Informacijski sustav podržan RFID tehnologijom u procesu prodaje i kontrole karata u brodskom putničkom prometu

Information System Supported by RFID Technology in the Process of Sale and Control of the Tickets in Ship's Passenger Traffic

Pančo Ristov
Pomorski fakultet Split
e-mail: panco@pfst.hr

Ante Mrvica
Jadrolinija d.o.o., Rijeka
e-mail: ante.mrvica@jadrolinija.hr

Pavao Komadina
Pomorski fakultet Rijeka
e-mail: komadina@pfri.hr

Vinko Tomas
Pomorski fakultet Rijeka
e-mail: tomas@pfri.hr

DOI 10.17818/NM.1.9.2015
UDK 621.3 : 656.615
Prethodno priopćenje / *Preliminary communication*
Paper accepted / *Rukopis primljen:* 24. 10. 2014.

Sažetak

U ovom radu predložen je podsustav za prodaju i kontrolu putničkih karata u brodskom putničkom prometu. Spomenuti podsustav temeljen je na uporabi RFID tehnologije. Podsustav se može jednostavno integrirati u postojeći integrirani informacijski sustav brodske putničke kompanije ili u integrirani lučki informacijski sustav. Kao prometne karte koriste se pasivni RFID tagovi koji se mogu kupiti u bilo kojoj ovlaštenoj agenciji za prodaju brodskih karata. Kontrola karata vrši se automatski, jednostavnim unošenjem kartice u polje RFID čitača. Kontrola karte traje veoma kratko i omogućava brzi protok putnika i automobila, a to znači i manje gužve u lukama i vezovima. Srž predloženog podsustava je softverska aplikacija koja povezuje sve komponente RFID tehnologije i distribuirana baza podataka. Primjenom RFID tehnologije ubrzava se proces ukrcaja putnika/auta, smanjuju se gužve u luci, eliminira ukrcaj putnika u pogrešnu brodsku liniju te se značajno smanjuje upotreba gotovinskog plaćanja.

KLJUČNE RIJEČI

kartica
RFID čitač
kontrola
informacijski sustav
računalo
vez
putnički brod
luka

Summary

In this paper, we have proposed a subsystem for sale and control of passenger tickets in the ship's passenger traffic. The proposed subsystem is based on the use of RFID technology. The subsystem can be easily integrated into an existing integrated information system of marine travel company or in an integrated port information system. Passive RFID tags which you can purchase at any authorized agency for the sale of ferry tickets are used as traffic ticketsThe control ticket is very short and thus allows rapid flow of passengers and cars, and that means less congestion in ports and docks. The core of the proposed subsystem is a software application that connects all the components of RFID technology and distributed database. The application of RFID technology accelerates the process of boarding passengers / cars, reducing congestion in the port, eliminating the passengers boarding the wrong boat line and significantly reducing the use of cash payments.

KEY WORDS

card
RFID
reader
control
information system
computer
berth
pasenger vessel
port

1. UVOD / *Introduction*

U širem smislu, RFID (*Radio Frequency Identification*) sustavi su svi sustavi koji koriste frekvencijske radio valove za prikupljanje informacija za identifikaciju i praćenje objekata ili osoba. U užem smislu pod RFID sustavom podrazumijevamo sustav koji se sastoji od RFID čitača, antene, sustava za obradu podataka i RFID transponder (***trans****mitter/res****ponder***) - tag koji je nositelj informacija za identifikaciju i praćenje objekta. RFID tehnologija omogućava funkcioniranje sustava bez izravne optičke vidljivosti i po bilo kakvim vremenskim uvjetima kao i istovremeno očitavanje više tagova. Velika raznolikost RFID sustava omogućuje izrazito velik broj primjena, koji s vremenom i tehnološkim napretkom sve brže raste. Ugrađivanje RFID tagova u doslovno sve što okružuje ljude, od donjeg rublja, preko automobila i vlakova, do kućnih ljubimaca pa i u same ljude, obećava brojne pogodnosti i nove dosad neslućene mogućnosti - lagodnije i učinkovitije obavljanje svih svakodnevnih

poslova [1,2]. Prednosti koja pruža RFID tehnologija, posebno sigurnost i jedinstvena identifikacija, sve više imaju primjenu i u pomorskim procesima [3], pa tako i u procesu prodaje i kontrole putničkih karata u brodskom prometu.

Ranih 2000-ih godina počela je primjena RFID tehnologije u lučke procese. Najbolji primjer je PierPass program u Los Angelesu/Long Beach, a zatim je uslijedila implementacija u Južnoj Africi, Finskoj, Georgia SAD, Dubai UAE i drugdje. Osim toga, u ovom razdoblju RFID tehnologija implementira se u logističke procese kontejnerskog prijevoza po američkim vojnim i brodskim linijama, uključujući APL, MATSON i Horizon Lines [12].

RFID tehnologija već se duži niz godina koristi u javnom prijevozu. RFID sustav koji se koristi u Helsinkiju je najveći sustav u Europi i obuhvaća sve vidove javnog prijevoza, pa tako i prijevoz trajektom (kao što je trajekt M/S Suomentlinna II). Norveški brodski operator *Fjord Line* koristi RFID tehnologiju za nadzor i praćenje brodskih karata i pristup kabinama na jednom od svojih trajekata (MS Stavangerfjord) te planira proširiti primjenu RFID tehnologije i na ostale nove trajekte i na druge usluge, kao što su usluge u brodskim restoranima. Implementirani RFID sustav kao brodske karte koriste pasivni tag (13.56MHz) koji je u skladu sa standardom ISO 14443 i ručne RFID čitače na ulazu u trajekt. Osim toga u sve brave brodskih kabina ugrađena je RFID tehnologija. Operator *Fjord Line* u svoj informacijski sustav ima integriranu i softversku podršku za rezervaciju i praćenje brodskih karata za sve svoje trajekte. Na starijim trajektima (*MS Bergen fjord and the Fjord Line Express*) koristi se bar kodom otisnutim na papirnatu brodsku kartu [13]. Informatička tvrtka CARUS osigurava kompletnu softversku i hardversku podršku i implementaciju RFID resursa u informacijski sustav [14].

U većini aplikacija, RFID tehnologija postiže 99,5 % do 100 % očitavanja u prvom skeniranju. Osim toga, bez pokretnih elemenata održavanje RFID resursa je daleko jednostavnije i učinkovitije.

