

RFID

Radio Frequency Identification

Contents

1	Zgodovina	3
2	Osnove	4
2.1	Prednosti RFID	4
2.2	Slabosti RFID	4
2.3	Delovanje	5
2.4	Vrste sistemov/značk	5
2.4.1	Vrste značk glede na napajanje	5
2.5	Vrste sistemov glede na kombinacijo čitalec-značka	5
2.6	Vrste sistemov glede na frekvenco	6
2.7	Komunikacija med čitalcem in značko	6
2.7.1	Kolizije	6
2.8	Primeri uporabe	7
2.9	Varnost	8
3	Protokol	8
3.1	Komunikacija	9
3.1.1	PIE Kodiranje	9
3.1.2	ALOHA	11
3.1.3	Ukazi in odgovori	12
3.1.4	Ukazi za izbiranje skupin značk	14
3.1.5	Napake	14
3.1.6	Manchester kodiranje	15
3.2	Shramba	15
4	Zaključek	16
5	Viri	17

1 Zgodovina

Leta 1945 je Léon Theremin za Sovjetsko zvezo izumil "the Thing", prisluškovalno napravo brez vgrajene baterije (pasivna).

To napravo so skrili v rezbarski ornament in ga podarili ameriški ambasadi. V bližnjo stavbo so namestili radijski oddajnik, ki je oddajal radijske valove proti napravi.

Zvočni valovi pogovorov v ameriški ambasadi so vibrirali diafragmo v napravi, kar je posledično povzročilo modulacijo oddanega radijskega valova oddajne naprave in s tem prenos pogovorov ruskim radijskim sprejemnikom.

Čeprav je bila ta naprava prikrita prisluškovalna naprava in ne identifikacijska značka, se lahko šteje za predhodnico RFID, ker so jo napajali in aktivirali valovi iz zunanjega vira.

Prvi pravi primer RFID tehnologije je bil predstavljen leta 1973. Naprava je bila pasivna (napajali so jo zunanji radijski valovi) in je vsebovala transponder ter 16 bitni spomin.



Figure 1: The thing

2 Osnove

RFID je tehnologija, ki uporablja radijske valove za identifikacijo in sledenje predmetov.

RFID sistem uporablja značke (tags) pritrjene na predmete ter radijski oddajnik/sprejemnik, imenovan čitalec (reader), ki pošlje signal znački (jo aktivira) in prebere njen odgovor. Ta odgovor lahko nato posreduje drugi napravi za nadaljno obdelavo.

Sestavni deli značke:

- mikrokrmilnik (integrirano vezje, ki shranjuje in obdeluje informacije ter modulira in demodulira radiofrekvenčne (RF) signale)
- antena, ki se uporablja za sprejemanje in oddajanje radijskih signalov
- baterija (samo v aktivnih značkah)
- obstojni pomnilnik za shranjevanje podatkov

2.1 Prednosti RFID

RFID ima številne prednosti pred tradicionalnimi sistemi identifikacije in sledenja.

- čitalec lahko značke bere na daljavo
- ni potrebno, da je značka v vidnem polju čitalca
- značke lahko hranijo velike količine informacij (več kB)
- omogoča zelo hitro in natančno branje večjih količin podatkov
- so odporne na zunanje dejavnike

2.2 Slabosti RFID

- ena glavnih je zasebnost, saj je lahko značka prebrana brez privolitve nosilca
- RFID tehnologija potrebuje precejšnjo investicijo v potrebno strojno in programsko opremo

2.3 Delovanje

RFID značka se aktivira, ko pride v doseg RFID čitalca:

1. Čitalec odda radijski signal
2. Antena značke ta signal sprejme
 - a. Značka lahko ta signal uporabi za napajanje mikrokrmilnika (pasivna značka)
3. Mikrokrmilnik značke pošlje podatke shranjene na znački preko antene kot odgovor (v obliki radijskega signala) čitalcu

RFID značka sprejme sporočilo in se nato odzove s svojimi podatki.

