework for virtualized networks and software-defined networking“, *Secur. Commun. Networks*, том 9, изд. 16, стр. 3059–3069, Нов. 2016.
- [74] M. Zhang, F. Sun, и X. Cheng, „Architecture of Internet of Things and its key technology integration based-on RFID“, у *Proceedings - 2012 5th International Symposium on Computational Intelligence and Design, ISCID 2012*, 2012, том 1, стр. 294–297.
- [75] M. Katayama, H. Nakada, H. Hayashi, и M. Shimizu, „Survey of RFID and its application to international ocean/air container tracking“, *IEICE Transactions on Communications*, том E95-B, изд. 3, стр. 773–793, 2012.
- [76] H. Chu, G. Wu, J. Chen, F. Fei, J. D. Mai, и W. J. Li, „Design and simulation of self-powered radio frequency identification (RFID) tags for mobile temperature monitoring“, *Sci. China Technol. Sci.*, том 56, изд. 1, стр. 1–7, Јан. 2013.
- [77] C. Occhiuzzi, S. Caizzone, и G. Marrocco, „Passive UHF RFID antennas for sensing applications: Principles, methods, and classifications“, *IEEE Antennas Propag. Mag.*, том 55, изд. 6, стр. 14–34, 2013.
- [78] S. Zhang, X. Liu, J. Wang, J. Cao, и G. Min, „Energy-efficient active tag searching in large scale RFID systems“, *Inf. Sci. (Ny)*, том 317, стр. 143–156, Окт. 2015.
- [79] I. Erguler, „A potential weakness in RFID-based Internet-of-things systems“, *Pervasive Mob. Comput.*, том 20, стр. 115–126, Јули 2015.
- [80] H. M. Fardoun, A. H. Altalhi, P. G. Villanueva, R. Tesoriero, и J. A. Gallud, „A Framework to Develop Web Applications based on RFID Panels“.
- [81] P. Pursula, I. Marttila, K. Nummila, и H. Seppa, „High frequency and ultrahigh frequency radio frequency identification passive sensor transponders for humidity and temperature measurement within building structures“, *IEEE Trans. Instrum. Meas.*, том 62, изд. 9, стр. 2559–2566, Сеп. 2013.
- [82] M. Ibrahimy и S. Motakabber, „Bridge scour monitoring by coupling factor between reader and tag antennas of RFID system“, *Int. J. GEOMATE*, том 8, изд. 2, стр. 1328–1332, 2015.
- [83] K. Chen, Q. Chen, K. Sawaya, M. Oouchida, и Y. Hirano, „Diversity reception of 920MHz RFID reader antenna in smart-shelf system“, 2015.
- [84] N. Li, G. Calis, и B. Becerik-Gerber, „Measuring and monitoring occupancy with an RFID based system for demand-driven HVAC operations“, *Autom. Constr.*, том 24, стр. 89–99, Јули 2012.
- [85] V. Daniel Hunt, A. Puglia, и M. Puglia, *RFID: A Guide to Radio Frequency Identification*. Wiley-Blackwel, 2007.
- [86] Dobkin, *The RF in RFID: Passive UHF RFID in Practice*. Elsevier Inc., 2007.
- [87] „Modern RFID Readers“. [На Интернету]. Доступно на:

