Zabezpečení zboží RFID technologiemi

Merchandise security using RFID technology

David Polák

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:	**David POLÁK**
Osobní číslo:	**A09787**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Zabezpečení zboží RFID technologiemi**

Zásady pro vypracování:

1. **Popište systém RFID a vysvětlete základní principy této technologie.**
2. **Vysvětlete princip činnosti čárového kódu a definujte hlavní rozdíly oproti technologii RFID.**
3. **Vyjmenujte anténní systémy využívané v ochraně zboží, specifikujte jejich technické problémy a zdůvodněte selhávání systému v podobě planých poplachů.**
4. **Jmenujte moderní RFID systémy s ohledem na jejich využití v průmyslu komerční bezpečnosti.**
5. **Popište problematiku komerční bezpečnosti v oblasti zabezpečení zboží s možnostmi využití signálu alarmu podle ustanovení o zadržení.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **LAUCKÝ, Vladimír. Technologie komerční bezpečnosti I. Vyd. 3. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010, 81 s. ISBN 978-80-7318-889-4 (BROž.).**
2. **LAUCKÝ, Vladimír. Technologie komerční bezpečnosti II. Vyd. 2. Zlín: Univerzita Tomáše Bati ve Zlíně, 2007, 123 s. ISBN 978-80-7318-631-9 (BROž.).**
3. **IVANKA, Ján. Systemizace bezpečnostního průmyslu I. Vyd. 3. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009, 123 s. ISBN 978-80-7318-850-4 (BROž.).**
4. **IVANKA, Ján. Mechanické zábranné systémy. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010, 151 s. ISBN 978-80-7318-910-5 (BROž.).**
5. **Trestní předpisy: trestní zákon, trestní řád, výkon trestu odnětí svobody, výkon vazby, Probační a mediační služba, peněžitá pomoc obětem trestné činnosti, Rejstřík trestů, soudnictví ve věcech mládeže, zajištění majetku, amnestie : přestupky : zákon o přestupcích, paušální částka nákladů řízení : podle stavu k 7.11.2005. Ostrava: Sagit, 2005, 368 s. Úplné znění, č. 498. ISBN 80-720-8501-8.**

Vedoucí bakalářské práce: **JUDr. Jiří Kameník**

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

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

Ve Zlíně dne 24. února 2012

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

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

ABSTRAKT

Bakalářská práce se zabývá studiem technologie RFID. Fenomén radio-frekvenční identifikace zaznamenal v posledních letech velký pokrok, a protože je dnes velmi aktuálním tématem, rozhodl jsem se napsat právě o RFID. Teoretická část vysvětluje základní principy této technologie a popisuje systém RFID jako takový, včetně srovnání s nejrozšířenějším způsobem automatické identifikace, který představuje čárový kód.

Hlavním cílem studie je zhodnotit současný stav anténních systémů integrovaných do stávajících variant ochrany zboží, především ochrany zboží v obchodních řetězcích, aktuálně nejrozšířenějších prodejních místech pro spotřebitele. Riziko krádeží v obchodech má stále rostoucí charakter a tato alarmující skutečnost upozorňuje na problematiku komerční bezpečnosti navazující právě na systémy ochrany zboží, kde zejména důvod technického selhání a jeho následné vlivy na zákonné omezení svobody případného pachatele stále zaznamenávají výraznou limitaci. Z tohoto důvodu je nutné definovat restrikční pravomoci příslušných složek a následně nastavit kompetence na základě maximálního využití všech možných výhod komplexně podloženého právního výkladu současné legislativy v oblasti komerční bezpečnosti.

V praktické části se zaměřuji na specifikaci výše uvedeného cíle studie a pojednávám o dostupných možnostech využití všech moderních systémů technologie RFID v průmyslu komerční bezpečnosti se zaměřením na aplikaci při ochraně zboží.

Klíčová slova: RFID technologie, RFID tag, anténní systémy

ABSTRACT

This Bachelor's work concerns topic of FRID technology studies. In the recent few years, the Radio Frequency Identification phenomenon has made an incredible progress and as for RFID being these days a remarkable topic of frequent discussions, I took a decision to choose it as a subject for my bachelor's work. The theoretical part describes RFID system as such, as well as it explains the basic principles of the technology itself, including comparison to the most commonly used Automatic identification method represented by a barcode.

The main focus of this study is to evaluate a current status of aerial systems integrated to the present alternatives of wares protection, primarily to protection of goods within supermarket chains as these are currently being understood as the most favored sale places approached by a common consumer. Unfortunately, the risk of shoplifting in general has an extremely increasing character, which is only one of alerting facts to be taken into consideration as far as commercial safety is concerned. This leads us to the point of great importance of good quality wares protection systems, as faulty or insufficient protection of wares is still subsequently held with difficulties due to a very limited potential influence on statutory freedom restriction of eventual offender. For this reason it is important to define restrictive lawful powers to particular organs and constituents and consequently set up their competencies appropriately, using full advantage of a complex and well defined juristic explication of current legislative in a field of commercial safety.

In a practical part of this work I focus on an above mentioned goal of study and I deal with variety of reasonable and generally approachable utilization of all modern RFID technology systems used within commercial safety industry, being used specifically for wares' protection.

Keywords: RFID technology, RFID tag, antenna systems

Děkuji JUDr. Jiřímu Kameníkovi za podporu a vedení při tvorbě mé bakalářské práce.

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

Se stále rostoucí kriminalitou roste i počet trestných činů v podobě krádeží zboží v obchodech. Největším problémem pro prodejní subjekty je učinit taková opatření, která budou všem těmto nežádoucím činům předcházet. Základním cílem bezpečnostních opatření je snížit riziko na akceptovatelnou úroveň a ochránit tak cenná aktiva, neboli zamezit případným finančním či majetkovým ztrátám. Jedním z efektivních způsobů protiopatření se jeví preventivní zabezpečení zboží s využitím dostupných technických prostředků, které bezpečnostní průmysl nabízí. Jednou z takto používaných technologií je právě RFID technologie.

Dnes jsou bezpečnostní systémy stále více využívány a to nejen v obchodních řetězcích, kde je jejich používání na denním pořádku. Moderní RFID systémy, které v současné době nabízí široké spektrum možností, jejichž využití v praxi představuje velmi významnou roli především k identifikaci objektů a to zejména v její automatizaci, nachází svá uplatnění v mnoha oblastech bezpečnostního průmyslu. Vedle již zmiňovaného systému zabezpečení zboží se technologie RFID integruje v průmyslu komerční bezpečnosti do přístupových a docházkových systémů, nebo se využívá k lokalizaci objektů ve střeženém prostoru.

I. TEORETICKÁ ČÁST

1 SEZNÁMENÍ S TECHNOLOGIÍ RFID

RFID je zkratka, která vznikla z anglických slov Radio Frequency Identification a do českého jazyka byla přeložena jako radio-frekvenční identifikace. Jedná se o bezkontaktní automatickou identifikaci objektů, využívající vysokofrekvenční pásma ze spektra elektromagnetického vlnění k přenosu a ukládání dat. Technologii RFID můžeme obecně popsat třemi základními prvky systému. Mezi hlavní komponenty patří: RFID tag (elektronicky programovatelný čip – transpondér), RFID reader (čtečka) a middleware (řídící počítač).

S myšlenkou na vznik bezdrátové technologie zpracování informací přišla před lety největší maloobchodní firma WalMart, která před několika desetiletími stála u zrodu čárového kódu. Základem vývoje 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. [6]

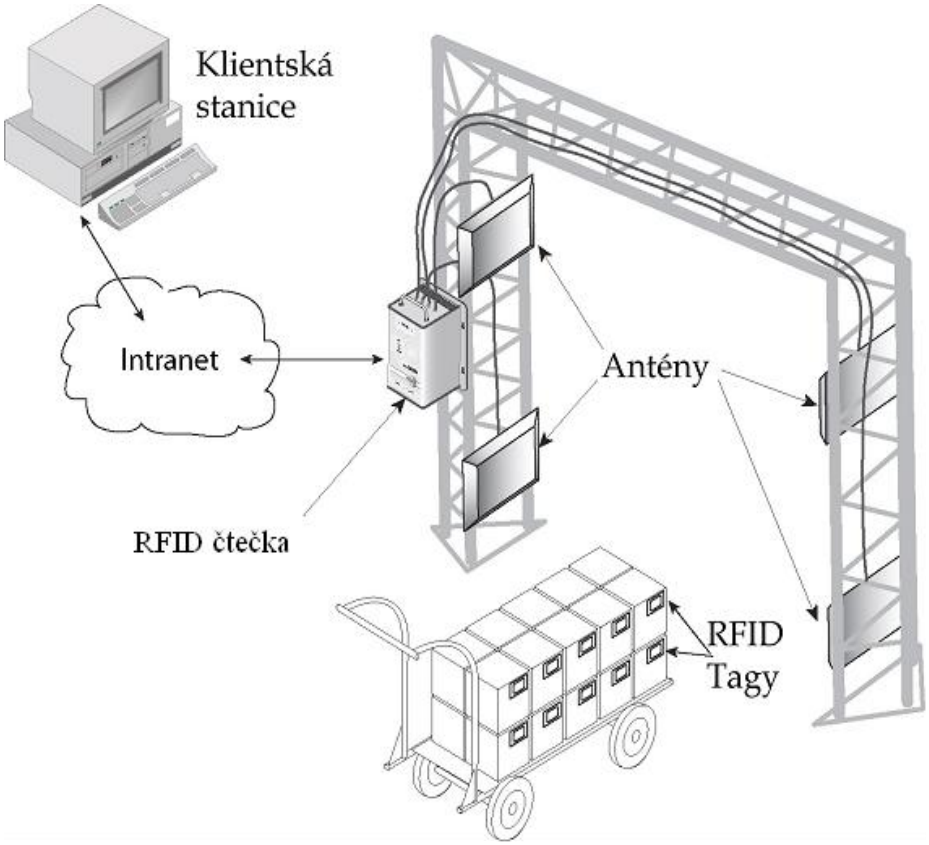
Automatická identifikace (AUTO ID) představuje registraci dat bez použití kláves. Využívání automatické identifikace vede k přesnosti, rychlosti, flexibilitě, produktivitě a efektivnosti při registraci velkého množství dat. Ruční zadávání dat trvá ve srovnání s AUTO ID poměrně dlouho a navíc při něm dochází k častým chybám. Chybovost lidského faktoru při fyzickém přepisování dat do počítače prostřednictvím klávesnice je velmi těžko odstranitelná. Výpadky soustředění, nepozornost, únava nebo překlepy z nedbalosti, patří k největším rizikovým faktorům lidské obsluhy. Eliminaci těchto chyb a zároveň rychlost načítání dat je možné zajistit jedině automatizací, právě AUTO ID. Technologie automatické identifikace jsou mnohoúčelové, spolehlivé a snadno se užívají. Bezkontaktní automatická identifikace se využívá v nejrůznějších prostředích, dokonce i v extrémních terénech a to vzhledem k dostupným materiálům.

RFID je technologií automatické identifikace, kde jsou data ukládána do tzv. RFID tagů. RFID tag je základ celého systému a představuje nosič informace, který se skládá z mikročipu, antény a popřípadě i baterie. Tyto tagy obsahují vždy svojí jedinečnou informaci, tzv. identifikátor určený výrobním číslem čipu. Informace se ukládá v digitální podobě a je realizována prostřednictvím čtečky za využití rádiových vln. Čtečka je tvořena vysílačem/přijímačem integrovaným s anténou a slouží nejen ke čtení, ale i k zapisování dat. Řídící počítač přebírá načtené údaje od čtecích zařízení a dále tyto informace zpracovává.

1.1 Princip činnosti RFID systému

Pro zjednodušení vysvětlím základní princip fungování RFID systému tvořeným tzv. pasivními tagy. Rozdíly mezi aktivním a pasivním systémem uvádím v kapitole RFID tag.