Te podatki so lahko edinstvena serijska številka značke ali pa informacije povezane z izdelkom, kot so, datum proizvodnje itd. . .

Ker imajo značke unikatne serijske številke, lahko RFID sistem razlikuje med več značkami, ki so istočasno v dosegu čitalnika in s tem bere podatki z vseh značk hkrati.

2.4 Vrste sistemov/značk

2.4.1 Vrste značk glede na napajanje

1. Pasivne
Za napajanje uporabljajo radijski signal čitalca. So manjše in cenejše, a za aktivacijo potrebujejo približno tisočkrat močnejši signal.
2. Delno pasivne
Imajo vgrajeno baterijo in se aktivirajo, ko zaznajo prisotnost čitalca.
3. Aktivne
Imajo vgrajeno baterijo in periodično oddajajo svoj ID preko radijskega signala.

2.5 Vrste sistemov glede na kombinacijo čitalec-značka

- Pasivni čitalec aktivna značka (PRAT)
 - čitalec samo sprejema radijske signale, ki jih značka periodično oddaja
 - uporablja se za varovanje in nadzor sredstev
- Aktivni čitalec pasivna značka (ARPT)
- Aktivni čitalec aktivna značka (ARAT)

Fiksni čitalniki ustvarijo specifično območje branja, ki ga je mogoče strogo nadzorovati. To omogoča visoko definirano območje branja, ko značke vstopijo in izstopijo iz območja branja.

Mobilni čitalniki so lahko ročni ali nameščeni na vozičkih/vozilih.

2.6 Vrste sistemov glede na frekvenco

RFID ločimo tudi glede na frekvenco signala:

- Nizko frekvenčne
 - Razpon: 120 – 150 kHz
 - Doseg: 10 cm
 - Prenosna hitrost: nizka
- Visoko frekvenčne
 - Razpon: 13.56 MHz
 - Doseg: 0.1 – 1 m
 - Prenosna hitrost: nizka/srednja
- Ultra visoko frekvenčne
 - Razpon: 865 – 928 MHz
 - Doseg: 1 – 12 m
 - Prenosna hitrost: srednja/visoka

2.7 Komunikacija med čitalcem in značko

Značka ima lahko ločen oddajnik in sprejemnik. To pomeni, da značka lahko odgovori z signalom drugačne frekvence, kot je bil signal čitalca.

EPC (Electronic Product Code) je trenutni standard, ki se uporablja za enlično identifikacijo značke in produkta na globalnem nivoju.

Sestava EPC po bitih:

- 8: glava, ki označuje verzijo protokola
- 28: identifikacijska številka organizacije (dodeli EPC Global consortium), ki upravlja s podatki značke
- 24: skupina produkta
- 36: serijska številka značke

2.7.1 Kolizije

Pogosto se več kot ena značka odzove na čitalec oznak. Zaznavanje kolizij oz. trkov je pomembno za omogočanje branja podatkov.

Za izolacijo določene oznake se uporabljata dva različna protokola, ki omogočata branje podatkov značke tudi, če se nahaja v bližini drugih značk.

Aloha s časovnimi rezinami

Časovno okno komunikacije razdelimo na enako velike časovne rezine (npr. 1 sekunda).

Naprave lahko pričnejo oddajo podatkov le ob začetku vsake časovne rezine. V primeru hkratnega oddajanja dveh ali več naprav se zgodi kolizija in mora vsaka naprava počakati naključno število časovnih rezin pred ponovno oddajo.

Čitalec pošlje inicializacijski signal in parameter. Značke s pomočjo parametra izračunajo naključno število.

Protokol prilagodljivega binarnega drevesa

Čitalec pošlje inicializacijski signal in nato posreduje po en bit ID značke naenkrat. Odzivajo se le značke z ujemajočimi biti. Ščasnoma se samo ena značka ujema s celotnim nizom ID-ja.

