

Primjena IOT tehnologije u industriji osiguranja

Oreški, Tomislav

Professional thesis / Završni specijalistički

2024

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Electrical Engineering and Computing / Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva**

Permanent link / Trajna poveznica: <https://um.nsk.hr/um:nbn:hr:168:797253>

Rights / Prava: [In copyright](#)/[Zaštićeno autorskim pravom.](#)

Download date / Datum preuzimanja: **2025-03-14**



Repository / Repozitorij:

[FER Repository - University of Zagreb Faculty of Electrical Engineering and Computing repository](#)



SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Tomislav Oreški

**PRIMJENA IOT TEHNOLOGIJE U INDUSTRIJI
OSIGURANJA**

SPECIJALISTIČKI RAD

ZAGREB, 2024.

UNIVERSITY OF ZAGREB
FACULTY OF ELECTRICAL ENGINEERING AND COMPUTING
SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Tomislav Oreški

**THE USE OF IOT TECHNOLOGY IN
INSURANCE INDUSTRY**

**PRIMJENA IOT TEHNOLOGIJE U INDUSTRIJI
OSIGURANJA**

SPECIALIST THESIS
SPECIJALISTIČKI RAD

ZAGREB, 2024.

Specijalistički rad izrađen je na Sveučilištu u Zagrebu Fakultetu elektrotehnike i računarstva na poslijediplomskom specijalističkom studiju Proizvodi, digitalne inovacije i tehnologije u osiguranju – INSURTECH.

Mentor: Prof. dr. sc. Vedran Bilas

Specijalistički rad ima: 81 stranica

Specijalistički rad br.: _____

Povjerenstvo za ocjenu u sastavu:

1. prof. dr. sc. Zvonko Kostanjčar – predsjednik
2. prof. dr. sc. Vedran Bilas - mentor
3. izv. prof. dr. sc. Maja Mihelja Žaja, Sveučilište u Zagrebu Ekonomski fakultet - članica

Povjerenstvo za obranu u sastavu:

1. prof. dr. sc. Zvonko Kostanjčar – predsjednik
2. prof. dr. sc. Vedran Bilas - mentor
3. izv. prof. dr. sc. Maja Mihelja Žaja, Sveučilište u Zagrebu Ekonomski fakultet - članica

Datum obrane: 14. studenog 2024.

Sažetak

Cilj specijalističkog rada je napraviti pregled stanja IoT (Internet stvari, engl. Internet of things) tehnologije, opisati prednosti i mane, navesti pregled izazova s kojima se možemo susresti prilikom njenog korištenja. Analizirati mogućnosti i prilike za primjenu IoT tehnologije u industriji osiguranja. U radu je predstavljena analiza tržišta primjene IoT tehnologije u osiguranju u Republici Hrvatskoj i odabranoj razvijenoj zemlji Europske unije (Italija) s pregledom proizvoda u kojima se koristi IoT tehnologija. Metodologija analize zasniva se na pregledu tržišta, analizi dostupnih podataka o proizvodima sa Internet stranica osiguravajućih društava. Analiza pokazuje da IoT tehnologija nije dovoljno razvijena u industriji osiguranja ne samo u Republici Hrvatskoj, već i u Italiji i da se ne primjenjuje dovoljno. Osiguravajuća društva koja žele opstati na tržištu moraju se tehnološki transformirati i iskoristiti puni potencijal IoT tehnologije.

Summary

The goal of the specialist's thesis work is to make an overview of IoT (Internet of things) technology, to describe the advantages and disadvantages and to provide an overview of the challenges that we may encounter when using it. Analyze the possibilities and opportunities for the use of IoT technology in the insurance industry. The work presents an analysis of the market for the application of IoT technology in insurance industry in the Republic of Croatia and a selected developed country of the European Union (Italy) with an overview of products where IoT technology is used. The analysis methodology is based on a market review, analysis of available data about products from insurance companies websites. The analysis shows that IoT technology is not sufficiently developed in the insurance industry, not only in the Republic of Croatia, but also in Italy, and that it is not sufficiently applied. Insurance companies that want to survive in the market must transform technologically and use the full potential of IoT technology.

Sadržaj

1. Uvod.....	9
2. IoT tehnologija	11
2.1. Definicija IoT tehnologije.....	11
2.2. Razvoj IoT tehnologije kroz povijest	12
2.3. IoT arhitektura.....	13
2.4. IoT senzori.....	15
2.5. IoT protokoli.....	18
2.6. Izazovi primjene IoT-a	21
2.7. Sigurnosni izazovi primjene IoT-a.....	24
3. Primjena IoT tehnologije.....	28
3.1. Primjeri primjene IoT tehnologije.....	31
3.1.1. Stanovanje (pametni dom).....	31
3.1.2. Automobili.....	37
3.1.3. Plovila	39
3.1.4. Zdravstvo	43
3.1.5. Prijevoz.....	45
3.1.6. Industrijski pogoni.....	45
3.2. Koristi za osiguravajuća društva nastale upotrebom IoT tehnologije.....	46
3.3. Modeli proizvoda osiguranja upotrebom IoT tehnologije.....	50
4. Pregled tržišta u Republici Hrvatskoj	51
4.1. Pregled proizvoda.....	51
4.1.1. CO Iskon SmartHome	51
4.1.2. Croatia kasko osiguranje brodica i jahti.....	52
4.1.3. Uniqa Smart kasko	53
4.1.4. LaqoPrevent	54
4.1.5. Toyota FHI kasko osiguranje	56
4.1.6. CroatiaFIT.....	57
4.2. Analiza proizvoda.....	59
5. Pregled tržišta u zemlji Europske unije.....	63
5.1. Pregled proizvoda.....	63
5.1.1. Assicurazioni Generali	64
5.1.2. UnipolSai	65
5.1.3. Intesa Sanpaolo.....	66

5.1.4.	Allianz.....	67
5.1.5.	Cattolica Assicurazioni	67
5.1.6.	Reale Mutua Assicurazioni.....	68
5.2.	Analiza proizvoda	69
6.	Zaključak.....	72
7.	Popis literature.....	74

1. Uvod

Za industriju osiguranja već se desetljećima govori da je tradicionalna i da ne prati trendove koji se tiču želja kupaca novijih generacija te da zaostaje u usvajanju tehnoloških inovacija.

Zadnjih godina svjedoci smo ubrzane digitalizacije i uvođenja novih tehnologija na svim razinama i u svim industrijama. Na ubranu digitalizaciju nije imun niti, inače konzervativni, financijski sektor. Tradicionalna industrija osiguranja se transformira pod utjecajem izraženih tehnoloških promjena i pojave novih tržišnih konkurenata. Kako bi adekvatno reagirali na promjene i ubranu pojavu novih igrača na tržištu, tradicionalni osiguratelji moraju na vrijeme prepoznati i odgovoriti na suvremene trendove u osiguranju. Suvremeni trendovi predstavljaju značajan izazov za ovu povijesno konzervativnu industriju, uslijed redefiniranja svih procesa u lancu vrijednosti osiguranja - od razvoja proizvoda do upravljanja štetama.¹

S razvojem digitalizacije i novih tehnologija industrija osiguranja omogućila je uvođenje novih prodajnih kanala, razvoj novih proizvoda i naprednih usluga prilagođenih zahtjevima korisnika. Razvoj tehnologije i novih usluga omogućuju društvima za osiguranje opstanak na tržištu i povećanje tržišnog udjela.²

Razvoj novih usluga omogućile su tehnološke inovacije kroz suradnju manjih specijaliziranih poduzeća (start up) za razvoj takvih proizvoda s osiguravajućim društvima. Jedna od prednosti tehnoloških inovacija je omogućavanje prikupljanja podataka od osiguranika i iz okoline u kojoj živimo, a na temelju kojih se mogu vrednovati rizici, određivati cjenici, određivati segmentacija osiguranika, predviđati trendovi i kreirati nove vrste proizvoda i modela osiguranja. Pomoću tehnologije i prikupljenih podataka moguće je osvijestiti i upozoriti osiguranika o potencijalnim opasnostima i time spriječiti štetne događaje na obostranu korist osiguranika i osiguravatelja.³

¹ Zdrilić M, <https://sinvest.com.hr/clanak/14>, Suvremene promjene i digitalizacija u industriji osiguranja

² Marović B., Njegomir V., Novi trendovi koji transformiraju osiguranje i reosiguranje; <http://sors.ba/UserFiles/file/SorS/2022/Zbornik/01%20Sors%202022%20-%20Zbornik%20radova%20-%20Marovic.pdf>

³ Mihelja Žaja M., Milanović Glavan Lj., Grgić M., Digitalna tehnologija kao čimbenik razvoja kanala distribucije u osiguranju; <https://hrcak.srce.hr/242255>

Razvoj novih tehnologija nosi i rizik osiguravajućim društvima. Osim tehnoloških izazova i kibernetičkih prijetnji, mijenjaju se i zahtjevi kupaca, tradicionalni modeli poslovanja su pod pritiskom i pojavljuju se novi igrači na tržištu.

Većina klijenata su spremni podijeliti svoje podatke ako će to za njih značiti potencijalnu mogućnost uštede za njihove police osiguranja, a IoT (Internet of Things) je tehnologija koja omogućuje takvo dijeljenje podataka. Društva za osiguranje mogu koristiti podatke iz IoT uređaja kao što su uređaji za pametni dom, automobilske senzori, senzori na plovilima, pametni nosivi uređaji. Na temelju tih podataka mogu kreirati i nove proizvode.⁴

Cilj ovog rada je dati pregled IoT tehnologije, njenog razvoja i tehnoloških i aplikativnih izazova. Dati pregled mogućnosti i prilika za primjenu u industriji osiguranja. Napraviti analizu i ustanoviti kako se IoT tehnologija koristi na tržištu osiguranja u Republici Hrvatskoj i u jednoj od članice Europske unije. Pregled ćemo napraviti analizom literature, stručnih članaka i radova, časopisa i javno dostupnih podataka na Internetu.

U drugom poglavlju rada detaljnije ćemo opisati IoT tehnologiju. Opisat ćemo razvoj IoT tehnologije kroz povijest, pregled IoT arhitekture, vrste senzora i protokole koji se upotrebljavaju u IoT tehnologiji te najčešće izazove s kojima se susrećemo prilikom primjene IoT tehnologije.

U trećem poglavlju navesti ćemo mogućnosti primjene IoT tehnologije. Opisat ćemo prednosti i nedostatke IoT tehnologije, primjere IoT tehnologije, navest ćemo koje su koristi korištenja IoT tehnologije za osiguravajuća društva, kako se IoT tehnologija primjenjuje u industriji osiguranja i koji su mogući načini izlaska na tržište za osiguravajuća društva.

Četvrto i peto poglavlje prikazat će analizu primjene IoT tehnologije u industriji osiguranja na tržištu Republike Hrvatske i jedne zemlje Europske unije (Italija).

Na kraju rada je zaključak o potencijalima IoT tehnologije, usporedbi tržišta u Republici Hrvatskoj i Italiji, te budućnosti IoT u industriji osiguranja.

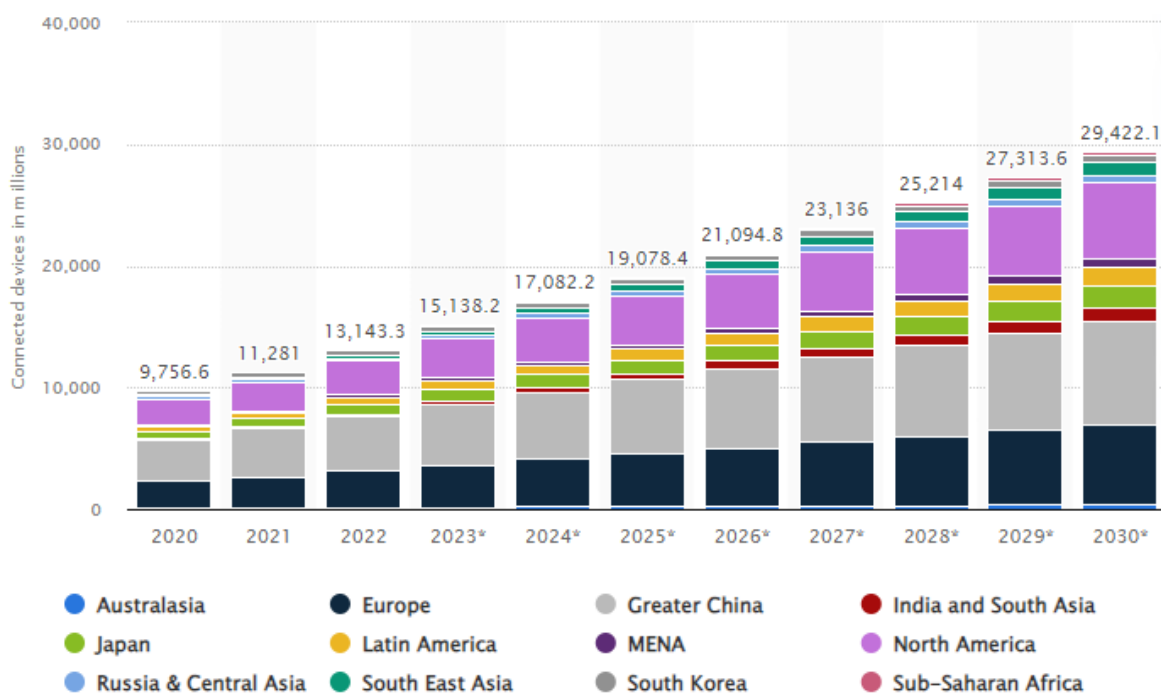
⁴ Marović B., Njegomir V., Novi trendovi koji transformiraju osiguranje i reosiguranje; <http://sors.ba/UserFiles/file/SorS/2022/Zbornik/01%20Sors%202022%20-%20Zbornik%20radova%20-%20Marovic.pdf>

2. IoT tehnologija

2.1. Definicija IoT tehnologije

Ne postoji jedinstvena definicija što je to IoT i one se razlikuju ovisno o perspektivi iz koje se promatraju i širini pogleda na procese koji se događaju, ali većina se odnosi na spajanje uređaja koje koristimo svakodnevno na internetu u svrhu mjerenja, prikupljanja, pohrane i razmjene podataka s ostalim „stvarima“ i ljudima. IoT daje mogućnost automatiziranja velike većine poslova i svakodnevnih aktivnosti. IoT uređaj može biti doslovno svaki uređaj u stvarnom životu, od osobnog računala, pametnih telefona, automobila, strojeva, kućanskih aparata pa do vrata, prozora, namještaja i svega ostalog što čovjek može zamisliti.⁵

Prema istraživanjima broj povezanih uređaja će do 2030. godine dosegnuti 30 milijardi. Slika 2-1. prikazuje razdiobu broja uređaja po kontinentima u razdoblju od 2020. do 2030. godine.⁶



Slika 2-1. Broj povezanih IoT uređaja od 2020. do 2030. godine

⁵ <https://www.cert.hr/sigurnost-interneta-stvari-IoT/>

⁶ <https://www.statista.com/statistics/1194677/IoT-connected-devices-regionally/>

Svrha IoT-a je prikupljanje i dijeljenje informacija. IoT uređaji rade po sljedećem principu: ⁷

1. Pametni uređaji skupljaju i prosljeđuju podatke pomoću interneta ostalim uređajima.
2. Podaci su analizirani centralno u data centrima i cloud servisima.
3. Završne informacije i instrukcije koje su temeljene na analizi podataka, vraćaju se drugim IoT uređajima.

2.2. Razvoj IoT tehnologije kroz povijest

Termin IoT ⁸ je definiran 1999. godine od strane računalnog znanstvenika Kevina Ashtona. Dok je radio u Procter & Gambleu Ashton je predložio stavljanje čipova za radiofrekvencijsku identifikaciju (RFID) na proizvode kako bi ih pratili kroz opskrbni lanac.

Tijekom 2002. godine Walmart i Ministarstvo obrane SAD-a bili su prve velike organizacije koje su prihvatile Ashtonov model praćenja stvari pomoću RFID-a.

2008. godine broj uređaja spojenih na Internet prestigao je broj svjetske populacije.

2012. godine Švicarska je započela pilot program imena „Smart City Switzerland“ gdje se gradovi povezuju putem Interneta te im se omogućava :

- Praćenje prometa - Praćenje i izvješćivanje o prometu u stvarnom vremenu.
- Praćenje kvalitete zraka - Integrirani IoT senzori mogu identificirati zagađivače.
- Pametan prijevoz - Pametni semafori koji pojednostavljaju učinkovitost prometa i javnog prijevoza.
- Pametno parkiranje - Senzori ugrađeni u kolnik koji omogućuju određivanje zauzetosti parkirališta.
- Pametna javna rasvjeta - Niskoenergetska rasvjeta u kombinaciji s mjerenjem vremena i sensorima.

⁷ <https://duplico.io/sto-je-IoT-ili-internet-of-things/>

⁸ <https://www.dataversity.net/brief-history-internet-things/>

2015. godine pametni telefoni postaju dio IoT zajednice. Povezuju se pametni telefoni, pametni satovi, pametne narukvice u svrhu slanja informacija za zdravstvenu industriju. Automobili i kamioni posjeduju veliku količinu senzora i tehnologije. Maksimalnim korištenjem ovih tehnologija, tvrtke mogu izvući informacije iz svojih voznih parkova o zahtjevima održavanja, uvjetima vožnje i rutama u stvarnom vremenu.

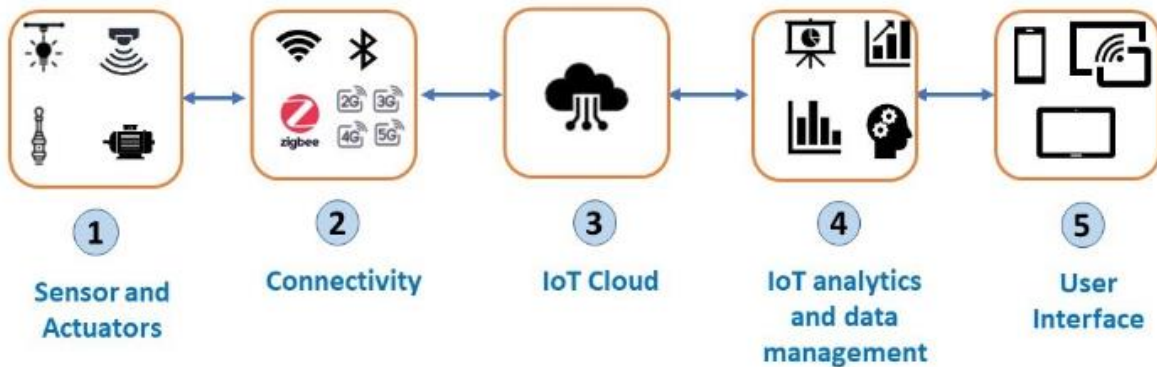
2021. godine pojavljuju se samovozeći automobili koji koriste podatke iz senzora, s podacima o prometu, kartama, vremenskoj prognozi, uvjetima na cesti itd. Korištenje tih podataka sa senzora pomaže vozilima da nadziru svoju okolinu i donose bolje odluke.

