Procjena rizika informacijskog sustava temeljenog na konceptu Interneta stvari

Zrinski, Petar

Sveučilište u Zagrebu
Fakultet prometnih znanosti

Petar Zrinski

Procjena rizika informacijskog sustava temeljenog na konceptu Interneta stvari

Diplomski rad

Zagreb, 2022.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
POVJERENSTVO ZA DIPLOMSKI ISPIT

Zagreb, 4. svibnja 2022.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Sigurnost i zaštita informacijsko komunikacijskog sustava**

DIPLOMSKI ZADATAK br. 6918

Pristupnik: **Petar Zrinski (0135234305)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Procjena rizika informacijskog sustava temeljenog na konceptu Interneta stvari**

Opis zadatka:

U radu je potrebno prikazati principe rada koncepta Interneta stvari i mogućnosti njegove primjena u industriji i poljoprivredi. Opisati sigurnosne aspeket primjene IoT. Potrebno je i prikazati opis sustava temeljnog na konceptu Interneta stvari. Opisati proces procjene rizika u informacijskom sustavu te napraviti procjenu za zamišljeni use case.

Mentor:

prof. dr. sc. Dragan Peraković

Predsjednik povjerenstva za diplomski ispit:

Sveučilište u Zagrebu
Fakultet prometnih znanosti

DIPLOMSKI RAD

Procjena rizika informacijskog sustava temeljenog na konceptu Interneta stvari

Mentor: prof. dr. sc. Dragan Peraković

Student: Petar Zrinski
JMBAG: 0135234305

SAŽETAK

Sve šira primjena Interneta stvari u industriji dovela do je eksponencijalnog rasta broja IoT uređaja pa se samim time sve veći fokus stavlja na aspekte sigurnosti i upravljanja rizikom u IoT sustavima. Procjena rizika za potrebe ovog rada provedena je nad konceptualnim informacijskim sustavom koji je utemeljen na konceptu Interneta stvari. Predmetni sustav služi za mjerenje parametara upotrebom raznih senzora te upravlja nizom aktuatora za različite svrhe u poljoprivredi, na primjer u sustavima za navodnjavanje, komorama za zrenje suhomesnatih proizvoda, posudama za fermentaciju vina itd. Sva mjerenja pohranjuju se u centralnom sustavu koji također upravlja aktuatorima, a sve to preko interneta. Procjena rizika provedena je prema NIST-ovim smjernicama uz specifične dorade potrebne za ovaj rad. Na temelju provedene procjene utvrđen je rizik nad imovinom te su dane preporuke za smanjenje te vrste rizika.

KLJUČNE RIJEČI: IoT; sigurnost; poljoprivreda; procjena rizika

SUMMARY

The increasing use of the Internet of Things in industry has led to an exponential growth in the number of IoT devices, which is why a growing focus is being placed on the aspects of security and risk management in IoT systems. For the purpose of this paper, a risk assessment was performed with regard to a conceptual information system based on the concept of the Internet of Things. The system in question is used to measure parameters using various sensors, and it controls a number of actuators for various agricultural purposes. for example those in irrigation systems, chambers for maturing cured meat products, wine fermentation vessels, etc. All measurements are stored in a central system that also controls the actuators, and all of this is done over the internet. The risk assessment was performed according to the NIST guidelines, with specific modifications necessary for the purposes of this paper. Asset risk was identified on the basis of the performed assessment, and recommendations were made to mitigate this type of risk.

KEYWORDS: IoT; security; agriculture; risk assessment

Sadržaj

1. Uvod

U ovom radu bit će predstavljen koncept informacijskog sustava temeljenog na konceptu interneta stvari. Predstavljeni informacijski sustav služi za nadzor i kontrolu različitih parametara, a neki od njih su temperatura i relativna vlažnost zraka, temperatura i relativna vlažnost tla, strujanje zraka, količina svjetlosti, potrošnja vode itd. Sustav je prvenstveno namijenjen malim poljoprivrednicima i onima koji se poljoprivredom bave u slobodno vrijeme.

Svrha je ovog rada utvrditi na koji će se način provoditi procjena rizika za predstavljeni informacijski sustav te koje se pretpostavke i ograničenja pojavljuju kod procjene rizika.

Rad je podijeljen u sedam poglavlja, od kojih je Uvod prvo poglavlje, a Zaključak posljednje poglavlje. Drugo poglavlje, Koncept interneta stvari i njegova primjena u industriji i poljoprivredi, daje pregled primjene interneta stvari u industriji i poljoprivredi općenito. Ondje su također prikazani i objašnjeni osnovni koncepti koji se upotrebljavaju u IoT ekosustavu, kao što su računalstvo u oblaku, strojno učenje, digitalni blizanci i ostalo.

Treće poglavlje, Sigurnost u IoT sustavima, daje pregled osnovnih pojmova o sigurnosti informacijskih sustava i interneta stvari.

U četvrtom poglavlju, Opis sustava temeljenog na internetu stvari, navode se i detaljno opisuju elementi informacijskog sustava temeljenog na konceptu interneta stvari predstavljenog u ovom radu. Odgovarajućim UML dijagramima prikazane su logička i fizička arhitektura sustava te razmjena informacija između elemenata sustava.

Peto poglavlje, Proces procjene rizika u informacijskom sustavu, sadržava detaljan prikaz procesa procjene rizika za predstavljeni sustav kao i metode za vrednovanje imovine.

U šestom poglavlju, Procjena rizika za informacijski sustav, prikazani su rezultati provedbe procjene rizika nad predstavljenim informacijskim sustavom. Za informacijski sustav utvrđena je imovina sustava te su određene relevantne prijetnje i uzroci prijetnji prema imovini. Utvrđene su i ranjivosti pojedinih elemenata informacijskog sustava, vjerojatnosti ostvarivanja prijetnji te utjecaji na operacije i imovinu u slučaju ostvarivanja prijetnje. Na kraju će biti iskazani rezultati procjene rizika kao i preporuke za smanjenje rizika za imovinu predstavljenog informacijskog sustava.

2. Koncept interneta stvari i njegova primjena u industriji i poljoprivredi

Sve do prije otprilike 10.000 godina *homo sapiens* živio je nomadskim načinom života lovca sakupljača. Lovci sakupljači živjeli su u malenim i usko povezanim zajednicama. Tipičan dan tadašnjeg *homo sapiensa* sastojao se od lova na divljač te prikupljanja šumskih plodova i raznih bobica za prehranu. S vremena na vrijeme skupina lovaca sakupljača selila se u druge krajeve kako bi si osigurala hranu. Prije otprilike 10.000 godina došlo je do pojave agrarne revolucije, odnosno prelaska s nomadskog na sjedilački način života, te su time ispunjeni preduvjeti za razvoj prvih primitivnih tehnologija. Ljudi su počeli pripitomljavati divlje biljke i životinje, pa su tako započete i prve djelatnosti, kao što su ratarstvo i stočarstvo. Tisućama godina nakon toga ljudi su živjeli s više-manje nepromijenjenom tehnologijom. Do eksponencijalnog rasta i razvoja tehnologije dolazi u 15. stoljeću, kada u Europi dolazi do znanstvene revolucije. Znanstvena revolucija u prvom je redu započela sa spoznajom da čovječanstvo ne zna i nema odgovore na sva pitanja. Nastavkom ulaganja u znanost i istraživačke ekspedicije diljem svijeta, ponajviše financirane od strane tada najvećih imperija poput Velike Britanije, Španjolske, Portugala i Nizozemske, došlo se do spoznaje da čovjek može upravljati pretvorbom energije iz jednog oblika u drugi. Tako je u 18. stoljeću baš u Velikoj Britaniji došlo do izuma parnog stroja za potrebe ispumpavanja vode u ugljenokopima. U tom trenutku započinje prva industrijska revolucija, koju obilježava mehanizacija. Svako novo znanstveno otkriće dalo je ljudima sve veću želju za ponovnim ulaganjem kapitala u razvoj znanosti. Tako je do početka druge industrijske revolucije prošlo svega oko 100 godina. Drugu industrijsku revoluciju obilježili su novi oblici energije kao što su nafta i električna energija te pomak načina proizvodnje dobara s pojedinačnih proizvoda na masovnu proizvodnju na pokretnim trakama. Trebalo je proći još nešto manje od 100 godina do pojave treće industrijske revolucije. Treća industrijska revolucija još se naziva i digitalnom revolucijom, a nastupila je oko 1980. godine pojavom računala te digitalnih i telekomunikacijskih tehnologija. Digitalnu revoluciju u pogledu industrije karakterizira visoka automatizacija proizvodnih procesa, kao što su robotizirani i automatizirani proizvodni pogoni, na primjer u tvornicama automobila. Danas, u 2022. godini, nalazimo se duboko u četvrtoj industrijskoj revoluciji, koja je poznata još pod nazivom industrija 4.0 [1], [2].

Koncept industrije 4.0 predstavlja pomak u industriji prema automatizaciji procesa i razmjeni podataka između pametnih entiteta. Proizvodna industrija sve više integrira nove tehnologije u svoja postrojenja, uključujući tehnologije poput interneta stvari (eng. *Internet of Things,* IoT),

računalstva u oblaku (eng. *Cloud Computing*, CC), strojnog učenja (eng. *Machine Learning*, ML) te umjetne inteligencije (eng. *Artificial Intelligence*, AI) [3], [4].

2.1 Internet stvari

Glavni dio industrije 4.0 je internet stvari (eng. *Internet of Things*, IoT). Internet stvari omogućava heterogenoj skupini strojeva, senzora, mrežnih sustava i ostalih entiteta međusobnu povezanost u svim smjerovima, prikupljanje i razmjenu podataka s centraliziranim sustavima za obradu podataka, ali i međusobnu razmjenu podataka [5]. Sve to u gotovo stvarnom vremenu i bez potrebe za interakcijom s čovjekom. Pojam "internet stvari" ili "IoT" generalno opisuje povezane sustave i uređaje koje upotrebljavaju krajnji korisnici (npr. pametne kuće, pametni kućni uređaji itd.), dok pojam "industrijski internet stvari" (eng. *Industrial Internet of Things*, IIoT) opisuje povezane sustave i uređaje u proizvodnji [3], [4], [6]. IoT u posljednje vrijeme postaje jedna od najrelevantnijih tehnologija u svijetu informacijskih tehnologija [7].

Broj IoT uređaja 2015. godine iznosio je oko 3,6 milijardi, dok je 2021. godine taj broj iznosio oko 12,3 milijarde. Procjene budućeg broja IoT uređaja vrlo su različite, no svim je procjenama zajednički zaključak da će u budućnosti broj IoT uređaja izrazito rasti. Prema [6] procjenjuje se da će do 2025. godine na svijetu biti između 40 i 75 milijardi uređaja. S druge strane, prema [8] procjenjuje se da će 2025. godine na svijetu biti oko 27,1 milijarde IoT uređaja, budući da procjene u tom izvoru uzimaju u obzir globalnu nestašicu čipova uzrokovanu pandemijom koronavirusa. No unatoč svemu i dalje se očekuje značajan porast broja IoT uređaja.

IoT ekosustav sastoji se od nekoliko osnovnih komponenti. Prva su komponenta sustava naravno sami IoT uređaji. S obzirom na to da se komunikacija temelji na internetu, onda je druga komponenta ekosustava komunikacijska tehnologija, budući da je za spajanje uređaja na internet potrebna komunikacijska tehnologija s pripadajućim pristupnikom (eng. *gateway*). Na kraju su još potrebni sustavi računalnih oblaka kako bi se obradili i pohranili podaci s IoT uređaja.

Pametnim entitetom (koristi se još i izraz "pametna stvar") može se smatrati svaki uređaj, stroj, naprava, nekretnina, pokretnina, industrijsko postrojenje, radni stroj, farma, kućanski uređaj itd., koji je preko komunikacijske mreže povezan s drugim pametnim entitetima te koji ima sposobnost prikupljanja i razmjene podatka s drugim entitetima unutar mreže. Većini pametnih entiteta pametne su značajke (odnosno značajke koje omogućavaju pametnom entitetu prikupljanje i razmjenu podatka) određene već u fazi planiranja entiteta (faza planiranja proizvoda), pa tako danas sve veći broj vozila i kućanskih uređaja dolazi s etiketom pametnog entiteta. Entitet također može postati

pametnim entitetom s pomoću naknadnih nadogradnji koje mu omogućavaju prikupljanje i razmjenu podataka.

2.2 Primjena interneta stvari u industriji i poljoprivredi

Sve je veća primjena interneta stvari u industriji, naročito kada se radi o velikim poduzećima kojima i mala optimizacija operativnih procesa donosi velike novčane uštede. Internet stvari u industriji se upotrebljava u mnogo različitih sektora i na mnogo različitih načina. Francuski proizvođač aviona Airbus u svojim je proizvodnim pogonima ugradio senzore u alate te je u kombinaciji s pametnim naočalama koje nose zaposlenici povećana sigurnost zaposlenika i smanjen broj grešaka prilikom sastavljanja aviona. Poduzeće Caterpillar svoje je radne strojeve opremio IoT senzorima, pa osobe koje su zadužene za upravljanje strojevima imaju pristup aplikaciji s pomoću koje dobivaju puni pregled nad strojem, od toga koliko ima goriva do toga kada je potrebno zamijeniti filtar zraka, a preko aplikacije mogu također dobiti i osnovne upute za servisiranje radnog stroja kako bi se smanjilo vrijeme kada je stroj izvan rada (eng. *downtime*). Proizvođač robotskih postrojenja Fanuc opremio je sve robotske elemente senzorima i s pomoću analize podatka sa senzora predviđaju moguće greške na komponentama i preventivno ih zamjenjuju. Struka je prepoznala inovativnost i korisnost te je američki proizvođač GM nagradio Fanucov sustav *Zero Downtime* nagradom *Supplier of the Year Innovation Award*. Poduzeće John Deere jedno je od najistaknutijih poduzeća kada je riječ o internetu stvari u području poljoprivrede, najviše zahvaljujući svojem razvoju autonomnih traktora i implementaciji preventivnog održavanja strojeva na temelju digitalnih blizanaca. Danska plovidbena kompanija Maersk ugrađuje senzore u kontejnere, naročito zbog nadzora i lokacije praznih kontejnera zbog kojih godišnje imaju oko milijardu američkih dolara troškova [9].

Neke od najčešćih primjena interneta stvari u poljoprivredi koje se pojavljuju kad se u internetsku tražilicu Google upiše pojam "*iot in agriculture"* upućuju na primjenu IoT-a u meteorološkim stanicama, automatizaciji plastenika i staklenika, nadzoru usjeva, nadzoru stoke, preciznoj poljoprivredi i poljoprivrednim dronovima. Neki od primjera IoT u poljoprivredi opisani su u nastavku.

Na primjer, pametne meteorološke stanice služe za prikupljanje podatka o temperaturi zraka, relativnoj vlažnosti zraka, brzini i smjeru vjetra, vlažnosti tla, količini sunčeva zračenja, količini padalina i sl. Podaci s meteoroloških stanica najjednostavnije se mogu upotrijebiti za upravljanje sustavima navodnjavanja kako bi se u potpunosti iskoristila dobrobit navodnjavanja i reducirala količina potrošene vode.

Automatizirani IoT plastenici mogu bez intervencije čovjeka regulirati parametre unutar plastenika. Putem senzora prikupljaju podatke o relativnoj vlažnosti tla, relativnoj vlažnosti zraka, temperaturi zraka i ostalo. Senzori prikupljene podatke šalju u jedinicu koja obrađuje te podatke. Jedinica za obradu podatka može se nalazi unutar samog plastenika, ali kada se radi o IoT plastenicima centralna jedinica često se nalazi na udaljenom računalu i najčešće je sa senzorima povezana putem interneta. Centrala jedinica tada upravlja aktuatorima unutar IoT plastenika kako bi se održali željeni parametri. Takvim način uzgoja biljaka ima više prednosti, neke od njih su manja potreba za zaštitom bilja zbog toga što se u kontroliranom ambijentu može spriječiti razvoj bolest i veći prinos plodova. Sve to bez potrebe za interakcijom čovjeka i sustava.

2.3 Tehnologije u IoT sustavima

U IoT sustavima upotrebljavaju se različite komunikacijske tehnologije. Odabir mrežne tehnologije najviše ovisi o potrebama IoT sustava i dostupnosti mrežne tehnologije na nekom području. Komunikacijska tehnologija može prema radiofrekvencijskom spektru biti svrstana u licencirani ili nelicencirani dio radiofrekvencijskog spektra. U tablici 1 stupac "Vrsta spektra" označava kojom se vrstom spektra koriste različiti standardi komunikacijskih tehnologija, pri čemu oznaka "L" označava licencirani radiofrekvencijski spektar, a "NL" nelicencirani radiofrekvencijski spektar.

Nelicencirani radiofrekvencijski spektar koristi se industrijskim i medicinskim radiofrekvencijskim spektrom poznatim pod nazivom "ISM". Nedostaci korištenja ISM radiofrekvencijskog spektra jesu veći sigurnosni rizici za sustav, viša cijena infrastrukture na strani korisnika te veća interferencija. S druge strane, licencirani radiofrekvencijski spektar nadoknađuje sve mane ISM radiofrekvencijskog spektra, ali uz višu cijenu pretplate za korisnika koja se većinom plaća po količini podataka koju prenose IoT uređaji.

