Využití RFID při vyčítání informací o zboží

Use of RFID for reading information about goods

Vlastimil Bělíček

Bakalářská práce
2012

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2011/2012

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Vlastimil BĚLÍČEK**
Osobní číslo:	**A08667**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Využití RFID při vyčítání informací o zboží.**

Zásady pro vypracování:

1. **Prostudujte doporučenou literaturu a další informační zdroje.**
2. **Vypracujte literární rešerši na dané téma.**
3. **Srovnejte použití RFID s jinými typy vyčítání informací a porovnejte výhody a nevýhody.**
4. **Vytvořte návrh optimálního systému vyčítání informací, umístění čteček i kódů RFI.**
5. **Zaměřte se na zabezpečení proti zneužití a vyřazení z provozu.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **GLOVER, Bill; BHATT, Himamsu. RFID essentials [online]. Beijing: O'Reilly, [cit. 2012-02-01]. 260 s.**
2. **WANT, Roy. RFID explained : a primer on radio frequency identification technologies. 1st ed. San Rafael, Calif. : Morgan & Claypool, 2006. 83 s. ISBN 1-59829-108-4.**
3. **BROWN, Dennis E. RFID implementation. New York : McGraw-Hill, 2007. 466 s. ISBN 0-07-226324-5**
4. **RANASINGHE, Damith C; SHENG, Quan Z; ZEADALLY, Sherali. Unique radio innovation for the 21st century : building scalable and global RFID networks. Berlin: Springer, 2010. 459 s. ISBN 978-3-642-03462-6**

Vedoucí bakalářské práce: **Ing. Jiří Pálka, Ph.D.**
Ústav elektroniky a měření

Konzultant: **Ing. Radek Pospíšil**

Datum zadání bakalářské práce: **24. února 2012**

Termín odevzdání bakalářské práce: **25. května 2012**

Ve Zlíně dne 24. února 2012

prof. Ing. Vladimír Vašek, CSc.
děkan

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT:

Tato bakalářská práce se zabývá studiem radiofrekvenčních technologií a jejich využití pro identifikaci. První část práce se zaměřuje převážně na základní definice RFID, jejich technické specifikace, související hardware a krátce je zmíněna také historie a možnosti využití. V druhé části se zaměříme na popis postupu při implementaci technologie RFID do podniku. Dále se práce věnuje zabezpečení RFID systémů proti zneužití a vyřazení z provozu.

Klíčová slova: RFID technologie, EPC global, automatické vyčítání informací, impementace RFID, vyřazení z provozu

ABSTRACT

This thesis deals with the study of radio frequency technologies and their usage for identification. The first part is mainly focused on the basic definition of RFID and the technical specifications, related hardware and briefly is mentioned also the history and posibilities of its usage. The second part is focused on description of how to implement RFID technology into the enterprise. Further it deals with a security of RFID systems against its abuse and decommissioning.

Keywords: RFID technology, EPCglobal, automatic reading of information, RFID implementation, decommissioning

Děkuji tímto mému vedoucímu bakalářské práce Ing. Jiřímu Pálkovi, Ph.D. za odbornévedení, cenné rady a připomínky během řešení mé práce.

Dále bych chtěl poděkovat panu Ing. Radkovi Pospíšilovi za rady ohledně praktické aplikace v oblasti RFID čipů.

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl jsem seznámen s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně 25.5.2012

.....
podpis diplomanta

[1] *zákon č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, § 47 Zveřejňování závěrečných prací:*

(1) Vysoká škola nevýdělečně zveřejňuje disertační, diplomové, bakalářské a rigorózní práce, u kterých proběhla obhajoba, včetně posudků oponentů a výsledku obhajoby prostřednictvím databáze kvalifikačních prací, kterou spravuje. Způsob zveřejnění stanoví vnitřní předpis vysoké školy.

(2) Disertační, diplomové, bakalářské a rigorózní práce odevzdané uchazečem k obhajobě musí být též nejméně pět pracovních dnů před konáním obhajoby zveřejněny k nahlížení veřejnosti v místě určeném vnitřním předpisem vysoké školy nebo není-li tak určeno, v místě pracoviště vysoké školy, kde se má konat obhajoba práce. Každý si může ze zveřejněné práce pořizovat na své náklady výpisy, opisy nebo rozmnoženiny.

(3) Platí, že odevzdáním práce autor souhlasí se zveřejněním své práce podle tohoto zákona, bez ohledu na výsledek obhajoby.

[2] *zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, § 35 odst. 3:*

(3) Do práva autorského také nezasahuje škola nebo školské či vzdělávací zařízení, užije-li nikoli za účelem přímého nebo nepřímého hospodářského nebo obchodního prospěchu k výuce nebo k vlastní potřebě dílo vytvořené žákem nebo studentem ke splnění školních nebo studijních povinností vyplývajících z jeho právního vztahu ke škole nebo školskému či vzdělávacího zařízení (školní dílo).

[3] *zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, § 60 Školní dílo:*

(1) Škola nebo školské či vzdělávací zařízení mají za obvyklých podmínek právo na uzavření licenční smlouvy o užití školního díla (§ 35 odst. 3). Odpírá-li autor takového díla udělit svolení bez vážného důvodu, mohou se tyto osoby domáhat nahrazení chybějícího projevu jeho vůle u soudu. Ustanovení § 35 odst. 3 zůstává nedotčeno.

(2) Není-li sjednáno jinak, může autor školního díla své dílo užít či poskytnout jinému licenci, není-li to v rozporu s oprávněnými zájmy školy nebo školského či vzdělávacího zařízení.

(3) Škola nebo školské či vzdělávací zařízení jsou oprávněny požadovat, aby jim autor školního díla z výdělku jím dosaženého v souvislosti s užitím díla či poskytnutím licence podle odstavce 2 přiměřeně přispěl na úhradu nákladů, které na vytvoření díla vynaložily, a to podle okolností až do jejich skutečné výše; přitom se přihlédne k výši výdělku dosaženého školou nebo školským či vzdělávacím zařízením z užití školního díla podle odstavce 1.

OBSAH

ÚVOD

RFID (RadioFrequencyIdentification) je jednou z nejvíce rozvíjejících se technologií dnešní doby. Slouží k označování předmětů, výrobků, osob či zvířat. Cílem této bakalářské práce je vytvořit literární rešerši a seznámit čtenáře s technologií radiofrekvenční identifikace „RFID“.

Začátek komerčního využití RFID se datuje přibližně od konce 20. století, začátek 21. století přináší vytvoření standardů a dále velký rozvoj čipů. Po počátečním několikaletém období postupného rozvoje se RFID stále více prosazuje v mnoha oblastech lidské činnosti. RFID technologie se uplatňuje již delší dobu například v oblasti sportu, kde se používají nejen pro uživatele lyžařských vleků, ale i na měření času závodníků podle čipu upevněného v jejich výstroji, a také jako bezdotykové čipové karty na kontrolu vstupu do objektů.

RFID nabízí vyšší rychlost snímání a zjednodušení automatizovaných systémů než při využití čárových kódů. Přestože technologie RFID je známá již několik desítek let, masivnější nasazení ji zřejmě teprve čeká. Tento miniaturní přístroj bez potřeby vlastního napájení je schopný v blízkosti snímacího zařízení poskytnout údaje, které uchovává.

Dále se praktická část zabývá optimálním řešením pro implementaci systému radiové identifikace. Tento návrh spočívá v analýze prostředí, kde bude systém zaveden, a ve zjištění vhodných typů komponentů.

V závěru práce se věnujeme jednotlivým možnostem poškození RFID tagů a vyřazení z provozu, předcházení zničení tagů a možným opatřením proti zneškodnění čipů.

I. TEORETICKÁ ČÁST

1 TECHNOLOGIE RFID

1.1 Základní definice RFID

RFID (Radio Frequency Identification) – identifikace založená na radio-frekvenčním systému je moderní technologie, která nám napomáhá k identifikaci objektů pomocí radio-frekvenčních vln. Jedná se o systém, který lze úspěšně nasadit v mnoha odvětvích a oblastech. Důraz je zde kladen především na co nejrychlejší přesné zpracování informací a okamžitý přenos těchto načtených dat k následnému zpracování. To následně vede ke zvýšení přesnosti, rychlosti a efektivnosti obchodních, skladových, logistických a výrobních procesů. [1]

1.1.1 Tagy

Informace jsou v elektronické podobě ukládány do malých čipů-tagů. Tyto čipy lze následně načítat a opakovaně přepisovat. Zápis i přepis probíhá za pomoci radiových vln. Velkou výhodou tohoto sytému ve srovnání s dnes nejčastěji používanými čárovými kódy je možnost hromadného čtení až několika set tagů za minutu. [1]

Obr. 1. RFID etiketa s čárovým kódem. [1]

1.1.2 RFID jako nástupce čárových kódů

Dnes můžeme technologii RFID považovat za **přímého nástupce čárových kódů**. Z hlediska budoucího vývoje se však nepředpokládá úplné nahrazení čárových kódů, budou oblasti trhu, kde budou dominovat RFID technologie, případně kombinace RFID značení s čárovým kódem. Již dnes se využívají tiskárny, které dokáží zapsat informace na RFID tag a natisknout informacemi s čárovým kódem. Takové tiskárny při potisku

zapisují informace a zároveň kontrolují funkčnost tagu. Pokud je RFID tag poškozen, jsou schopny jej označit jako vadný. [1]

S myšlenkou o vzniku bezdrátové technologie a zpracování informací přišla před lety největší maloobchodní firma WalMart, která před několika desetiletími stála u zrodu čárového kódu. Základem byla myšlenka vyvinout takovou technologii, která dokáže objekt identifikovat na větší vzdálenost, bez přímé viditelnosti tak, aby v reálném čase bylo možno zpracovat více objektů současně.

V současné době se technologie RFID velice rozvíjí a dochází k nasazení v mnoha dalších oblastech trhu. Největší uplatnění nachází v logistice, výrobě, sledování objektů - logistických jednotek (zboží, palet, kontejnerů), sledování majetku, sledování zavazadel na letištích a při evidenci osob. [1]

RFID tagy mají oproti štítkům s čárovým kódem několik zásadních **výhod**. Štítek s čárovým kódem musí být umístěn na viditelném místě pro čtecí zařízení a tím je zároveň vystaven celé řadě možných poškození - odtržení, poškození, teplotní vlivy, povětrností vlivy. RFID tagy lze také umístit do značeného objektu tak, aby nebyl těmto vlivům vystaven, a tím je několikanásobně odolnější oproti štítku s čárovým kódem. Mnoho výrobců v současné době již umísťuje RFID tagy do svých výrobků, palet, kontejnerů přímo ve výrobě.