- <https://www.microwavejournal.com/articles/5271-modern-rfid-readers>. [Приступљено: 07-Мај-2020].
- [88] M. Langheinrich, F. Mattern, K. Römer, и H. Vogt, „First Steps Towards an Event-Based Infrastructure for Smart Things“, Zurich, 2004.
- [89] „125KHz USB Proximity RFID Reader – Genius Solutions“. [На Интернету]. Доступно на: <https://genius.or.ke/product/125khz-usb-proximity-rfid-reader/>. [Приступљено: 27-Апр-2020].
- [90] „Juno T41 R Handheld Computer“. [На Интернету]. Доступно на: <https://www.trimble.com/Mobile-Computing/Juno-T41-R-Product-Page.aspx>. [Приступљено: 27-Апр-2020].
- [91] „RFID Handhelds. ATID AT870N Handheld UHF RFID Reader“. [На Интернету]. Доступно на: <http://www.rfidhandhelds.com/at870n-handheld-rfid-reader>. [Приступљено: 27-Апр-2020].
- [92] „Beacons | Google Developers“. [На Интернету]. Доступно на: <https://developers.google.com/beacons/>. [Приступљено: 14-Мај-2018].
- [93] „Estimote – experts in location and proximity solutions“. [На Интернету]. Доступно на: <https://estimote.com/>. [Приступљено: 07-Мај-2020].
- [94] „Bluetooth Beacons“. [На Интернету]. Доступно на: <http://bluetoothbeacons.com/>. [Приступљено: 14-Мај-2018].
- [95] P. Umate Sahebrao, A. Shaikh Samad, и A. Khan M, „Comparative study of rfid tags for metallic products in inventory tracking system“, *JournalNX- A Multidiscip. Peer Rev. J.*, том 4, изд. 11, Нов. 2018.
- [96] „RFID UHF Anti-metal Tag 135-22\_Nubian-rfid“. [На Интернету]. Доступно на: <http://www.nubian-rfid.com/RFID-UHF-Anti-metal-Tag-135-22-57.html>. [Приступљено: 27-Апр-2020].
- [97] F. Caro и R. Sadr, „The Internet of Things (IoT) in retail: Bridging supply and demand“, *Bus. Horiz.*, том 62, изд. 1, стр. 47–54, Јан. 2019.
- [98] „The Future of Retail“. [На Интернету]. Доступно на: <https://www.richardvanhooijdonk.com/en/keynote/the-future-of-retail/>. [Приступљено: 05-Јуни-2020].
- [99] „Touch 'n Go RFID“. [На Интернету]. Доступно на: <https://rfid.touchngo.com.my/>. [Приступљено: 27-Апр-2020].
- [100] „Kontrola pristupa“, 2017.
- [101] „13.5 MHz RFID Tag - Key Fob (5pk) - RobotShop“. [На Интернету]. Доступно на: <https://www.robotshop.com/en/135-mhz-rfid-tag-key-fob-5pk.html>. [Приступљено: 27-Апр-2020].
- [102] „Uvod u RFID tehnologiju - Inženjerski portal Balkana“. [На Интернету]. Доступно на: <https://www.automatika.rs/baza-znanja/obrada-signala/uvod-u-rfid-tehnologiju.html>. [Приступљено: 27-Апр-2020].
- [103] M. Bresciani и други аутори, „Monitoring water quality in two dammed reservoirs from multispectral satellite data“, *Eur. J. Remote Sens.*, том 52, изд. sup4, стр. 113–122, Дец. 2019.
- [104] C. Strangfeld, S. Johann, и M. Bartholmai, „Smart RFID Sensors Embedded in Building Structures for Early Damage Detection and Long-Term Monitoring“, *Sensors*, том 19, изд. 24, стр. 5514, Дец. 2019.