IoT tehnologija već danas omogućava mnogobrojne mogućnosti povezivanja senzora i uređaja, a možemo samo zamišljati kako će to izgledati u budućnosti. Povezivanje mijenja način na koji ljudi koriste automobile i domove. IoT tehnologija ima široki raspon primjene u osiguravajućoj industriji te može preoblikovati način na koji osiguravajuća društva rade, procjenjuju rizike i određuju cijene proizvoda.⁹

2.3. IoT arhitektura

IoT ima veliki broj senzora i aplikacija i korištenje IoT raste velikom brzinom. Ovisno o različitim područjima primjene IoT-a, funkcionira u skladu s načinom na koji je dizajniran ili razvijen i nema standardno definiranu arhitekturu. Arhitektura IoT-a ovisi o funkcionalnosti i implementaciji u različitim sektorima. Ipak, postoji osnovna arhitektura i tok procesa na temelju kojeg se IoT gradi. Slika 2-2. prikazuje logičku arhitekturu IoT sustava.

⁹ <https://www2.deloitte.com/tr/en/pages/financial-services/articles/innovation-in-insurance-internet-of-things-IoT.html>



Slika 2-2. Arhitektura IoT sustava¹⁰

Arhitektura IoT sustava sastoji se od 5 slojeva, to su:

1. **Sloj senzora** – zadužen za prikupljanje podataka iz uređaja i senzora. Sloj uključuje senzore koji su smješteni u okolišu, uređajima, vozilima, strojevima, itd.... Senzori prikupljaju različite podatke kao što su temperatura, tlak, visina, brzina, protok, svjetlost, zvuk, otkucaji srca te razne druge parametre. Senzori pretvaraju prikupljene podatke u formate pogodne za računalnu obradu. Senzori mogu biti analogni ili digitalni.
2. **Mrežni sloj** – odgovoran je za pružanje komunikacije i povezanosti između uređaja u IoT sustavu. Mrežni sloj uključuje protokole i tehnologije koje omogućuje uređajima povezivost i međusobnu komunikaciju putem Interneta. Povezanost može biti implementirana preko žice ili bežičnim načinom, ovisno o specifičnim potrebama aplikacija. Najčešći korišteni mrežni protokoli u IoT tehnologiji su WiFi, Bluetooth, Zigbee, RFID/NFC te mobilni mrežni protokoli 3G, 4G i 5G. Izbor protokola može ovisiti o udaljenosti ili tehničkim ograničenjima uređaja. Dodatno, mrežni sloj može uključivati usmjerivače (*Router*) i pristupnike (*Gateway*) kojima je uloga povezivanje između uređaja, senzora i sloja spremišta podataka te uređaje kojima je uloga pružanje sigurnosnih mehanizama kao što su šifriranje, autentikacija, a u svrhu zaštite podataka i neovlaštenog pristupa podacima.
3. **Sloj spremišta podataka (IoT Cloud)** – odgovoran za upravljanje i organizaciju podataka prikupljenih iz mrežnog sloja u svrhu prebacivanja podataka u četvrti sloj. U

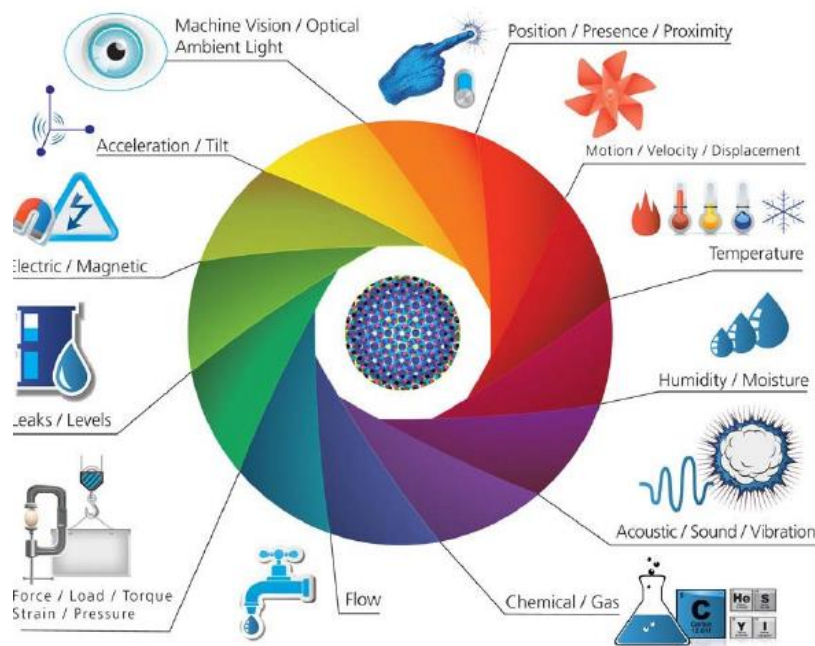
¹⁰ <https://www.youtube.com/watch?v=yMdTgsqWGAA>

sloju spremišta podataka podaci se obrađuju te je odgovoran za analitiku nad prikupljenim podacima. Umjesto korištenja IoT Clouda podaci se mogu obrađivati i lokalno ovisno o potrebama aplikacija koji se naslanjaju na podatke.

4. **Sloj analitike i upravljanja podacima** – primarno zadužen za operacije nad podacima uključujući ekstrakciju podataka, analitiku nad podacima, agregaciju podataka, klasifikaciju podataka. Sloj analitike ima ključnu ulogu u transformaciji sirovih podataka u korisne informacije nad kojima se mogu donositi odluke za buduće radnje. Analitika nad podacima uključuje algoritme i modele strojnog učenja koji mogu napraviti predikciju ponašanja, proaktivno planirati radnje, itd.
5. **Sloj korisničkog sučelja** – omogućuje krajnjim korisnicima praćenje i kontrolu nad uređajima kroz funkcionalnosti kao što su obavijesti, upozorenja, daljinsko upravljanje, slanje naredbi i uputa. Obradeni podaci, radnje i trendovi su prikazani krajnjim korisnicima kroz aplikacije i korisnička sučelja, pružajući im intuitivne kontrole i vizualnu reprezentaciju podataka.

2.4. IoT senzori

IoT senzori su jedna od najvažnijih karika u IoT arhitekturi. IoT senzori su uređaji koji mjere neku veličinu. Senzor radi na način da dobiva fizički poticaj i pretvara ga u signal prikladan za obradu. Izlaz senzora je signal koji se nakon obrade pretvara u oblik čitljiv ljudima kao što su promjene karakteristika, promjene otpora, promjena kapaciteta, temperature, gibanja, itd... Slika 2-3. prikazuje najčešće vrste senzora.



Slika 2-3. IoT senzori¹¹

Vrste senzora ¹²:

1. **Senzor temperature** – mjeri količinu topline koju stvara neko područje ili predmet. Oni otkrivaju promjenu temperature i pretvaraju nalaze u podatke. Senzori temperature koriste se u raznim industrijama, uključujući proizvodnju, zdravstvo i poljoprivredu.
2. **Senzor blizine** – radi na principu otkrivanja koliko je neka komponenta blizu ili daleko od položaja senzora. Senzori blizine otkrivaju prisutnost ili odsutnost objekata u blizini senzora bez fizičkog kontakta. Emitiraju snop zračenja poput infracrvenog ili elektromagnetskog polja. Senzori blizine uobičajeni su u maloprodajnim objektima, industrijskim kompleksima i parkiralištima.
3. **PIR (pasivni infracrveni senzor)** – može detektirati ili emitirati infracrveno zračenje. Koriste se za otkrivanje pokreta ili gibanja u okolnom području.

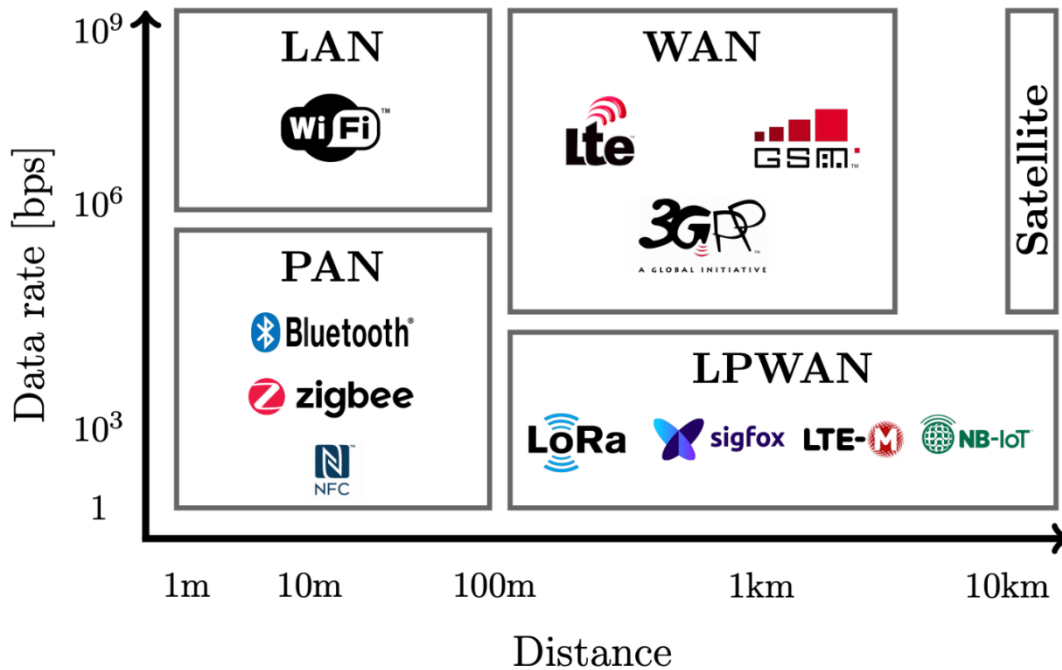
¹¹ <https://www.embedded.com/sensor-systems-in-the-industrial-IoT/>

¹² <https://www.theIoTacademy.co/blog/sensor/>

4. **Plinski i kemijski senzori** - nadziru kvalitetu zraka na prisutnost otrovnih ili opasnih plinova. Obično se koriste u industrijskim i proizvodnim postavkama. U domaćinstvima se koriste u detektorima ugljičnog monoksida.
5. **Senzor tlaka** – otkrivaju promjene u plinu ili tekućini. Senzori mjere tlak i raspon tlaka unutar postavljenih granica. Ovaj senzor nalazi se i u mobitelima, pametnim satovima i GPS navigacijskim uređajima. Vozila koriste ove senzore za nadzor tlaka u gumama te javljaju kada je tlak prenizak.
6. **Senzor dima** – otkriva prisutnost dima i vatre. Učestalo se koriste u poslovnim i stambenim objektima.
7. **Žiroskop** – senzor žiroskopa mjeri brzinu rotacije oko osi. Koristi se za navigaciju u pametnim mobitelima, dronovima i u auto industriji.
8. **Senzor slike** – pretvara slike u signale. Nalazi se u kamerama, radarima, sonarima, biometrijskim uređajima, opremi za noćno gledanje i u automobilima.
9. **Senzor vlage** – mjeri količinu vlage u zraku. Koristi se u sustavima grijanja, klimatizacije i praćenja atmosfere.
10. **Akcelerometar** – detektira promjenu brzine objekta, uključujući dodir, protresanje, nagnjanje i pozicioniranje. Koristi se za pedometre, zaštitu od krađe i nadzor voznih parkova. Nalazi se u zrakoplovima, pametnim telefonima, računalima, kamerama, strojevima za pranje rublja, navigacijskim uređajima.
11. **Senzor razine** - otkriva razinu tvari, kao što su prah, čvrsti materijal i tekućine. Detektiraju razinu tekućine u spremniku ili razinu količine otpada u kontejneru.
12. **Optički senzor** – mjere svjetlo i pretvaraju ga u električni signal.
13. **Senzor dodira** – radi na principu detekcije fizičkog podražaja, kao što je dodir prsta ili olovke.
14. **Senzori brzine** – koriste se za mjerenje brzine bilo kojeg objekta u pokretu ili vozila.

2.5. IoT protokoli

Postoji nekoliko vrsta IoT protokola ovisno o njihovoj namjeni i dometu. Većina IoT uređaja su malih dimenzija, rade na niskom naponu, imaju malu memoriju te su stoga razvijeni posebni protokoli koji omogućuju prijenos podataka. Slika 2-4. prikazuje protokole koji se koriste u IoT tehnologiji.



Slika 2-4. IoT protokoli¹³

IoT protokole prema doseg radijske komunikacije možemo podijeliti u tri kategorije:

1. **Protokoli kratkog dosega** – primjer ovog protokola je **Bluetooth**. Bluetooth ima kratki radni domet, ali zato mu je mala potrošnja energije, između 5 do 50 mA. Bluetooth je najčešće korišteni protokol u nosivim uređajima, pametnim uređajima i za jeftine senzore u okolišu, koji mogu prenijeti podatke središnjem uređaju koji djeluje kao pristupnik. Bluetooth protokol omogućuje dugo trajanje baterije na uređajima i

¹³ <https://emanuelepagliari.it/2020/10/13/internet-of-things-wireless-communication-protocols/>

senzorima. Brzina prijenosa podataka je između 1-3 Mbit/s, ovisno o Bluetooth standardu. Domet Bluetooth komunikacije je do 30 metara bez prepreka.¹⁴

2. **Protokoli srednjeg dosega** – primjeri ovog protokola su Wi-Fi protokol i ZigBee protokol. Protokoli srednjeg dometa mogu biti korišteni za bežične lokalne mreže. Ovi protokoli mogu se koristiti na udaljenostima između 10 i 100 metara bez prepreka.

Wi-Fi protokol je vrlo zastupljen i nalazi se u gotovo svakom pametnom uređaju. Glavne prednosti Wi-Fi protokola su visoka rasprostranjenost i integracija između uređaja, ali prije svega veliki prijenosni kapacitet (do 300 Mbit/s), niska latencija i veliki doseg dovoljan da pokrije stambenu kuću s jednom pristupnom točkom. Wi-Fi komunikacija lako može doseći 50 metara s preprekama i zidovima. Bez prepreka i zidova doseg može biti i do 100 metara. Najveći nedostatak Wi-Fi protokola je velika potrošnja energije (između 10-50mA), što nije pogodno za IoT aplikacije.

ZigBee protokol - Osmišljen je 2004. godine kao alternativa za Wi-Fi i Bluetooth protokole za aplikacije niske potrošnje energije. U usporedbi sa Wi-Fi troši malo energije za rad, što im omogućuje da se godinama napajaju baterijama. ZigBee protokol ima mali prijenosni kapacitet (20-250 Kbit/s), nedovoljan za prijenos podataka između multimedijских uređaja, ali dovoljan za IoT aplikacije. Doseg ZigBee-a je do 200 metara. Zbog svojih karakteristika ZigBee se upotrebljava umjesto Bluetooth protokola. ZigBee se često koristi u velikim IoT mrežama i ima veliku primjenu u gospodarstvu i industriji.¹⁵

3. **Protokoli dugačkog dosega** – često se upotrebljavaju kako bi se kreirala Low Power Wide Area Networks (LPWAN) čiji je doseg između 300 metara do 10 kilometara. Ovi protokoli mogu se oslanjati na postojeće mobilne mreže s mnogo čvorova koji se nalaze desecima kilometara međusobno udaljenih ili na postojeću besplatnu mrežu otvorene arhitekture.¹⁶

¹⁴ <https://www.videostrong.com/news-show/wifi-zigbee-ble-for-smart-home>

¹⁵ <https://www.nabto.com/guide-IoT-protocols-standards/>

¹⁶ <https://emanuelepagliari.it/2020/10/13/internet-of-things-wireless-communication-protocols/>

LoRa protokol – može imati doseg od nekoliko stotina metara do 10 kilometara. LoRa je baziran na otvorenoj arhitekturi te je zato jedan on najpoznatijih i najkorištenijih LPWAN protokola. LoRa mreža ima definirana pravila u pogledu broja i vremenskog odmaka slanja podataka koja se moraju poštivati za korištenje mreže.

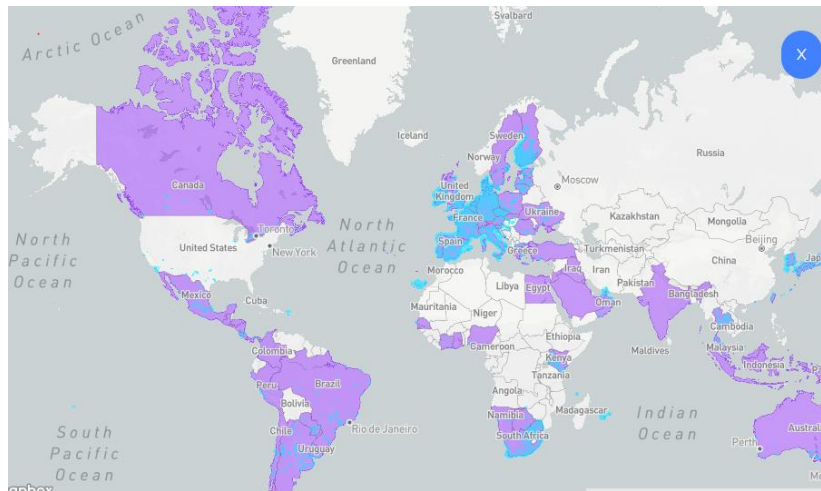
NB-IoT protokol – razvijen je za povezivanje IoT aplikacija male snage i niske cijene. Uređaji koji koriste ovaj protokol mogu se napajati preko baterije. Primjer takvog uređaja je pametno brojilo. Protokol je jeftin za implementaciju budući da se oslanja na postojeću LTE infrastrukturu radio baznih stanica.

LTE-M protokol – koristi se uglavnom uz mobilne uređaje i usluge. Kako bi se smanjila potrošnja energije uređaja brzina prijenosa podataka je bitno smanjena. Jedna od glavnih prednosti LTE-M u odnosu na NB-IoT i LoRa je mogućnost većeg prijenosa podataka (do 7 Mbit/s) zbog korištenja mobilne tehnologije koje pruža LTE mreža. Ali je zato i cijena veća jer zahtijeva ugovor s mobilnim operaterom. LTE-M uređaji imaju i veću potrošnju energije od NB-IoT i LoRa protokola.