Čtecí zařízení generuje do okolního prostředí skrze anténu signál, konkrétně elektromagnetické vlnění na nosném kmitočtu rádiových vln. Anténa tagu, který se vyskytuje v dosahové vzdálenosti, přijme vlnu na základě rezonance. Rezonancí rozumíme kooperativní jev mezi dvěma objekty sdílejícími stejnou frekvenci. V systému RFID to v praxi znamená, že anténa tagu i anténa readeru jsou naladěny na stejné kmitočtové pásmo. Energie šířícího se elektromagnetického pole vyslaného readerem indukuje elektrické napětí na anténě tagu. Vzniklé elektrické napětí vyvolá střídavý proud, který je usměrněn a nabije kondenzátor (aktivní prvek elektrického obvodu schopný akumulovat energii) transpondéru. Elektrická energie je využita pro napájení mikroprocesoru. Aktivovaný mikročip vyšle čtečce zpět identifikátor v podobě kódovaných dat. Modulace (kódování) do rádiového signálu probíhá prostřednictvím rezistoru (aktivní prvek elektrického obvodu mající určitý elektrický odpor), který mění parametry antény. Modulovaný signál, který je zajištěn změnou impedance antény, je detekován čtečkou. Ve čtecím zařízení probíhá dekódování dat z čipu, převedení rádiových signálů do digitální informace, a následné předání řídícímu počítači, který je součástí middlewaru, k dalšímu zpracování. V některých případech si může čtečka přijatá data uložit, aby je sama zpracovala.



Obrázek 1 Schéma systému RFID [7]

2 ČÁROVÝ KÓD

Jednou z alternativ využití techniky automatické identifikace objektů jsou čárové kódy. Technologie čárového kódu je jedním z nejefektivnějších způsobů pořízení dat. Do stejné oblasti patří rovněž technologie RFID nebo magnetické kódy používané na kreditních kartách. Avšak čárové kódy jsou nejrozšířenější, a proto jsou dnes stále ještě nejvíce používanou technologií v automatické identifikaci. Je to dáno tím, že používání této technologie je pro uživatele celkem levným a nenáročným řešením. Čárovým kódem lze označit téměř vše, protože jeho užívání je univerzální a jednoduché.

2.1 Jak pracuje čárový kód

Čárový kód je zobrazením numerických informací. Skládá se z tmavých čar a světlých mezer, které jsou vytištěny na etiketu. Nosič informace v podobě tištěné etikety může mít různé podoby. Čárové kódy mohou být např. plastové, papírové, textilní, kovové, keramické atd.

Přesně definované šířky čar a mezer čárového kódu představují jednotlivé číslice či písmena. Aby bylo možné čárový kód přečíst, musí být snímač v krátké vzdálenosti namířen přímo na etiketu s kódem. Realizace samotného čtení bývá většinou uskutečněna pomocí laseru. Snímač, čtecí zařízení, vyzařuje v případě využití laseru červené světlo. Tmavé čáry toto světlo pohlcují a bíle mezery ho naopak odrážejí. Snímač umí zjistit rozdíly v reflexi, které přeměňuje na elektrické signály odpovídající šířce čar a mezer. Systém čárového kódu poté převede signály na číslice nebo písmena odpovídající příslušnému kódu. Prostřednictvím čtečky se tedy informace dostanou velmi rychle ke zpracování v počítači.

Existuje několik typů čárových kódů, z nichž každý má svou vlastní charakteristiku. Při volbě typu čárového kódu rozhodují různé aspekty. Základní kódy umí kódovat pouze číslice, jiné mohou kódovat vedle číslic i písmena nebo dokonce i speciální znaky. Nejznámějším a nejrozšířenějším typem čárového kódu je kód EAN. Tento kód může používat každý stát zapojený do mezinárodního sdružení EAN International. Kód EAN kóduje číslice 0 až 9, kde každá číslice je kódována dvěma čarami a dvěma mezerami. EAN využívá různé kódovací formáty. Základním formátem je EAN 13, ten obsahuje číslic 13. První dvě nebo tři číslice vždy určují stát původu výrobku, další 4 až 6

číslic určují výrobce a zbývající číslice, kromě poslední kontrolní číslice, která ověřuje správnost dekódování, specifikují konkrétní zboží.

Obrázek 2 EAN 13 [8]

2.2 Porovnání RFID a čárových kódů

Vedle čárových kódů se k identifikaci různých objektů využívá technologie RFID, která vzhledem k možnostem jejího využití má do budoucna velký potenciál. Identifikace na rádiové frekvenci je další generace identifikátorů navržených k bezkontaktní identifikaci objektů. Jde o systém identifikace, který navazuje na systém čárových kódů, a proto se o RFID technologii často hovoří jako o nástupci právě čárových kódů. Přestože by RFID mohla v příštích letech nahradit systém čárového kódu, tak si tohle v současné době neklade za svůj cíl, a spíše doplňuje čárové kódy o další aplikační možnosti. Existuje řada aplikací, kde je nejvýhodnější použít kombinaci obou těchto identifikačních technologií, jako například ve smart labelech.

Výhody čárového kódu:

- jednoduchý tisk včetně nízkých nákladů (pro nejjednodušší potištění stačí libovolná tiskárna)
- možnost převést téměř libovolnou informaci do čárového kódu
- jedna z nejpřesnějších a nejrychlejších metod k registraci většího množství dat
- možnost ověřování správnosti čtení, kontrolní mechanizmy jsou obsaženy v kódu

Nevýhody čárového kódu:

- ke čtení je nutno využít speciální zařízení s optickými snímači
- nutnost přímé viditelnosti při snímání
- při snímání musí být vždy kód orientovaný směrem ke snímači

Výhody RFID technologie:

- bezkontaktní povaha / pro čtení a zápis dat není potřeba přímá viditelnost ani přesné polohování
- výrazně vyšší datová kapacita nosiče / možnost zapsat velké množství informace do čipu
- rychlost čtení dat
- digitální získávání informace
- snížení chybovosti
- mobilita
- možnost mnohačetného čtení - možnost načíst najednou velké množství RFID tagů na velkou vzdálenost-hromadná identifikace tagů v jednom okamžiku
- variabilita média
- RFID tag lze umístit do značeného objektu tak, aby nebyl vystaven vnějším vlivům a proto je RFID tag daleko odolnější než štítek s čárovým kódem, např. proti mechanickému poškození, teplotě, vlhkosti či povětrnostním podmínkám
- přenosu dat nebrání špatné optické ani atmosférické podmínky
- aktivní čipy přináší nové možnosti funkcionality do identifikačního procesu
- schopnost identifikovat nejen druh zboží, ale i každou jednotku zboží zvlášť
- RW tagy umožňují aktualizovat či doplňovat již zapsaná data v tagu/možnost přepisování dat
- bezobslužný provoz/čtecí zařízení pracují bez nutnosti neustálé obsluhy - šetří náklady spojené s obsluhou

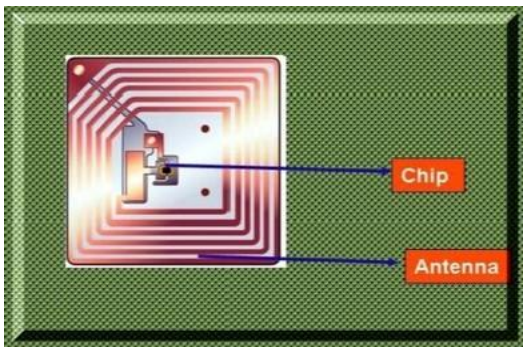
Nevýhody RFID technologie:

- vyšší ceny nosičů informací i dalších prvků systému (terminály, antény, snímače)
- nemožnost číst informace pouhým okem / kompenzuje se to používáním smart-labelů s možností potisku
- výkonnost signálu může být omezena fyzikálními vlastnostmi RF zařízení (negativní vliv kovů a kapalin)

3 STRUKTURA RFID SYSTÉMU

3.1 RFID tag

Paměťové médium využívané v technologii RFID se nazývá RFID tag neboli transpondér. Význam slova tag vznikl spojením anglických slov transmit (přenos) a response (odpověď). RFID tag je vlastně nosič informací tvořící základ systému RFID a jeho hlavní funkcí je digitální uložení dat do vnitřní paměti a následné poskytnutí těchto uložených údajů RFID systému. RFID tag se skládá ze dvou a v případě aktivních tagů tří součástek. Tag musí vždy obsahovat mikročip a anténu. Velikost tagu nejvíce ovlivňuje velikost integrované antény, která je jeho největší komponentou. Anténa je vodivý element umožňující přijímat a vysílat data a její rozměry jsou tak závislé na použitém frekvenčním pásmu. Velikost samotného čipu je dnes již menší než 1mm. Aktivní tagy dále obsahují velmi malou baterii. Všechny tyto části jsou pak umístěné v zapouzdření.



Obrázek 3 RFID tag [9]

3.1.1 Dělení tagů dle účelu použití

Forma, tvar, materiál a rozměry tagů bývají různé. Ze specifik jednotlivých aplikací vyplývá, že RFID tagy mohou sloužit k různým účelům. Proto realizace tagu velmi úzce souvisí s aplikací, které bude sloužit. Tagy jsou dnes neustále vyvíjeny pro nové účely využití tak, aby se co nejlépe přizpůsobily daným podmínkám. Rozdělení dle provedení zahrnuje rozmanitost tvarů, materiálů a rozměrů. Zapouzdření tagu ovlivňuje životnost a možnost použití v různých prostředích, zatímco čip udává kapacitu a anténa kvalitu komunikace. Na základě těchto vlastností z hlediska výrobní technologie existují spousty tagů v několika variantách provedení. Rozšířené podoby tagů jsou např. mince, smart card

(formát platební karty), skleněný tag, smart label (kombinace RFID tagu a etikety s čárovým kódem).

3.1.2 Dělení tagů dle typu napájení

Problematika typu napájení rozděluje RFID systémy na aktivní a pasivní. Pasivní systém obsahuje tagy, které nemají vlastní zdroj energie. Energii jim dodává čtecí zařízení, které vysílá elektromagnetické pole prostřednictvím rádiového signálu a poskytuje tak energii pasivnímu tagu. Čtení zprávy probíhá na principu RTF - reader talks first. Pasivní systémy jsou primárně nasazovány pouze k identifikaci objektů. U aktivních RFID systémů, které využívají tagy s vlastním zdrojem napájení, rozšiřujeme funkci identifikace předmětů o další užitečné funkce, jako jsou např. měření teploty, lokalizaci atd. Činnost aktivních tagů je tedy nezávislá na čtecím zařízení, a proto může také obsahovat snímače pro měření fyzikálních veličin či schopnost optické a akustické komunikace s uživateli. Aktivní čipy vysílají samy své údaje do okolí. Tento komunikační proces nazýváme TTF-tags talk first. RFID tagy jsou tedy v základu dvojího typu podle toho, jestli mají nebo nemají vlastní baterii. Z hlediska zdroje energie rozlišujeme tagy aktivní, pasivní a semipasivní.

Aktivní RFID tagy:

Jedná se o tagy s vlastním zdrojem energie v podobě integrované baterie, která napájí elektronický obvod, posiluje signál a umožňuje tak čipu vysílat skrze anténu své údaje do okolí. Výhodou je vysoká čtecí vzdálenost (stovky metrů) a větší vysílací výkon, což v některých aplikacích zajistí lepší efektivitu ve stíženém prostředí. Velikost paměti dosahuje až 100 kB. Tagy jsou však v důsledku vestavěné baterie dražší a těžší. Mají nižší odolnost na teplotu a je nutné provádět výměnu baterie. Pro šetření vlastní baterie lze tagy uvést do úsporného režimu. Sníží se tak spotřeba energie a prodlouží se životnost baterie. Zpětné probuzení, aby mohla probíhat standardní komunikace, zajistí zachycení signálu vyslaného čtečkou. Těchto tagů se využívá např. ke sledování osob, vozidel nebo zvířat a všude tam, kde lze čip opětovně použít.

Pasivní RFID tagy:

Tyto tagy nemají vlastní baterii a jsou závislé na přísunu energie ze čtecího zařízení, které tyto tagy napájí přímo z vyslaného elektromagnetického pole. Nevysílají do okolí žádné signály, pracují jen v okamžiku, kdy jsou v dosahu čtečky a mají s ní navázanou komunikaci. Výhodou jsou zanedbatelné požadavky na údržbu a dlouhá doba životnosti. Ve srovnání s tagy aktivními jsou cenově dostupnější. Mají různou akční vzdálenost, praktická vzdálenost čtení se pohybuje mezi 10 cm a několika metry. V současné době jsou v aplikacích nejvíce rozšířeny právě pasivní tagy.