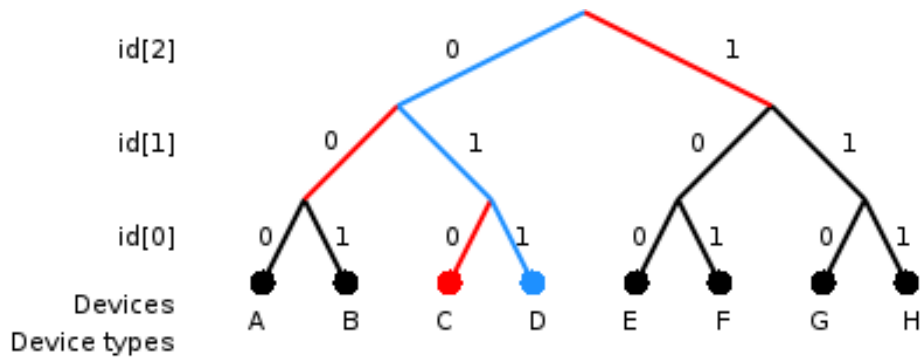


Figure 2: Primer izogibanja koliziji z binarnim drevesom

2.8 Primeri uporabe

- omgočajo učinkovito vodenje sredstev (zaloga, vrsta produkta)
- zaščita proti kraji v trgovinah in skladiščih
- kontrola dostopa v zavarovanih območjih
- identifikacija živali
- vodenje knjižnic

2.9 Varnost

Glavna varnostna skrb RFID tehnologije je nedovoljeno sledenje in branje podatkov na značkah.

Za varnost lahko poskrbimo na 2 načina:

1. Uporabimo RFID, ki deluje na krajše razdalje za visoko rizične dokumente (potni list, plačilne kartice). Z uporabo nizkofrekvenčnih značk je verjetnost za “skimming” (nedovoljeno branje z značke) manjša. Kljub temu pa je bilo dokazano, da je še vedno možno prebrati nizkofrekvenčne značke tudi na razdaljah več metrov.
2. Uporabimo kriptografski pristop:
 - a. Cover-coding: Značka generira naključno število. Čitalec uporabi to število za enkripcijo vseh nadaljnjih sporočil, ki jih pošlje znački.
 - b. Rolling code: Čitalec in značka za vsako poslano sporočilo dogovorita za nov šifrirni ključ.

3 Protokol

Iz standarda ISO/IEC 18000 (Information technology — Radio frequency identification for item management), specifično 6. del (komunikacija na UHF).

Za druge frekvence je standard podoben, z manjšo/večjo zmogljivostjo. Poleg tega standarda, mora vsaka naprava tudi slediti lokalnim standardom uporabljanja frekvenc.

Standard podpira dve vrsti naprav:

- Vrsta A - uporablja Pulse interval encoding (PIE) in ALOHA algoritem za preprečitev kolizij (tem se bomo tukaj bolj posvetili)
- Vrsta B - uporablja Manchester encoding in binary tree collision za preprečitev kolizij

3.1 Komunikacija

3.1.1 PIE Kodiranje

Pulse Interval Encoding (Impulzno Intervalno Kodiranje) deluje tako, da izmeri čas med 2 negativnima frontama. Ta čas določi podatek ('1' ali '0').