5G protokol – očekuje se da će široka primjena 5G protokola uvesti revoluciju u IoT svijet omogućujući povezivanje velikog broja uređaja. 5G mreža prilagođena je IoT zahtjevima i pruža 1.000 do 5.000 puta više kapaciteta od 3G mreže, omogućuje brzine od 10 do 100 Gbps. Kombinacija vrlo niske latencije s velikom pokrivenošću podržati će povezivanje velikog broja uređaja. Očekuje se brzi razvoj pametnih gradova, aplikacija za poljoprivredu, povezivanje automobila, kamiona, dronova, ali i usluge analize podataka u stvarnom vremenu velikih količina podataka.

Sigfox – je globalna bežična mreža nastala 2009. godine. Sigfox služi za povezivanje IoT uređaja male snage, a koji trebaju biti neprekidno uključeni i emitirati male količine podataka. Sigfox omogućuje dvosmjernu komunikaciju, koju uvijek inicira uređaj. Svaka zemlja ima Sigfox partnera koji izgrađuje mrežu. Mrežni uređaji obično se postavljaju na postojeće bazne stanice mobilnih operatera. Signal se može koristiti za jednostavno pokrivanje velikih područja. SigFox mreža je izgrađena u više od 70 zemalja. Za razliku od 5G protokola koji omogućava prijenos multimedije, SigFox je

specijaliziran i podržava samo kratke poruke i malu količinu podataka.¹⁷ Slika 2-5. prikazuje pokrivenost SigFox protokola u svijetu.



Slika 2-5. Sigfox pokrivenost¹⁸

2.6. Izazovi primjene IoT-a

Iako se IoT koristi već duže vrijeme i transformirala je mnoge industrije, primjena IoT suočava se s mnogim izazovima. Korištenje IoT konstantno raste i milijarde uređaja su povezane diljem svijeta. Osim što je IoT otvorio vrata mnogim novim mogućnostima, donio je i nove izazove programerima, proizvođačima opreme i kupcima koji se oslanjaju na njihove proizvode i usluge. Iako izazovi prilikom primjene IoT-a postoje od samih početaka, oni su sve izraženiji kako IoT postaje rašireniji, pristupačniji i jednostavniji za korištenje. U nastavku ćemo pobrojati glavne izazove u korištenju IoT tehnologije.¹⁹

1. **IoT sigurnost i zaštita podataka** – od samog početka primjena IoT-a ima izazova s računalnim napadima. IoT uređaji su malih dimenzija, napajanje imaju preko baterija, pa svi napredni mehanizmi poput dodavanja enkripcije, autentifikacije, uvođenje naprednih sigurnosnih protokola, mogu drastično utjecati na potrošnju energije tih

¹⁷ G. Dregvaite; R. Damasevicius (30 October 2016). Information and Software Technologies: 22nd International Conference, ICIST 2016

¹⁸ <https://www.sigfox.com/coverage/>

¹⁹ <https://www.emnify.com/blog/IoT-challenges-2023>

uređaja pa se oni često ne uvode. Kako je sigurnost i zaštita podataka najveći izazov u primjeni IoT tehnologije, u nastavku rada dodatno ćemo se osvrnuti na problematiku IoT sigurnosti.

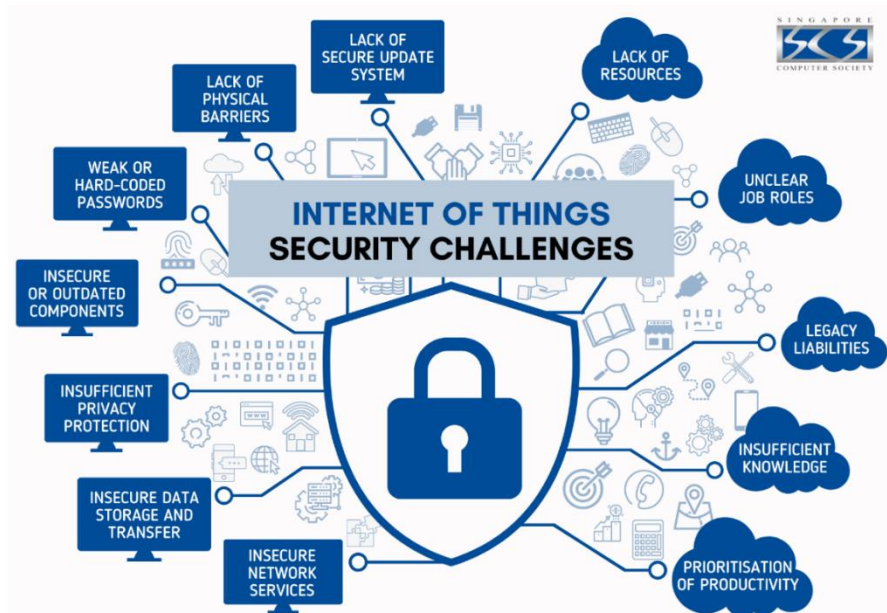
2. **Pokrivenost** – IoT uređaji trebaju biti povezani na mrežu za slanje i primanje podataka. Ako IoT uređaj izgubi povezanost na mrežu, uređaj neće raditi. Iako postoji više načina mrežnog povezivanja, svaki od njih ima različit spektar pokrivenosti. Npr, ako odaberemo WiFi kao način za povezivanje, IoT uređaji mogu raditi samo u doseg u smjerivača, odnosno samo na lokaciji gdje imamo pokrivenost s WiFi signalom. Ako želimo pričuvno rješenje, moramo dodatno uložiti ili platiti za neka od rješenja s kojima ćemo imati pokrivenost, kao što su mobilna mreža, Sigfox, LoRa ili preko satelita.
3. **Skalabilnost** – velike IoT instalacije podrazumijevaju veliki broj uređaja. Kako tvrtke rastu, raste i broj povezanih IoT uređaja, a koji su povezan na različite načine. Svaki od IoT uređaja može biti temeljen na različitim tehnologijama, operacijskim sustavima za upravljanje. Što je veći opseg različitih IoT uređaja u jednoj organizaciji teže je upravljati takvim heterogenim okruženjem. Operativna podrška, praćenje i logistika postaju sve veći problem. Ovaj problem odnosi se i na povezivanje putem mobilne mreže jer je potrebno uspostaviti roaming ugovore s više telekomunikacijskih tvrtki.
4. **Interoperabilnost** – jedna od karakteristika IoT tehnologije je što se IoT okruženje može definirati na mnogo načina i konfigurirati prema jedinstvenim potrebama korisnika. Ova karakteristika ujedno predstavlja i veliki izazov jer nisu sva IoT rješenja međusobno kompatibilna. Dodavanje novog uređaja, novog hardvera ili softvera u postojeće okruženje može zahtijevati lančani niz promjena i prilagodbu novoj tehnologiji kako bi se zadržale postojeće funkcionalnosti. Drugi izazov je upotreba tehnologije otvorenog koda. Često uređaji i tehnologije otvorenog koda nisu kompatibilni s drugim uređajima jer ne postoji međunarodno regulatorno tijelo koje bi stvorilo jedinstvenu normu. Ovaj problem posebno je izražen u međunarodnom poslovanju ili u poslovanju s različitim tvrtkama koje koriste varijacije otvorenog koda. Trend u IoT industriji je da IoT rješenja ipak budu što je više moguća kompatibilna.
5. **Širina frekvencijskog pojasa (Bandwith)** – kako raste broj IoT uređaja javlja se izazov prilikom korištenja frekvencijskog pojasa. Kada previše uređaja koristi iste frekvencijske pojase na istoj lokaciji, njihovi signali međusobno interferiraju. Primjer za to je WiFi u stambenim zgradama. Budući da su uređaji međusobno smješteni vrlo

blizu, njihovi signali mogu se lako ometati. U IoT također postoje slučajevi gdje su tisuće međusobno povezanih uređaja na malom prostoru pa se mogu javljati smetnje i nedostupnost usluge.

6. **Trajanje baterija na IoT uređajima** – većina IoT uređaja je malih dimenzija pa stoga imaju male baterije za napajanje. Velike baterije nisu pogodne za IoT uređaje jer mogu ograničiti njihovu uporabu, odnosno utjecati na postavljanje i ugradnju. Baterija na IoT uređajima može trajati godinama, ali samo ako IoT uređaj u redovnom radu troši minimalnu energiju. Prečesto odašiljanje ili primanje podataka tijekom duljeg razdoblja pojačano troši bateriju stoga treba optimizirati rad IoT uređaja. Veliki ulogu u trajanju baterije imaju usmjerivači i pristupnici na način da oni djeluju kao posrednici između IoT uređaja, aplikacija i mrežnih čvorova s kojima komuniciraju. Usmjerivači i pristupnici mogu obavljati sigurnosne mehanizme, kao što su enkripcija i autentifikacija, osiguravajući time manju potrošnju baterije na IoT uređajima.
7. **Visoki početni troškovi** – uvođenje u IoT sustav zahtijeva visoka početna ulaganja. Potrebna je nabava različitih hardverskih i softverskih komponenti, te stručnjaci koji će raditi na tim tehnologijama. Na početku implementacije neophodno je napraviti procjenu troškova cijelog projekta i isplativost samog projekta i ulaganja.
8. **Analiza podataka** – najvažniji dio IoT sustava je analiza nad prikupljenim podacima. Ključna svrha svakog IoT sustava je prikupljanje podataka s uređaja i senzora. Bez analize tih podataka IoT sustav ne bi imao smisla. Prikupljeni podaci u sirovom obliku imaju malu vrijednost pa ih je za izdvajanje važnih informacija potrebno obraditi. Za obradu podataka potrebno je implementirati platformu za analizu velikih količina podataka.

2.7. Sigurnosni izazovi primjene IoT-a

Kako raste broj povezanih IOT uređaja, rastu i sigurnosni izazovi koji se javljaju u uvođenju i održavanju. U nastavku ovog poglavlja obradit ćemo neke od najvažnijih sigurnosnih izazova primjene IoT tehnologije ²⁰. Slika 2-6. prikazuje najčešće IoT sigurnosne izazove.



Slika 2-6. Sigurnosni izazovi primjene IoT-a ²¹

1. **Nedostatak normi** – odnosi se na različitost u korištenju IoT uređaja i opreme. Ukoliko se koriste IoT uređaji koji nisu međusobno kompatibilni, mogu se javljati pogreške u komunikaciji prilikom razmjene informacija. Nedostatak normi u IoT uređajima otežava i onemogućuje njihovu primjerenu zaštitu. Manjak normi može dovesti do ranjivosti koje napadači mogu iskoristiti. Kako bismo smanjili rizike, potrebno je usvajanje industrijskih normi i protokola za IoT uređaje koji će omogućiti interoperabilnost i kompatibilnost ili korištenje certificirane opreme. To uključuje i norme za sigurnost uređaja, privatnost podataka ,te usvajanje ostalih sigurnih komunikacijskih protokola.

²⁰ <https://www.peerbits.com/blog/biggest-IoT-security-challenges.html>

²¹ <https://www.scs.org.sg/articles/IoT-security-how-to-secure-your-devices>

2. **Autentifikacija** – je postupak koji omogućuje određivanje identiteta nekog subjekta. Autentifikacije u IoT uređajima često ne postoji ili je vrlo slaba. Potrebno je implementirati jake autentifikacijske mehanizme koji će osigurati da samo ovlaštene osobe mogu pristupiti uređajima. Vrlo dobro rješenje za rješavanje autentifikacije je primjena Public Key Infrastructure (PKI) infrastrukture.
3. **Ažuriranje sistemskog softvera** – IoT uređaji rade na sustavima s ograničenim resursima, često imaju baterijsko napajanje, što otežava njihovu zaštitu. IoT uređaji imaju specijalizirani hardver i softver što uvodi dodatne izazove za njihovu zaštitu. Mnogi uređaji više nisu ni podržani od proizvođača, a i dalje se koriste te nije niti moguće primanje sigurnosnih ažuriranja ili zakrpa. Neažurirani softver može otvoriti ranjivosti koji napadači mogu iskoristiti. Potrebno je redovito omogućiti ažuriranje softvera kako bi se osiguralo da uređaj radi s najnovijim verzijama koje u sebi imaju uklonjene sigurnosne propuste.
4. **Nedovoljna mrežna sigurnost** – IoT uređaji često su povezani na Internet koristeći nezaštićene mreže. Na taj način uređaji su izloženi napadačima, koji mogu presresti podatke, ostvariti pristup osjetljivim podacima ili izmijeniti podatke. Kako bismo uklonili ovu opasnost potrebno je implementirati sigurne mrežne protokole kao što su VPN ili HTTPS (koji omogućuju da su podaci preneseni na siguran način).
5. **Fizička zaštita** – uvođenje fizičke sigurnosti na IoT uređajima je dosta komplicirana. Uređaji su ranjivi na fizičke napade kao što su neovlašteno pristupanje uređaju, krađa ili uništavanje. Takvi napadi mogu rezultirati neovlaštenim pristupom osjetljivih informacija, prekidom rada samog sustava ili gubitkom podataka. Kako bismo spriječili takve napade potrebno je uvoditi sigurnosne mjere fizičke zaštite kao što su kamere, brave, zaštićena kućišta ili ograde.
6. **Zaštita podataka** – IoT uređaji prikupljaju velike količine podataka stoga je vrlo važna zaštita podataka. Ti podaci mogu biti vrlo osjetljivi kao što su osobni podaci fizičkih osoba, financijski podaci i drugi osjetljivi podaci. Ako ti podaci nisu ispravno zaštićeni mogu pasti u pogrešne ruke i koristiti se u zlonamjerne svrhe. Kako bi se zaštitili osjetljivi podaci potrebno je uvoditi sigurnosne mehanizme kao što je enkripcija podataka. Enkripcija omogućava da su podaci zaštićeni od napada i da samo ovlaštene osobe imaju pristup tim podacima. Upotreba sigurnih algoritma šifriranja kao što su AES ili RSA omogućiti će sigurnost podataka u mirovanju i prijenosu. Potrebno je i

redovito implementirati ažuriranje softvera s najnovijim sigurnosnim zakrpama. Još jedna važna karika u zaštiti podataka je uvođenje kontrole pristupa podacima, odnosno potrebno je osigurati da samo ovlašteni korisnici imaju pristup podacima.

7. **Zaštita privatnosti** – vrlo je važno voditi računa o zaštiti privatnosti korisnika. Podaci koji se prikupljaju mogu sadržavati osobne podatke kao što su: podaci o lokaciji korisnika, podaci o navikama korisnika, zdravstvene podatke te ostale osjetljive informacije. Ako ti podaci nisu zaštićeni mogu se koristiti u razne zlonamjerne svrhe kao što su: ciljano oglašavanje, krađa identiteta, puštanje podataka u javnost, itd. Kako bismo zaštitili osobne podatke potrebno je implementirati mjere zaštite, kao što su anonimizacija ili pseudoanonimizacija podataka. Ovim postupcima nemoguće je identificirati i povezati pojedince s podacim te time omogućujemo da se podaci ne mogu koristiti u zlonamjerne svrhe. Potrebno je postaviti jasna i transparentna pravila, koja se zovu privole te informirati korisnike o tome kako se podaci prikupljaju, pohranjuju i koriste, s kime se podaci dijele te koje su mogućnosti isključivanja ili brisanja podataka.
8. **Ograničeni regulatorni nadzor** – korištenje IoT uređaja još uvijek nije propisano i definirano u regulatornom nadzoru. Zbog toga je teško osigurati da su ti uređaji sigurni, što predstavlja sigurnosnu prijetnju. Ovu problematiku moguće je riješiti na nekoliko načina. Prvi je razvoj i provedba propisa za IoT uređaje, odnosno potrebno je da zakonodavstvo i regulatorna tijela propišu propise kako IoT uređaji trebaju biti dizajnirani i proizvedeni. U propise treba uključiti određene sigurnosne standarde. Drugi mehanizam je certifikacija IoT uređaja. Certifikacija uređaja može definirati ispunjavanje određenih sigurnosnih standarda. Certifikacija može uključivati certifikate za određene sigurnosne značajke kao što su enkripcija ili autentifikacija ili usklađenost s određenim sigurnosnim standardima kao što je ISO 27001. Treći mogući mehanizam je izrada plana kao odgovora na sigurnosne incidente, oni pomažu u brzom i učinkovitom rješavanju sigurnosnih incidenata ukoliko do njih dođe.
9. **Kontrola i upravljivost** – IoT uređaji su dizajnirani na način da rade u pozadini, bez potrebe za ljudskom interakcijom. IoT uređaj poput pametne kamere može slati podatke na podatkovni server, bez znanja korisnika. Takav način rada i korištenje uređaja bez kontrole može otežati nadzor nad samim uređajima i sprječavanje potencijalne zlonamjerne radnje. Potencijalni napadač može preuzeti i kontrolu nad uređajem bez znanja korisnika i pokrenuti neki kibernetički napad. Potrebno je razviti ili uvesti

mehanizme i alate za nadzor IoT uređaja kako bismo dobili uvid u njegovo ponašanje, kao što su nadzor i mjerenje količine mrežnog prometa, prepoznavanje sumnjivih aktivnosti i praćenje rada uređaja. Također važno je i da uređaji redovito budu nadograđeni sigurnosnim zakrpama te imati plan u slučaju sigurnosnih incidenata.

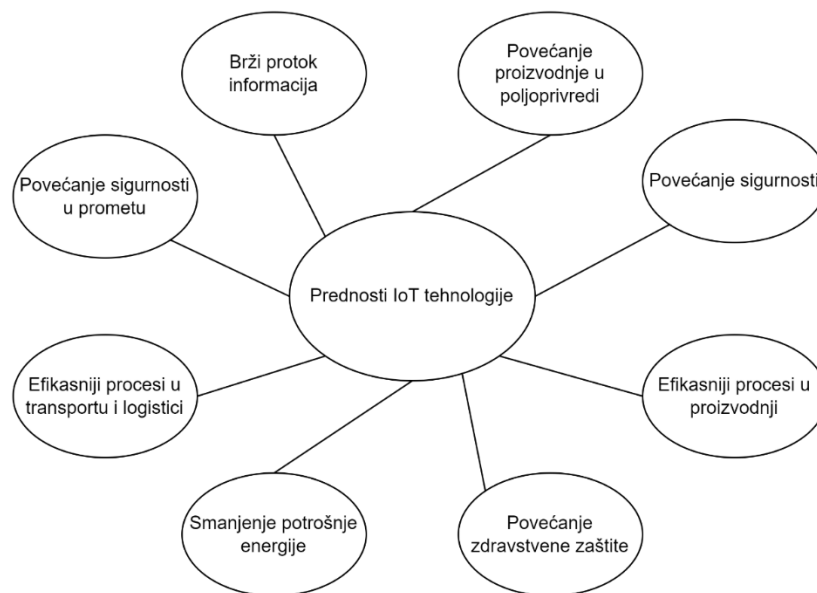
3. Primjena IoT tehnologije

IoT uređaje i aplikacije koristimo u svakodnevnom životu. Neki od primjera IoT-a koje svakodnevno koristimo su: pametni nosivi uređaji, uređaji za praćenje zdravlja, praćenje prometa, praćenje stanja u poljoprivredi, pametni gradovi, itd.