Integracijom RFID tehnologije u integrirane informacijske sustave brodske kompanije ili u lučke informacijske sustave omogućava sigurno praćenje putnika/automobila u realnom vremenu, automatizirani unos podataka, pruža uvid u realno stanje putnika/automobila na svakom brodu, kontrolu karata bez prisustva brodskog časnika, povećanje kapaciteta luke na način da se ubrzaju procesi provjere, nadzora i upravljanja putnicima/autima, smanjenje operativnih troškova, pravovremene i točne informacije o putnicima/automobilima ispred vezova kako bi se planirale potrebe lučkih resursa, povećanje upravljačkih funkcija svih razina upravljanja te optimizaciju brodskog prometa u luci. Tako, integrirani informacijski sustav pruža učinkovitu i neprekidnu razmjenu podataka i informacija između svih subjekata uključenih u integrirano prometni lanac, uz uvjet da se svi učesnici koriste standardiziranim sučeljima i postupcima.

U standardizaciju RFID tehnologije uključene su Međunarodna organizacija za standardizaciju - ISO (*International Organization for Standardization*) i EPC (*Electronic Product Code*) global. EPC global je odgovoran za definiranje specifikacija za sve aspekte RFID tehnologije. Distribucija i kontrola dodjeljivanja EPC brojeva u nadležnosti je međunarodne organizacije GS1 (*Global standard one*) i odgovarajućih nacionalnih GS1 organizacija (kod nas GS1 Hrvatska) [4,5].

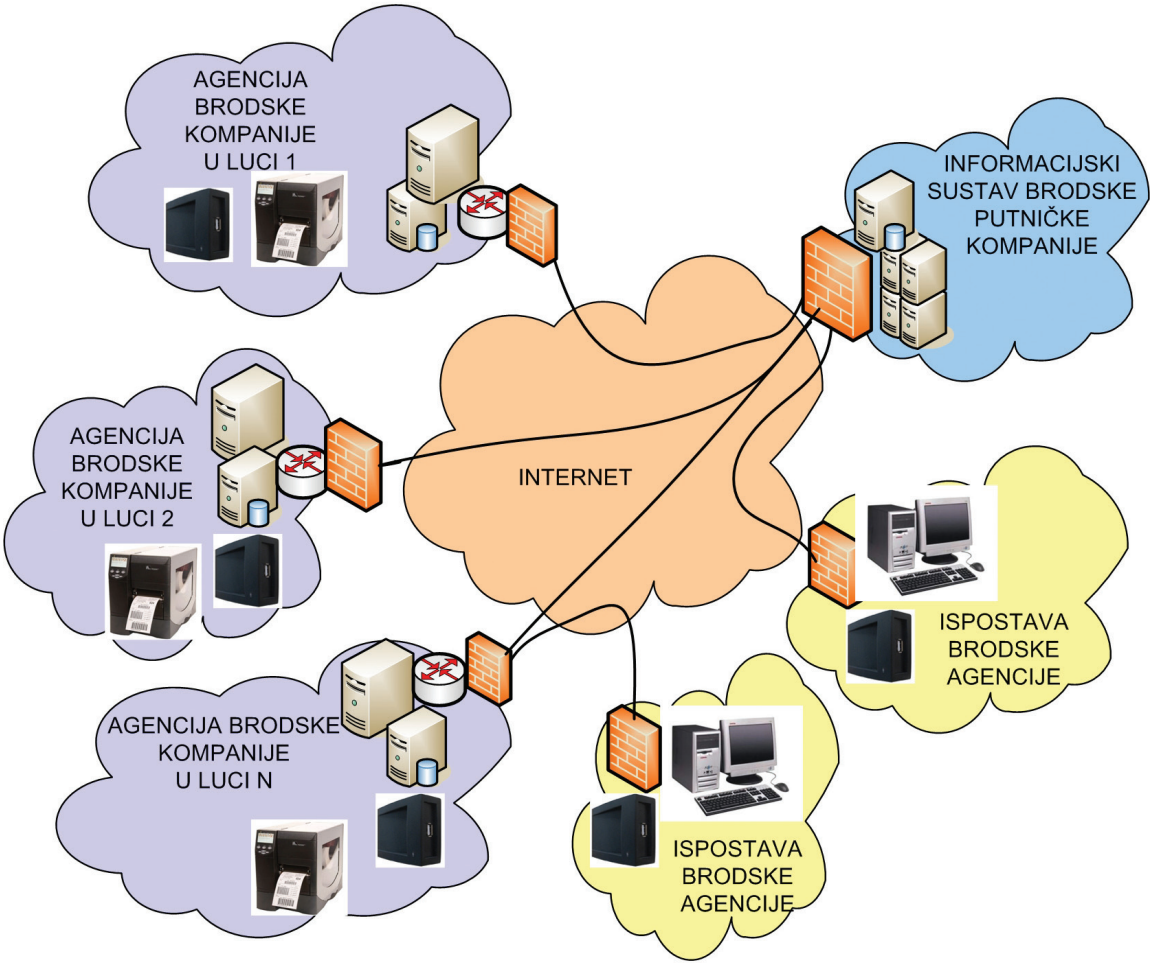
Postojeći sustav prodaje karata u hrvatskim lukama je poluautomatski, odnosno kupnja papirnate karte vrši se u agencijama ili ispostavama agencije, dok se kontrola karata odvija u dva koraka. U prvom se koraku vrši ručna kontrola tijekom ulaska u brod (uzima se kupon karte za brodara, a putniku ostaje dio karte za navedeno putovanje), a drugi korak je poluautomatski tijekom kontrole svake karte. Svaka se karta skenira i prikupljene podatke automatski šalje u ured za kontrolu karata. Pored toga, zaduženi časnik razvrstava karte po putnicima i vozilima (osobna vozila, kombi vozila, kamioni do 3t, kamioni od 3 do 5t, kamioni preko 7t, putnički kombi do 7 putnika, preko 7 putnika i autobus do 30 putnika i više od 30 putnika) te popunjene standardne formulare kompanije šalje u ured za kontrolu karata. Također, obveza broda je da se prikupljeni podaci šalju i Lučkoj kapetaniji – odjel sigurnosti plovidbe. Ovaj je način spor i nepouzdan, posebno u procesu kontrole karata od strane brodskog časnika tijekom ulaska u brod. U praksi je bilo slučajeva kada su se putnici ukrcavali na pogrešne brodske linije pa je brodska kompanija obvezna osigurati putnicima adekvatni smještaj i povratak u luku polaska što zahtijeva dodatne financijske i materijalne gubitke kompanije. Zbog toga je potrebno automatizirati cijeli proces prodaje i kontrole karata, odnosno uvesti RFID tehnologiju.