Prema dometu signala komunikacijske tehnologije razvrstavaju se u sljedeće kategorije:

- P2P (eng. *Peer-to-peer*)
- WPAN (eng. *Wireless Personal Area Network*)
- WHAN (eng. *Wireless Home Area Network*)l
- WLAN (eng. *Wireless Local Area Network*)
- WWAN (eng. *Wireless Wide Area Network*)
- LPWAN (eng. *Low Power Wide Area Network*)

U vrstu mreže LPWAN spadaju standardi komunikacijskih tehnologija SigFox, LoRaWAN, NB-IoT. LPWAN mreža ima značajke vrlo velikog dometa signala uz vrlo malu snagu odašiljačkog

uređaja i malu brzinu prijenosa podataka. LPWAN mreža koristi se u IoT sustavima koji imaju mali promet podataka i nisku potrošnju energije, na primjer oni koji se upotrebljavaju za periodična mjerenja na udaljenim lokacijama. Primjer upotrebe LPWAN mreža mogu biti senzori za mjerenje vodostaja vode na rijekama i jezerima. U hrvatskoj uslugu korištenja NB-IoT tehnologije nude teleoperateri A1 i Hrvatski Telekom [10], [11], a pokrivenost NB-IoT signalom u Republici Hrvatskoj je 100 % [5]. LoRaWAN također spada u LPWAN standard radiotehnologije, no pokrivenost signalom je u Hrvatskoj trenutačno mala, te je trenutačno dostupna samo u četiri najveća grada; Zagreb, Split, Rijeka i Osijek [5], [12]. Dostupnost NB-IoT usluge u Republici Hrvatskoj je na 100% područja dok je dostupnost

Vrsta mreže WLAN jedna je od najzastupljenijih mreža te gotovo svako domaćinstvo u zapadnom svijetu ima pristup WLAN mreži, a najpoznatiji standard u WLAN mreži je 802.11a/b/g/n/ac poznatiji kao WiFi. WiFi se u IoT sustavima upotrebljava zbog svoje velike raširenosti i dostupnosti, ali ima nedostatka koji mu ograničavaju primjenu u određenim slučajevima. Jedan od nedostataka WiFi standarda jest taj da on zahtijeva više procesorske snage za komunikaciju s pristupnikom, što ujedno povećava potrošnju baterija IoT uređaja, dok je još jedan nedostatak domet WiFi signala, kao što je vidljivo u tablici 1, koji uglavnom iznosi 50 metara, pa mu je samim time i upotreba ograničena.

Jedna od mreža koje se danas upotrebljavaju u pametnim kućanstvima je i WHAN, a standardi u WHAN mrežama jesu ZigBee i Z-Wave. Iako ZigBee i Z-Wave upotrebljavaju isti radiofrekvencijski spektar, domet tih standarda višestruko je veći u odnosu na WiFi, iako nauštrb brzine prijenosa podataka koja je kod WHAN mreža višestruko manja. Danas se često ZigBee standard može vidjeti u primjeni u različitim *SmartHome* aplikacijama kao što je pametna rasvjeta i slično.

Za nosive IoT uređaje kao što su među ostalim pametni satovi, pametne narukvice i pametne naočale primjenjuje se vrsta mreže WPAN, u okviru koje je najpoznatiji standard svakako Bluetooth. Bluetooth standard ima relativno mali domet, manji od 100 m, i malu brzinu prijenosa podataka, između 2 i 26 Mbps. Ipak, novije inačice Bluetooth standarda zahtijevaju sve manje energije za razmjenu podataka.

Tablica 1: Karakteristike bežičnih komunikacijskih standarda korištenih u IoT sustavima

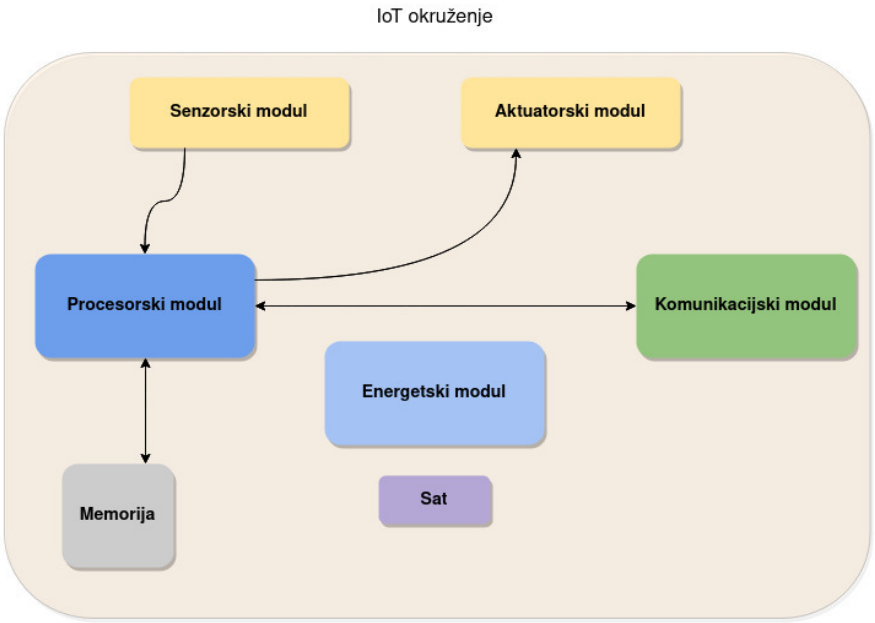
Izvor: [13]

Tip	Vrsta spektra	Domet	Vrsta mreže	Frekvencija	Dvosmjerna komunikacija	Brzina prijenosa podataka
802.11a/b/g/n/ac	NL	6 - 50m	WLAN	2,4GHz ili 5 GHz	DA	2 Mbps - 7 Gbps
802.11ah	NL	1km	WLAN	različite, manje od 1 GHz	DA	78 Mbps
802.11p	L	< 1 km	WLAN	5,9 GHz	DA	
SigFox	L	ruralni: 30-50 km, urbani: 3-10 km	LPWAN	868 MHz ili 902 MHz	DA	100 bps (uzlazno), 600 bps (silazno)
LoRaWAN	L	< 20 km	LPWAN	različite frekvencije manje od 1 GHz	DA	0,3 - 37,5 kbps
3GPP NB-IoT	L	< 35 km	LPWAN	450 MHz - 3,5 GHz	DA	250 kbps
WiMax	L i NL	50 - 80 km	WWAN	2 - 11 GHz, 10 - 66 GHz	DA	70 Mbps
Bluetooth	NL	< 100 m	WPAN	2,4 GHz	DA	2 - 26 Mbps
ZigBee	NL	< 1 km	WHAN	2,4 GHz	DA	250 kbps
Z-Wave	NL	< 100 m	WHAN	900 MHz	DA	100 kbps
NFC	NL	< 20 cm	P2P	13,56 MHz	NE	424 kbit/s

Internetski protokoli služe za razmjenu podataka unutar IoT sustava. Najčešće upotrebljavani protokoli u IoT sustavima jesu HTTP, XMPP, AMQP i MQTT. Korištenjem protokola bez praćenja stanja (eng. *stateless*), kao što je HTTP protokol u kojem se uz svaki zahtjev šalje i odgovor, može stvoriti poteškoće u mrežnom prometu i IoT uređajima zbog veće količine *overhead* podataka (informacije koje se dodaju na podatak prilikom slanja podataka kroz mrežu) [6]. Zbog iznimno malog zaglavlja, od svega 2 bajta, MQTT protokol primjeren je za gotovo stvarnovremenske aplikacije na uređajima s ograničenim resursima. MQTT protokol objavio je IBM 1999. godine, a dana se najčešće se upotrebljava verzija protokola 3.1.1. Svoje prednosti ima u nestabilnim vezama i vezama s malom pojasnom širinom. MQTT protokol standardiziran je prema normi ISO 20922 [6], [14].

2.4 Generički model IoT entiteta

Osnovni sastavni blokovi IoT entiteta jesu: senzorski modul, procesorski modul, aktuatorski modul, komunikacijski modul, energetski modul i sat. Na slici 1 prikazan je apstraktni model međusobne komunikacije i povezanosti između pojedinih modula. Energetski modul i sat zajednički su za sve module, odnosno dostupni su za korištenje svim drugim navedenim modulima. Procesorski modul ima dvosmjernu komunikaciju s memorijom i komunikacijskim modulom. Dvosmjerna komunikacija prema memoriji znači da procesorski modul čita i upisuje podatke iz pohrane, a dvosmjerna komunikacija s komunikacijskim modulom znači da može primati i slati informacije [15].



Slika 1: Osnovni blokovi IoT entiteta [15]

2.4.1 Senzorski modul

Senzorski modul dio je IoT entiteta koji ima mogućnost praćenja varijabli i reagiranja na varijable u svojem okruženju. Senzorski moduli dijele se u dvije skupine prema načinu izvršavanja mjerenja: procesorski kontrolirano mjerenje i reakcija na promjenu stanja varijable. Kad je riječ o procesorski kontroliranom mjerenju, mjerenje senzora odvija se samo u trenutku u kojem procesorski modul zatraži vrijednost mjerenja na senzoru. Kad je riječ o senzorima koji reagiraju na promjenu stanja varijable, mjerenje se odvija neprekidno u beskonačnoj petlji. Prilikom svakog ciklusa mjerenja vrijednost mjerenja uspoređuje se s referentnom vrijednošću, a u slučaju da mjerena vrijednost zadovoljava zadane uvjete senzorski modul šalje signal prema procesorskom modulu.

2.4.2 Aktuatorski modul

Aktuatorski modul služi za aktivaciju fizičkih uređaja koji obavljaju neki zadatak. U aktuatorskim modulima ne odvija se obrađivanje podataka niti slanje podataka prema komunikacijskom modulu. Ulazni podaci na aktuatorskom modulu dobiveni su kao rezultat obrade podataka sa senzorskih modula na procesorskom modulu ili obrade podataka na posredničkom sloju.

2.4.3 Komunikacijski modul

Komunikacijski modul služi za slanje podataka s procesorskog modula odgovarajućim protokolom u mrežu te je stoga komunikacijski modul spojnica između IoT uređaja i mreže. Primjeri komunikacijskih modula jesu WiFi modul, LoRaWAN modul, NB-IoT modul, SIM modul, SigFox modul itd.

2.4.4 Energetski modul

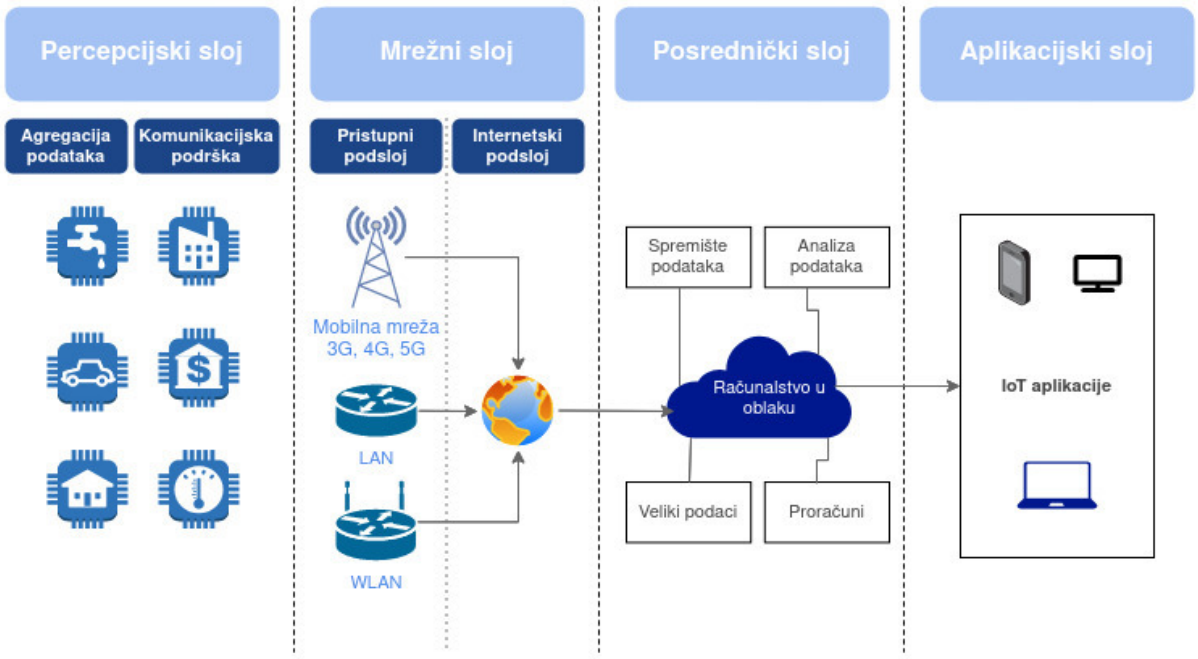
Energetski modul služi za napajanje ostalih modula energijom potrebnom za obavljanje njihovih funkcija. Energetski modul je svaki sklop ili uređaj koji napaja entitet električnom energijom, a to može biti obična baterija, integrirana baterija s dodatnim digitalnim sklopovima za punjenje i kontrolu napunjenosti baterije, solarne ćelije, zavojnice za proizvodnju električne energije itd.

2.4.5 Procesorski modul

Procesorski modul kao glavnu zadaću ima prikupljanje podataka sa senzorskih modula i slanje neobrađenih informacija ili obrađenih podataka prema komunikacijskom modulu. Procesorski modul jedini je modul kojeg se može pratiti ili kontrolirati preko sučelja u aplikacijskom sloju. Procesorski modul komunicira s aktuatorskim modulom [15].

2.5 Generička slojevita arhitektura IoT sustava

Koncept generičke slojevite arhitekture IoT sustava sastoji se od četiriju osnovnih slojeva, a to su: percepcijski sloj, mrežni sloj, posrednički sloj i aplikacijski sloj. Apstraktni prikaz koncepta generičke slojevite arhitekture IoT sustava prikazan je na slici 2 [16]. Svaki pojedini sloj detaljnije je opisan u sljedećim poglavljima.



Slika 2: Slojevita arhitektura IoT sustava [16]

2.5.1 Percepcijski sloj

Percepcijski sloj nalazi se na korisničkoj strani te se u njemu nalaze pametni IoT uređaji, senzori, komunikacijski moduli i komunikacijski pristupnici. Kao što je vidljivo na slici 1, svaki IoT entitet ima komunikacijski modul. Ovisno o tome koju komunikacijsku tehnologiju upotrebljava IoT entitet, taj entitet može komunicirati direktno s mrežnim slojem ili preko komunikacijskog pristupnika. Na primjer ako IoT entitet upotrebljava WiFi ili NB-IoT komunikaciju tehnologiju, on onda može komunicirati direktno s mrežnim slojem, a ako upotrebljava Bluetooth ili ZigBee komunikacijsku tehnologiju, tada entiteti komuniciraju s pristupnikom koji dalje komunicira s mrežnim slojem.

U percepcijskom sloju općenito se nalazi najveći broj uređaja, koji su ujedno veoma heterogeni u svojim karakteristikama.

2.5.2 Mrežni sloj

Mrežni sloj dijeli se u dva podsloja: pristupni podsloj i internetski podsloj. Pristupni podsloj omogućava pristupanje internetu putem više različitih komunikacijskih tehnologija. Kao što je prikazano na slici 2, u pristupnom podsloju nalaze se uređaji koji omogućavaju pristup internetu (odnosno internetskom podsloju) preko mobilnih 3G, 4G, 5G i LTE mreža te WiFi i LAN mreža.

2.5.3 Posrednički sloj

Posrednički sloj središte je svakog IoT sustava. Zadaće posredničkog sloja uključuju spremanje podataka, obradu podataka, analizu podatka, donošenje odluka itd.

Posrednički sloj temelji se na računalstvu u oblaku, što znači da nasljeđuje sve prednosti i nedostatke računalstva u oblaku. Najveće prednosti računalstva u oblaku jesu velika elastičnost i skalabilnost sustava, relativno jednostavno uvođenje, veća iskoristivost računalnih resursa zbog dijeljenja resursa i sl. Nedostaci računalstva u oblaku najviše se gledaju kroz prizmu sigurnosti i zakonodavstva. S gledišta zakonodavstva problem predstavlja činjenica za korisnici često ne znaju gdje se nalaze podaci, a često su ti podaci i podijeljeni na redundantne poslužitelje u više država ili čak kontinenata.

Spremanje podataka

Zbog velikog broja različitih uređaja u percepcijskom sloju posrednički sloj mora biti u mogućnosti spremiti velik broj heterogenih i nekonzistentnih podataka.

Relacijske baze podatka često su usko grlo u IoT informacijskim sustavima, a tome ima više razloga. Na primjer, kod heterogenih podataka teško je definirati strukturu relacijske baze podataka, a u slučaju definiranja neke apstraktne tablice za zapisivanje mjerenja, pretraživanje podataka izrazito je neefikasno, zbog čega se u stvarnom svijetu u konačnici izbjegava korištenje takvih tablica.

U IoT sustavima danas se češće upotrebljavaju nerelacijske (*NoSQL*) baze podataka, kao što su *MongoDB* ili *Cassandra*. Prednosti nerelacijskih baza podataka jesu, među ostalim, velika fleksibilnost strukture podatka i mogućnost rada u decentraliziranom načinu rada na više čvorova. U IoT sustavima također se upotrebljavaju baze podataka specijalizirane za vremenske podatke, kao što je *InfluxDB*.

Prihvat podataka

Za ulaz IoT podataka u posrednički sloj često se implementira MQTT poslužitelj.

MQTT poslužitelji također omogućavaju amortizaciju fluktuacija u količini zahtjeva koji dolaze u sustav. MQTT poslužitelj može prihvatiti iznimno velik broj zahtjeva u kratkom vremenu i zadržati te zahtjeve u radnoj memoriji, što mu omogućava da bude kratkotrajni međuspremnik prije obrade i spremanja podataka.

2.5.4 Aplikacijski sloj

Aplikacijski sloj može se gledati kao sučelje između IoT sustava i krajnjeg korisnika. U aplikacijskom sloju nalaze se korisničke aplikacije. Aplikacije mogu biti namijenjene za pametne telefone, stolna i prijenosna računala ili pametne televizore. Prema tehnologijama za izradu aplikacija one mogu biti *web* ili nativne aplikacije.