U ovom poglavlju obradit ćemo primjere IoT tehnologije, koristi za osiguravajuća društva koja koriste IoT tehnologiju, primjenu IoT tehnologije u industriji osiguranja i pristupe lansiranju proizvoda u osiguranju upotrebom IoT tehnologije. IoT ima svojih prednosti i nedostataka koji će biti obrađeni u ovom poglavlju.

Prednosti primjene IoT tehnologije²²:

Slika 3-1. prikazuje prednosti koje možemo dobiti primjenom IoT tehnologije.



Slika 3-1. IoT prednosti

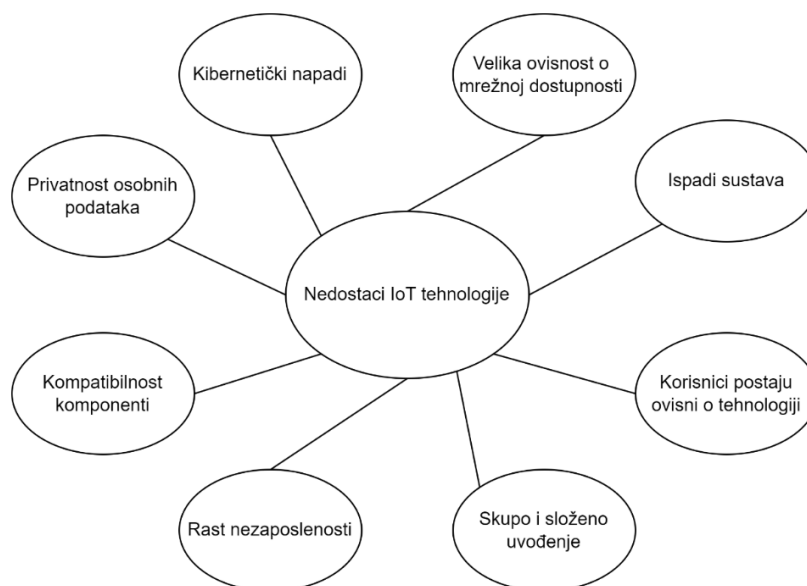
- Pomoću IoT možemo implementirati pametnu kontrolu domova putem mobilnih uređaja. Pametni domovi povećavaju osobnu zaštitu i sigurnost kućanstva.

²² <https://www.geeksforgeeks.org/advantages-and-disadvantages-of-IoT/>

- IoT nudi priliku za automatizaciju procesa i aktivnosti te nam tako štedi vrijeme i resurse. Minimizira se ljudski rad jer IoT uređaji obavljaju zadatke bez potrebe za ljudskom intervencijom.
- Informacije postaju lako dostupne, često se ažuriraju i brzo se prenose te ih možemo dobiti kao obavijesti na mobilnom uređaju.
- Kućanski uređaji izravno su povezani i komuniciraju s upravljačkim računalom, poput mobilnog telefona, što rezultira učinkovitom potrošnjom električne energije. Kao rezultat toga, neće biti nepotrebne upotrebe električne energije.
- IoT uređaji mogu pratiti naše aktivnosti, pružati osobnu pomoć i upozoravati nas na opasne trendove u zdravlju. Skrb za pacijente može se provoditi učinkovitije u stvarnom vremenu bez potrebe za posjetom liječnika. Dobiva se mogućnost donošenja odluka, kao i pružanje skrbi utemeljene na dokazima.
- IoT tehnologija može pomoći u opasnim situacijama ili nezgodama. Sustav u automobilima može identificirati sudar ili nesreću te automatski uputiti poziv nadležnim službama.
- IoT tehnologija u transportu i logistici omogućuje praćenje vozila ili transporta, kontrolu zaliha, isporuka, nadzor i praćenje pojedinačnih narudžbi.

Nedostaci primjene IoT tehnologije: ²³

Slika 3-2. prikazuje IoT potencijalne nedostatke prilikom njenog uvođenja.



Slika 3-2. IoT nedostaci

- Mogućnost kibernetičkih napada. Potencijalni napadači mogu dobiti pristup sustavu i doći do osobnih podataka. Budući da je velika količina IoT uređaja povezana na Internet postoji rizik da se naši podaci zloupotrijebe.
- IoT aplikacije oslanjaju se na Internet i bez njega ne mogu normalno funkcionirati.
- IoT sustavi su vrlo složeni, arhitektura se sastoji od puno komponenata, postoji opasnost da neka od komponenata zakaže što rezultira da nam usluga bude nedostupna.
- Postoji opasnost o prevelikoj ovisnosti korisnika o tehnologiji. Postoji opasnost da naši životi budu previše kontrolirani.
- Prekomjerna uporaba tehnologije u ljudskim životima čini ljude neinteligentnima jer se oslanjaju na tehnologiju, umjesto da sami razmišljaju i obavljaju fizički posao. Nekvalificirani radnici su u velikom riziku od gubitka posla što bi moglo dovesti do nezaposlenosti.
- Uvođenje IoT tehnologije je vrlo skupo i vremenski dugotrajan projekt.

²³ <https://www.geeksforgeeks.org/advantages-and-disadvantages-of-IoT/>

3.1. Primjeri primjene IoT tehnologije

U ovom poglavlju obradit ćemo primjere primjene IoT tehnologije.

3.1.1. Stanovanje (pametni dom)

Pametni dom može se definirati kao kućanstvo opremljeno sensorima, pametnim uređajima, računalnom i informacijskom tehnologijom, koja predviđa i odgovara na potrebe stanara, radeći na promicanju njihove udobnosti, sigurnosti i zabave kroz upravljanje tehnologijom unutar doma i sa svijetom oko sebe.²⁴ U pametnim domovima kamere, senzori vode, dima, pokreta, kućanski aparati, grijanje, rasvjeta, sustavi za zabavu mogu međusobno komunicirati preko središnje jedinice. Ovim uređajima može se udaljeno upravljati, putem mobitela ili drugog uređaja koji je spojen na Internet. Većinu uređaja u sigurnom domu do sada su činili senzori za vodu i dim te sustavi za nadzor. Očekuje se da će se u budućnosti širiti primjena i ostalih senzora. U idealnom slučaju pametni dom je kućanstvo u kojem su svi uređaji povezani i komuniciraju zajedno, međutim najčešće to nije slučaj. Najveća prepreka su još uvijek manjak normi između uređaja različitih uređaja. Za masovno korištenje biti će neophodno pronaći način za usvajanje norma za interoperabilnost uređaja.



Slika 3-3. Pametni dom²⁵

²⁴ <https://www.semanticscholar.org/paper/Smart-Homes%3A-Past%2C-Present-and-Future-Aldrich/34c0fb597f6314cc8a676614358705bece01d112>

²⁵ <https://www.nawy.com/blog/34382-welcome-to-the-future-pros-and-cons-of-smart-homes>

Slika 3-3. prikazuje funkcionalnosti pametnog doma. Senzori i uređaji imaju ili svoje kontrolere ili su povezani na zajednički kontroler preko jednog od protokola za povezivanje (Bluetooth, WIFI, Zigbee), a koji je zatim povezan na Internet. Uređajima možemo upravljati preko aplikacije na mobilnom uređaju.

IoT uređaji u pametnom domu:

Pametni termostat – pomoću pametnog termostata možemo kontrolirati grijanje i hlađenje s bilo koje lokacije. Pametni termostat omogućuje definiranje prilagođenog rasporeda uključivanja i isključivanja grijanja, izvještava o mjesečnoj potrošnji i uštedi energije. Slika 3-4. prikazuje primjer pametnog termostata.



Slika 3-4. Pametni termostat ²⁶

Pametna kamera – je kamera koja donosi odluke na temelju slike. Pametna kamera aktivira se pokretom i snima video scene, detektira kretanje u zadanom području te može aktivirati alarm ili poslati obavijest ako se zadovolje postavljeni uvjeti. Pametne kamere imaju i mogućnost prepoznavanja siluete čovjeka. Već sama prisutnost kamere u domu ili ispred doma imat će pozitivan učinak na odbijanje provalnika. Slika 3-5. prikazuje primjer pametne kamere.

²⁶ <https://exterim.hr/blog/najbolji-pametni-termostati-2019-55/>



Slika 3-5. Pametna kamera ²⁷

Detektor svjetla – je senzor koji možemo spojiti na mrežu pametnog doma, a koji očitava jačinu svjetla čime se može automatizirati rasvjeta. Ukoliko jačina svjetla dosegne neki definirani prag možemo automatski uključiti ili isključiti rasvjetu. Slika 3-6. prikazuje primjer detektora svjetla.



Slika 3-6. Detektor svjetla ²⁸

²⁷ <https://hr.xiaomiplanet.sk/xiaomi-pametna-kamera-c400-globalno/>

²⁸ <https://led-zarulje.com/detektor-pokreta-svjetla-360-bijeli-ip20-st07/>

Pametna rasvjeta – je rasvjeta kojom je moguće definirati vremena automatskog uključivanja i isključivanja svjetla. Ukoliko pametnu rasvjetu povežemo s ostalim uređajima, možemo automatizirati uključivanje rasvjete kada se otvore vrata ili neki prozor. Pametna rasvjeta korisna je iz aspekta osiguranja jer možemo definirati intervale uključivanja svjetla kada nismo u domu, što ima pozitivne aspekte za odbijanje eventualnih nepoželjnih posjetitelja. Slika 3-7. prikazuje primjer pametnog rasvjetnog tijela, kojim se upravlja pametnim telefonom.



Slika 3-7. Pametna rasvjeta ²⁹

Detektor CO – CO je plin bez boje i mirisa i nemoguće ga je osjetiti. Detektor može detektirati CO i može alarmirati ili obavijestiti treću osobu. Ovo je detektor niske cijene, a može spasiti živote ljudima. Detektor dima može detektirati i pojavu dima te tako možemo ugasiti požar u nastajanju. Slika 3-8. prikazuje primjer detektora CO.



Slika 3-8. Detektor CO ³⁰

²⁹ <https://www.svjetlo.hr/pametna-rasvjeta>

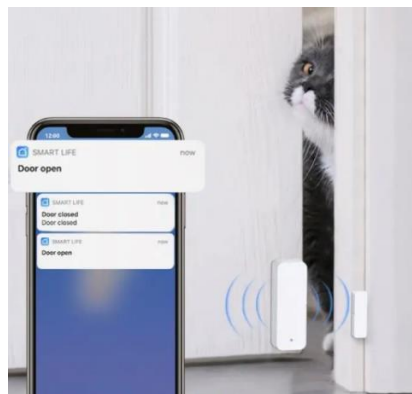
³⁰ <https://www.svijet-svjetiljki.hr/solight-1d39-detektor-dima-i-ugljičnog-monoksida-1-5v-3xaa/>

Pametno zvono – omogućuje nadzor nad vratima. Snima posjetitelje pred vratima i šalje obavijest ukoliko se ispred njih nalazi netko nepoznat. Pametno zvono prepoznaju slike i lica poznatih osoba. Jednom kada se aktivira senzor pokreta zvono šalje isječke filma i obavijesti u realnom vremenu. Pametno zvono možemo integrirati s drugim uređajima tako da možemo i komunicirati s posjetiteljem iako nismo kod kuće. Slika 3-9. prikazuje pametno zvono.



Slika 3-9. Pametno zvono ³¹

Detektor za otvorena vrata/prozore – uređaj koji detektira otvorena vrata ili prozore. Korisnici putem mobilne aplikacije mogu dobiti obavijesti koje će ih upozoriti kada se vrata ili prozori otvore. Kada je detektor povezan s drugim pametnim uređajima, kao što su sigurnosni sustavi ili kamere, može se stvoriti vrlo učinkovit sigurnosni sustav koji će upozoriti korisnika u slučaju neovlaštenog ulaza u dom. Slika 3-10. prikazuje primjer detektora.



Slika 3-10. Detektor za otvorena vrata/prozore ³²

³¹ <https://wiproconsumerlighting.com/products/smart-product/smart-doorbell/wipro-smart-wireless-doorbell-black%C2%A0-2-mp-1080p-full-hd-camera>

³² <https://homemate.co.in/product/door-window-sensor/>

Detektor vode – može otkriti curenje vode u domu ili mogućnost poplave. Detektor vode pruža dodatnu dozu sigurnosti kako bismo zaštitili dom od eventualne štete nastale nekontroliranim curenjem vode. U slučaju detekcije vode, uređaj će nam poslati obavijest putem mobilne aplikacije. Ukoliko detektor vode povežemo s elektromagnetskim ventilom možemo automatski zatvoriti vodu. Slika 3-11. prikazuje primjer upotrebe detektora vode.



Slika 3-11. Detektor vode ³³

Pametna utičnica – može pratiti potrošnju struje u realnom vremenu i možemo odrediti vrijeme uključivanja i isključivanja uređaja koji su na nju priključeni. Pomoću pametne utičnice možemo odrediti vremena uključivanja i isključivanja rasvjete te će provalnici imati dojam da je netko u domu. Slika 3-12. prikazuje primjer pametne utičnice.



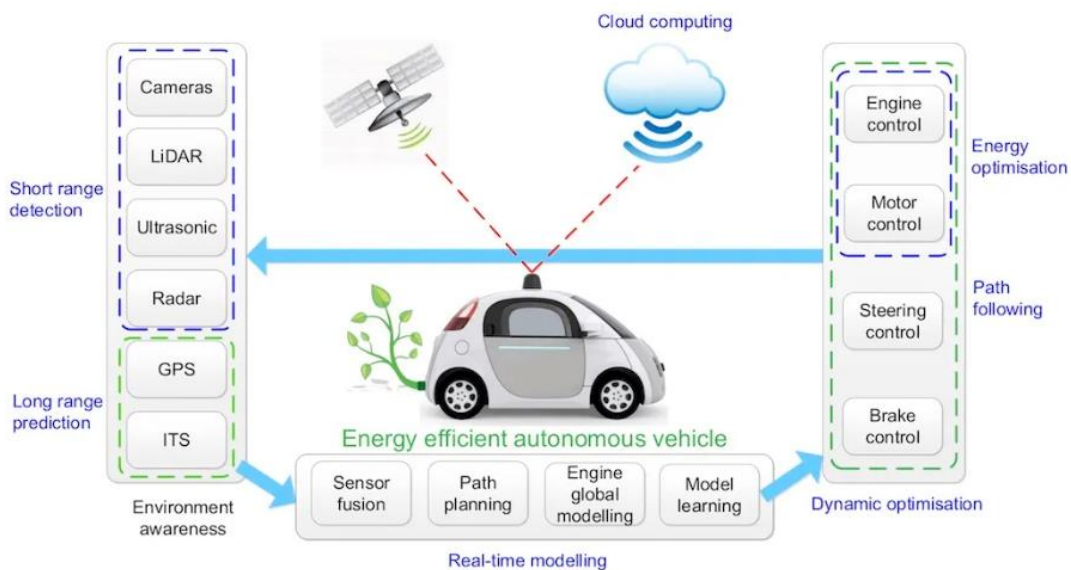
Slika 3-12. Pametna utičnica ³⁴

³³ <https://www.x-sense.com/products/sws51-smart-water-leak-detector>

³⁴ <https://mi.hr/mi-smart-plug-wifi.html>

3.1.2. Automobili

Najviše IoT primjera u osiguranju nalazimo u osiguranju vozila. Jedan od poznatijih primjera su Tesla ili noviji Toyota automobili. Tesla automobili u potpunosti su elektrificirani, automobil je povezan s Internetom. Automobil posjeduje mnoštvo senzora koje koristi u vožnji za praćenje okoline, pozicionira se pomoću geo lokacije, prepoznaje situacije u prometu te je, u nekim verzijama, osposobljen i za autonomnu vožnju. Ovi senzori koriste se prilikom vožnje te se tako povećava sigurnost u prometu. Automobil je spojen na Internet te se može nadograđivati softver, koristiti navigacija, multimedija. Preko Tesla aplikacije moguće je pristupiti povijesti punjenja vozila, povijesti vožnji, kontrolirati klimu u vozilu te ju koristiti za zakazivanje servisa i pomoći na cesti. Senzori u automobilima mogu detektirati mehaničke probleme i sudare te prenijeti detalje hitnim službama i 24-satnom servisnom savjetniku. Slika 3-13. grafički prikazuje senzore koje možemo susretati u današnjim novijim automobilima.



Slika 3-13. IOT u automobilima³⁵

Telematika obuhvaća tehnologije koje služe povezivanje automobila s IoT aplikacijama. Telematika može biti izvedena kao hardverska ili kao softverska. Hardverska telematika

³⁵ <https://IoT4beginners.com/self-driving-cars-and-IoT/>

zasniva se na senzorima koji se nalaze ugrađeni u automobilima, a softverska se zasniva na senzorima koji se nalaze u mobilnim uređajima vlasnika vozila. Osiguravajuće tvrtke mogu pratiti ponašanje vozača putem telematike, što im omogućuje praćenje ruta, brzine, ubrzanja, naglih kočenja ili upotrebu mobitela u vožnji. Može se pratiti i rad motora, razina ulja, stanje kočnica, upotreba sigurnosnog pojasa, ljudska prisutnost, temperatura i vlažnost unutar automobila i desetke drugih parametara. Ovi podaci kada su obrađeni mogu se primijeniti na različite načine: ³⁶

- Pomoći algoritama strojnog učenja moguće je odrediti koliko je svako pojedinačno putovanje bilo sigurno te se ti podaci mogu upotrijebiti za nagrađivanje dobrog vozača i dobro ponašanje u prometu ili za kažnjavanje u slučaju prekršaja ili rizičnog ponašanja. Ovi podaci mogu se upotrijebiti i za određivanje personalizirane cijene police.
- Moguće je kreirati proizvode osiguranja po modelu „plati koliko voziš“, odnosno moguće je kreirati kasko osiguranja vozila prema potrebama korisnika.
- U suradnji s servisima podatke je moguće koristiti za preventivno održavanje vozila i za otkrivanje potencijalnih anomalija na vozilu. Na taj način serviseri i osiguravatelji mogu detektirati potrebu za popravak motora, potrošenost kočnica, razinu ulja, potrošenost guma, a kako bi se izbjegli potencijalno veći kvarovi ili opasnosti, s ciljem smanjena odštetnih zahtjeva i povećanju sigurnosti prometa na cestama.
- Na temelju prikupljenih podataka moguće je detektirati i otkriti lažne prijave oštećenja, nemar vlasnika ili namjerno oštećenje vozila od strane vlasnika.
- U slučaju detekcije zaboravljenih osoba u automobilu, moguće je aktiviranje alarma za slučaj opasnosti prema vlasniku vozila ili aktiviranje automatskog otvaranja vrata.
- Noviji automobili imaju ugrađenu kameru koja prepoznaje izraze lica ili očiju vozača, prema kojima se prepoznaje umor, pospanost, vrtoglavica ili ako je vozač pod utjecajem alkohola. U tom slučaju javiti će se upozorenja ili se vozilo neće moći pokrenuti.
- Na temelju prikupljenih podataka moguće je implementirati program vjernosti i sustav za nagrađivanje pojedine vožnje vozača.