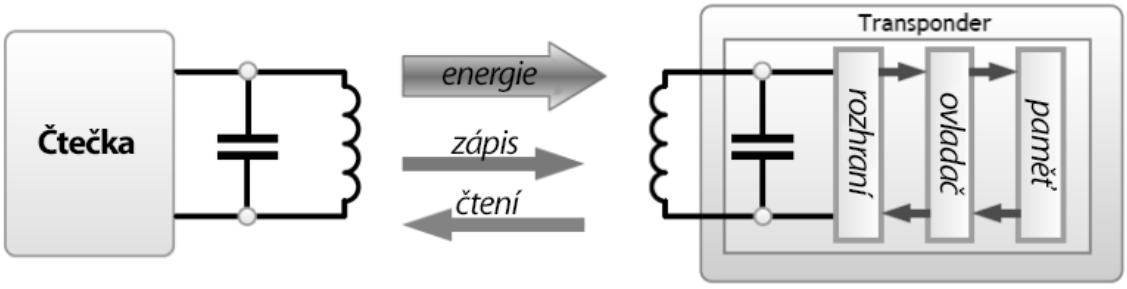
Mezi dvě největší výhody RFID tagů patří následující. Za prvé je to **možnost pomocí čtecího zařízení načíst najednou velké množství tagů na větší vzdálenost** (např. průjezd paletového vozíku čtecím portálem v reálném čase). V případě štítků s čárovým kódem se musí načíst postupně čárové kódy ze všech výrobků na paletovém vozíku. Za druhé je to **možnost zápisu či změny informací přímo do RFID tagu**. [1]

Obr. 2. Různé provedení RFID tagů. [1]

1.1.3 Princip

Podobně jako u čárových kódů se informace zaznamenávají na nosič dat - tzv. RFID tag, který je připevněn na sledované objekty, tag obsahuje malý čip s anténou a pamětí. RFID tagy jsou základem systému pro ukládání a přenos informací pomocí elektromagnetických vln. Může je hromadně přečíst a zaznamenat příslušné čtecí zařízení, které může být pevné nebo mobilní. Pomocí elektromagnetických vln vyzářených z čtecího zařízení dojde k nabití čipu a následně se informace uložená v čipu bezdrátově přenese zpět do čtecího zařízení (každý tag obsahuje tzv. EPC kód (Eletronic Product Code), jedná se o jednoznačné sériové číslo tagu. [1]

Každá implementace RFID technologie obsahuje tagy pro označení objektů, čtecí zařízení a tzv. middleware (řídicí systém, který zajišťuje hromadné zpracování všech načtených tagů v dosahu čtecích zařízení a přenesení zpracovaných dat do návazného informačního či řídicího systému). [1]



Obr. 3. Základní schéma komunikace v RFID. [2]

1.2 EPC KÓD

Pro široké využití RFID v logistice bylo nutné nějakým způsobem tento systém standardizovat. První významnou roli ve standardizaci RFID byl projekt EPC, realizovaný v Auto-ID Centre. Jedná se o vývojové centrum podporované neziskovým společenstvím několika univerzit a průmyslových podniků, které se stalo průkopníkem rozvoje infrastruktury pro sledování zboží. Vizí pracovníků v Auto-ID bylo vytvoření globálního seznamu věcí, který bude jakýmsi „internetem věcí“, kde každá položka bude jednoznačné identifikovatelná svým RFID čipem a bude součástí sítě EPC Network, podobně jako je tomu u počítačů připojených jednoznačnou IP adresou do internetu. Základním předpokladem systémů fungujících v takové síti je, aby byly levné, dostupné v mnoha

verzích od různých výrobců a zároveň dokázaly spolupracovat. Postupně se tak začaly vytvářet specifikace EPC.

Veškeré aktivity byly později ze skupiny Auto-ID Centre převedeny na organizaci EPCglobal. Jedná se o společný podnik celosvětové organizace GS1 (dříve EAN International) starající se o standardizaci a amerického UCC (Uniform Code Council). Úkolem těchto dvou organizací je řídit další rozvoj standardů, zabezpečení vlastnických práv, řídit číslovací databázi EPC a stát se tak celosvětovou informační sítí zvanou EPCglobal Network. [2]

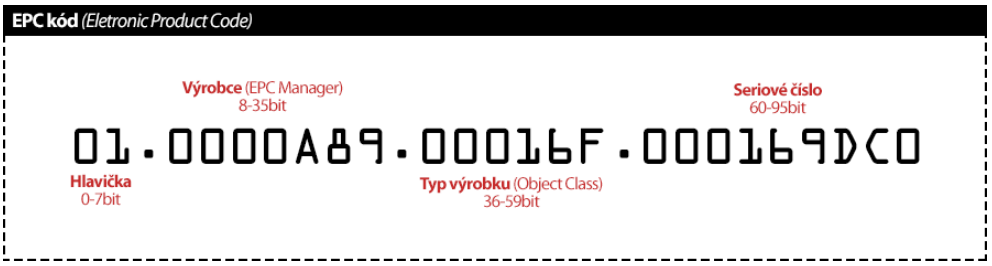
Standard EPC je založen na koncepci registrovaných prefixů a to z důvodu snížení ceny štítků na minimum. O veškeré přiřazené informace se starají externí aplikace, které disponují seznamy výrobců, zboží apod. Tento standard se jeví jako výhodnější než samotné údaje o výrobci ukládat na kapacitně omezené čipy. První generace čipu RFID nese ve své paměti pouze jediné unikátní číslo EPC. Pro představu EPC o velikosti 96 bitů nám dává dostatečný prostor pro 268 miliónů výrobců, z nichž každý může produkovat až 16 miliónů různých výrobků a každý tento výrobek má prostor až pro 68miliónů sériových čísel. V dnešní době zatím nemáme ani teoretický výhled pro využití tak velkého množství čísel EPC a tak se mohou používat také levnější a jednodušší čipy o délce pouze 64 bitů. [2]

Naopak se ale ve standardu počítá i s budoucím využitím 128 nebo 256 bitů, pokud by někdy přestal vyhrazený číslovací prostor dostačovat. [3]

Cena nejjednodušších štítků pro RFID se dnes pohybuje v řádu několika desítek amerických centů za kus a výhledově při velkých objemech výroby se předpokládá, že se sníží jen na jednotky amerického centů za kus.

1.2.1 Datová struktura EPC

Formát EPC je dán jeho specifikací. Část označující výrobce je přidělována organizací EPCglobal tak, aby byla zaručena světová unikátnost každého kódu. Samotné sériové čísla už si výrobce obhospodařuje sám. [3]



Obr. 4. Struktura EPC. [3]

EPC se skládá z následujících částí:

- **Hlavička** - definuje typ údaje v EPC: GTIN, SSCC….

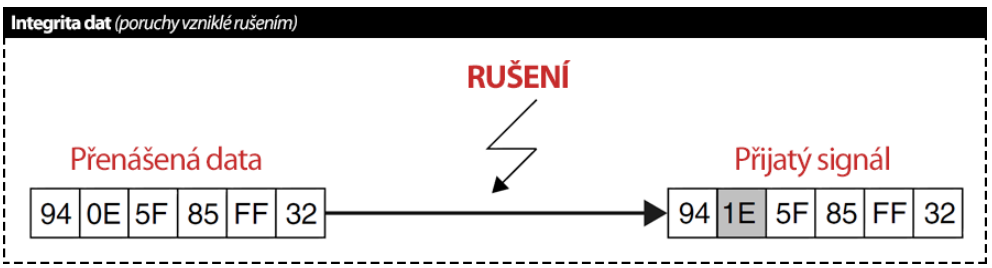
  Filtr - definuje typ jednotky: spotřebitelská, obchodní, logistická

  Parita - definuje pozici, na které končí EPC manažer

- **EPC manažer** - identifikace „vydavatele“ tagu - číslo firmy
- **Objekt manažer** - identifikace druhu zboží
- **Pořadové číslo** - sériové číslo výrobku

1.2.2 Integrita dat

Při přenosu dat pomocí bezkontaktní technologie je velmi pravděpodobné, že může dojít k rušení. Působením nežádoucích vlivů dochází ke změnám přenášených dat a to vede k přenosovým chybám.



Obr. 5. Rušení během přenosu. [3]

1.2.2.1 Kontrola parity

Kontrola parity je velmi jednoduchý postup a proto také hojně využívaný.

Při této proceduře je paritní bit začleněn do každého byte a vysílán společně, s tím že každý byt má poté 8bitů a k nim je přiřazen kontrolní paritní bit. Před samotným přenosem musí být rozhodnuto, zdali má být kontrolována sudá nebo lichá parita, aby kontrolu příjemce učinil podle stejné metody.

Hodnota paritního bitu je nastavena tak, aby v případě liché parity byla výsledná hodnota devíti bitu rovna jedné, ale také každý z devíti bitů nabýval hodnoty jedna. Paritní bit může být také interpretován jako horizontální kontrolní součet (modulo 2) údajů bitů.

Jednoduchost této metody je vyvážena její slabou schopností rozpoznat chyby. Například lichý počet inverzních bitů (1, 3, 5, …) bude možné ověřit vždy, ale pokud je sudý počet inverzních bitu (2, 4, 6,…) chyby zruší jedna druhou a paritní bit vypadat jako správný. [2]

1.2.2.2 Kontrolní součet

Kontrola cyklickým kódem nebo cyklická kontrola (Cyclic Redundancy Check, zkráceně CRC) je druh kontrolního součtu používaného pro kontrolu správnosti přenášených údajů v telekomunikační technice a počítačových sítích, jakož i uložených dat na paměťových médiích jako je například pevný disk.

Na základě jednotlivých bitů se vypočítává zabezpečovací údaj. Ten se na konci celého bloku porovná se zabezpečovacím údajem, který podle stejných pravidel vypočítal odesilatel a připojil k přenášenému bloku dat. Pokud se tyto dva údaje shodují, dá se přenesen blok s vysokou pravděpodobností předpokládat za správný. K výpočtu zabezpečovacího údaje nám postačí jednoduchý posuvný registr, umožňující operaci EX-OR (tj. výhradní NEBO jednotlivých bitů) s pevně danou maskou. Hodnota této masky je jednoznačně určena tzv. generujícím polynomem (generating polynomial), na kterém musí být příjemce i odesílatel předem domluveni. Použitelných polynomů těchto tvarů je více. V síťové komunikaci se nejčastěji používá polynom, doporučený organizací CITT (Center for International Trade and Transportation).

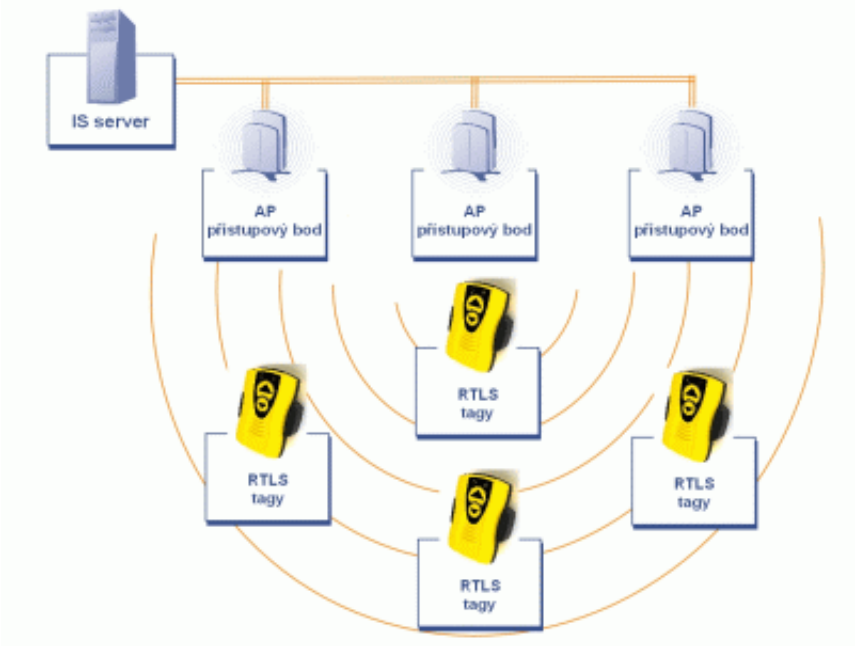
Kontrola cyklickým kódem - jako každý kontrolní součet - mírně zvětšuje redundanci zprávy, ale zvyšuje její spolehlivost. [2]

1.3 RTLS

Systém lokalizace v reálném čase (RTLS) elektronický tag nejen identifikuje, ale navíc umožňuje lokalizaci a následné sledování pohybu v reálném čase. Systém využívá malých elektronických zařízení – aktivních RFID tagů. Tato technologie je využívána převážně pro sledování a určování polohy objektů převážně uvnitř budov případně v rámci areálu. Tento systém dosahuje typicky přesnosti v řádu jednotek metrů, některé komplexnější dokonce v řádu desítek centimetrů. [4]

1.3.1 Topologie systému

Všechny systémy RTLS využívají nějaký typ infrastruktury. Pro správnou funkci systému musí mít každý tag dostatečný signál této bezdrátové sítě. Jednotlivé aktivní tagy za pomocí této sítě vysílají data na server. Získaná data jsou zpracována na serverových aplikacích a ty následně vyhodnocují polohu tagu, či jeho trasu pohybu. [4]



Obr. 6. Topologie RTLS. [4]

1.3.2 Dělení RTLS dle použité infrastruktury

V dnešní době se na světovém trhu setkáváme s mnoha systémy RTLS, které využívají řadu frekvencí a bezdrátových infrastruktur. Dle těchto parametrů systémy můžeme také rozdělit.