2.6 Računalstvo u oblaku

Prema [17] računalstvo u oblaku model je koji omogućava sveprisutan, jednostavan i dostupan pristup dijeljenim računalnim resursima kao što su računalne mreže, poslužitelji, sustavi za pohranu podataka, aplikacije, usluge. Pristup resursima može biti pružen korisniku gotovo trenutačno i gotovo bez potrebe za ikakvom intervencijom pružatelja usluga. NIST u svojoj publikaciji [17] navodi pet osnovnih karakteristika modela računalstva u oblaku:

- Usluga dostupna na zahtjev - korisnik može dobiti dijeljene računalne resurse od pružatelja usluge u bilo koje vrijeme i gotovo bez potrebe za ljudskom intervencijom na strani pružatelja usluge.
- Usluga dostupna putem internetske mreže na velikom području - računalni resursi korisniku su dostupni putem internetske mreže i može im se pristupiti preko standardnih mehanizama koje upotrebljava veliki broj heterogenih tankih[1] (eng. *thin client*) ili debelih[2] klijenata (eng. *thick client*).
- Dijeljenje računalnih resursa - računalni resursi na strani pružatelja usluge dijele se između više korisnika na način da više korisnika dijeli jednu instancu softvera ili jednu instancu baze podataka (eng. *multy-tenant*), pri čemu se fizički i virtualni računalni resursi dinamički dodjeljuju korisniku u odnosu na korisnikove potrebe za resursima. Računalni resursi koji su dostupni korisniku u jednom trenutku u odnosu na računalne resurse koji su dostupni korisniku u nekom drugom trenutku mogu se nalaziti na potpuno dugim lokacijama unutar podatkovnog centra, ili se čak mogu nalaziti u nekom drugom podatkovnom centru, drugom gradu, državi ili kontinentu. Korisnik obično nema kontrolu nad dijeljenim resursima.
- Velika elastičnost sustava - dijeljeni računalni resursi za nekog korisnika mogu biti dodijeljeni i povučeni s obzirom na opterećenost i zahtjeve sustava. U nekim slučajevima

1 Tanki klijenti jesu računalni sustavi u kojima se većina podataka i aplikacija nalazi u udaljenom poslužiteljskom računalu. Također se i većina računalnih operacija odvija na udaljenom računalu. Tanki klijenti povezani su sa udaljenim računalom najčešće putem internetske mreže. [18]

2 Debeli klijenti jesu računalni sustavi koji mogu biti povezani s udaljenim računalom, ali nisu ovisni o njemu, te se većina podatka i aplikacija nalazi na lokalnom računalu. Isto tako se većina računalnih operacija obavlja na lokalnom računalu. [18]

računalni resursi mogu se automatski dodjeljivati i povlačiti s obzirom na opterećenje sustava.

- Mjerenje usluge - sustavi računalstva u oblaku automatski nadziru i optimiziraju računalne resurse na način da koriste dostupna mjerenja stanja sustava kao ulazne podatke za optimizaciju.

Uz pet osnovnih karakteristika računalstva u oblaku prema NIST-u, prema [19] još jedna je karakteristika niska početna cijena računalnih resursa, a samim time i niža početna cijena uvođenja novih usluga.

Najčešći modeli uvođenja usluge računalstva u oblaku jesu privatni oblak (eng. *Private Cloud*), javni oblak (eng. *Public Cloud*), zajednički oblak (eng. *Community Cloud*) i hibridni oblak (eng. *Hybrid Cloud*) [20].

Privatni računalni oblak znači da su svi resursi koje pruža računalni oblak dostupni samo jednoj organizaciji. Zasigurno je moguće zamisliti da se takvim računalnim oblacima koriste najveće IT kompanije kao što su Google, Apple i Microsoft, ali takav oblik računalnog oblaka pojavljuje se i u puno manjim poduzećima i organizacijama. Privatni računalni oblaci mogu biti smješteni unutar organizacije ili u podatkovnim centrima. Kad je riječ o računalnim oblacima smještenima unutar organizacije, sav mrežni promet prolazi samo kroz računalnu mrežu korisnika, što doprinosi sigurnosti računalnog oblaka. Kad je riječ o računalnim oblacima smještenima u podatkovnim centrima, mrežni promet prolazi internetom, pa se u tom slučaju komunikacija između podatkovnog centra i klijentske mreže najčešće odvija unutar VPN-a.

Javni računalni oblak znači da se računalni resursi dijele između više različitih korisnika koji nisu međusobno povezani. Korisnik javnog računalnog oblaka može biti bilo koje poduzeće, organizacija, javna ili privatna osoba. Svaki korisnik povezan je s pružateljem usluge računalnog oblaka preko interneta.

Resursi zajedničkog računalnog oblaka dijele se među skupinom korisnika koji imaju određene zajedničke karakteristike, vizije, ciljeve ili politike. Smještaj i održavanje zajedničkog računalnog oblaka može biti unutar organizacije ili za to može biti odgovorna treća strana u podatkovnom centru.

Hibridni računalni oblak sastoji se od dvaju ili više navedenih vrsta računalnih oblaka od kojih je svaki oblak nezavisan, ali mogu biti povezani na temelju standardnih tehnologija koje omogućavaju prijenos podataka i aplikacija.

2.7 Koncept digitalnih blizanaca

Moderna industrija i poljoprivreda više nisu moguće bez pouzdanih i ažurnih informacija o operativnim procesima. Poljoprivredna proizvodnja sve se više oslanja na digitalnu tehnologiju, senzore, nadzorne uređaje, naprednu analitiku i pametne uređaje. U svijetu se sve više poljoprivrednika okreće pametnim sustavima predvođenima razvojem računalstva u oblaku, interneta stvari, velikih podataka (eng. *big data*), strojnog učenja, virtualne stvarnosti i robotike. Pametna poljoprivreda (eng. *Smart Farming*) pojavljuje se kao sljedeća faza precizne poljoprivrede (eng. *Precision Farming*). Pod pojmom pametne poljoprivrede podrazumijeva se digitalno-fizički kontrolni ciklus koji uključuje mjerenje, nadzor, analizu i kontrolu nad svim relevantnim poljoprivrednim procesima [21].

Pojam digitalnog blizanca (eng. *Digital Twin*) predstavila je NASA za potrebe simulacije rada svemirskih vozila u stvarnom vremenu s parametrima mjerenima na svemirskom vozilu. Taj pristup dao je inženjerima mogućnost stvarnovremenskog nadzora vozila i predviđanje budućeg stanja vozila. Digitalni blizanac u stvari je virtualni (digitalni) primjerak stvarnog fizičkog objekta u digitalnom obliku te je povezan direktno sa svojom fizičkom inačicom putem senzora i mjerenja u stvarnom vremenu.

Digitalni blizanac sveobuhvatni je fizički i funkcionalni opis nekog objekta, proizvoda, sustava ili procesa. Riječ je o probabilističkom modelu simulacije kompleksnih objekata, sustava i procesa koji upotrebljava podatke sa senzora kako bi u stvarnom vremenu prikazao fizički objekt. Integracija podataka između fizičkog i virtualnog objekta odvija se u oba smjera. Digitalni blizanci služe da bi opisali, analizirali i simulirali trenutačno i buduće stanje nekog fizičkog objekta, sustava ili procesa [21], [22].

Prema [21] digitalni blizanci mogu se podijeliti u šest različitih skupina:

1. zamišljeni digitalni blizanci (eng. *Imaginary Digital Twins*)
2. digitalni blizanci za nadzor (eng. *Monitoring Digital Twins*)
3. digitalni blizanci za predikciju (eng. *Predictive Digital Twins*)
4. digitalni blizanci za korekciju (eng. *Prescriptive Digital Twins*)
5. autonomni digitalni blizanci (eng. *Autonomous Digital Twins*)
6. digitalni blizanci za čuvanje povijesnih podataka entiteta (eng. *Recollection Digital Twins*)

Kod zamišljenih digitalnih blizanca virtualni entiteti nisu povezani s fizičkim entitetima, već virtualni entiteti predstavljaju simulaciju fizičkog entiteta. Zamišljeni digitalni blizanci digitalni su prototipovi fizičkih objekata. Oni su se počeli upotrebljavati pojavom CAD/CAM softvera.

Digitalni blizanci za nadzor u stvarnom vremenu prikazuju trenutačno stanje i smjer kretanja fizičkog entiteta. Na primjer, digitalni blizanac autonomnog kombajna za žetvu prikazivao bi parametre trenutačnog stanja kao što su, među ostalim, količina goriva, trenutačna brzina, razina napunjenosti žita, broj radnih sati, temperatura motora, temperatura ulja, temperatura okoline itd. te parametre za smjer kretanja kao što su brzina, smjer kretanja i akceleracija vozila.

Digitalni blizanci za predikciju simuliraju buduće stanje fizičkog entiteta s pomoću probabilističkih metoda, a kao ulazni parametri koriste se mjerenja u stvarnom vremenu s fizičkog entiteta. Na primjeru kombajna za žetvu digitalni blizanac bi u simulaciji na temelju temperature okoline i trenutačnog režima rada motora mogao ustanoviti da će doći do pregrijavanja motora.

Digitalni blizanci za korekciju daju "savjete" za prevenciju i korekciju stanja na fizičkim objektima. Digitalni blizanci za korekciju mogli bi predložiti način za prevenciju pregrijavanja motora, npr. smanjenje broja okretaja motora i usporenje žetve ili u krajnjem slučaju gašenje stroja.

Autonomni digitalni blizanci funkcioniraju samostalno bez interakcije s čovjekom te imaju potpunu kontrolu nad fizičkim entitetom. Autonomni digitalni blizanac imao bi potpunu kontrolu nad kombajnom iz primjera te bi u slučaju simulacije pregrijavanja on automatski prilagodio režim rada motora kako bi izbjegao pregrijavanje.

Digitalni blizanci za čuvanje povijesnih podataka entiteta prikupljaju i prikazuju cijelu povijest stanja fizičkog entiteta. Na primjeru kombajna u žetvi, ovaj koncept digitalnih blizanaca omogućava ponovno pregledavanje žetve, tj. moglo bi se reći da bi to bila reprodukcija prema stvarnim parametrima tijekom žetve. Tako se može omogućiti otkrivanje nekih anomalija koje nisu nužno dovele do incidenta ili greške, ali ih je potrebno pregledati i ispraviti kako se to ne bi dogodilo u budućnosti.

3. Sigurnost u IoT sustavima

Informacijska sigurnost definira se kao stanje povjerljivosti, cjelovitosti i raspoloživosti podatka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade tih mjera i standarda [23]. Cilj zaštite informacijsko-komunikacijskog sustava podrazumijeva tri osnovna načela: povjerljivost, cjelovitost i dostupnost. Povjerljivost je načelo koje osigurava otkrivanje podataka i informacija isključivo ovlaštenim osobama, entitetima i procesima u određeno vrijeme i u skladu s određenim postupkom. Cjelovitost je načelo koje podrazumijeva zaštitu podataka i informacija od namjerne ili slučajne neovlaštene izmjene uzrokovane ljudskim utjecajem ili greškom u radu sustava. Dostupnost je načelo koje se odnosi na mogućnost pristupanja traženim podacima, informacijama i ostalim resursima ovlaštenim korisnicima prema definiranim uvjetima, što uključuje poštovanje načela cjelovitosti i povjerljivosti.

Razlike između klasične informacijske sigurnosti i sigurnosti IoT sustava najviše su vidljive u topologiji mreže i percepcijskom sloju sustava. IoT uređaji često se puštaju u rad u LLN mrežama (eng. *Low Power and Lossy Network*) koje karakterizira velika dinamičnost topologije mreže i veći gubici podatka, za razliku od topologije u klasičnim informacijsko-komunikacijskim sustavima koja je gotovo statična. U percepcijskom sloju IoT sustava većinom se nalaze senzori i ostali uređaji pokretani mikroprocesorima koji imaju ograničene resurse za napajanje, spremanje podataka i izvršavanje računalnih operacija pa zbog toga nisu u mogućnosti koristiti postojeće enkripcijske algoritme. Danas se za IoT uređaje razvijaju procesorski manje zahtjevni enkripcijski algoritmi [4], [16]. Sigurnost u ostalim slojevima generičke arhitekture jednaka je kao i kod klasične informacijske sigurnosti [16].

Trenutačno postoji nekoliko izazova u području IoT sigurnosti koji zahtijevaju rješenje, a to su identifikacija IoT entiteta, autentifikacija i autorizacija, privatnost, procesorski manje zahtjevni enkripcijski algoritmi i sigurnosni protokoli, ranjivosti softvera.

Identifikacija IoT entiteta ključan je preduvjet za osiguravanje cjelovitosti podataka dobivenih s IoT entiteta. Trenutačni DNS sustav (eng. *Domain Name System*) više nije dovoljan zbog napada koji mogu iskoristiti njegove ranjivosti (napad preko posrednika i *DNS cache poisoning*). Razvijen je i DNSSEC (eng. *Domain Name System Security Extension*) koji omogućava cjelovitost i autentifikaciju IoT uređaja. Neki od najvećih nedostataka DNSSEC sustava jesu kompleksna integracija u IoT sustave i veliki *overhead.*

Kod očuvanja privatnosti pojavljuju se dva glavna izazova; prikupljanje podataka i anonimizacija

podataka. U okviru politike prikupljanja podataka određuju se vrste podataka i informacija koje se prikupljaju te tko ima pristup tim podacima i informacijama. Da bi se osigurala anonimizacija podataka, potrebno je enkriptirati podatke i ukloniti povezanost između podataka i vlasnika podataka [24].

Prema [25] IoT uređaji jako su ranjivi zbog tri glavna razloga:

- česti fizički napadi na uređaje zbog toga što su uređaji nezaštićeni i nalaze se na otvorenim mjestima; najčešće je riječ o uređajima u domenama pametnih gradova i pametne poljoprivrede
- komunikacija između uređaja najčešće je bežična, što dovodi do ranjivosti na napade prisluškivanjem
- uređaji se često baziraju na mikroprocesorima i ne mogu koristiti enkripcijske mehanizme, zbog čega su podložni napadima preko posrednika.

3.1 Izvori prijetnji

Prijetnja (eng. *threat*) predstavlja okolnost ili pojavu koja ima potencijal uzrokovati štetu ili gubitak. Prijetnja se sastoji od potencijalne aktivnosti ili pojave koja može negativno utjecati na osnovna načela informacijske sigurnosti. Prijetnje se ne javljaju samostalno već moraju sadržavati uzroke. Uzorci prijetnje (eng. *threat agents*) mogu biti ljudski faktor, prirodna pojava ili nesretni događaj [26].

Najčešći izvori prijetnji prema entitetima u percepcijskom sloju jesu zlonamjerni korisnici, zlonamjerni proizvođači, vanjski napadači i loše programiranje.

Zlonamjerni korisnici vlasnici su IoT uređaja koji imaju namjeru izvođenja napada u svrhu otkrivanja podataka koji su poslovna tajna proizvođača i ostvarivanja pristupa skrivenim ili zatvorenim funkcionalnostima IoT uređaja. Nakon otkrivanja takvih informacija zlonamjerni korisnici žele prodati informacije konkurentskim proizvođačima uređaja ili izvoditi napade nad sličnim sustavima.

Zlonamjerni proizvođači jesu oni proizvođači koji namjerno ostavljaju ranjivosti na uređajima ili tehnologiji, a sve u svrhu iskorištavanja istih ranjivosti za prikupljanje informacija o korisnicima.

Vanjski napadač onaj je napadač koji se ne nalazi unutar IoT sustava i nema odobren pristup sustavu. Vanjski napadači obično žele ostvariti pristup informacijama korisnika unutar sustava u svrhu nelegitimnih radnji kao što su stvaranje financijske štete za korisnika ili narušavanje reputacije korisnika ili proizvođača.

Za razliku od dosad navedenih izvora prijetnji, **loše programiranje** ne proizlazi iz namjere ostvarivanja pristupa sustavu ili prikupljanja korisničkih podataka, nego iz nekompetentnosti proizvođača softvera. Glavni problem kod ranjivosti koje se pojavljuju zbog grešaka u programskom kodu jest taj što greška može jako dugo ostati neprimijećena [15], [27].

3.2 Ranjivosti

Ranjivost (eng. *vulnerability*) je vjerojatnost da prijetnja postane realnost, odnosno riječ je o slabostima sustava koje mogu biti iskorištene u svrhu uzrokovanja gubitka informacija ili nanošenja štete sustavu. Ranjivosti mogu biti različite, kao i način njihova iskorištavanja. Taj se pojam odnosi na stanje, nedostatak ili slabost u sigurnosnim postupcima, tehničkim kontrolama, fizičkim i drugim kontrolama sustava te dizajnu i implementaciji tih kontrola i postupaka koje je moguće iskoristiti. Slučajno ili namjerno iskorištavanje ranjivosti može prouzrokovati operativne i financijske gubitke sustavu [26].

4. Opis sustava temeljenog na internetu stvari

Informacijski sustav temeljen na konceptu interneta stvari koji će se promatrati u ovom radu, u nastavku rada koristit će se jednostavno izraz "informacijski sustav", služi za prikupljanje, obradu i pohranu podataka dobivenih mjerenjem na udaljenim IoT senzorskim jedinicama. Informacijski sustav u mogućnosti je samostalno, bez interakcije s čovjekom, kontrolirati aktuatorske jedinice unutar mjernog mjesta na temelju ulaznih parametara dobivenih sa senzorskih jedinica.

Mjerno mjesto stvarni je prostor koja ima određeni volumen i svoje granice, a u kojem je potrebno zbog nekih tehničkih razloga regulirati ambijentalne uvijete. Primjer mjernog mjesta može biti komora za zrenje suhomesnatih proizvoda, pušnica, sušara za duhan, silos za žito, plastenik, staklenik, prostorija za skladištenje povrća itd. Mjerno mjesto također može biti i spremnik tekućine, kao što su na primjer metalni ili drveni spremnici za vino u kojima je potrebno održavati određenu temperaturu, posebno u fazi vrenja.