³⁶ <https://www.cigniti.com/blog/IoT-insurance-use-cases-benefits/>

3.1.3. Plovila

IoT tehnologija vlasnicima plovila omogućuje da spriječe probleme koji mogu uzrokovati velike štete u vrlo kratkom vremenu. U opasnim situacijama najvažnija je brza reakcija. IoT tehnologija omogućuje kontinuirani nadzor ključnih sigurnosnih rizika plovila i detekciju potencijalne opasnosti za brod puno prije nastanka štete. U slučaju incidenta, možemo biti obavješteni emailom, SMS-om, kroz mobilnu aplikaciju ili se može alarmirati osoblje u marinama koje će spriječiti daljnji nastanak štete.

IoT uređaji u plovilima

Senzor stanja baterije

Brodaska baterija je važan dio brodske opreme. Brodske baterije napajaju kaljužne pumpe koje sprječavaju ulazak mora u plovilo. Senzor baterije kontinuirano nadzire bateriju te može upozoravati o važnim informacijama ili aktivnostima potrebnim za održavanje baterija. Primjerice detektira kada je potrebno napuniti baterije kako bismo izbjegli njena oštećenja. Senzor također detektira početak odnosno kraj punjenja baterija. Senzori se preko centralne jedinice ili izravno preko Sigfox mreže spajaju na Internet. Preko mobilne aplikaciju možemo pratiti stanje baterije. Slika 3-14. prikazuje senzor baterije.



Slika 3-14. Senzor baterije ³⁷

³⁷ <https://www.sense4boat.com/hr/proizvod/pamet-an-senzor-baterije/>

Senzor kaljuže

Senzor kaljuže detektira prodor vode u plovilo i štiti plovilo od potapanja, ali i od plijesni do koje dolazi uslijed nakupljanja kišnice u brodu. Senzor pomoću plovka detektira povećanje razine vode u plovilo. Senzor najčešće ima interno napajanje preko baterije. Senzor se preko IoT protokola (Sigfox, Bluetooth, Zigbee, 4G, 5G) spaja direktno na Internet ili na centralnu jedinicu, preko koje se upozorava korisnika na opasnost od prodiranja vode u plovilo. U slučaju prodora vode, sustav će nas upozoriti glasovnim pozivom, emailom, SMSom ili obavijestima. Slika 3-15. prikazuje primjer senzora kaljuže.



Slika 3-15. Senzor kaljuže³⁸

Senzor temperature

Senzor temperature osigurava da je plovilo sigurno od samozapaljena. Samozapaljenje plovila može se dogoditi u marinama dok je plovilo na vezu. Jedan od mogućih razloga su kvarovi na instalaciji i uređajima gdje dolazi do pojave iskrenja i požara. Takvi požari se najčešće pojavljuju u prostorijama gdje se nalazi motor plovila, ali su ovom riziku izloženi i ostali dijelovi plovila. Senzor kontinuirano prati temperaturu u zatvorenom prostoru (poput strojarnice ili električnih ormarića) i otkriva promjenu temperature. Kada temperatura prijeđe definirani prag, generira se upozorenje kao mogući znak požara, koji se pravovremenom reakcijom osoblja marine može ugasi dok je još u razvojnoj fazi. Senzor se ugrađuje u

³⁸ <https://www.sense4boat.com/hr/proizvod/pametan-senzor-kaljuze/>

unutrašnjost broda, izrađen je na način da podržava visoke temperature. Senzor svakih nekoliko sekundi nadzire temperaturu i svaku uvećanu promjenu temperature u definiranom vremenskom intervalu, šalje u centralni sustav. Podaci se u centralni sustav šalju preko IoT protokola (Sigfox, Bluetooth, Zigbee, 4G, 5G). Centralna jedinica obrađuje podatke i u slučaju kada temperatura raste brže od normalnih promjena, šalju se upozorenja o mogućem požaru. Slika 3-16. prikazuje senzor temperature.



Slika 3-16. Senzor temperature ³⁹

Senzor dima

Dođe li do zapaljenja, osim povećane temperature, dim će otkriti pojavu požara. Razloga za zapaljenje je puno, a dobar dio razloga vezan je ili za električnu instalaciju i uređaje ili za motorni dio. Senzorom dima detektira se požar na samom plovilu, ali i potencijalno širenje požara na ostala plovila. U slučaju pojave dima senzor dima će generirati zvučni signal i/ili obavijestiti kontrolni centar marine. Senzor je preko IoT protokola (Sigfox, Bluetooth, Zigbee, 4G, 5G) komunicira s centralnom jedinicom. Ukoliko senzor detektira pojavu dima poslati će signal centralnoj jedinici koja će zatim korisniku ili nadzornom centru poslati obavijest o mogućnosti požara. Slika 3-17. prikazuje senzor dima koji se ugrađuje na plovila.

³⁹ <https://www.sense4boat.com/hr/proizvod/pametna-senzor-temperature/>



Slika 3-17. Senzor dima za plovila ⁴⁰

GPS

GPS je uređaj za praćenje kretanja plovila pomoću kojeg znamo poziciju plovila, ali i ostale parametre vezane za navigaciju – poput brzine. GPS ima mogućnost postavljanja zone kretanja. Pomoću GPS-a možemo obavijestiti vlasnika plovila ako plovilo izađe iz definirane zone kretanja. To je vrlo korisno protiv krađe plovila i neovlaštenog korištenja. Kada se plovilo kreće GPS šalje svoju lokaciju u definiranom vremenskom rasporedu, obično svakih nekoliko minuta. Kada plovilo stoji šalje u kraćim intervalima. Zbog velike pokrivenosti mreže GPS komunicira s centralnom jedinicom najčešće preko SigFox ili 3G/4G mreže. Slika 3-18. prikazuje GPS uređaj.



Slika 3-18. GPS ⁴¹

⁴⁰ <https://www.sense4boat.com/product/smart-smoke-sensor/>

⁴¹ <https://www.sense4boat.com/product/smart-gps-locator/>

Senzor za privezne konope

Iz perspektive osiguranja plovila zanimljivi su senzori za privezne konope plovila na stalnom vezu. Kod nevremena može doći do odvezivanja ili pucanja priveznih konopa. Senzor koji bi upozorio da je jedan ili više konopa popustio smanjio bi ili u potpunosti spriječio nastanak štete na plovilu kao i susjednim plovilima čime bi se znatno povećala sigurnost.

3.1.4. Zdravstvo

Nosivi uređaji (satovi, ogrlice, narukvice, vage ili odjeća) imaju zdravstvene i sportske primjene u kojima se mogu prepoznati rani simptomi bolesti. Najčešća zdravstvene primjene IoT-a su monitori pacijenata i uređaji za praćenje koju mogu biti korišteni u dijagnostičke svrhe ili za udaljeni nadzor pacijenata. Uređaji za praćenje mjere vitalne znakove kao što su broj otkucaja srca, temperatura, krvni tlak i razina glukoze. Popis zdravstvenih IoT aplikacija raste iz dana u dan. Iako su mnogi IoT uređaji nosivi, neki se ugrađuju kirurški. Na primjer, postoje stimulatori srčanog ritma s mogućnošću povezivanja na Internet, a koji se koriste za održavanje života pacijenata sa sporim ili nepravilnim otkucajima srca. Slika 3-19. prikazuje primjer pametnog sata.



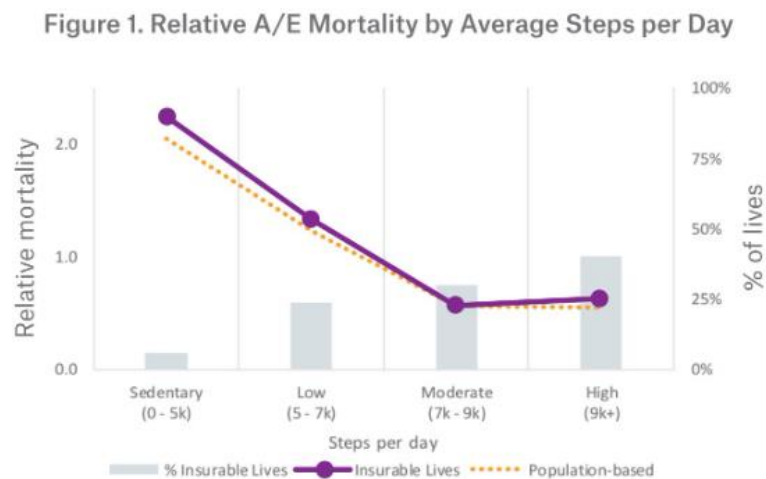
Slika 3-19. Primjer pametnog sata sa senzorima pogodnim za zdravstvo⁴²

⁴² <https://www.tres.in/shop/product/tres-smart-watch-care-c303/>

Trenutno većina nosivih uređaja na tržištu su narukvice ili satovi, koji prikupljaju podatke o broju prijeđenih koraka, minutama aktivnosti, prijeđenoj daljini, broju prijeđenih katova ili potrošenim kalorijama. Napredniji senzori mogu pratiti tlak, otkucaje srca, zasićenost kisika, san, razinu šećera u krvi, količinu kretnje tijekom dana.

Nosivi uređaji mogu automatski pozvati hitnu službu ili osobu za pomoć u slučaju pogoršanja zdravlja ili drugih opasnih situacija. Osiguravatelji iz nosivih uređaja mogu dobivati informacije o korisniku te imati mogućnost prevencije opasnih stanja korisnika, kao i izradu personaliziranih polica osiguranja. Moguće je i motivirati osobe koje nose nosive uređaje na zdraviji život, potaknuti ih na kretanje i tjelovježbu u zamjenu za popuste na police osiguranja, nagrade za postignute ciljeve, planove vjernosti, itd.

Slika 3-20. prikazuje da osobe sa sjedilačkim načinom života i malim brojem koraka dnevno imaju mnogo veći rizik od smrtnosti, dok umjereni i visoki broj koraka dnevno odgovaraju nižem riziku smrtnosti. Ova analiza pruža snažnu podršku za osiguravajuća društva da u svoje upravljanje rizicima uključe IoT tehnologiju i podatke s nosivih uređaja.⁴³



Slika 3-20. Prikaz broja koraka u korelaciji sa smrtnošću

⁴³ <https://www.munichre.com/us-life/en/perspectives/wearables/wearables-the-future-is-now-wearables-for-insurance-risk-asses.html>

3.1.5. Prijevoz

IoT nudi mogućnost praćenja i zaštite robe u prijevozu. Zahvaljujući IoT logistika i prijevoz raspolažu rješenjem za upravljanje robom na svakom koraku unutar logističke mreže. Logistička rješenja koja omogućava IoT prilično su jednostavna za primjenu. Mali uređaj za praćenje, ugrađuje se na kontejner, kamion ili vagon u kojem se nalazi roba. Nakon što je ugrađen u realnom vremenu prikuplja informacije o lokaciji robe. Na taj način povećava se sigurnost i smanjuje se mogućnost krađe. Unutar kamiona ili kontejnera s robom moguće je postavljanje senzora za praćenje temperature u prijevozu za robu koja je osjetljiva na temperaturu. Ukoliko temperatura izađe iz dozvoljenog intervala javljaju se upozorenja. Te se informacije mogu prikupljati i prikazivati na aplikacijskim platformama logističkog informacijskog sustava.⁴⁴

3.1.6. Industrijski pogoni

Tvornički ili naknadno ugrađeni senzori u infrastrukturne objekte ili dijelove mogu nadzirati parametre kao što su pojava vatre, dima, vlage, otrovnih para te na taj način prevenirati ili ublažiti mogućnost pojave potencijalno opasnih događaja. Integrirani senzori ugrađeni u industrijska postrojenja omogućuju osiguravateljima dinamičko modeliranje ocjenjivanja, koji omogućuju da svojim klijentima ponude cijene temeljene na procjeni rizika.

Nosivi senzori mogu nadzirati kretanje zaposlenika u područjima visokog rizika i prenositi podatke u sigurnosni centar u stvarnom vremenu te tako upozoriti na potencijalne opasnosti. Također, nosivi uređaji u industrijskim postrojenjima mogu smanjiti prijevare uzrokovane nezgodama na radnom mjestu.⁴⁵

⁴⁴ Galina V. Ivankova; Internet of Things (IoT) in logistics; (<https://iopscience.iop.org/article/10.1088/1757-899X/940/1/012033/pdf>)

⁴⁵ <https://www.capgemini.com/wp-content/uploads/2020/05/IoT-Insurance-of-Things-1.pdf>

3.2. Koristi za osiguravajuća društva nastale upotrebom IoT tehnologije

Predviđa se da će IoT preoblikovati budućnost industrije osiguranja te će ona imati prilike za razvoj novih proizvoda i mogućnosti za smanjenje iznosa odštetnih zahtjeva. Potencijal IoT tehnologije u osiguranju prepoznat je u ovim područjima.⁴⁶

- Razvoj modela osiguranja prema stvarnom korištenju usluge
- Razvoj personaliziranih ponuda osiguranja
- Razvoj modela osiguranja u stvarnom vremenu
- Proaktivno djelovanje u pogledu smanjenja šteta ili veličine štete
- Sinergija s proizvođačima IoT uređaja, automobilskom industrijom i ostalim proizvođačima opreme ili elektroničkih uređaja.

Podaci temeljeni na IoT tehnologiji, koji su prikupljeni, obrađeni i analizirani, omogućuju osiguravajućim društvima promjenu modela poslovanja. Osiguravajuća društva transformiraju se iz modela raspodjela rizika među osiguranicima i kompenziranja gubitaka, prema modelu da osiguranici sprječavaju ili smanjuju visinu štete, a osiguravajuća društva izbjegavaju potraživanja od strane osiguranika. Smanjivanjem pojavnosti štete i potraživanja, osiguravajuća društva imala bi veću profitabilnost. Mogla bi imati i prostora za smanjivanje cijene premije i višu stopu zadržavanja klijenata.

IoT tehnologija omogućuje osiguravajućim društvima nove načine interakcije s klijentima i stvaranje novih poslovnih modela. Zadnjih nekoliko godina prihvaćanje IoT uređaja u domovima je doživjelo procvat. Ipak, osiguravajuća društva te trendove sporo usvajaju. Vjeruje se da će se trend ubrzo promijeniti. U nastavku ovog poglavlja bit će opisane prednosti osiguranja doma pomoću IoT tehnologije za osiguravajuća društva i za osiguranike.⁴⁷

⁴⁶ <https://www2.deloitte.com/tr/en/pages/financial-services/articles/innovation-in-insurance-internet-of-things-IoT.html>

⁴⁷ <https://fintechos.com/blogpost/6-ways-IoT-devices-are-changing-home-insurance/>

Smanjenje prijavljenih šteta

IoT uređaji mogu otkriti vatru, dim, curenje vode, istjecanje plina, provale i ostale opasnosti. Ako se opasnosti otkriju u ranoj fazi možemo izbjeći tragedije ili nastanak štete. Događaji kao što su pojava vatre, pojava curenja vode mogu putem senzora poslati vlasniku obavijest na mobilni uređaj. Tako će šteta biti umanjena ili spriječena. Kamere koje se nalaze unutar ili okolo kuće prenose snimke putem aplikacija vlasniku objekta na telefon. Već i sama prisutnost kamera će udaljiti neželjene posjetitelje od objekta. Rezultat ovih aktivnosti je smanjenje visine potraživanja za štete od osiguravajućih društava. Pojedina osiguravajuća društva na tržištu nude do 20% popusta na osiguranje klijentima koji imaju ugrađene IoT uređaje i senzore.⁴⁸

Određivanje visine premije osiguranja

Napredniji način korištenja IoT uređaja je prikupljanje, obrada i analiza podataka s IoT uređaja. Podaci se mogu koristiti kao izvor informacija za analizu i modeliranje proizvoda prilagođenih klijentima. Podaci iz raznih izvora kao što su lokacija građevine, starost, opasnosti iz geografskog položaja poput poplava, klizišta, vrijeme, podaci o sigurnosti susjedstva mogu biti upareni s podacima s IoT uređaja kako bi se izračunali rizici i izradili modeli klijenta te tako izradile personalizirane premije osiguranja za svakog klijenta. Osiguravajuća društva nude do 25% popusta na osiguranje korištenjem podataka sa IoT uređaja.⁴⁹

Učenje modela analize rizika i izračuna premije

Podaci prikupljeni s IoT uređaja mogu pomoći osiguravajućim društvima odgovoriti na pitanja za koje još nemaju odgovore i egzaktno činjenice. Npr. smanjuju li kamere na osiguranom objektu mogućnost provala za 50%. Osiguravajuća društva analizom velikog skupa prikupljenih podataka s IoT uređaja mogu izračunati taj postotak. Porast prihvaćanja pametnih

⁴⁸ <https://www.nerdwallet.com/article/insurance/smart-home-insurance-discount>

⁴⁹

https://www.seedrs.com/hiro?utm_source=wordpress&utm_medium=blog&utm_term=hiro_campaignspotlight

uređaja i korištenja statističkog modeliranja uskoro će dati odgovore na takva pitanja i pomoći će osiguravajućim društvima u izračunima rizika.⁵⁰

Prikupljanje podataka o ponašanju klijenata

Podaci prikupljeni s IoT uređaja mogu se iskorištavati u različite svrhe. To mogu biti podaci o broju osoba koji žive u kućanstvu, vremenu provedenom u domu, korištenim pametnim uređajima, potrošnji električne energije ili vode. Model prikupljenih podataka skriva i mnogo opasnosti koje zadiru do etičkih i zakonskih okvira. Poznati su slučajevi gdje su pametni uređaji snimali i prikupljali podatke o razgovorima u kućanstvima. Model može biti iskorišten kada je potrošač dao pristanak za prikupljanje podataka i kada zna u koje svrhe će se ti podaci upotrijebiti. Primjer za korištenje tih podataka u osiguranju može biti podatak koristi li se nekretnina kao stalno ili je povremeno nastanjena jedinica. Prema istraživanjima 27% klijenata dijelilo bi svoje podatke u zamjenu za popust na police osiguranja.⁵¹

Sprječavanje prijevara

IoT tehnologija može omogućiti osiguravajućim društvima sprječavanje prijevara. Podaci s nosivih uređaja mogu biti upotrijebljeni kako bi se analiziralo ponašanje i zdravstveno stanje klijenata. Poznat je slučaj s danskim osiguravateljem, gdje je klijentica prijavila štetu u osiguranju koja je pokrivala nesposobnost za rad zbog ozljede. Njezin profil na aplikaciji za trčanje otkrio je da je bila puno aktivnija i redovito sudjelovala u sportskim događajima, što bi bilo nemoguće da je bila ozlijeđena kako je tvrdila.⁵²

⁵⁰ <https://www.mckinsey.com/industries/financial-services/our-insights/insurance-2030-the-impact-of-ai-on-the-future-of-insurance>

⁵¹ <https://research.aimultiple.com/insurance-IoT/#3-customized-insurance-practices>

⁵² <https://www.forbes.com/sites/blakemorgan/2018/05/16/heres-how-IoT-will-impact-the-insurance-claims-process/?sh=15e29184366e>

Pomoć zajednici

Podaci s IoT uređaja mogu koristiti osiguravajućim društvima, ali i široj zajednici. Podaci prikupljeni sa senzora o poplavama tijekom oluja mogu se iskoristiti kako bi se preventivno obavijestila zajednica da postoji šira opasnost o poplavama. Podaci s kamera mogu biti upotrijebljeni u pronalasku počinitelja kaznenog djela. Mogu se slati obavijesti u susjedstvo ako su zabilježeni pokušaji provale na nekom području. Naravno ti podaci mogu se dijeliti samo ako vlasnici daju svoju suglasnost za dijeljenje podataka.

