Využití RFID v průmyslu komerční bezpečnosti

Using of RFID in the Commercial Security Industry

Vít Kratochvíl

Bakalářská práce
2013

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2012/2013

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

Jméno a příjmení:	**Vít KRATOCHVÍL**
Osobní číslo:	**A10217**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Využití RFID v průmyslu komerční bezpečnosti**

Zásady pro vypracování:

1. **Vypracujte literární rešerši zaměřenou na využití rádio-frekvenčních systémů v průmyslu komerční bezpečnosti.**
2. **V rámci literární rešerše porovnejte rozdíly využití čárových kódů a RFID čipů.**
3. **Zpracujte analýzu kontroly vstupů oprávněných osob do objektu.**
4. **U vybraného typu snímače určeného ke kontrole vstupů do objektu testujte hardwarovou a softwarovou odolnost spolehlivosti.**
5. **Zhodnoťte ekonomickou náročnost implementace nového zařízení pro průmyslové podniky.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **BROWN, Dennis E. RFID Implementation . USA : McGraw-Hill Osborne Media, 2006. 466 s. ISBN 978-0072263244.**
2. **RFID portal. Rfid portál [online]. 2011 [cit. 2013-1-15]. Dostupné z: http://www.rfidportal.cz**
3. **SOMMEROVÁ, Martina. Základy RFID technologií. In: RFID všb Ostrava [online]. 2013 [cit. 2013-01-18]. Dostupné z: http://rfid.vsb.cz/miranda2/export/sites-root/rfid/cs/okruhy/informace/RFID_pro_Logistickou_akademii.pdf**
4. **RFID. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001, last modified on 3.1.2013 [cit. 2013-01-18]. Dostupné z: http://cs.wikipedia.org/wiki/RFID**
5. **CIHLÁŘOVÁ, Pavla. Úvod do EPC global network. In: RFID – EPC [online]. 2013 [cit. 2013-01-18]. Dostupné z: http://www.rfid-epc.cz/download/prezen/RFIDWorkingGroup-EPCglobalNet.pdf**

Vedoucí bakalářské práce: **doc. Mgr. Milan Adámek, Ph.D.**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **25. února 2013**

Termín odevzdání bakalářské práce: **30. května 2013**

Ve Zlíně dne 25. února 2013

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

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

ABSTRAKT

Předložená práce pojednává o problematice rádio-frekvenční technologie, zabývá se jejich využitím, možnostmi aplikací a zejména jejich bezpečností. V úvodu teoretické části seznamuje čtenáře s historií a počátky RFID systémů. Dále jsou pojednány rozdíly mezi aktivními a pasivními RFID systémy. V další části práce rozebírá využitá frekvenční pásma, podává detailní popis komponent RFID, porovnává otázku čárových kódů a RFID. Poslední část teoretického pojednání je zaměřena na využití RFID v průmyslu komerční bezpečnosti.

Praktická část se nejprve zaměřuje na: 1) analýzu přístupového systému v podniku, 2) na použité komponenty, 3) programové vybavení, 4) režimová opatření a 5) nedostatky stávajícího systému. V druhé části je provedena konkrétní analýza vybraného typu snímací jednotky, která zahrnuje testování hardwarové a softwarové odolnosti. Výsledkem praktické části je návrh zlepšení dosavadního systému, analýza odolnosti a ekonomické zhodnocení náročnosti nového systému. Závěr práce tvoří komplexní shrnutí poznatků získaných studiem problematiky identifikačních systémů.

Klíčová slova: RFID, snímač, čip, přístupový systém, bezpečnostní analýza.

ABSTRACT

The work deals with the problem of radio-frequency technology, applications, applications possibilities and their safety. At the beginning of the theoretical part introduces the reader to the history and origins of the RFID systems. Further on, it addresses the differences between active and passive RFID systems. The next section of the chapter discusses frequency bands, gives a detailed description of RFID components, compares to barcodes and RFID. The last part focuses on the use of RFID in commercial security industry.

The practical part in the first part contrentates: 1) on the analysis of the access system in the enterprise, 2) the used components, 3) software, 4) routine measures and 5) shortcomings of the current system. The second part is an analysis of the selected type sensor unit, which includes hardware and software testing resistance. The final part deals with the practical improvement of the existing system design, analysis and economic

evaluation of the durability performance of the new system. In the conclusion there is a summary of experience gained in studying the issue of identification systems.

Keywords: RFID, sensor, chip, access systém, security analysis.

Poděkování:

Touto formou bych rád poděkoval panu doc. Mgr. Milanu Adámkovi, Ph.D. za vedení práce, poskytnutí odborných konzultací a pomoci při tvorbě bakalářské práce. Dále svým rodičům za jazykové i technické konzultace a poznatky, které výrazně přispěly k mé vlastní práci.

Vít Kratochvíl

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/a jsem seznámen/a 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 …….……

podpis diplomanta

OBSAH

ÚVOD **10**
I TEORETICKÁ ČÁST **12**
1 RFID SYSTÉM **13**
1.1 HISTORIE RFID 14
1.2 AKTIVNÍ RFID SYSTÉM 17
1.3 PASIVNÍ RFID SYSTÉM 18
1.4 EFEKTIVITA FUNGOVÁNÍ RFID SYSTÉMU 19
1.5 ZPŮSOBY KOMUNIKACE 19
2 FREKVENČNÍ PÁSMA RFID **20**
2.1 LF PÁSMO 21
2.2 HF PÁSMO 21
2.3 UHF PÁSMO 21
2.4 MW PÁSMO 22
3 KOMPONENTY RFID **23**
3.1 RFID TAG 23
3.1.1 Členění podle výrobní technologie 25
3.1.2 Dělení podle typu paměti 28
3.2 SNÍMAČ 29
3.2.1 Komponenty snímače 29
3.2.2 Druhy snímačů 29
3.3 MIDDLEWARE 31
3.4 PŘÍSLUŠENSTVÍ 31
4 ČÁROVÝ KÓD **32**
4.1 PRINCIP ČINNOSTI 32
4.2 SROVNÁNÍ ČÁROVÝCH KÓDŮ S RFID 33
5 VYUŽITÍ RFID V KOMERČNÍ BEZPEČNOSTI **34**
5.1 PŘÍSTUPOVÝ A DOCHÁZKOVÝ SYSTÉM 34
5.2 ZÁKLADNÍ FUNKCE PŘÍSTUPOVÉHO SYSTÉMU 35
5.3 INTEGRACE RFID S BEZPEČNOSTNÍMI SYSTÉMY 35
II PRAKTICKÁ ČÁST **37**
6 ANALÝZA KONTROLY VSTUPŮ **38**
6.1 ANALÝZA POUŽÍVANÉHO SYSTÉMU 38
6.1.1 Kontrola vstupů 39
6.1.2 Hardwarové a softwarové vybavení systému 39
6.1.2.1 Turnikety a elektrické dveřní zámky 39
6.1.2.2 Transpondéry 41
6.1.2.3 Terminály a snímače 41
6.1.2.4 Programové vybavení 43
6.1.3 Režimová opatření 44
6.1.4 Nedostatky stávajícího systému 44
7 ANALÝZA SNÍMAČE **45**

7.1 CHARAKTERISTIKA SNÍMAČE 45
7.2 HARDWAROVÁ ODOLNOST 46
7.2.1 Průnik metodou propojení svorkovnice 46
7.2.2 Průnik metodou elektromagnetického impulsu 48
7.3 SOFTWAROVÁ ODOLNOST 48
8 NÁVRH IMPLEMENTACE NOVÉHO RFID ZAŘÍZENÍ 49
8.1 ANALÝZA RIZIK NOVÉHO SYSTÉMU 50
8.2 EKONOMICKÉ ZHODNOCENÍ 50
ZÁVĚR 51
ZÁVĚR V ANGLIČTINĚ 52
SEZNAM POUŽITÉ LITERATURY 53
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK 56
SEZNAM ZOBRAZENÍ 58
SEZNAM TABULEK 59

ÚVOD

Rádio-frekvenční identifikační systémy (dále RFID) jsou v dnešní době neodmyslitelnou součástí každodenního života. Člověk, aniž by si uvědomoval, se s RFID potýká každý den v mnoha odvětvích a situacích. Při otevírání garážových vrat, vstupu do knihovny, učeben, laboratoří, při parkování nebo při obyčejném nakupování. Ať už chceme nebo ne, s RFID jsme neustále konfrontováni.

Zkratka RFID pochází z anglického slova „*Radio frequency identification*“ a představuje jeden z nejrozšířenějších principů identifikace, který je založen na bezdrátovém přenosu identifikačního čísla nebo dat prostřednictvím elektromagnetických rádiových vln [3]. Je tedy pochopitelné, že zásadní otázkou u těchto systémů je rozvoj jejich dalšího komplexnějšího využití.

Při vývoji aplikací systému je vždy třeba dbát na dodržení vysokého standardu, který zahrnuje soubor vlastností, jakými jsou především, kompaktnost a spolehlivost a v neposlední řadě jednoduchost obsluhy u koncového uživatele. Tyto faktory jsou pro spotřebitele důležitými prvky. Budeme-li hovořit o aplikaci RFID v oblasti čipových karet, elektronických peněženek nebo klíčenek, komfort, kompatibilita a jednoduchost jsou klíčovou prioritou. Karty nebo klíčenky, se kterými se setkáváme nejčastěji, musí vyhovovat každodennímu používání po řadu let. Koncový uživatel – senior i dítě předškolního věku – si se systémem musí být schopen poradit.

Problematika identifikačních karet a klíčenek je využívána rovněž v oblasti docházkového nebo přístupového systému pro kontrolu vstupu oprávněných osob do objektů. V průmyslu komerční bezpečnosti je zejména tento prvek zabezpečení využíván při aplikaci elektronického zabezpečení objektů.

Je známo, že RFID čipy jsou dnes jedny z nejbezpečnějších prostředků uchovávání dat. Avšak i naše okolí se vyvíjí velkou rychlostí a hrozba zcizení nebo poškození dat, ztráty naší identity, zvláště pokud se jedná o čipy bez kryptografických opatření nebo čipy s nízkou bezpečnostní ochranou, se zvyšuje. Do budoucna lze očekávat nástup technologie RFID při úřední identifikaci osob, např. v občanských průkazech a pasech nebo aplikací čipu intradermálně, tj. pod kůži člověka. Extrémní fikce dokonce spekulují o aplikacích čipů do mozku a získání možnosti čtení myšlenek nebo utváření snů.

Bezkontaktní identifikační systémy jsou zajímavou součástí i mého života, proto jsem se rozhodl právě jim věnovat pozornost při volbě tématu práce, která se zabývá otázkou teorie RFID a jejího využití v průmyslu komerční bezpečnosti. Výstupem práce bude komplexní analýza konkrétního RFID systému, otestování jeho hardwarové a softwarové odolnosti a zhodnocení implementace nového zařízení.

I. TEORETICKÁ ČÁST

1 RFID SYSTÉM

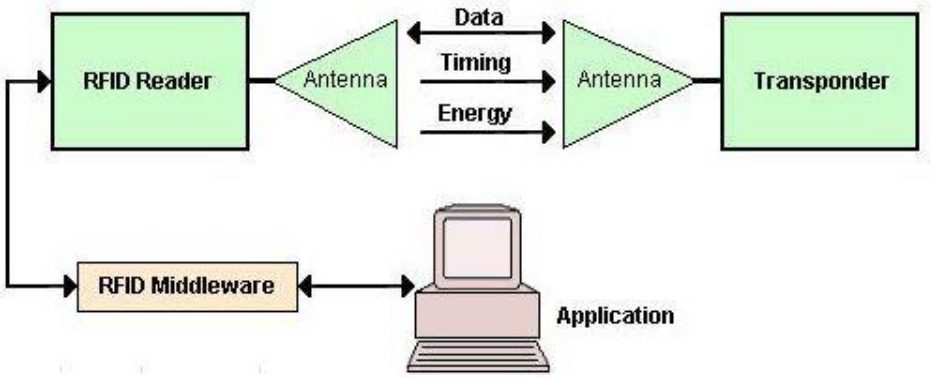
Rádio-frekvenční identifikace nebo RFID (z anglického označení Radio Frequency Identification), je bezkontaktní automatická identifikace sloužící k přenosu a ukládání dat pomocí elektromagnetických vln. Systémy jsou na základě elektromagnetického přenosu schopny

- zaznamenávat informace,
- uchovávat informace,
- poskytovat informace o objektech v reálném čase [1].

Tato technologie je využívána v mnoha odvětvích průmyslu. Například v logistice, lékařství, obchodních řetězcích, stravovacích, docházkových nebo přístupových systémech, ale i při platebních úkonech.

Mezi největší výhody RFID patří

- bezkontaktní technologie, která pro svou činnost nevyžaduje přímou viditelnost (jako je tomu u infračerveného přenosu dat),
- vysoká odolnost RFID čipů proti vlhkosti, teplotě, atmosférickým jevům, opotřebení,
- rychlost čtení dat (většinou kolem 100 milisekund),
- mobilita – výhodou je snadná manipulace díky velikosti čipů,
- možnost identifikace přes vrstvy různých materiálů (včetně kovů),
- ekonomická stránka daná cenou čipu.