Semipasivní tagy:

Tagy obsahující vlastní napájecí zdroj stejně jako tagy aktivní. Baterie je ale papírově tenká a tak nemá dostatečnou sílu k posilování signálu, proto slouží k napájení integrovaných obvodů nebo pro uchování energie vyslané čtečkou pro pozdější využití. Tato technologie spojuje výhody pasivních a aktivních systémů dohromady. Čtecí vzdálenost může být až desetinásobek pasivního dosahu čtečky. Výhodou je také vyšší životnost baterie než u čipů aktivních. Semipasivní tagy umí pracovat i v době, kdy reader nevysílá nebo není v dosahu a tak jsou často vybaveny senzorikou pro měření teploty, tlaku, vlhkosti vzduchu, navíc umí měřit třeba i vibrace. Tímto rozšiřují možnosti pasivních tagů.

3.1.3 Dělení tagů dle typu paměti

Z hlediska uchování informací a možnosti zápisu rozdělujeme tagy do tří skupin:

RO (Read-Only): Tagy určené pouze pro čtení. Obsahují pouze sériové číslo, které je zakódované při výrobním procesu a dále ho již nelze měnit. Nejčastěji se aplikují jako vstupní zařízení u přístupových systémů.

WORM (Write ONCE Read Many): Tagy určené také jen pro čtení dat. Informace do tagu nejsou naprogramovány ve výrobě. Data vypaluje prodejce či dodavatel. Zapsané údaje podobně jako u tagů RO nejsou přepisovatelné. S WORM tagy se nejčastěji setkáme v knihovně, kde slouží k evidenci majetku místo čárového kódu.

RW (Read Write): Uložené údaje lze mnohokrát přepsat. Tyto tagy mají adresovatelnou paměť, která se snadno mění. Kapacita paměti nabízí možnost uchování velkého množství dat. Tyto data pak lze podle potřeby libovolně přepisovat. Využívají se u procesů ve skladech, jedná se o sledování zboží ve výrobě.

3.2 RFID čtečka

Zařízení vytvořené na komunikaci s RFID tagem se nazývá RFID reader. Přestože slouží primárně ke čtení dat uložených na RFID čipu, je tento přístroj specializovaný nejen na čtení, ale i zápis či programování dat tagu. Reader je v podstatě mikropočítač propojující RFID tag a řídící počítač. V základním provedení je tvořen elektronickým vysílacím/přijímacím obvodem s dekodérem a anténou. Vylepšené čtecí zařízení může být vybaveno vlastním operačním systémem se základní softwarovou funkcionalitou. Standardní čtecí zařízení načítá data a ve stejné podobě je předává serveru (middlewaru). Složitější čtečky umí data před předáním sami filtrovat a usnadnit tak serveru práci.

Anténa může být jedna, ale někdy se využívá i více antén, které bývají buď integrované, nebo externí. Tyto antény vysílají rádiové vlny a také přijímají signály vyslané čtečkou. Hlavní funkcí dekodéru, rádiového rozhraní, je modulace, demodulace, přenos a příjem rádiového signálu. Aby přenos rádiového signálu vyhovoval požadavkům, jsou většinou přenosové cesty pro příjem a vysílání odděleny. Řídící mozek celé čtečky je tzv. řídící jednotka, která obsahuje mikroprocesor a pomocné obvody. Hlavním úkolem mikroprocesoru je zpracovat přijatá data. Díky připojeným pomocným obvodům komunikuje nejen s RFID tagy, ale i s počítačem řídícím celý RFID systém.

Komunikace, která probíhá mezi tagem a readerem se řídí určitými standardy. Systém může zahrnovat mnoho čteček od různých výrobců, které nejsou vždy úplně totožné. Různé čtečky jsou vyrobeny s různými vlastnostmi a pro komunikaci s tagy používají různý komunikační protokol. Jednotné rozhraní pro čtečky s různým chováním poskytuje řídící software, middleware.

Základní funkce RFID readeru:

- Čtení údajů uložených v paměti RFID tagu
- Přenos dat z a do řídícího počítače
- Dodávání energie pasivním tagům
- Zapisování dat do tagů typu RW

Nástavbové funkce RFID readeru:

- Filtrace dat
- Ovládání vstupně-výstupních integrovaných obvodů
- Šifrování a ochrana integrity dat
- Realizace antikolizních opatření k zajištění RW komunikace s mnoha tagy najednou- schopnost čteček vyřešit problém vzájemného rušení (pokud jsou blízko sobě) přeladěním na jiný kanál v určitém pásmu
- Ověřování tagů – snaha zabránit podvodům a neoprávněného přístupu do systému
- Schopnost pracovat s tagy různých frekvencí

Ve srovnání s kategorizací RFID tagů je rozdělení readrů značně jednodušší. Rozlišujeme dva typy čtecích zařízení na úrovni rádiově-identifikační komunikace. Na trhu nalezneme nejrůznější varianty stacionárních, mobilních nebo tunelových čteček. Zda je reader mobilní, nebo stacionární závisí na dané konstrukci.

Stacionární čtečky jsou nepřenosné, pevně vestavěné na určitém místě dle potřeby (např. u vstupu do skladu). Nejsou konstruovány pro přímou manipulaci člověka se čtečkou. Řídící systém mívají oddělený od antény. Externí anténu je možno doplnit připojením dalších antén, které zajistí vetší pokrytí prostoru ke čtení signálu. Hovoříme zejména o čtecích bránách nebo o vysokozdvižných vozících. Brány neboli tunelové čtečky se skládají ze systému čteček a jejich antén. Vstupní/výstupní bránu je možné zabudovat do ostění. Využívají se v průmyslových aplikacích.

Mobilní čtečky jsou konstruovány jako jeden přístroj pro držení v ruce. Obě součástky jsou tedy implementovány v jednom společném pouzdře. Mobilní terminály jsou

přenosná čtecí zařízení s vlastním operačním systémem a obrazovkou. Jsou stavěné do průmyslových prostředí, a tak jsou odolné vůči pádu. Vedle bezdrátových mobilních čteček se vyrábí i varianty s kabelem. Hybridní zařízení je pak schopno načítat nejen data z tagů, ale dokonce i čárové kódy.

Obrázek 4 Mobilní RFID terminál [10]

3.3 Middleware

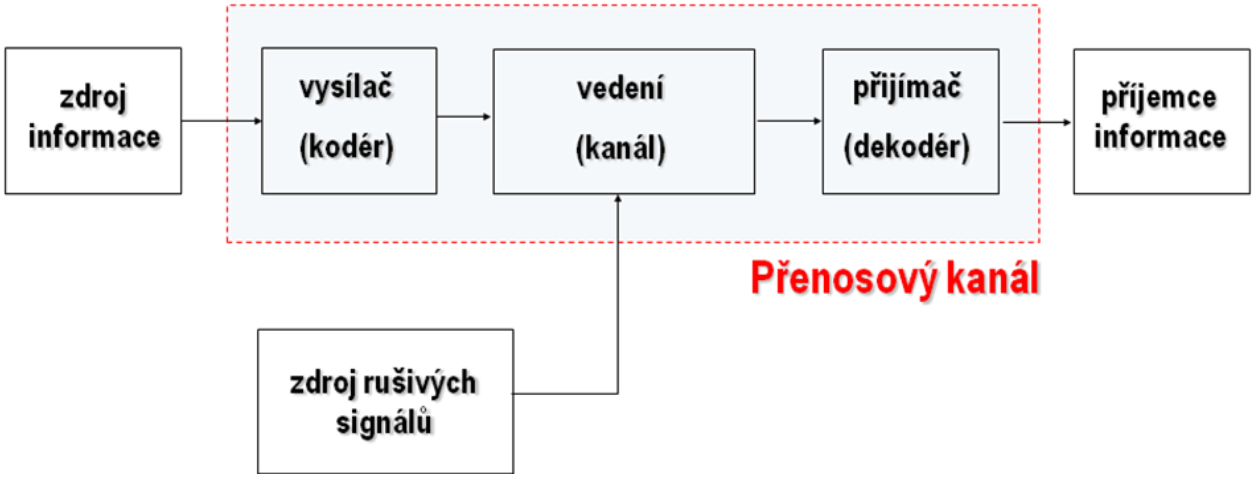
O Middlewaru hovoříme zjednodušeně jako o řídícím softwaru, ale můžeme se setkat i s informací, že middleware je specializovaný hardware. Skládá se z podpůrných systémů, které tvoří řídící počítače, databáze a telekomunikační sítě a ze systémů na strategické úrovni řízení. Middleware obecně představuje soubor služeb, který umožňuje spolupráci mezi procesy běžícími na více zařízeních. Tato technologie je nejčastěji používána k podpoře a zjednodušení složitých systémů a tak je middleware nedílnou součástí moderní RFID technologie. V RFID terminologii se tedy jedná o software běžící na serveru. Dovede koordinovat a provádět správu čteček v síti a ve struktuře systému tak zajišťuje filtrování dat ze čtecího zařízení a postupuje je dále ke zpracování podnikové aplikaci.

Schopnost komunikovat se čtečkami s různými komunikačními protokoly od různých výrobců umožňuje tomuto softwaru řídit celou populaci čteček obsažených v samotném systému RFID. Jeho hlavní úlohou je prvotně zpracovat data načtená jednotlivými čtečkami. Mezi základní funkce middlewaru patří vedle správy dat i filtrace a

analýza získaných údajů. Výsledky dále uchovává v databázi a poskytuje je přes stanovené rozhraní dalším aplikacím.

4 PŘENOS RÁDIOVÝCH VLN

Přenos je jednou ze základních operací s informacemi. Všechny komunikační systémy vychází z obecného komunikačního systému, který lze znázornit v následujícím schématu:



Obrázek 5 Obecný komunikační systém [11]

Zdroj informace musí mít k dispozici zásobu symbolů, ze kterých zprávu sestaví. Pro přenos musí být tyto symboly převedeny na fyzikální signály, které jsou technicky schopné přenosu. Informace tedy bývá přeložena do řeči kanálu, což v praxi znamená kódování zprávy do signálů. Přenosový kanál představuje souhrn prostředků sloužících k přenosu signálu od zdroje k příjemci. Po přenosu dat dochází k dekódování zprávy, neboli signály se převádí zpět do původních symbolů.

V systému RFID zastupuje zdroj informace RFID tag. Symboly pro sestavení zprávy jsou logické jedničky a nuly. Tato digitální informace se pro potřeby přenosu kóduje do rádiového signálu, který čtecí zařízení jako příjemce dekóduje zpět do podoby binárního čísla (řeči mikropočítače).

4.1 EPC (Electronic Product Code)

Radio-frekvenční identifikace je obecný název pro technologie určené k identifikaci objektů popřípadě osob, která přenáší data přes rádiové vlny. RFID tag, tedy komunikující mikropočítač, uchovává jedinečné číslo. V současnosti se nejvíce osvědčilo zaznamenání čísla EPC. EPC znamená v překladu elektronický kód produktu a jde o jednoduchý kompaktní kód, který jednoznačně identifikuje daný tag. Představuje sériové číslo zapsané v mikročipu sloužící prakticky jako identifikátor. Tento jedinečný kód obsahuje informaci, kterou RFID tag předává RFID readeru.

Společnosti využívají pro automatickou identifikaci různých identifikačních znaků. Většina identifikátorů užívaných při RFID nejsou v globálním měřítku harmonizovány. Číselné schéma EPC je globální standard pro RFID identifikaci. Jeho smyslem je vytvoření mezinárodního standardu a sjednotit tak RFID pro celý svět. Stal se klíčem k získání informací o produktu, který existuje v celosvětové síti. Přesto se vždy najdou důvody pro firmy a jejich aplikace, aby využily libovolnou identifikaci, která nespadá do globálního standardu a neumožňuje snadnou kompatibilitu mezi přístroji od různých výrobců. EPC je spravován a přidělován světovou organizací Global Standards (GS1).