Slika 3: Mjerno mjesto

Na slici 3 prikazani su osnovni elementi mjernog mjesta i njihovi međusobni odnosi. Mjerno mjesto sastoji se od točno jednog IoT pristupnika (eng. *IoT gateway*), jedne ili više senzorskih jedinica i jedne ili više aktuatorskih jedinica (no one nisu obvezan element mjernog mjesta stoga njihov broj može biti i nula). Pristupnik služi kao poveznica između komunikacijske tehnologije senzorskih i aktuatorskih jedinica i interneta. Senzorske i aktuatorske jedinice imaju mogućnost korištenja više različitih komunikacijskih tehnologija, ovisno o izvedbi i potrebama jedinice.

Na slici 4 prikazana je logička struktura predstavljenog informacijskog sustava u okviru generičke slojevite arhitekture IoT sustava. U percepcijskom sloju sustava nalaze se pametne senzorske jedinice, pametne aktuatorske jedinice i IoT pristupnik. Percepcijski sloj informacijskog sustava smješten je unutar mjernog mjesta. Mrežni sloj spojnica je između percepcijskog i posredničkog sloja. Posrednički sloj temelji se na računalstvu u oblaku, a u njemu se nalaze HTTP poslužitelj, MQTT poslužitelj, baza podataka, servisi za obradu podataka te sustav za autonomno donošenje

odluka. Posrednički sloj prikuplja, sprema i obrađuje podatke te priprema i pruža podatke za aplikacije koje se nalaze u aplikacijskom sloju. U aplikacijskom sloju nalaze se korisničke aplikacije za pregled prikupljenih i obrađenih podatka.

4.1 Percepcijski sloj informacijskog sustava

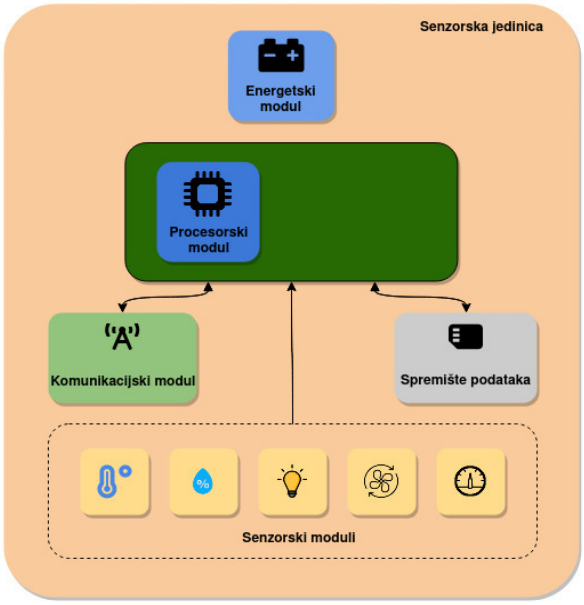
Na slici 5 prikazani su moduli od kojih je sastavljena senzorska jedinica. Model senzorske jedinice napravljen je prema generičkom modelu IoT entiteta [2]. Senzorska jedinica sadržava više senzorskih modula; na slici se senzorski moduli nalaze unutar okvira označenog isprekidanom crtom, a ikone u kvadratima gledajući s lijeva na desno predstavljaju senzore temperature, vlage, svjetlosti, brzine protoka zraka i tlaka.

Na slici 6 prikazan je model pametne aktuatorske jedinice u okviru generičkog modela IoT entiteta. Aktuatorska jedinica sastoji se od energetskog modula, procesorskog modula, komunikacijskog modula i aktuatora.

Komunikacijski moduli koriste ZigBee komunikacijsku tehnologiju. Korištenje ZigBee tehnologije odabrano je na temelju više faktora, a to su, među ostalim, niska potrošnja baterije, dvosmjerna komunikacija, dovoljan domet (između 10 i 100 metara) i zadovoljavajuća brzina prometa (oko 20 KB/s).

Procesorski modul kao procesor koristi mikročip ESP8266EX. Ovaj mikročip ima na sebi ugrađenu podršku za komunikaciju preko WiFi protokola. Podrška za WiFi je kod aktuatorskih i senzorskih jedinica upotrijebljena za početno pristupanje jedinici i namještanje njezinih postavki.

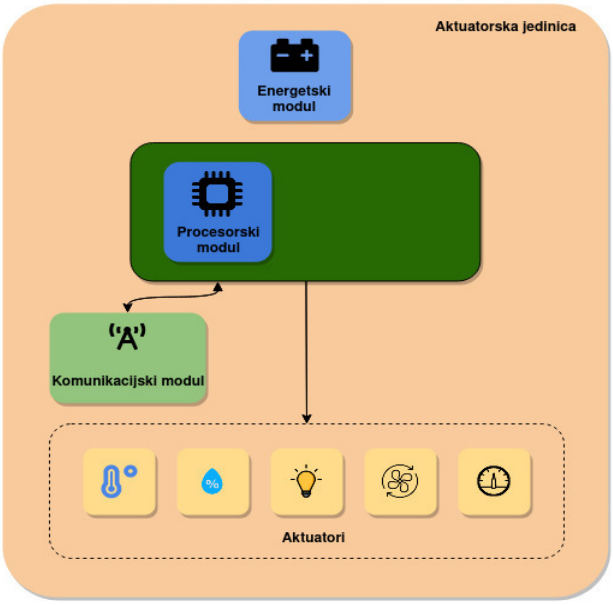
Energetski moduli u senzorskim jedinicama koriste baterije kao izvor napajanja. Predviđa se korištenje dviju ICR18650 baterija spojenih paralelnim spojem. S baterijom kao izvorom napajanja senzorske jedinice lako se prenose i lako ugrađuju na željena mjesta. S druge strane, energetski modul na aktuatorskim jedinicama koristi mrežu od 12 V kao izvor napajanja.



Slika 5: Logička struktura senzorske jedinice

Senzorske se jedinice više od 95 % vremena nalaze u stanju dubokog mirovanja (eng. *deep sleep*), što znači da u tom režimu troše minimalno energije. Očekuje se da će u fazi eksploatacije baterija izdržati oko 12 mjeseci. U preostalih manje od 5 % vremena senzorske jedinice obavljaju mjerenja senzorima i šalju izmjerene vrijednosti na centralni sustav gdje se podaci obrađuju.

Aktuatorske jedinice nalaze se u načinu rada u kojem uvijek imaju aktivnu konekciju prema MQTT poslužitelju kako bi mogle primiti zahtjeve za aktiviranje aktuatora. Takav način rada troši mnogo više energije u odnosu na način rada senzorskih jedinica pa su zbog tog razloga aktuatorske jedinice priključene direktno na izvor napajanja.



Slika 6: Aktuatorska jedinica

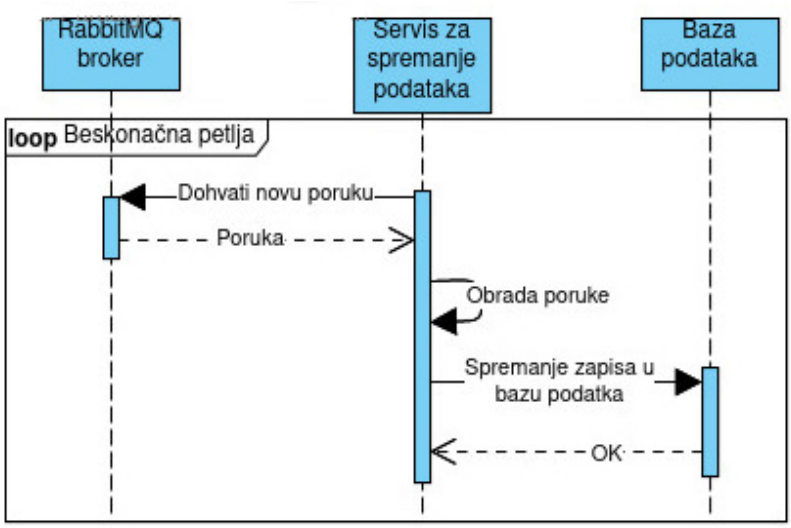
Aktuatori su najčešće elektromagnetski releji, tranzistori, solenoidni ventili, elektro-pneumatski ventili itd.

Predstavljenom informacijskom sustavu potreban je ZigBee pristupnik deklariran za IIoT. Pristupnik se bira ovisno o uvjetima unutar mjernog mjesta.

4.2 Posrednički sloj informacijskog sustava

Posrednički sloj prikazan na slici 4 služi za prikupljanje, spremanje te obradu podataka dobivenih s pametnih senzorskih jedinica.

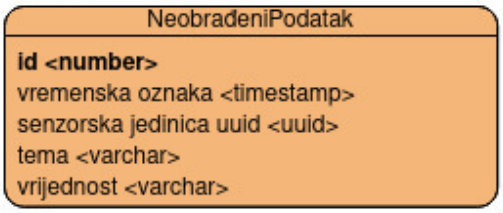
Za spremanje podataka u ovom informacijskom sustavu upotrebljava se relacijska baza podataka, točnije PostgreSQL verzije 10.17.



Slika 7 Sekvencijalni dijagram spremanja podataka iz MQTT brokera u bazu podataka

U posredničkom sloju nalaze se dva javno dostupna sučelja: MQTT poslužitelj i *web* poslužitelj. MQTT poslužitelj koristi se isključivo za M2M (eng. *machine-to-machine*) komunikaciju s pametnim senzorskim jedinicama, dok se *web* poslužitelj upotrebljava za komunikaciju s korisničkim aplikacijama.

Nakon što poruka stigne do MQTT brokera, ona se obrađuje i sprema u bazu podataka. Na slici 7 prikazan je sekvencijalni dijagram spremanja podataka iz reda čekanja u MQTT brokeru u bazu podataka. Servis za spremanje podataka funkcionira tako da se nalazi u beskonačnoj petlji, pri čemu u svakoj iteraciji traži novu poruku iz reda čekanja, a nakon što dobije poruku, poruka se obrađuje i sprema u bazu podatka. Kao MQTT broker koristi se softver RabbitMQ, koji ima mogućnost spremanja poruka u red čekanja. Red čekanja nalazi se u radnoj memoriji, što znači da nije predviđen za dugotrajno čuvanje podatka. Red čekanja na brokeru nadoknađuje usko grlo do kojeg može doći pri zapisivanju podataka u bazu podatka u slučaju kratkotrajnog naglog povećanja prometa. Svaki zapis sprema se u bazu podataka kao entitet NeobrađeniPodatak čiji su atributi vidljivi na slici 8.



Slika 8: ER model relacijske baze podataka

Atribut "tema" predstavlja temu na koju senzorska jedinica objavljuje mjerenja. Jedna senzorska jedinica objavljuje poruke na više tema. Atribut "vrijednost" predstavlja vrijednost koju senzorska jedinica šalje na određenu temu. U tablici 2 prikazani su primjeri tema na koje objavljuje jedna senzorska jedinica. U primjeru u nastavku senzorska jedinica identificira se u korijenu teme gdje:

- /sensor_unit - označava da se radi o senzorskoj jedinici
- /sensor_unit_uuid - predstavlja jedinstveni identifikator senzorske jedinice, mora biti jednaka vrijednosti *sensor_unit_uuid*

Dalje se teme dijele na skupine podatka, u primjeru su prikazane skupine:

- /measure - što označava da se radi mjerenju senzora
- /health - označava da se radi podacima koji se koriste za nadzor sustava

Tablica 2: Primjer vrijednosti za određene teme

Tema	Vrijednost
/sensor_unit/1e75...5912/measure/sensor/274f...7a69/humidity	75,00
/sensor_unit/1e75...5912/health/sensor/ 274f...7a69/status	1
/sensor_unit/1e75...5912/health/cpu/temp	60,1
/sensor_unit/1e75...5912/health/memory/usage	34,4

4.3 Aplikacijski sloj

Na korisničkoj strani nalazi se sučelje za korisnika prema sustavu. Na slici 4 prikazane su ikone računala, pametnog telefona i pametnog sata, koje predstavljaju pametne uređaje koji se nalaze na korisničkoj stani i funkcioniraju kao spomenuto sučelje za pristup sustavu. Korisnik putem njih može pristupiti *web*-aplikaciji, na primjer upotrebom internetskog preglednika na računalu, tabletu

ili pametnom telefonu. Nativne aplikacije za pametne telefone, osim svih značajki koje su dostupne u *web*-aplikaciji, pružaju i mogućnost slanja automatskih poruka (eng. *push notification*) koje se prikazuju korisniku na pametnom telefonu ili pametnom satu.

5. Proces procjene rizika u informacijskom sustavu

Sigurnosni rizik podrazumijeva prijetnje i ranjivosti na određenom dijelu imovine. Sigurnosni rizik je funkcija vjerojatnosti da će prijetnja iskoristiti ranjivost sustava i negativno utjecati na imovinu sustava.

Sigurnosni rizik povećava se što je veći broj prijetnji, veći broj ranjivosti ili što je veća vrijednost imovine sustava. Na primjer, ako je neki dio imovine sustava izložen prijetnjama i ima mnogo ranjivosti, ali nema nikakvu vrijednost za organizaciju, tada je sigurnosni rizik nizak jer nema utjecaja na poslovanje organizacije.

Svrha procjene rizika može se razlikovati ovisno o tome radi li se o prvoj procjeni rizika nad informacijskim sustavom ili se radi o ponovnoj procjeni rizika nakon praćenja rizičnih faktora u tom sustavu. Svrha prve procjene rizika može biti određivanje početnih vrijednosti za procjenu rizika ili pak određivanje prijetnji, ranjivosti i utjecaja na imovinu i poslovanje organizacije, kao i definiranje rizičnih faktora koje je potrebno nadzirati u budućnosti. Svrha ponovne procjene rizika može biti ažuriranje rezultata prethodne procjene rizika zbog promjena u informacijskom sustavu ili poslovanju organizacije, određivanje efikasnosti sigurnosnih kontrola uvedenih u informacijski sustav, ili ponavljanje procjene rizika zbog incidenta koji se dogodio u sustavu. Promjene u informacijskom sustavu koje mogu dovesti do potrebe za ponovnom procjenom rizika jesu promjene na softveru u sustavu, promjene na hardveru u sustavu, promjene u poslovnim planovima i ciljevima organizacije, promjene u pogledu ranjivosti u sustavu, kao i promjene u pogledu prijetnji i izvora prijetnji u sustavu.

Definiranje djelokruga procjene rizika odnosi se na opisivanje svega što je uključeno u procjenu rizika. Određivanjem djelokruga procjene rizika organizacija može jasno odrediti kojem je sloju organizacije procjena rizika namijenjena, koji su dijelovi organizacije uključeni u procjenu rizika, koje se odluke žele potkrijepiti procjenom rizika i sl. U okviru djelokruga može se definirati imovina koja je uključena u procjenu rizika, dijelovi informacijskog sustava itd.

Kao dio pripreme za procjenu rizika organizacija mora eksplicitno definirati pretpostavke i ograničenja pod kojima se provodi procjena rizika. Eksplicitno definirane pretpostavke osiguravaju jasniju sliku procjene rizika i ponovljivost rezultata procjene rizika te povećavaju mogućnost dijeljenja postupka procjene rizika među organizacijama. Elementi u pogledu kojih je potrebno eksplicitno definirati pretpostavke jesu izvori prijetnji, prijetnje, ranjivosti, vjerojatnosti pojave prijetnji i iskorištavanja ranjivosti, utjecaj na imovinu te analitičke metode procjene rizika.

Organizacija mora odrediti relevantne izvore prijetnji. Pretpostavke se mogu iskazati tako da se svi izvori prijetnji uzimaju u obzir, tako da se u obzir uzima samo jedna kategorija izvora prijetnji, kao što je na primjer kategorija prirodnih nepogoda, ili pak tako da se u obzir uzme još konkretnije definiran izvor prijetnji, na primjer potres na širem zagrebačkom području. Definirane prijetnje upotrebljavaju se u procjeni rizika.

Pretpostavke za prijetnje mogu biti opisane na apstraktnoj razini ili na detaljnoj razini. Primjer pretpostavke za prijetnje definirane na apstraktnoj razini prijetnji jest napad uskraćivanja usluge bez specificiranja odakle napad dolazi, kojom snagom i prema kojem dijelu imovine je usmjeren, dok detaljno definirane pretpostavke daju jasan opis prijetnje i prema čemu je napad usmjeren.

Pretpostavkama za ranjivosti određuje se koji se tipovi ranjivosti informacijskog sustava uzimaju u obzir prilikom procjene rizika. Pretpostavke za ranjivosti mogu biti vezane direktno uz informacijski sustav (softver, hardver, mrežna oprema, sigurnosne kontrole) ili uz vanjske utjecaje kao što su organizacija poslovanja, partnerski odnosi itd.

U svrhu određivanja vjerojatnosti pojave prijetnje i iskorištavanja ranjivosti u pretpostavkama je potrebno eksplicitno definirati na koji se način izračunava vjerojatnost. U pretpostavkama je također potrebno odrediti način na koji se izračunava utjecaj na imovinu.

Definiranjem pretpostavki za analitičke metode procjene rizika određuje se do koje je razine detalja potrebno raditi analizu procjene rizika. Može se definirati da se traži detaljnija razina analize za kritičniju imovinu dok za imovinu manje vrijednosti nije potrebna toliko detaljna analiza.

Prema [29] procjena rizika prva je faza u upravljanju sigurnosnim rizicima u informacijskom sustavu. Upravljanje rizikom uključuje procjenu rizika, nadzor rizika i odgovaranje na rizik.

U tablici 3 prikazana je skupna lista smjernica dobivena iz više različitih izvora koja sadržava zadatke koje je potrebno provesti u svrhu provedbe procjene rizika nad informacijskim sustavom. Popis smjernica za procjenu rizika u informacijskim sustavima prikazan u tablici 3 nije obvezujući, već svaka organizacija može prilagoditi proces svojim potrebama.

Smjernice u tablici 3 podijeljene su četiri segmenta: predradnje, procjena rizika, prezentiranje rezultata procjene rizika i radnje nakon procjene rizika.