Obr. 1**:** *Obecné schéma RFID* [9]

Základní systém se skládá ze tří komponentů, kterými jsou

- **anténa,**
- **přijímač a vysílač,**
- **nosič informace** (elektronicky programovatelný čip).

Přijímač resp. vysílač vysílá prostřednictvím antény rádiové signály, které aktivují čip a ten následně provede zápis nebo čtení dat. Snímač (také *čtečka* či *reader*) je elektronické zařízení (obsahující přijímače integrované s anténami) sloužící ke komunikaci s čipy. Transpondér je tvořen čipem, který je základním nosičem informace a anténou pro komunikaci se snímačem. Poslední základní součástí k funkčnosti celého systému je softwarové vybavení (tzv. *middleware*), které filtruje a překládá data pro použití v informačním systému (*řídící počítače, databáze, telekomunikační sítě*) [1], [2].

1.1 Historie RFID

Předpokladem pro vytvoření RFID systému byl vznik dvou důležitých technických prvků - radaru a rádiové komunikace.

Jeden z klíčových okamžiků nastal v roce 1906 v USA, kde se pomocí zaměstnance společnosti *General Electric* Ernsta Alexandersona ozvalo první rozhlasové vysílání o frekvenci 75 kHz. Frekvence užitá při tomto rozhlasovém vysílání byla více než tisíckrát větší, než se v té době běžně používalo. Díky tomu bylo vysílání slyšitelné až v Karibském moři [4].

Za skutečné objevení RFID technologie lze však považovat teprve konec třicátých a počátek čtyřicátých let 20. století. V roce 1935 skotský fyzik sir Robert Alexander Watson-Watt vynalezl radar. Je známo, že rádiové vlny po střetu s překážkou se vrátí zpět do místa vzniku, čímž je možné lokalizovat a detekovat objekt. Armády si v tehdejší bouřlivé době velmi rychle uvědomovaly význam radaru, a investovaly mnoho prostředků do rozvoje této technologie. Způsobem radarové detekce bylo tedy možné zachytit letadla na obloze, i když byla ještě na kilometry vzdálená. Problém však nastal při identifikaci letadel. Nebyl znám způsob, jak zjistit, která letadla patřila nepříteli, a která letadla vracející se z mise byla vlastní. Němečtí vojenští odborníci zjistili, že získávají poněkud odlišný signál, když vracející se letadlo provede otočku kolem podélné osy. Tato metoda upozornila obsluhu radaru, že se nejedná o spojenecké letadlo. Byl to vlastně první způsob identifikace – první

pasivní prvek RFID systému. Mezitím podle Watson-Watta (vedoucího tajného britského projektu) vyvinuli Britové první aktivní identifikační prvek, kterým bylo možné identifikovat spojenecká letadla. Do každého britského letadla byl zabudován vysílač, což vedlo k okamžité identifikaci v pozemních rádiových stanicích, a objekt byl snadno identifikován jako vlastní letadlo. Můžeme říci, že RFID systém je ve všech aplikacích dodnes založen na stejném konceptu. Signál je odeslán do transpondéru, který se oživí, a buď signál odráží zpět (pasivní systém) nebo vysílá signál sám (aktivní systém) [5].

V 50. a 60. letech po ukončení války pokračoval vývoj rádio-frekvenčních systémů velkými kroky. Vědci v Japonsku, USA a Evropě prováděli výzkum, jak by rádio-frekvenční energie mohla být použita pro identifikaci objektů na větší vzdálenosti. Obchodní společnosti začaly využívat RFID proti krádežím s pomocí tzv. EAS systému (*Electronic article surveillance*). EAS je technologie sloužící pro odhalování krádeží v obchodních řetězcích s použitím tagů. Na každé zboží byl připnut jednobitový tag, který byl schopen vyslat pouze 1 nebo 0. V případě, že zákazník zboží zaplatil, pokladní tag deaktivoval, čímž umožnil zákazníkovi odejít bez narušení. V případě, že pokladní tag nedeaktivoval, při průchodu kolem detektoru byl spuštěn alarm.

V této době docházelo k udělování patentů. Roku 1973 Mario W. Cardullo obdržel první americký patent pro aktivní RFID tag s přepisovatelnou pamětí. Tentýž rok získal patent Charles Walton na pasivní transpondér, který umožňoval odemykání dveří bez klíče. Pasivní transpondér (v podobě karty) vyslal signál do čtečky na dveřích. Čtečka vyhodnotila platnost a číslo průkazu uložené v RFID tagu a v případě ověření totožnosti vpustila majitele transpondéru dovnitř [5].

V 70. a 80. letech se prohluboval vývoj technologie RFID a docházelo ke stále větší integraci RFID s komerčním průmyslem. V roce 1970 byla společnost Los Alamos National Laboratory (významné centrum pro vývoj RFID) požádána Ministerstvem energetiky USA o vývoj systémů pro sledování jaderných materiálů. Jiná skupina vědců přišla s konceptem uvedení transpondéru do kamionů a čtecím zařízením v podobě bran. Anténa v bráně aktivuje transpondér v kamionu a získá tak informace např. o zásilce nebo o řidiči. Systém byl aplikován kolem roku 1980, kdy zaměstnanci pracující na projektu v Los Alamos založili novou společnost pro rozvoj automatizovaných systémů mýtného, který se dodnes široce používá na dálnicích, tunelech či mostech na celém světě.

Žádosti o implementaci RFID systémů přicházely také z řad amerického Ministerstva zemědělství. Los Alamos National Laboratory přišla s pasivním prvkem RFID systému, který využívá UHF (*Ultra-high frequency*) rádiové vlny, a který byl využit pro identifikaci krav. 80. léta představovala širokou škálu implementace RFID do komerční oblasti. Na americkém kontinentu se více prosazoval systém v dopravě a bezkontaktních vstupech do objektů. V Evropě byl spíše kladen důraz na aplikace v zemědělském odvětví, ale později i v dopravě. Postupem 90. let se rozvíjely RFID systémy ve frekvenční oblasti do 125 kHz a postupně se přesunuly do rádiového spektra na vysoké frekvenci (13,56 MHz), které do té doby nebylo globálně využito. Vysoká frekvence zajistila v prvé řadě vyšší přenosovou rychlost [5].

V dnešní době se frekvenční spektrum 13,56 MHz komerčně využívá v oblasti platebních systémů a bezkontaktních čipových karet, ale také v oblasti bezpečnosti řízení vstupů a bezpečnostních systémů proti krádeži aut. Roku 1990 byl vyvinut a patentován UHF systém společností *IBM*. UHF umožnil rychlejší přenos dat a větší dosah. Systém byl testován společně se společností *Wal-Mart*, ale nikdy nedošlo k jejímu komerčnímu využití. V tomtéž roce společnost *IBM* přišla do krize a prodala své patenty společnosti *Intermec*, která byla zaměřena na aplikaci čárových kódů [5].

Změna nastala v roce 1999, kdy byl zaznamenán nárůst zájmu o UHF RFID technologie. Společnost *Uniform Code Council* investovala prostředky na vybudování *Auto-ID center* na *Massachussets Institute of Technology*. V tomto centru probíhal vývoj levných vysokorychlostních čipů. Čipy měly sloužit ke značení výrobku tak, aby mohly být po celou dobu sledovány. Profesoři David Brock a Sanjay Sarma provedli výzkum v možnostech využití levných RFID tagů na všechny výrobky. Jejich nápad spočíval v pouhé aplikaci sériového čísla na štítek. Tím Brock se Sarmou ušetřili náklady na výrobu - jednoduchý mikročip s malou kapacitou je několikanásobně levnější než složitý čip s více paměťmi. Sériová čísla byla uložena v databázi, ke které byl neustálý přístup přes internet. Tito výzkumníci naprosto změnili náhled veřejnosti na RFID systémy. Propojili RFID s internetem, což pro obchodníky znamenalo obrovskou změnu. Nyní mohli totiž sledovat cestu svého výrobku. V letech 1999 až 2003 *Auto-ID center* získalo podporu více než 100 velkých společností včetně amerického Ministerstva obrany nebo důležitých RFID dodavatelů. Došlo k otevření výzkumných laboratoří v Austrálii, Švýcarsku, Velké Británii a Japonsku.

Byly vyvinuty dva protokoly mezi RFID tagem a čtečkou (Class 0 a Class 1), soubor pravidel pro přidělování elektronického kódu (*Electronic Product Code* – EPC) a také systém vyhledávání produktu prostřednictvím internetu.

V dnešní době se usiluje o vyvinutí systému použitelných globálně na celém světě bez jakéhokoliv rizika. Cílem je vyvinout takový RFID systém, který bude levný a kompatibilní se všemi obchodními řetězci. Mnoho obchodních řetězců zveřejnilo své plánování využití EPC technologie pro kontrolu pohybu zboží v dodavatelských i odběratelských řetězcích [5].

1.2 Aktivní RFID systém

Aktivní RFID systém je charakterizován podle aktivního čipu. Tag má schopnost periodicky vysílat signály do okolí, tzv. funkce TTF (*Tag talk first*). Aktivní tagy využívají systému RTLS (*Real time location system*), což je možnost sledování a komunikace s tagem v okamžitém čase. Energii získává z miniaturní baterie uložené v čipu, která má životnost 1-5 let [8]. Doba životnosti baterie závisí na aktivitě čipu. Čip může vysílat signál každou vteřinu, nebo také jednou za den. Čím méněkrát bude čip svůj signál vysílat do okolí, tím déle baterie vydrží. U aktivních systémů nejde pouze o identifikaci předmětů, ale i o další funkce (např. lokalizaci nebo měření teploty). Standardně se používají tagy, které pracují na frekvencích 455 MHz, 2,45 GHz nebo 5,8 GHz. Aktivní čipy mají schopnost čtení až 100 m. Nevýhodou těchto čipů je jejich pořizovací cena a oproti pasivním tagům i větší velikost. Výhodou je silnější signál, a proto je možné komunikovat na delší vzdálenosti. Typickým příkladem využití je sledování distribuovaného zboží (kontejnerů, aut, vagónů). Cena aktivního tagu se pohybuje v rozmezí 200-1000 Kč. Záleží na velikosti kapacity baterie nebo velikosti paměti čipu [7].

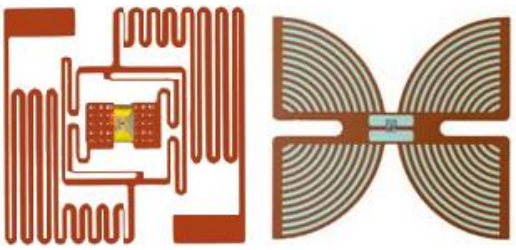
Obr. 2: *Aktivní tagy RFID* [6]

1.3 Pasivní RFID systém

Pasivní RFID systémy a čipy, na rozdíl od aktivních, nemají žádný zdroj energie ani vysílač. Jsou tedy plně závislé na dodávce energie z antény čtecího zařízení. Čtečka šíří pomocí antény elektromagnetické pole, které slouží jako zdroj energie pro RFID tag a zároveň také jako komunikační kanál [1]. Cena pasivního tagu je mnohem nižší (3-8 Kč). Další výhodou pasivního tagu je skutečnost, že nevyžaduje žádnou údržbu, což je jeden z důvodů, proč obchodníci neustále hledají způsoby, jak pasivní tagy využít v dodavatelském řetězci. Důsledkem absence vysílače je kratší čtecí dosah (uvádí se několik centimetrů). Pasivní RFID transpondér se skládá z mikročipu připojeného k anténě a může být vyroben v mnoha různých způsobech zapouzdření, např. jako klíčenky, čipové karty, papírové štítky nebo náramky. Výběr vhodného transpondéru pak závisí na druhu aplikace. Navrhuje se tak, aby dobře fungoval v prostředí, ve kterém se bude používat. Špatně zvolený transpondér může vést k poruchovosti a chybám čtení [13].

Obr. 3: *Pasivní RFID tagy* [10]

Pasivní RFID systémy mohou pracovat při využití nízkých, vysokých, ale i UHF frekvencí. Rádiové vlny se chovají odlišně v každém z těchto prostředí, což znamená, že každá frekvence je vhodná pro různé aplikace. Při volbě designu antény je nutné často experimentovat, než se docílí uspokojivých výsledků v prostředí, kde má anténa pracovat.



Obr. 4: *Pasivní RFID čipy* [11] a [12]

1.4 Efektivita fungování RFID systému

Hlavní podmínkou úspěšného a efektivního fungování při návrhu kompletního RFID systému je zvolení vhodného druhu tagů, antén a jejich rozmístění. RFID systémy jsou velmi náchylné k rušení z okolních rádiových systémů, protože rádiové systémy užívají podobné frekvence. Celkový výkon systému je rovněž nepříznivě ovlivněn kapalinami, vlhkostí nebo mokrým povrchem, ale také kovy, které působí jako elektromagnetický reflektor a přes ně nemohou signály proniknout. Kovy tedy brání přímé komunikaci mezi čtečkou a tagem. Každý z druhů RFID signálů je schopen v určitých prostředích pracovat více, či méně efektivně [1].

Mezi základní prvky ovlivňující výkon patří

- volba vhodného frekvenčního pásma,
- přítomnost problémových materiálů (kovy, kapalina),
- umístění jednotlivých komponentů,
- rušení jinými zařízeními.