- [105] „CDC - Mining - Advanced Wireless Communication and Tracking“. [На Интернету].  
Доступно на: <https://www.cdc.gov/niosh/mining/content/emergencymanagementandresponse/commtracking/advcommtrackingtutorial3.html>. [Приступљено: 05-Јуни-2020].
- [106] „Different Types of Bluetooth Technology, Working, and Its applications“. [На Интернету].  
Доступно на: <https://www.watelectronics.com/different-types-bluetooth-technology-working-applications/>. [Приступљено: 30-Апр-2020].
- [107] P. Akash, „What is the Range of Bluetooth? How Can It Be Extended?“, 2018. [На Интернету].  
Доступно на: <https://www.scienceabc.com/innovation/what-is-the-range-of-bluetooth-and-how-can-it-be-extended.html>. [Приступљено: 04-Феб-2020].
- [108] R. Shorey и B. A. Miller, „Bluetooth technology: merits and limitations“, у *IEEE International Conference on Personal Wireless Communications*, 2000, стр. 80–84.
- [109] A. J. Jara, D. Fernandez, P. Lopez, M. A. Zamora, A. F. Skarmeta, и L. Marin, „Evaluation of bluetooth low energy capabilities for tele-mobile monitoring in home-care“, 2013.
- [110] J. Zapata, M. Egeling, и D. Schwanenberg, „Digitalisation of the measurement data acquisition on the dam monitoring with FieldVisits“, *WasserWirtschaft*, том 108, изд. 10, стр. 64–67, Окт. 2018.
- [111] E. Köppe, L. Moldenhauer, F. Naamkens, и R. Helmerich, „Feuchtemessungen in Bauteilen und anderen Strukturen mit Bluetooth Low Energy“, *Bautechnik*, том 93, изд. 10, стр. 747–751, Окт. 2016.
- [112] „Bluetooth Technology- How bluetooth works? | Digitaliana“. [На Интернету].  
Доступно на: <https://www.digitaliana.com/2014/02/bluetooth-technology-introduction.html?m=1>.  
[Приступљено: 30-Апр-2020].
- [113] J. Tillison, „Developing Beacons with Bluetooth ® Low Energy (BLE) Technology“.
- [114] „A complete guide to Bluetooth Low Energy Beacons | Beaconstac“. [На Интернету].  
Доступно на: <https://blog.beaconstac.com/2018/08/ble-made-simple-a-complete-guide-to-ble-bluetooth-beacons/>. [Приступљено: 28-Апр-2020].
- [115] „AltBeacon - The Open Proximity Beacon“. [На Интернету].  
Доступно на: <https://altbeacon.org/>. [Приступљено: 28-Апр-2020].
- [116] „GitHub - AltBeacon/spec: AltBeacon Technical Specification“. [На Интернету].  
Доступно на: <https://github.com/AltBeacon/spec>. [Приступљено: 28-Апр-2020].
- [117] „GitHub - Tesno-World/GeoBeacon: Protocol for Bluetooth LE Beacon for using with geocaching applications“. [На Интернету].  
Доступно на: <https://github.com/Tesno-World/GeoBeacon>. [Приступљено: 28-Апр-2020].
- [118] „iBeacon vs Eddystone - what works for you? | Beaconstac“. [На Интернету].  
Доступно на: <https://blog.beaconstac.com/2016/01/ibeacon-vs-eddystone/>. [Приступљено: 28-Апр-2020].
- [119] S. Kasera, N. Narang, и A. P. Priyanka, *2.5G Mobile Networks: GPRS and EDGE*. McGraw-Hill Education, 2008.
- [120] „Network coverage“. [На Интернету].  
Доступно на: <https://www.gsmarena.com/network-bands.php3>. [Приступљено: 25-Јуни-2020].
- [121] W. Mohr и W. Konhäuser, „Access network evolution beyond third generation mobile communications“, *IEEE Commun. Mag.*, том 38, изд. 12, стр. 122–133, 2000.
- [122] J. Anitha, „4G Mobile Communications - Emerging Technologies“, *Int. J. Multidiscip. Approach Stud.*, 2015.

- [123] „ITU Radiocommunication Sector“. [На Интернету]. Доступно на: <https://www.itu.int/en/ITU-R/Pages/default.aspx>. [Приступљено: 25-Јуни-2020].
- [124] N. K. Bao, S. Joung, и M. Park, „A new access mode for femtocells in 5G networks“, у *International Conference on ICT Convergence 2015: Innovations Toward the IoT, 5G, and Smart Media Era, ICTC 2015*, 2015, стр. 1368–1370.
- [125] A. Kumar и M. Gupta, „A review on activities of fifth generation mobile communication system“, *Alexandria Eng. J.*, том 57, изд. 2, стр. 1125–1135, Јуни 2018.
- [126] „5G Network Architecture“, 2016.
- [127] „5G Applications and Use Cases | Digi International“. [На Интернету]. Доступно на: <https://www.digi.com/blog/post/5g-applications-and-use-cases>. [Приступљено: 30-Апр-2020].
- [128] „How 5G Technology will revolutionize our life?“ [На Интернету]. Доступно на: <http://network.futuretechinsider.com/@munawar1235/how-5g-technology-will-revolutionize-our-life-what-are-its-applications-and-when-5g-will-start-rolling-out-in-the-world>. [Приступљено: 30-Апр-2020].
- [129] M. Despotović-Zrakić, K. Simić, A. Labus, A. Milić, и B. Jovanić, „Scaffolding environment for e-learning through cloud computing“, *Educ. Technol. Soc.*, том 16, изд. 3, стр. 301–314, 2013.
- [130] M. Despotović-Zrakić, V. Milutinović, и A. Belić, *Handbook of research on high performance and cloud computing in scientific research and education*. IGI Global, 2014.
- [131] B. Radenković, M. Despotović-Zrakić, V. Vujin, и D. Varać, „Designing network infrastructure for an e-learning cloud“, у *eLearning 4th Conference one-Learning 2013*, 2013, стр. 26–27.
- [132] „Cloud Computing Concept | atalupadhyay“. [На Интернету]. Доступно на: <https://atalupadhyay.wordpress.com/this-is-my-new-page-of-wordpress/cloud-computing-concept/>. [Приступљено: 15-Апр-2020].
- [133] A. A. Barakabitze, A. Ahmad, R. Mijumbi, и A. Hines, „5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges“, *Comput. Networks*, том 167, стр. 106984, Феб. 2020.
- [134] „Types of cloud computing“. [На Интернету]. Доступно на: <https://aws.amazon.com/types-of-cloud-computing/>. [Приступљено: 15-Апр-2020].
- [135] „Cloud Computing – Types of Cloud“. [На Интернету]. Доступно на: <https://www.esds.co.in/blog/cloud-computing-types-cloud/#sthash.jmHgi1Uq.dpbs>. [Приступљено: 15-Апр-2020].
- [136] K. (Network W. Shaw, „What is edge computing and why it matters“, 2019. [На Интернету]. Доступно на: <https://www.networkworld.com/article/3224893/what-is-edge-computing-and-how-it-s-changing-the-network.html>. [Приступљено: 10-Апр-2020].
- [137] C. Jiang и други аутори, „Energy aware edge computing: A survey“, *Comput. Commun.*, том 151, стр. 556–580, Феб. 2020.
- [138] „Azure IoT Edge, Machine Learning and Containers - The New Stack“. [На Интернету]. Доступно на: <https://thenewstack.io/azure-iot-edge-machine-learning-containers/>. [Приступљено: 10-Апр-2020].
- [139] „Non-relational data and NoSQL - Azure Architecture Center | Microsoft Docs“. [На Интернету]. Доступно на: <https://docs.microsoft.com/en-us/azure/architecture/data-guide/big-data/non-relational-data>. [Приступљено: 23-Јуни-2020].