Tablica 3: Pregled literature za proces provedbe procesa procjene rizika u informacijskim sustavima

Zadatak	**Opis zadatka**	**Literatura**
Predradnje		
Odrediti svrhu provedbe	Određivanje svrhe provedbe procjene rizika u smislu	[29]

procjene rizika	određivanja toga koje se informacije žele dobiti procjenom rizika i koje se odluke žele poduprijeti tom procjenom rizika	
Odrediti djelokrug	Određivanje vremenskog okvira provedbe procjene rizika te dijelova sustava i tehnologije nad kojima se provodi procjena rizika	[29]
Odrediti pretpostavke i ograničenja	Određivanje jedinstvenih pretpostavki i ograničenja unutar kojih se provodi procjena rizika	[29]
Odrediti izvore informacija	Određivanje izvora informacija u pogledu opisa sustava, prijetnji, ranjivosti i utjecaja na imovinu koji se koriste u procjeni rizika	[29]
Odrediti model rizika i pristupa analitici	Određivanje modela rizika i modela za analizu rizika koji se koristi u procjeni rizika	[29], [30]
Odrediti imovinu sustava	Određivanje i popisivanje relevantne imovine sustava	[30]–[33]
Procjena rizika		
Odrediti relevantne izvore prijetnji	Određivanje i karakteriziranje relevantnih izvora prijetnji	[29]
Odrediti relevantne prijetnje	Određivanje potencijalnih prijetnji i relevantnosti navedenih prijetnji te izvora iz kojih potencijalno mogu nastati prijetnje	[29]–[33]
Odrediti ranjivosti i okolnosti informacijskog sustava	Određivanje ranjivosti sustava i okolnosti u organizaciji koje pogoduju ostvarivanju utjecaja nad imovinom u slučaju ostvarivanja prijetnje	[29]–[33]
Odrediti vjerojatnosti	Određivanje vjerojatnosti da ostvarena prijetnja iskoristi ranjivost sustava	[29]–[33]
Odrediti utjecaj	Određivanje utjecaja na imovinu sustava u slučaju ostvarivanja prijetnje i iskorištavanja ranjivosti sustava	[29]–[32]
Odrediti rizik	Određivanje rizika koji prijeti sustavu na temelju vjerojatnosti iskorištavanja ranjivosti i utjecaja na imovinu sustava	[29]–[33]
Prezentiranje rezultata procjene rizika		
Dokumentirati rezultate procjene rizika	Izrada jasno strukturiranog dokumenta o provedbi i rezultatima procjene rizika	[30]–[32]
Prezentirati rezultate procjene rizika	Prezentiranje rezultata procjene rizika osobama u organizaciji zaduženima za provedbu upravljanja rizikom	[29]
Distribuirati informacije povezane s rizikom	Dijeljenje informacija povezanih s rizikom dobivenih u okviru provedbe procjene rizika odgovornim osobama	[29]
Radnje nakon procjene rizika		
Nadzirati rizične faktore	Provedba nadzora nad faktorima koji povećavaju rizik koji prijeti sustavu	[29]
Ažurirati procjenu rizika	Ažuriranje postojeće procjene rizika rezultatima proizašlima iz provedbe nadzora nad rizičnim faktorima	[29]

Smjernice iz tablice 3 prilagodit će se za potrebe ovog diplomskog rada. Provedba nekih zadataka nije potrebna s obzirom na to da iza ovog sustava ne stoji organizacija već je riječ o konceptu sustava koji je razvijen u svrhu izrade ovog rada. Proces procjene rizika sastojat će se od sljedećih zadataka:

1. Predradnje za procjenu rizika
    1. Određivanje modela procjene rizika i analitike rizika
    2. Određivanje imovine informacijskog sustava
2. Procjena rizika
    1. Određivanje relevantnih prijetnji za informacijski sustav
    2. Određivanje ranjivosti informacijskog sustava
    3. Određivanje vjerojatnosti pojave sigurnosnog incidenta u informacijskom sustavu
    4. Određivanje utjecaja sigurnosnog incidenta na imovinu informacijskog sustava
    5. Određivanje rizika nad imovinom informacijskog sustava
3. Prezentiranje rezultata procjene rizika
    1. Izrada jasno strukturiranog poglavlja s opisanim procesom i rezultatima procjene rizika

Svaki od navedenih koraka biti će detaljnije opisan sljedećim poglavljima.

5.1 Izvori informacija

Izvori informacija za procjenu rizika mogu dolaziti iz organizacije ili izvan organizacije. U tablici 4 prikazani su relevantni izvori informacija u pojedinom segmentu procjene rizika u odnosu na organizacijsku razinu. Upravljačka razina u svakom od segmenata daje informacije vezane uz najviše razine upravljanja, poslovna razina daje informacije vezane uz obavljanje svakodnevnih djelatnosti organizacije, dok razina informacijskog sustava daje više tehničke i specifične informacije vezane uz informacijski sustav.

Tablica 4: Relevantni izvori informacija u pojedinom segmentu procjene rizika s obzirom na organizacijsku razinu

Izvor: [29]

	Organizacijska razina		
Segment procjene rizika	Upravljačka razina	Poslovna razina	Informacijski sustav
Izvor prijetnji	- izvori prijetnji utvrđeni u prijašnjim procjenama rizika - izvori prijetnji povezanih s upravom organizacije, poslovanjem organizacije, vanjskim odnosima itd.	- poslovno specifične informacije o izvorima prijetnji (npr. zajednička infrastruktura s drugim organizacijama, partneri, vanjski odnosi itd.)	- specifične tehničke informacije o izvorima prijetnji i karakteristike izvora prijetnji
Prijetnje	- prijetnje utvrđene u prijašnjim procjenama rizika - prijetnje povezane s upravom organizacije, poslovanjem organizacije, vanjskim odnosima itd.	- poslovno specifične prijetnje povezane s poslovanjem organizacije, zajedničkom infrastrukturom, vanjskim odnosima itd.	- povijest incidenata u informacijskom sustavu - specifične tehničke informacije o prijetnjama - prijetnje povezane s informacijskim sustavima, komponentama računala, aplikacijama, operativnim sustavima itd.
Ranjivosti	- informacije o ranjivostima iz pouzdanih izvora - planovi za kontinuitet poslovanja - informacije o ranjivostima povezanima s organizacijskom strukturom, politikama organizacije itd.	- informacije o ranjivostima povezanim s poslovnim procesima, zajedničkom infrastrukturom, vanjskim odnosima itd. - planovi za kontinuitet poslovanja	- ranjivosti povezane s informacijskim sustavima, komponentama računala, aplikacijama, operativnim sustavima itd. - rezultati penetracijskih testiranja - informacije dobivene nadzorom sustava - izvještaji o procjenama ranjivosti sustava - izvještaji proizvođača o ranjivosti komponenti - izvještaji o incidentima
Vjerojatnosti	- informacije o vjerojatnostima specifične za organizacijsku razinu - procjene vjerojatnosti pojave prijetnji specifičnih za organizacijsku razinu - procjene vjerojatnosti iskorištavanja ranjivosti specifičnih za organizacijsku razinu	- informacije o vjerojatnostima specifične za poslovnu razinu	- informacije o vjerojatnostima specifične za informacijsku razinu - povijesni podaci o uspješnim i neuspješnim kibernapadima - rezultati validacije sigurnosti - izvještaji proizvođača o ranjivosti komponenti

	Organizacijska razina		
Segment procjene rizika	Upravljačka razina	Poslovna razina	Informacijski sustav
Utjecaj	- informacije o utjecaju specifične za organizacijsku razinu - primjeri utjecaja na organizacijskoj razini - procjene utjecaja specifične za organizacijsku razinu - informacije o ključnim poslovima organizacije	- informacije o utjecaju specifične za poslovnu razinu - informacije o imovini velike vrijednosti	- informacije o utjecaju specifične za informacijski sustav - povijesni podaci o uspješnim i neuspješnim kibernapadima - rezultati validacije sigurnosti

Kako je definirano u pretpostavkama, procjena rizika odnosi se samo na tehnički dio informacijskog sustava, pa su tako, gledajući tablicu 4, relevantni izvori informacija prikazani u stupcu informacijski sustav.

5.2 Predradnje za proces procjene rizika

Dobra priprema omogućava organizaciji jasno tumačenje rezultata procjene rizika te također omogućava ponovljivost rezultata s obzirom na to da su u pripremi definirane pretpostavke pod kojima je provedena procjena rizika.

Postoji nekoliko radnji koje je potrebno odraditi prije početka same provedbe procesa procjene rizika, a to su određivanje kritične imovine sustava, određivanje ključnih poslovnih procesa organizacije te određivanje kritičnih prijetnji koje mogu poremetiti poslovanje organizacije [29]–[32].

5.2.1 Određivanje modela procjene i analize rizika

Prije provedbe procjene rizika potrebno je odrediti model procjene rizika i model analize rizika. Modelom procjene rizika opisuje se metoda kojom se određuju rizici.

Prema [29] metode koje se primjenjuju jesu kvalitativna, kvantitativna i polukvantitativna metoda, do se u [34] spominje i PRA metoda (eng. *Probabilistic Risk Assasmet*). U PRA metodi koristi se stablo događaja te se izračunavaju vjerojatnosti lanaca događaja i time se izračunava vjerojatnost greške u sustavu. PRA metoda je prvotno korištena u procjeni rizika nuklearnih postrojenja, a kasnije je našla primjenu i u informacijskim sustavim [33], [34].

Kvalitativna metoda procjene rizika ne koristi apsolutne vrijednosti parametara, već se vrijednosti parametara opisuju u vrijednostima od *vrlo nisko* do *vrlo visoko*. Kvalitativna metoda zahtijeva visoku stručnost i znanje o informacijskom sustavu kako bi rezultati procjene rizika bili što vjerodostojniji. Glavni nedostatak kvalitativne metode procjene rizika jest taj što različite osobe mogu različito procijeniti vrijednosti parametara. Za razliku od kvalitativne metode, kvantitativna metoda koristi apsolutne vrijednosti. Polukvantitativna metoda pak koristi brojčane vrijednosti za opisivanje vrijednosti parametara, ali ne koristi stvarne vrijednosti već vrijednost iz u rasponu od 0 do 10 ili 0 do 100. U tablici 5 prikazana je poveznica između vrijednosti za upotrebu u kvalitativnoj metodi i polukvantitativnoj metodi. U tablici 6 prikazan je primjer vrednovanja imovine, utjecaja i ranjivosti ovisno o odabranoj metodi procjene rizika. Na tom primjeru određivanjem vrijednosti imovine kvalitativnom metodom dobivena vrijednost prikazana je kao niska, primjenom kvantitativne metode dobivena je stvarna vrijednost od 120,00 kuna, dok je primjenom polukvantitativne metode vrijednost imovine ocijenjena vrijednošću 4.

Tablica 5: Skala vrijednosti za kvalitativnu i polukvantitativnu metodu procjene rizika

Izvor: [28]

Kvalitativne vrijednosti	Polukvantitativne vrijednosti	
Vrlo visoko	96-100	10
Visoko	80-95	8
Srednje	21-79	5
Nisko	5-20	2
Vrlo nisko	0-4	0

Tablica 6: Primjer vrijednosti parametara za kvalitativnu, kvantitativnu i polukvantitativnu metodu procjene rizika

Parametar	Kvalitativni	Kvantitativni	Polukvantitativni
Vrijednost imovine	Niska	120,00 kuna	4
Utjecaj	Vrlo visok	100.000,00 kuna	97
Ranjivost	Srednja	13 ranjivosti	43

Model analize rizika opisuje pristup analizi rizika. Primjeri modela analize rizika jesu analiza rizika prema prijetnjama, prema ranjivostima ili prema imovini [33]. Analiza rizika prema prijetnjama

započinje utvrđivanjem relevantnih izvora prijetnji i prijetnji za organizaciju, zatim se prema prijetnjama definiraju relevantne ranjivosti sustava koje mogu biti iskorištene u slučaju pojave prijetnje te se iz definiranih ranjivosti utvrđuje imovina na koju iskorištavanje ranjivosti može imati utjecaj. Analiza rizika prema ranjivostima započinje definiranjem relevantnih ranjivosti sustava, nakon čega se definiraju izvori prijetnji i prijetnje koje mogu iskoristiti navedene ranjivosti te se na kraju utvrđuje utjecaj iskorištenja ranjivosti na imovinu. Analiza rizika prema imovini započinje određivanjem najvrednije imovine, zatim se definiraju ranjivosti čije iskorištavanje može uzrokovati utjecaj nad imovinom, te se na kraju utvrđuju relevantni izvori prijetnji i prijetnje koje mogu iskoristiti definirane ranjivosti. Postupak i način izračuna u okviru procjene rizika u ovom radu opisan je u nastavku.

Metoda procjene rizika koja se primjenjuje jest polukvantitativna metoda, a pristup analizi rizika orijentiran je prema imovini sustava. Imovina sustava prikazana je u tablici 14. Za svaku stavku u tablici pridružena je vrijednost imovine u rasponu od 0 do 100, gdje 0 označava imovinu bez ikakve vrijednosti za poslovanje dok 100 znači ključnu imovinu čijim gubitkom može doći do nenadoknadivih troškova za poslovanje.

Prijetnje koje se razmatraju one su koje potencijalno mogu uzrokovati gubitak podataka, curenje podataka i nedostupnost usluge.

5.2.2 Određivanje imovine sustava

Imovina informacijskog sustava obuhvaća sve što ima neku vrijednost za pojedinca, poduzeće, organizaciju ili naciju. Imovina se dijeli na nekoliko kategorija ovisno o vrsti imovine [34].

- fizička imovina - na primjer računala, računalna oprema, telefoni, namještaj, nekretnine
- informacije ili podaci - dokumenti, baze podataka
- softver
- mogućnost pružanja proizvoda ili usluge
- ljudi
- ostala nematerijalna imovina - reputacija organizacije, znanja i sl.

Imovina informacijskog sustava trebala bi biti zabilježena na jednom mjestu, za što će se u nastavku rada koristiti pojam "katalog imovine". Katalog imovine može biti fizički zapis na papiru ili u digitalnom formatu u obliku proračunskih tablica, baze podatka i slično. U kojem god obliku se nalazi katalog imovine informacijskog sustava, svaki zapis o imovini informacijskog sustava mora sadržavati neki minimalni set atributa.

U tablici 7 prikazan je osnovni set atributa koji opisuje imovinu informacijskog sustava. Način dodjeljivanja interne kataloške oznake drugačiji je za svaku organizaciju ovisno o njezinim potrebama. Za potrebe ovog rada interna kataloška oznaka bit će sastavljena od šifre kategorije imovine i slijednog niza brojeva unosa u katalog imovine u formatu SIFRA-NN, pri čemu se šifra definira kao:

- FIZ - fizička imovina
- POD - informacije i podaci
- SOF - softver
- POS - mogućnost pružanja proizvoda ili usluge
- LJU - ljudi
- NMI - nematerijalna imovina

Tablica 7: Osnovni set atributa zapisa imovine informacijskog sustava

Atribut	Opis
Interna kataloška oznaka	Interna kataloška oznaka predstavlja jedinstvenu identifikacijsku oznaku unutar sustava. Kataloška oznaka je proizvoljna i ovisi o potrebama sustava.
Kategorija imovine	Kategorija imovine ovisno o vrsti imovine (npr. fizička imovina, softver, informacije i podaci, ljudi, nematerijalna imovina itd.).
Naziv imovine	Naziv imovine odnosi se na općeniti naziv za imovinu unutar sustava (npr. prijenosno računalo, kontakt podaci korisnika itd.).
Opis imovine	Opis imovine detaljni je opis imovine sustava kako bi se imovina mogla lakše identificirati (npr. za naziv imovine "prijenosno računalo" opis imovine bi mogao biti: Lenovo ThinkPad E590 intel i5 8th gen).

U tablici 8 prikazan je dodatan set atributa koji može opisivati imovinu ovisno o potrebama organizacije.

Tablica 8: Dodatni set atributa zapisa imovine informacijskog sustava

Atribut	Opis
Količina	Količina imovine (npr. za prijenosna računala količina imovine može se izraziti numeričkom vrijednošću 5, 10 itd., dok se informacije i podaci mogu izraziti u količini podatka, npr. 6 GB, ili broju zapisa, npr. 1.300.000 zapisa). Količina imovine nije obavezan atribut jer se ne može pridružiti svakom zapisu imovine.
Proizvođač	Naziv proizvođača.

Kataloški broj proizvođača	Interna oznaka koju proizvođač pridružuje svakom proizvodu (npr. bar kod).
Vrijednost imovine	Vrijednost imovine izražena prema kvalitativnoj, kvantitativnoj ili polukvantitativnoj metodi.
Garancija	Garancija koju daje proizvođač.

Za potrebe ovog diplomskog rada katalog imovine bit će zapisan u obliku prikazanom u tablici 9

Tablica 9: Primjer kataloga imovine za potrebe rada

Interna kat. oznaka	Kategorija imovine	Naziv imovine	Opis imovine	Vrijednost imovine

Svaka organizacija ima vlastiti pogled na vrijednost imovine, pa tako ne postoji generički model za određivanje vrijednosti. Svaka organizacija oblikuje svoj postupak procjene vrijednosti imovine u skladu s vlastitim potrebama. Vrijednost imovine u ovom radu definira se prema polukvantitativnoj skali iz tablice 5. Vrijednosti za neku imovinu dobivaju se prema navedenom upitniku. Upitnik se sastoji od četiri pitanja gdje maksimalan broj bodova iznosi 100. Ukupan zbroj bodova ostvarenih odgovorima na sva četiri pitanja daje procjenu vrijednosti imovine. Izradom ovakvih upitnika u organizaciji omogućava se da više osoba procjenjuje vrijednost imovine. Moguće je definirati pitanja sa specifičnijim odgovorima kako bi se uklonio subjektivni dojam osobe koja provodi procjenu imovine, ali za potrebe ovog rada dovoljan je ovakav jednostavan upitnik.