Při aplikaci RFID systémů je proto důležité provést kompletní analýzu prostředí, ve kterém má RFID systém fungovat, abychom se vyvarovali omezení funkčnosti a efektivity celého systému v důsledku negativních vlivů působících na RFID systém.

1.5 Způsoby komunikace

V systémech RFID rozlišujeme dva druhy komunikace, které lze podle principu metody charakterizovat takto:

Induktivní metoda je založena na principu vzájemné indukce dvou cívek (primární cívkou ve čtečce a sekundární v tagu). Dosah cívek je až několik centimetrů. Využívá se především při aplikaci pasivního RFID systému. Základem je tag, který obsahuje čip s cívkou. Čtečka vysílá do okolí magnetické pole, které proniká do závitů cívky a dodá energii čipu [1].

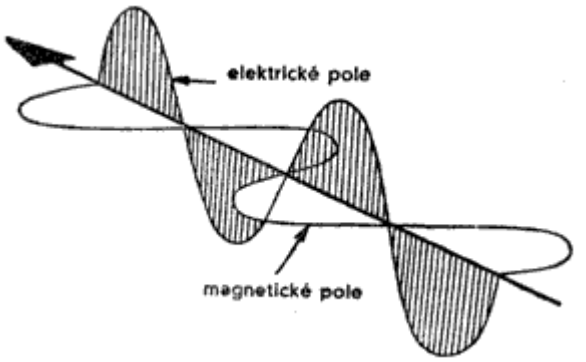
Odrazová metoda, nazývána také radiační metoda, je schopna funkce až na několik metrů. Funguje na principu komunikace vzdáleným polem, podobně jako radar. Čtečka vyšle vysokofrekvenční signál, který slouží k aktivaci čipu a následného změnění parametrů antény. Z toho vyplývá, že odražený signál je jiný, než signál přijatý [1].

2 FREKVENČNÍ PÁSMA RFID

RFID systémy využívají ke komunikaci rádiové vlny, které pracují na různých vlnových délkách. Rádiové vlny jsou vlastně elektromagnetické vlny tvořeny pohybujícími se elektrony, jejichž součástí jsou oscilující elektrická a magnetická pole. Propustnost různými druhy materiálů závisí právě na vlnové délce, která je dána vztahem

$$\gamma = c / f$$

c je rychlost světla ($3 \cdot 10^8$ *m/s*) a f představuje frekvenci [1]. Rádiové vlny se pohybují v oblasti od 0,1 MHz až po 300 GHz, což už je spektrum infračerveného záření. Tyto kmitočty odpovídají vlnové délce od několika milimetrů až po stovky metrů [14]. Vzdálenost mezi nejvyšším a nejnižším bodem se nazývá vlnová délka. Cyklem nazýváme proces, kdy dojde ke kompletní oscilaci vlnové délky. Čas potřebný k dokončení cyklu se nazývá perioda. Počet cyklů za jednu sekundu je označován jako frekvence vlny, jejíž jednotkou je hertz – Hz, podle německého fyzika Heinricha R. Hertze, objevitele elektromagnetických vln [1].



Obr. 5: *Elektromagnetická vlna* [15]

Pracovní kmitočet je určujícím parametrem pro čtecí dosah a interakci s okolním prostředím. Obecně platí, že čím vyšší frekvence, tím rychlejší přenos dat a současně delší vzdálenost, ve které je RFID snímač schopen komunikovat s RFID čipem. Avšak na úkor zvýšené citlivosti na okolní materiály, které mohou výrazně ovlivnit šíření rádiových vln. Jedna z nejdůležitějších fází návrhu RFID systému je právě volba vhodné frekvence pro určitou aplikaci. Protože na základě této volby vznikají omezení, která mohou mít pro danou činnost nepříznivé důsledky. Jedná se o omezení např. rychlost snímání a zapisování, dosahu čtení nebo omezení vyzářené energie [1].

2.1 LF pásmo

LF – *low frequency*, česky nízkofrekvenční pásmo, se pohybuje v oblasti od 125 kHz do 134 kHz. LF pásmo je charakterizováno velmi krátkou (téměř kontaktní) čtecí vzdáleností (udává se do 0,5 m) s nízkou přenosovou rychlostí. Nízkofrekvenční systém používá většinou pasivní tagy s nepřepisovatelnou pamětí. Tagy s nízkofrekvenčním přenosem jsou vhodné ke čtení přes kapalinu, částečně i kov a jsou využívány ve vlhkém prostředí. Nevýhodou nízkofrekvenčních tagů jsou vysoké výrobní náklady. Tato technologie se využívá převážně v identifikačních průkazech (evidence docházky), při evidenci zvířat nebo k identifikaci komponentů v zařízení během výroby [1]. Klasickou formou nízkofrekvenčních tagů jsou skleněné trubicové tagy, čipové karty s krytím nebo inteligentní etikety.

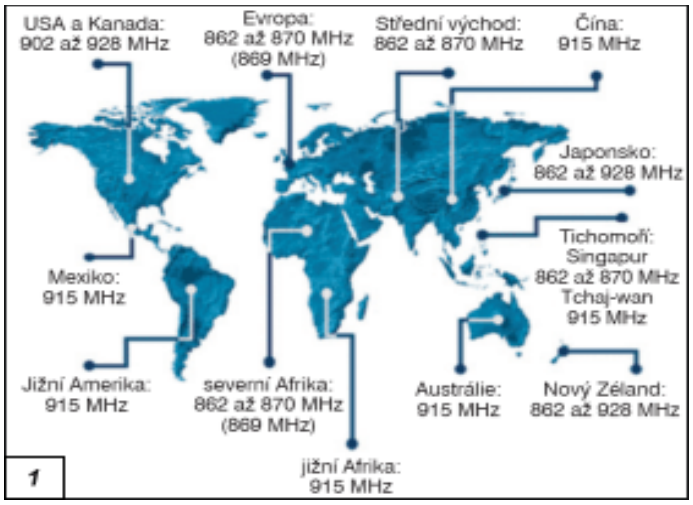
2.2 HF pásmo

HF – *high frequency,* v doslovném překladu vysoká frekvence, využívá konkrétní část spektra - 13,56 MHz. Oproti nízkofrekvenčním tagům má až dvojnásobnou čtecí vzdálenost a dosahuje vyšší komunikační rychlosti. Opět je převážně využíváno pasivními tagy ale již s pamětí typu RO (*Read Only*), které slouží pouze ke čtení a RW (*Read Write*) s možnost přepisování uložených dat. V porovnání s ostatními tagy, jsou vysokofrekvenční tagy nejlevnější, což má za následek, že jsou nejrozšířenější na světě. Nevýhodou vysokofrekvenčních tagů je velké zkrácení čtecí vzdálenosti skrz kapalinu a obtížné čtení z tagů umístěných na kovové podložce. Vysokofrekvenční RFID systémy jsou používány nejčastěji v knihovnách, muzeích, v docházkových systémech nebo v identifikačních kartách. Nejpoužívanějšími transpondéry využívající HF pásma jsou etikety, čipové karty nebo průmyslové transpondéry.

2.3 UHF pásmo

UHF – *ultra high frequency* (ultra vysoké frekvence) se pohybuje v oblasti 860 – 960 MHz. Dosah čtení se uvádí až několik metrů. Signál je zcela absorbován kovy a prakticky zcela kapalinami. Další vlastností UHF tagu je vysoká rychlost čtení a zápisu. Tagy UHF jsou v dnešní době také nejpoužívanější. Zvláštností UHF systémů je, že v různých zemích

světa se používají různá frekvenční pásma (obr. 6). Využití nachází v docházkových systémech, knihovních systémech, při identifikaci zboží a palet, ale hlavně logistických jednotek díky zavedení jednotného standardu EPC (*Electronic Product Code*), což je elektronický kód produktu [1].



Obr. 6: *Užívání kmitočtových UHF pásem ve světě* [16]

2.4 MW pásmo

MW – *microwave* (mikrovlny) jsou frekvence pohybující se v části 2,45 – 5,8 GHz. Čtecí dosah mikrovlnných tagů je až 10 metrů. MW frekvenční část je celosvětově využívána Wi-Fi sítí. Typickým charakterem MW technologie je velká čtecí vzdálenost a možnost čtení v extrémně vysokých rychlostech. Jsou nejméně citlivé na rušivé vlivy rádiových systémů. Avšak signál extrémně absorbují kapaliny. Není vyloučena situace, kdy se signál může dostat do kolize s některým typem bezdrátové počítačové sítě nebo jiných zařízení používající stejnou frekvenci [16]. Další nevýhodnou vlastností MW tagu je vysoká pořizovací cena. MW tagy jsou spojovány hlavně s aktivními systémy RFID, protože obsahují vlastní zdroj energie, který může signál zesílit až na desítky metrů. Využití nacházejí při identifikaci vozidel, logistice, pohybujících se předmětů (RTLS – *Real Time Location Services*) nebo také v dopravě, kde se MW systémy implementují do mýtných bran [1].

3 KOMPONENTY RFID

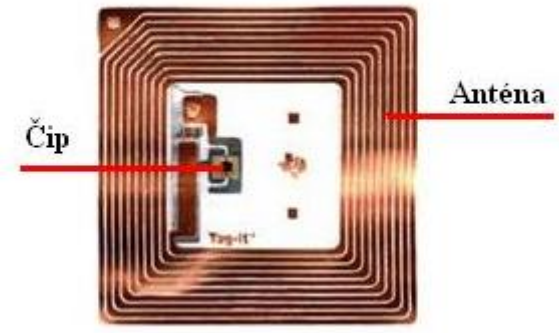
V následující kapitole se seznámíme se základními komponenty systému RFID.

V nejjednodušší podobě se RFID systém skládá z těchto komponent

- **RFID tag** – je nosičem základní informace, nazývá se taky transpondér, obsahuje vlastní anténu a čip,
- **RFID snímač** – je zařízení sloužící k vysílání a příjímání signálu, je určeno ke komunikaci mezi RFID tagem a řídícím počítačem,
- **RFID middleware** – je software (ve speciálních případech i hardware) pro správu, filtrování a analýzu získaných dat z RFID tagů,
- **RFID příslušenství** – zahrnuje veškeré díly potřebné k sestavení celého systému (kabeláž, akumulátory, napáječe, turnikety aj.).

3.1 RFID tag

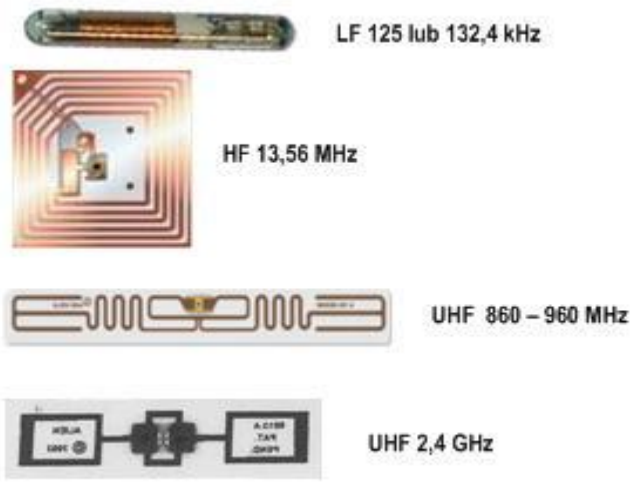
RFID tag, nebo také transpondér, jehož význam vznikl sloučením dvou anglických slov *transmit* (přenos) a *response* (odpověď), je nositelem všech informací. Jeho základní funkcí je ukládat a poskytovat údaje RFID systému [1].



Obr. 7: *RFID tag* [17]

Každý tag se skládá z mikročipu a antény. Aktivní tagy jsou navíc osazeny baterií, díky které je aktivní tag mnohokrát větší, než tag pasivní, který baterii nemá. Některé tagy mohou obsahovat ještě navíc paměť, senzory sledující teplotu, vlhkost a jiné měřicí přístroje. Integrovaný obvod se skládá z mikroprocesoru, paměti a odpovídače. Mikroprocesor zpracovává informace vedoucí ze snímače a paměť následně jednoznačně

tag identifikuje. Z toho plyne, že každý tag je jedinečný a má svůj vlastní identifikátor. Velikost čipu je dnes menší než 1 mm. Celková velikost celého tagu závisí hlavně na velikosti antény, která je jeho největší součástkou. Anténa se vyrábí v mnoha různých provedeních tak, aby vyhovovala prostředí, ve kterém bude pracovat. Špatně navržená anténa může vést k nízké spolehlivosti komunikace mezi tagem a čtečkou. Obecně platí, že čím vyšší použitá frekvence, tím menší může být anténa [7].



Obr. 8: *RFID tagy* [18]

RFID tagy mají několik typů zapouzdření. Mohou to být PVC karty o velikosti kreditní karty, skleněné trubičky, tenké nálepky nebo disky, náramky, hřebíky nebo klíčenky. Existují také tagy, které jsou schopny odolávat extrémním teplotám od -40°C až po +300°C [1].