2. INFORMACIJSKI SUSTAV PODRŽAN RFID TEHNOLOGIJOM / *Information system supported of RFID technology*

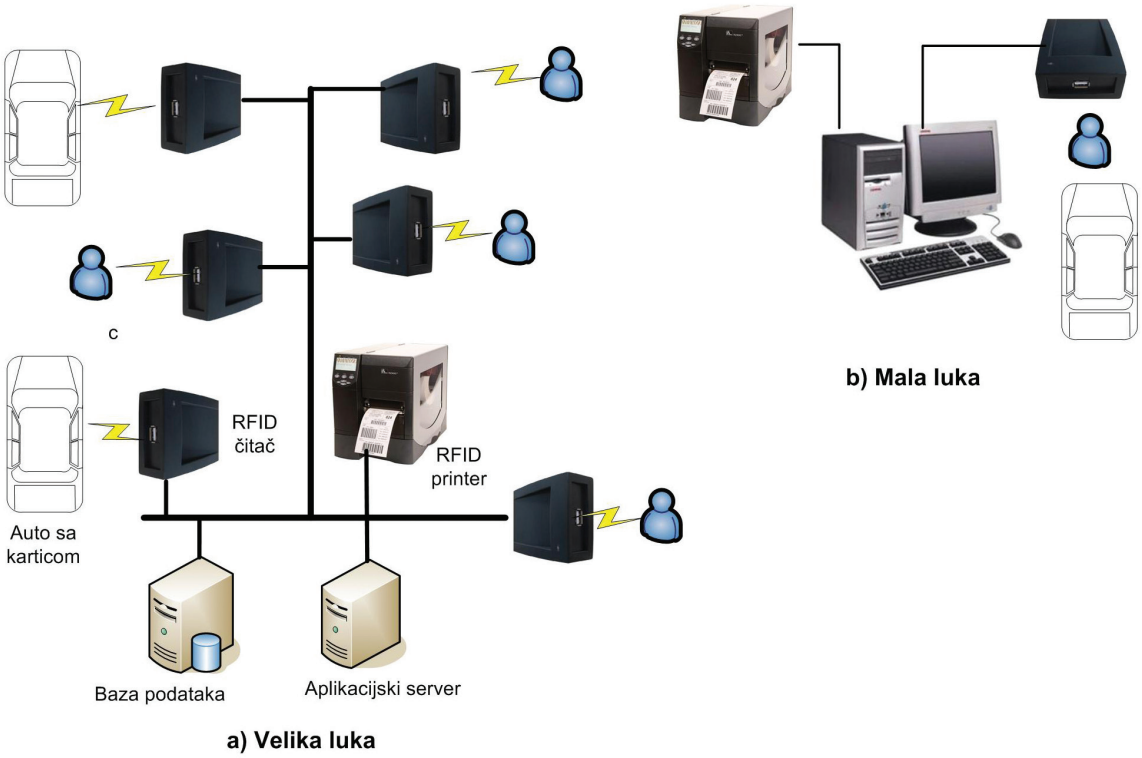
Uprava brodarske kompanije mora raspolagati točnim, pravovremenim, preciznim i pouzdanim informacijama koje omogućuju menadžeru kvalitetno donošenje odluka. Zbog toga suvremena brodarska kompanija mora imati integrirani informacijski sustav (IIS) koji će osigurati dovoljnu količinu informacija te podržati menadžment u modernome poslovanju. Protok informacija treba biti dinamičan i približiti se realnom vremenu, što znači da mora osigurati pravovremenost, kvalitetu obrade, odgovarajući kontrolni mehanizam i kontinuirano praćenje poslovnog procesa.

Dizajn suvremenih IIS-a je modularnog tipa i općenito se mogu podijeliti na različite načine, ovisno o veličini i organizaciji brodarske kompanije [2]. Na slici 1. prikazan je pojednostavljeni model IIS brodske kompanije podržan RFID tehnologijom. Postojeći IIS-ovi brodskih kompanija sadrže podsustav uredskog poslovanja, funkcijske podsustave (financijski, knjigovodstveni, prodaja – internetska prodaja i rezervacija karata i marketing) i podsustav tehničkih resursa. Također, svaka ovlaštena agencija podržana je informacijskim elementima. Kod svih podsustava podaci se unose ručno ili poluautomatski posebno u procesu prodaje i kontrole brodskih karata.

U cilju povećanja sigurnosti i pouzdanosti podataka i informacija svi podsustavi se umrežavaju u VPN (*Virtual Private Network*) mrežu. VPN je tehnologija koja omogućava sigurno povezivanje privatnih mreža u zajedničku VPN kroz javnu mrežnu infrastrukturu. Ostvaruje se siguran „tunel" između krajnjih točka. Kod tuneliranja provodi se kompresija i/ili kriptiranje podataka. VPN mreža može biti implementirana hardverski ili programski. U praksi se često koristi



Slika 1. Model IIS podržan RFID tehnologijom
Figure1 Model IIS supported of RFID technology



Slika 2. Blok shematski prikaz informacijsko-komunikacijskih resursa podržan RFID tehnologijom
Figure 2 Block schematic representation of information and communication resources supported RFID technology

kombinacijom ove dvije implementacije. Dok vrste VPN mreža mogu biti intranet (povezivanje više lokacija unutar jedne organizacije), ekstranet (povezivanje različitih poslovnih partnera i tvrtki) i udaljeni pristup (povezivanje udaljenih korisnika s lokalnom mrežom organizacije). VPN mreža osigurava siguran i zaštićen prijenos podataka, a to podrazumijeva: autentifikaciju (kontrolu pristupa), povjerljivost (enkripciju), integritet (neizmijenjenost podataka) i zaštitu od ponavljanja.

Zahvaljujući korištenju suvremenih informacijsko-komunikacijskih rješenja za povezivanje svih informacijskih resursa u luci u jednu cjelinu (TCP/IP, Ethernet), podsustav može raditi na više vezova istovremeno. Pojednostavljeni model informacijskog podsustava podržan RFID tehnologijom prikazan je na slici 2.