Izgradnja čvrstih veza s klijentima

Uobičajena komunikacija osiguravajućih društava s osiguranicima je jednom godišnje kada je potrebno platiti premiju ili ako se podnosi zahtjev za štetnim događajem. Moderna osiguravajuća društva trude se izgraditi čvrste veze s korisnikom u obostranu korist, a kako bi mogla biti konkurentna ne samo s cijenom već i s drugim uslugama. Osiguravajuća društva mogu ponuditi osiguranicima IoT uređaje i povezane aplikacije putem koje mogu biti u kontaktu s klijentima, nuditi im preko nje nadzor doma, slanje notifikacija za upozorenja, pružiti analitiku o „ponašanju“ doma ili davati kompletnu uslugu centra za nadzor doma. U tom modelu i klijenti i osiguravajuća društva imaju koristi te klijenti ostvaruju čvrste veze i grade povjerenje sa svojim osiguravajućim društvom.

3.3. Modeli proizvoda osiguranja upotrebom IoT tehnologije

Osiguravajuća društva imaju izbor nekoliko vrsta strategija za izlazak na tržište osiguranja gdje se koristi IoT tehnologija. U ovom poglavlju bit će opisano nekoliko načina izlaska na tržište.

Davanje popusta na proizvode gdje su korišteni IoT senzori

U ovom načinu izlaska na tržište osiguravajuća društva promiču nabavu IoT uređaja kao komplementarne proizvode za svoje usluge. To rade na način da nude velike popuste za njihovu nabavu ili ih besplatno nude svojim korisnicima. Ova opcija je najjednostavnija za implementaciju, pomaže usvajanje tehnologije, ali osiguravatelji od nje nemaju značajne koristi jer je ograničen pristup podacima. Prednost koju osiguravatelji mogu imati je povećana svijest o sigurnosti krajnjih korisnika i smanjenje broja odštetnih zahtjeva.

Suradnja s postojećim partnerima na tržištu

U ovom načinu izlaska na tržište osiguravajuća društva surađuju s partnerima koji su aktivni na tržištu i koji nude usluge i IoT uređaje. Preko partnera postoji ugovor o dijeljenju podataka. Ovaj način implementacije jednostavan je za osiguravajuća društva, ali ima ograničenja u pogledu pristupa podacima, jer partner može nametnuti ograničenja. Kao i u prethodnom modelu, ovaj način izlaska na tržište nudi više prednosti dobavljačima uređaja. Za osiguravatelja može smanjiti broj odštetnih zahtjeva, ali malo pomaže u izgradnji bliskosti s potrošačem ili u povećanju prihoda.

Razvoj i brendiranje vlastitih IoT uređaja

U ovom načinu izlaska na tržište osiguravajuća društva nude vlastitu robnu marku IoT uređaja i odabrane proizvode i usluge. Osiguravajuća društva mogu razvijati vlastite proizvode pomoću dobavljača koji nude uređaje koji nisu brendirani. U ovom modelu osiguravajuća društva nude kompletan proizvod u koji potrošači mogu imati povjerenje, a osiguravajuća društva pristup podacima iz IoT uređaja. Ovaj pristup ima puno prednosti za osiguravajuća društva jer mogu ostvarivati ​​prihode iz prodaje uređaja i korištenja podataka, ali je i najriscantniji jer zahtijeva najviše ulaganja.⁵³

⁵³ <https://www.the-digital-insurer.com/wp-content/uploads/2019/02/1437-ParksAssoc-LeveragingSmartHomeforInsuranceBusinessModels.pdf>

4. Pregled tržišta u Republici Hrvatskoj

4.1. Pregled proizvoda

U ovom poglavlju napravljen je pregled tržišta i opisani su proizvodi u osiguranju temeljeni na IoT tehnologiji u Republici Hrvatskoj. Neki proizvodi su aktivni na tržištu, ali postoje i proizvodi koje više nisu aktivni.

4.1.1. CO Iskon SmartHome

Croatia osiguranje u suradnji s poduzećem Iskon do prije nekoliko godina nudila je proizvod osiguranja imovine sa IoT uređajima. Uz svako kupljeno osiguranje nekretnina u minimalnom trajanju od 5 godina korisnik je na poklon dobio IoT paket za osiguranje doma. Slika 4-1. prikazuje proizvod Iskon SmartHome.



Slika 4-1. Iskon SmartHome paket ⁵⁴

Centralna jedinica spaja postavljene senzore te omogućuje upravljanje putem mobilne i web aplikacije. Uz centralnu jedinicu, osnovni komplet ima četiri senzora, koji se lako postavljaju u stanu. To su senzor za vodu, senzor za pokret sa senzorom mikrokline i senzor za dim. Mobilna

⁵⁴ <https://www.iskon.hr/O-Iskonu/Press-centar/Press/Iskon.Smarthome-sustav-za-upravljanje-domom-na-daljinu>

aplikacija omogućuje jednostavni pregled trenutnog stanja u domu, slanje notifikacija u slučaju promjena, upravljanje uređajima i senzorima na daljinu.

Korist ovakvog izlaska na tržište za Croatia osiguranje je proaktivna zaštita osiguranih nekretnina, smanjivanje broja i visine štete te izgradnja dugoročnih i čvrstih veza s korisnikom.

Prednosti za korisnike koji koriste ovaj proizvod su povećana zaštita nekretnine, mogućnost brže reakcije u slučaju opasnosti te nadzor nekretnine pomoću mobilne aplikacije.

4.1.2. Croatia kasko osiguranje brodica i jahti

Tvrtka Sense4Boat u suradnji s Croatia osiguranjem nudi proizvod kasko osiguranja plovila. Plovila koja su opremljena s dva ili više senzora ispunjavaju uvjete za dobivanje 20% popusta na osiguranje plovila (kasko osiguranje, uključujući osiguranje od odgovornosti za vlasnike/korisnike plovila i gubitak najma). Ukoliko je plovilo opremljeno senzorima pokriveni su rizici požara, krađe ili potonuća plovila.⁵⁵

Prema podacima tvrtke Sense4Boat trenutno ima preko 600 plovila u 17 marina koji su opremljeni sa senzorima. U zadnjih 18 mjeseci zahvaljujući senzorima spriječeno je 16 oštećenja uslijed prodora vode, 3 potonuća plovila i 3 požara na plovilima.⁵⁶

Proizvod radi na način da su senzori koji se nalaze u plovilima povezani na centralnu jedinicu i nadzorni centar preko Sigfox mreže. Korisnici mogu instalirati mobilnu aplikaciju preko koje mogu pratiti podatke sa senzora za svoje plovilo.

U ovom proizvodu tvrtka Croatia osiguranje ne prikuplja podatke sa senzora. Podatke prikuplja Sense4boat koji nadzire plovila opremljena sa senzorima. Strategija ovakvog izlaska na tržište za Croatia osiguranje je stjecanje novih korisnika preko dodijeljenog popusta. Korist za Croatia osiguranje je proaktivna zaštita osiguranih plovila, smanjivanje broja i visine štete koje u slučaju plovila mogu biti velikih razmjera.

Korist za korisnika je povećana zaštita plovila te nadzor nad plovilom pomoću mobilne aplikacije.

⁵⁵ <https://crosig.hr/osiguranje-plovila/kasko-osiguranje-brodica-i-jahti/>

⁵⁶ <https://www.sense4boat.com/>

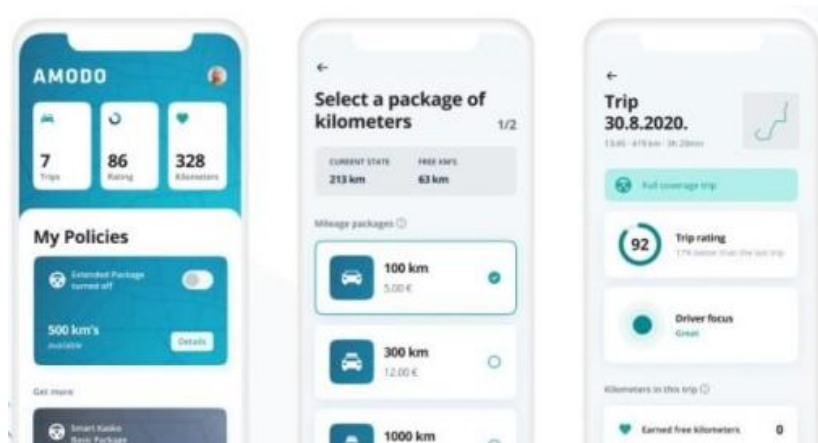
4.1.3. Uniqa Smart kasko

Smart kasko je proizvod Uniqa osiguranja.⁵⁷ Smart kasko je osiguranje vozila po principu plati koliko koristiš. Korisnik preko mobilne aplikacije može kupiti određeni broj kilometara (100, 300, 1200) te može koristiti te kilometre kada i koliko želi. Sve dok ima dovoljan broj zakupljenih kilometara vrijedi i kasko osiguranje. Preko mobilne aplikacije može se aktivirati ili deaktivirati kasko osiguranje prema potrebama i željama korisnika.

Smart kasko za bilježenje potrošenih kilometara koristi senzore koji se nalaze u mobitelu korisnika. Uniqa osiguranje prikuplja podatke o lokaciji korisnika, detekciji pokreta, vremenima vožnje i stanju mreže.⁵⁸ Na temelju tih podataka određuju se potrošeni kilometri zakupljenog osiguranja.

Ovaj proizvod idealan je za one korisnike koji ne želi plaćati puno kasko osiguranje ili voze manji broj kilometara godišnje. Korisnici mogu osigurati svoje vozilo po nižoj cijeni od standardnog kaska osiguranja.

Prednost za osiguravajuće društvo je dobivanje novih korisnika koji ne žele plaćati punu cijenu kasko osiguranja. Slika 4-2. prikazuje mobilnu aplikaciju preko koje korisnik upravlja i zakupljuje kilometre za svoje kasko osiguranje.⁵⁹



Slika 4-2. Uniqa Smart kasko

⁵⁷ <https://www.uniqa.hr/o-nama/vijesti/smart-kasko-prvo-kasko-osiguranje-koje-placas-koliko-vozis/4235>

⁵⁸ <https://www.uniqa.hr/kampanje/usk/privacy/4222>

⁵⁹ <https://coverager.com/amodo-introduces-next-generation-pay-per-mile/>

4.1.4. LaqoPrevent

LaqoPrevent je proizvod LAQO osiguranja i nalazi se u mobilnoj aplikaciji.⁶⁰ LaqoPrevent je aplikacija temeljena na IoT tehnologijama koja prikuplja podatke o vožnji s mobilnog uređaja korisnika. Kada korisnik sjedne u automobil senzori u mobilnom uređaju i mobilna aplikacija prate način vožnje korisnika. Različiti kontekstualni podaci koji se povezuju sa GPS točkama unutar vožnje stvaraju podlogu za ocjenjivanje pojedinačne vožnje.

Korisnik za svaku vožnju dobiva ocjenu koja se temelji na brzini i stilu vožnje. Ako je vožnja sigurna, korisnik će dobiti dobre ocjene. S druge strane, prekoračenja brzine, nagla ubrzanja, kočenja i nagla skretanja za vrijeme vožnje smanjit će ocjenu vožnje.

Druga komponenta ocjene je usredotočenost prilikom vožnje. Korisnik će dobiti nižu ocjenu ako upotrebljava mobitel za vrijeme vožnje. Bilježe se podaci kao što su broj uporaba mobitela, trajanje poziva i druge radnje mobitelom. Ovi podaci čine osnovu za izračun ocjene usredotočenosti. Slika 4-3. prikazuje LAQO mobilnu aplikaciju gdje korisnik može vidjeti svoje ocjene za svaku vožnju i ukupnu ocjenu svih vožnji.



Slika 4-3. LaqoPrevent program⁶¹

⁶⁰ <https://www.laquo.hr/laquo-prevent/>

⁶¹ <https://www.bug.hr/mobilne-aplikacije/vozio-sam-mjesec-dana-uz-telematiku-laqoprevent--jesam-li-sada-bolji-vozac-20477>

LaqoPrevent za korisnike s dobrim ocjenama nudi mogućnost osvajanja nagrada, dok one s lošim ocjenama ne kažnjava. Nagrade mogu biti materijalne ili popusti na nove proizvode i usluge iz portfelja Croatia osiguranja (specijalistički pregledi u zdravstvenim ustanovama, kontrolni pregledi, popusti na police zdravstvenog osiguranja, police osiguranja osobnih stvari i dokumenata, itd.).

Preko aplikacije moguće je pratiti i emisiju CO₂ (ugljičkov dioksid). Ekonomičnijom vožnjom korisnik može izravno smanjiti svoj ugljični otisak i ima pozitivan utjecaj na okoliš i potrošnju goriva. Emisija CO₂ računa se na osnovi dva parametra. U prvom dijelu se računa prosječna emisija s obzirom na starost vozila, radni obujam motora i vrstu goriva. U drugom dijelu bazira se na telematičkim podacima (duljina, trajanje i brzina vožnje).⁶²

U LaqoPreventu Croatia osiguranje prikuplja sljedeće podatke: lokacija korisnika, detekcija pokreta, broj zaprimljenih poziva, trajanje poziva, datuma uspostave poziva, stanje mreže.⁶³

LaqoPrevent ovim načinom izlaska na tržište potiče sigurnu i ekonomičnu vožnju te potiče smanjivanje emisije CO₂.

Prednost za korisnika je mogućnost dobivanja nagrada i popusta, mogućnost analize i pregled podataka o vožnjama u mobilnoj aplikaciji.

Prednost za Croatia osiguranja ovim proizvodom je dobivanje novih korisnika mlađe generacije koji su dobro upoznati digitalnim trendovima, te izgradnja čvrstih i dugoročnih odnosa s korisnicima.

⁶² https://media.laqa.hr/uploads/laqa_prevent_210x297_13102022_715753cc86.pdf

⁶³ <https://www.laqa.hr/zastita-privatnosti/>

4.1.5. Toyota FHI kasko osiguranje

Generali osiguranje u suradnju s Toyotom nudi proizvod kasko osiguranja imena Toyota FHI.⁶⁴ Proizvod je posebno dizajniran za hibridna vozila. Proizvod se zasniva na telematici gdje su senzori ugrađeni u vozilo. Putem SIM kartice u vozilu podaci o vožnjama korisnika se šalju na centralnu lokaciju. Telemetrijske podatke prikuplja Toyota i osiguravatelj. Na temelju tih podataka analizira se način korištenja vozila i postotak vožnje na električni pogon motora. Korisnik vozila na temelju podataka o učestalosti vožnje na električni pogon i ukupne ostvarene kilometraže u prethodnoj godini ostvaruje dodatne popuste na premiju osiguranja prilikom obnove kasko police koji sežu do 8%.

Popust koji će korisnik ostvariti ovisi o učestalosti korištenja čistog električnog pogona vozila i bit će veći što ga korisnik više koristi. Toyota smatra da je korisnik koji vozi više na električni pogon smireniji vozač, a samim time i sigurniji vozač. Korisnik može pratiti rezultate preko mobilne aplikacije MyT. Tablica 4-1. prikazuje shemu popusta prilikom obnove kasko police osiguranja. U shemi je vidljivo da što je veći udio električne vožnje (EV) veći, da je veći i popust prilikom obnove kasko police osiguranja.

Tablica 4-1. Toyota FHI shema popusta prilikom obnove police osiguranja⁶⁵

Udio EV vožnje (%)	Prijedeno km u godinu dana			
	0 – 4.999	5.000 – 9.999	10.000 – 19.999	20.000 – 29.999
0 - 24%	0%	0%	0%	0%
25 - 35%	0%	3%	3%	0%
36 - 40%	5%	5%	5%	3%
41 - 49%	5%	5%	5%	3%
>=50%	8%	8%	8%	5%

Toyota FHI prikuplja podatke o lokaciji korisnika, detekciji pokreta, ubrzanju i kočenjima, kretanju vozila, vremenima vožnje, potrošnji goriva, udjelu električne vožnje, prijeđenim kilometrima, itd.

⁶⁴ <https://www.toyota.hr/owners/warranty/full-hybrid-insurance>

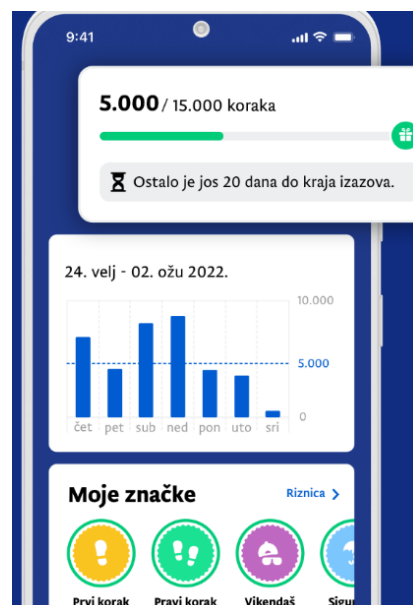
⁶⁵ Generali osiguranje uvjeti osiguranja; FHI_Toyota hibrid osiguranje.pdf

Ovim načinom korištenja IoT tehnologije motivira se korisnike na veći udio ekološke vožnje, odnosno na češće korištenje vozila na električni pogon, a kao nagradu korisnici dobivaju popust na kasko osiguranje.

Generali osiguranje na ovaj način radi čvrste veze s korisnikom, a pridonosi i ekološkom aspektu poticanjem ekološke vožnje. Prednost za Generali osiguranje s ovim proizvodom je izgradnja dugoročnih veza sa korisnikom i poticanje na produženje kasko osiguranja.