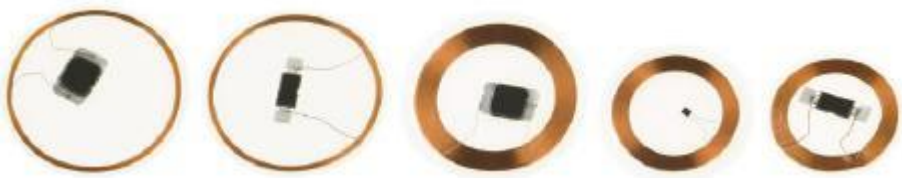
Tagy můžeme rozdělit do několika skupin podle

- výrobní technologie,
- druhu paměti,
- frekvenčního pásma, ve kterém pracují,
- zdroje energie.

3.1.1 Členění podle výrobní technologie

Volba tagu úzce souvisí s aplikací, ve které bude fungovat. Určitý druh tagů je zhotoven tak, aby odolával extrémním teplotám. Jiný druh zase proti vlhkosti a nepříznivým atmosférickým vlivům, nebo existují i takové, které odolávají chemickým látkám. Musíme proto tag zvolit takový, aby vyhovoval našim požadavkům a správně fungoval v daném prostředí [1].

Z hlediska výrobní technologie existuje celá řada druhů tagů resp. transpondérů. V poslední době je zaznamenán velký vzrůst RFID tagů v provedení **Disk** (viz obr. 9). Anténa má kruhovitý tvar o průměru od několika milimetrů až po 10 cm. Výhodou těchto tagů je snadná implementace do různých součástek. Disky se implementují nejčastěji do klíčenek, imobilizérů nebo náramků. Disk je zapouzdřen do plastového obalu (PET, PVC, PETG), což mu poskytuje vysokou odolnost. Některé obaly mohou mít robustnější charakter. V případě klíčenkového obalu pro jednoduché umístění ke svazku s klíči je možná varianta s malým otvorem. Klíčenky se využívají v oblasti bezpečnosti, např. při střežení prostorů, kanceláří a kontroly průchodů oprávněných osob [1].



Obr. 9: *Diskové tagy* [19]

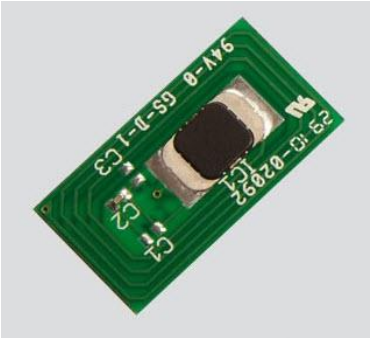
Dalším druhem transpondéru je **Smart label** neboli „chytrá etiketa“ (viz obr. 10). Vyrábí se v papírové nebo plastové formě nejčastěji jako nálepka. Jedná se vlastně o tištěnou etiketu, která obsahuje pasivní tag. Velkou výhodou chytré etikety je nízká pořizovací cena a možnost vytisknutí uložené informace v paměti tagu do textové podoby nebo čárového kódu. Čárový kód slouží v tomto případě jako záložní identifikátor. Nevýhodou oproti diskovým transpondérům je nízká odolnost proti okolním vlivům. Etiketu lze snadno přetrhnout nebo poškodit. Chytré etikety se využívají k označování krabic, kartonů nebo palet [1].

Obr. 10: *Smart labels – „chytré etikety“* [20]

Oblíbeným a plošně využívaným transpondérem jsou **identifikační karty** tzv. **Smart cards**. Jak už název napovídá, jde o karty obdélníkového tvaru velikosti platebních karet (jako standardní rozměr se uvádí 58 x 55 x 0,75 mm). V případě tzv. Smart cards je možnost použít poměrně velkou anténu, což je výhoda pro celkový dosah systému. Výrobní technologie funguje na principu vrstvení. Při teplotě 100°C se mezi vrstvy PVC zataví anténa. Karty se dále mohou potisknout grafikou nebo fotografií uživatele (což přispívá k bezpečnosti, protože jde o další identifikační prvek). Karty jsou ohebné, odolné, mají vysokou životnost, PVC zajišťuje ochranu tagu proti nečistotám a vlhkostí. Karty jsou využívány pro identifikaci, autentifikaci nebo ukládání dat [1].

Obr. 11: *Smart card – „chytrá karta“* [21]

Jiný druh výrobní technologie tagů představují **PCB tagy**. Jedná se o RFID čip s PCB (*Printed Circuit Board*) anténou. PCB tagy jsou vhodné pro specifické návrhy zákazníků na tvar tagů, protože se dají snadno upravovat. Výhodou u těchto tagů je také možnost rozšířit tag dodatečným kondenzátorem, což zvýší jejich čtecí vzdálenost. PCB je možné jednoduše zabudovat přímo do předmětu (krabice, přepravky, kontejnery). Je také možné je uložit do obalů z laminátu. Oproti předchozímu typu (Smart label), jehož odolnost není příliš vysoká, jsou PCB tagy mnohem odolnější a pevnější. Čili mohou být použity v prostředích, kde by etikety neobstály. Protože je tag po celou dobu uložen a zapuštěn do předmětu, je možné ho neustále kontrolovat, ukládat do něj informace a tak sledovat celý výrobní koloběh od výrobního pásu až ke spotřebiteli [1].



Obr. 12: *PCB tag* [22]

Posledním druhem tagů jsou tzv. **skleněné tagy** nebo také trubičkové tagy. Fungují především v nízkofrekvenčním pásmu, a jejich hlavní využití je v oblasti zemědělství a lékařství (např. pro kontrolu zvířat). Celý tag je chráněn skleněnou trubičkou (viz obr. 13) o velikosti 1-3 cm. Čip je uložen v plastovém obalu a od něj je navinutá cívka po celé délce trubičky. Čip a cívka jsou potom společně zapuštěny do přilnavé hmoty pro získání vyšší odolnosti [1].

Obr. 13: *Skleněné tagy* [23]

3.1.2 Dělení podle typu paměti

Každý tag po naprogramování má své vlastní identifikační číslo. Některé tagy mohou ještě navíc mít paměť. Tagy na základě druhu paměti mohou být rozděleny na

- tagy RO (*Read-only*),
- tagy WORM (*Write Once Read Many*),
- tagy RW (*Read-write*).

Tagy RO (*read only*) jsou tagy, jak už anglický název napovídá, určeny pouze pro čtení. Jinak řečeno tagy bez možnosti dalšího zápisu. Principiálně jsou vlastně podobné jako čárové kódy nebo CD-ROM. Čárový kód má své vlastní ID, které nelze změnit. Obdobně CD-ROM není schopen ukládat nová data po vypálení. Po naprogramování ve výrobě už tedy vnitřní informace v tagu nelze změnit a od této chvíle je veškerá komunikace mezi tagem a čtečkou pouze jednosměrná. Čtečka nemá již možnost uložit nebo změnit další informace. Tento druh tagů není schopen pojmout větší množství dat (udává se 40-512 bitů). Rychlost čtení je cca 1000 tagů/s [1].

Oproti tomu tagy s pamětí typu **RW** (***Read-write)*** mohou uchovat větší množství dat (pasivní tagy 386 b - 8 Kb, aktivní tagy 16 Kb - 2 Mb), obsahují adresovanou paměť, kterou lze snadno měnit. Největší rozdíl oproti RO tagům je však v možnosti vymazávat nebo přepisovat uchovaná data až tisíckrát. Můžeme tedy sériové číslo i s identifikátorem měnit dle potřeby [1].

Posledním typem jsou paměti **WORM** (*Write Once Read Many*), které jsou určeny pouze pro čtení. Rozdíl oproti tagům typu RO je v době programování tagu. Ten není naprogramován při výrobě, ale až u prodejce nebo dodavatele. Prodejce zapíše potřebnou informaci do WORM tagu, kterou již dále nelze přepsat. Rychlost čtení z paměti je 200 tagů/s. Můžeme se taky setkat s WORM tagy, kde se uvádí, že tag může být několikrát přepisovatelný, ale bez záruky spolehlivosti (počet přepisování se uvádí až 100krát) [1].

V budoucnu se očekává používání pamětí s větší kapacitou. Rozhodnutí, který typ paměti použít, záleží na způsobu použití tagu. Někdy je postačující použití tagu pouze jako nosič informace (RO tag) s jasnou identifikací, jindy zase je výhodnější mít tag, který je schopen ukládat informace (např. informace o údržbě výrobku). Tagy typu RO jsou logicky levnější než tagy s přepisovatelnou pamětí [7].

3.2 Snímač

RFID snímač (můžeme se setkat i s pojmenováním *RFID reader* nebo *čtečka*) je elektronické zařízení, které přijímá a vysílá rádio-frekvenční vlny, jimiž komunikují s transpondéry. Snímač je aktivní zařízení, které vysílá do svého okolí elektromagnetické pole, a které dodává energii pasivním tagům. Dalšími funkcemi snímače jsou zapisování dat do tagů, přenosy dat, filtrace a čtení údajů z tagů.

3.2.1 Komponenty snímače

Součástí každého snímače je anténa a integrovaný obvod. Anténa stejně jako u tagů zajišťuje komunikaci a přenos informací. I v tomto případě mohou antény nabývat různých podob. Záleží na prostředí, ve kterém se čtečka nachází. Nevhodně zvolená anténa může způsobit nízkou efektivitu a spolehlivost celého systému. Integrovaný obvod ve čtecím zařízení slouží k řízení procesů komunikace s tagem a počítačem. Má také za úkol vypořádat se s tzv. kolizí, což je případ, kdy se dva tagy současně snaží okamžitě komunikovat se čtečkou. Tento problém je vyřešen tzv. metodou „gap pulse“, což technicky znamená, že snímač vyšle opakovaný signál tagům, a ty po zachycení tohoto příkazu zopakují své vysílání za dobu určitou na základě algoritmu využívajícího generaci náhodného čísla. Tím pádem snímač načte veškeré informace od více tagů ve svém okolí [7].

3.2.2 Druhy snímačů

Snímače můžeme rozdělit do dvou základních kategorií, kterými jsou

- stacionární snímače (čtečky),
- mobilní snímače (čtečky).

Stacionární čtečky jsou zařízení nepřenosná, většinou pevně zabudovaná v určeném prostoru, kde probíhá identifikace (např. za pokladnou v obchodě). Tyto čtečky je možné ještě rozšířit o více antén, což umožní získat lepší pokrytí čtecího prostoru. Systém s více anténami je aplikován např. ve čtecích bránách nebo vysokozdvižných vozících [1].

Obr. 14: *Stacionární čtečky* [24] a [25]

Mobilní čtečky jsou čtecí zařízení, která lze libovolně přenášet. Jsou navržena tak, aby se daly držet v ruce (viz obr. 15). Fungují a komunikují s počítačem bezdrátově, není proto nutná žádná kabeláž při snímání tagů. Často se objevuje i tzv. hybridní provedení. Jedná se o zabudované RFID čtečky a zároveň čtečky čárových kódů. Nejčastěji se tyto čtečky využívají ve skladech a při logistických úkonech [1].

Obr. 15: *Mobilní čtecí zařízení* [26]

3.3 Middleware

RFID technologie při svém provozu generuje obrovské množství dat, se kterými je velmi obtížné pracovat. Pro zpracování, analýzu, správu a filtraci těchto dat slouží software (nebo také specializovaný hardware) tzv. RFID middleware. Jak už název napovídá, jedná se o prostřední systém mezi jednotlivými snímači a aplikacemi používanými ve společnostech, který řídí datový tok. Jako příklad lze uvést prvotní informaci, kterou snímač odešle do middlewaru. Jde o událost „tag zachycen čtecím zařízením“, což je informace o tom, že tag byl zaznamenán v blízkosti snímače. Obvykle se k takovéto informaci dají získat ještě navíc data např. o stavu baterie, identifikace čipu, lokalizace tagu nebo čas načtení tagu.

Největším úkolem middlewaru je však filtrace a čištění dat, protože RFID systémy posílají souvisle obrovské množství dat v náhodném pořadí a do systému je potřebné zapsat pouze určitou část informací, které jsou pro uživatele informačního systému důležité. Ve většině případů je nezbytné získat informace, kdy snímač tag identifikuje, a kdy tag čtecí pole snímače opustil. Ostatní načtená data jsou pro řídící aplikace irelevantní. Avšak další informace (např. znalost prostředí, ve kterém se tag nachází) nalézají svůj úkol při opravách chyb způsobených chybou čtení z důvodů chybného detekování tagů, zastínění tagů nebo chybného načtení tagů z jiné zóny. Spolehlivost snímačů bohužel zatím není stoprocentní, a tak je potřeba, aby middleware měl schopnost oddělovat pravdivé informace od chybového načtení [1], [7].

3.4 Příslušenství

Pro kompletaci celého systému zbývá stanovit prostředky, které zajišťují funkčnost celého systému. Mezi příslušenství celého RFID systému můžeme zahrnout kompletní strukturovanou kabeláž, konektory, propojovací komponenty, terminály, komunikační LAN boxy, napájecí zdroje, akumulátory, turnikety nebo externí antény.

V předchozích kapitolách jsme si popsali kompletní RFID systém, principy systému a vlastnosti jednotlivých komponent. Nyní už se budeme zabývat pouze jeho aplikacemi a využitím.

4 ČÁROVÝ KÓD

V této kapitole se seznámíme s jiným používaným prvkem identifikace, a sice čárovým kódem a porovnáme jeho vlastnosti a využití s RFID systémem.