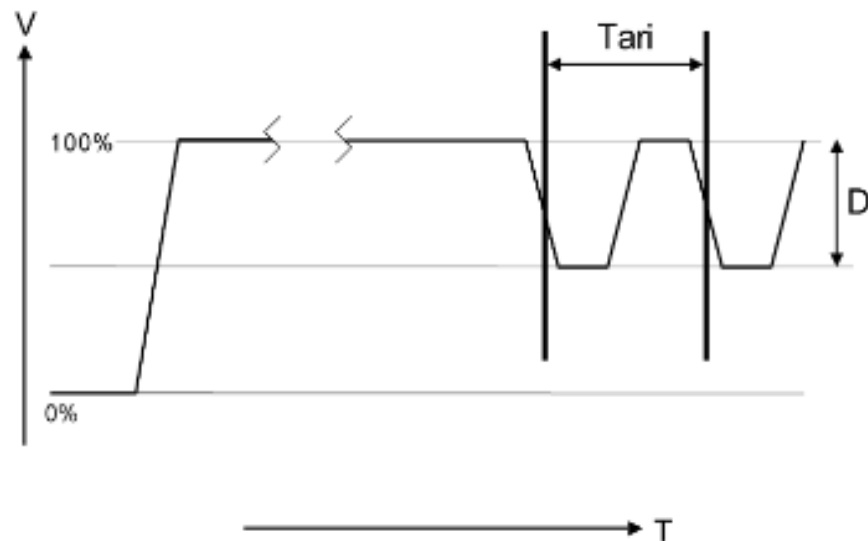


Figure 3: PIE - Dolžina 1 T_{ari}

T_{ari} predstavlja čas med 2 negativnima frontama pri vrednosti '0'. Za predstavitev '1' se pogosto uporablja signal dolžine 2 T_{ari} . SOF (Start of frame) je predstavljen z 1 T_{ari} + 3 T_{ari} . EOF (End of frame) je predstavljen z 4 T_{ari} .

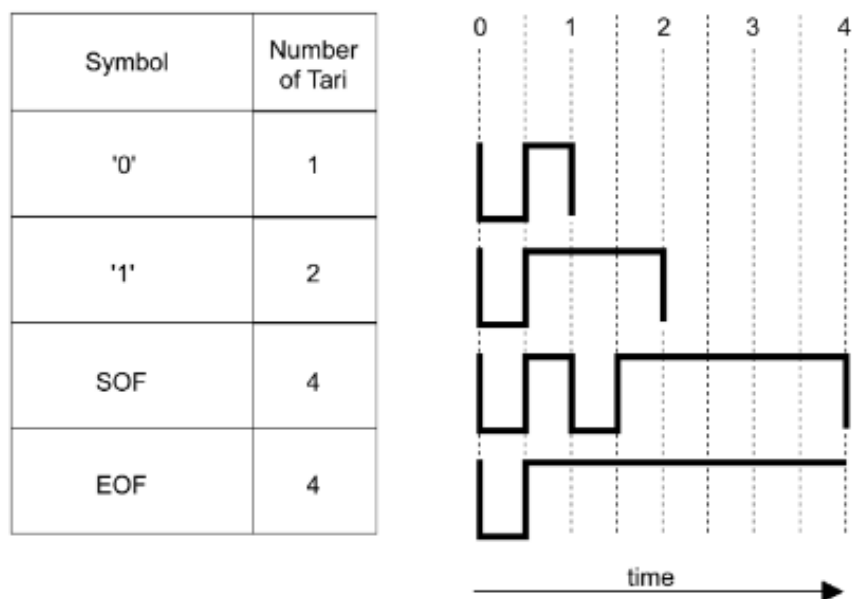


Figure 4: PIE - Simboli

Ko značka bere te vrednosti, moramo imeti nekaj tolerance za motnje pri prenosu. Vrednosti Tari na znački se kalibrira pri SOF.

Table 14 — Pie symbols, decoding

Symbol	Mean duration	Limits
0	1 Tari	$1/2 \text{ Tari} < '0' \leq 3/2 \text{ Tari}$
1	2 Tari	$3/2 \text{ Tari} < '1' \leq 5/2 \text{ Tari}$
SOF	1 Tari followed by 3 Tari	Calibration sequence
EOF	4 Tari	$\geq 4 \text{ Tari}$

Figure 5: PIE - Zaznavanje vrednosti na znački

Pred začetkom pošiljanja mora čitalec poskrbeti, da je preteklen določen čas tišine ($300\mu\text{s}$).

Po poslanem EOF, mora čitalec ohraniti enakomern signal, da je značka napajana za njen odgovor.