Struktura kódu EPC umožňuje definovat vedle výrobce nejen název produktu (př. Cola light), ale i jeho výrobní číslo konkrétní šarže, a tak je možné zajistit rychlou a přesnou identifikaci dalších údajů, jako je např. datum výroby, datum spotřeby atd. EPC dokáže, na rozdíl od jiných kódů, jedinečně identifikovat každou jednotku zboží. Kombinace RFID a EPC představuje účinný nástroj současné moderní automatické identifikace.

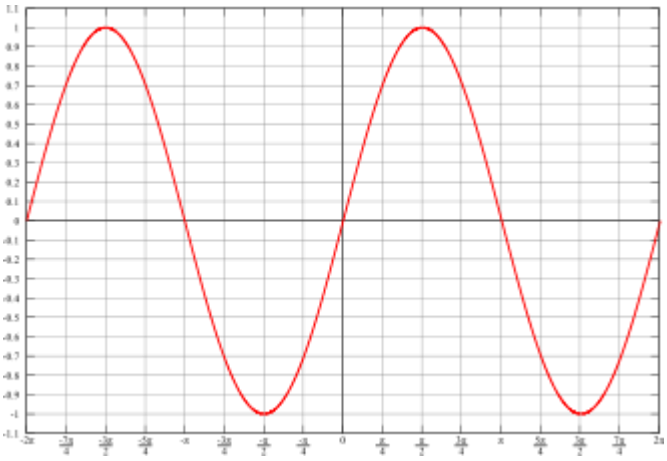
Dnes se používají EPC o velikosti 64 nebo 96 bitů. Jejich struktura se však může lišit, je udávána vždy výrobcem, ale většinou jsou bity rozděleny do jednotlivých kategorií velmi podobně.

8 bitů	**Hlavička** - velikost, typ, struktura, verze EPC	Přiděleno EPC global
28 bitů	**Informace o firmě** - definice výrobce (268 miliónů firem)	Přiděleno EPC global
24 bitů	**Třída výrobku** - definice druhu produktu (16 miliónů tříd)	Přiděleno vedením společnosti
36 bitů	**Sériové číslo produktu** - definice jednotky zboží (68 miliónů čísel)	Přiděleno vedením společnosti

Tabulka 1 Struktura 96 bitového EPC kódu [6]

4.2 Přenosová pásma

Technologie RFID, založená na pracovním kmitočtu v oblasti elektromagnetického vlnění o stanovené frekvenci může, jak již z názvu vyplývá, využívat celého spektra vln rádiových. Radio-frekvenční vlny jsou vlnami elektromagnetickými, které tvoří pohybující se elektrony. Elektromagnetické vlnění se šíří rychlostí světla 300 000 km/s. Skládá se z oscilujících navzájem kolmých elektrických a magnetických polí, proto můžeme elektromagnetickou vlnu znázornit sinusoidou. Rozpětí rádiových vlnových délek se pohybuje v rozmezí 1 mm a 1000 km, což odpovídá frekvenci 30 Hz až 300 GHz. Vztah mezi frekvencí a vlnovou délkou vyjadřuje matematický vzoreček: $\lambda = c/f$. Vlnová délka (λ) je přímo úměrná rychlosti světla (c) a nepřímo úměrná frekvenci (f).



Obrázek 6 Graf funkce sinus [12]

Vlastnosti a následné chování systémů RFID jsou odlišné v závislosti na zvolené frekvenci. Existují čtyři hlavní třídy frekvenčních typů pro RFID, které využívají převážně rádiových vln o provozní frekvenci 30 KHz až 5,8 GHz. Vyšší frekvence zajišťují rychlý přenos dat, zvládnou tak větší datové toky. Využívají malých antén, které jsou levnější, než ty velké. Malá anténa umožňuje menší rozměry komponent systému RFID.

Název	**Rozsah**
Low Frequency (LF)	125 – 134 kHz
High Frequency (HF)	13,56 MHz
Ultra High Frequency (UHF)	860 – 960 MHz
Microwave (MW)	2,4 a 5,8 GHz

Tabulka 2 Rozdělení kmitočtových pásem

Nízká frekvence (LF):

- krátký dosah cca 20 cm (téměř kontaktní čtecí vzdálenost)
- nízká přenosová rychlost
- využívá především pasivních tagů
- tagy s nepřepisovatelnou pamětí – pouze pro čtení
- odolné přítomnosti kovů a kapalin
- frekvenční rozsah LF přijímán celosvětově
- nejstarší a nejdéle používaný typ
- velká anténa – vyšší cena
- využití: čipování - evidence zvířat, parkovací systémy, identifikační průkazy, přístupové a docházkové systémy

Vysoká frekvence (HF):

- krátký dosah, čtecí vzdálenost cca 1m
- nižšší přenosová rychlost
- využívá zejména pasivních tagů
- varianty tagů RO nebo RW
- slušný výkon v přítomnosti kovů a tekutin
- velká anténa – vyšší cena
- možnost potiskovat (smart label)
- frekvenční rozsah HF přijímán celosvětově
- využití: knihovní systémy, zdravotnictví, identifikační karty (e-peněženky, přístupové a docházkové systémy), evidence zboží v regálech

Velmi vysoká frekvence (UHF):

- dlouhý dosah, přenos informace na vzdálenost jednotek metrů
- vysoká přenosová rychlost (až 1000 načtených čipů za sekundu)
- možnost číst, zapisovat i přepisovat
- využívá aktivních i pasivních tagů
- malá anténa - nízká a stále klesající cena
- nelze číst přes kapaliny, obtížné čtení na kovu (špatný výkon v jejich přítomnosti)
- možnost potiskovat (smartlabel)
- legislativní omezení rozdělují svět na tři regiony: USA, Kanada a Mexiko: 902 – 928 MHz, Evropa a Afrika: 865 – 869 MHz, Japonsko a Asie: 950 – 956 Mhz [6]
- využití: knihovní systémy, docházkové systémy, supply chain (zásobovací řetězec), obchodní řetězce, sklady, výroba (výrobní proces), logistika (identifikace zboží a logistických jednotek, identifikace palet)

Mikrovlnné pásmo (MW):

- velká čtecí vzdálenost, dosah desítky metrů
- vysoká přenosová rychlost
- frekvenční pásmo blízko k technologii Wi-Fi
- možnost číst, zapisovat i přepisovat
- nejběžněji využívá aktivní či pasivní tagy, možnost aplikovat semipasivní tagy
- malá anténa
- špatný výkon v přítomnosti kovů a kapalin- protože délka antény je nepřímo úměrná frekvenčnímu rozsahu
- MW pásmo je přijímáno celosvětově
- využití: dodavatelský řetězec, systémy elektronického mýta, identifikace vozidel a pohybujících se předmětů (R-t L service)

4.3 Výkonnost systému

Selhávání RFID je pro nás v praxi velmi důležitým aspektem. Aby byl systém účinný, musí jeho výkon dosáhnout určitých hodnot. Na komunikaci mezi komponentami systému, a s tím související kvalitu čtení zpráv, působí vnější podmínky. Interakce s okolním prostředím je závislá na pracovním kmitočtu. RFID systémy se provozují na různých vlnových délkách. Nosný kmitočet neboli frekvence je zásadním parametrem pro výkonnost systému. Určuje dosah čtení, rychlost snímání a zapisování údajů a použitelnost v různém prostředí. Čím vyšší frekvence, tím rychlejší přenos dat a možnost delší komunikační vzdálenosti mezi readerem a tagem. Nevýhodou vysoké frekvence oproti nižšímu kmitočtu je citlivost na přítomnost problematických materiálů (např. kov, voda, uhlík).

K problémovým materiálům, které nepříznivě ovlivňují šíření rádiových vln, patří především kapaliny a kov. Pokud aplikujeme RFID systém do místa, kde kapaliny mohou nějakým způsobem zasahovat do pracovního prostředí systému v podobě vlhkosti vzduchu nebo způsobí mokrý povrch, je vhodné zvolit frekvenční pásmo HF. Frekvence s dlouhou vlnovou délkou lépe pronikají do vody, zatímco signály vysokých frekvencí jsou dobře absorbovány ve vodě (UHF, MW).

Přítomnost kovového materiálu také nepodporuje výkonnost systému, narušuje zejména vysokofrekvenční pásma. Negativní vliv kovu na funkci systému RFID se projevuje nežádoucími odrazy signálu a možným vznikem stojatého vlnění. Pokud se kovové těleso vyskytne mezi čtečkou a tagem, úplně brání komunikaci - přenosu informací, protože rádiové signály nemohou proniknout skrz kov. Kovový materiál činní v praxi potíže především v podobě planých poplachů u radio-frekvenčních systémů využívaných k předmětové ochraně volně vystaveného zboží na prodejnách. Viz. praktická část: Technické problémy ochrany EAS.

RFID systémy jsou citlivé na rušení elektromagnetickými vlnami. Problematikou elektromagnetického rušení se zabývá EMC, elektromagnetická kompatibilita. EMC rozdělujeme na EMS (elektromagnetická susceptibilita - odolnost) a EMI (elektromagnetická interference - rušení). Pokud dané zařízení splňuje požadavky EMC, můžeme říci, že přístroj je dostatečně odolný elektromagnetickému rušení a zároveň hodnota vyslaného nežádoucího rušivého signálu, kterou vysílá do okolního prostředí, nepřekračuje určitou standardizovanou mez. Splní-li zařízení tyto parametry, označujeme

ho za elektromagneticky kompatibilní. Naneštěstí rušivé signály se v okolí integrovaných systémů mohou vyskytovat a my se tímto nesmíme nechat zaskočit. Náchylnost na interferenci je u RFID závislá na frekvenčním pásmu, ve kterém jednotlivé komponenty systému pracují. Mikrovlnné pásmo je odolné nejvíce a naopak pásmo HF je nejzranitelnější, jelikož většina komunikačních systémů využívá tuto frekvenci velmi často.

Z důvodu elektromagnetického rušení může v praxi někdy docházet ke kolizím čteček, jejichž signály se navzájem ruší. V této situaci není tag schopen odpovídat na několik signálů ve stejném čase. Proto se často v systémech využívá tzv. antikolizní protokol. Ten umožňuje, aby tagy odpovídaly jednotlivým čtečkám postupně. Stejně jako u čtecích zařízení může docházet i ke kolizi tagů. Stává se to v případech, kdy je v malém prostoru příliš mnoho tagů současně. Při dnešních možnostech rychlosti čtení je možné se tomuto problému alespoň částečně vyhnout. Pro vyvarování se kolizím tagů musíme zvolit vhodný typ tagu pro dané využití.

4.4 Chybovost systému

Obecně můžeme říci, že v komunikačním kanálu mohou nastat chyby, které zapříčiní nekvalitní přenos dat od zdroje k příjemci. Je zřejmé, že vyslaná zpráva nemusí být vždy totožná se zprávou přijatou a to zejména v důsledku rušivých signálů nebo přítomnosti problematických materiálů. Chyby při komunikaci mezi dvěma zařízeními nazýváme šumy. V ideálním systému neexistují poruchy a přijatá zpráva přesně souhlasí s vyslanou. Skutečné systémy bezporuchové nejsou a působí tak problémy ve všech aplikačních oblastech systému RFID, nejen v průmyslu komerční bezpečnosti.

Do jaké míry souhlasí přijatý signál s vyslaným, charakterizuje spolehlivost spojení. Spolehlivost závisí na poměru výkonu signálu k výkonu šumu v přenosovém kanálu. Obecně platí, že spolehlivost klesá se vzdáleností. Dosah spojení pak určuje mezní vzdálenost, ve které je splněna potřebná spolehlivost. Šumy jsou tedy poruchy náhodné povahy, které působí při přenosu na signál a více či méně ho zkreslují. Snižují tak kvalitu kanálu a zmenšují velikost přenesené informace za jednotku času. Nárůst šumu v signálu vede až k úplné nemožnosti čtení přijaté zprávy. Pokud se tedy setkáme se selháním systému RFID, tak většina chyb nastává v přenosovém kanálu, který zajišťuje komunikaci mezi RFID reader a RFID tagem.

V praxi je nutné zabývat se otázkou, do jaké míry je možno poruchám předejít. Pro opravu chyb při načítání dat z tagů lze využít data z okolních čteček nebo znalost prostředí, ve kterém se čtečka s chybou čtení nachází. Ne vždy je však možné takto chybovost systému obejít, a proto je nutné řešit tyto technické problémy.