Što će se dogoditi ako organizacija ostane bez navedene imovine? (P1, najviše 15 bodova)

- 0 ništa
- 3 neke operacije mogu kasniti, ali nije kritično
- 8 nedostatak imovine je primjetan, ali može se nadoknaditi
- 12 dolazi do velikih troškova
- 15 zastoj u poslovanju, moguće veće posljedice za poslovanje

Koliki su troškovi za nadoknadu imovine? (P2, najviše 40 bodova)

- 3 zanemarivo mali troškovi
- 8 mali troškovi
- 20 veliki troškovi
- 32 iznimno veliki troškovi
- 40 troškovi koje poslovanje ne može podnijeti

Koliko je vremena potrebno za nadoknadu imovine? (P3, najviše 30 bodova)

- 2 zanemarivo malo
- 6 malo
- 15 puno
- 24 izrazito puno
- 30 nije moguće nadoknaditi imovinu

Postoje li zakonske obaveze vezane uz gubitak imovine? (P4, najviše 15 bodova)

- 0 nema ih
- 3 postoje ali su zanemarive
- 8 postoje jasni zakoni koji propisuju male kazne
- 12 postoje jasni zakoni koji propisuju velike kazne
- 15 jako stroge sankcije

5.3 Procjena rizika informacijskog sustava

5.3.1 Određivanje relevantnih prijetnji za informacijski sustav

Organizacija mora utvrditi i specificirati relevantne izvore prijetnji. Izvori informacija za izvore prijetnji određuju se u pripremi za procjenu rizika, a u tablici 4 prikazane su vrste informacija koje pruža određena organizacijska razina. Kad je riječ o konkurenciji kao posebnom izvoru prijetnje, potrebno je odrediti sposobnost konkurencije, namjeru konkurencije i cilj konkurencije, dok je za ostale izvore dovoljno odrediti raspon mogućih utjecaja.

U tablici 10 prikazana je podjela prijetnji prema njihovom izvoru. Konkurencija predstavlja izvor prijetnje od strane pojedinih osoba unutar ili izvan organizacije, grupa izvan organizacije ili drugih organizacija. Konkurencija predstavlja prijetnju informacijskom sustavu kroz fizičku sabotažu, elektroničku sabotažu, otkrivanje informacija, krađu, prijevaru ili špijunažu. Slučajne ljudske greške prijetnje su koje nastaju zbog slučajnih pogrešaka zaposlenika za vrijeme obavljanja njihovih svakodnevnih zadataka. Slučajne greške nastaju zbog nepažnje, nemara, nezanimanja za obavljanje zadataka ili neznanja. Organizacijske prijetnje jesu prijetnje za imovinu (softver ili hardver) zbog eksploatacije hardverske opreme izvan propisanih operativnih parametara proizvođača ili neažuriranja softvera. Operativne prijetnje najčešće nastaju zbog neodgovarajućih ili neadekvatnih procedura u organizacijama, neznanja osoblja ili zbog različitosti i nekompatibilnosti opreme. Prijetnje koje predstavljaju prirodnih sila obuhvaćaju prirodne nepogode ili ostale događaje koji su

izvan kontrole organizacije. U prirodne nepogode spadaju poplave, požari, potresi i bolesti, a u ostale događaje mogu se svrstati rat, građanski nemiri, demonstracije i protesti, oštećenja na električnim i telekomunikacijskim mrežama i drugo.

Tablica 10: Klasifikacija izvora prijetnji

Izvor: [29]

Izvor prijetnje	Opis prijetnje	Oblik djelovanja
Tehnološki kriminal	Pojedinci, grupe ili organizacije koje žele iskoristiti ovisnost organizacije o digitalnim resursima	Fizička sabotaža, elektronička sabotaža, otkrivanje informacija, krađa, prijevara, špijunaža
Ljudske prijetnje	Greške zaposlenika i ostalog osoblja nastale za vrijeme obavljanja njihovih svakodnevnih aktivnosti	Nepažnja, nemar, nezanimanje, neznanje
Organizacijske prijetnje	Incidenti nastali na opremi i softveru zbog neadekvatnog održavanja, zamjene ili ažuriranja ili zbog njihova korištenja izvan operativnih parametara	Neodgovarajuće procedure, nemotiviranost, različitost opreme, nekompatibilnosti
Utjecaji prirodnih sila	Prirodne nepogode i ostali događaji izvan kontrole organizacije	Vatra, poplava, potres, bolest, rat, građanski nemiri

Prijetnja je svaka okolnost ili događaj čija pojava može imati negativne posljedice na poslovanje, imovinu, ljude, druge organizacije i naciju. Organizacija utvrđuje relevantne prijetnje koje nastaju iz identificiranih izvora prijetnji.

U tablici 11 prikazana je skala za određivanje vjerojatnosti pojave prijetnje. Procjenu za tehnološki kriminal teško je potkrijepiti dokazima pa se stoga najčešće oslanja na iskustvo osobe ili tima koji sudjeluje u procesu procjene rizika. Vjerojatnost pojave prijetnje za ostale kategorije moguće je potkrijepiti dokazima pa se ona često određuje prema učestalosti pojave prijetnje. Na primjer, učestalost pojave prijetnji koje proizlaze iz grešaka programera može se odrediti na temelju prijavljenih grešaka u nekom vremenskom rasponu, za potrebe čega organizacije mogu upotrebljavati informacijski sustav koji omogućava jednostavno prijavljivanje i praćenje grešaka te dobivanje informacija o broju grešaka. Primjeri takvih informacijskih sustava mogu biti jednostavni i besplatni alati kao što su Todoist, Assana i Trello, pa sve do velikih sustava kao što je Jira.

U nastavku rada za vjerojatnost pojave prijetnje koristiti će se oznaka $P_{prijetnja}$.

Tablica 11: Skala za određivanje vjerojatnosti pojave prijetnje prema polukvantitativnoj metodi

Izvor: [29]

Vrijednost	Procjena za tehnološki kriminal	Procjena za ostale prijetnje
96-100	vrlo vjerojatno	Više od 100 pojava na godinu
80-95	vjerojatno	Između 10 i 100 pojava na godinu
21-79	moguće	Između 1 i 10 pojava u godini
5-20	nije vjerojatno	Jedna ili manje pojava u godini, ali više od jedne pojave u 10 godina
0-4	izrazito nije vjerojatno	Jedna ili manje pojava u 10 godina

5.3.2 Određivanje ranjivosti informacijskog sustava

Ranjivosti su greške, mane, slabosti ili karakteristike sustava ili elementa sustava koje potencijalne prijetnje mogu iskoristiti te negativno utjecati na imovinu sustava. Ranjivosti mogu biti na infrastrukturi, okolini, hardveru, softveru, operativnim procesima, komunikacijama itd. U postupku procjene rizika potrebno je odrediti relevantne ranjivosti koje mogu biti iskorištene pojavom prijetnje.

Različiti se izvori informacija mogu upotrebljavati za određivanje ranjivosti informacijskog sustava: analize sustava, izvještaji revizija sigurnosti, baze podataka o ranjivosti sustava, podaci dobiveni od proizvođača o ranjivostima i greškama proizvoda, alati za otkrivanje ranjivosti u informacijskim sustavima, sigurnosna testiranja, penetracijska testiranja itd.

U ovom će radu primarni izvor informacija za ranjivosti sustava biti vlastita analiza sustava i baze podataka dostupne na internetu:

- NIST National Vulnerability Database [37]
- snyk Vulnerability DB [38]
- Exploit Database [39]
- White Source Vulnerability Database [40]
- VulDB [41]

Određivanje vjerojatnosti iskorištavanja ranjivosti izvršava se prema skali iz tablice 12; u nastavku rada za vjerojatnost iskorištavanja ranjivosti koristiti će se oznaka $P_{ranjivost}$.

Tablica 12: Skala za određivanje vjerojatnosti toga da će prijetnja iskoristiti ranjivost prema polukvantitativnoj metodi

Izvor: [29]

Vrijednost	Opis
96-100	Ranjivost je velika, izložena i lako iskoristiva, iskorištavanjem je moguće uzrokovati veliki utjecaj na imovinu. Sigurnosni postupci nisu planirani niti implementirani.
80-95	Ranjivost je velika, a ovisno o izloženosti ranjivosti i načinu iskorištavanja moguće su velike posljedice na imovinu. Sigurnosni postupci su planirani, ali nisu implementirani.
21-79	Ranjivost je srednja, a ovisno o izloženosti ranjivosti i načinu iskorištavanja moguće su veće posljedice na imovinu. Sigurnosni postupci djelomično su implementirani i djelomično učinkoviti.
5-20	Ranjivost je malena. Sigurnosni postupci su implementirani i djelomično učinkoviti.
0-4	Ranjivost nije potrebno uzimati u obzir. Sigurnosni postupci su implementirani i učinkoviti.

5.3.3 Određivanje vjerojatnosti pojave sigurnosnog incidenta u informacijskom sustavu

Vjerojatnost pojave incidenta u informacijskom sustavu određuje se kao umnožak vjerojatnosti pojave prijetnje ($P_{prijetnja}$) i vjerojatnosti iskorištavanja ranjivosti u slučaju pojave prijetnje ($P_{ranjivost}$). Umnožak ovih dviju vjerojatnosti dijeli se s faktorom veličine skale koji u ovoj procjeni iznosi 100. Tako će vrijednost vjerojatnosti pojave incidenta ($P_{incident}$) biti u rasponu od 0 do 100. To se može opisati sljedećom jednadžbom:

$$P_{incident} = \frac{P_{prijetnja} \, x \, P_{ranjivost}}{100}$$

gdje je:

- $P_{incident}$ - vjerojatnost pojave incidenta u informacijskom sustavu
- $P_{prijetnja}$ - vjerojatnost pojave prijetnje
- $P_{ranjivost}$ - vjerojatnost iskorištavanja ranjivosti
- 100 - veličina skale

5.3.4 Određivanje utjecaja pojave sigurnosnog incidenta na imovinu informacijskog sustava

Za svaki navedeni sigurnosni incident potrebno je odrediti vjerojatnost njegova utjecaja na imovinu sustava. Sigurnosni incident može imati utjecaj na jednu ili više stavki iz kataloga imovine.

Vjerojatnost utjecaja sigurnosnog incidenta na imovinu sustava u nastavku rada bit će označena kao $P_{utjecaj}$.

Radi pojednostavnjenja procjene rizika u ovom radu uzeta je pretpostavka da svaki sigurnosni incident ima ili 0 % ili 100 % vjerojatnosti da utječe na imovinu, stoga formula za izračun izgleda ovako:

$$P_{utjecaj} = \frac{P_{utjecajimovina} \times P_{incident}}{100}$$

gdje je:

- $P_{utjecaj}$ - vjerojatnost utjecaja sigurnosnog incidenta na imovinu
- $P_{utjecajimovina}$ - vjerojatnost da će sigurnosni incident utjecati na imovinu u vrijednostima 0 ili 100
- $P_{incident}$ - vjerojatnost pojave sigurnosnog incidenta

5.3.5 Određivanje rizika

Određivanje rizika moguće je provoditi s više različitih gledišta. Prema [29] dva najčešća gledišta za procjenu rizika u informacijskim sustavima jesu:

- procjena rizika s gledišta imovine
- procjena rizika s gledišta prijetnje

U ovom će se radu razmatrati procjena rizika s gledišta imovine.

Izračun rizika koji prijeti nekoj imovini određuje se kao umnožak vjerojatnosti utjecaja na imovinu u slučaju pojave prijetnje ($P_{utjecaj}$) i vrijednosti imovine ($V_{imovina}$). Taj umnožak vjerojatnosti utjecaja i vrijednosti imovine dijeli se faktorom veličine skale 100. Tako će vrijednost rizika nad nekom imovinom od određene prijetnje biti u rasponu od 0 do 100. To se može opisati sljedećom jednadžbom:

$$R_{imovina} = \frac{P_{utjecaj} \, x \, V_{imovina}}{100}$$

gdje je:

- $R_{imovina}$ - rizik za imovinu u slučaju pojave određene prijetnje
- $P_{utjecaj}$ - vjerojatnost utjecaja na imovinu
- $V_{imovina}$ - vrijednost imovine

6. Procjena rizika za informacijski sustav

6.1 Pretpostavke i ograničenja za procjenu rizika za informacijski sustav

Budući da je riječ o konceptualnom sustavu za određivanje relevantnih prijetnji, potrebno je postaviti neke pretpostavke, s obzirom na to da ne postoji prijetnja za sustav koji ne postoji. Pretpostavke su sljedeće:

- Baza podataka nalazi se u hipotetskom podatkovnom centru koji se nalazi u Nizozemskoj.
- MQTT i HTPP poslužitelji nalaze se u podatkovnom centru istog vlasnika, ali u Francuskoj.
- Jedna osoba je administrator sustava i ima pristup bazi podataka i poslužiteljima.
- Jedna osoba je programer koji razvija sustav.
- Sustav ima 10 hipotetskih klijenata od kojih svaki klijent posjeduje jedno mjerno mjesto.
- Sigurnosna kopija baze podataka izrađuje se svakih 7 dana.
- Vraćanje sigurnosne kopije traje 8 sati.

6.2 Određivanje imovine informacijskog sustava

Tablica 13 predstavlja katalog imovine informacijskog sustava. Budući da je riječ o konceptu informacijskog sustava, u katalogu imovine nalazi se samo imovina vezana uz podatke i informacije te intelektualno vlasništvo.

Tablica 13: Procjena rizika: imovina informacijskog sustava

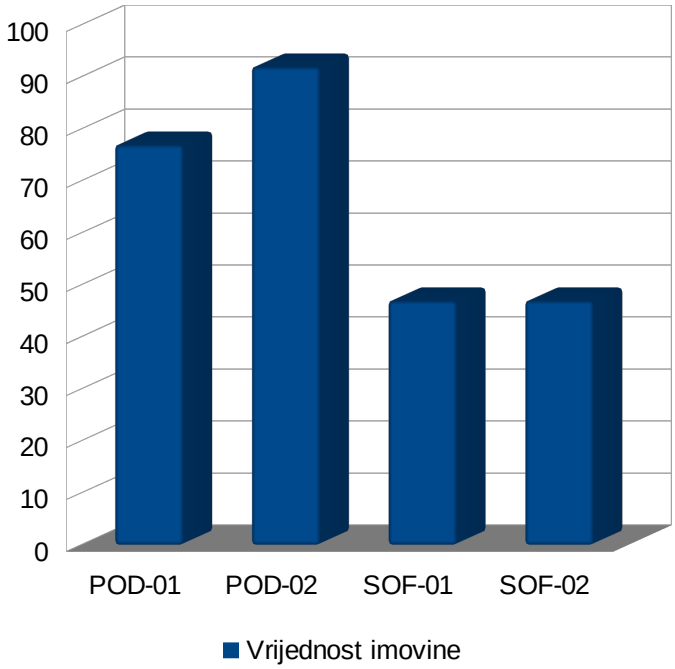
Interna kat. oznaka	Kategorija imovine	Naziv imovine	Opis imovine
POD-01	POD	Podaci mjerenja	Podaci mjerenja sa senzorskih jedinica
POD-02	POD	Podaci o korisnicima sustava	Korisnička imena, adrese elektroničke pošte, lozinke
SOF-01	SOF	Model dozrijevanja proizvoda	Softverski model za detekciju zrelosti proizvoda
SOF-02	SOF	Softver za analizu i obradu podataka	Softver za analizu i obradu podataka sa senzorskih jedinica

Određivanje imovine sustava prikazano je u tablici 14. Interna kataloška oznaka predstavlja vezu s opisom imovine u tablici 13. Stupci P1, P2, P3 i P4 prikazuju rezultat dobiven na temelju odgovora na svako pitanje iz upitnika za procjenu rizika, dok je stupac "vrijednost imovine" ukupna suma

svih odgovora. Prema rezultatima upitnika, imovina od najveće vrijednosti u sustavu jesu podaci mjerenja i podaci o korisnicima sustava. Na slici 9 grafički je prikazana utvrđena vrijednost imovine iz tablice 14.

Tablica 14: Procjena rizika: vrijednost imovine informacijskog sustava

Interna kat. oznaka	P1	P2	P3	P4	Vrijednost imovine
POD-01	15	32	30	0	77
POD-02	15	32	30	15	92
SOF-01	12	20	15	0	47
SOF-02	12	20	15	0	47



Slika 9 Vrijednost imovine informacijskog sustava

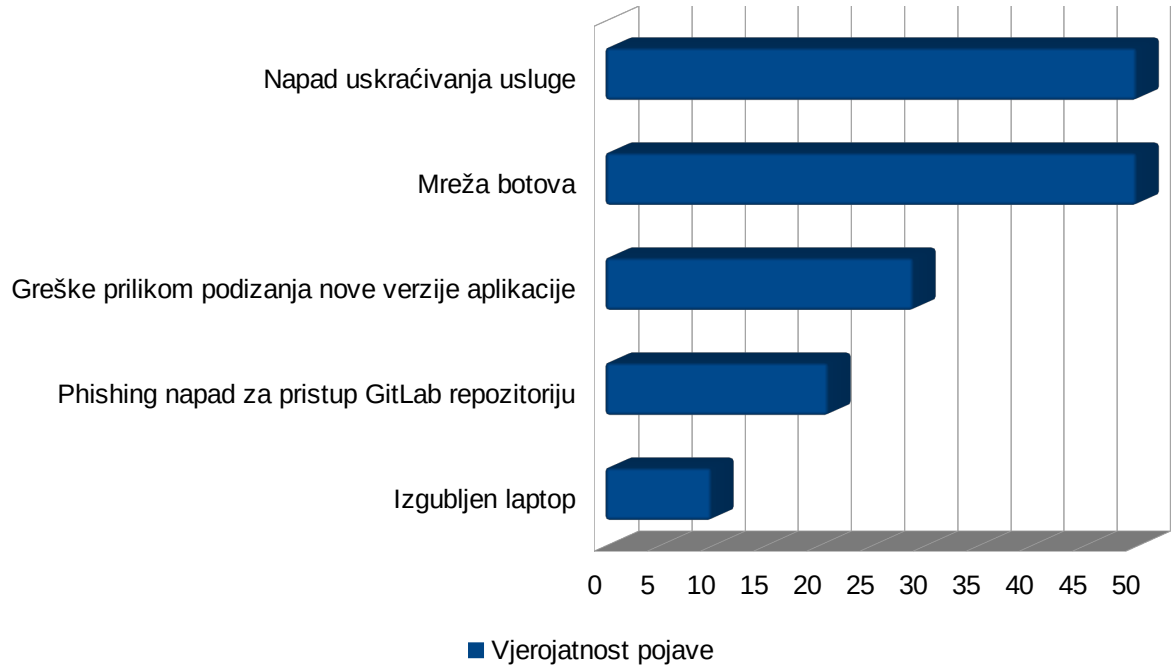
6.3 Određivanje relevantnih prijetnji prema informacijskom sustavu

U tablici 15 prikazane su relevantne prijetnje prema informacijskom sustavu. Relevantne prijetnje određene su na temelju iskustava autora u radu s informacijskim sustavima. Vjerojatnost pojave također je određena empirijski, a vrijednost vjerojatnosti pojave izražena je prema skali iz tablice 11.