Čárový kód je prostředek pro automatizovaný sběr dat. Je tvořen sadou vytištěných černých pruhů definované šířky, které je možné načíst laserovými čtečkami. První patent byl udělen v roce 1949. Čárové kódy, se kterými se dnes nejčastěji setkáváme (tzv. EAN) přišly na trh v roce 1976. Dnes se již aplikují i různé modifikace tištěných kódů např. QR kódy, mozaikové kódy nebo kruhové kódy. Je evidováno zhruba 200 typů čárových kódů [27].

Obr. 16: *Čárový kód typu EAN* [27]

4.1 Princip činnosti

Celý systém je založen na principu odrazu červeného světla. Tradiční laserové snímače čárového kódu vyzařují právě červený pruhový paprsek, který je pohlcován tmavými čárami a odráženo světlými mezerami. Snímač zanalyzuje rozdíly v reflexi a ty přemění na elektrické signály odpovídající šířkám čar a mezer. Tyto signály jsou následně převedeny na číslice (nebo písmena), která obsahuje čárový kód. Což tedy znamená, že každá číslice (písmeno) je na čárovém kódu zaznamenáno pomocí předem určených šířek. Obsahem čárového kódu může být číslo výrobku, místo uložení ve skladu, jméno osoby s povolením pro vstup do uzavřeného prostoru apod.

Moderním trendem je přechod z laserových snímačů na snímače digitální. Pracují jako fotoaparát. Vyfotí si čárový kód a následně dekódují jeho obsah. Na stejném principu dnes umí „chytré“ telefony načítat QR kódy pouhým vyfocením [28].

4.2 Srovnání čárových kódů s RFID

Čárové kódy se pro identifikaci používají o mnoho let déle než RFID. V nejbližší době se neočekává závratný průlom a celkové nahrazení čárových kódů systémem RFID. Avšak i RFID může nabídnout širokou škálu výhod. Základní rozdíly oproti čárovým kódům jsou

- rádiová komunikace,
- čtení na větší vzdálenost,
- rychlost čtení,
- možnost zápisu nebo změny informací,
- odolnost.

Výhoda rádiové komunikace spočívá ve faktu, že RFID tag nevyžaduje přímou viditelnost na snímač. Stačí, aby byl v dosahu čtecího pole snímače. Čárový kód musí být rovný, čistý a nenarušený (pokřivené nebo jinak poškozené pruhy znamenají znemožnění načtení kódu. Typický příklad, který každý zná, je z obchodních řetězců s potravinami, kde je zboží v drtivé většině opatřeno čárovými kódy, a kde často dojde právě k narušení jeho čitelnosti. Obsluha poté musí zboží identifikovat ručně zadáním číselného kódu zboží, což je časově náročná operace).

Nezanedbatelným pozitivem rádiové komunikace je také rychlost čtení – možnost načtení většího počtu RFID tagů. Čárové kódy je nutné načíst separátně (využití ve skladech).

Dalším rozdílem RFID tagů oproti čárovým kódům je jejich mechanická odolnost. Jak již bylo uvedeno v předchozím odstavci, čárové kódy jsou náchylnější na mechanické poškození, jelikož nejsou nijak kryty. Může tedy dojít k odtržení nebo poškození štítku. RFID tagy jsou zakryty v PVC nebo jiných obalech, a uplatňují se v prostředí, kde by papírová etiketa byla zničena (RFID tag vydrží např. lakování, mytí pivovarských sudů nebo odolává atmosférickým vlivům venkovního prostředí).

Hlavním faktorem, proč se štítky s čárovými kódy stále udržují na trhu je cena. Štítky jsou zatím mnohem levnější než RFID tagy, avšak s rostoucím zájmem o RFID tagy lze předpokládat pokles ceny tagů na takovou úroveň, kdy se ekonomicky vyplatí používat RFID systémy jak v menších společnostech, tak i v potravinových řetězcích [29].

5 VYUŽITÍ RFID V KOMERČNÍ BEZPEČNOSTI

RFID systémy v oblasti průmyslu komerční bezpečnosti jsou nejčastěji využívány v odvětví tzv. *access systems*, což jsou přístupové systémy (ACS) resp. systémy kontroly řízení vstupů do objektu (SKV). Můžeme je chápat jako soubor opatření k řízení a zajištění evidence přístupu do zabezpečeného objektu nebo prostor na základě přidělení přístupových oprávnění. Tato opatření se mohou v rámci komerční bezpečnosti rozdělit na

- systémová,
- fyzická (ostraha),
- mechanická (prvky MZS),
- elektronická (ACS).

Zpravidla bývají nejúčinnější různé kombinace prvků zabezpečení. Přístupová oprávnění jsou rozdělena uživatelům podle personálního postavení ve firmě, stupně oprávnění apod. Na základě jednoznačné identifikace je pak uživateli přístup povolen nebo zamítnut. Některé systémy umožňují sledovat jednotlivé uživatele v zabezpečeném prostoru a mohou za chodu systému měnit přístupová práva [30].

V mnoha případech dochází k zaměňování významů pojmů „přístupové systémy“ a „docházkové systémy“. Proto si v další kapitole přesně tuto terminologii definujme.

5.1 Přístupový a docházkový systém

Přístupový systém můžeme označit i jako řízení vstupů, což je selektivní omezení přístupu do zabezpečeného místa nebo zdroje. Povolení k přístupu se nazývá autentizace. Správní řízení přístupu bývá hlídáno zaměstnanci (vrátný, recepce), v častějších případech mechanickou zábranou. Jedná se především o turnikety, které po autentizaci vpustí oprávněnou osobu do objektu.

U docházkového systému je identifikace také nedílnou součástí funkce systému. Hlavním cílem je však monitorovat čas a důvody průchodu daným vstupním bodem (o čemž hovoří zákonná povinnost monitorování pracovní doby zaměstnanců, povinné přestávky a pauzy). Přístupové a docházkové systémy mohou být integrovány do jednoho systému. Mezi přístupovým a docházkovým systémem však existuje jeden zásadní rozdíl.

Přístupových bodů bývá v objektu několik, zatímco docházkový bod bývá obvykle pouze jeden (hlavní vstup do objektu) [30].

5.2 Základní funkce přístupového systému

Řízení vstupů u přístupového systému princip spočívá na funkcích, kterými jsou

- identifikace,
- zpracování dat,
- řízení přístupového místa,
- stavová hlášení,
- komunikace (s aplikacemi systému),
- kontakt s uživatelem (světelné signály, akustické signály).

Konkrétní provedení přístupového systému je posuzováno podle mnoha kritérií, která ovlivňují celý chod přístupového systému. Také je nutné posuzovat bezpečnostní rizika (hmotná, fyzická nebo informační). Podle tohoto bezpečnostního rizika existují stupně zabezpečení pro každé přístupové místo, které je definováno pomocí tříd identifikace a tříd přístupu [30], jak vyplývá z tab.1.

Třída identifikace	Druh identifikace	Příklad identifikace
0	není přímá identifikace	tlačítko, kontakt, detektor pohybu
1	data uložená v paměti	heslo, ID zaměstnance
2	biometrie nebo jiné identifikační prvky	identifikační karta, přívěšek, token, čip, otisk prstu, oční duhovka
3	kombinace 1. a 2. třídy	identifikační karta + otisk + heslo

Tab 1: *Třídy identifikace* [30]

5.3 Integrace RFID s bezpečnostními systémy

RFID systémy jsou v kombinaci s bezpečnostními systémy velmi rozšířené. Nejčastěji to bývá se slaboproudými bezpečnostními systémy. V praxi se integrují převážně tyto systémy:

- **Docházkový systém** – je přístupový systém v kombinaci s docházkovým systémem.
- **Stravovací systém** – funguje na obdobném principu jako docházkový systém. Uživatel se identifikuje na „přístupovém“ bodě (na pokladně), kde se odečítají kredity z celkové částky na kartě.
- **Poplachový zabezpečovací systém** (PZS) – je inteligentnější sběrnicový systém PZS, má možnosti deaktivace poplachového systému při identifikaci na snímači, obvyklé je ovládání PZS prostřednictvím přístupových identifikátorů.
- **Elektrická požární signalizace** (EPS) – využívá RFID při vyhlášení požárního poplachu, slouží k zajištění všech přístupových bodů a odblokování únikových cest, případně zablokování vstupů v místech, kde se již požár rozšířil.
- **Kamerový systém** (CCTV) – využívá kamerového systému pro vizuální kontrolu uživatele při každé průchodové události. Využívá se v bankovních sektorech např. v prostorách s bankomaty.
- **Informační systémy** – propojují databáze a PC s RFID.
- **Měření a regulace** – systém reaguje na přítomnost uživatelů (osvětlení, vytápění) [30].

II. PRAKTICKÁ ČÁST

6 ANALÝZA KONTROLY VSTUPŮ

V komerční oblasti snad každá společnost usiluje o možnosti mít co nejlepší přehled a kontrolu nad vstupy do svého objektu a zároveň hlídat a chránit vchody a přístupy proti nepovolaným osobám. Mnoho z nich ale podceňuje rizika a důslednost při zavádění přístupového systému, který se po zavedení stane neefektivním. Je také nezbytně nutné, aby přístupový a docházkový systém byl co nejjednodušší, aby jej zaměstnanci mohli jednoduše a bez větších omezení využívat. V teoretické části jsme si uvedli prostředek – RFID systém, který problém s kontrolou a hlídáním vstupů dokáže snadno a efektivně vyřešit. V kombinaci s funkčním obslužným softwarem se z celého zařízení stává multifunkční systém s velkým potenciálem.

V dalším pojednání se budeme zabývat konkrétním identifikačním systémem, který je aplikován v mnoha objektech. V rámci zachování obchodního tajemství a technologie společnosti, která byla předmětem analýzy, není možné konkrétně specifikovat místa, kde se daný systém nachází.

6.1 Analýza používaného systému

Přístupový systém (vstupní systém) zahrnuje omezení volného a nekontrolovatelného pohybu osob ve vyhrazených prostorách a zamezení vstupu nepovolaných osob. Současně monitoruje pohyb zvolených osob se zajištěním jejich přítomnosti či nepřítomnosti v určeném prostoru. K tomuto je možné zadávat víceúrovňová přístupová práva s možností restrikce v libovolném počtu uživatelsky vytvořených časových zón. Kompletní systém je tvořen vstupními branami, terminály, turnikety, snímacími jednotkami, komunikačním rozhraním a transpondéry (nejčastěji čipovými kartami). Přístupový bod tvoří v konkrétním případě vrátnice s turnikety. V objektu se dále používají elektromagnetické zámky a dveřní ovladače pro získání kontroly pohybu osob uvnitř objektu. U každých dveří se nachází snímací jednotka pro identifikaci zaměstnance. Každý zaměstnanec podniku je držitelem identifikačního transpondéru, s nímž se může pohybovat po objektu a vstupovat do místností, do kterých má oprávnění.

6.1.1 Kontrola vstupů

Celý proces identifikace začíná ve chvíli, kdy uživatel projde branou a dostane se k turniketu. Při standardním procesu přiloží zaměstnanec transpondér do čtecí vzdálenosti snímače, poté dojde k ověření identity a porovnání s databází. Primárně existují tzv. „offline“ a „online“ systém. V případě využití „online“ systému probíhá kontrola a porovnání identifikačního čísla čipové karty s databází na serveru a identifikační procesy a historii vstupů je možné sledovat prakticky v reálném čase. „Offline“ systém oproti „online“ systému nevyžaduje žádné připojení a veškeré informace s daty jsou uloženy přímo ve snímací jednotce. Analyzovaný systém pracuje s „offline“ verzí a veškerá zaznamenaná data včetně historie identifikací a průchodů je možné načíst po propojení snímací jednotky s počítačem. Po ověření zaměstnance se turniket otevře a zaměstnanec je vpuštěn do objektu. Do databáze je současně zapsán čas příchodu. Stejný proces se provede při odchodu s rozdílem, že do databáze se ukládá čas odchodu.

6.1.2 Hardwarové a softwarové vybavení systému

6.1.2.1 Turnikety a elektrické dveřní zámky

U vstupních přístupových bodů jsou použity otočné tříramenné trnové turnikety *Aproks* s obchodním označením TPB S01. Jedná se o tříramennou bariéru pro automatickou kontrolu vstupů. Turniket má certifikát NBÚ se stupněm utajení tajné. Konstrukce turniketu je z nerezového trubkového rámu se zabudovaným terminálem a nerezovou otočnou bariérou. V případě výpadku proudu se sklopí středová zábrana a systém umožní únikový východ. Po zpětné dodávce elektrické energie se turniket automaticky vrátí do původní funkční polohy. Turniket dovoluje oboustranný průchod řízený systémem přístupové kontroly. Řízení je integrováno uvnitř konstrukce, turniket je napájen ze sítě 230V / 50Hz. Kapacita průchodnosti je 15-25 osob za minutu.

Obr. 17: *Turniket TPB S01 s otočnou tříramennou bariérou* [31]

V objektu se dále nacházejí elektrické dveřní zámky, které jsou zabudovány ve dveřích do místností, nad nimiž chceme mít dohled. Zámky jsou napojeny na jednotlivé snímače u každých dveří. Identifikační proces je obdobný jako u přístupového bodu. Zaměstnanec přiloží svůj identifikátor do čtecí oblasti snímací jednotky, kde po porovnání a ověření shody identifikačního čísla karty a čísla v databázi dojde k uvolnění kotvy v elektrickém zámku a dveře je možné snadno otevřít. Na snímací jednotce dojde opět k zápisu identifikačního čísla a času průchodu. Elektrický zámek je napájen 9-12V a otevírá se po dobu, kdy je pod napětím, to je přibližně 5 sekund.