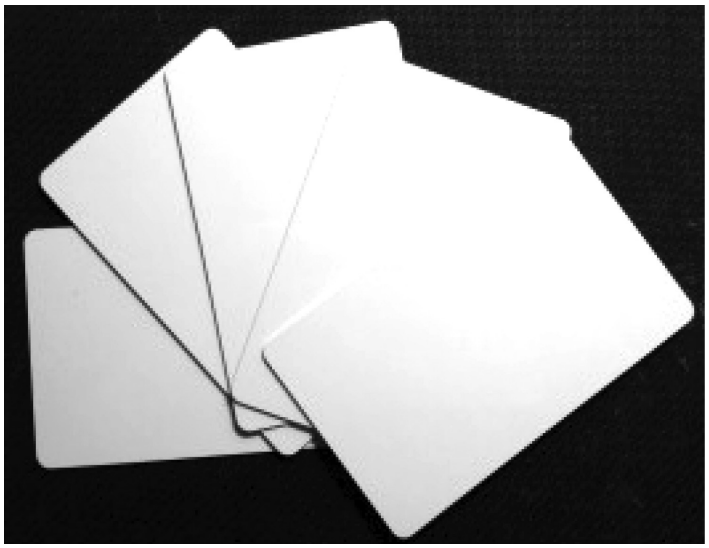
Osnovni dijelovi RFID tehnologije su:

- RFID tag (kartica)
- RFID čitač
- RFID pisač
- Računalo
- Server baze podataka
- Server aplikacije

U lukama s više vezova RFID čitači su spojeni Ethernet mrežom na aplikacijski server i server baze podataka, dok se u malim lukama (agencijske ispostave) implementira osobno računalo sa stacionarnim ili mobilnim čitačem. Na osobnom računalu instaliran je aplikacijski server. Osobno računalo se preko VPN mreže spaja na agencijski server baze podataka. Zbog sigurnosti, brzine rada, pouzdanosti i raspoloživosti usluga u većini aplikacija, server baze podataka i aplikacijski server instalirani su na jednom serveru.

2.1. RFID KARTICA / *RFID ticket*

RFID tag ili kartica (veličine bankovne kartice) je mali čip koji sadrži podatke. Za ovakve sustave koriste se većinom multiaplikacijskim pametnim karticama. Kartica spada u grupu pasivnih RFID tagova, kao što je MIFARE tag koji radi na 13,56 Mhz, vidi sliku 3 [6,7]. U kartici se ugrađuje antikoalizioni algoritam (algoritam protiv sudaranja) koji omogućava komunikaciju RFID čitača s više kartica selektirajući ih jednu po jednu i na taj način podaci se upisuju/čitaju iz baze podataka. Također, antikoalizioni algoritam sprječava očitavanje istih kartica više puta. Sastavni dijelovi kartice su: antena, mikročip, EEPROM memorije i plastično kućište.



Slika 3. RFID kartica (MIFARE)
Figure 3 RFID ticket (MIFARE)

Kapacitet EEPROM (*Electricaly Erasable Programmable Read - Only Memory*) memorije ovisi o količini podataka koji se želi upisati. Kapacitet EEPROM memorije može biti od 1kB do 4kB. Memorija je podijeljena u određeni broj sektora (kartica od 1kB je podijeljena u 16 sektora), a svaki sektor sadrži 4 bloka. Svaki blok ima 16B. Korisnik može definirati različite uvjete pristupa podacima za svaki sektor (obično je to četvrti blok unutar sektora). Multiaplikacijska pametna karta može predstavljati digitalni novac za izravno plaćanje prijevoza i/ili predstavljati vremensku brodsku kartu za određenu brodsku liniju, odnosno plovno područje. Kartica s digitalnim novcem pogodna je za turiste, jer ima mogućnost dopune (produživanje) novcem, kao prepaid račun za mobilne telefone, dok je vremenska kartica (tjedna, mjesečna ili godišnja) pogodna za otočno stanovništvo. Prvi blok prvog sektora rezerviran je za podatke proizvođača (serijski broj kartice).

Korištenjem RFID tagova može se potpuno eliminirati korištenje novca, posebno sitnog, tijekom plaćanja brodske karte. Ovim bi se gužve ispred ovlaštenih agencija smanjile, što je jedan od velikih problema tijekom sezone. Pored toga, ubrzao bi se proces ukrcaja, smanjio broj pomoraca uključenih u proces ukrcaja te broj zaposlenika koji rade u ovlaštenim agencijama, odnosno ispostavama agencija. Za predloženi podsustav potrebno je upisati podatke prikazane u tablici 1.

Prednost korištenja RFID karticom je u tome što korisnik jednu karticu može koristiti više puta odnosno više godina, posebno za turiste koji dolaze svake godine. Također, otočno stanovništvo svoje RFID kartice treba samo produljiti u agenciji ili ispostavi. To se postiže korištenjem uređaja za dopunu (pametni RFID printer) ili u ovlaštenoj brodskoj agenciji. Podatke u kartici može mijenjati samo ovlaštena osoba. Uređaji za dopunu smješteni su na više lokacija u luci i/ili ovlaštenoj agenciji. Istim uređajem može se koristiti i za kupnju nove karte. Kupljena karta ostaje aktivna sve dok se karta ne izbriše iz baze podataka.

Tablica 1.
Table 1

Blok	Naziv polja
1.	Vremenski interval valjanosti
2.	Digitalni novac i vremenski rok važenja
3.	Šifra kompanije
4.	Šifra plovnog područja
5.	Šifra brodske linije i broj veza
6.	Ime i prezime putnika
7.	Registracija automobila
8.	Vrijeme polaska broda
9.	Kontrolno polje – sadrži ključ za pristup svim poljima

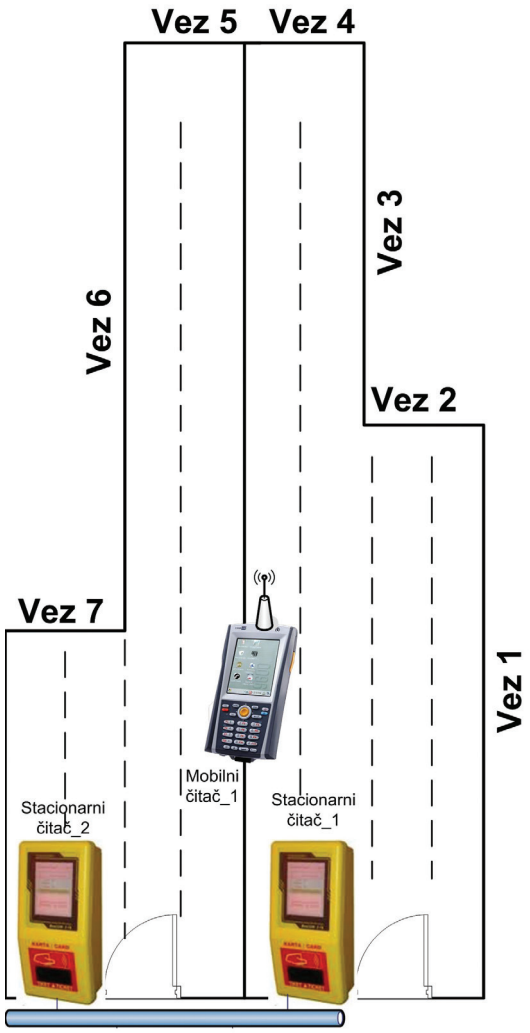
2.2. RFID ČITAČ / *RFID reader*

Drugi element podsustava je RFID čitač. RFID čitač u predloženom podsustavu može biti stacionaran ili mobilan uređaj čiji je zadatak komunikacija s karticom i prijenos podataka do računala gdje