Abychom zamezili problémům se čtením, musíme věnovat každé aplikaci individuální pozornost. Ke správnému návrhu RFID systému jsou potřeba široké znalosti v oboru. Spolehlivost systému zvýšíme vhodnou strukturou systému. Správná instalace a rozmístění jednotlivých součástí se jednoduše projeví na celkové funkčnosti. Ve vzájemné komunikaci mezi jednotlivými tagy a readery hraje velkou roli frekvence zvolená k přenosu signálu. Volba správného kmitočtu je velmi důležitou částí návrhu řešení systému RFID. Z volby vhodné frekvence pro konkrétní aplikaci vyplývají vlastnosti a fyzikální chování jako například dosah a rychlost čtení, a proto je podmínkou úspěchu vhodný výběr druhu antén podle daného pásma. Čím vyšší je použitá frekvence, tím menší může anténa být. Nepříznivé vlivy elektromagnetické interference jiných systémů v blízkém okolí lze zmírnit elektromagnetickým stíněním, popřípadě zvětšením odstupu mezi signálem a šumem. Vedle infrastruktury a kmitočtového pásma je důležité dbát na volbu vhodného nosiče informace - vyhovující RFID tag podle účelu použití a také volbu správného kódu. Jinak obecně platí, čím dokonalejší technologii a kvalitnější technické prostředky k dané aplikaci využijeme, tím spolehlivější systém dostaneme. V poslední řadě je ke správné funkčnosti potřeba pravidelná kontrola a údržba všech komponent celku.

II. PRAKTICKÁ ČÁST

5 APLIKAČNÍ OBLASTI TECHNOLOGIE RFID V PRŮMYSLU KOMERČNÍ BEZPEČNOSTI

Bezkontaktní identifikaci RFID využívá stále širší spektrum aplikací. Jednoduše identifikuje předměty, osoby či zvířata, a zároveň je schopna poskytovat další různé informace v reálném čase nebo dokonce určit jejich polohu. RFID technologie se aplikují všude, kde je potřeba rychlá, přesná a jednoznačná identifikace, a proto lze tento systém úspěšně nasadit v mnoha odvětvích a oblastech lidské činnosti. Avšak velký význam v aplikacích pro nás nemá jen rychlost a přesnost samotné identifikace, ale také převod informací k následnému zpracování. Rychlost zpracování načtených dat umožňuje okamžité využití této informace a vede tak ke zefektivnění procesů.

Možnosti a vlastnosti radio-frekvenční identifikace slouží ke sběru dat. Dnes toho využíváme zejména pro evidenci majetku nebo logistické a výrobní procesy. V průmyslu komerční bezpečnosti aplikujeme RFID s přístupovými systémy, elektronickými systémy zabezpečení zboží, nebo systémy lokalizace objektů. Dále vyjmenuji jen pro zajímavost speciální aplikace této technologie, které dále nebudu rozvádět: zdravotnictví, letištní kontrola zavazadel, elektronické pokladny v obchodech, bezhotovostní platby v podobě elektronické peněženky atd.

5.1 Data Capture Systems

Po seznámení se základními principy technologie RFID z teoretické části této bakalářské práce se dostávám k první aplikační oblasti. RFID patří do oblasti automatické identifikace objektů, jejímž nejjednodušším využitím je sběr dat. Data capture systémy můžeme do českého jazyka přeložit jako systémy pro sběr nebo zachycení dat. Systém funguje relativně jednoduše. Terminály - čtečky, zachycují data vložená do RFID tagů a dále tyto informace zasílají firemnímu systému. Přenos dat mezi RFID čtečkou a firemní aplikací může probíhat dvěma způsoby: off-line nebo on-line.

Off-line provedení je realizováno tzv. dávkovými terminály, které slouží pro ukládání a sběr dat do vlastní paměti. Poté proběhne přenos do systému prostřednictvím stanoveného rozhraní, aby došlo ke zpracování a vyhodnocení pořízených dat. Tohoto využíváme např. při odečítání elektroměrů, plynoměrů nebo vodoměrů nebo dokonce ke sledování zásilek přepravních společností.

On-line komunikace mezi čtečkou a aplikací běžící na řídícím serveru pracuje na principu Wi-Fi popřípadě Bluetooth. Největší uživatelskou výhodou tohoto řešení jsou informace, které má obsluha k dispozici v reálném čase. Typickou aplikací je sledování toku výrobků ve výrobním procesu.

Systémy pro sběr dat, na rozdíl od systémů, které se zabývají problematikou kontroly vstupu, určování polohy nebo zabezpečení zboží, nepatří do spektra bezpečnostních aplikací využívajících rádiové komunikace. Data capture systémy jsou dnes jako moderní technologie automatické identifikace využívány zejména ve výrobě, logistice a evidenci majetku.

Z výroby se dostávají produkty do distribučních řetězců, které jsou součástí celého složitého procesu, odkud se dále celý sortiment produktů dostává až ke koncovému zákazníkovi. Dlouhá cesta od dodavatelů, přes všechna distribuční centra až do obchodů, může být díky RFID zásadně zjednodušena a sjednocena. RFID systémy můžeme použít v různém nastavení. Podle aplikačních potřeb využíváme různé druhy terminálů, jak mobilních, tak stacionárních.

Všechny procesy začínají ve výrobě. Čtečky pro odvádění výroby jsou určené k monitorování celého výrobního procesu. Umožňují podrobné sledování materiálu a rozpracovanost zakázek. Přesné řízení toku materiálu ve výrobě a okamžitá informace o stavu výroby je důležitým krokem vedoucím ke snižování zásob. Identifikace pohybu materiálu zajišťuje produktivitu pracovníků a efektivitu výrobních operací. Velkou výhodou je možnost zápisu informací na čip během výroby, to umožňuje umístit tagy natrvalo na výrobky a data poté využívat při distribuci. Výrobci označí jednotlivé výrobky, palety i kartony RFID tagy. Na čipu transpondéru jsou uložena data v podobě čísla EPC. Jedinečný kód EPC zajistí jednoznačnou identifikaci daného zboží. Aktivní tagy umožní při přepravě produktů do určeného skladovacího místa monitorovat například teplotu. Tato funkce je neocenitelným pomocníkem především při distribuci léčiv a potravin. Zboží, které kamion přiveze do distribučního centra, je prostřednictvím čtecích zařízení hromadně přijato a uloženo na sklad centra. Data z kartonů a palet jsou porovnána s informacemi v databázi objednaného zboží. Přijaté zboží se dle dílčích objednávek distribuuje do jednotlivých obchodů, kde jsou příjmy dodávek na sklad opět bezpečně realizovány RFID systémem. Tento způsob řešení pomáhá zajišťovat efektivitu výrobních procesů, celistvost dodávek, zásadně zjednoduší logistické procesy včetně kontroly kvality (zrychlení příjmů, výdejů, přesunů mezi sklady a inventarizaci produktů), minimalizuje náklady se značením

produktů a sníží chybovost v evidenci majetku.

5.2 Access Control Systems

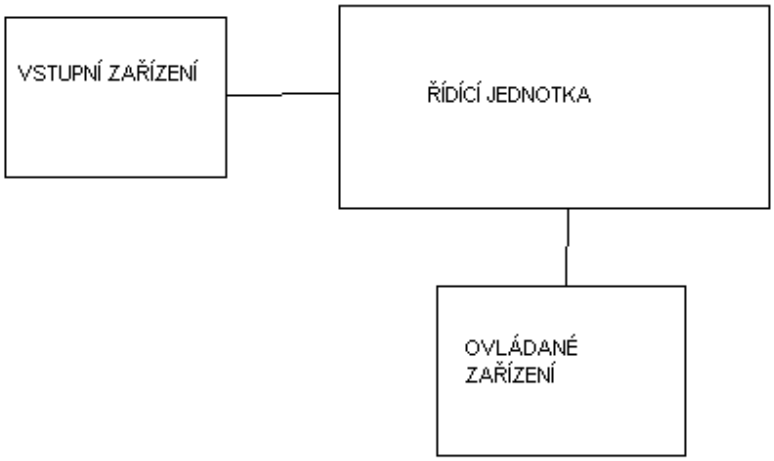
Přístupové systémy (ACS) slouží jako systémy elektronické kontroly vstupu (EKV). Jedná se o identifikační systémy, jejichž úlohou je ověřování identity osob nebo předmětů. Identifikovaným předmětem může být například vozidlo. Ověřování identity se nejčastěji děje prostřednictvím čipových bezkontaktních karet. Softwary následně vymezují identifikovaným osobám stupeň jejich oprávnění. Systémy kontroly vstupu patří do oblasti bezpečnostních technologií. Bývají používány samostatně nebo v kombinaci s dalším bezpečnostním systémem. V současné době se systémy kontroly vstupu integrují nejčastěji s docházkovými systémy, poplachovým zabezpečovacím systémem (PZS) nebo s monitorovacím zařízením CCTV. Přístupové systémy přispívají k ochraně objektů také režimovým opatřením. Plní dvě hlavní funkce:

1. Řídí pohyb osob v objektech
2. Zaznamenávají a poskytují informace o pohybu osob v objektech

V praxi konkrétně využíváme funkce přístupových systémů k omezení přístupu nepovolaných osob do určitých prostor objektů (sklady, výpočetní centra, kanceláře), k omezení pohybu v předem definovaných časových zónách (noční režim, zásobování, úklid), k registraci délky, místa a účelu pobytu, k evidenci doby pobytu osob na pracovištích nebo ke sledování a dokumentování nespecifického pohybu, místa a času osob či zařízení.

V místech, kde je potřeba monitorovat a řídit pohyb osob podle jejich oprávnění, instalujeme tzv. přístupové body. Základem každého přístupového bodu je řídící jednotka. Ta je připojena bezdrátově či kabelem ke vstupnímu zařízení a zároveň k zařízení výstupnímu. Vstupní zařízení je tvořeno nosičem identifikačního kódu a čtecím zařízením. Systémy kontroly vstupu jsou založeny na různých fyzikálních principech. Nosič informace se používá jako průkaz jednoznačné identifikace a v přístupových systémech může mít různou podobu. Využívají se čárové kódy, magnetické kódy, biometrické údaje, nebo kontaktní a bezkontaktní karty. Spolehlivé řešení představují bezkontaktní RFID karty. Jako nosič informace je použit pasivní transpondér v podobě identifikační karty ve formátu EURO. K účelům jednoznačné identifikace využíváme nepřepisovatelné RO čipy,

do kterých je při výrobě vložen originální 64 bitový kód. Čtecí terminál pro kontrolu vstupu je zařízení stacionárního typu s integrovanou anténou. Každá anténa má vlastní vyzařovací charakteristiku elektromagnetického pole, které vytváří ve svém okolí. Kondenzátor vyskytující se v dosahové vzdálenosti aktivního pole antény se nabije natolik, že dokáže správně vyslat svůj identifikační kód. Doba identifikace trvá asi 100 milisekund. Komunikace tagu s čtečkou nepotřebuje přímou viditelnost, informace se přenáší přes většinu nekovových materiálů. Pokud se v aktivním poli antény objeví více jak jedna karta, nelze přečíst žádnou z nich. Ke zvýšení bezpečnosti můžeme vybavit čtečku klávesnicí pro ruční zadání údajů nositelem karty, ochranný kód. Řídící jednotka tedy na základě načtení vnitřního kódu karty příslušným terminálem pustí/nepustí prostřednictvím ovládaného zařízení příslušnou osobu dle oprávnění do chráněného prostoru. Ovládaným zařízením může být třeba zámek, závora, brána atd. Řídící jednotka jako ovládací software dále bez ohledu na práva držitele karty, provede záznam o dané události. Historie obsahuje databázi událostí s příslušnými parametry (kdo, kdy, kam). V komplexu, kde máme více přístupových bodů, propojujeme tyto body celého systému přes sběrnici na řídící server.