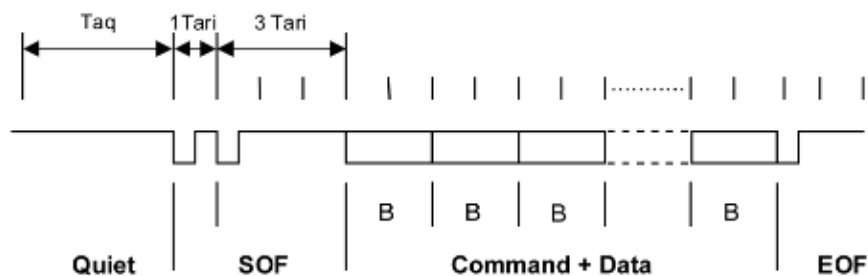


Figure 6: PIE - Pošiljanje ukaza

3.1.2 ALOHA

Za preprečevanje kolizij se uporablja ALOHA protokol.

RFID uporablja protokol ALOHA, tako da značke razdeli v kroge. Ko prvič pride do kolizije, morajo vse značke, ki so sodelovale v prejšnjem krogu pošiljanja pognati svoj naključni generator števil. Vrednost, ki je bila generirana, znački pove v katerem krogu naj začne pošiljati podatke, pri čemer vrednost 0 pomeni naslednji krog.

Če v naslednjem krogu ponovno pride do kolizije, morajo vse značke, ki niso sodelovale v pošiljanju svoj krog povečati za 1. Vse značke ki pa so sodelovale v pošiljanju ponovno poženejo svoj generator števil in dobijo nov krog.

Vsaka značka na začetku komunikacije tudi generira svoj podpis, ki se kasneje uporablja pri komunikaciji z čitalnikom. Značka na začetku komunikacije svoj podpis posreduje čitalniku, ta pa mora v vse naslednje pakete, ki so namenjeni tej znački vključiti njen podpis. Značka vse pakete, ki ne vsebujejo njenega podpisa ignorira, saj misli, da niso namenjeni njej.

3.1.3 Ukazi in odgovori

Protokol deluje, na principu čitalec govori prvi. To pomeni, da značka ne odgovori, dokler ne prejme pravilno dekodiranega ukaza.

Značka je v resnici končni stroj:

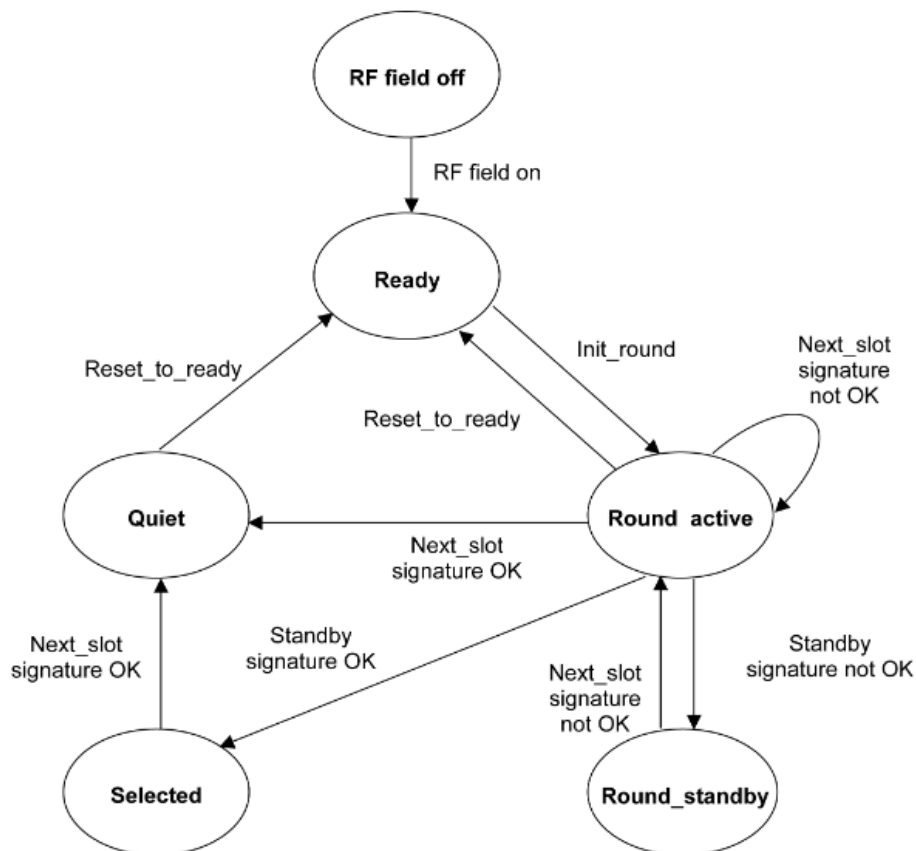


Figure 7: Končni stroj značke

RF Field off state pomeni, da značka ne dobiva napajanja.

Ready state pomeni, da značka dobiva dovolj napajanja za pravilno delovanje.

Quiet state pomeni, da bo značka odgovorila na vse ukaze z njenim podpisom, ne bo pa odgovarjala na ukaze brez podpisov.

Selected state pomeni, da značka odgovarja tudi na ukaze, ki ne vsebujejo katerega koli podpisa.

Round active state pomeni, da značka sodeluje v naslednjem poskusu pošiljanja (ALOHA).

Round standby state pomeni, da značka ne sodeluje v naslednjem poskusu

pošiljanja (ALOHA).

Ukazi in odgovori se izmenjujejo v obliki okvirjev.
Oblika ukaza:

SOF	RFU	Command code	Parameters or flags	CRC-5	SUID (optional)	Data	Data (optional)	CRC-16	EOF
	1 bit	6 bits	4 bits	5 bits	40 bits	8 bits	8 to n	16 bits	

Figure 8: Oblika okvirja pri ukazu

Če ukaz vsebuje SUID zastavico, mora značka primerjati svoj podpis, s tistim, ki ga je poslal čitalec in odgovori le v primeru, da se ta ujema. Če ukaz ne vsebuje SUID zastavice, na ta ukaz odgovorijo vse značke, ki so v izbranem stanju.

RFU - Reserved for future use

Ukazi se delijo na 4 različne skupine:

1. Mandatory - obvezni ukazi
2. Optional - neobvezni ukazi (ob nepodpiranju ukaza, značka odgovori z napako "command not supported")
3. Custom - ukazi, ki jih definira proizvajalec in so odprti za uporabnike
4. Proprietary - ukazi, ki jih uporablja proizvajalec za testiranje, ni nujno da so odprte za uporabnike

Čitalec mora podpirati vse obvezne in neobvezne ukaze.

Primeri ukazov:

- Init_round
- Next_slot
- Close_slot
- Standby_round
- Read_block
- Get_system_information
- Write_block
- Write_multiple_blocks
- Lock_blocks
- Get_block_lock_status

3.1.4 Ukazi za izbiranje skupin značk

Za to se uporabljata ukaza `GROUP_SELECT` in `GROUP_UNSELECT`.

Obema ukazoma dodamo tudi primerjalno pripono: EQ, NE, GT, LT.

Značka, ki zadostuje pogoju odgovori s svojim UID.

Primerja se lahko katerakoli vrednost, za katero vemo na katerem naslovu se nahaja.

3.1.5 Napake

Oblika paketa z sporočilom o napaki:

Preamble	Flags	Error code	Terminator
	2 bits	Optional 4 bits See Table 27	'0' 1 bit

Figure 9: Oblika okvirja pri odgovoru

Vrste napak:

Code	Description
'0'	RFU
'1'	The command is not supported, i.e. the command code is not recognised
'2'	The command is not recognised, for example: a format error occurred
'3'	The specified block is not available (does not exist)
'4'	The specified block is locked and its content cannot be changed
'5'	The specified block was not successfully programmed and/or locked
'6' – 'A'	RFU
'B'-'E'	Custom command error codes
'F'	Error with no information given or a specific error code is not supported.

Figure 10: Vrste napak

Čitalec mora tudi poslati odgovor o uspešno prejetem sporočilu iz strani značke.