4.1.6. CroatiaFIT

CroatiaFIT je proizvod Croatia osiguranja. CroatiaFIT je aplikacija u sklopu mobilne aplikacije Moja Croatia. ⁶⁶ Aplikacija za članove koji su se uključili u program broji aktivnosti i korake koje je korisnik napravio tokom dana. Aplikacija koristi podatke s mobilnih uređaj korisnika. Članovi trebaju dati odobrenje da se prikupljaju podaci putem servisa sa Iphone (Apple Health) ili Android (Google fit) uređaja. Prikupljaju se podaci o prijeđenoj udaljenosti, broju koraka, nadmorskoj visini i lokaciji korisnika. Slika 4-4. prikazuje CroatiaFIT aplikaciju.



Slika 4-4. CroatiaFIT aplikacija ⁶⁷

⁶⁶ <https://crosig.hr/croatia-fit/>

⁶⁷ <https://crosig.hr/croatia-fit/>

Croatia osiguranje nagrađuje korisnike koji sakupe najveći broj koraka u nekom vremenskom periodu ili kreira izazove gdje korisnik skuplja značke na temelju kojih može biti nagrađen. Nagrade su vrijednosti od 3 do 700 EUR i mogu biti materijalne ili ostvarenje prava na nove proizvode osiguranja kao što su posebno kreirani proizvodi osiguranja od nezgode za članove CroatiaFIT programa, popusti na dodatno i dopunsko zdravstveno osiguranje.

Croatia osiguranje ovim proizvodom i upotrebom IoT tehnologije promiče zdrav život, motivira članove programa na što aktivnije kretanje. Tijekom 2022. godine članovi programa napravili su više od 6 milijardi koraka, što je jednako kao da su obišli Zemlju više od 100 puta.

CroatiaFit je vrlo uspješan primjer korištenja IoT tehnologije u osiguranju. U ovom trenutku preko 48000 članova je uključeno u program. Ovim načinom izlaska na tržište Croatia osiguranje radi čvrste veze sa svojim klijentima, potiče čestu upotrebu mobilne aplikacije, a kroz nagrade osigurava da članovima nudi i druge proizvode iz svojeg portfelja.

4.2. Analiza proizvoda

Analiza pregleda primjene IoT tehnologije u Republici Hrvatskoj napravljena je prikupljanjem dostupnih podataka putem Internet stranica osiguravajućih društava i pregledu dostupnih uvjeta poslovanja. Analizirani su slijedeći proizvodi:

1. CO Iskon SmartHome
2. CO kasko plovila
3. Uniqa Smart kasko
4. CO Laqo Prevent
5. Generali Toyota FHI Kasko
6. CO CroatiaFit

Analiza i usporedba proizvoda napravljena je u nekoliko kategorija:

- Je li proizvod aktivan?
- Koji senzori su korišteni u proizvodima?
- Koji podaci se prikupljaju?
- Koje su koristi za korisnika osiguranja?
- Koje su koristi za osiguravajuće društvo?
- Koje su koristi za zajednicu?
- Koji je model suradnje prilikom izlaska na tržište?

Tablica 4-2 prikazuje i analizira navedene proizvode.

Tablica 4-2. Analiza proizvoda na tržištu Republike Hrvatske

	CO Iskon SmartHome	CO kasko plovila	Uniqa Smart Kasko	CO LAQO Prevent	Generali Toyota FHI kasko	CO CroatiaFit
Aktivan	Ne	Da	Ne	Da	Da	Da
Vrsta	Osiguranje imovine	Osiguranje plovila	Osiguranje vozila	Osiguranje vozila	Osiguranje vozila	Osiguranje zdravlja
Korišteni senzori	Senzor dima Senzor vode/kaljuže Senzor za pokret	Senzor dima Senzor vode Senzor za pokret Senzor baterije Senzor topline GPS	GPS Senzor ubrzanja Žiroskop	GPS Senzor ubrzanja Žiroskop	GPS Senzor ubrzanja Žiroskop	GPS Pedometar
Vrsta prikupljenih podataka	Podaci se ne prikupljaju	Podaci se ne prikupljaju	Lokacija Ubrzanje Kočenja Kretanje vozila Stanje mreže Vrijeme	Lokacija Ubrzanje Kočenja Korištenje handsfree funkcije. Uspostava poziva Kretanje vozila Stanje baterije Stanje mreže Vrijeme Korištenje bluetootha	Lokacija Ubrzanje Kočenja Kretanje vozila Vrijeme Stanje mreže Potrošnja goriva Korištenje hibridne baterije Prijedeni kilometri Podaci o vozilu	Prijedena udaljenost. Broj koraka. Nadmorska visina. Lokacija. Vrijeme.

Korist za kupca	Proaktivna zaštita osigurane nekretnine.	Niža cijena police osiguranja. Proaktivna zaštita plovila.	Fleksibilno korištenje kasko osiguranja prema potrebi klijenata. Niža cijena police.	Osvajanje nagrade kroz natjecanja i izazove.	Niža cijena kasko osiguranja.	Poticanje na kretanje i očuvanje zdravlja. Osvajanje nagrada kroz natjecanja i izazove.
Korist za osiguravajuće društvo	Manja visina štete ili izbjegavanje štete.	Pribavljanje i zadržavanje klijenata. Manja visina štete zbog proaktivne zaštite.	Pribavljanje novih klijenata koji nemaju potrebu za potpunim kaskom.	Izgradnja čvrstih veza sa klijentom. Manja visina štete zbog promicanja sigurne vožnje.	Zadržavanje klijenata. Moguće profiliranje klijenata.	Zadržavanje klijenata. Kanal za prodaju novih proizvoda klijentima.
Korist za zajednicu		Povećanje sigurnosti prometa na moru i sigurnost plovila u marinama.		Povećanje sigurnosti prometa. Smanjenje emisije CO2.	Povećanje sigurnosti prometa. Poticanje vožnje na električni pogon. Smanjenje emisije CO2.	Promicanje zdravog života.
Model suradnje	Davanje popusta na IoT uređaje	Davanje popusta na IoT uređaje	Kolaboracija sa postojećim partnerima	Kolaboracija sa postojećim partnerima	Kolaboracija sa postojećim partnerima	Vlastiti razvoj.

Analiza proizvoda u industriji osiguranja pokazala je da su na tržištu aktivna 4 proizvoda na kojima se upotrebljava IoT tehnologija. Od toga se dva proizvoda koriste u osiguranju vozila (Laqo Prevent, Toyota FHI Kasko), jedan u osiguranju plovila (CO kasko plovila) i jedan u osiguranju zdravlja (CroatiaFit).

U proizvodima CO kasko plovila i Iskon SmartHome ne prikupljaju se podaci od strane osiguravajućeg društva te se modeli proizvoda zasnivaju na proaktivnoj zaštiti imovine korisnika i popusta prilikom sklapanja osiguranja.

U proizvodima za osiguranje vozila prikupljaju se podaci. Uniqa kasko na temelju podataka omogućuje fleksibilno korištenje kasko osiguranja vozila prema potrebama korisnika. Laqo Prevent koristi podatke kako bi korisnicima omogućila osvajanje nagrada. Toyota FHI kasko koristi podatke kako bi korisnicima koji voze ekonomičnije smanjila cijenu prilikom obnove police.

CroatiaFit podatke koristi za osvajanje nagrada kroz izazove i natjecanja.

U većini proizvoda prednost koje osiguravajuća društva dobivaju kroz korištenje IoT tehnologije je izgradnja čvrstih veza s klijentima bilo kroz natjecanja i osvajanja izazova ili kroz popuste za obnovu police. CroatiaFit ima najveći broj aktivnih korisnika, nagrade koji korisnici osvajaju služe kao kanal za prodaju novih osiguravateljskih proizvoda ili zdravstvenih usluga.

5. Pregled tržišta u zemlji Europske unije

5.1. Pregled proizvoda

U ovom poglavlju napravljen je pregled tržišta i opisani su proizvodi u osiguranju temeljeni na IoT tehnologiji na tržište zemlje Europske unije. Italija je izabrana za primjer razvijene članice Europske unije kao zanimljivo tržište za analizu i usporedbu sa Republikom Hrvatskom.

Analizirano je deset najvećih osiguravajućih društava koje djeluju u Italiji. To su: ⁶⁸

1. Assicurazioni Generali
2. Unipol
3. Poste italiane
4. Intesa Sanpaolo
5. Allianz
6. Banca Mediolanum
7. Cattolica Assicurazioni
8. BNP Paribas's Italian subsidiary
9. Reale Mutua Assicurazioni
10. CNP Assurances–UniCredit

Analiza je napravljena prikupljanjem dostupnih podataka putem Internet stranica osiguravajućih društava. Samo neka od njih nude proizvode osiguranja zasnovana na IoT tehnologiji.

⁶⁸ <https://www.worldatlas.com/articles/the-biggest-insurance-groups-in-italy.html>

5.1.1. Assicurazioni Generali

Generali osiguranje u Italiji, korisnicima koji imaju u vozilima ugrađenu „crnu kutiju“ nudi popust do 35% na policu osiguranja.⁶⁹ Crna kutija je uređaj koji omogućuje osigurateljima nadzor automobila tijekom njegove upotrebe. Uređaj korisnik ugrađuje bez dodatnih troškova u radionici koja ima ugovor s osiguravajućem društvom. Podatke sa uređaja može koristiti policija i osiguravajuća društva u slučaju nezgode. Podaci su dostupni policiji koja u slučaju nesreće može rekonstruirati stil vožnje i ponašanje vozača za volanom. Uređaj prikuplja podatke o lokaciji putem GPS uređaja, detaljima putovanja i zaustavljanja, prijeđenim kilometrima sa statističkim analizama udaljenosti (danju i noću), vrsti rute (gradska, izvan gradska, autocesta), sudarima i udarcima, stilu vožnje (nagla kočenja i ubrzanja).⁷⁰ Korisnik može birati između pet uređaja sa različitim funkcionalnostima.

Prednost za osiguravajuće društvo korištenja ovog proizvoda je mogućnost rekonstrukcije događaja nesreće, sprječavanje prijevara, brz pronalazak vozila u slučaju krađe vozila, mogućnost dobivanje brze informacije u slučaju nesreće te izgradnja dugoročnih i čvrstih veza s korisnikom.

Prednost za korisnika je niža cijena premije osiguranja i proaktivna pomoć na cesti u slučaju nesreće.

⁶⁹ <https://www.generali.it/preventivatori/preventivatore-auto-quota-facile/conosciamoci>

⁷⁰ <https://www.generali.it/magazine/auto/scatola-nera#e>

5.1.2. UnipolSai

UnipolSai osiguranje nudi proizvode Unibox 2 Wheel i Unibox Auto.⁷¹ Proizvodi su namijenjeni za osiguranje automobila i motora. Proizvod se temelji na uređaj koju radi nadzor vozila, prati podatke o vožnji, lokaciji te omogućuje automatski poziv u operativni centar u slučaju nesreće, čak i ako vozač nije u stanju komunicirati.

Uređaj prati podatke o vožnjama korisnika i prijeđenim kilometrima. Na temelju tih podataka korisnik ima mogućnost ugovaranja osiguranja po modelu „plati koliko voziš“. Preko aplikacije koja je integrirana s uređajem korisnik u svakom trenutku može znati lokaciju svog vozila i ostale podatke o vozilu. Na temelju podataka o vožnji kao što su brzina prilikom udarca, kočenje, moguća je rekonstrukcija događaja u slučaju nesreća koja može policiji ili korisniku pomoći u dokazivanju ili osporavanju krivnje.

Osiguravajuće društvo preko podataka može brzo pronaći automobil u slučaju krađe, brzo reagirati u slučaju nesreće, zaštititi se od prijevara. Na taj način moguće je smanjiti troškove u slučaju prijave štete.

Proizvod koristi četiri milijuna korisnika.⁷² Korisnik može izabrati tri paketa funkcionalnosti ovisno o cijeni godišnje pretplate. UnipolSai korisnicima nudi izbor više uređaja ovisno o funkcionalnostima po početnoj cijeni od 12 eura godišnje. Za uzvrat korisnik dobiva 30% popusta na cijenu police.⁷³

⁷¹ <https://www.unipolsai.it/unibox-2ruote>

⁷² <https://www.unipolsai.it/unibox-auto>

⁷³ <https://www.unipolsai.it/plus/mobilita/scatola-nera-smart>

5.1.3. Intesa Sanpaolo

Intesa Sanpaolo osiguranje nudi proizvod ViaggiaConMe za osiguranje automobila.⁷⁴ Proizvod se temelji na uređaju sa ugrađenim GPS senzozom i GSM karticom. Uređaj prati podatke o vožnji, lokaciji, te broju prijeđenih kilometara. Korisnik može odabrati između dva uređaja, ovisno o njegovim funkcionalnostima.

Korisnik može izabrati nekoliko opcija proizvoda. Opcija „TravelWithMe on consumption“ prilagođena je korisnicima koji malo koriste automobil. Ova opcija ugovara se po modelu „plati koliko voziš“. Ukoliko korisnik godišnje prijeđe do 3500 kilometara može ostvariti uštedu od 50% popusta na policu premije. Dodatno uz opciju dobiva i osiguranje kada putuje biciklom.⁷⁵ U ovoj opciji korisnika se stimulira da se vozi manje sa autom, a više koristi bicikl ili drugačije načina prijevoza.

Osiguravatelj na taj način smanjuje rizik jer korisnik manje koristi automobil. Sa druge strane korisnici koji rade malo kilometara sa automobilom dobivaju vrlo jeftino osiguranje vozila.

Opcija „TravelWithMe Unlimited km“ prilagođena je korisnicima koji često koriste automobil. Ugrađeni uređaj korisniku omogućuje da u svakom trenutku ima automatski aktiviranu pomoć na cesti u slučaju nezgode. Ugradnja uređaja je besplatna.⁷⁶

⁷⁴ <https://www.intesasanpaoloassicura.com/assicurazione-auto>

⁷⁵ <https://www.intesasanpaoloassicura.com/assicurazione-auto/viaggia-con-me-correntisti>

⁷⁶ <https://www.intesasanpaoloassicura.com/assicurazione-auto/viaggia-con-me-correntisti>

5.1.4. Allianz

Allianz osiguranje nudi proizvod Columbus za osiguranje plovila.⁷⁷ Proizvod se zasniva na Nautisat 24 uređaju. Nautisat 24 je satelitski uređaj koji se nudi preko partnerske tvrtke. Uređaj se može samostalno instalirati na plovilo, i u slučaju nezgode potrebno je pritisnuti alarm na uređaju kako bi korisnik prenio svoju točnu lokaciju. Operativni centar po primitku signala alarma poduzeti mjere kako bi se korisniku pružila pomoć.

Ukoliko korisnik želi ovaj uređaj morati će ga posebno platiti. Korisnik uređajem dobiva dodatnu zaštitu i sigurnost prilikom plovidbe.

Osiguravajuća kuća ovim proizvodom može smanjiti rizike koje mogu nastati u slučaju nezgode na moru.

5.1.5. Cattolica Assicurazioni

Cattolica Assicurazioni nudi proizvod Autopiu za osiguranje automobila.⁷⁸ Korisnik može odabrati dvije opcije proizvoda. Autopiu Live uređaj i Autopiu Box uređaj.

Autopiu Live uređaj se ugrađuje na vjetrobransko staklo i namijenjen je korisnicima koji žele imati dodatnu sigurnost prilikom vožnje. Pomoću uređaja korisnik može: komunicirati sa operativnim centrom u slučaju nezgode, jednim pritiskom na gumb alarma pozvati pomoć, te pratiti stil vožnje. Autopiu Box je dodatak na Live uređaj i namijenjen je korisnicima koji žele dodatno osigurati vozilo od rizika krađe. Uređaj omogućuje praćenje automobila u realnom vremenu.

Osiguravajuća kuća ovim proizvodom može smanjiti rizike koje mogu nastati u slučaju nezgode i krađe vozila.

Oba uređaja potrebno je ugraditi u ovlaštenim servisnim radionicama.

⁷⁷ <https://www.allianz.it/le-soluzioni-per-te/mobilita/nautica/allianz-columbus.html>

⁷⁸ <https://www.cattolica.it/active-veicoli-autopiu/>

5.1.6. Reale Mutua Assicurazioni

Reale Mutua osiguranje nudi nekoliko proizvoda za auto osiguranje.⁷⁹ Proizvod Real Automia Full Box se zasniva na uređaju koji omogućuje praćenje podataka o vožnji u realnom vremenu. Preko uređaja korisnik može pratiti lokaciju svojeg vozila, kontaktirati operativni centar u slučaju nezgode na cesti, dobiti popust na policu osiguranja ili onemogućiti korištenje vozila u slučaju krađe. Popust na policu osiguranja korisnik može dobiti jer pomoću podatka sa uređaja osiguranje kreira profil vozača.

Korisnik može dodatno birati između četiri modela proizvoda. Ovisno o broju i vrstu ugrađenih senzora, korisnik može dobiti različite popuste prilikom obnove osiguranja ili na pokriće u slučaju krađe.⁸⁰

Osiguravatelj ovim proizvodom želi smanjiti rizike od krađe vozila, te zadržati klijenta omogućujući mu popust na obnovu police zavisno o stilu vožnje vozača.

⁷⁹ <https://www.realemutua.it/veicoli-e-viaggi/assicurazione-auto>

⁸⁰ <https://www.realemutua.it/veicoli-e-viaggi/assicurazione-auto/full-box-reale>

5.2. Analiza proizvoda

Analiza pregleda primjene IoT tehnologije na tržištu Italije napravljena je prikupljanjem dostupnih podataka putem Internet stranica osiguravajućih društava. Analizirani su slijedeći proizvodi:

1. Generali Imagine New Roads
2. UnipolSai – Unibox
3. Intesa Sanpaolo – ViaggiaConMe
4. Allianz – Columbus
5. Cattolica – Autopiu
6. Reale Mutua - Real Automia Full Box

Analiza i usporedba proizvoda napravljena je u nekoliko kategorija:

- Je li proizvod aktivan?
- Koji senzori su korišteni u proizvodima?
- Koji podaci se prikupljaju?
- Koje su koristi za korisnika osiguranja?
- Koje su koristi za osiguravajuće društvo?
- Koje su koristi za zajednicu?
- Koji je model suradnje prilikom izlaska na tržište?

Tablica 5-1 prikazuje i analizira navedene proizvode.