Obrázek 7 Přístupový bod [13]

5.3 Real – time Location Service

Pojmem RTLS (Real-time location service) jsou v sektoru komerční bezpečnosti nazývány systémy pro určování polohy majetku (př. zboží) a osob v reálném čase. Tato technologie pracující na principu RFID dokáže sledovat polohu objektu v rámci vymezeného prostoru. Každý takovýto systém je založen na rádiové bezdrátové síti. Infrastruktura sítě musí být realizována tak, aby signál pokryl veškerý prostor, kde má systém fungovat. RTLS pak lokalizuje všechny objekty, které označíme aktivními RFID tagy. Přesnost systému se pohybuje v řádu jednotek metrů.

Real-time location service je založen na kombinaci bezdrátové počítačové Wi-Fi sítě a technologie pracující v pásmu rádiových vln. Vedle aktivních RFID čipů, které komunikují s tzv. accespointy, přístupovými body představujícími v praxi čtecí zařízení, obsahuje celý systém také datové sítě, software na serveru a aplikační software pro koncové uživatele. K přesnému určení polohy jsou potřeba nejméně tři accespointy, které je nutné strategicky rozmístit. Informace nejen o aktuální poloze, ale také o pohybu objektu v časovém intervalu, jsou poskytnuty podnikovým aplikacím k využití těchto dat.

Nevýhodou tohoto systému jsou velké pořizovací náklady vzhledem k většímu počtu čteček včetně antén. Na druhé straně, hlavní výhodou RTLS, je rychlá a přesná lokalizace objektů. Na uživatelském softwaru máme možnost zjistit, kam se který objekt přenášel a kde by se měl v danou chvíli nacházet.

Tato technologie se využívá převážně ke sledování polohy objektů v budovách či ve venkovních prostorech v rámci areálů. Můžeme sledovat například zaměstnance ve firmách, pohyb pacientů v nemocnicích nebo vysokozdvižné vozíky na letištích atd.

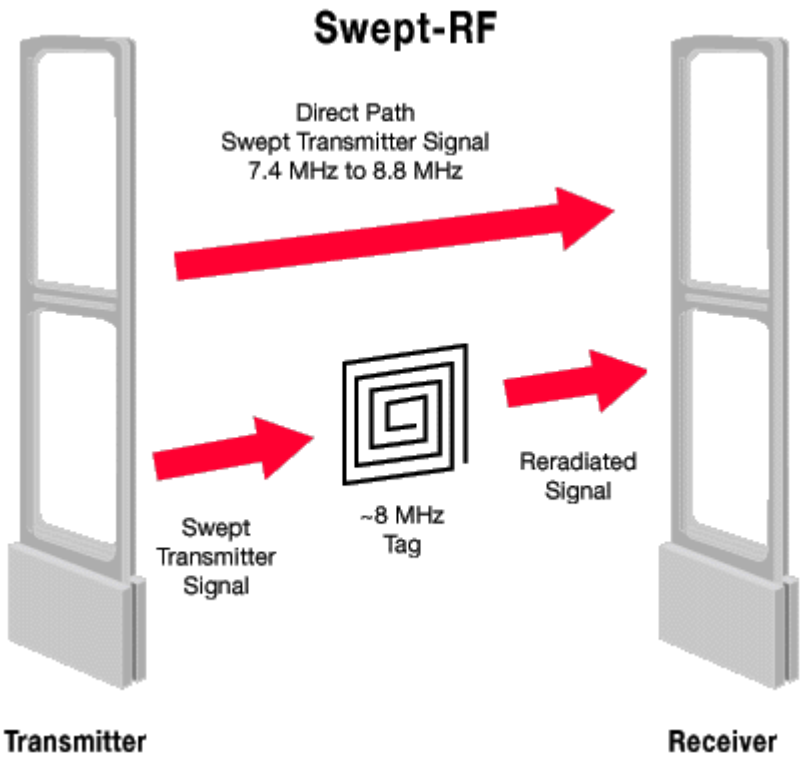
6 ANTÉNNÍ SYSTÉMY

Ochrana zboží a předmětů je dnes neodmyslitelnou součástí bezpečnostních systémů v obchodech. Jedním z nejefektivnějších způsobů zabezpečení vystavěných produktů na prodejně je v dnešní hektické době elektronická ochrana pomocí anténních systémů. Anténní systémy mají v ochraně zboží své nezastupitelné místo a to zejména proto, že ze statistického hlediska jde do obchodu za účelem krádeže průměrně každý patnáctý zákazník. Vývoj techniky a stále rostoucí počet krádeží v obchodních řetězcích podpořil velkou oblibu prodejců a obchodníků právě v zabezpečení s využitím etiket a detekčních rámů. Jedná se většinou o obchody s volně vystavěným zboží, kde kvůli velkému počtu zákazníků mohou prodejci ztratit přehled o situaci na pracovišti. Bezpečnostní anténní systémy tedy slouží jako pomocný prostředek bezpečnostní kontroly, především pro kontrolu zboží při placení. Tyto systémy napomáhají přistihnout pachatele, ale pravdou je, že významnou roli hraje i psychický faktor, tedy skutečnost, kdy zákazník s úmyslem krást raději navštíví obchod, kde je zřejmé, že tento systém není zaveden.

Anténní systém se skládá vždy ze tří základních prvků: detekční brány, etikety a deaktivátoru etiket. Systémy detekce pak můžeme rozdělit podle použité technologie, přičemž každá technologie má své výhody i úskalí. Velmi často jsou využívány elektromagnetické systémy, které jak již z názvu vyplývá, detekují prostřednictvím elektromagnetického pole. Další skupinou jsou systémy akustomagnetické, jejichž výhodou je, že nepodléhají elektromagnetickému rušení. Jelikož tato bakalářská práce pojednává o problematice a využití technologie RFID, budu se dále v této kapitole věnovat radio-frekvenčním anténním systémům, které využívá tzv. EAS systém. EAS, electronic article surveillance, jako elektronická ochrana zboží proti krádeži na bázi technologie anténní radio-frekvenční identifikace, je v současnosti účinnou metodou ochrany zboží za přímého provozu. RF systémy se využívají např. ke kontrole potravin, alkoholických nápojů a drogerie, textilních výrobků, obuvi a kožené galanterie, sportovního zboží, keramiky, skla, hraček, apod.

6.1 Princip činnosti EAS systému

Standardní EAS systém využívá jednobitové tagy, které znají pouze dva stavy: zapnuto/vypnuto. Těmito RFID transpondéry, které mají podobu samolepících papírových etiket (knihy, spotřební zboží, elektronika, paměťová média) nebo pevných etiket (Obuv, Oděv) označíme dané zboží. Vysílací/přijímací detekční brány, které jsou umístěny u východu z prodejny, vyhodnocují dle softwarového vybavení, v jakém stavu se daná položka při průchodu nachází, je-li zaplacená či nikoli a vyhlašují tak případný poplach. K deaktivaci měkkých etiket slouží deaktivátor, který bývá instalován u pokladen. Po zaplacení dojde k deaktivaci tagu a zákazník může se zakoupeným zbožím bez problémů projít skrze detekční rám, aniž by radio-frekvenční systém signalizoval poplach.



Obrázek 8 Etiketa v aktivním poli detekční brány [14]

6.2 Čtecí brány

Samotný detekční rám představuje 1, 2 nebo více-anténní systém s integrovaným nebo externím vysílačem a přijímačem. Velikost průchodu mezi anténami je dána podle druhu zboží a příslušného zabezpečovacího systému. U dvouanténního systému bývá aktivní pole široké kolem dvou metrů. Výška se pohybuje kolem 160 cm. Povrchová

úprava anténních oblouků bývá plastová, dřevěná, chromová, nerezová či plexisklová, vzhled tedy může být přizpůsoben designu obchodu. Provozovatel se může také rozhodnout antény skrýt a zabudovat je do dveřního rámu či ostění. Anténa, která má za úkol chránit provozovatele před krádežemi, dokáže detekovat etiketu v jakékoli poloze bez přímé viditelnosti. Radio-frekvenční detekční systém pracuje většinou na frekvencích: 2,2 MHz, 3,25 MHz, 4,75 MHz, 8,2 MHz, 10 MHz.

Čtecí brány dekódují data z etikety a na základě softwaru vyhodnocují stav tagu: vypnuto/zapnuto. Z praktických důvodů se nachází vždy u vstupu či výstupu z prodejny tak, aby jimi musel projít každý. Při průchodu kontrolním místem u východu z obchodního oddělení s nezaplaceným zbožím a tedy nedeaktivovanou etiketou je spuštěn odpovídající alarm, zloděj je za přítomnosti akustické či optické signalizace přistižen. V případě pronášení nezaplaceného zboží mohou antény nejen vyhlásit signalizaci, ale také zablokovat východ, ohlásit poplach do kanceláře vedoucího, přivolat ostrahu provozovny a podobně.

Obrázek 9 Dvouanténa [15]

6.3 Bezpečnostní etikety

Systém elektronické ochrany proti odcizení využívá pasivních RFID-EPC tagů. Vhodný výběr těchto tagů-etiket je důležitým faktorem pro správnou funkčnost EAS systému. Neméně důležitým předpokladem pro fungování systému je vhodné umístění etikety na daný produkt. Je nutné si tedy uvědomit, že zabezpečení se může lišit podle druhu zboží. Zboží, které potřebujeme zabezpečit, se rozděluje do několika skupin. Každé skupině je potřeba věnovat individuální pozornost. Podle typu zboží, které budeme tagy označovat a podle specifikace dané aplikace (podle účelu použití) rozdělujeme etikety na tvrdé a měkké. Například při ochraně textilních výrobků zvolíme tvrdé etikety, které znesnadní případnému zloději nasadit na sebe několik vrstev oblečení.

RFID tagy využívané systémem EAS mají podobu nejrůznějších visaček, samolepek nebo upínacích etiket. Po odbavení u pokladny je etiketa deaktivována nebo odstraněna bez poškození zakoupeného zboží. Pro zajištění kontroly manipulace se zbožím vlastními zaměstnanci je důležité nasadit režimová opatření. Odstranění a deaktivaci etiket by měli provádět pouze osoby s příslušným oprávněním.

6.3.1 Tvrdá etiketa

Tvrdá RFID etiketa je umístěna na zboží. Připevňuje se pomocí lanka či jehly. Pokud není etiketa při placení pomocí uvolňovače sejmuta, detekční anténa u východu vyhlásí poplach. Výhodou je, že po sejmutí je možné etiketu opět použít. Průměr etikety bývá kolem 50 mm a hmotnost cca. 13 g. Existují také speciální etikety, které při neoprávněné manipulaci znehodnotí oděv barvivem.

Obrázek 10 Tvrdá etiketa [16]

6.3.2 Měkká etiketa

Lehká varianta etikety, lepí se na zboží, v případě oděvu se připevňuje pomocí textilních kleští nebo jehly a softfixu. Používají se samostatně nebo jako možnost druhého jištění. Výhodou je, že mohou poskytnout skrytou ochranu. Měkké samolepící etikety vkládáme volně do zboží nebo je můžeme potisknout falešným čárovým kódem. Samolepicí ochranná etiketa má bílou barvu a rozměry od 35 x 35 mm do 50 x 50 mm.

Obrázek 11 Měkká etiketa [17]

6.3.3 Uvolňovače a deaktivátory

Deaktivátor slouží k deaktivaci bezpečnostní funkce samolepících etiket, zatímco uvolňovač slouží k odstranění bezpečnostní tvrdé etikety. Oba tyto prvky bývají instalovány do prostoru pokladen. Uvolňovače se dělají ve verzi do skladu a verzi pro zabudování do pultu s možností montáže na dřevěný, kovový nebo skleněný povrch pokladního pultu. Na objednávku se dodávají se zámkem na klíč zabraňující zneužití. Deaktivátor bývá zabudován do tzv. deaktivační desky, která se nachází v prostoru pokladen. Vedle této možnosti můžeme deaktivátor integrovat do scanneru čárových kódů. Hlavní výhodou deaktivátoru je, že působí i na etikety schované uvnitř zboží.

Obrázek 12 Uvolňovač tvrdých etiket [18]

Obrázek 13 Deaktivátor měkkých etiket [19]

6.4 Problémy systému ochrany EAS

Ani sebelepší systém nefunguje se stoprocentní spolehlivostí tak, jak bychom si představovali. Nedokonalost a nedostatky EAS s sebou nesou svá rizika, která plynou jednak z technických vlastností systému, ale také z chování lidí. V praxi existuje několik problémů souvisejících s elektronickou ochranou zboží, které vedou k selhávání nasazených bezpečnostních opatření.