Systémy využívané ve standardizovaných infrastrukturách:

- ZigBee (2,4GHz)
- UWB (Ultra Wide Band)
- WiFi (802.11 b/g/n, 2,4GHz)

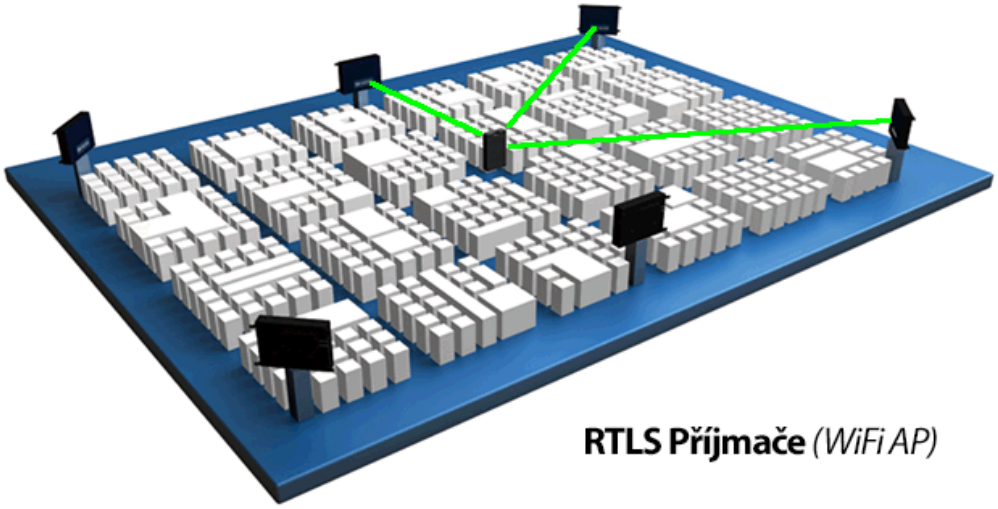
Proprietální systémy – pro svou funkci využívají speciální bezdrátové infrastruktury, které jsou určeny pouze pro systém RTLS. Samozřejmě se jedná o spolehlivější řešení, kde nehrozí rušení či jiné problémy způsobené ostatními zařízeními využívajícími bezdrátové infrastruktury. [2]

- Využívají zejména frekvence 433 MHz, 860/900 MHz a 2,4 GHz

1.3.3 Metody stanovení polohy u systému RTLS

Pro zjištění polohy RTLS tagů se setkáváme hned s několika metodami zjištění polohy. Převážná část těchto metod využívá závislosti vzdálenosti na času potřebném k překonání vzdálenosti mezi přijímačem / vysílačem.

Metoda využívající pouze tohoto principu se nazývá **ToA** (Time of Arrival). Tato metoda vyžaduje synchronizaci času na přijímači a vysílači, což má dramatický vliv na přesnost a stává se tak největší nevýhodou této metody. Odstranit tuto nevýhodu se podařilo díky metodě **TDoA** (Time Diferece of Arrival), kdy se vychází nikoli z absolutních hodnot času, ale i z rozdílů mezi sousedními vysílači. Podobnou metodu využívají systémy GPS. Všechny tyto metody pracující s časem, jsou vhodné převážně pro venkovní prostory s minimem odrazů a s přímou viditelností z vysílače na přijímač.



Obr. 7. Metoda TDoA pro určení polohy tagu v objektu. [4]

Další metodou je **RSSI** (Received Signal Strength Indication). V této metodě vycházíme intenzity síly signálu radiově viditelných přístupových bodů. Využívá se závislost síly signálu na vzdálenosti od vysílače. Pro přesné určení polohy RTLS tagu je důležité znát sílu signálu alespoň od tří přijímačů. Tato metoda je vhodná pro systémy pracující uvnitř budov. [4]

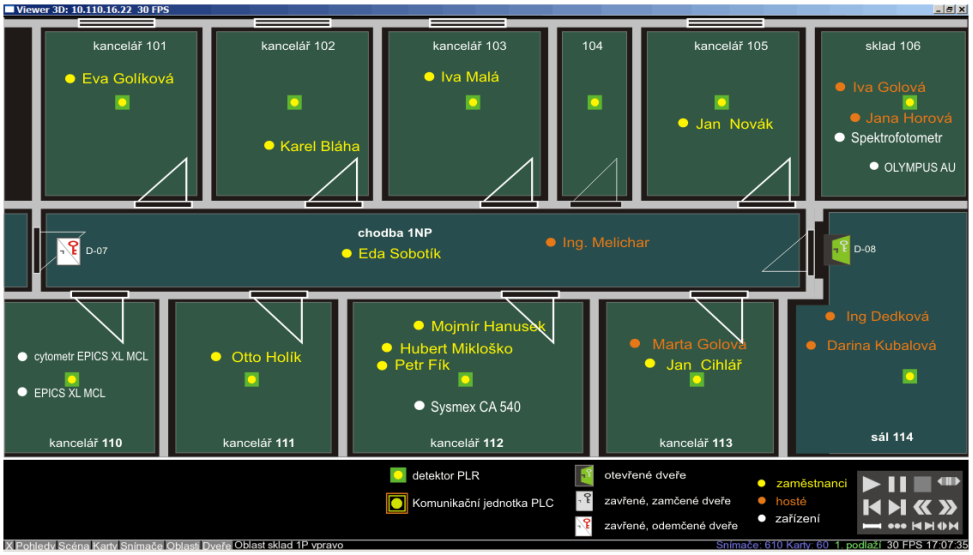
ToF (Time of Flight) RTLS systém vyhodnocuje polohu RFID tagu na základě času letu signálu. Tato metoda je technologický náročnější, ale sledovaný RFID tag lze zaměřit velmi přesně. Systém pracuje na frekvenci 2,4 GHz a je vhodný pro výrobní haly a distribuční centra.

1.3.4 Možnosti rozšíření RTLS systémů:

Automatická identifikace a lokalizace osob či majetku pomocí RFID technologie může být využita napříč obory v kombinaci s dalšími technologiemi a senzory. [13]

- Integrace do kamerových systémů CCTV
- Integrace do zabezpečovacích systémů EZS
- Integrace senzorů na úrovni RFID čtečky
- Integrace senzorů na úrovni RFID tagu

Tento systém je vhodný a hojně využíván například pro sledování pohybu zaměstnanců a návštěv ve firmách, vysokozdvižných vozíků po halách, nákupních vozíků, pacientů v nemocnicích atd.

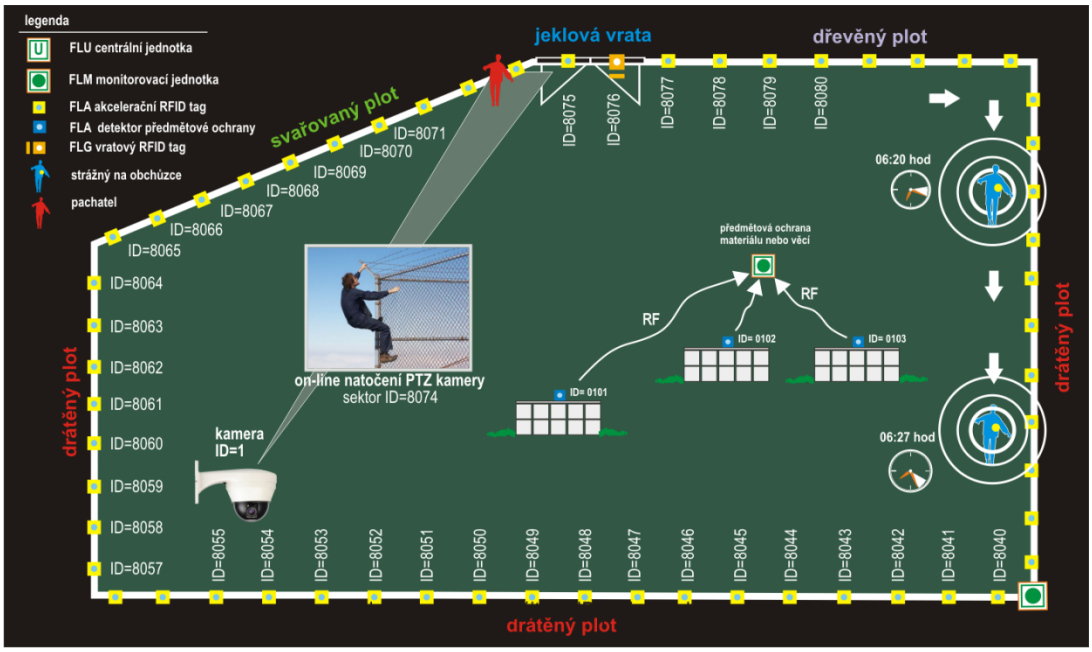


Obr. 8. RTLS vizualizace osob a zařízení v 3D modelu objektu. [5]

1.3.5 Novinky v RTLS sledování

Mezi aktuální novinky na trhu v oblasti RTLS tagů přicházejí systémy perimetrické ochrany umožňující střežení plotu pomocí speciálních akceleračních RFID detektorů připevněných na plotu a vratech. Akcelerační RFID detektory nevyžadují kabeláž a životnost jejich baterií je cca 8 let. [5]

Perimetrický systém založený na RTLS ve spojení s kamerovým systémem vybaveným otočnými kamerami PTZ dokáže velmi přesně tyto kamery nasměrovat na místo incidentu. Pomocí tohoto systému můžeme nahradit kontrolu obchůzkové činnosti strážných v rámci perimetru. Tyto systémy jsou obzvláště vhodné pro fotovoltaické elektrárny. Díky speciálním ochranám se vyhneme i riziku přepětí v těchto elektrárnách. [5]



Obr. 9. Ukázka využití RFID perimetrického systému. [5]

Princip systému

Na perimetrickou ochranu (plot) se namontují v pravidelných vzdálenostech akcelerační RFID detektory FLA, které za pomocí 3osého akceleračního čipu detekují veškeré otřesy plotu. Detekují také veškeré dynamické změny polohy pletiva, které jsou typické pro prostřižení pletiva pachatelem. Pro funkci detektorů FLA není nutná žádná kabeláž. Jednotlivé detektory spolu komunikují na principu „tiché pošty“. Jednotlivé detektory postupně retranslatují naměřené informace od jednoho tagu k druhému

nejbližšímu až do centrální jednotky FLU. Přeposílají si tak informace o pohybu plotu, síle větru, technických stavech či sabotážích apod. Rychlost tohoto předávání je až 300tagů za sekundu. O vyhodnocování celého systému se stará centrální jednotka FLU, která je schopna předávat veškeré informace nadřazenému systému EZS (Elektronický Zabezpečovací Systém) nebo přímo řídí otočné PTZ kamery. [5]

Obr. 10. Model systému perimetrické ochrany za pomocí RFID. [5]

2 HARDWARE

2.1 RFID tagy

V tagu jsou informace uloženy v elektronické podobě, které jsou v energeticky nezávislé paměti. RFID tag obsahuje malý RF vysílač a přijímač. Čtečka RFID tagů vyšle kódovaný rádiový signál pro přečtení. Tag obdrží zprávu a odpovídá svými identifikačními údaji. To může být jen unikátní sériové číslo, nebo informace související s produktem jako skladové číslo, číslo šarže, datum výroby nebo jiné konkrétní informace.

Tagy mohou být pouze pro čtení s přiděleným sériovým číslem při výrobě, které slouží jako klíč do databáze, nebo může být i zapisovací, kde je možné zapsat specifické údaje uživatelem. Na programovatelné tagy může zápis proběhnout jen jednou, číst lze vícekrát. Na „prázdné“ tagy mohou uživatelé zapsat elektronický kód produktu.

RFID tagy obsahují nejméně dvě části: integrovaný obvod pro ukládání a zpracování informací, modulaci a demodulaci radio-frekvenčního (RF) signálu, sbírání stejnosměrného proudu z dopadajícího signálu čtečky, další specializované funkce a anténu pro příjem a vysílání signálu.

Komunikace mezi tagem a čtečkou probíhá několika vzájemně nekompatibilními způsoby, v závislosti na používaném frekvenčním pásmu. U nízkých frekvencí (LF) a vysokých frekvencí (HF) tag může modulovat signál vysílaný ze čtečky změnou elektrického zatížení. Přepínáním mezi nižším a vyšším zatížením tag produkuje změny, které musí čtečka zachytit. U velmi vysokých frekvencí (UHF) čtečka produkuje více jak jednu frekvenci. Aktivní tagy mohou obsahovat funkčně oddělený vysílač a přijímač a tag nemusí reagovat na frekvenci náležící čtecí frekvenci čtečky. [5], [6]

2.1.1 Rozdělení podle zdroje energie

Tagy dělíme do dvou základních skupin dle napájení a to pasivní a aktivní.