- [140] „What Is A Non Relational Database | MongoDB“. [На Интернету]. Доступно на: <https://www.mongodb.com/scale/what-is-a-non-relational-database>. [Приступљено: 23-Јуни-2020].
- [141] K. Davis и D. Patterson, *Ethics of Big Data*. O'Reilly Media, Inc., 2012.
- [142] R. Patgiri и A. Ahmed, „Big Data: The V's of the Game Changer Paradigm“, у *Proceedings - 18th IEEE International Conference on High Performance Computing and Communications, 14th IEEE International Conference on Smart City and 2nd IEEE International Conference on Data Science and Systems, HPCC/SmartCity/DSS 2016*, 2017, стр. 17–24.
- [143] „Big Data: What it is and why it matters | SAS“. [На Интернету]. Доступно на: [https://www.sas.com/en\\_us/insights/big-data/what-is-big-data.html](https://www.sas.com/en_us/insights/big-data/what-is-big-data.html). [Приступљено: 19-Мај-2020].
- [144] X. Nie, T. Fan, B. Wang, Z. Li, A. Shankar, и A. Manickam, „Big Data analytics and IoT in Operation safety management in Under Water Management“, *Comput. Commun.*, том 154, стр. 188–196, Март 2020.
- [145] A. Sun Y и B. Scanlon R, „How can Big Data and machine learning benefit environment and water management: a survey of methods, applications, and future directions - IOPscience“, *Environ. Res. Lett.*, том 14, изд. 7, Јули 2019.
- [146] G. Pavlovic-Lažetic, „Uvod u relacione baze podataka“.
- [147] „Osnove SQL-a“. [На Интернету]. Доступно на: <https://raf.edu.rs/citaliste/tutoriali/5067-ha-osnove-sql-a-ha>. [Приступљено: 11-Апр-2020].
- [148] „JSON Introduction“. [На Интернету]. Доступно на: [https://www.w3schools.com/js/js\\_json\\_intro.asp](https://www.w3schools.com/js/js_json_intro.asp). [Приступљено: 17-Јуни-2020].
- [149] „XML Introduction“. [На Интернету]. Доступно на: [https://www.w3schools.com/xmL/xml\\_whatIs.asp](https://www.w3schools.com/xmL/xml_whatIs.asp). [Приступљено: 17-Јуни-2020].
- [150] „JSON vs XML: What's the Difference?“ [На Интернету]. Доступно на: <https://www.guru99.com/json-vs-xml-difference.html>. [Приступљено: 17-Јуни-2020].
- [151] B. Pramono Yakti, M. Bagus Adityawan, I. Kridasantausa Hadihardaja, Y. Suryadi, J. Nugroho, и A. Adi Kuntoro, „Analysis of flood propagation and its impact on Negeri Lima Village due to the failure of Way Ela Dam“, *MATEC Web Conf.*, том 270, стр. 04011, Феб. 2019.
- [152] P. Cui, G. G. D. Zhou, X. H. Zhu, и J. Q. Zhang, „Scale amplification of natural debris flows caused by cascading landslide dam failures“, *Geomorphology*, том 182, стр. 173–189, Јан. 2013.
- [153] H. Agurto-Detzel, M. Bianchi, и M. Assumpcao, „The tailings dam failure of 5 November 2015 in SE Brazil and its preceding seismic sequence“, *Geophys. Res. Lett.*, том 43, изд. 10, стр. 4929–4936, Мај 2016.
- [154] A. R. Chavan и S. S. Valunjkar, „A Study of Instruments used for Dam Instrumentation in Gravity and Earthen Dams“, *Int. J. Eng. Tech. Res.*, том 3, изд. 5, стр. 355–361, 2015.
- [155] Д. Дивац и други аутори, „Књига 2 - Извештај о опреми и софтверу за привремено складиштење података“, Београд, 2016.
- [156] L. Dong, W. Shu, D. Sun, X. Li, и L. Zhang, „Pre-Alarm System Based on Real-Time Monitoring and Numerical Simulation Using Internet of Things and Cloud Computing for Tailings Dam in Mines“, *IEEE Access*, том 5, стр. 21080–21089, 2017.
- [157] „Knjiga 21-Izveštaj o geometrijskim, fizičkim i funkcionalnim karakteristikama MKE modela