V průmyslu komerční bezpečnosti nám činí značné potíže chybovost systému v podobě planých poplachů. V těchto případech dochází k velmi nepříjemným situacím, kdy poctivý zákazník přesvědčuje bezpečnostního pracovníka, že produkt neukradl, ale zakoupil. Tento problém souvisí s přítomností kovových předmětů ve sledovaném poli mezi anténami nebo se selháním obsluhy u pokladny, která zapomene etiketu ze zakoupeného zboží odstranit či deaktivovat.

Technické problémy související s technologií RFID, které souvisí s rušením radio-frekvenčního signálu, jsem zmiňoval již v teoretické části. Rušení vzniká při výskytu energie na konkrétní frekvenci nebo v blízkosti kapalin a kovů. O kovu se v souvislosti s technologií RFID hovoří jako o problematickém materiálu, který v nejrůznějších aplikacích této technologie činí potíže a systém EAS není výjimkou. Kovový materiál je vedle kapalin a uhlíku jedním z elektromagnetických reflektorů. Rádiové signály nemohou proniknout skrz kovové předměty, které úplně brání komunikaci mezi tagem a readerem. Přítomnost kovu v blízkosti čtecího zařízení má negativní vliv na jeho fungování. Průchod kovového nákupního vozíku mezi anténami či přítomnost notebooku a jiné elektroniky kolem čtecí brány mohou způsobit falešnou signalizaci. Jedině za předpokladu správné instalace, především volby kmitočtového pásma, mají RF systémy vysokou spolehlivost a zároveň nízkou četnost vyvolání falešných poplachů.

6.5 Metody obcházení systému EAS

Hlavní článek, na který se anténní ochrana soustředí, jsou nepoctiví zákazníci neboli zloději. Právě kvůli zlodějům všeho druhu zavádíme nejrůznější bezpečnostní systémy, mezi které patří třeba EAS. Musíme si uvědomit, že bohužel ani nejmodernější radio-frekvenční systém nezabrání všem krádežím v prodejnách. Ze zkušeností v praxi docházíme po čase vždy k závěru, že člověk s nekalými úmysly se bude vždy snažit prolomit jakoukoliv ochranu, mnohdy i s použitím kuriózních prostředků. Nepoctivý zákazník ve snaze odcizit zboží využívá technických nedostatků nasazené technologie a snaží se tak najít způsoby, jak systém zabezpečení obejít. Nekalé jednání ze strany lupičů a zlodějů můžeme definovat v podobě zneškodnění RFID tagů, které se přidávají na zboží nebo rušení samotného systému EAS různými způsoby.

Stínění je častým způsobem obelhání RF systému. Principiálně stačí jakýmkoli způsobem odstínit etiketu umístěnou na zboží tak, aby byla znemožněna čitelnost. Brána etiketu nevidí, a nemůže reagovat na její přítomnost v detekčním prostoru. Nejčastěji se k tomuto využívají tašky plněné alobalem nebo oděvy s hlubokými vnitřními kapsami, které jsou také vyplněny alobalem či jiným materiálem k odstínění RFID tagu.

Známou metodou obcházení EAS systému je také rušení rádiového pásma. Pomocí rušičky, která vysílá signál na stejných frekvencích jako detekční rámy, můžeme snížit

účinnost nebo dokonce vyřadit anténní systém z provozu.

Dalším z prostředků využívaných k odcizení zboží v obchodech jsou kleště. Kleště nebo nůžky na drát dokážou mechanicky odstranit etiketu ze zboží. Zboží se tak stane nechráněné a nepoctivý zákazník odchází s nezaplaceným zbožím bez povšimnutí.

7 PROBLEMATIKA KOMERČNÍ BEZPEČNOSTI

V dnešní době je ochrana osob a majetku zabezpečována nejen státními orgány, ale také soukromými bezpečnostními službami (SBS). Role soukromého bezpečnostního sektoru není hlavní, ale pouze doplňující. Hlavní roli ochrany tvoří zejména Armáda České Republiky a Policie ČR. Soukromé bezpečnostní agentury jsou podřízené těmto složkám. SBS nabízejí zákazníkovi zvýšení bezpečnosti za úplatu. Zákazník si tak může dovolit nadstandard, který stát neposkytuje. Počet soukromých bezpečnostních firem během posledního desetiletí výrazně vzrostl. Nebývalý nárůst SBS na trhu České republiky byl zapříčiněn mnoha aspekty. Například zvyšujícím se objemem soukromého majetku, rozvojem elektroniky a s tím spojenou produkcí alarmů a jiných elektronických zabezpečovacích zařízení nebo vysokým počtem majetkových trestných činů. Soukromé bezpečnostní služby se ve svém sektoru zabývají rozmanitou činností ochrany majetku a osob. Zákazník si sám určí, podle poskytovaných služeb agentury co, jak, kdy a za jakou cenu požaduje chránit. Role bezpečnostního průmyslu ve společnosti je především podnikatelská a tvorba zisku je hlavním motivem činnosti majitelů a provozovatelů těchto služeb. Zvláštnost oboru jejich podnikání je však v očích veřejnosti často předurčuje do pozice jakési soukromé policie a jsou dnes v podstatě vnímány jako prvek vnitřní bezpečnosti státu. Je však třeba si připomenout, že tyto složky nemohou nikdy nahrazovat veřejnoprávní bezpečnostní sbory, ani jim konkurovat ve statutu, kompetencích a pravomocích. Hlavní ochranu na území České republiky poskytuje stát. SBS jsou pouze doplňující složkou a nemají charakter státní donucovací moci. Přesto princip bezpečnostní, který je předmětem podnikání v bezpečnostním průmyslu, umožňuje hodnotit toto podnikání v celém kontextu souvislostí jako vysoce společensky prospěšnou činnost, která vede k zamezování nebo snižování ztrát v ekonomice soukromých i státních podniků, zvyšuje produktivitu práce, upevňuje pracovní kázeň zaměstnanců, odrazuje od páchání trestné činnosti na chráněných objektech a má i další efekty v oblasti situační prevence kriminality. [3]

Při provozu soukromé bezpečnostní agentury se setkává vedení firem s mnoha problémy patřícím k řízení podniku. Vnitrostátní konkurence, ale i činnost zahraničních firem zejména ze západních zemí Evropy, stěžují činnosti v soukromém bezpečnostním sektoru. Zahraniční subjekty z některých zemí Evropské unie mají v tomto oboru tradici a dlouholeté zkušenosti, zatímco v České republice vzhledem k mládí tohoto odvětví chybí odbornost a zkušenosti ze strany zaměstnanců. Vedle kvality nabízených služeb a produktů

musí každá úspěšná firma právně ošetřit každou činnost v oblasti ochrany majetku a osob. Vzhledem k tomu, že je průmysl komerční bezpečnosti oborem velmi mladým, v našem právním řádu dosud nebyl přijat zákon o civilních bezpečnostních službách tak, jak je tomu v některých zemích Evropské unie. Sektor komerční bezpečnosti je nucen aplikovat právní řád na naše podmínky. Soukromý bezpečnostní sektor se řídí danými platnými právními řády a normami. K této činnosti se využívá zejména živnostenský zákon, obchodní zákoník, trestní zákon a řád nebo listina základních práv a svobod. Průmysl komerční bezpečnosti je oborem mladým a stále se rozvíjejícím a vzhledem k chybějícímu zákonu o SBS není nucen se podřizovat tradičním přístupům, a může se tak přizpůsobovat změněným podmínkám.

7.1 Ochrana zboží v obchodních řetězcích

Ochrana zboží v obchodních řetězcích představuje speciální problematiku v oblasti zabezpečení. Jde o speciální problematiku komerční bezpečnosti. Jedná se o specifickou předmětovou ochranu, která však patří do speciální elektronické ochrany zcela mimo klasicky známá zabezpečení. Ochrana zboží v obchodech je z hlediska zabezpečení samostatný specifický problém, neboť jiná bude ochrana zboží v provozní době a jiná po zavírací době. Protože v pracovní době mají firmy zájem dostat se co nejblíže se svým zbožím zákazníkovi, vzniká zde velký problém ochrany před „nenechavci“, chcete-li zloději, a minimalizovat ztráty zboží, ty ale mohou způsobovat jak náhodní zákazníci, tak organizované skupiny, ale i vlastní zaměstnanci. [2]

7.1.1 Jak se ztrácí zboží

Již v kapitole EAS jsem se zmínil o nepoctivých zákaznících, kteří navštěvují obchody za účelem odcizení majetku z důvodu osobního prospěchu.

Dle typu nabízeného zboží dochází ze strany zákazníků nejčastěji ke krádežím spotřební elektroniky, knih a časopisů, hraček, domácích a sportovních potřeb, ošacení, potravin a alkoholu, drogistických a parfumeristických potřeb. Jde většinou o zboží, které je atraktivní a lze snadno odcizit tak, že je ukryto pod kabátem, či v tašce. [2]

Nepoctivý zákazník se však mnohdy nezastaví před ničím. Vymýšlí nejrůznější způsoby jak získat zboží z obchodu bez placení. Jako příklad uvedu nejčastější metody odcizení produktů z provozoven:

1. umístění dražšího zboží do obalu od levnějšího
2. přelepení kódu EAN
3. ukrytí zboží do obalu jiného většího zboží
4. ukrytí zboží do novin či reklamních letáků
5. odstranění bezpečnostních prvků ze zboží
6. nahlášení na pokladně menšího počtu kusů
7. konzumace zboží přímo v prodejně
8. ukrytí zboží pod bundu či umístění spodní části nákupního vozíku a vynesení z objektu prodejny bez placení

Krádeže jsou v dnešní době obecně známá témata a provozovatelé obchodů se musí na tento problém přímo zaměřovat a nasazovat různé systémy ochrany. Málo-kdo si uvědomuje, že největším rizikem pro obchodní řetězce je rozkrádání zboží ze strany vlastních zaměstnanců. Vnitřní způsob rozkrádání tvoří až 70 % celkových ztrát zboží. Vlastní personál se může volně pohybovat po obchodě, čímž získává snadný přístup ke zboží. Často dochází ke spojení zaměstnanců se zákazníky, se kterými mají rodinné či přátelské vztahy. Personál svým spolupachatelům dává informace a návody co, kdy a jak odcizit. Vedle řadových zaměstnanců se na rozkrádání podílí dodavatelé služeb jako například uklízečky nebo opraváři, kteří mají rovněž volný přístup a pohyb v prostorách provozního řetězce. Personál i dodavatelé služeb jsou mnohdy součástí organizované skupiny a navzájem si vytváří jim vyhovující podmínky za účelem páchání trestné činnosti. Pro tvorbu machinací, realizaci účetních podvodů a další manipulaci se zbožím mají největší možnosti nadřízení objektu, provozní nebo vedoucí zaměstnanci. Často spolupracují přímo s dodavateli služeb a produktů. Objednané zboží naskladňují jako celek, přičemž u části produktů nedojde k jeho vyložení a přijetí. Účastníci podvodu odcizenou část produktů ihned odvezou a prodají sami jinému odběrateli. Při následující

inventuře zkušený vedoucí využije chybovosti zabezpečovacích systémů a ztráty zboží svede na běžné zloděje, přitom se mnohdy dané zboží v podniku nikdy ani neobjevilo.

7.1.2 Provádění ochrany

Realizace bezpečnostních opatření by měla vycházet z bezpečnostní politiky podniku. Jde o soubor organizačně řídících opatření, norem, standardů, pravidel chování s cílem zajistit bezpečnost organizace. Ochranu zboží lze zajistit několika způsoby, přičemž nejoptimálnějším řešením je jejich vzájemná kombinace a provázanost. [2]

Většinou se dnes integrují mechanické a elektronické systémy, integrovaný bezpečnostní systém vyžaduje propojení mechanických zábranných systémů, signalizačních a monitorovacích systémů a systémů organizačních opatření a ostrahy. [4]

Technická ochrana zboží

Technickou ochranu majetku rozdělujeme na mechanickou a elektronickou. Základním stavebním kamenem technické ochrany jsou prvky mechanických zábranných systémů. MZS, mechanické zábranné systémy charakterizuje mechanická odolnost. Jedná se o schopnost odolávat napadení. V případě ochrany volně vystaveného zboží hovoříme o lokálním mechanickém zabezpečení, které ztěžuje v pracovní době nepovolané osobě možnost odcizit předměty v zabezpečené zóně. Po zavírací době plní svou úlohu zejména zabezpečovací prvky plášťové ochrany, které brání pachateli průniku do střežených prostor. Do mechanické ochrany zboží řadíme zámkové systémy, zarážky, zastavovače dveří, turnikety, otočné bariéry, sejfy, úchytky, parabolická bezpečnostní zrcadla, zajišťovací úhelníky, bezpečnostní schránky, háky, bezpečnostní fólie a podobně.