Aktivní tagy vysílají do okolí samy své údaje (TTF tag talks first), pro samotné vysíláni je nutný zdroj energie nejčastěji vlastní miniaturní baterie umístěna v čipu, která vydrží cca 1-5 let. Baterie jsou náchylnější na teplotu, z toho důvodu se aktivní RFID čip stává méně spolehlivým a je tedy nutné dbát na výměnu baterií.

Nejčastěji se aktivní tagy se využívají pro sledování osob, vozového a technologického parku, sledování zvířat a tam, kde leze čip opětovně použít a lehce

baterie vyměnit. Díky vlastnímu zdroji energie jsou aktivní tagy vhodné pro čtení z větší vzdálenosti (až 100 m).

Náklady na pořízení jsou poměrně vysoké a velikost paměti na čipu může dosahovat až 100 Kb. [1]

Pasivní čipy jsou cenově výrazně levnější, mají různou akční vzdálenost čtení od 0,5 m do 10 m, dlouhou životnost čipu a používají metodu (RTF reader talk first). Tagy, které pracují na nejvyšší frekvenci UHF mají rádius - cca 3 až 10 m, ty s frekvencí nejnižší LF 125 kHz mají dosah jen cca 0,5 m.

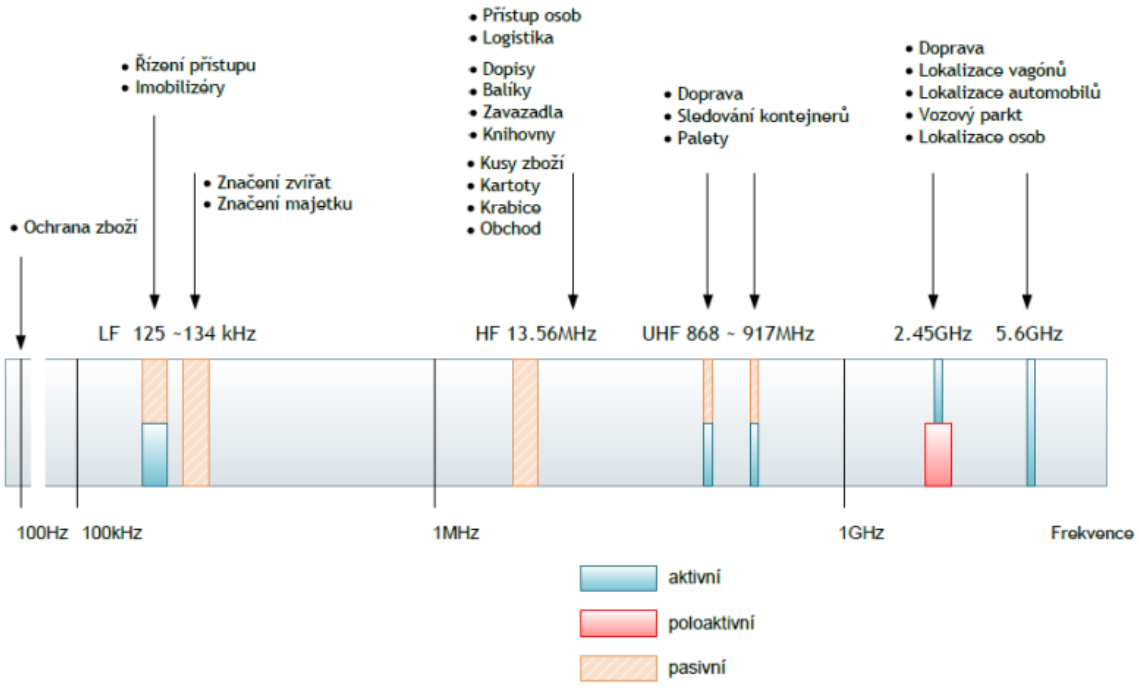
V současné době jsou nejvíce rozšířeny pasivní čipy a to zejména kvůli své nízké ceně, nenáročnosti na obsluhu a odolnosti, velikost paměti 64 - 256 bitů. [1]

2.1.2 Přidělená frekvenční pásma pro UHF tagy

Region 1 865 - 869 MHz Evropa a Afrika

Region 2 902 - 928 MHz USA, Kanada a Mexiko

Region 3 950 - 956 MHz Japonsko a Asie



Obr. 11. Frekvence používané různými aplikacemi RFID. [2]

2.1.3 Rozdělení tagů dle tříd

Class 0	pouze pro čtení, programováno ve výrobě, 64 nebo 96bit, čtení 1000tagů/sec
Class 1	zápis jednou/zápis mnohokrát, programováno při použití, 64 nebo 96bit, čtení 200tagů/sec
Class 0+	čtení/zápis, programováno kdykoliv, 256bit, čtení 1000tagů/sec
Gen 2	čtení/zápis, programováno kdykoliv, 256 bit, čtená 1600tagů/sec

Tab. 1. Třídy RFID tagů. [2]

2.1.4 Rozdělení tagů dle použití

RFID tagy se v současné době vyrábějí v několika variantách, dle velikosti a materiálu. S více variantami souvisí i použití (tagy produktové, kartonové, paletové, malé tagy na láhve) a dále tagy dělíme dle způsobu použití (nalepení přímo na objekt), tzv. "Inlays" pro další použití pro výrobce - přímo zabudované do produktů a zapouzdřené (například plastové - mají větší odolnost a používají se i v případě umístění tagu na kovový materiál, zde zajišťují oddálení čipu a antén od rušivého podkladního materiálu kovu). [1]

2.1.5 Cena

V roce 2011 cena pasivního tagu začínala na 0,05 USD. Speciální tagy aplikované na kovové prvky, nebo odolné vůči gama záření dosahovala až 5 USD. Aktivní tagy pro sledování kontejnerů, zdravotnických prostředků nebo sledování podmínek životního prostředí datových center začínaly na 50 USD a mohly jít až na 100 USD za kus. Battery Assisted Passive (BAP) tagy byly v rozmezí 3-10 USD. [6]

2.2 Čtečky

RFID je bezkontaktní identifikace, a proto není nutné, aby čtečka kódu přišla do přímého kontaktu s tagem, a nemusí být ani v přímé viditelnosti.

Třetí důležitou částí RFID systémů jsou čtečky nosičů informací. Vedle tagů existuje na trhu jejich rozsáhlá paleta na zdokonalení systému RFID. Základním požadavkem na vlastnosti čtečky je schopnost zpracovávat enormní množství dat, zvláště při současném nasazení několika čteček. Přitom musí být rozeznávány opakovaně čtené etikety a rušivé signály vznikající odrazem signálu od kovových předmětů v okolí. Navíc je často potřeba současně zpracovávat 100 - 1000 etiket obsažených například v jednom kontejneru.

Čtečka se skládá z řadiče a příslušných elektricky přizpůsobených antén s různou konstrukcí. Emituje elektromagnetické vlny do okolí. Mohou být zkonstruovány buď jako jeden přístroj nebo odděleně řadič a anténa. Dle toho je členíme na stacionární a mobilní. Stacionární bývají nepřenosné, jsou pevně vestavěné v určeném identifikačním bodě (například vstup / výstup ze skladu, začátek dopravníku, stůl na přípravu výrobků a další). U mobilních čteček jsou oba komponenty implementovány ve společné v jednom zařízení. Tyto zařízení jsou určené pro držení v ruce.

Obr. 12. Mobilní RFID čtečky. [8]

2.2.1 RFID portály/brány

Za pomocí brán či portálů vytváříme čtecí zóny ve vstupech, výstupech, průjezdech či expedičních rampách.

Obr. 13. RFID brány. [8]

2.3 Tiskárny

RFID tiskárny slouží k naprogramování RFID tagů a následnému tisku etikety s daným tagem. [1]

Tiskárny RFID tagů jsou speciální zařízení schopna zapsat data do tagu, vytisknout čárkový kód a zároveň textové informace čitelné pro člověka. Takové to tiskárny jsou schopny tisknout na speciální etikety obsahující RFID tag. Tiskárny zároveň obsahují čtečku, která ověří správnost zapsaných dat. [8]

Obr. 14. RFID tiskárny. [8]

Obr. 15. První mobilní RFID tiskárna. [8]

3 RFID V PRAXI

RFID tagy jsou používány v mnoha průmyslových odvětvích. V automobilovém průmyslu je možné sledovat postup výroby pomocí RFID při průchodu výrobní linkou. Léčiva mohou být sledována uvnitř skladů. Hospodářská a domácí zvířata mohou mít tagy implementované pomoci injekce k následné identifikaci zvířete. RFID identifikační karty mohou dát zaměstnancům přístup k uzamčeným prostorám budovy a transpondéry umístěné v automobilech mohou být použity k vyúčtování motoristů při vstupu na zpoplatněné silnice nebo parkoviště. [6]

Vzhledem k tomu, že RFID tagy lze připevnit k oděvu a majetku, nebo dokonce implantovat lidem pod kůži, možnost čtení osobních informací bez souhlasu může narušit soukromí osob. [6]

3.1 Příklady komerčního využití

3.1.1 Platby mobilními telefony

Od poloviny roku 2009 jsou vyvíjeny specializované microSD karty, které po vložení do mobilního telefonu můžou být jak pasivní tagy, tak i RFID čtečky. Po vložení microSD může být uživatel mobilního telefonu spojen s bankovními účty a používat mobilní platby. [6]

Obchodní řetězec Diry Queen ve spojení s Vivotech začal používat RFID pro mobilní telefony v rámci svého nového věrnostního programu a odměn. Zákazníci mohou požádat o RFID tag pro jejich telefon. Po aktivaci telefon může přijímat propagační materiály a kupóny, které lze číst ve specializovaných ViVOtech NFC (Near Field Communication) zařízení. [6]

Podobně, 7-Eleven pracuje spolu s MasterCard na propagaci nového bezdotykového platebního systému. Zákazníci obdrží mobilní telefon např. Nokia 3220. Po aktivaci může být použit jako RFID kompatibilní s kartou MastrCard v jakékoli pobočce řetězce 7-Eleven. [6]

3.1.2 Sledování stavu zásob

Pokročilé automatické identifikační technologie založené na RFID technologii mají velkou hodnotu pro sledování stavu zásob. Systém může poskytovat přesné informace o aktuálním stavu zásob. V akademické studii prováděné ve Wal-Martu RFID snižuje

množství starých zásob o 30 % u produktů, kterých je prodáno 0,1 až 15 denně. Dalšími výhodami používání RFID je snižování mzdových nákladů, zjednodušení podnikových procesů a snížení nepřesností v zásobování.

V roce 2004 společnost Boeing integrovala technologii RFID s cílem snižovat náklady na údržbu a skladových zásob pro Boeing 787 Dreamliner. S vysoce nákladnými části letadel technologie RFID umožnila sledovat zásoby navzdory unikátní velikosti, rozložení a politiky koncernu. Během prvních šesti měsíců po nasazení společnost ušetřila 29 000 dolarů na práci. [6]

3.1.3 Sledování výrobku

V roce 2005 kasino Wynn v Las Vegas umístilo RFID tagy na žetony s vysokou hodnotou. Tyto tagy umožnily detekovat padělané žetony, sledování návyků jednotlivých hráčů, zrychlit sčítání žetonů a počítat chyby dealerů.

V roce 2010 bylo kasino Bellagio okradeno o 1,5 milionu dolarů v žetonech. RFID tagy těchto žetonů byly okamžitě znehodnoceny, čímž se peněžní hodnota těchto žetonů změnila na 0 dolarů.

RFID může být také použit pro řízení dodavatelského řetězce v módním průmyslu. Štítek RFID je připojen k oděvu při výrobě. Je možné číst / sledovat průběh celého dodavatelského řetězce a štítek je odstraněn až v místě prodeje (point ofsale – POS). [6]

3.1.4 Řízení přístupu

HF tagy jsou široce používány u identifikačních karet, kde nahrazují starší karty s magnetickým proužkem. Tyto karty se nemusí přímo dotýkat čtečky k ověření držitele. [6]

3.1.5 Reklama

Když zákazník vstoupí do převlékací kabinky, zrcadlo odráží jejich obraz a také možnosti jejich oblečení, které nosí celebrity, na interaktivním displeji. Webová kamera dále promítá obraz spotřebitele na webové stránky komukoliv k podívání. To vytváří interakci mezi zákazníky uvnitř obchodu a jejich sociální sítí mimo obchod. Použitá technologie v tomto systému je RFID přijímací anténa v kabince a EPC RFID tag v zobrazovacím zařízení. [6]

3.2 Doprava a logistika

Logistika a doprava jsou hlavními oblastmi uplatňující RFID technologii. K řízení dopravy, lodní, nákladní logistiky a distribučních center se využívá RFID sledovací technologie. V železničním průmyslu jsou RFID tagy umístěny na lokomotivy a vozovém parku identifikující jejich majitele za pomoci identifikačního čísla, informací o typu zařízení a jeho vlastnostech. Ty mohou být použity s databází k identifikaci nákladu, původu, cíli atd. z komodit, které se převáží.