elektrane“, Beograd, 2017.

- [158] M. Nefovska-Danilović, „Metod konačnih elemenata“.
- [159] Д. Дивац и други аутори, „Књига 5 - Извештај о централној бази података и бази метаподатака“, Београд, 2016.
- [160] L.-C. Wang, „Enhancing construction quality inspection and management using RFID technology“, *Autom. Constr.*, том 17, изд. 4, стр. 467–479, Мај 2008.
- [161] „Microsoft Windows Mobile Device Center 6.1“. [На Интернету]. Доступно на: <https://www.microsoft.com/en-us/download/details.aspx?id=14>. [Приступљено: 10-Јули-2019].
- [162] M. Alba и други аутори, „Measurement of dam deformations by terrestrial interferometric techniques“, 2008.
- [163] J. F. A. Moore, „Monitoring Building Structures“, стр. 1–154, 1992.
- [164] N. Branisavljević, D. Prodanović, и D. Pavlović, „Automatic, semi-automatic and manual validation of urban drainage data“, *Water Sci. Technol.*, том 62, изд. 5, стр. 1013, Сеп. 2010.
- [165] „SUB HE Đerdap 1‘ 2018 - Korisnički alat za pregled istorijskih podataka“. Institut za vodoprivredu „Jaroslav Černi“, Beograd, 2018.
- [166] J. B. Cowen, „The Influence of Perceived Usefulness, Perceived Ease of Use, and Subjective Norm on the Use of Computed Radiography Systems: A Pilot Study“, *Desertation, Master*, 2009.
- [167] F. D. Davis, „Perceived usefulness, perceived ease of use, and user acceptance of information technology“, *MIS Q. Manag. Inf. Syst.*, том 13, изд. 3, стр. 319–339, Сеп. 1989.
- [168] P. Van Tien и други аутори, „Formation process of two massive dams following rainfall-induced deep-seated rapid landslide failures in the Kii Peninsula of Japan“, *Landslides*, том 15, изд. 9, стр. 1761–1778, Сеп. 2018.
- [169] I. Mallakpour, A. AghaKouchak, и M. Sadegh, „Climate-Induced Changes in the Risk of Hydrological Failure of Major Dams in California“, *Geophys. Res. Lett.*, том 46, изд. 4, стр. 2130–2139, Феб. 2019.
- [170] „HE Đerdap - Ispunjen godišnji plan proizvodnje“. [На Интернету]. Доступно на: <http://www.djerdap.rs/sr/news/72/Ispunjen+godisnji+plan+proizvodnji>. [Приступљено: 10-Јули-2019].
- [171] B. Stojanovic, M. Milivojevic, M. Ivanovic, N. Milivojevic, и D. Divac, „Adaptive system for dam behavior modeling based on linear regression and genetic algorithms“, *Adv. Eng. Softw.*, том 65, стр. 182–190, Нов. 2013.
- [172] Z. Pala и Ā. Nihat, „Automation with RFID technology as an application: Parking lot circulation control“, 2008.
- [173] „The Growth in Connected IoT Devices“, 2019. [На Интернету]. Доступно на: <https://www.idc.com/getdoc.jsp?containerId=prUS45213219>. [Приступљено: 01-Феб-2020].
- [174] „AutoML“. [На Интернету]. Доступно на: <https://www.automl.org/automl/>. [Приступљено: 04-Феб-2020].