Tablica 15: Procjena rizika: prijetnje prema informacijskom sustavu

Izvor prijetnje	Prijetnja	Vjerojatnost pojave
Zlonamjerni korisnici	Mreža botova	50
Zlonamjerni korisnici	Napad uskraćivanja usluge	50
Ljudske pogreške	Greške prilikom podizanja nove verzije aplikacije	29
Ljudske pogreške	Izgubljeno prijenosno računalo	10
Tehnološki kriminal	Phishing napad za pristup GitLab repozitoriju	21

Dvije najveće prijetnje ovom informacijskom sustavu, kao što je vidljivo na slici 10, jesu napad uskraćivanja usluge i mreža botova. Empirijskom analizom obiju prijetnji određena je vjerojatnost pojave od 50 bodova, što označava da je moguće da će u prosjeku doći do oko pet pojava prijetnje u jednoj godini. Ostale prijetnje ocjenjene su manjim vjerojatnostima pojave, a najmanjom vjerojatnošću pojave ocjenjena je prijetnja "izgubljeno prijenosno računalo", za koju se računa da je učestalost pojave između jednog i dva događaja u 10 godina.



Slika 10: Grafički prikaz vjerojatnosti pojave prijetnje u informacijskom sustavu

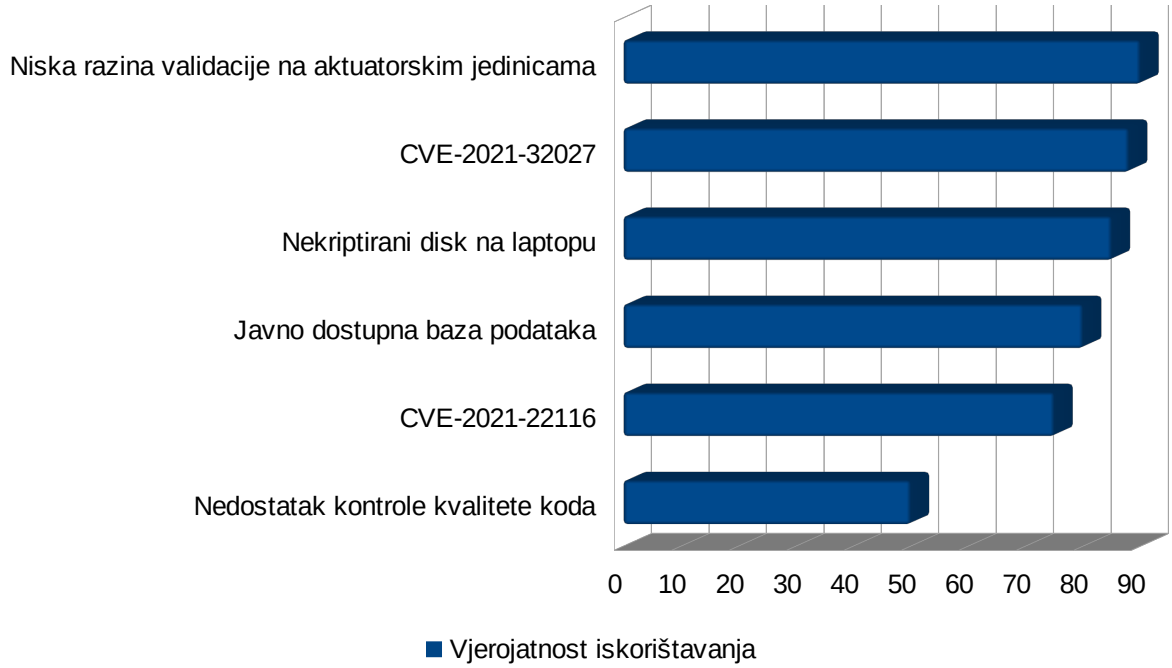
6.4 Određivanje ranjivosti informacijskog sustava

Tablica 16 prikazuje ranjivosti informacijskog sustava. Kad je riječ o prijetnjama sustavu kojima je izvor baza podataka s ranjivostima elemenata informacijskog sustava, vjerojatnost iskorištavanja ranjivosti definirana je prema njihovoj CVE ocjeni, odnosno razini ozbiljnosti, uvećanoj za faktor 10 kako bi se uklopilo u skalu korištenu u ovom radu. Vjerojatnost iskorištavanja ranjivosti sustava kojima je izvor analiza sustava dobivene su empirijski.

Tablica 16: Procjena rizika: ranjivosti informacijskog sustava

Ranjivost	Opis	Izvor	Vjerojatnost
CVE-2021-32027	Mana u pogledu validacije pri modifikaciji pojedinih SQL upita zbog nepostojećih zagrada omogućava autoriziranom korisniku upisivanje proizvoljnih bajtova u serversku memoriju.	[37]	88
CVE-2021-22116	Sve verzije RabbitMQ poslužitelja starije od verzije 3.8.16 imaju manu zbog neadekvatne validacije u AMQP konekciji zbog koje mogu biti izložene napadu uskraćivanja usluge. Zlonamjerni korisnik može iskoristiti ranjivost za slanje malicioznih AMQP poruka na RabbitMQ poslužitelja.	[37]	75
Javno dostupna baza podataka	Baza podataka nalazi se na javno dostupnoj IP adresi pa bilo koji zlonamjerni korisnik može iskoristiti tu ranjivost za izvršavanje napada uskraćivanja usluge baze podatka i pokušaja dobivanja nelegitimnog pristupa bazi podatka.	Analiza sustava	80
Nekriptirani disk na prijenosnom računalu	Ako u slučaju gubitka prijenosnog računala to računalo pronađe zlonamjerna osoba, ona vrlo jednostavno može doći do svih podataka na računalu, uključujući pristup bazi podataka i repozitoriju koda.	Analiza sustava	85
Niska razina validacije na aktuatorskim jedinicama	Zbog niske razine validacije koda na aktuatorskim jedinicama, prilikom dohvata naredbi s MQTT poslužitelja moguće je ubacivanje malicioznog koda na uređaj.	Analiza sustava	90
Nedostatak kontrole kvalitete koda	Zbog nedostatka kontrole kvalitete softvera prije puštanja u rad moguće su pojave grešaka koje uzrokuju gubitak podatka ili nedostupnost sustava.	Analiza sustava	50

Na slici 11 vidljivo je da je najveća ranjivost sustava niska razina validacije na aktuatorskim jedinicama, čija vjerojatnost iznosi 90 bodova, Slijede ranjivosti CVE-2021-32027 s 88 bodova i nekriptirani tvrdi disk na prijenosnom računalu s 85 bodova. Najmanju vjerojatnost iskorištavanja ima ranjivost nedostataka kontrole kvalitete koda s 50 bodova.



Slika 11: Ranjivosti informacijskog sustava

6.5 Određivanje vjerojatnosti pojave sigurnosnog incidenta

U tablici 17 opisani su mogući sigurnosni incidenti koji prijete informacijskom sustavu. U stupcu "Prijetnja" nalaze se prijetnje utvrđene u tablici 15, a u stupcu "Ranjivost" nalaze se ranjivosti utvrđene u tablici 16. Stupac "Opis incidenta" daje kratak opis sigurnosnog incidenta u informacijskom sustavu u slučaju da prijetnja sustavu uspješno iskoristi ranjivost sustava.

Tablica 17: Procjena rizika: procjena sigurnosnih incidenata u informacijskom sustavu

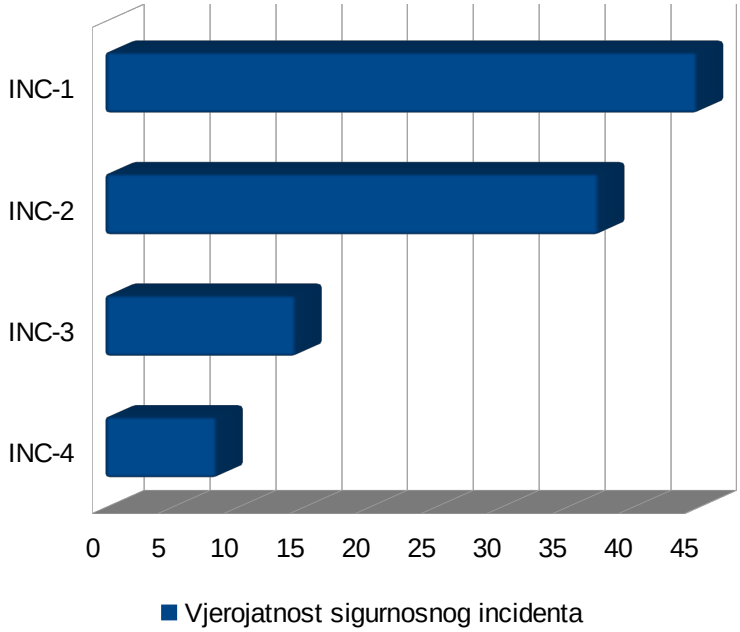
Inc.	Prijetnja	Ranjivost	Opis incidenta
INC-1	Mreža botova	Niska razina validacije na aktuatorskim jedinicama	Zbog niske razine validacije na aktuatorskim jedinicama na njih je poslan maliciozni kod s pomoću kojeg botnet mreža ima kontrolu nad aktuatorskim jedinicama.

Inc.	Prijetnja	Ranjivost	Opis incidenta
INC-2	Napad uskraćivanja usluge	CVE-2021-22116	Nedostupan poslužitelj zbog napada uskraćivanja usluge na MQTT poslužitelj. Iskorištavanje ranjivosti CVE-2021-22116, pri čemu je zbog manjka validacije omogućen napad uskraćivanja usluge na AMQP klijentu.
INC-3	Greške prilikom podizanja nove verzije aplikacije	Nedostatak kontrole kvalitete koda	Gubitak podataka mjerenja zbog greške u radu servisa za prikupljanje podataka.
INC-4	Izgubljeno prijenosno računalo	Nekriptirani disk na prijenosnom računalu	Nakon gubitka/krađe prijenosnog računala zlonamjerni korisnik imao je vrlo jednostavan pristup repozitoriju koda na prijenosnom računalu.

U tablici 18 izračunana je vjerojatnost pojave sigurnosnog incidenta prema postupku prikazanom u poglavlju 5.3.3. Najveću vjerojatnost pojave ima sigurnosni incident INC-1, 45 bodova, dok je najmanju vjerojatnost pojave sigurnosnog incidenta INC-4, samo 8,5 bodova. Na slici 12 prikazan je graf s vjerojatnostima pojave sigurnosnog incidenta, gdje INC-1 ima najveću vjerojatnost, a INC-4 ima najmanju vjerojatnost pojave.

Tablica 18: Procjena rizika: vjerojatnosti sigurnosnog incidenta u informacijskom sustavu

Inc.	Vjerojatnost prijetnje	Vjerojatnost ranjivosti	Vjerojatnost sigurnosnog incidenta
INC-1	50	90	45
INC-2	50	75	37,5
INC-3	29	50	14,5
INC-4	10	85	8,5



Slika 12: Vjerojatnosti pojave sigurnosnog incidenta u informacijskom sustavu

U tablici 19 prikazan je utjecaj sigurnosnog incidenta na imovinu sustava. Ako određeni sigurnosni incident ima utjecaj na imovinu sustava, onda je polje označeno sa 100, a ako sigurnosni incident nema utjecaj na imovinu onda u polju stoji vrijednost 0. Utjecaj sigurnosnog incidenta na imovinu može biti u rasponu do 0 do 100, ali u ovom radu se zbog pojednostavnjenja procjene rizika upotrebljavaju samo dvije krajnje vrijednosti.

Tablica 19: Procjena rizika: utjecaj sigurnosnog rizika na imovinu sustava

		Sigurnosni incident			
		1	2	3	4
Imovina	POD-01	100	100	100	100
	POD-02	0	0	100	100
	SOF-01	0	0	0	100
	SOF-02	0	0	0	100

6.6 Određivanje rizika za informacijski sustav

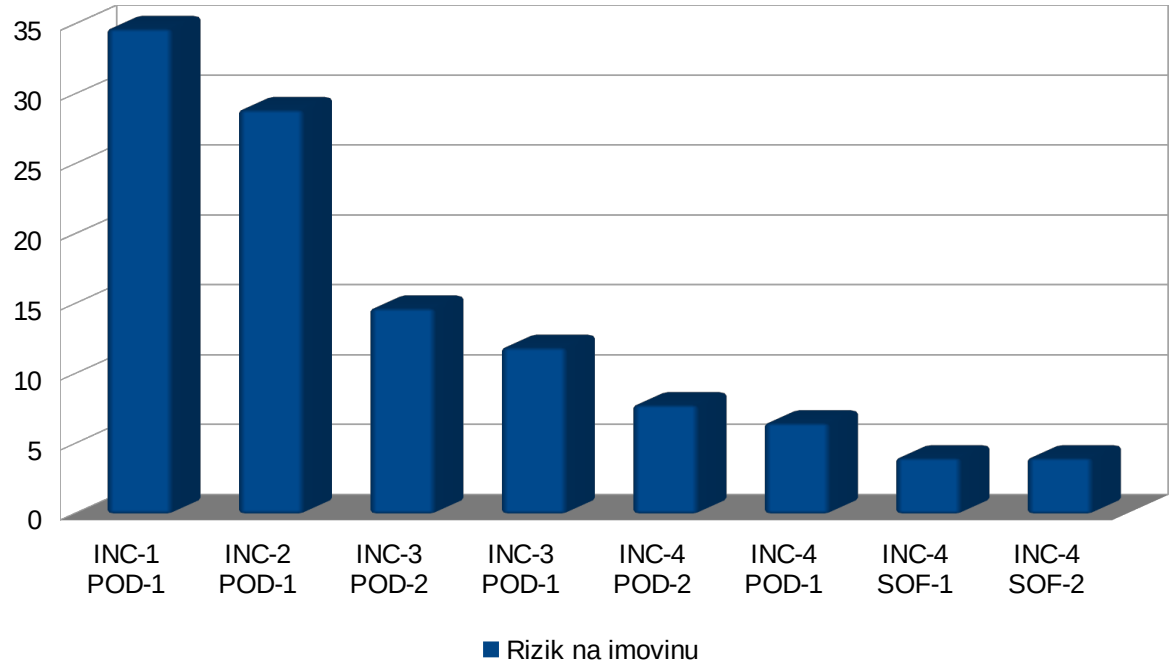
Nakon što su svi prethodni koraci odrađeni, provodi se izračun rizika za imovinu. U tablicu 20 upisani su parovi "imovina - sigurnosni incident" iz tablice 19 čija je vrijednost veća od nula, odnosno oni za koje je utvrđeno da sigurnosni incident ima utjecaj na imovinu sustava.

Rizik za imovinu sustava određuje se na način opisan u poglavlju 5.3.5.

Tablica 20: Procjena rizika: rizik za imovinu sustava

Imovina	Sigurnosni incident	Vjerojatnost sigurnosnog incidenta	Vrijednost imovine	Utjecaj na imovinu	Rizik sigurnosnog incidenta za imovinu	Ukupan rizik za imovinu
POD-1	INC-1	45	77	100	34,7	73
	INC-2	37,5	77	100	28,9	
	INC-3	15,5	77	100	11,9	
	INC-4	8,5	77	100	6,5	
POD-2	INC-3	15,5	92	100	14,7	21
	INC-4	8,5	92	100	7,8	
SOF-1	INC-4	8,5	47	100	4	4
SOF-2	INC-4	8,5	47	100	4	4

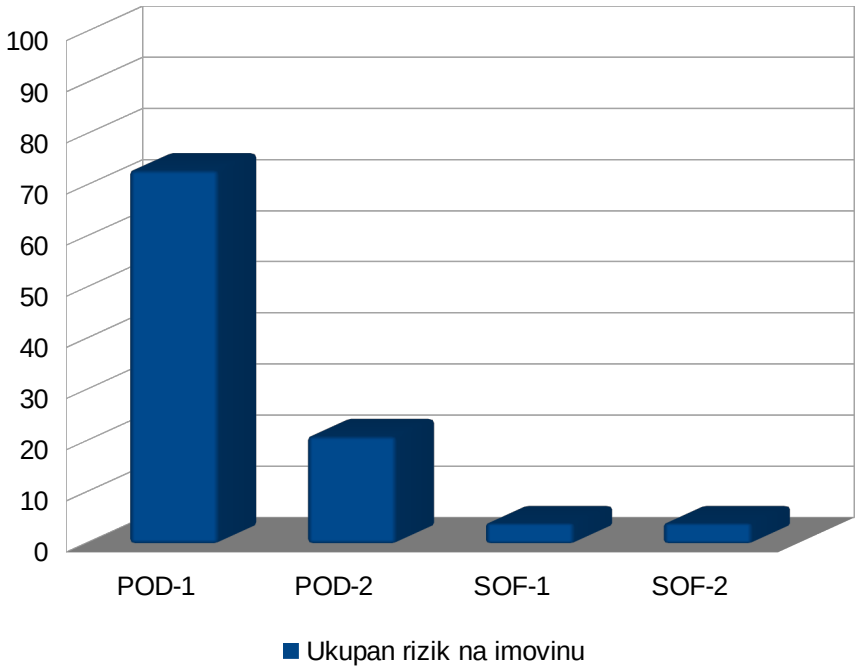
Na slici 13 vidljivo je da najveći rizik postoji za imovinu POD-1 u slučaju pojave sigurnosnog incidenta INC-1.