se izvršava daljnja obrada. Arhitektura RFID čitača prilično se razlikuje po kompleksnosti, što ovisi o tipu taga i o funkcijama koje mora obavljati. Također, RFID čitači se mogu proširiti čitačem magnetske trake (stara X-ica) ili barcode zapisa do ekrana za prikaz trenutnih podataka s kartice i prikaz tekstualnih ili grafičkih poruka putniku.

Kao što je prikazano na slici 2., svi RFID čitači su putem mreže (Ethernet protokol) povezani sa serverom baze podataka i aplikacijskim serverom. Osim toga, RFID čitači se mogu povezati bežičnom vezom većeg dometa (WI-FI) i/ili bežičnom vezom manjeg dometa (Bluetooth). Izbor načina povezivanja ovisi o konfiguraciji vezova i postojećoj mreži u luci. Rješenja se mogu kombinirati (bežični i žični uređaji istovremeno u mreži).

Osnovne komponente čitača su: upravljačka jedinica (mikroupravljač), antena i komunikacijsko sučelje (čip MFRC531). Njihova zadaća je komunikacija s karticama i prijenos podataka do računala. U čipu je integriran modulator/demodulator za sve vrste pasivnih kartica. RFID čitač radi na istoj frekvenciji kao i kartice. U mikroupravljaču se nalazi softver čija je glavna uloga da ostvari komunikaciju s komunikacijskim sučeljem i po potrebi komunikaciju na višoj razini (računalo). Komunikacija između čitača i računala odvija se preko komunikacijskog sučelja, a može biti RS-232 i/ili RS485, USB, WiFi i TCP/IP. RFID čitači komuniciraju s pasivnim RFID karticama u trenutku kada se kartica dovoljno približi čitaču, od njega će primati napajanje, što je temeljeno na principu magnetske indukcije. Nije potrebna izravna veza između čitača i kartice. RFID čitač može biti ugrađen u stacionarnu verziju za opsluživanje više vezova, kao što je gat sv. Petra u luci Split ili mobilni kada luka ima jedan, odnosno dva veza, kao što je luka Supetar (otok Brač). Izbor RFID čitača ovisi o organizaciji luke, odnosno o konfiguraciji i broju vezova u luci te o točnoj horizontalnoj i vertikalnoj signalizaciji. Pojednostavljeni blok shematski prikaz vezova i RFID čitača prikazan je na slici 4. Ukoliko se koristi jedan čitač za više vezova, on mora biti stalno uključen kako bi registrirao svakog putnika, odnosno vozilo.



Slika 4. Raspored RFID čitača u luci
Figure 4 Schedule of RFID readers in the port

2.3. RFID PISAČ / *RFID printer*

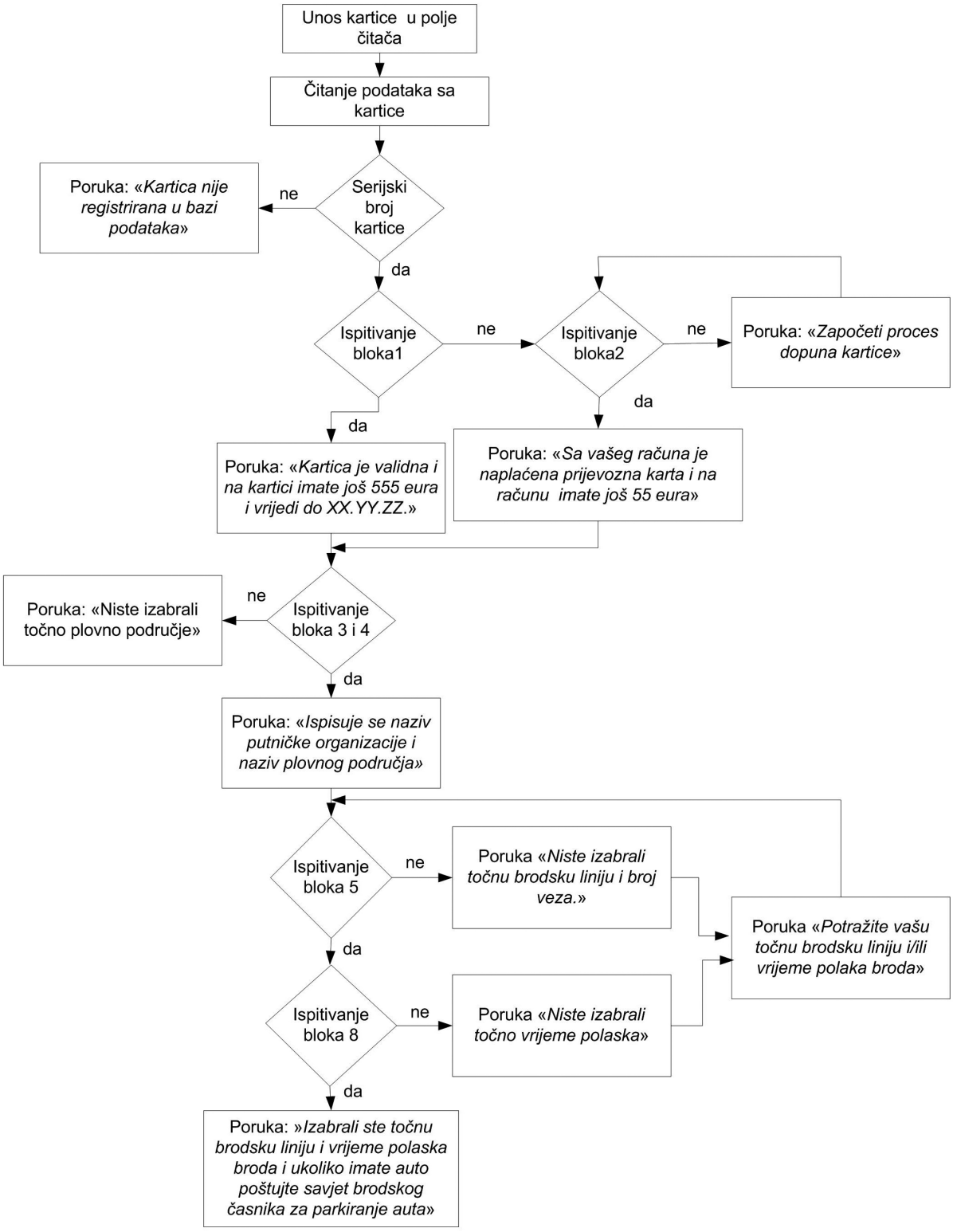
Treći uređaj je pametni RFID printer koji ujedinjuje mogućnosti čitanja, upisivanja i ispisa na RFID kartici. Robustan dizajn omogućava rad u teškim uvjetima i veliku brzinu ispisa. Suvremeni RFID printeri imaju veliki izbor komunikacijskih priključaka (802.11 a/b/g WLAN-a, IEEE 1284 sučelje, Etherneta ili USB-a.). RFID printer može biti instaliran na više lokacija u luci i/ili u ovlaštenoj agenciji, odnosno ispostavi.