Obr. 18: *Elektrický dveřní zámek*

6.1.2.2 Transpondéry

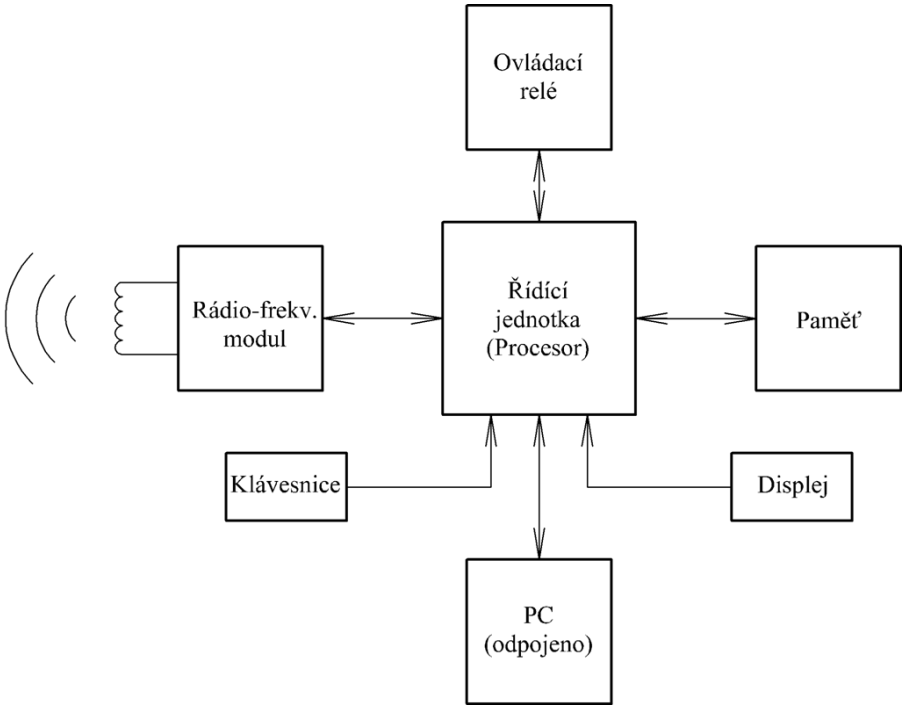
Jako identifikátory zaměstnanců jsou využity čipové karty o standardním rozměru dle normy ISO 7816. Čipové karty pracují na frekvenci 125 kHz. Z hlediska bezpečnosti tato frekvence není příliš vhodná z důvodů nízké přenosové rychlosti a malé paměti. Čipy s anténou jsou chráněny pevným obalem z PVC. Karta každého zaměstnance obsahuje fotku o rozměrech 45 x 34 mm, jméno, příjmení logo firmy a identifikační číslo karty a osobní číslo zaměstnance.

Pro účely testování byla vytvořena nová čipová karta (viz obr. 19), která rovněž sloužila k analýze identifikačního systému v objektu.

Obr. 19: *Čipová karta*

6.1.2.3 Terminály a snímače

U přístupového bodu analyzovaného objektu jsou nainstalovány 3 terminály, které jsou kompatibilní s identifikačními kartami zaměstnanců. Terminál je vybaven čtecí hlavou pro všechny typy čipových karet, grafickým displejem 160 x 32 pixelů, membránovou klávesnicí s akustickou signalizací, napájením 12V DC, odběrem 450 mA a kapacitou paměti 200 až 20 000 záznamů. Komunikace je možná prostřednictvím ethernetu s konektorem RJ45, dvojlinkou RS485 nebo canon RS232. Přístupový terminál slouží zároveň i jako docházkový, což je systém určený pro evidenci pracovní doby zaměstnanců.



Obr. 20: *Blokové schéma terminálu*

V okamžiku, kdy rádio-frekvenční modul zaregistruje ve své blízkosti čip, vyšle signál do řídící jednotky (procesoru), která informaci zpracuje a přepošle identifikační kód do paměti terminálu. V paměti jsou nahrány identifikační kódy všech čipů, které mají oprávnění projít tímto terminálem. Dojde k vyhodnocení o shodě identifikačního čísla snímaného čipu a identifikačního čísla v databázi uložené v paměti. V případě shody se na displeji objeví jméno zaměstnance s nápisem „vstup povolen“ a ovládací relé umožní protočení turniketu. V případě zamítnutí se na displeji zobrazí zpráva „vstup zamítnut“ a řídící jednotka nevyšle signál k rozpojení ovládacího relé.

Uživatel si na snímací jednotce může na klávesnici zvolit druh příchodu nebo odchodu, např. *lékař, oběd, dovolená, neplacené volno, nemoc* apod. Příchody a odchody jsou párované, nesmí se proto zapomenout u každého druhu průchodu stejným příkazem ukončit zaznamenaný stav. Například v případě návratu z dovolené zaměstnanec nesmí zapomenout zadat při vstupu opět položku „dovolená“ a ukončit tím tento status systému.

V dalších částech objektu jsou aplikovány menší snímače bez displeje, které kontrolují vstupy do místností. Analýzou tohoto typu snímače se budeme zabývat v další kapitole.

6.1.2.4 Programové vybavení

Jedná se o software, který ovládá a řídí celý přístupový systém. Tento systém je plně konfigurován a sledován obslužným počítačem. Operátor přidělí pomocí PC kódy karet nebo čipů k oprávněným vstupům do jednotlivých dveří, turniketů nebo objektů. Řídící jednotky systému jsou schopny sledovat veškeré informace týkající se přístupové aplikace a současně dokážou vyhodnotit násilné otevření dveří nebo nedovření a tuto informaci předat do obslužného počítače. Řídící jednotky jsou také zabezpečeny proti ztrátě dat při výpadku zdroje napětí.

Základní funkce programového vybavení jsou

- přiřazování přístupových práv pro jednotlivce, skupiny nebo všechny uživatele,
- tvorba neomezeného počtu časových zón individuálně pro každý den,
- možnost vytvořit nezávislé zóny v jediném dni,
- přiřazování časových zón pro jednotlivce, skupinu nebo všechny uživatele,
- sledování přítomnosti osoby v objektu,
- sledování a statistika o době pobytu osoby ve sledovaném prostoru.

☐	5009	V12 Hlavní vchod	Komunikuje	26.4.2013 12:40	101 - přístupový
☐	5010	V 12 Hlavní vchod 2	Komunikuje	26.4.2013 12:40	101 - přístupový

Obr. 21: *Ukázka seznamu snímačů v systému*

Na obrázku 21 jsou zobrazeny dva přístupové snímače, jejich identifikační čísla, místo, stav, čas s datem a typ. Obrázek 22 pak ukazuje výpis měsíčních průchodů uživatele. Z tabulky lze vyčíst jméno uživatele, osobní číslo, datum a čas, kdy došlo k identifikačnímu procesu.

Měsíční průchody

Jméno: Kratochvíl Vít **Os.číslo:** 2 **Datum:** 4 / 2013 **Šablona:** Základní

Uložit | Obnovit | Zavřít

Datum	Čas	Kód	Přerušení	Autor	Adresa	Ignorovat	Příznaky
2.4.2013	16:34:32	0		uživatel	0	☐	
2.4.2013	16:50:32	0		uživatel	0	☐	

Obr. 22: *Ukázka měsíčního výpisu průchodů konkrétního uživatele*

6.1.3 Režimová opatření

Režimová opatření by měla být navržena tak, aby příliš neomezovala pohyb osob v objektu podniku a zároveň zajistila požadovaný stupeň bezpečnosti. Samotný systém není úplně bezpečný. V případě ztráty nebo odcizení identifikátoru nastává velké riziko spojené s vniknutím nepovolané osoby do podnikové infrastruktury. Zaměstnanci bez identifikační karty se musejí prokázat např. občanským průkazem a po ověření mohou být vpuštěni do objektu. Pro předcházení těchto komplikací je zavedena fyzická ostraha v přístupových bodech, která vlastní univerzální čipové karty nebo tlačítkové ovladače pro ovládání turniketů. V zásadě se jedná o vrátnici v bezprostřední blízkosti turniketů, kde probíhají namátkové kontroly totožnosti (na základě fotografie a příjmení zaměstnance).

6.1.4 Nedostatky stávajícího systému

Podrobné testování systému a jeho analýza ukázala, že přístupový systém vykazuje nedostatky.

1) Slabým místem systému je skutečnost, že celý systém pracuje na frekvenci 125 kHz, která je v dnešní době zastaralá. Snímače a čipy fungující na této frekvenci mají velmi nízkou přenosovou rychlost a malou paměť, což vede ke snadnějšímu prolomení bezpečnosti čipu. Snímače musejí být osazeny silnými anténami (což jsou cívky s velkým množstvím závitů), které snadno indukují elektromagnetické pole. Silné elektromagnetické pole je pak snadným potenciálním terčem útoku zařízením pro zahlcení procesoru, vyvolání jeho chybových a nekorektních stavů a následného průniku do objektu.
2) Přístupové body by měly být doplněny kamerovým systémem s možností záznamu procházejících osob.
3) Dalším problémem jsou snímače, které jsou vestavěny přímo před vchody, což přináší riziko možnosti snadné manipulace s jejich elektrickými obvody. Řešením je uložit snímač do střežené místnosti a před dveře nainstalovat pouze rádio-frekvenční anténu. Druhou možností je používat ve snímačích tamper.
4) Celý systém funguje v tzv. „offline“ režimu, což zamezuje sledovat okamžitý provoz v objektu a v přístupových bodech. Dnes se již aplikují tzv. „duální“ systémy, kdy jsou snímací jednotky schopny pracovat jak v režimu „offline“ tak v režimu „online“ dle aktuálních potřeb.

   V následující analýze bude ověřena hardwarová a softwarová odolnost snímače.

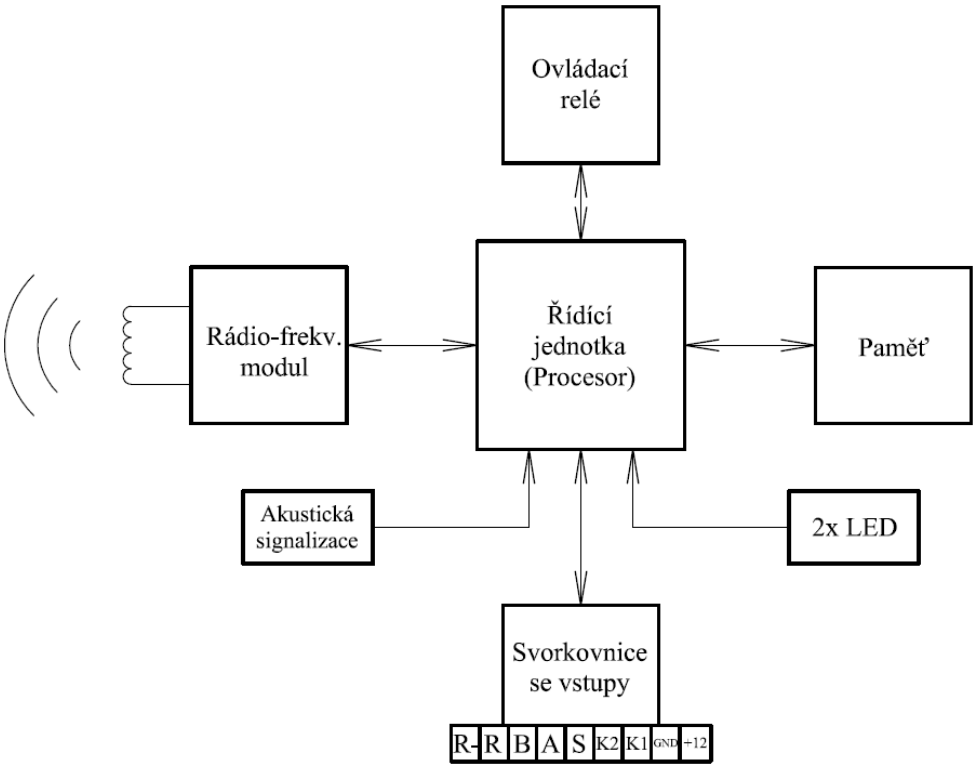
7 ANALÝZA SNÍMAČE

V této kapitole bude posouzeno, do jaké míry vybraný snímač aplikovaný v objektu dokáže odolávat softwarovým a hardwarovým útokům a je-li jeho odolnost dostatečná pro ochranu před poškozením nebo odkrytím elektrických obvodů. To znamená, že ověřujeme možnost proniknutí do střežené místnosti bez použití identifikačního prostředku (čipové karty). Testovaný snímač získal certifikát se stupněm zabezpečení NBÚ *Přísně tajné*, což pro zkoumaný objekt představuje důležité kritérium při výběru systému.

7.1 Charakteristika snímače

Jedná se o základní přístupový snímač vybaven dvěma LED diodami a akustickou signalizací. Zámek dveří je ovládán spínacím relé až na 10A. Snímač nemá displej ani klávesnici, je napájen 12V stejnosměrného napětí s odběrem 150mA. Komunikace je možná pouze RS 485 dvojlinkou, kapacita paměti je 200 až 20 000 záznamů.