Tablica 5-1. Analiza proizvoda na tržištu Italije

	Generali – Imagine New Roads	UnipolSai – Unibox	Intesa Sanpaolo - ViaggiaConMe	Allianz - Columbus	Cattolica - Autopiu	Reale Mutua - Real Automia Full Box
Aktivan	Da	Da	Da	Da	Da	Da
Vrsta	Osiguranje vozila	Osiguranje vozila	Osiguranje vozila	Osiguranje plovila	Osiguranje vozila	Osiguranje vozila
Korišteni senzori	GPS Senzor ubrzanja Žiroskop	GPS Senzor ubrzanja Žiroskop	GPS Senzor ubrzanja Žiroskop	GPS	GPS Senzor ubrzanja Žiroskop	GPS Senzor ubrzanja Žiroskop
Vrsta prikupljenih podataka	Lokacija Ubrzanje Kočenje Kretanje vozila Vrijeme	Lokacija Ubrzanje Kočenje Kretanje vozila Vrijeme	Lokacija Ubrzanje Kočenje Kretanje vozila Vrijeme	Lokacija Vrijeme	Lokacija Vrijeme	Lokacija Ubrzanje Kočenje Kretanje vozila Vrijeme
Korist za kupca	Niža cijena police. Pomoć u slučaju nezgode. Pravni dokazi.	Niža cijena police. Fleksibilno korištenje osiguranja prema potrebi klijenata Pomoć u slučaju nezgode. Pravni dokazi.	Fleksibilno korištenje osiguranja prema potrebi klijenata. Proizvod namijenjen vozačima koji manje voze.	Sigurnost tijekom plovidbe. Brza reakcija u slučaju nezgode.	Pomoć u slučaju nezgode.	Niža cijena police. Pomoć u slučaju nezgode.

Korist za osiguravajuće društvo	Sprječavanje prijevara. Smanjivanje iznosa štete. Dugoročne i čvrste veze sa korisnikom.	Sprječavanje prijevara. Smanjivanje iznosa štete. Dugoročne i čvrste veze sa korisnikom.	Pribavljanje klijenata koji nemaju potrebu za potpunim osiguranjem. Smanjivanje rizika poticanjem manje uporabe automobila.	Smanjivanje rizika i smanjivanje štete.	Smanjivanje rizika krađe vozila.	Smanjivanje iznosa štete. Smanjivanje rizika osiguranja profiliranjem vozača. Dugoročne i čvrste veze sa korisnikom
Korist za zajednicu	Povećanje sigurnosti prometa.	Povećanje sigurnosti prometa.	Povećanje sigurnosti prometa. Poticanje vožnje alternativnim načinima prijevoza. Smanjenje emisije CO2.	Povećanje sigurnosti prometa na moru.	Povećanje sigurnosti prometa.	Povećanje sigurnosti prometa.
Model suradnje	Vlastiti razvoj.	Vlastiti razvoj.	Kolaboracija sa postojećim partnerima	Kolaboracija sa postojećim partnerima	Kolaboracija sa postojećim partnerima.	Vlastiti razvoj.

6. Zaključak

IoT tehnologija ostvaruje veliki rast i primjenjuje se u industriji osiguranja, a očekuje se i pojačana primjena u budućnosti. Široki spektar senzora omogućuje njeno korištenje u razvoju proizvoda u industriji osiguranja.

Prilikom prihvaćanja IoT tehnologije, osim njenih prednosti nužno je prihvatiti i nositi se s izazovima koje donosi. Najveći izazovi su sigurnost od kibernetičkih napada, zaštita podataka i ispravno postupanje s podacima zbog osjetljivih informacija o korisnicima. Ostali izazovi su interoperabilnost, troškovi implementacije i analiza velikih količina podataka.

Prednosti IoT tehnologije su povećanje sigurnosti u prometu, povećanje sigurnosti nad vlasništvom, poboljšanje zdravstvene zaštite, brži protok informacija u različitim procesima u osiguranju, razvoj novih i personaliziranih proizvoda, smanjenje rizika od pojave šteta te smanjenje troškova.

IoT tehnologija može se primjenjivati u osiguranju imovine, vozila, plovila, praćenja robe, zdravlja ljudi, kućnih ljubimaca i putnom osiguranju.

Na našem tržištu trenutno postoje četiri aktivna proizvoda u osiguranju koja koriste IoT tehnologiju. Postojala su još dva proizvoda koji više nisu aktivni. Aktivni proizvodi su iz domene osiguranja plovila, vozila i zdravlja. U tri od četiri proizvoda prikupljaju se podaci o korisnicima i iskorištavaju se mogućnosti i potencijal IoT tehnologije. Jedan aktivni proizvod ne skuplja podatke i nudi samo popust na policu imatelju senzora.

Na tržištu razvijene članice Europske unije (Italija), analizirano je deset najvećih osiguravajućih društava. Šest ih nudi proizvode koje koriste IoT tehnologiju, od toga pet nudi proizvode za osiguranje automobila i jedno za osiguranje plovila.

U usporedbi sa Republikom Hrvatskom, tržište u Italiji je razvijenije jer nudi više različitih proizvoda osiguranja vozila koji se zasnivaju na IoT tehnologiji. Na tržištu Italije postoje i više osiguravajućih društava koji imaju proizvode razvijene na IoT tehnologiji. Korisnik može izabrati više različitih proizvoda osiguranja i modela uređaja. Odabir ovisi o potrebama korisnika, načinu dodijeljenog popusta na policu osiguranja i načinu nabave uređaja. Za razliku od tržišta Republike Hrvatske, osiguravajuća društva u Italiji više koriste podatke prikupljene s IoT uređaja. Zanimljiv podatak je da, za razliku od tržišta Republike Hrvatske, prikupljene

podatke u Italiji može koristiti i policija u svrhu dokazivanja krivnje, te u slučaju potrebe za rekonstrukcijom nesreće.

Pregledom i analizom tržišta u Republici Hrvatskoj i Italiji vidimo da se IoT tehnologija koristi većinom u osiguranju vozila i manjim dijelom u osiguranju plovila. Možemo zaključiti da potencijal IoT tehnologije u industriji osiguranja nije dovoljno iskorišten. Osiguravajuća društva nisu značajno unaprijedila svoje usluge i proizvode. Budući da je financijska industrija tradicionalna i tromija u prihvaćanju novih tehnoloških trendova, možemo zaključiti da je tek probijen led u prihvaćanju IoT tehnologije. U budućnosti možemo očekivati razvoj većeg broja proizvoda koji koriste IoT tehnologiju. Kako bi osiguravajuća društva koristila puni potencijal IoT tehnologije potrebna im je tehnološka transformacija i suradnja sa startup zajednicom koja je naprednija i dinamičnija u razvoju inovativnih proizvoda s IoT tehnologijom.

7. Popis literature

➤ Internetski izvor

- [1] Zdrilić M, sinvest.com.hr/clanak/14, Suvremene promjene i digitalizacija u industriji osiguranja (10. svibanj 2024.)
- [2] Marović B., Njegomir V., Novi trendovi koji transformiraju osiguranje i reosiguranje;
<http://sors.ba/UserFiles/file/SorS/2022/Zbornik/01%20Sors%202022%20-%20Zbornik%20radova%20-%20Marovic.pdf> (10. svibanj 2024.)
- [3] Mihelja Žaja M., Milanović Glavan Lj., Grgić M., Digitalna tehnologija kao čimbenik razvoja kanala distribucije u osiguranju; <https://hrcak.srce.hr/242255> (10. svibanj 2024.)
- [4] Marović B., Njegomir V., Novi trendovi koji transformiraju osiguranje i reosiguranje;
<http://sors.ba/UserFiles/file/SorS/2022/Zbornik/01%20Sors%202022%20-%20Zbornik%20radova%20-%20Marovic.pdf> (10. svibanj 2024.)
- [5] <https://www.cert.hr/sigurnost-interneta-stvari-IoT/> (11. svibanj 2024.)
- [6] <https://www.statista.com/statistics/1194677/IoT-connected-devices-regionally/> (11. svibanj 2024.)
- [7] <https://duplico.io/sto-je-IoT-ili-internet-of-things/> (11. svibanj 2024.)
- [8] <https://www.dataversity.net/brief-history-internet-things/> (11. svibanj 2024.)
- [9] <https://www2.deloitte.com/tr/en/pages/financial-services/articles/innovation-in-insurance-internet-of-things-IoT.html> (18. svibanj 2024.)
- [10] <https://www.youtube.com/watch?v=yMdTgsqWGAA> (18. svibanj 2024.)
- [11] <https://www.embedded.com/sensor-systems-in-the-industrial-IoT/> (18. svibanj 2024.)
- [12] <https://www.theIoTAcademy.co/blog/sensor/> (21. svibanj 2024.)
- [13] <https://emanuelepagliari.it/2020/10/13/internet-of-things-wireless-communication-protocols/> (21. svibanj 2024.)

- [14] <https://www.videostrong.com/news-show/wifi-zigbee-ble-for-smart-home>
(21.svibanj 2024.)
- [15] <https://www.nabto.com/guide-IoT-protocols-standards/> (21.svibanj 2024.)
- [16] <https://emanuelepagliari.it/2020/10/13/internet-of-things-wireless-communication-protocols/> (21.svibanj 2024.)
- [17] G. Dregvaite; R. Damasevicius (30 October 2016). Information and Software Technologies: 22nd International Conference, ICIST 2016 (21.svibanj 2024.)
- [18] <https://www.sigfox.com/coverage/> (21.svibanj 2024.)
- [19] <https://www.emnify.com/blog/IoT-challenges-2023> (21.svibanj 2024.)
- [20] <https://www.peerbits.com/blog/biggest-IoT-security-challenges.html>
(21.svibanj 2024.)
- [21] <https://www.scs.org.sg/articles/IoT-security-how-to-secure-your-devices>
(21.svibanj 2024.)
- [22] <https://www.geeksforgeeks.org/advantages-and-disadvantages-of-IoT/>
(21.svibanj 2024.)
- [23] <https://www.geeksforgeeks.org/advantages-and-disadvantages-of-IoT/>
(21.svibanj 2024.)
- [24] <https://www.semanticscholar.org/paper/Smart-Homes%3A-Past%2C-Present-and-Future-Aldrich/34c0fb597f6314cc8a676614358705bece01d112> (24.svibanj 2024.)
- [25] <https://www.nawy.com/blog/34382-welcome-to-the-future-pros-and-cons-of-smart-homes> (24.svibanj 2024.)
- [26] <https://exterim.hr/blog/najbolji-pametni-termostati-2019-55/> (24.svibanj 2024.)
- [27] <https://hr.xiaomiplanet.sk/xiaomi-pametna-kamera-c400-globalno/> (24.svibanj 2024.)
- [28] <https://led-zarulje.com/detektor-pokreta-svjetla-360-bijeli-ip20-st07/>
(24.svibanj 2024.)
- [29] <https://www.svjetlo.hr/pametna-rasvjeta> (24.svibanj 2024.)

- [30] <https://www.svijet-svjetiljki.hr/solight-1d39-detektor-dima-i-ugljicnog-monoksida-1-5v-3xaa/> (24.svibanj 2024.)
- [31] <https://wiproconsumerlighting.com/products/smart-product/smart-doorbell/wipro-smart-wireless-doorbell-black%C2%A02-mp-1080p-full-hd-camera> (24.svibanj 2024.)
- [32] <https://homemate.co.in/product/door-window-sensor/> (24.svibanj 2024.)
- [33] <https://www.x-sense.com/products/sws51-smart-water-leak-detector> (24.svibanj 2024.)
- [34] <https://mi.hr/mi-smart-plug-wifi.html> (24.svibanj 2024.)
- [35] <https://IoT4beginners.com/self-driving-cars-and-IoT/> (24.svibanj 2024.)
- [36] <https://www.cigniti.com/blog/IoT-insurance-use-cases-benefits/> (24.svibanj 2024.)
- [37] <https://www.sense4boat.com/hr/proizvod/pametna-senzor-baterije/> (24.svibanj 2024.)
- [38] <https://www.sense4boat.com/hr/proizvod/pametna-senzor-kaljuze/> (24.svibanj 2024.)
- [39] <https://www.sense4boat.com/hr/proizvod/pametna-senzor-temperature/> (24.svibanj 2024.)
- [40] <https://www.sense4boat.com/product/smart-smoke-sensor/> (24.svibanj 2024.)
- [41] <https://www.sense4boat.com/product/smart-gps-locator/> (24.svibanj 2024.)
- [42] <https://www.tres.in/shop/product/tres-smart-watch-care-c303/> (24.svibanj 2024.)
- [43] <https://www.munichre.com/us-life/en/perspectives/wearables/wearables-the-future-is-now-wearables-for-insurance-risk-asses.html> (01.lipanj 2024.)
- [44] Galina V. Ivankova; Internet of Things (IoT) in logistics; (<https://iopscience.iop.org/article/10.1088/1757-899X/940/1/012033/pdf>) (01.lipanj 2024.)
- [45] <https://www.capgemini.com/wp-content/uploads/2020/05/IoT-Insurance-of-Things-1.pdf> (01.lipanj 2024.)

- [46] <https://www2.deloitte.com/tr/en/pages/financial-services/articles/innovation-in-insurance-internet-of-things-IoT.html> (01.lipanj 2024.)
- [47] <https://fintechos.com/blogpost/6-ways-IoT-devices-are-changing-home-insurance/> (01.lipanj 2024.)
- [48] <https://www.nerdwallet.com/article/insurance/smart-home-insurance-discount> (01.lipanj 2024.)
- [49] https://www.seedrs.com/hiro?utm_source=wordpress&utm_medium=blog&utm_term=hiro_campaignspotlight (04.lipanj 2024.)
- [50] <https://www.mckinsey.com/industries/financial-services/our-insights/insurance-2030-the-impact-of-ai-on-the-future-of-insurance> (04.lipanj 2024.)
- [51] <https://research.aimultiple.com/insurance-IoT/#3-customized-insurance-practices> (04.lipanj 2024.)
- [52] <https://www.forbes.com/sites/blakemorgan/2018/05/16/heres-how-IoT-will-impact-the-insurance-claims-process/?sh=15e29184366e> (06.lipanj 2024.)
- [53] <https://www.the-digital-insurer.com/wp-content/uploads/2019/02/1437-ParksAssoc-LeveragingSmartHomeforInsuranceBusinessModels.pdf> (04.lipanj 2024.)
- [54] <https://www.iskon.hr/O-Iskonu/Press-centar/Press/Iskon.Smarthome-sustav-za-upravljanje-domom-na-daljinu> (04.lipanj 2024.)
- [55] <https://crosig.hr/osiguranje-plovila/kasko-osiguranje-brodica-i-jahti/> (04.lipanj 2024.)
- [56] <https://www.sense4boat.com/> (04.lipanj 2024.)
- [57] <https://www.uniqa.hr/o-nama/vijesti/smart-kasko-prvo-kasko-osiguranje-koje-placas-koliko-vozis/4235> (05.lipanj 2024.)
- [58] <https://www.uniqa.hr/kampanje/usk/privacy/4222> (05.lipanj 2024.)
- [59] <https://coverager.com/amodo-introduces-next-generation-pay-per-mile/> (05.lipanj 2024.)
- [60] <https://www.laquo.hr/laquo-prevent/> (05.lipanj 2024.)

- [61] <https://www.bug.hr/mobilne-aplikacije/vozio-sam-mjesec-dana-uz-telematiku-laqoprevent--jesam-li-sada-bolji-vozac-20477> (05.lipanj 2024.)
- [62] https://media.laqa.hr/uploads/laqa_prevent_210x297_13102022_715753cc86.pdf (05.lipanj 2024.)
- [63] <https://www.laqa.hr/zastita-privatnosti/> (05.lipanj 2024.)
- [64] <https://www.toyota.hr/owners/warranty/full-hybrid-insurance> (05.lipanj 2024.)
- [65] Generali osiguranje uvjeti osiguranja; FHI_Toyota hybrid osiguranje.pdf (05.lipanj 2024.)
- [66] <https://crosig.hr/croatia-fit/> (05.lipanj 2024.)
- [67] <https://crosig.hr/croatia-fit/> (05.lipanj 2024.)
- [68] <https://www.worldatlas.com/articles/the-biggest-insurance-groups-in-italy.html> (10.lipanj 2024.)
- [69] <https://www.generalit.it/preventivatori/preventivatore-auto-quota-facile/conosciamoci> (10.lipanj 2024.)
- [70] <https://www.generalit.it/magazine/auto/scatola-nera#e> (10.lipanj 2024.)
- [71] <https://www.unipolsai.it/unibox-2ruote> (10.lipanj 2024.)
- [72] <https://www.unipolsai.it/unibox-auto> (10.lipanj 2024.)
- [73] <https://www.unipolsai.it/plus/mobilita/scatola-nera-smart> (12.lipanj 2024.)
- [74] <https://www.intesasanpaoloassicura.com/assicurazione-auto> (12.lipanj 2024.)
- [75] <https://www.intesasanpaoloassicura.com/assicurazione-auto/viaggia-con-me-correntisti> (12.lipanj 2024.)
- [76] <https://www.intesasanpaoloassicura.com/assicurazione-auto/viaggia-con-me-correntisti> (12.lipanj 2024.)
- [77] <https://www.allianz.it/le-soluzioni-per-te/mobilita/nautica/allianz-columbus.html> (12.lipanj 2024.)
- [78] <https://www.cattolica.it/active-veicoli-autopiu/> (12.lipanj 2024.)
- [79] <https://www.realemutua.it/veicoli-e-viaggi/assicurazione-auto> (12.lipanj 2024.)

[80] <https://www.realemutua.it/veicoli-e-viaggi/assicurazione-auto/full-box-reale>
(12.lipanj 2024.)

Životopis

Tomislav Oreški rođen je 25.06.1981. godine u Zagrebu. U Zagrebu je završio osnovnu školu i XV. Gimnaziju. 2006. Godine završava Fakultet elektrotehnike i računarstva. Tomislav je Enterprise architect u Croatia osiguranju. Ima više od 15 godina iskustva u području razvoja i implementacije IT sustava (arhitektura, analiza, dizajn, razvoj, testiranje, integracija servisa i komponenata). Tomislav ima iskustva u implementacijama velikih poslovnih informacijskih sustava za javni sektor i u području financija, kao što su: središnji informatički sustavi osiguravajućih društava, informatički sustavi Porezne uprave i Ministarstva uprave, razvoj informacijskog sustava za HZJZ (Hrvatski zavod za javno zdravstvo).

Biography

Tomislav Oreški was born in Zagreb on June 25, 1981. He attended primary school and high school in Zagreb. In 2006 he graduated at the Faculty of Electrical Engineering and Computer Science. Tomislav is a Enterprise architect at Croatia osiguranje. He has more than 15 years of work experience in field of development and implementing of ICT systems (architecture, analyse, design, development, testing, deployment and integration of software solutions and components). He has experience in implementation of large business information systems in finance and public sector like: Core information systems for insurance industry, information system for Tax Administration, development of information system for Croatian Office for Public Health.