2.4. RAČUNALO / *Computer*

Četvrti element je osobno ili industrijsko računalo. Na jedno se računalo može spojiti više RFID čitača, ovisno o organizaciji vezova u luci. Kao što je prikazano na slici 2., osobno računalo (male luke) putem VPN mreže povezuje se sa serverom baze podataka. Na računalu se izvršava aplikacija za obradu podataka s RFID čitača. Aplikacija prihvaća sve podatke s čitača, procesuira ih i u odgovarajućem formatu šalje u bazu podataka. Princip rada aplikacije prikazan je blok dijagramom i algoritmom na slici 5. Tijekom kontrole kartice ispituju se glavni blokovi, i to: serijski broj kartice, digitalni novac i vremenski rok važenja, vremenski interval valjanosti, šifra kompanije, šifra plovnog područja, šifra brodske linije, broj veza i vrijeme polaska broda. Nakon ispitivanja svakoga polja, programska podrška generira tekstualnu poruku kao što je prikazano na blok dijagramu i/ili na grafičkoj poruci. Aplikacija prikupljene podatke obrađuje i u odgovarajući format upisuje u distribuiranu bazu podataka koja je instalirana na računalu.

2.5. DISTRIBUIRANA BAZA PODATAKA / *Distributed database*

Distribuirana baza podataka je baza podataka koja se ne nalazi u cjelini na jednom serveru, već je razdijeljena na više mjesta (agencije) koja su povezana VPN mrežom. Većina je današnjih baza podataka relacijskog tipa i temeljena je na SQL programskom jeziku. Svako čvorište ima svoj vlastiti autonomni sustav za upravljanje bazom podataka. Server baze podataka je temeljen na klijent/server



Slika 5. Dijagram toka kontrole i dopune brodske karte
Figure 5 Flowchart of control and additions boat tickets

konceptu s visoko standardiziranim aplikacijskim sučeljem, definirani standardima SQL-a i standardima komunikacije s bazom podataka. Baza podataka je potrebna kako bi uprava plovnog područja ili uprava kompanije imale uvid u broj putnika i automobila u realnom vremenu na određenoj liniji. Osim toga, uprava kompanije može vršiti procjenu rentabilnosti pojedinog broda, odnosno pojedine brodske linije. Redovita sinkronizacija podataka i informacija osigurava da se osoblje u ispostavama, agencijama i upravi brodske kompanije koristi istim podacima i informacijama.

2.6. APLIKACIJSKI SERVER / *Application server*

U lukama s više vezova svi RFID čitači i pametni RFID printeri spojeni su preko Ethernet protokola na aplikacijski server na kojem se izvršava programska podrška za obradu prikupljenih podataka s čitača. Programska podrška ima modul za kontrolu kartice i modul za dopunu digitalnog novca. Blok dijagram i algoritam rada programske podrške prikazan je na slici 5. Tijekom kontrole kartice ispituju se glavni blokovi, i to: serijski broj kartice, digitalni novac i rok

važenja, vremenski interval valjanosti, šifra kompanije, šifra plovnog područja, šifra brodske linije, broj veza i vrijeme polaska broda. Oba modula generiraju određene tekstualne poruke i/ili grafičke poruke koje su prikazane i u dijagramu tijeka. Izbor sučelja, kao što su dopuna kartice digitalnim novcem, produživanje vremenske kartice (dnevno, tjedno, mjesečno ili godišnje), sučelje za provjeru stanja kartice itd., stvar je zahtjeva korisnika, dizajna i implementacije programske podrške.

Na aplikacijskom serveru izvršava se i aplikacija izvješćivanje - programska podrška koja omogućava kreiranje dinamičkih standardnih ili vlastitih izvješća po različitim kriterijima (brod, brodska linija, plovno područje, vrsta vozila i sl.) te standardne dokumente koji pružaju trenutni pregled stanja pojedinog broda ili flote brodova te pravovremene i točne informacije donositeljima odluka (zapovjedniku broda, koordinatoru plovnog područja te menedžmentu brodske kompanije).

Npr., moguće je dobiti:

- popis posade
- popis putnika
- broj, vrstu i tip automobila
- pojedinačne i zbirne izvještaje o broju putnika i automobila po svakom brodu
- pojedinačne i zbirne izvještaje o broju putnika i automobila po svakom odredištu, ukoliko brod pristaje u više luka
- pojedinačne i zbirne izvještaje o broju putnika i automobila po pojedinačnom plovnom području
- pojedinačne i zbirne izvještaje o broju putnika i automobila na razini brodske kompanije itd.

Svi se podaci i informacije mogu dobiti za određeno razdoblje.

Aplikacija prikupljene podatke procesuira i u odgovarajući format upisuje u bazu podataka. Osoblje u brodskoj kompaniji ima pristup središnjoj bazi podataka u realnom vremenu putem sigurne VPN mreže, bez obzira gdje se nalazi.