Elektrický obvod je chráněn plastovým obalem o rozměrech 150 x 81 x 34 mm. Snímač je upevněn čtyřmi šrouby ke stěně v blízkosti průchodových dveří.



Obr. 23: *Blokové schéma snímače*

Na rozdíl od terminálu na vstupech tato snímací jednotka nemá klávesnici ani displej a pro ověření vstupu vizuálně a akusticky jsou aplikovány signalizační LED diody a akustická signalizace. Na svorkovnici nás budou zajímat především vstupy K2, K1, GND a +12V. K2 a K1 jsou určeny pro zapojení elektrického dveřního zámku. GND a +12V slouží k připojení zdroje napětí. Ostatní vstupy slouží k programování a komunikaci snímače.

7.2 Hardwarová odolnost

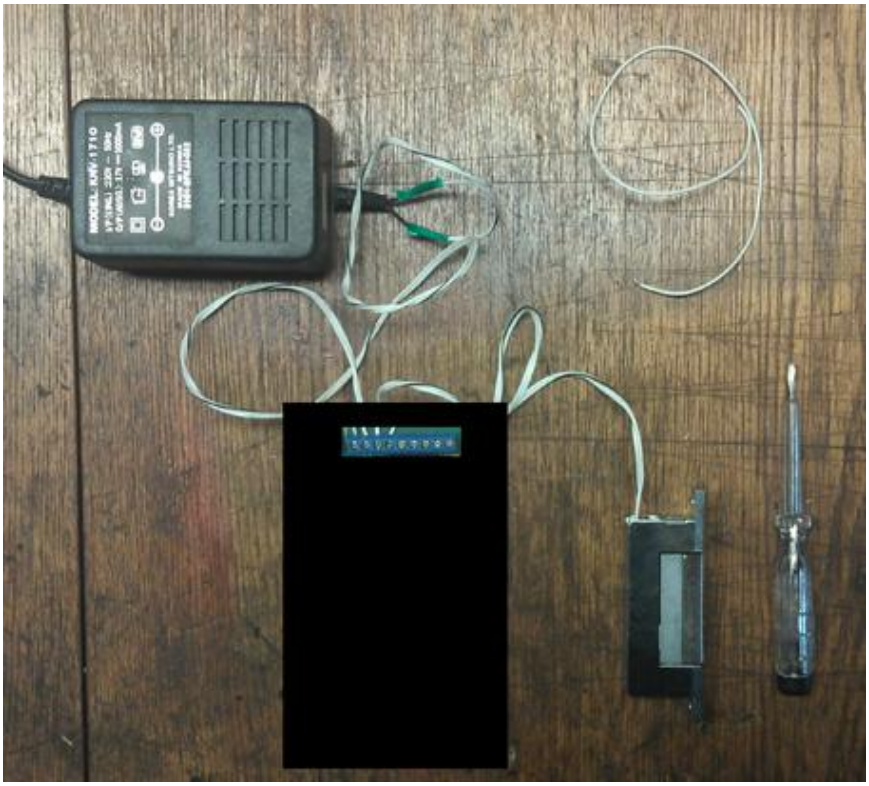
7.2.1 Průnik metodou propojení svorkovnice

Samotný kryt snímače je připevněn ke skeletu čtyřmi plastovými západkovými kolíky. K sejmutí krytu postačil menší plochý šroubovák a minimální síla. Západkové kolíky kladly jen malý odpor a z časového hlediska trvalo sejmutí ochranného krytu zhruba 3 sekundy.

Obr. 24: *Připevnění krytu snímače*

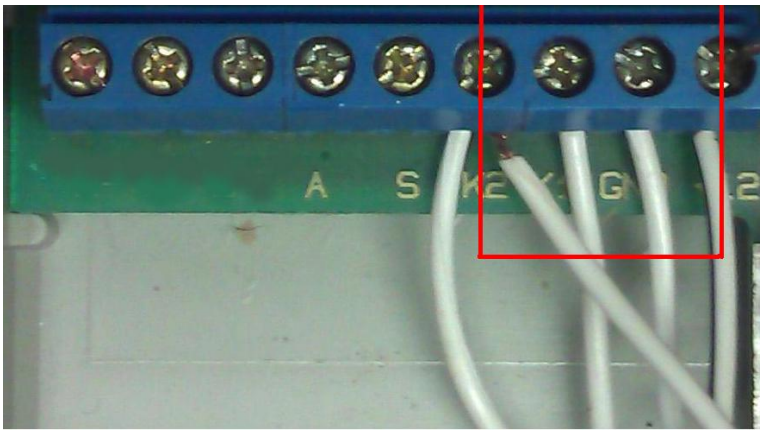
Sejmutím krytu snímací jednotky byl umožněn přístup ke kompletnímu elektrickému obvodu snímače. Absence tamperu dovoluje bez potíží pokračovat v činnosti, aniž by byl pokus o vniknutí do místnosti zaznamenán.

Celý pokus byl proveden laboratorně, kdy byl sestaven a nasimulován celý pokus proniknutí do střežené místnosti. K napájení snímače byl použit transformátor model KNV 1710 se vstupním napětím 230V střídavého napětí o frekvenci 50Hz a výstupním napětím 17V stejnosměrného napětí s proudem 1000mA. K propojení jednotlivých komponent byla použita jednoduchá dvojlinka. Na snímač byl připojen elektrický zámek dveří k ověření funkčnosti celého experimentu. K provedení celého pokusu byl zapotřebí ještě krátký vodič a malý plochý šroubovák.



Obr. 25: *Laboratorní zapojení analyzovaného snímače*

Experimentem bylo zjištěno, že při přivedení napětí +12V na elektrický zámek dveří uvedeme elektrický zámek k činnosti. Tedy stačilo pouze propojit svorky K2 a +12V vodičem a elektrický zámek umožnil vstup, aniž by to řídící jednotka zaznamenala.



Obr. 26: *Propojení svorek K2 a +12V*

K provedení celé operace by stačily maximálně dvě minuty s připraveným vodičem a šroubovákem.

7.2.2 Průnik metodou elektromagnetického impulsu

Další možností, jak obejít přístupový systém je metoda elektromagnetického impulsu (EMP). Celý systém pracuje na frekvenci 125 kHz, je proto možné využít elektromagnetických vlastností snímače k jeho prolomení. Kvůli nízké frekvenci musí být snímač osazen silnou anténou (cívkou) o mnoha závitech. Takto silná cívka produkuje silnou elektromagnetickou indukci do svého okolí. Obecně platí, že čím má cívka více závitů, tím je větší elektromagnetická indukce. Bylo zjištěno, že při vytvoření silného elektromagnetického impulsu dojde buď ke zničení procesoru, nebo k narušení pracovních procesů a vyvolání falešného povelu k otevření dveří. Při tak silných elektromagnetických impulsech dochází k narušení elektrického obvodu a k nepředpokládanému chování celého systému. V našem případě by to znamenalo přijít s nástrojem na vyvolávání elektromagnetických impulsů ke snímači a pár sekund nechat proudit impulsy do snímací jednotky. Zanedlouho dojde v určitém momentu k sepnutí relé ovládací jednotky a otevření elektrického zámku dveří.

7.3 Softwarová odolnost

Dalším prostředkem jak získat průchod analyzovaným snímačem jsou softwarové nástroje. Jádro problému se ukrývá v použité frekvenci přístupového systému. Nízká přenosová rychlost nedovoluje použít sofistikovanější kryptografické metody čipu nebo složitější bezpečnostní prvky. Čipy využívající frekvenci 125 kHz jsou tedy snadno duplikovatelné.

S pomocí počítačového softwaru a antény napojené na PC je možné prostřednictvím osciloskopu najít požadované frekvenční vlastnosti čipové karty a naskenovat identifikační číslo karty, čímž získáme kompletní podklady pro vytvoření funkční duplicitní čipové karty a tím možnost průchodu v daném bodě. Existují dvě možnosti, jak vytvořit identickou čipovou kartu se stejnými vlastnostmi jaké má originální čipová karta určena k průchodu: 1) Zapůjčením originální čipové karty a provedení její analýzy v domácích podmínkách (bezpečnější varianta) nebo 2) analýzou snímače přímo v terénu (větší pravděpodobnost odhalení).

Vyvarovat se těmto útokům je možné při použití vyšší frekvence v přístupovém systému (např.: 13,56 MHz a vyšší), které jsou již mnohem odolnější proti vnějším vlivům.

8 NÁVRH IMPLEMENTACE NOVÉHO RFID ZAŘÍZENÍ

Analýza ukázala, že systém fungující v subjektu je značně zastaralý a technologicky překonaný. V současné době existují výkonnější, spolehlivější a efektivnější identifikační systémy s vysokými bezpečnostními nároky. V této kapitole bude navrženo několik možností, jak celý systém zmodernizovat, zvýšit jeho bezpečnost, efektivitu a minimalizovat tak riziko vniknutí neoprávněné osoby do objektu.

1) Prvním základním komplexním bodem je přechod z dosud využívané frekvence 125 kHz na frekvenci vyšší např. 13,56 MHz. Čipy využívající tuto frekvenci byly prolomeny v prosinci roku 2012, nic méně prolomit kryptografickou ochranu tohoto čipu vyžaduje speciální zařízení a čas (několik hodin na dešifrování). Vyšší frekvence umožňuje rychlejší komunikaci mezi snímačem a čipem, což povoluje použít modernější a výkonnější kryptografické zabezpečení. S vyšší frekvencí odpadá také riziko spojené s elektromagnetickým polem. Konkrétně na snímač využívající frekvenci 13,56 MHz je potřeba cívka o jediném závitu.
2) Dalším prvkem modernizace je ochrana elektrického obvodu snímací jednotky. Tuto ochranu lze získat dvěma způsoby:
    a) implementací tamperu do snímací jednotky,
    b) prodloužením vzdálené antény od elektrického obvodu snímače.

Hlavním přínosem implementace tamperu je chránit snímač proti sabotáži. Je to jednoduchý spínač, který kontroluje, je-li kryt snímače v kontaktu se skeletem snímače. V případě sejmutí krytu dojde k přerušení kontaktu a následně k vyhlášení poplachu s přesnou lokalizací.

Při prodloužení vzdálenosti antény od snímače získáme další bezpečnostní opatření. V praxi znamená ukrytí celého snímače do střežené místnosti a anténu napojit pouze před vlastní vstup do místnosti. Tím zamezíme jakékoliv manipulaci s obvody snímače.

3) Celý systém by měl fungovat v tzv. „duálním rozhraní“. Hovoříme o napojení celého systému na server, možnosti sledování průchodů v reálném čase a zároveň možnosti některých snímacích jednotek pracovat v „offline“ režimu.
4) Modernizován by měl být také vstupní terminál za novější typ s dotykovým LCD displejem, větší kapacitou paměti, s moderním a efektivním nastavitelným uživatelským rozhraním. Toto opatření zajistí kompatibilitu komponent při přechodu na bezpečnější frekvenci 13,56 MHz.

5) Další možností jak zvýšit efektivitu a bezpečnost je zavedení biometrických senzorů do přístupové jednotky. Tím získáme další prvek identifikace, který se v kombinaci s použitím čipových karet v současné době stává prakticky neprolomitelným. Při využití kombinace biometrických metod identifikace hrozí pouze riziko proniknutí do hardwaru jednotky.

8.1 Analýza rizik nového systému

Přechod systému ze 125 kHz na 13,56 MHz přinesl významné zvýšení bezpečnosti a snížení rizik dálkového odposlechu a prolomení systému. Přesto však existují rizika, jak do systému proniknout. Nebezpečí může nastat např. v případě nevhodného umístění kabeláže od snímací jednotky. V dnešní době se mnohdy kabely umisťují do plastových lišt umístěných na zdi. Jsou pak snadno přístupné a vodiče vedoucí k tamperu lze jednoduše odhalit a vyřadit tak tamper z činnosti.

Předpokládá se, že pachatelé se do budoucna zaměří na vývoj softwarového prostředku pro prolomení snímací jednotky. Existují útoky postranními kanály, které využívají chyby v běžícím procesu, a na základě chybových hlášek je možné získat informace z čipu. Podrobnější popis tohoto rizikového útoku by vyžadoval prostor nad rámec zaměření této práce.

8.2 Ekonomické zhodnocení

Přechod ze systému využívajícího frekvenční rozhraní 125 kHz na 13,56 MHz z ekonomického hlediska může nabýt dvojího rozměru. Při aplikaci v menším podniku o jediném přístupovém bodu a počtu zaměstnanců v desítkách, nebude inovace příliš finančně náročná. Avšak při modernizaci v obrovském a rozsáhlém podniku se stovkami zaměstnanců a mnoha přístupovými body (např. městská hromadná doprava, městská karta) je vždy nutné počítat z větší investicí.

Největší finanční položkou je výměna čipových karet uživatelů a výměna rádio-frekvenčních modulů ve snímacích jednotkách. Čipová karta se cenově pohybuje v rozmezí 50-100 Kč / ks a rádio-frekvenční modul cca 1000 Kč / ks.

Praxe ukazuje, že při prolomení systému podniky na vzniklou situaci okamžitě reagují a identifikační systém modernizují bez ohledu na investiční náročnost.