## 11. СПИСАК СЛИКА

Слика 1. Концепт паметне бране (хидроелектране) [17] .....	10
Слика 2. Алгоритам за отварање или затварање затварачница на брани [20] .....	11
Слика 3. <i>IoT-DWM</i> [22] .....	12
Слика 4. Управљање јаловишним бранама [23], [24] .....	12
Слика 5. Систем упозоравања на бранама и акумулацијама [25] .....	13
Слика 6. Систем за предвиђање кретања и нивоа вода [26] .....	13
Слика 7. Комуникациони дијаграм у <i>Salgar</i> пројекту [27] .....	14
Слика 8. Софтвер који се користи у <i>Salgar</i> пројекту [27] .....	14
Слика 9. Систем за узбуну у случају поплава [33] .....	15
Слика 10. Унапређени систем <i>FEWDS</i> [34] .....	15
Слика 11. <i>WSN</i> мрежа [41] .....	16
Слика 12. <i>IoT</i> структура .....	19
Слика 13. Паметан град [58] .....	22
Слика 14. <i>Wearables</i> [59] .....	23
Слика 15. Топологије <i>LR-WPAN</i> мрежа .....	25
Слика 16. <i>ZigBee</i> мрежне топологије .....	26
Слика 17. Основне компоненте <i>RFID</i> система .....	32
Слика 18. <i>RFID</i> ток података [87] .....	32
Слика 19. Схематски приказ <i>RFID</i> хардвера [88] .....	32
Слика 20. Фиксни <i>RFID</i> читач [89] .....	33
Слика 21. <i>RFID Handheld Juno T41R</i> [90] .....	34
Слика 22. <i>RFID Handheld</i> [91] .....	34
Слика 23. <i>RFID UHF</i> анти-метал и водоотпорни таг [96] .....	35
Слика 24. Електронска наплата путарина [99] .....	36
Слика 25. <i>RFID</i> наруквица [100] .....	37
Слика 26. <i>RFID</i> привезак за кључ [101] .....	37
Слика 27. Примена <i>RFID</i> у логистици [102] .....	38
Слика 28. Систем за мерење одговарајуће релативне влажности са уграђеним сензором базираним на пасивној <i>RFID</i> технологији [104] .....	39
Слика 29. <i>RFID</i> праћење по зонама [105] .....	39
Слика 30. <i>RFID</i> праћење рудара [105] .....	40
Слика 31. <i>RFID GPS</i> систем за праћење возила [105] .....	40
Слика 32. <i>Bluetooth</i> веза са мобилним уређајима .....	41
Слика 33. Разноврсност примене <i>Bluetooth</i> технологије [112] .....	42
Слика 34. Функционисање <i>Beacon</i> -а [114] .....	43