3. RANJIVOST I SIGURNOST RFID ELEMENATA INFORMACIJSKOG SUSTAVA / *Vulnerability and safety RFID elements of information system*

U predloženom sustavu osnovni problem je kako zaštititi privatnost i onemogućiti neovlašteno praćenje kada kartica na svaki upit čitača odgovara slanjem informacija koja je upisana u njih. Ovakve informacije mogu neovlaštenom korisniku omogućiti kompromitiranje sustava, odnosno to dovodi do rizika od neovlaštenog pristupa i izmjene podataka u kartici. Drugim riječima, nezaštićene kartice mogu biti ranjive na ometanje radio signala, fizičke napade, neovlaštenu analizu prometa, prisluškivanje, krivotvorenje i podvale [8,10].

Fizički napad na kartice u ovom podsustavu podrazumijeva promjene elektroničkih karakteristika, sondiranje i ometanje signala takta. Kartice ovoga tipa imaju slabu ili nikakvu zaštitu od ovakvih napada. Neovlaštena analiza komunikacije odnosi se na presretanje i analizu informacijskih poruka koje se izmjenjuju između kartice i čitača. Cilj je prikupiti informacije ili identificirati komunikacijske uzorke. Korištenje alata za prikupljanje informacija može se vršiti i kada su poruke kriptirane i nije ih moguće dekriptirati. Općenito, što je veći broj analiziranih poruka moguće je dobiti više informacija.

Grupa istraživača s voditeljem Andrew Tanenbaum s *Amsterdam Free University* napravila je zlonamjerni program (*malware*), prvi program za RFID. Oni su dokazali da, ukoliko postoji propusti u RFID programskoj podršci, lako i jednostavno se RFID tag može zaraziti virusom. Rad sa zaraženim RFID tagom može se proširiti i na bazu podataka koja koristi RFID programsku podršku [11]. Zbog toga, programeri zaduženi za pisanje programske podrške koja podržava RFID tehnologiju moraju implementirati sve sigurnosne mjere i procedure za sprječavanje i širenje virusa.

Jedan od osnovnih koraka pri uspostavi sigurnosne politike je procjena ranjivosti sustava. Sigurnosna ranjivost definira se kao nedostatak koji zlonamjernom korisniku omogućava narušavanje sigurnosti sustava i/ili informacija. Svaka hardverska i softverska komponenta informacijskog sustava sadrži sigurnosne ranjivosti. Na temelju analize stručne i znanstvene literature i nekoliko RFID aplikacija može se zaključiti problem sigurnosti uključuje pitanje lažnih ili nelegitimnih kartica (tagova) i vrlo rijetko čitača. Sigurnosni problemi javljaju se ukoliko podaci na kartici nisu kriptirani i/ili ako su elementi RFID tehnologije bez fizičkog nadzora. Zbog toga su mnoge sigurnosne organizacije razvile vlastite metode za njihovo sustavno praćenje. Svaka metoda uključuje pronalaženje i analizu ranjivosti, obavještavanje proizvođača, suradnju pri otklanjaju te javnu objavu informacija i način rješavanja. Cilj procjene ranjivosti je identifikacija potencijalnih rizika povezanih s različitim aspektima informacijskog sustava, odnosno RFID tehnologije.

Mjere koje se mogu primijeniti kako bi povećali sigurnost i smanjili ranjivosti RFID elemenata su [12]:

- samouništenje – u tag se upisuje jedinstvena zaporka koja se programira tijekom procesa proizvodnje. Tag koji primi poruku s točnom zaporkom automatski i nepovratno deaktivira (njime se koristi za označavanje proizvoda koji se kupuju u prodajnim centrima i pri prolaz kroz kasu se deaktivira tag čime se onemogućava njegovo daljnje praćenje).
- Blokirajući tag – to je pasivni tag koji može simulirati veliki broj običnih tagova i tako blokira rad RFID čitača. Ovaj tag se može iskoristi da onemogući rad RFID čitača, odnosno za napade na RFID sustave.
- kriptografija – korištenjem tagova s mogućnošću višestrukog programiranja moguće je čestim promjenama kriptografskog ključa onemogućiti neovlašteno čitanje i praćenje. U praksi se koriste simetričnom enkripcijom (AES algoritam) te enkripcijom s javnim ključem temeljenim na konceptu *Re-Encryption*.
- korištenje Hash funkcija – u praksi postoje tri funkcije: Hash zaključavanje je sigurnosni sustav kod kojeg svaki tag posjeduje jedinstvenu oznaku (metaID). Dok je zaključan, tag odgovara samo slanjem svoje oznake – metaID i čeka da mu čitač na nju odgovori ključem *k* (metaID = hash(k)). Ključevi su pohranjeni u bazi podataka na računalu (serveru baze podataka) koje je povezano s čitačem. Nasumično hash zaključavanje je proširenje prethodno opisane metode čiji je glavni nedostatak to što omogućava neovlašteno praćenje taga. Ovo podrazumijeva učestale i nepredvidive promjene metaID-a. Kada bi se koristila ova metoda, tagovi bi morali imati hash funkciju i generator pseudo-slučajnih brojeva. Hash-Chain metoda se koristi dvijema ili više hash funkcija ugrađenih

u tag za onemogućavanje fizičkih napada na tagove.

- TBF (*Tree – Based Private*) autorizacija – radi tako što smanjuje opterećenje poslužitelja (kod metoda temeljenih na hash funkcijama) koje je proporcionalno broju tagova.
- PRF (*Pseudo Random Function*) autorizacija – omogućava međusobnu autorizaciju čitača i taga uz osiguranu zaštitu privatnosti taga koji sudjeluje u procesu. Ova metoda koristi zajednički ključ za komunikaciju između taga i čitača.
- Faradayev kavez – osigurava zaštitu privatnost taga tako što se izolira od vanjskih elektromagnetskih utjecaja (spremnik od metalne mreže).
- HB+ autorizacija (Hopper i Blum) – nadogradnja HB protokola. Koristi se simetričomn kriptografskim ključem, pruža zaštitu od aktivnog i pasivnog prisluškivanja. Jednostavnost ove autorizacije čini je primjenjivom i na jeftine tagove.
- Aktivno ometanje – vrši se ometanjem na radnoj frekvenciji RFID sustava čime se u potpunosti onemogućava radio komunikacija i time blokira rad RFID čitača.Alternativa je zaštiti privatnost primjenom Faradayevog kaveza.
- Metode koje se ne koriste enkripcijom – ove metode ostvaruju se se uz pomoć jednostavnih autoriziranih algoritama koji se temelje na odgovaranju na upite (*challenge-response*) i na taj način se provjerava njegova autentičnost. Jedan od pristupa je da se u tag pohranjuje lista znakova. Na svaki upit tag odgovara sljedećim znakom s liste te se na temelju takvog niza provodi njegova identifikacija.
- Odvajanje EPC koda od bilo koje osjetljive informacije po kompaniji ili kupcu.
- Korištenje tagova s mogućnošću višestrukog programiranja samo tamo gdje je prikladno i gdje postoji dodatni sustavi zaštite.
- RFID čitači trebaju zahtijevati odgovarajuću potvrdu ovlaštenja ili dozvolu kako bi omogućili pristup svim servisima.
- Ako je mreža temeljena na internetu, moraju se osigurati vatrozid i mehanizmi otkrivanja neovlaštenog upada u sustav. Ovi mehanizmi mogu se implementirati na jednom računalu (*Host Intrusion Detection System*), cjelokupnoj mreži (*Network Intrusion Detection System*) i mješoviti mehanizam.