V komerční letecké dopravě je technologie RFID začleněna pro podporu údržby letadel. RFID tagy jsou používány také k identifikaci zavazadel a nákladu na několika letištích a v několika leteckých společnostech. Některé země používají RFID technologie pro registraci a následné odhalení odcizených vozidel. [6]

3.3 Cestovní pasy

První RFID cestovní pas byl vydán v Malajsii v roce 1998. Kromě informací obsažených vizuálně v pasu, tento pas obsahuje historii cestování (čas, datum a místo). Mezi ostatní země, které vkládají RFID do pasů patří Norsko, Japonsko, většina zemí EU, USA, Srbsko, Korejská republika, Tchaj-wan, Albánie, Filipíny a Makedonie (do roku 2010). Normy pro cestovní pasy RFID jsou stanoveny Mezinárodní organizací pro civilní letectví (ICAO). [6]

Obr. 16. Cestovní pas s integrovaným RFID tagem. [8]

3.4 Dopravní poplatky

V mnoha zemích je RFID používán k úhradě jízdného hromadné autobusové dopravy, tramvají, podchodů, nebo k výběru mýtného na dálnicích. Některé zámky na kolo jsou přidruženy k RFID kartě konkrétního majitele. [6]

3.5 Identifikace

RFID tagy pro zvířata představují jednu z nejstarších využití technologie RFID. Původně je využívaly velké farmy, pro zvířata v těžkém terénu. Od vypuknutí nemoci šílených krav je RFID důležité pro identifikaci zvířat v oblasti managementu. Implantabilní RFID transpondéry implantované zvířatům jsou známy jako „čipy“ pro zvířata. Kanadská agentura pro identifikaci skotu (CCIA) začala používat tagy jako náhradu čárových kódů. [6]

Implantabilní RFID čipy určené pro označování zvířat jsou nyní používány u lidí. První experiment byl proveden profesorem kybernetiky Kevinem Warwickem, který implantoval čip do vlastní paže v roce 1998. V roce 2004 Conrad Chse začal nabízet implantování čipů v jeho nočních klubech v Barceloně a Rotterdamu k identifikaci svých VIP zákazníků, kteří přes ně platí nápoje. Tyto čipy vzbuzují nevoli u ochránců osobních údajů, kteří varují před případným zneužitím. [6]

3.6 Instituce

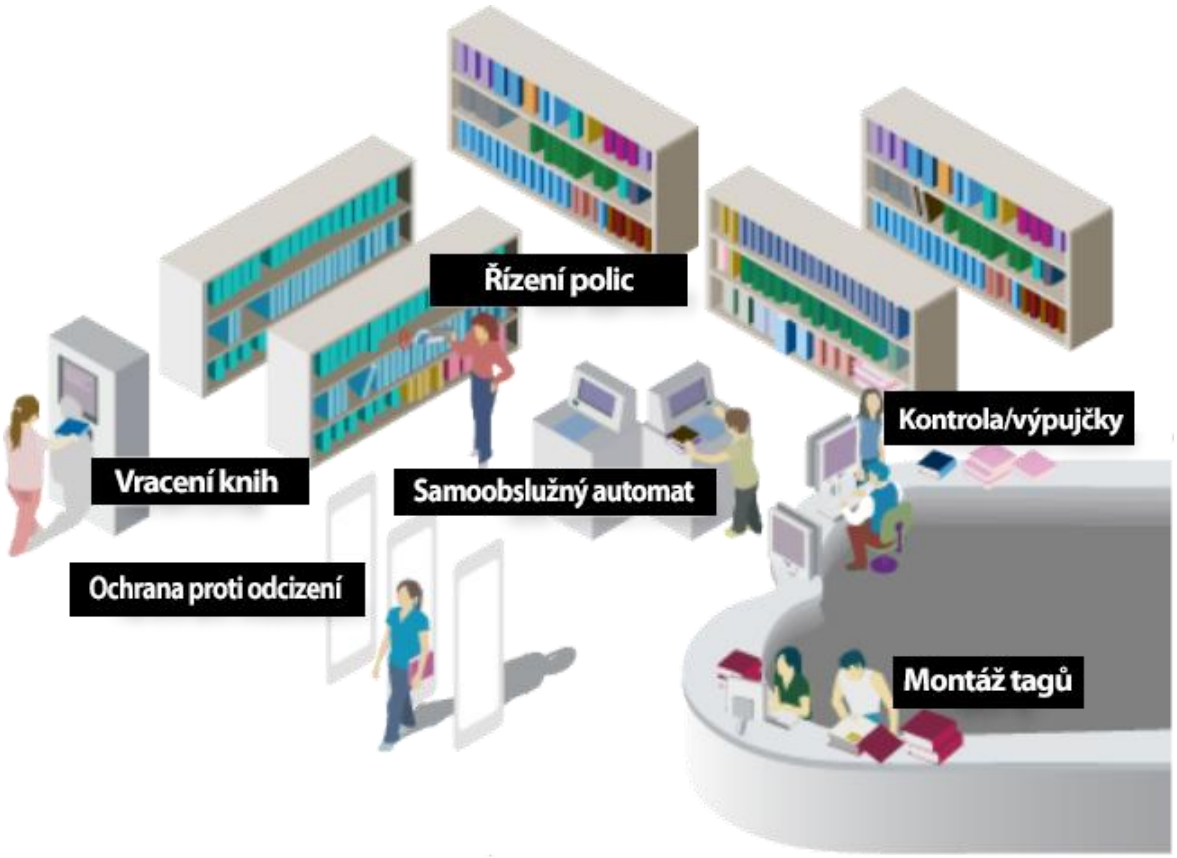
3.6.1 Nemocnice a zdravotnická zařízení

Přijetí RFID ve zdravotnickém průmyslu má široké uplatnění a je velmi efektivní. Nemocnice patří mezi první uživatele, kteří kombinují pasivní i aktivní RFID technologie. [6]

V nemocnicích RFID umožňuje elektronické označování nemocničního majetku, zásob, personálu a pacientů. U zboží mohou být ve formě samolepek a u lidí v podobě náramků nebo klíčenek s RFID čipy. Věci a lidé mohou být identifikovány, sledovány a řízeny skrze centrální databázi. Pro sledování je taková nemocnice vybavena systémem pro sledování polohy zařízení a osob. [9]

3.6.2 Knihovny

Knihovny využívají RFID k doplnění či nahrazení čárových kódů u knihovních položek. Tag může obsahovat identifikační údaje, nebo může být jen klíčem do databáze. Odhaduje se, že více než 30 miliónů knihovních jednotek po celém světě nyní obsahují RFID tagy, včetně některých ve Vatikánské knihovně v Římě. [6]



Obr. 17. Implementace technologie RFID v Knihovně. [18]

3.6.3 Školy a univerzity

Ve školských zařízeních je RFID využíváno k řízení přístupu a také k výpůjčnímu systému knihoven v daných zařízeních. [6]

3.6.4 Sport

V závodě nosí tagy závodníci připevněné na těle. Tagy jsou čteny anténami v průběhu celé tratě nebo pouze ve startu a následně v cíli. UHF tagy se speciálními anténami poskytují přesné údaje o časech, kdy závodník prošel kontrolním bodem.

Pasivní i aktivní tagy jsou využívány při událostech, jako je orientační běh či cyklistika apod. Závodníci mají transpondér umístěný obvykle na paži nebo kotníku. Orientační běžci například po dosažení kontrolního stanoviště přiloží paži k přijímači, který je připojen k počítači zapisujícím časy na kolo.

Řada lyžařských středisek již přijala skipasy obsahující RFID tagy. Lyžařům tak umožňují pohodlný přístup k lyžařským vlekům. Takto vybavený skipas stačí nést u sebe ukrytý například v kapse bundy. Po vstoupení k turniketům (vybavených RFID čtečkou) jsou z tagu vyčteny informace o platnosti skipasu a lyžaři je povolen vstup na lanovky. Nyní v Evropě RFID využívá většina lyžařských areálů. [10]

Obr. 18. Náramek obsahující RFID tag. [6]

3.7 Telemetrie

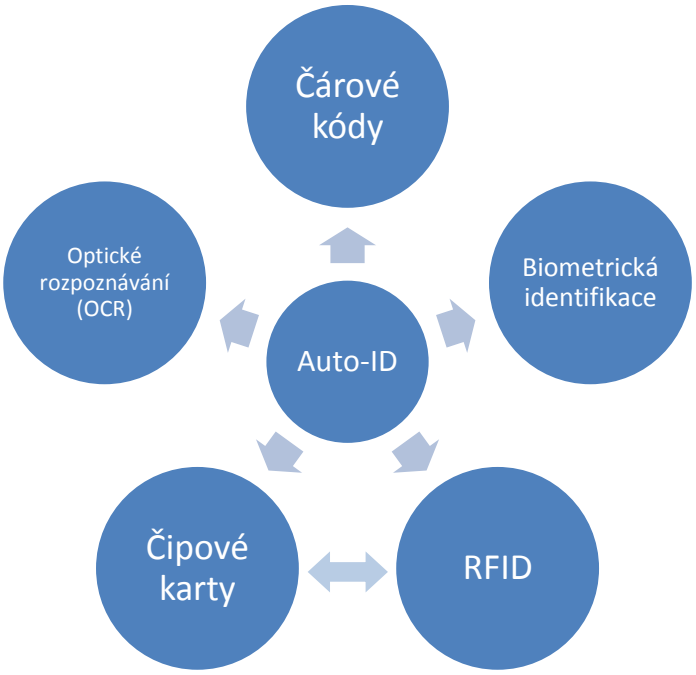
Aktivní RFID mají potenciál nízko nákladových vzdálených senzorů, které vysílají telemetrická data základně. Mezi aplikace snímacích RFID tagů patří snímání podmínek na silnici, údaje o počasí nebo monitorování hluku. [6]

4 SROVNÁNÍ S JINÝMI TYPY VYČÍTÁNÍ INFORMACÍ

V posledních letech se automatické identifikační procesy (Auto-ID) stávají velmi populární v mnoha odvětvích služeb, průmyslu, logistice, ale také ve výrobě. Automatické identifikační systémy existují, aby nám pomohly identifikovat informace o lidech, zvířatech, zboží a produktech v oběhu.

Všudypřítomné štítky s čárovými kódy, které spustily revoluci v identifikačních systémech, již delší dobu přestávají dostačovat ve stále větším počtu případů. Čárové kódy jsou sice velmi levné, ale jejich překážkou je jejich nízká skladovací kapacita a skutečnost, že není možné je později přeprogramovat.

Jako technicky optimální řešení se tedy nabízí ukládání dat v křemíkovém čipu. Mezi nejběžněji dnes používané formy pro uchovávání dat řadíme čipové karty využívající kontaktního pole (telefonní čipové karty, bankovní karty). Slabou stránkou čipových karet se tak stává právě jejich mechanický kontakt se čtečkou. Bezkontaktní výměna informací mezi čtečkou a paměťovým mediem, nesoucím data by byl mnohem flexibilnější. Díky těmto nesporným nevýhodám se ubíráme spíše k bezkontaktnímu čtení a zde přicházejí na řadu RFID systémy s bezdrátovým přenosem energie i dat.



Obr. 19. Přehled nejdůležitějších Auto-ID procedur. [2]

4.1 Čárový kód

Čárové kódy jsou jedním z nejrozšířenějších prostředků automatické identifikace. Mezi jejich největší výhody patři především **přesnost**. Oproti ručnímu zadávání, kdy dochází k chybě při každém třístém zadání, při použití čárových kódů se počet chyb sníží, můžeme mluvit až o jedné miliontině. Pokud jsou použity k čárovému kódu ještě i kontrolní číslice, jsme schopni toto číslo udávající počet chyb ještě dále snížit.

Oproti ručnímu zadávání můžeme dále vyzdvihnout rychlost při snímání, avšak tento parametr v mnohém překonávají ostatní metody automatické identifikace.