Слика 35. 5G троугао [127] .....	48
Слика 36. Употреба 5G мреже [128] .....	48
Слика 37. Концепт виртуелизације [132].....	50
Слика 38. <i>Cloud computing</i> архитектура [132].....	51
Слика 39. Концепт виртуелизације и <i>cloud computing</i> -а .....	52
Слика 40. <i>Schneider Electric</i> систем пумпи [138] .....	53
Слика 41. <i>Edge computing</i> на брани .....	54
Слика 42. Централна база података [13].....	56
Слика 43. Дијаграм предложеног <i>RREW</i> модела [9].....	58
Слика 44. <i>TDMPAS</i> систем [47] .....	59
Слика 45. <i>IoT</i> модел осматрања бране [21].....	59
Слика 46. <i>KDSMS</i> систем мониторинга брана [44].....	60
Слика 47. Дијаграм система за аутоматско прикупљање података .....	62
Слика 48. Архитектура информационог система за управљање безбедношћу брана [18].....	63
Слика 49. Систем раног узбуђивања базиран на <i>cloud computing</i> -у и <i>IoT</i> -у [156].....	63
Слика 50. МКЕ мрежа секције I бране ХЕ „Ђердап 1” [157].....	64
Слика 51. МКЕ мрежа секције I бране ХЕ „Ђердап 1” [157].....	64
Слика 52. Структура модела система за управљање безбедношћу брана [159] .....	65
Слика 53. Систем техничког мониторинга [1] .....	66
Слика 54. Процес мануелног прикупљања података (мануелна аквизиција) [13].....	67
Слика 55. Дијаграм класа за модел компаратер.....	68
Слика 56. Дијаграм класа за модел механички дилатометар .....	70
Слика 57. Слојеви у архитектури система за управљање безбедношћу брана, заснованог на <i>IoT</i> -у.....	71
Слика 58. Вишеслојни модел инфраструктуре система за управљање безбедношћу брана, заснованог на <i>IoT</i> -у [156] .....	72
Слика 59. Концептуални модел интеграције система мануелног техничког осматрања брана са <i>IoT</i> технологијом [13] .....	73
Слика 60. Концептуални модел комуникације између мерних уређаја и <i>RFID</i> технологије ...	74
Слика 61. Контрола сигурности бране [1] .....	75
Слика 62. Употреба <i>cloud computing</i> -а на брани.....	77
Слика 63. Дијаграм систем мануелног техничког осматрања брана .....	78
Слика 64. Дијаграм систем мануелног техничког осматрања брана (фаза 1).....	78
Слика 65. Унапређени модел система осматрања брана (фаза 2) .....	79
Слика 66. Дијаграм случајева коришћења службе осматрања .....	80
Слика 67. Дијаграм секвенци мануелног техничког осматрања, заснован на <i>RFID</i> и <i>Bluetooth</i> технологијама .....	80

Слика 68. Систем валидације података [13].....	82
Слика 69. Историјски подаци дилатометра <i>D-31</i> пре и после имплементације новог модела осматрања .....	84
Слика 70. Дилатометар <i>Pizzi 700</i> [165] .....	85
Слика 71. Компаратер <i>Huggenberger ERDM25</i> [165].....	86
Слика 72. Дилатометар на мерном месту <i>D-20-H</i> [165] .....	86
Слика 73. Клинометар на мерном месту <i>CL-42R-H</i> [165] .....	87
Слика 74. Компаратер на мерном месту <i>DP-20</i> [165].....	87
Слика 75, Будућа истраживања – употреба <i>Beacons</i> -а .....	95

## 12. СПИСАК ТАБЕЛА

Табела 1. Пројекти мониторинга брана и речних сливова.....	17
Табела 2. Развој <i>Bluetooth</i> технологије [106].....	41
Табела 3. Упоредна анализа <i>iBeacon</i> и <i>Eddystone</i> [118] .....	44
Табела 4. Разлика између <i>XML</i> и <i>JSON</i> формата [150].....	56
Табела 5. Мерни уређаји .....	61
Табела 6. Модел компаратер.....	67
Табела 7. Модел механички дилатометар .....	69
Табела 8. Процент тачности .....	85
Табела 9. Примена <i>TAM2</i> у евалуацији <i>RFID</i> технологије у техничком осматрању бране.....	88
Табела 10. Сугестије и примедбе добијене из отворених питања.....	90
Табела 11. Кључне импликације за главне интересне групе .....	91

## БИОГРАФИЈА АУТОРА

Растко Мартаћ је рођен 01. јула 1984. године у Београду. Основну школу „Дринка Павловић” и гимназију „Прва београдска гимназија” завршио је у Београду.

Основне студије је уписао 2004. године на Факултету организационих наука у Београду, где је дипломирао 2009. године са просечном оценом 7,73, смер Информациони системи и технологије. Дипломски рад под називом „Примена Веб 2.0 технологија у промету некретнина” одбранио је са оценом 10.

Током основних студија био је студент-демонстратор на катедри за Електронско пословање.

Мастер студије уписао је 2009. године на Факултету организационих наука, на катедри за Електронско пословање. Завршни (мастер) рад под називом „Примена SMS сервиса у развоју апликације за промет некретнина” одбранио је 2011. године са оценом 10.