Cjelovit i kvalitetan program sigurnosti omogućava uspostavu sigurnosti na svim kritičnim točkama informacijskih sustava u brodskoj organizaciji, a jedan od najboljih programa zasigurno je definiranje sigurnosne politike. Sigurnosna politika je dinamički dokument kojeg treba stalno pregledavati, mijenjati i nadopunjavati kada se za to pruži prilika. Sigurnosnom politikom definirana su pravila koja se odnose na: svu informacijsku opremu, osobe odgovorne za posluživanje i održavanje informacijskog sustava, sve osobe koje imaju pravo pristupa i vanjske suradnike koje imaju pravo pristupa.

4. ZAKLJUČAK / *Conclusion*

Mogućnost primjene informacijsko-komunikacijske tehnologije pri upravljanju, nadzoru i praćenju putnika i automobila u lukama su izuzetno velike, što se može vidjeti u svim velikim domaćim i svjetskim lukama. Zbog toga se stalno nastoji usavršavati postojeće IIS-ove i primjenjivati nove tehnologije. Najnovija tehnologija je RFID tehnologija

U ovom radu predložen je podsustav za automatizaciju procesa kontrole brodskih karata temeljen na RFID tehnologiji koja se može implementirati u postojeće IIS brodske putničke organizacije ili u lučki IIS i na taj način poboljšati učinkovitost, pouzdanost i raspoloživost resursa organizacije. Kontrola brodskih karata izvršava se automatski i traje veoma kratko (90-100ms) što omogućava brzi protok putnika/automobila te nema potrebe za angažiranje većeg broja pomoraca. Kao prijevozna brodska karta predloženo je korištenje pasivnog taga. Dan je opis MIFARE taga s memorijskim kapacitetom od 1kB i prijedlog koji se podaci trebaju upisati te blok dijagram i algoritam validacije.

Prednost korištenja RFID tehnologije u odnosu prema drugim tehnologijama su: prilagodljivost uvjetima rada (vlaga, nečistoća, visoke temperature, mehanička otpornost), dugi životni vijek (standardi propisuju 10-godišnje trajanje RFID medija s min. 100000 očitanja), zaštita podataka na kartici, sve povoljnija cijena RFID elemenata itd.

Uz pomoć RFID tehnologije putnike/automobile moguće je pratiti uz minimalnu ljudsku intervenciju. Ovo potencijalno može utjecati na ubrzanje svih procesa, smanjenje operativnih troškova i transparentnost od početka do kraja putovanja u realnom vremenu, povećanje sigurnosti putnika i automobila te učinkovito, sigurno i pouzdano rukovanje podacima.

Ranjivost standardnih hardverskih i programskih komponenti ujedno je postala i ranjivost elemenata RFID tehnologije. Zbog toga su sigurnosna rješenja informatičke industrije potpuno jednaka. Uspostavljanje i održavanje sustava upravljanja sigurnosti informacijskih sustava osigurava uvjete za kontinuirano, učinkovito i djelotvorno upravljanje te stjecanje financijske dobiti brodarske organizacije.

LITERATURA / *References*

[1] Ristov, P., Mrvica, A., „Primjena RFID tehnologije u pomorstvu", Proceeding of 3th International Maritime Science Conference (ISSN 1847 1498),Split, 2011.

[2] Ristov, P., Mrvica, A. ,"Pomorski integrirani informacijski sustavi", knjiga, PFST, 2014.

[3] Ristov, P., „Primjena RFID tehnologije na brodu i u lučkim kontejnerski terminalima", 1. RFID konferencija, Zagreb - 2014, nastupno predavanje.

[4] http://www.gs1.org/epcglobal/

[5] http://www.gs1hr.org/djelatnosti/prikupljanje/rfid

[6] http://www.nxp.com/products/identification_and_security/smart_card_ics/mifare_smart_card_ics/ (dostupno 30.08.2014)

[7] http://www.daidaatdei.com/mz/mifare-s50-1k/68-nfc-thin-smart-card-tag-tags-mifare-1k-s50-ic-1356mhz-read-write-rfid-android.html

[8] CARNet, CCERT-PUBDOC-2007-01-179, „RFID identifikacija", Revizija v1.1

[9] Hansen, G., „RFID for Optimization of Business Processes", Wiley, 2008.

[10] The Government of the Hong Kong Special Administrative Region,„RFID security", February 2008.

[11] http://www.rfidvirus.org/media/theregister.com.pdf.

[12] Zhang, Y., Kitsos, P., "Security in RFID and Sensor Networks" Auerbach Publications.

[13] PEMA, „ RFID in ports and terminals", 3 Pretoria Road, London E4 7HA, UK.

[14] Swedberg, C., Fjord Line Puts RFID Aboard Ferry" RFID Jurnal, 2013, http:// www.rfidjournal.com/articles/

[15] http://www.carus.com/2015/01/08/worlds-longest-ferry-route-operator-chooses-carus/

[16] Finkenzeller, K.,„RFID Handbook: Fundamentals and Application in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication, Third Edition, Wiley, 2010.

[17] Juels, A., "RFID security and privacy: a research survey", IEEE Journal on Selected Areas in Communications, Vol.24, Is.2. Feb. 2006, pp: 381- 394.

[18] "Beligian Group Report on Two Yea NFC Voucher Study", Near Field Communication World, March 8, 2011.

[19] Banks, J., Hanny, D., Manual A. Pachano, Les G., Thompson, "RFID applied", New Jersey, 2007.

[20] Juels, A., "RFID security and privacy: a research survey", IEEE Journal on Selected Areas in Communications, Vol.24, Is.2. Feb. 2006, pp: 381- 394.

[22] "Common RFID Implementation Issues: 10 Considerations for Deployment", white paper, www.alientechnology.com