Momentálně je největší výhodou **cena** čárových kódů. V drtivé většině jsou veškeré náklady na označení zboží čárovými kódy pouze nosič (papír) a tisk. Ve srovnání s ostatními typy vyčítání jsou náklady tedy zanedbatelné.

Mezi nejznámější druhy čárových kódů v našem regionu patří EAN 13 a jeho kratší varianta EAN 8. Ty se používají pro označení zboží v obchodních řetězcích (EAN = European Article Numbering).

Obr. 20. Čárové kódy EAN13 a EAN8.[15]

V poslední době se také setkáváme s QR kódy, jedná se o 2D maticový kód, který je tvořen černými a světlými buňkami čtvercového nebo obdélníkového tvaru. Dokáže pojmout až 2kB a zároveň však maximálně 2335 alfanumerických znaků. Používá se zejména u elektronických součástek, jako jsou čipy, procesory apod. [2]

4.2 Optické rozpoznávání znaků

Optické rozpoznávání znaků zkráceně ORC (Optical Character Recognition) je metodou, která za pomoci skeneru digitalizuje tištěné texty, s nimiž lze poté pracovat jako s obyčejným textem. Za specializovaného softwaru jsou jednotlivá písmena porovnávána a přirovnávána znakům v počítači. Přesnost rozpoznávání úzce souvisí s kvalitou tisku předlohy.

Největší výhodou OCR je velká hustota informací a možnost číst data vizuálně (lehce čitelné pro člověka). V dnešní době se používá převážně v bankovnictví pro čtení informací z šeků (soukromá data jako jsou jméno, příjmení, číslo účtu, apod.). Ve srovnání s ostatními systémy automatické identifikace se příliš nepoužívají kvůli drahým čtečkám a také z důvodu velké chybovosti.

4.3 Biometrické identifikace

Biometrika je definována jako věda zabývající se měřením tělesných znaků živých bytostí. V rámci identifikačních systémů biometrie je obecný pojem pro všechny postupy, které dokáží identifikovat osoby na základě porovnávání nezaměnitelných znaků a fyzikálních charakteristik dané osoby. V praxi se setkáváme s otisky prstů a dlaní, hlasovým rozpoznáváním, kontrolou sítnice či duhovky.

4.3.1 Hlasové rozpoznávání

Hlasové rozpoznávání je využíváno ve specializovaných systémech pro identifikaci jedince pomocí ověřování řečníka. Toto rozpoznávání je prováděno také za pomocí počítače, který mluvená slova převádí na digitální signály a ty následně ověřuje s nasbíranými vzorky.

Cílem rozpoznávání je určit předpokládanou totožnost osoby na základě hlasu. Pokud je totožnost ověřena, může být dále rozpoznávání použito pro hlasové příkazy. Například vyslovením „zhasnout světla“ je akce systémem vykonána.[2]

4.3.2 Otisk prstů (daktyloskopie)

Kriminalistika využívá metodu identifikace zločinců za pomoci otisků prstů již od počátku dvacátého století. Tento proces je založen na porovnávání papilárních linií na prstech, dlaních, ploskách nohou.

Pokud jsou otisky prstů využívány pro identifikaci osob, je nutné přiložit prst ke speciální čtečce. Systém vypočítá záznam dat a porovná je s databází referenčních vzorů. Dnešní systémy na ověřování otisků prstů jsou velmi rychlé, stačí půl sekundy pro správnou identifikaci. Moderní čtečky kontrolují také teplotu a krevní řečiště přiloženého prstu. [2]

4.4 Čipové karty

Čipová karta je elektronické zařízení určené pro ukládání dat, případně s přidanou výpočetní jednotkou (karty s mikroprocesorem). Toto elektronické zařízení je vloženo do plastové kartičky velikosti kreditní karty. S prvními čipovými kartami jsme se setkali ve formě předplacených telefonních čipových karet.

Při umístění do čtečky jsou kontakty karty galvanicky spojeny. Energie je do čipové karty dodávána čtečkou.

Jednou z hlavních výhod čipové karty je skutečnost, že data jsou uložena přímo na čipu karty. V poslední době se společnosti vyvíjející čipové karty snaží hlavně o snížení ceny na minimum a zároveň zvýšení bezpečnosti. Karty se používají převážně v bankovnictví.

Jednou z nevýhod čipových karet je naopak snadná zranitelnost karty, a to hlavně její kontakty, na které působí mnoho vlivů (opotřebení, koroze a nečistoty). [2], [10]

4.4.1 Paměťové karty

Do paměťových karet (používají paměť typu EEPROM) zaznamenáváme nejčastěji citlivá data. Jsou hojně využívány pro specifické aplikace, dost často pro záznam šifrovacích klíčů, algoritmů apod.

Díky využití pro specifické aplikace nejsou paměťové karty příliš flexibilní, avšak jsou velmi levné.

4.4.2 Mikroprocesorové karty

Jak nám název napovídá, jedná se o karty obsahující mikroprocesor, který je připojen k nějakému typu paměti (ROM, RAM, EEPROM). Paměť ROM (Read-Only Memory) obvykle obsahuje operační systém (vyšší programový kód), který je do mikroprocesoru vložen v průběhu výroby. Je stejný pro všechny karty z dané série

a nelze jej později změnit. Mikroprocesorové karty s pamětí EEPROM (Electrically Erasable Programmable Read-Only Memory) obsahují aplikační data a prostor zápis dat do rezervované části paměti, která se dá několikanásobně přepsat. Dalším typem paměti je typ RAM (Read And Memory), která je u mikroprocesorových karet využívána převážně jako dočasná a dá se několikanásobně přepisovat. Informace uchovává pouze při aktivním napájení.

V moderních systémech čipových karet je možná integrace několika aplikací na jedné kartě, bavíme se tak o multi-aplikačních čipových kartách.

Mikroprocesorové čipové karty jsou používány především v aplikacích citlivých na bezpečnost. Nejčastěji se s nimi setkáváme ve formátu SIM (Subscriber Identity Module) karet do mobilních GSM telefonů a nových typů platebních karet.

4.5 RFID systémy

Systémy RFID úzce souvisí s čipovými kartami. Stejně jako u čipových karet jsou data uložena na elektronickém zařízení - transpondéru. Nejpodstatnější rozdíl je ve výměně dat mezi zařízením a čtečkou. RFID nepoužívají galvanického spojení kontaktů, namísto toho používají magnetické nebo elektromagnetické pole.

RFID systémy vynikají ve většině parametrů ve srovnání s ostatními systémy automatického vyčítání informací. Jsou velmi rychlé, používáním se neopotřebovávají a jsou jen těžko napadnutelné. Ze všech systémů pro vyčítání informací mají nejvyšší hustotu informace a zároveň je možné do nich uložit velké množství dat. [2], [10]

Systémový parametr	Čárový kód	OCR	Hlasové vyčítání	Biometrika	Smart karty	RFID systémy
Množství uložených dat (byty)	1-100	-	-	-	16-64k	16-196k
Hustota dat	Nízká	Nízká	Vysoká	Vysoká	Velmi vysoká	Velmi vysoká
Strojová čitelnost	Dobrá	Dobrá	Obtížná	Obtížná	Dobrá	Dobrá
Čitelnost pro člověka	Omezená	Jednoduchá	Jednoduchá	Těžká	Nemožná	Nemožná
Vliv nečistot/vlhkosti	Velmi náchylný	Velmi náchylný	-	-	Možný zkrat	Žádný vliv
Náchylnost na optické překrytí	Totální selhání	Totální selhání	-	Možné	-	Žádný vliv
Náchylnost na směr a pozici při čtení	Nízká	Nízká	-	-	Nesměrové	Žádný vliv
Degradace	Omezená	Omezená	-	-	Kontakty	Není
Náklady na pořízení	Velmi nízké	Střední	Velmi vysoké	Velmi vysoké	Nízké	Střední
Provozní náklady	Nízké	Nízké	Žádné	Žádné	Střední (kontakty)	Žádné
Neautorizované kopírování/modifikace	Nepatrné	Nepatrné	Možná audio nahrávka	Nemožné	Nemožné	Nemožné
Rychlost čtení	Nízká ~4s	Nízká ~3s	Velmi nízká >5s	Velmi nízká >5-10s	~4s	~0,5s
Maximální vzdálenost mezi poskytovatelem dat a čtečkou.	0-50cm	<1cm (Skener)	0-50cm	Přímý kontakt	Přímý kontakt	0-5m, mikrovlny

Tab. 2. Srovnání jednotlivých typů vyčítání informací. [2]

II. PRAKTICKÁ ČÁST

5 NÁVRH OPTIMÁLNÍHO SYSTÉMU VYČÍTÁNÍ INFORMACÍ, UMÍSTĚNÍ ČTEČEK I KÓDŮ RFID

Při návrhu nového systému založeného na RFID si pokládáme mnoho otázek, které je třeba zodpovědět, aby výsledek zavedení nové technologie byl co nejpříznivější.

Použití RFID nemusí být ve všech případech a oblastech přínosem. Obecně platí, že RFID systém můžeme nasadit pouze v případech, kde jsou dobře definované a zvládnuté procesy.

Původní myšlenkou pro použití RFID bylo jejich masivní nasazení v obchodních řetězcích a nákupních centrech. Důvodem bylo hlavně zjednodušení logistiky. Ideálním modelem by tak byla například situace, kdy kamion naložený zbožím s RFID tagy, dorazí do zásobovacích prostor nákupního centra a brána (RFID čtečka) načte všechny tagy v co nejkratším čase.

Každá implementace RFID si tedy žádá individuální přístup a je třeba volit vhodné typy tagů, čtecích zařízení, často také tyto typy kombinovat anebo použít společně s čárkovým kódem.

5.1 Návrh implementace RFID

Při zavádění nového sytému musíme dbát na několik důležitých bodů, které je třeba dodržet. Pokud si předem stanovíme své cíle, můžeme lépe dosáhnout představy o potřebných vlastnostech čipů, čteček a dalších komponent systému. Správné stanovení cílů nám pomůže udržet představu o tom, co je opravdu důležité.

Dále je nutné se připravit na změny procesů, které použití RFID zasáhne. Zároveň s použitím nového systému vznikne mnoho nových procesů, na které je nutné se připravit. Jedná se například o zavedení značení, čtení čipů nebo zpracování dat.

5.1.1 Uplatnění systému

V této počáteční fázi návrhu systému je úkolem definovat cíl, kretrého chceme implementací dosáhnout. Aplikujeme systém tedy na konkrétní situaci. Definujeme například, že potřebujeme sledovat produkt putující distribučním řetězcem, pozorovat materiál ve výrobě až po finální produkt, určit polohu konkrétní věci v konkrétním čase, nebo se pouze snažíme navýšit bezpečnostní standarty. Při definici uplatnění systému

dokážeme určit, co je třeba značit. Bude-li se jednat o jednotlivé produkty, celá balení, palety obsahující dané množství produktů anebo vše zvlášť.

5.1.2 Analýza prostředí

Díky analýze prostředí, v němž budeme systém zavádět, můžeme předejít spoustě problémům. Analýza nám pomůže identifikovat možné problémy spojené s radiofrekvenční komunikací a potencionální elektromagnetické rušení. Budeme také schopni určit rozmístění antén pro čtení, a tím pokrytí RF vln, rozvedení kabeláže a možnosti napájení jednotlivých prvků. Zjistíme také požadavky na vybavení a optimální rozmístění dalších potřebných komponentů. Určíme přesné polohy čtecích zón a míst zpracování dat. Dále si určíme množství, případně i jaká data budeme na tagy ukládat.

Během analýzy je vhodné zjistit, jakým stávajícím technickým vybavením prostory disponují a zda by bylo možné jej využít v kombinaci s nově zaváděnou technologií. Například můžeme využít stávající bezdrátové infrastruktury pro využití RTLS technologie s aktivními čipy k určení polohy palet ve skladu.

Po dokončení základní analýzy cílů a prostředí, určení potřebného pokrytí a dalších komponentů můžeme začít s určováním ostatních faktorů. Mezi tyto faktory řadíme typy a množství použitých tagů, čtecích zařízení, antén a čtecích zařízení.

5.1.3 Výběr tagů

Za pomocí analýzy jsme si přiblížili, jaký typ tagu budeme přibližně pro naši implementaci potřebovat resp., co od něj očekáváme. V dnešní době existuje mnoho typů, a proto je vhodné tagy vybírat dle třech základních kritérií: cena, velikost a výkon.