ZÁVĚR

Východiskem teoretické části předložené práce byla skutečnost, že první systémy identifikace jsou známy už od 40. let 20. století a v praxi označovány jako RFID. RFID systémy po dobu své existence prošly řadou vývojových vylepšení a zdokonalení. V dnešní době je systém dobře známý a ve značné míře využívaný ve všech sférách. Nejčastější aplikace najdeme v logistice při skladování a sledování zásilek, ve zdravotnictví, v automobilovém průmyslu, ve vězeňství a v neposlední řadě v systémech identifikace osob. Stále však existují dvě strany názorů na využívání rádio-frekvenční technologie. Zastánci hovoří o revolučním průlomu identifikace a odpůrci poukazují na příliš velká rizika při používání RFID konkrétně o možnostech odcizení osobních dat a zcizení identity. Hovoří se také o rozdílech mezi RFID a biometrickými systémy. Faktem je, že každý čip a každé identifikační číslo lze nahradit. Biometrické údaje jsou naprosto jedinečné a těžko duplikovatelné. Biometrické systémy jsou však v současné době zatím příliš nákladnou investicí, proto dostávají přednost levnější metody identifikace – RFID. Obavy z odcizení citlivých údajů jsou tak zcela na místě. Dnešní bezpečnostní technologie nabízí však velké množství opatření, která se neustále zdokonalují a prolomit ochranu čipu se tak pro pachatele stává stále těžším úkolem. Technologie RFID v sobě ukrývá obrovský potenciál, který se neustále vyvíjí a zdokonaluje.

Praktická část práce se zaměřila na analýzu přístupového systému v objektu konkrétního podniku. Seznámila nás s komponenty využívanými při identifikačních procesech, jejich technickými parametry a následně rozborem nedostatků celého systému. V ověřovací analýze byl testován používaný snímač z hlediska hardwarové a softwarové odolnosti. Při testování bylo zjištěno, že je možné snímač několika různými hardwarovými i softwarovými metodami překonat a systém prolomit. Součástí rozboru je podrobný popis a vysvětlení slabých míst systému s návrhem protiopatření. Dalším dílem praktické části je také návrh nového identifikačního systému, který by umožnil bezpečnější, efektivnější a modernější provoz. Závěrečná část práce představuje analýzu rizik nového systému a rozbor ekonomické náročnosti modernizace stávajícího systému.

ZÁVĚR V ANGLIČTINĚ

The starting point for the theoretical part of the thesis was that the identification systems are a reference since the 40th Years and are being referred to as RFID. RFID systems for their existence have undergone a series of developmental improvements and enhancements. In today's world the system is well known and largely used in all spheres. Most applications can be found in logistics storage and shipment tracking, healthcare, automotive, prison, and not least in the systems of personal identification. However, there are two views on the use of radio-frequency technology. Proponents talk about a revolutionary breakthrough identification and opponents point to too much risk in the use of RFID in particular the possibility of theft of personal data and the possibility of identity theft. There is also talk about the differences between RFID and biometric systems. The fact is that each and every chip identification number can be replaced. Biometrics are unique and difficult to duplicate. Biometric systems are currently far too expensive investment, so take precedence cheaper methods of identification - RFID. Concerns about the theft of sensitive data are completely in place. Today's security technology, however, offers a large number of measures constantly improving protection and break the chip and the perpetrator becomes increasingly difficult task. RFID technology conceals the huge potential that is constantly evolving and improving.

The practical part is focused on the analysis of the access system in the building in specific company. Acquainted us with the components used in the identification process, their technical parameters and subsequently analyzing the shortcomings of the system. In an exploratory analysis was tested used sensor from its hardware and software resistance. During testing it was found that the sensor can be a number of different hardware and software techniques to overcome and break the system. The analysis is a detailed description and explanation of the weak points of the proposed countermeasures. Another part of the practical part is also proposed a new identification system that would enable safer, more efficient and streamlined operation. The final part of the paper presents a new system of risk analysis and performance analysis of economic modernization of the existing system.

SEZNAM POUŽITÉ LITERATURY

[1] SOMMEROVÁ, Martina. Základy RFID technologií. In: *RFID všb Ostrava* [online]. 2013 [cit. 2013-01-21]. Dostupné z: http://rfid.vsb.cz/miranda2/export/sites-root/rfid/cs/okruhy/informace/RFID_pro_Logistickou_akademii.pdf

[2] RFID technologie a RTLS. *RFID technologie a RTLS* [online]. 2012 [cit. 2013-01-21]. Dostupné z: http://www.barco.cz/?id=produkty&sel=15

[3] *ID-KARTA* [online]. 2013 [cit. 2013-01-21]. Dostupné z: http://www.id-karta.cz/identifikace-3/rfid-34/

[4] Ernst Alexanderson. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2013-01-22]. Dostupné z: http://en.wikipedia.org/wiki/Ernst_Alexanderson

[5] ROBERTI, Mark. The history of RFID technology. In: *RFID journal* [online]. 2002 [cit. 2013-01-23]. Dostupné z: http://www.rfidjournal.com/article/view/1338

[6] MoreRFID. *MoreRFID* [online]. 2004 [cit. 2013-01-23]. Dostupné z: http://www.morerfid.com/details.php?subdetail=Product&action=details&product_id=Yy8qUMjH

[7] ČERNÝ, Tomáš. *Technologie RFID možnosti jejich využití a nasazení v podniku*. Praha, 2007. Diplomová práce. Vysoká škola ekonomická v Praze.

[8] Základy RFID. In: *RFID portál* [online]. 2009 [cit. 2013-01-23]. Dostupné z: http://www.rfidportal.cz/index.php?page=rfid_obecne

[9] HANSON, Jeff. An Introduction to RFID. In: *Devx* [online]. 2006 [cit. 2013-01-29]. Dostupné z: http://www.devx.com/enterprise/Article/31108

[10] PRYCLOVÁ, Magda. RFID ve výrobě. *Identifikační systémy* [online]. 2007, roč. 50, č. 2 [cit. 2013-01-29]. Dostupné z: http://www.automatizace.cz/article.php?a=1635

[11] PTI's RFID Technologies. In: *Petro telemetrics Inc.* [online]. 2008 [cit. 2013-01-29]. Dostupné z: http://petrotelemetrics.com

[12] LECKEY, Mark. RFID chip. In: *Printed editions* [online]. 2011 [cit. 2013-01-29]. Dostupné z: http://www.printed-editions.com/artwork/mark-leckey-rfid-chip--1063

[13] The basics of RFID technology. In: *RFID journal* [online]. 2002 [cit. 2013-01-29]. Dostupné z: http://www.rfidjournal.com/article/view/1337/2

[14] Elektromagnetické spektrum. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-2013 [cit. 2013-01-30]. Dostupné z: http://cs.wikipedia.org/wiki/Elektromagnetick%C3%A9_spektrum

[15] BOHÁČOVÁ, Margita. Principy. In: *Elektrika* [online]. 2004 [cit. 2013-01-30]. Dostupné z: http://elektrika.cz/data/clanky/clanek.2005-02-26.6962238066

[16] ZVELEBIL, Vladislav. Použití metody RFID ve světě a u nás. In: *Automa* [online]. 2013 [cit. 2013-02-09]. Dostupné z: http://www.odbornecasopisy.cz/index.php?id_document=30655

[17] Near Field Communication. *Www.siongboon.com* [online]. 2012 [cit. 2013-02-14]. Dostupné z: http://www.siongboon.com/projects/2012-03-03_rfid/index.html

[18] Anteny stosowane w technice RFID. *Www.rfid4all.pl* [online]. 2012 [cit. 2013-02-14]. Dostupné z: http://www.rfid4all.pl/baza-wiedzy/technika-rfid/anteny-stosowane-w-technice-rfid

[19] Diskové tagy. *Inplastor* [online]. 2013 [cit. 2013-02-22]. Dostupné z: http://www.chipkarten.at/cz/rfidmedien/disctags/index.html

[20] RFID labels / Smart labels. *Unipress* [online]. 2013 [cit. 2013-02-22]. Dostupné z: http://www.unipress.de/en/rfid.php

[21] Smart cards. In: *Identicard* [online]. 2011 [cit. 2013-02-22]. Dostupné z: http://www.identicard.com/onlinestore/blog/tag/smart-cards/

[22] PCB tagy. In: *lux-ident* [online]. 2013 [cit. 2013-02-26]. Dostupné z: http://www.lux-ident.com/cs/produkty/prumysl-logistika/pcb-tagyhttp://www.lux-ident.com/cs/produkty/prumysl-logistika/pcb-tagy

[23] RFID glass tube. In: *Tradevy* [online]. 2007 [cit. 2013-02-26]. Dostupné z: http://www.tradevv.com/chinasuppliers/rfidandcard_p_159d54/china-Glass-Tube-Animal-Tag-LF-RFID-Glass-Tube.html

[24] Nahraďte čárový kód RFID zabezpečením. In: *Www.ceskestavby.cz* [online]. 2013 [cit. 2013-03-15]. Dostupné z: http://www.ceskestavby.cz/clanky/nahradte-carovy-kod-rfid-zabezpecenim-21845.html

[25] Nec představil RFID bránu pro výrobu. In: *Www.ceskestavby.cz* [online]. 2013 [cit. 2013-03-15]. Dostupné z: http://www.rfidportal.cz/index.php?page=clanek&art=223

[26] RFID a čárový kód. In: *Www.pointx.cz* [online]. 2009 [cit. 2013-03-15]. Dostupné z: http://www.pointx.cz/cz/nabidka-hardware/rfid-carovy-kod.html?PHPSESSID=72a700c86b4b07204a76fb4f3cf0440c

[27] Čárový kód. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-2013 [cit. 2013-03-16]. Dostupné z: http://cs.wikipedia.org/wiki/%C4%8C%C3%A1rov%C3%BD_k%C3%B3d

[28] Čárové kódy. In: *Www.kodys.cz* [online]. 2009 [cit. 2013-03-16]. Dostupné z: http://www.kodys.cz/carovy-kod.html

[29] DOKOUPIL, Aleš a Monika KOCHANÍČKOVÁ. RFID z pohledu bezpečnosti. *Www.odbornecasopisy.cz* [online]. 2009, č. 7 [cit. 2013-03-16]. Dostupné z: http://www.odbornecasopisy.cz/res/pdf/39331.pdf

[30] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management I.* 1. vyd. Zlín: VeRBuM, 2011, 316 s. ISBN 978-80-87500-05-7.

[31] APROKS S.R.O. *Katalog turniketů*. Praha, 2004.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACS access systems

b bit

CCTV Kamerový systém

DC Stejnosměrný elektrický proud

EAN European Article Number

EAS Electronic article surveillance

EMP Elektromagnetický impuls

EPC Electronic product code

EPS Elektrická požární signalizace

GHz gigahertz

HF High frequency

Kb kilobit

kHz kilohertz

LF Low frequency

Mb Megabit

MHz megahertz

MW Microwave frequency

MZS Mechanické zábranné systémy

NBÚ Národní bezpečnostní úřad

PCB Printed circuit board

PET polyethylentereftalát

PETG glykolem upravený PET

PVC polyvinylchlorid

PZS Poplachový zabezpečovací systém

RFID Rádio-frekvenční identifikace

RO Read-only

RTLS Real time location systém

RW Read-write

SKV Systém kontroly vstupů

TTF Tag talk first

UHF Ultra high frequency

WORM Write Once Read Many

SEZNAM ZOBRAZENÍ

Obr. 1**:** *Obecné schéma RFID* [9] 13
Obr. 2: *Aktivní tagy RFID* [6] 17
Obr. 3: *Pasivní RFID tagy* [10] 18
Obr. 4: *Pasivní RFID čipy* [11] a [12] 18
Obr. 5: *Elektromagnetická vlna* [15] 20
Obr. 6: *Užívání kmitočtových UHF pásem ve světě* [16] 22
Obr. 7: *RFID tag* [17] 23
Obr. 8: *RFID tagy* [18] 24
Obr. 9: *Diskové tagy* [19] 25
Obr. 10: *Smart labels – „chytré etikety“* [20] 26
Obr. 11: *Smart card – „chytrá karta“* [21] 26
Obr. 12: *PCB tag* [22] 27
Obr. 13: *Skleněné tagy* [23] 27
Obr. 14: *Stacionární čtečky* [24] a [25] 30
Obr. 15: *Mobilní čtecí zařízení* [26] 30
Obr. 16: *Čárový kód typu EAN* [27] 32
Obr. 17: *Turniket TPB S01 s otočnou tříramennou bariérou* [31] 40
Obr. 18: *Elektrický dveřní zámek* 40
Obr. 19: *Čipová karta* 41
Obr. 20: *Blokové schéma terminálu* 42
Obr. 21: *Ukázka seznamu snímačů v systému* 43
Obr. 22: *Ukázka měsíčního výpisu průchodů konkrétního uživatele* 43
Obr. 23: *Blokové schéma snímače* 45
Obr. 24: *Připevnění krytu snímače* 46
Obr. 25: *Laboratorní zapojení analyzovaného snímače* 47
Obr. 26: *Propojení svorek K2 a +12V* 47

SEZNAM TABULEK

Tab 1: *Třídy identifikace* [30] 35