3.1.6 Manchester kodiranje

V manchester kodirnanju se za predstavitev vrednosti uporabljajo prehodi med stanji.

Vrednost	Prehod
1	High to Low
0	Low to High

Table 1: Tabela vrednosti v Manchester kodiranju

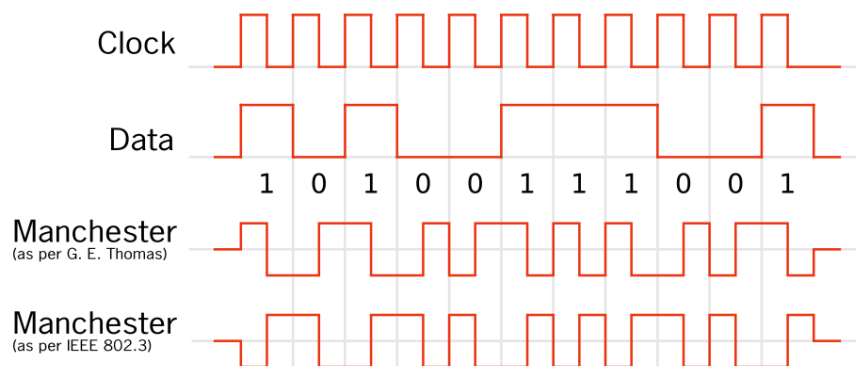


Figure 11: Manchester kodiranje

3.2 Shramba

Protokol dovoljuje do 256 blokov podatkov, kjer je vsak blok velikosti do 256 bitov (skupaj 64kBits). Kasnejše iteracije tega standarda dovoljujejo razširitev te shrambe.

Vsak blok podatkov je lahko zaključen uporabniško ali tovarniško. Uporabniško zaklenjene bloke je mogoče odkleniti z uporabniško določenim geslom, medtem ko tovarniško zaklenjenih blokov ni mogoče odkleniti.

4 Zaključek

RFID je zmogljiva tehnologija, ki ima številne primere uporabe v različnih panogah. Ponuja številne prednosti pred tradicionalnimi sistemi identifikacije in sledenja, kot so branje na daljavo, hiter in natančen zajem podatkov ter odpornost. Vendar pa ima tudi nekaj pomanjkljivosti, kot so pomisleki glede zasebnosti in varnosti ter visoki stroški implementacije. Kot pri vsaki tehnologiji je tudi pri RFID pomembno pretehtati prednosti in slabosti ter oceniti, ali je prava rešitev za določen primer uporabe.

5 Viri

- [1] Avery Dennison. *RFID basics*. Youtube. URL: <https://youtu.be/um8HZ1PED-k>. (accessed: 22.03.2023).
- [2] ALL ABOUT ELECTRONICS. *What is RFID? How RFID works? RFID Explained in Detail*. Youtube. URL: <https://youtu.be/Ukfpq71BoMo>. (accessed: 22.03.2023).
- [3] ISO/IEC. *18000-6 Information technology — Radio frequency identification for item management - Part 6: Parameters for air interface communications at 860 MHz to 960 MHz*. ISO/IEC.
- [4] MAHSA University. *Introduction of Radio Frequency Identification (RFID) Technology in New Era*. Youtube. URL: https://www.youtube.com/live/I7Q_nxuYBI?feature=share. (accessed: 22.03.2023).
- [5] Wikipedia. *Anti-theft system*. Wikipedia. URL: https://en.wikipedia.org/wiki/Anti-theft_system. (accessed: 26.03.2023).
- [6] Wikipedia. *Automatic identification and data capture (AIDC)*. Wikipedia. URL: https://en.wikipedia.org/wiki/Automatic_identification_and_data_capture. (accessed: 26.03.2023).
- [7] Wikipedia. *NFC*. Wikipedia. URL: https://en.wikipedia.org/wiki/Near-field_communication. (accessed: 26.03.2023).
- [8] Wikipedia. *Radio-frequency identification*. Wikipedia. URL: https://en.wikipedia.org/wiki/Radio-frequency_identification. (accessed: 22.03.2023).