V případě, že budeme využívat pasivních čipů, hlavními kritérii budou převážně cena a velikost. Cena pasivních čipů za několik posledních let rapidně klesla. Podařilo se to díky optimalizaci výrobních procesů, technologického vývoje, standardizace, ale převážně díky množství dnes produkovaných čipů. Právě díky nižším nákladům na kus je možné vytvářet úspory ve výrobě.

Velikost tagu úzce souvisí s předmětem, na který bude umístěn, ale také na materiálu, z něhož je předmět vyroben. Musíme si také uvědomit, že menší tagy dosahují nižší citlivosti a menším dosahem čtení. V dnešní době je možné využít moderní křemíkové tagy s výkonnou anténou, které i při velmi malé velikosti dosahují vysokých

výkonů. Cena a velikost tagu spolu nijak nesouvisí. Menší tag neznamená levnější, spíše naopak.

Výkon je u RFID tagů také velmi důležitým faktorem. Například při značení vagonů je třeba číst tagy až ze vzdálenosti několika desítek metrů. Zde se nejčastěji využívají tagy s vysokou citlivostí a velkým dosahem čtení. S výkonem souvisí také materiál předmětu, na nějž je tag připevněn. Například při značení palet produktů s vysokým obsahem vody budeme muset volit tagy s nejvyšším výkonem a citlivostí. Můžeme se také setkat s materiály způsobujícími rozladění antény RFID tagu, a tím posunutí pracovní frekvence, což má za následek nižší výkon. V takovýchto případech je nutné volit tagy s velkou šířkou frekvenčního pásma (většinou v rozmezí 860-960MHz).

Při výběru tagu je také důležitým faktorem, jakým způsobem bude na požadovaný předmět připevněn. Nejpoužívanější metodou je dnes tzv. „slap and ship," a to převážně kvůli nízkým nákladům na pořízení. Pro tisk tagů stačí obyčejná stolní programovací tiskárna. Takto vytištěný štítek poté ručně nalepíme na produkt. Při aplikaci je třeba zvýšeně pozornosti. Sice se použitím tohoto systému tisku štítků ušetří na prvotních investicích do vybavení, ale naopak se zvýší náklady spojené s obsluhou. Navíc je tento postup nejčastěji až na konci výrobního či balícího procesu. Firma tak přichází o cenné informace o výrobním procesu a vnitřních návratností investic. S řešením těchto problémů přichází automatizovaný proces označování. Původní investice jsou vyšší, avšak docílíme snížení nákladů na obsluhu, a získáme tak přesné označování na stále stejném místě. Díky přesnému označení dosáhneme často i spolehlivějšího a snadnějšího čtení, což vede k vyššímu výkonu celého systému. Automatizované čtení je také mnohem rychlejší, a nabízí tak řešení například pro zvýšení objemu produkce. [11]

Obr. 21. Příklad automatizovaného značení. [17]

Při použití RFID musíme také dbát na použitý materiál označovaného produktu či jejího balení. Vlastnosti produktu, resp. jeho materiál může velmi ovlivňovat výkon čipu. Například voda v kosmetice, syrovém dřevě, vlhčených ubrouscích a spoustě dalších produktech, díky svým fyzikálním vlastnostem absorbuje RF energii, a snižuje tak výkon RFID čipu. Naopak je tomu u kovových materiálů, kdy při vhodném připevnění tagu na kovový materiál může být součástí tagu a zvýšit jeho výkon.

Zvážit bychom také měli možnosti využití varianty tzv. „Near field“ a „far field“ technologii. Ve variantě „Near field“, neboli blízkého pole, využíváme rychlého oslabování RF vln. Tento typ se velmi dobře hodí například pro čipové karty ke kontrole přístupu, díky malému dosahu RF vln tak nedochází k rušení kartami, které jsou v blízkosti. Můžeme se zde řídit obecnou poučkou, že čtecí vzdálenost je limitována přibližně jednou vlnovou délkou. Jedna vlnová délka u UHF má délku zhruba 30 cm. U druhé varianty tzn. „far field“ využíváme vzdáleného čtení spíše pro čtečky balíků a palet. Volba správné varianty opět závisí na konkrétním případu. [11]

5.1.4 Správné umístění tagu

Pokud se vrátíme k parametrům a vlastnostem RFID tagů, tak jsme se dozvěděli, že není potřebná přímá viditelnost mezi čtečkou a tagem. Dále jsme se dozvěděli,

že se můžeme setkat s materiály, které mohou RF signál oslabovat a jiné naopak při správném použití zesílit. Proto je důležité správné umístění tagu na označovaném produktu. Budeme-li umisťovat tagy na spodní stranu krabic, pak velmi záleží na obsahu balíku. Pokud bude balík obsahovat velké množství vody, je důležité tak zajistit, aby byl čip přímo mezi čtecím zařízením a produktem.

Obecně také platí, že pro spolehlivé čtení je vhodné umístit antény čtečky stejným způsobem jako antény tagů. Tímto pravidlem se zejména řídíme u lineárně polarizovaných antén. Musíme pak dodržet správnou horizontální či vertikální polarizaci.

Dalším doporučením je značit jednotlivé balíky na paletě asymetricky, jednoduše řečeno vyhýbat se středu balíku. Pokud se na balík dostanou dva a více tagů, může jeden čip překrývat druhý a vznikat stínění. Avšak i tento problém má své řešení za pomoci RFID tagů na bázi křemíku s jinými druhy antén. [11]

5.1.5 Optimalizace parametrů čteček

Stejně jako většina moderních zařízení, tak i čtečky RFID nabízejí spoustu předdefinovaných režimů a osobních nastavení. Tyto možnosti nám nabízí nejnovější protokol EPC druhé generace.

Zpravidla nám bude dostačovat základní nastavení předdefinované výrobcem. Pokud jsme nuceni některé z parametrů doladit, je třeba být velmi dobře seznámeni s konkrétním přístrojem, aby nedošlo ke zhoršení výkonu namísto zlepšení.

Správný výběr čtečky je velmi důležitý a může velmi ovlivnit další náklady spojené s nepřesným čtením apod. V dnešní době existuje celá škála druhů a modelů od řady výrobců. Je proto důležité se poradit se specializovanou firmou, která má s touto problematikou bohaté zkušenosti. Nemůžeme se spoléhat pouze na dobré hodnocení čtečky, ale musíme vzít v potaz, jak se bude čtečka chovat v našem požadovaném prostředí. Dodržením všech těchto kroků můžeme dosáhnout snížení množství transferů v síti, a vylepšit tak výkon celého sytému.

5.1.6 RF rušení

Při implementaci nového systému je nutné také důkladně zvážit, v jakém frekvenčním pásmu budeme systém provozovat. Zejména se jedná o vzájemné rušení čtecích zařízení, rušení WiFi signálem bezpečnostního systému nebo jiných přístupových bodů.

Musíme tedy správně rozmístit jednotlivé prvky tak, aby k rušení nedocházelo. Musíme brát také zřetel, abychom naopak naším systémem nerušili ostatní technologie v podniku již nasazené. Pokud je umístění několika čtecích zařízení na malém prostoru nevyhnutelné, můžeme použít čtečky s tzv. hustým čtením. Husté čtení umožnuje čtečkám přeskakovat po jednotlivých kanálech v konkrétním frekvenčním spektru. Při čtení čtečky naslouchají, zda se zrovna ve stejném čase v jejím okolí vyžadovaný kanál již nepoužívá a je-li volný, tak je použije. V opačném případě zvolí následující a provede stejnou kontrolu.[11]

Vhodným rozmístěním a volbou různých typů komponent lze proto dosáhnout snížení rušení a snížit nebezpečí neoprávněného čtení.

5.1.7 Volba antén

Budovy, zdi, podlaží a okolní prostředí ovlivňuje výkon antén, jejich zaměření a cílení radio-frekvenční energie. Běžně se setkáváme se čtyřmi typy antén.

• **Lineárně polarizované antény** jsou vhodné v případech kdy je možná kontrola orientace tagů. Jsou díky svému výkonu vhodné i pro vzdálenější čtení.

• **Kruhově polarizované antény** nedosahují sice takového výkonu jako lineární antény, ale není nutná kontrola orientace tagu. Proto jsou v těchto případech hojně využívány.

• **Yagi antény** se v běžné praxi nepoužívají. Jsou sice velmi výkonné, ale mají velmi úzký úhel vyzařování, a jsou proto vhodné pro vzdálenější čtení.

• Posledním typem jsou tzv**. close-coupled antény**, které jsou určeny do prostředí s velkým počtem tagů na malém místě. Soustřeďují RF energii pouze do blízkého okolí čipu.

Často se setkáváme v praxi také s potřebou zjistit vzdálenost tagu od antény. Zde jsou vhodné antény s nezávislým nastavením výkonu. Pokud na takové anténě nastavíme tři různé intenzity výkonu čtení, můžeme číst tři rozdílně vzdálené tagy. [11]

5.1.8 Školení nového systému

Pokud se podnik rozhodl implementovat RFID technologii pro zjednodušení a zefektivnění logistiky či jiného typu evidence zboží, měl by mít v tuto chvíli jasno, co od nové technologie může očekávat a jakým způsobem se bude technologie zavádět. Společnost může za pomoci vlastních sil a proškolených zaměstnanců implementovat

technologii sama. To však sebou může nést již zmíněné problémy. V ideálním případě firma naváže kontakt s dodavatelskou společností, která kompletaci systému a jeho zprovoznění kompletně zajistí.

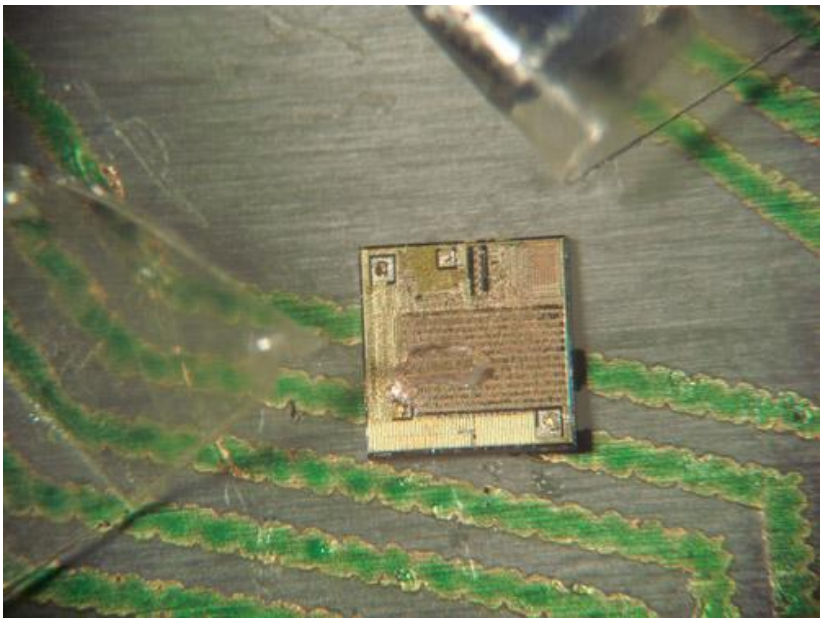
Pokud máme v podniku alespoň z části systém zaveden, je nutné jej testovat. Samotné testování by mělo probíhat na pestrém vzorku produktů. Měly by být otestovány všechny možné situace, které za provozu mohou nastat. Pro správné otestování systému je nutné zaškolit všechny pracovníky, kteří s ním přijdou do styku.

6 ZABEZPEČENÍ PROTI ZNEUŽITÍ A VYŘAZENÍ Z PROVOZU

V této kapitole bych se rád věnoval nejznámějším metodám pro zneškodnění a vyřazení z RFID čipů z provozu. Existuje několik cest jak zničit RFID čip. Jednou z běžných možností jak čip vyřadit z provozu, nám nabízejí i samotné čtečky tagů. Obsahují zařízení zvané RFID deaktivátor. Toto zařízení nastaví RFID čip do režimu spánku. Samotný čip takto samozřejmě nezničíme. Čip může být znovu probuzen (pochopitelně i bez vědomí vlastníka produktu s tímto čipem).

V následujících kapitolách se zmíním, jak je možné za pomocí jednoduchých metod úplně zneškodnit RFID tag. Existuje celá škála možností, jak spolehlivě zničit RFID tag.