Slika 13 Rizik sigurnosnog incidenta za imovinu sustava

Kako je vidljivo u tablici 20, na imovinu sustava POD-1 utjecaj imaju četiri moguća sigurnosna incidenta. Tako se ukupan rizik za imovinu POD-1, iskazan u stupcu "Ukupan rizik za imovinu", izračunava kao vjerojatnost da se pojavi jedan ili više incidenata koji imaju utjecaj na imovinu. Na isti se način dobiva sigurnosni rizik za imovinu POD-2.

Ukupan rizik za imovinu prikazan je na slici 14, iz koje je vidljivo da daleko najveći rizik postoji za imovinu POD-1, dok je najmanji rizik prijeti imovini SOF-1 i SOF-2.



Slika 14: Ukupan rizik za imovinu sustava

6.7 Preporuke za smanjenje rizika

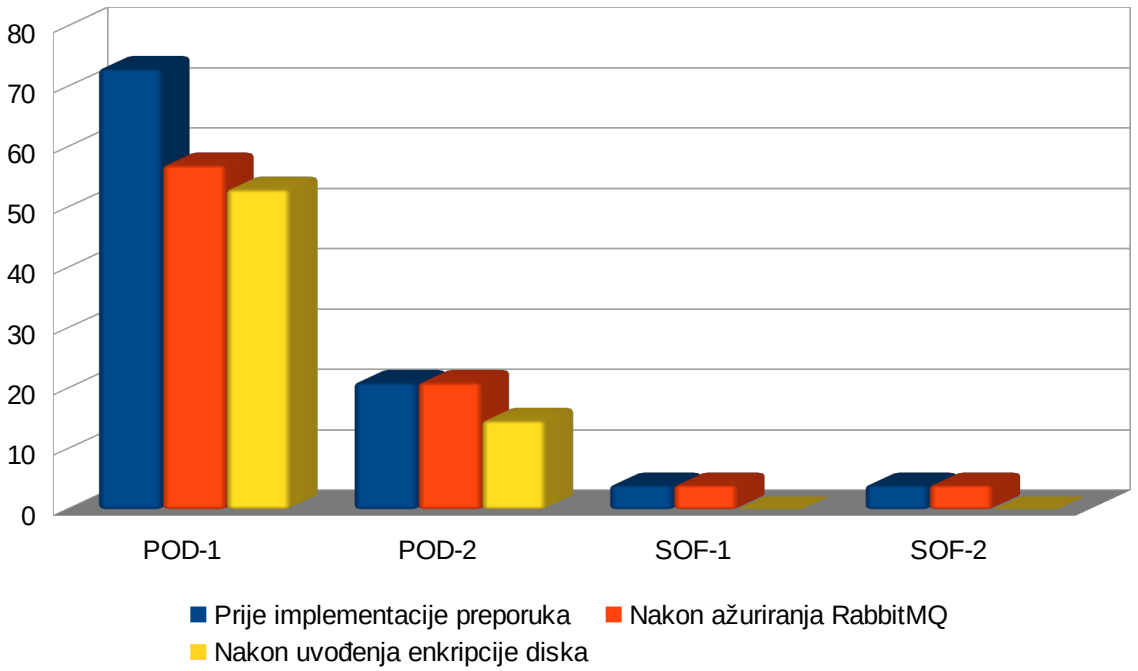
U ovom poglavlju iznose se preporuke kojima se može smanjiti utvrđeni rizik za imovinu POD-1.

Ažuriranjem RabbitMQ MQTT poslužitelja na verziju noviju od 3.8.16 uklanja se ranjivost CVE-2021-22116. Nakon ažuriranja RabbitMQ poslužitelja rizik za imovinu POD-1 smanjen je sa 73 na 57 bodova, što je vidljivo u tablici 21 i grafički prikazano na slici 15.

Uvođenje enkripcije tvrdog diska na prijenosnom računalu uklanja ranjivost koju zlonamjerna osoba potencijalno može iskoristiti u slučaju da se izgubi prijenosno računalo. Nakon uvođenja enkripcije tvrdog diska na prijenosnom računalu smanjen je rizik za svu imovinu. U tablici 21 vidljivo je da je rizik za imovinu POD-1 smanjen sa 57 na 53 boda, rizik za imovinu POD-2 smanjen je s 21 na 14,7 bodova, dok je rizik za imovinu SOF-1 i SOF-2 potpuno uklonjen jer u okviru procjene rizika za potrebe ovog rada nije preostala niti jedna ranjivost koja ima utjecaj na imovinu SOF-1 i SOF-2. Svi rezultati iz tablice 21 prikazani su grafički na slici 15.

Tablica 21: Rizik za imovinu sustava nakon usvajanja preporuka za smanjenje rizika

Imovina	Rizik za imovinu prije implemetacije preporuka	Rizik za imovinu nakon ažuriranja RabbitMQ	Rizik za imovinu nakon uvođenja enkripcije diska
POD-1	73	57	53
POD-2	21	21	14,7
POD-3	4	4	0
POD-4	4	4	0



Slika 15: Rizik za imovinu nakon usvajanja preporuka

7. Zaključak

Internet stvari donosi mogućnosti za poboljšanje i napredak u svim granama industrije. Implementacija interneta stvari ne zamjenjuje nijednu tehnologiju već se njome želi postići razvoj pametnih proizvoda i pametnih procesa. Internet stvari već se ukorijenio u poljoprivrednoj industriji, gdje se primjenjuje u brojnim segmentima, od pametnih poljoprivrednih strojeva, pametnih staklenika i plastenika pa do nadzora polja i farmi. Koncept informacijskog sustava prikazanog u ovom radu primjer je primjene IoT tehnologije u relativno jeftinom sustavu za nadzor različitih parametara na različitim mjestima i za različite potrebe, koji je prvenstveno namijenjen malim poljoprivrednicima i onima koji se poljoprivrednom bave u slobodno vrijeme.

Tema ovog diplomskog rada bila je početna procjena rizika za informacijski sustav utemeljen na konceptu interneta stvari prije puštanja informacijskog sustava u rad. Za navedeni informacijski sustav ispunjeni su svi preduvjeti za ponavljanje procjene rizika nakon puštanja tog informacijskog sustava u rad.

Procjena rizika u ovom radu provedena je u odnosu na imovinu sustava. Budući da se radi o konceptualnom informacijskom sustavu, uvedene su neke pretpostavke kod popisivanja imovine sustava. Rezultati procjene rizika u informacijskom sustavu pokazuju rizik od 73 boda (od mogućih 100 bodova) za gubitak podataka mjerenja, dok je rizik za ostalu imovinu gotovo zanemariv. Kako bi se smanjio rizik za podatke mjerenja, predložene su nadogradnje sustava koje bi smanjile rizik za imovinu. Izračunom je dobiveno da bi se nakon uvođenja predloženih nadogradnji rizik koji prijeti podacima mjerenja smanjio za 20 bodova, što predstavlja smanjenje rizika za 27 %.

Budući koraci vezani uz upravljanje rizikom ovog informacijskog sustava, nakon njegova puštanja u rad, uključuju među ostalim praćenje incidenata koji se pojavljuju u informacijskom sustavu kako bi se mogli točnije pripremiti ulazni parametri (prijetnje, ranjivosti itd.) za ponovnu procjenu rizika.

Popis literature

[1] Y. N. Harari, *Sapiens: Kratka povijest čovječanstva*. Zagreb: Fokus, 2015.

[2] A. El Saddik, „Digital Twins: The Convergence of Multimedia Technologies“, *IEEE MultiMedia*, sv. 25, izd. 2, str. 87–92, tra. 2018, doi: 10.1109/MMUL.2018.023121167.

[3] D. Peraković, M. Periša, i R. E. Sente, „Information and Communication Technologies Within Industry 4.0 Concept“, u *Advances in Design, Simulation and Manufacturing*, V. Ivanov, Y. Rong, J. Trojanowska, J. Venus, O. Liaposhchenko, J. Zajac, I. Pavlenko, M. Edl, i D. Perakovic, Ur. Cham: Springer International Publishing, 2019, str. 127–134. doi: 10.1007/978-3-319-93587-4_14.

[4] F. A. Alaba, M. Othman, I. A. T. Hashem, i F. Alotaibi, „Internet of Things security: A survey“, *Journal of Network and Computer Applications*, sv. 88, str. 10–28, lip. 2017, doi: 10.1016/j.jnca.2017.04.002.

[5] D. Peraković, M. Periša, i P. Zorić, „Challenges and Issues of ICT in Industry 4.0“, u *Advances in Design, Simulation and Manufacturing II*, V. Ivanov, J. Trojanowska, J. Machado, O. Liaposhchenko, J. Zajac, I. Pavlenko, M. Edl, i D. Perakovic, Ur. Cham: Springer International Publishing, 2020, str. 259–269. doi: 10.1007/978-3-030-22365-6_26.

[6] D. Kant, A. Johannsen, i R. Creutzburg, „Analysis of IoT Security Risks based on the exposure of the MQTT Protocol“, str. 8.

[7] V. Casola, A. De Benedictis, M. Rak, i U. Villano, „Toward the automation of threat modeling and risk assessment in IoT systems“, *Internet of Things*, sv. 7, str. 100056, ruj. 2019, doi: 10.1016/j.iot.2019.100056.

[8] S. Sinha, „State of IoT 2021: Number of connected IoT devices growing 9% to 12.3 billion globally, cellular IoT now surpassing 2 billion“, 22. rujan 2021. [Na internetu]. Dostupno na: https://iot-analytics.com/number-connected-iot-devices/

[9] B. Buntz, „The Top 20 Industrial IoT Applications“, 20. rujan 2017. https://www.iotworldtoday.com/2017/09/20/top-20-industrial-iot-applications/

[10] „HT Internet stvari“. https://www.hrvatskitelekom.hr/poslovni/ict/m2m-internet-of-things (pristupljeno 21. srpanj 2021.).

[11] „A1 Internet stvari“. https://www.a1.hr/poslovni/internet/internet-stvari (pristupljeno 21. srpanj 2021.).

[12] „The Things Network - Gateway Map“. https://www.thethingsnetwork.org/map

[13] O. Elijah, T. A. Rahman, I. Orikumhi, C. Y. Leow, i M. H. D. N. Hindia, „An Overview of Internet of Things (IoT) and Data Analytics in Agriculture: Benefits and Challenges“, *IEEE Internet Things J.*, sv. 5, izd. 5, str. 3758–3773, lis. 2018, doi: 10.1109/JIOT.2018.2844296.

[14] J. Kotak, A. Shah, A. Shah, i P. Rajdev, „A Comparative Analysis on Security of MQTT Brokers“, u *2nd Smart Cities Symposium (SCS 2019)*, Bahrain, Bahrain, 2019, str. 7 (5 pp.)-7 (5 pp.). doi: 10.1049/cp.2019.0180.

[15] N. H. Nik Zulkipli, A. Alenezi, i G. B. Wills, „IoT Forensic: Bridging the Challenges in Digital Forensic and the Internet of Things“:, u *Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security*, Porto, Portugal, 2017, str. 315–324. doi: 10.5220/0006308703150324.

[16] I. Cvitić, M. Vujic, i S. Husnjak, „Classification of Security Risks in the IoT Environment“, u *DAAAM Proceedings*, 1. izd., sv. 1, B. Katalinic, Ur. DAAAM International Vienna, 2016, str. 0731–0740. doi: 10.2507/26th.daaam.proceedings.102.

[17] P. Mell i T. Grance, „The NIST Definition of Cloud Computing“, str. 7.

[18] „Difference between Thin clients and Thick Clients“, *Difference between Thin clients and Thick Clients*. https://www.geeksforgeeks.org/difference-between-thin-clients-and-thick-clients/ (pristupljeno 24. siječanj 2022.).

[19] G. Ramachandra, M. Iftikhar, i F. A. Khan, „A Comprehensive Survey on Security in Cloud Computing“, *Procedia Computer Science*, sv. 110, str. 465–472, 2017, doi: 10.1016/j.procs.2017.06.124.
[20] F. Liu *i ostali*, „NIST Cloud Computing Reference Architecture“, str. 35.
[21] C. Verdouw, B. Tekinerdogan, A. Beulens, i S. Wolfert, „Digital twins in smart farming“, *Agricultural Systems*, sv. 189, str. 103046, tra. 2021, doi: 10.1016/j.agsy.2020.103046.
[22] D. Jones, C. Snider, A. Nassehi, J. Yon, i B. Hicks, „Characterising the Digital Twin: A systematic literature review“, *CIRP Journal of Manufacturing Science and Technology*, sv. 29, str. 36–52, svi. 2020, doi: 10.1016/j.cirpj.2020.02.002.
[23] Republika Hrvatska, „Zakon o informacijskoj sigurnosti“. Narodne novine, Zagreb, 2007.
[24] Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, i S. Shieh, „IoT Security: Ongoing Challenges and Research Opportunities“, u *2014 IEEE 7th International Conference on Service-Oriented Computing and Applications*, Matsue, Japan, stu. 2014, str. 230–234. doi: 10.1109/SOCA.2014.58.
[25] A. Shakdher, S. Agrawal, i B. Yang, „Security Vulnerabilities in Consumer IoT Applications“, u *2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, Washington, DC, USA, svi. 2019, str. 1–6. doi: 10.1109/BigDataSecurity-HPSC-IDS.2019.00012.
[26] D. Perakovic i I. Cvitić, „Nastavni materijali za kolegij: Sigurnost i zaštita informacijsko komunikacijskog sustava“, Zagreb, 2019.
[27] A. W. Atamli i A. Martin, „Threat-Based Security Analysis for the Internet of Things“, u *2014 International Workshop on Secure Internet of Things*, Wroclaw, Poland, ruj. 2014, str. 35–43. doi: 10.1109/SIoT.2014.10.
[28] J. Rathke i V. Sassone, „Cyber Security in the internet of things“, *Cryptology and Information Security Series*, sv. 4, str. 109–124, 2010.
[29] Joint Task Force Transformation Initiative, „Guide for conducting risk assessments“, National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-30r1, 2012. doi: 10.6028/NIST.SP.800-30r1.
[30] C. Biscoe, „7 steps to a successful ISO 27001 risk assessment“, *IT Governance Blog*, 18. lipanj 2020. https://www.itgovernance.co.uk/blog/7-steps-to-a-successful-iso-27001-risk-assessment (pristupljeno 22. veljača 2022.).
[31] I. Sotnikov, „How to Perform IT Risk Assessment“, 16. siječanj 2018. https://blog.netwrix.com/2018/01/16/how-to-perform-it-risk-assessment/ (pristupljeno 28. veljača 2022.).
[32] J. Zhao, „How to Perform a Successful IT Risk Assessment“, *How to Perform a Successful IT Risk Assessment*, 20. prosinac 2021. https://hyperproof.io/resource/it-risk-assessment/ (pristupljeno 28. veljača 2022.).
[33] M. Musa, P. Zorić, T. M. Kuljanić, i N. Gabelica, „Use Case: Information Security Risk Assessment for Providers of Services in a Virtual Environment“, u *5th EAI International Conference on Management of Manufacturing Systems*, Cham, 2022, str. 379–395.
[34] P. Zorić, M. Musa, i T. M. Kuljanić, „Use of Probabilistic Risk Assessment Methodology for Providers of Services in a Virtual Environment“, u *Sustainable Management of Manufacturing Systems in Industry 4.0*, L. Knapcikova, D. Peraković, M. Perisa, i M. Balog, Ur. Cham: Springer International Publishing, 2022, str. 129–142. doi: 10.1007/978-3-030-90462-3_9.
[35] J. R. C. Nurse, S. Creese, i D. De Roure, „Security Risk Assessment in Internet of Things Systems“, *IT Prof.*, sv. 19, izd. 5, str. 20–26, 2017, doi: 10.1109/MITP.2017.3680959.
[36] „ISO/IEC 13335-1:2004 Information technology — Security techniques — Management of information and communications technology security“. 15. studeni 2004.

[37] „NATIONAL VULNERABILITY DATABASE“. https://nvd.nist.gov/vuln (pristupljeno 03. ožujak 2022.).
[38] „Open Source Vulnerability Database“. https://security.snyk.io/
[39] „Exploit Database“. https://www.exploit-db.com/
[40] „WhiteSource Vulnerability Database“. https://www.whitesourcesoftware.com/vulnerability-database/
[41] „VulDB“. https://vuldb.com/

Popis slika

Popis tablica

Sveučilište u Zagrebu
Fakultet prometnih znanosti
Vukelićeva 4, 10000 Zagreb

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOSTI

Izjavljujem i svojim potpisom potvrđujem da je diplomski rad
(*vrsta rada*)
isključivo rezultat mojega vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju upotrijebljene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedopušten način, odnosno da je prepisan iz necitiranog rada te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog/diplomskog rada pod naslovom Procjena rizika informacijskog sustava temeljenogna konceptu Interneta stvari, u Nacionalni repozitorij završnih i diplomskih radova ZIR.

Student/ica:

U Zagrebu, 28.6.2022.

Petar Zrinski
(ime i prezime, *potpis*)