Докторске студије, студијски програм Електронско пословање, уписао је на Факултету организационих наука у Београду, 2013. године.

Запослен је у Институту за водопривреду „Јарослав Черни” од 2011. године, Сектор за информационе технологије и софтверски инжењеринг.

## Изјава о ауторству

Име и презиме аутора **Растко Маргаћ**

Број индекса **5050/2013**

### Изјављујем

да је докторска дисертација под насловом

### **Примена IoT модела и сервиса у управљању и одржавању брана**

- резултат сопственог истраживачког рада;
- да дисертација у целини ни у деловима није била предложена за стицање друге дипломе према студијским програмима других високошколских установа;
- да су резултати коректно наведени и
- да нисам кршио/ла ауторска права и користио/ла интелектуалну својину других лица.

**Потпис аутора**

У Београду, 08.07.2020.

---

## **Изјава о истоветности штампане и електронске верзије докторског рада**

Име и презиме аутора **Растко Маргаћ**

Број индекса **5050/2013**

Студијски програм **Информациони системи и менаџмент**

Наслов рада **Примена *IoT* модела и сервиса у управљању и одржавању брана**

Ментор **проф. др Душан Бараћ**

Изјављујем да је штампана верзија мог докторског рада истоветна електронској верзији коју сам предао/ла ради похрањена у **Дигиталном репозиторијуму Универзитета у Београду**.

Дозвољавам да се објаве моји лични подаци везани за добијање академског назива доктора наука, као што су име и презиме, година и место рођења и датум одбране рада.

Ови лични подаци могу се објавити на мрежним страницама дигиталне библиотеке, у електронском каталогу и у публикацијама Универзитета у Београду.

**Потпис аутора**

У Београду, 08.07.2020.

---

## Изјава о коришћењу

Овлашћујем Универзитетску библиотеку „Светозар Марковић“ да у Дигитални репозиторијум Универзитета у Београду унесе моју докторску дисертацију под насловом:

### **Примена IoT модела и сервиса у управљању и одржавању брана**

која је моје ауторско дело.

Дисертацију са свим прилозима предао/ла сам у електронском формату погодном за трајно архивирање.

Моју докторску дисертацију похрањену у Дигиталном репозиторијуму Универзитета у Београду и доступну у отвореном приступу могу да користе сви који поштују одредбе садржане у одабраном типу лиценце Креативне заједнице (Creative Commons) за коју сам се одлучио/ла.

1. Ауторство (CC BY)

2. Ауторство – некомерцијално (CC BY-NC)

③ Ауторство – некомерцијално – без прерада (CC BY-NC-ND)

4. Ауторство – некомерцијално – делити под истим условима (CC BY-NC-SA)

5. Ауторство – без прерада (CC BY-ND)

6. Ауторство – делити под истим условима (CC BY-SA)

(Молимо да заокружите само једну од шест понуђених лиценци.

Кратак опис лиценци је саставни део ове изјаве).

**Потпис аутора**

У Београду, 08.07.2020.

---



1. **Ауторство.** Дозвољаваате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце, чак и у комерцијалне сврхе. Ово је најслободнија од свих лиценци.
2. **Ауторство – некомерцијално.** Дозвољаваате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца не дозвољава комерцијалну употребу дела.
3. **Ауторство – некомерцијално – без прерада.** Дозвољаваате умножавање, дистрибуцију и јавно саопштавање дела, без промена, преобликовања или употребе дела у свом делу, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца не дозвољава комерцијалну употребу дела. У односу на све остале лиценце, овом лиценцом се ограничава највећи обим права коришћења дела.
4. **Ауторство – некомерцијално – делити под истим условима.** Дозвољаваате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце и ако се прерада дистрибуира под истом или сличном лиценцом. Ова лиценца не дозвољава комерцијалну употребу дела и прерада.
5. **Ауторство – без прерада.** Дозвољаваате умножавање, дистрибуцију и јавно саопштавање дела, без промена, преобликовања или употребе дела у свом делу, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца дозвољава комерцијалну употребу дела.
6. **Ауторство – делити под истим условима.** Дозвољаваате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце и ако се прерада дистрибуира под истом или сличном лиценцом. Ова лиценца дозвољава комерцијалну употребу дела и прерада. Слична је софтверским лиценцама, односно лиценцама отвореног кода.