Jde například o metody jako je přestřižení, přeříznutí antény, záměna RFID čipů mezi různými produkty. Dále snahy o zastínění cívky čipu za pomoci hliníkových fólií, zničení v mikrovlnné troubě, ale také s komplexnější a hůře zjistitelnou metodou zničení za pomocí EMP (Electro Magnetic Pulse). Nejčastěji se setkáváme se snahami zničit RFID při drobných krádežích v obchodních domech.



Obr. 22. RFID čip oddělený od antény. [12]

6.1 Fyzické zničení tagu

Fyzické zničení tagu je jednou z nejčastějších příčin vyřazení tagu z provozu. Při špatné aplikaci tagu se může stát, že neopatrným zacházením poškodíme cívku tagu,

a ten se tak stává nefunkčním. Často se také setkáváme s poničenými čipy úmyslně. Například prořízlý anténní systém, nebo jinak poničený tag za úmyslem krádeže. Takto poničený tag není již možné detekovat.

Předejít fyzickému poničení můžeme docela lehce, a to aplikací tagů na nedostupná místa. Například dovnitř krabice, sklenice nebo pod plastové kryty produktu. Takové značení je poté v kompetenci výrobce daného produktu. Například pokud RFID tag vložíme dovnitř obalu CD, tak máme jistotu, že nebude mechanicky poškozen, dokud nebude krabička otevřena.

6.2 Elektromagnetický impulz (EMP)

V blízké budoucnosti očekáváme prudký nárůst RFID tagů a dá se říct, že jimi budeme obklopeni na každém kroku. RFID má řadu výhod, ale i nevýhod (ty byly zmíněny v předchozích kapitolách). V budoucnosti bude nutné vytvořit jisté standarty pro ochranu soukromí zákazníků využívajících zboží označené tagy. Je tak vhodné uvažovat o vytvoření zařízení, které dokáže tyto tagy bezpečně zničit, proto vznikla řada projektů, které tento problém řeší propálením RC článku obsaženého v každém tagu. Je to proces, který nevratně zničí cívku i celý RFID čip za pomoci elektromagnetického impulzu. V diskuzních fórech se setkáváme s pracovním názvem „RFID Zapper“, jedná se o podomácku sestrojené zařízení. Toto zařízení neodpovídá a pravděpodobně ani nikdy nebude odpovídat standardům FCC (Federal Communications Commission). Z předešlých důvodů není ani nijak komerčně vyráběn.

Pokud se zaměříme jen na zachování bezpečnosti zákazníků, je vše pořádku, avšak setkáváme se zde s častým využitím při krádežích apod. V praxi se dokonce setkáváme s organizovanými skupinami, které využívají nic netušící nakupující a potají jim vloží do nákupního vozíku zařízení speciálně upravené pro vyzáření EMP.

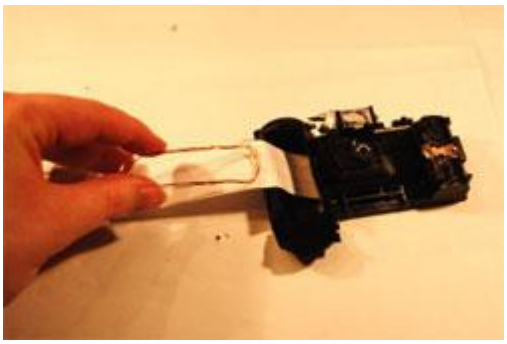
6.2.1 Princip vyřazení RFID pomocí EMP

V předchozích kapitolách jsme se seznámili s tím, že pasivní čipy nemají vlastní napájení a pro jejich funkci je potřeba elektrický proud indukovaný v anténě (cívce) z elektromagnetického pole vytvářeného čtečkou. Takto naindukovaný proud poskytuje dost energie pro CMOS (Complementary Metal–Oxide–Semiconductor) obvod integrovaný uvnitř RFID čipu.

Principiálně se vyřazení za pomoci elektromagnetického výboje podobá běžné aktivaci čipu za pomoci indukce v anténě. Avšak v případě EMP se jedná o krátkodobý a velice silný energetický výboj, který spolehlivě zničí CMOS strukturu čipu navždy.

6.2.2 Podoby EMP

Elektromagnetického impulzu můžeme dosáhnout za pomoci mnoha zařízení k tomu určených. Většina takových zařízení je ale velmi drahých a ne zrovna mobilních. V obchodních řetězcích se bezpečnostní agentury setkávají s několika typy podomácku vyrobenými zařízeními, která jsou schopna vyzářit velmi silný elektromagnetický impulz. Nejčastěji používanými EMP generátory jsou staré kinofilmové fotoaparáty s drobnými technickými úpravami. Kinofilmová cívka je nahrazena cívkou z lakovaného měděného drátu a vhodně umístěna do těla fotoaparátu. Jeden konec cívky je připojen ke kondenzátoru, kde byl dříve připojen blesk, druhý konec ke spínači, který je připojen na druhý pól kondenzátoru. Takové úpravy jsou velmi levné a technicky nenáročné a lze si tak vytvořit zařízení na ničení RFID čipů na tužkové baterie.



Obr. 23. RFID Zapper. [13]

6.2.3 Ochrana před EMP

Ochrana před elektromagnetickými pulzy je možná, avšak velmi nákladná, a nepříliš spolehlivá. Jednou z možností jak se chránit před silnými energetickými výboji, je použití Zenerovy diody mezi anténu a čip RFID tagu. Zenerova dioda nám v tomto případě funguje jako jakýsi proudový regulátor, a tak vysoký energetický výboj udrží a nepropusti až k čipu. Bohužel Zenerovy diody, které by spolehlivě zadržely i velmi vysoké výboje, jsou rozměrné a poměrně drahé pro montáž do většiny RFID tagů.

Další možností jak odhalit EMP, je použití detektoru elektromagnetických zářičů. Bohužel takové zařízení dokáže detekovat až vyzářený pulz. Zjistíme sice, že byl odpálen

elektromagnetický pulz, a nabízí se nám možnost pachatele chytit při činu, avšak většina čipů v okolí bude již zničena.

6.3 Další známé metody vyřazení z provozu

Mezi další metody vyřazení RFID tagů z provozu patří například zastínění čipů pomocí tenké hliníkové fólie (alobal). Takto překrytý čip není schopen přijmout vysílanou energii od čtečky a stává se tak dočasně nefunkční. Moderní čtečky však pokusy o zastínění umí detekovat.

ZÁVĚR

Práce se podrobněji věnuje automatickému vyčítání informací za použití bezkontaktní radiofrekvenční technologie RFID. V jednotlivých kapitolách seznamuje s použitými technologiemi, využití čipů jako nástupce čárových kódů. V krátkosti nás také seznámí s historií RFID tagů. V jedné samostatné kapitole se práce věnuje srovnání s jinými typy automatického vyčítání informací.

V práci se můžeme setkat se zajímavou novinkou v oblasti aktivních RFID tagů, které jsou využívány jako bezpečnostní perimetrický systém střežení plotů, vrat a materiálů. Při použití těchto speciálně upravených čipů dokážeme zabezpečit opravdu velké plochy s mnohem nižšími náklady, než nabízejí jiné typy perimetrického zabezpečení velkých ploch.

V praktické části se práce uvádí návrh optimálního řešení sytému pro vyčítání informací za použití RFID čipu. V jednotlivých krocích je popsáno, kdy je tuto technologii vhodné použít, a následně se analyzuje prostředí, ve kterém má být systém zaveden. V dalších krocích nás práce seznámí svýběrem tagů a jejich správného umístění. Seznámime se s řadou čteček, s jejich optimalizací parametrů důležitých při implementaci. A dále s problémy, které mohou během zavádění tohoto sytému nastat.

Praktická část se také zabývá zabezpečením proti zneužití a vyřazení RFID tagů z provozu. Zmíněny jsou jednoduché metody (roztržení tagu či přelepení), ale také složitější metody vyřazení (zničení RFID tagu přeříznutím antény od čipu, zneškodněním v mikrovlnné troubě či nejkomplexnější metodu zničení tagu pomocí EMP).

SEZNAM POUŽITÉ LITERATURY

[1] PROJECT INVEST, s. r. o. *RFID Portál* [online]. [cit. 2012-03-22]. Dostupné z: http://www.rfidportal.cz

[2] FINKENZELLER, Klaus. *RFID handbook: radio-frequency identification fundamentals and applications*. New York: Wiley, c1999, 304 s. ISBN 04-719-8851-0.

[3] MACHŮREK, Filip. *Radiofrekvenční identifikace RFID a její použití v automatizaci a logistice.* [online]. [cit. 2012-05-25]. Dostupné z: http://www.odbornecasopisy.cz/index.php?id_document=30654

[4] *Systémy pro sledování majetku, zboží a osob v reálném čase.* [online]. [cit. 2012-02-25]. Dostupné z: http://www.barco.cz/?id=produkty&sel=rtls-1#101

[5] *Princip systému PerimetrLocator a detekce pachatele.* [online]. [cit. 2012-03-21]. Dostupné z: http://www.7md.cz/reseni/perimetr-locator/

[6] *Radio-frequency identification*. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2012-03-22]. Dostupné z: http://en.wikipedia.org/wiki/Radio-frequency_identification

[7] BROWN, Dennis E. *RFID implementation*. New York: McGraw-Hill, c2007, 466 s. ISBN 978-007-2263-244.

[8] *Records Management, Document Management & Scanning*. [online]. [cit. 2012-03-21]. Dostupné z: http://www.alliancegroup.co.uk

[9] GLOVER, Bill a Bhatt HIMANSHU. *RFID essentials*. 1st ed. Beijing: O´Reilly, 2006, 260 s. ISBN 05-960-0944-5.

[10] WANT, Roy. *RFID explained: a primer on radio frequency identification technologies*. 1. ed. San Rafael, Calif.: Morgan, 2006. ISBN 15-982-9108-4.

[11] AlienTechnology [online]. 2007 [cit. 2012-03-15]. Common RFID Implementation

[12] *RFID Transplantation*. [online]. [cit. 2012-03-21]. Dostupné z: http://www.bunniestudios.com/blog/?p=1379

[13] *RFID Zapper*. [online]. [cit. 2012-03-21]. Dostupné z: https://events.ccc.de/congress/2005/static/r/f/i/RFID-Zapper(EN)_77f3.html

[14] *Sledování polohy v reálném čase.* [online]. [cit. 2012-03-23]. Dostupné z: http://www.systemonline.cz/it-pro-logistiku/sledovani-polohy-v-realnem-case.htm

[15] EPRIN [online]. [cit. 2011-02-05]. *Obecně čárový kód.,* Dostupné z WWW: <www.eprin.cz/>.

[16] BARCO S.R.O. *Čárové kódy, RFID & RTLS technologie pro automatickou identifikaci, evidenci a lokalizaci majetku, zboží či osob. IT řešení pro skladovou evidenci, mobilitu pracovníků, řízení logistiky, skladů a výroby*." [online]. [cit. 2012-02-23].

[17] *Records Management, Document Management & Scanning*. [online]. [cit. 2012-03-21]. Dostupné z: http://www.alliancegroup.co.uk

[18] *Library RFID Management System*. [online]. [cit. 2012-03-21]. Dostupné z: http://www.rfid-library.com

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AP		Access Point
BAP		Battery Assisted Passive
CCIA		Canadian Cattle Identification Agency
CCTV		Closed Circuit Television
CMOS		Complementary Metal–Oxide–Semiconductor
CRC		Cyclic Redundancy Check
EAN		European Article Number
EEPROM		Electrically Erasable Programmable Read-Only Memory
EMP		Electro Magnetic Pulse
EPC		Electronic Product Code
EZS		Elektronická Zabezpečovací Signalizace
FCC		Federal Communications Commission
GTIN		Global Trade Item Number
HF		High Frequency
ICAO		International Civil Aviation Organization
IP		Internet Protocol
LF		Low Frequency
MW		Microwave
NFC		Near Field Communication
OCR		Optical Character Recognition
POS		Point of Sale
PTZ		Pan Tilt Zoom
RAM		Random-Access Memory
RF		Radio Frequency

RFID		Radio Frequency Identification
ROM		Read-Only Memory
RSSI		Received Signal Strength Indication
RTLS		Real-time Locating Systems
SSCC		Serial Shipping Container Code
TDoA		Time Differenceof Arrival
ToA		Time of Arrival
ToF		Time of Flight
UCC		Uniform Code Council
UHF		Ultra High Frequency
USD		United States Dollar
UWB		Ultra Wide Band
WiFi		Wireless Fidelity

SEZNAM OBRÁZKŮ

SEZNAM TABULEK