Speciální ochranu zboží tvoří elektronická ochrana. Nejefektivnější je elektronická ochrana zboží EAS (Electronic Article Surveillance) za využití radio-frekvenčního či elektromagnetického anténního systému. Tento bezpečnostní detekční systém se stal velmi populární a účinnou variantou zabezpečení a tak se s ním můžeme v obchodech velmi často setkat. Jeho největší výhodou oproti lokálnímu mechanickému zabezpečení je možnost prohlížet si zboží bez omezení. Zákazník může se zbožím libovolně manipulovat, což oceníme zejména u oblečení, které je potřeba si před zakoupením vyzkoušet. Anténní systémy však mají i své nevýhody. Svou signalizací na pachatele pouze upozorní. Z tohoto

důvodu nemá smysl aplikovat anténní systém bez stráže v podobě security pracovníka u východu. Vedle zabezpečovacích komponent anténního systému se využívá kamerový CCTV systém, který umožňuje elektronicky monitorovat střežený prostor. Pro noční režim využívají obchodníci poplachový zabezpečovací systém. Ústředna poplachového systému dokáže zjistit přítomnost pachatele prostřednictvím detektorů a následně ohlásit narušení hlídané zóny na bezpečnostní agenturu či Policii ČR.

Fyzická ostraha

1. Fyzická ochrana prostá: slouží k ochraně obchodních řetězců a je prováděna pracovníkem soukromé bezpečnostní služby. Jedná se v podstatě o strážného v obchodě. Jeho náplní práce je kontrolovat a sledovat manipulaci se zbožím a pohyb zákazníků a hlídat zákazníky, aby nevynášeli z prodejny nezaplacené zboží. Bývá oblečený v uniformě a hlídá u vstupu a výstupu prodejny. Bezpečnostní pracovník je často nasazen v kombinaci s detekčním systémem. Stará se o fyzický zásah proti pachatelům krádeží a ověřuje falešné poplachy.
2. Detektivní ochrana: detektiv v obchodě má na starost zajišťovat ochranu majetku a osob v obchodech skrytým způsobem. V civilním oděvu za využití forem a metod detektivní činnosti zejména sledováním osob a dohledem na dění eliminuje všechny způsoby odcizování zboží. Provádí dozor nad dodržováním veřejného pořádku, tipuje podezřelé osoby, kontroluje rozkrádání zboží personálem a zvýšenou pozornost věnuje pokladnám.

Režimová ochrana

Doposud jsem jmenoval způsoby ochrany zboží, které se soustředily zejména na nepoctivé zákazníky. V první části této kapitoly jsem uvedl, že největším problémem pro obchodní řetězce je rozkrádání zboží vlastními zaměstnanci.

Každý podnik by měl mít stanovenou alespoň základní bezpečnostní politiku, jejíž pravidla by byla pro všechny zaměstnance závazná. Bezpečnostní politika by měla vedle fyzické a technické ochrany zahrnovat i režimová opatření, která bývají někdy podceňována. Režimovým opatřením bývá ve firmách průmyslu komerční bezpečnosti věnována minimální pozornost a mnohdy se vůbec nedávají do souvislosti s ochranou.

Většinou však každá firma má svá režimová opatření, aniž by si to mnohdy vedení uvědomovalo. Například pokud je konkrétní osoba zodpovědná za zamykání dveří po ukončení pracovní doby, má firma touto jasně definovanou zodpovědností stanovenou část režimové ochrany. Dále do režimové ochrany rozhodně patří i výstražné nápisy, které již mnohokrát prokázaly svou účinnost. Režimová opatření bývají někdy záměrně vynechávána. Jedním z důvodů je fakt, že lidé obecně nemají disciplínu a neradi dodržují stanovená pravidla. Dalším důvodem záměrného nezavedení režimových opatření jsou nepoctiví zaměstnanci, jejichž zájmem je si finančně či majetkově přilepšit nepoctivým způsobem. Veškerá technická ochrana v kombinaci s fyzickou ztrácí smysl, pokud nejsou nasazena opatření eliminující rozkrádání majetku zevnitř podniku. Málo-kdo si uvědomuje, že režimová opatření představují nejlevnější způsob ochrany majetku v podnicích a slouží jako prevence nejen proti vlastnímu personálu firmy, ale také proti nepoctivým zákazníkům.

Režimová ochrana se zaměřuje na:

- **Vstupní a výstupní režim osob a dopravních prostředků**, který zahrnuje zejména kontrolu vstupu a výstupu zaměstnanců, návštěv a zákazníků do provozovny a jejích částí, oprávněnost vynášení a vyvážení předmětů
- **Režim pohybu zaměstnanců** v prostorách provozovny, který zahrnuje i určení částí provozovny s omezenou přístupností pro zaměstnance
- **Materiálový a expediční režim** stanoví postup při příjmu, skladování, výdeji a pohybu materiálu. Chrání se jím majetek před rozkrádáním, poškozováním a znehodnocováním
- **Provozní režim**, který zajišťuje plynulost a bezpečnost provozu a činnosti při mimořádných událostech
- **Klíčový režim provozu**, kterým se stanoví označování, přidělování, předávání klíčů, způsob jejich použití, výroba náhradních klíčů, výměna zámků v důležitých částech objektu a podobně.
- **Provozní režim** spojený s fungováním systémů zabezpečovací techniky

Režimovou ochranu tvoří souhrn administrativních a organizačních opatření k zajištění chráněných zájmů a hodnot. Pro správné fungování podniku slouží dokumenty režimové ochrany, které přesně stanovují pravidla a postupy. Mezi základní dokumenty režimové ochrany patří statut organizace, který vyjadřuje důležitost jejího postavení. V něm je vyjádřen účel, cíl a činnost firmy. Dále organizační řád, který konkretizuje

strukturu podniku a vlastní provozní činnost. V organizačním řádu by měl být zmíněn způsob ochrany, dále pak stupeň důležitosti ochrany jako celku nebo alespoň jeho části. Neméně důležitým dokumentem je pracovní řád podrobně určující jednotlivé pracovní náplně zaměstnanců. Součástí tohoto způsobu zabezpečení, kromě nastavení pravidel a povinností všech zaměstnanců, by měla být i pravidelná kontrola toho, jestli personál stanovená opatření dodržuje. Součástí firemních pravidel by mohla být také osobní prohlídka zaměstnanců, kterou má provozovatel podle zákoníku práce právo učinit. Efektivním způsobem proti rozkrádání zboží zaměstnanci může být namátková osobní prohlídka, kterou je možné urychlit a zjednodušit využitím EAS systému.

7.2 Využití signálu alarmu podle ustanovení o zadržení

Při poskytování služeb v průmyslu komerční bezpečnosti (PKB) je nutné dodržovat platné zákony a normy. V případě zabezpečení volně vystaveného zboží v obchodech před nepoctivými zákazníky, představuje nejefektivnější a nejpoužívanější ochranu kombinace anténního poplašného systému a pracovníka soukromé bezpečnostní agentury jako strážného v obchodě. K praktickému využití nasazených bezpečnostních opatření je nutné zabývat se nejen otázkou způsobu ochrany, ale také jejím právním ošetřením. Pro konkrétní využití aplikace EAS systému se musíme řídit ustanovením o zadržení osoby podezřelé.

7.2.1 Trestní řád: § 76 Zadržení osoby podezřelé

(1) Osobu podezřelou ze spáchání trestného činu může, je-li dán některý z důvodů vazby, policejní orgán v naléhavých případech zadržet, i když dosud proti ní nebylo zahájeno trestní stíhání. K zadržení je třeba předchozího souhlasu státního zástupce. Bez takového souhlasu lze zadržení provést, jen jestliže věc nenese odkladu a souhlasu předem nelze dosáhnout, zejména byla-li osoba přistižena při trestném činu anebo zastižena na útěku. [5]

(2) Osobní svobodu osoby, která byla přistižena při trestném činu nebo bezprostředně poté, smí omezit kdokoli, pokud je to nutné ke zjištění její totožnosti, k zamezení útěku nebo k zajištění důkazů. Je však povinen tuto osobu předat ihned policejnímu orgánu; příslušníka ozbrojených sil může též předat nejbližšímu útvaru

ozbrojených sil nebo správci posádky. Nelze-li takovou osobu ihned předat, je třeba některému z uvedených orgánů omezení osobní svobody bez odkladu oznámit. [5]

7.2.2 Možnosti příslušníka SBS při zadržování osob

Zaměstnanec bezpečnostní agentury nemá oprávnění zasáhnout v takové míře jako příslušník ozbrojených složek. Strážný není v žádném případě roven policistovi, je roven jakémukoliv občanu České republiky bez ohledu na to, jak je oblečen (např. uniforma). Zatímco příslušník Policie ČR má právo zadržet osobu na základě podezření z trestné činnosti, bezpečností pracovník může osobu páchající trestný čin zadržet jen tehdy, jeli tomuto činu přítomen. V této souvislosti je nutné upozornit na skutečnost, že signalizace poplachu vyhlášeného bezpečnostním detekčním rámem nemá žádnou právní váhu a v právním světě nic neznamená. Na základě vyhlášené signalizace není strážný v obchodě oprávněn nikoho zadržet ani jinak omezit. Signalizace alarmu dává dohledovým pracovníkům pouze důvod k podezření, nikoli však možnost pachatele zadržet.

Zadržení osoby v PKB nesmí být provedeno pouze na základě samotného signálu alarmu. Interpretace zákona je taková, že občan musí být přítomen trestnému činu, musí jej přímo vidět, aby mohl dotyčnou osobu zadržet či zkontrolovat. Trestní řád dává oprávnění kterékoli osobě omezit osobní svobodu osoby, která byla přistižena při trestném činu nebo bezprostředně poté, tedy toto oprávnění má i bezpečnostní pracovník. Aby omezení osobní svobody bylo zákonné, musí být splněny následující podmínky:

- Osoba musí být přistižena při trestném činu nebo bezprostředně poté.
- Omezení osobní svobody je nezbytně třeba ke zjištění totožnosti osoby, k zamezení jejímu útěku, nebo k zajištění důkazů. [1]

Avšak ten, kdo takovou osobu omezil na osobní svobodě je povinen ihned ji předat policii. V žádném případě ji nesmí nechat někde sedět (např. v kanceláři, ve sklepě atd.). Pokud není policista ihned k dispozici, je povinen ihned policistu telefonicky přivolat a zadržet pachatele do doby jeho příchodu. Osobní prohlídku, na rozdíl od osobní prohlídky vlastního personálu může udělat až přivolaný policista.

Bezpečnostní pracovník, který hlídá prostor kolem pokladen a u východu z prodejny, musí být velmi dobře proškolen a obeznámen s možnostmi a riziky zadržení potenciálního pachatele trestné činnosti. Největším rizikem pro ostrahu v obchodě je

nesprávné zadržení. Pokud strážný nezadrží zloděje přesně v souladu s ustanovením o zadržení, sám činí trestný čin omezení osobní svobody a může za to být potrestán. Ze všech těchto skutečnostní je zřejmé, že v praxi je obtížné zloděje zadržet a prokázat mu, že nejednal v mezích zákona. Zejména z důvodu chybovosti anténních systémů v podobě planých poplachů se o tyto systémy nemůže strážný v obchodě spolehnout. Samotná technologie RFID nedává důvod k zadržení. Úspěch při zadržování osob vynášejících z obchodu nezaplacené zboží závisí na schopnostech, zkušenostech a znalostech nasazeného pracovníka ostrahy. Znalost technických nedostatků spojených s nasazeným bezpečnostním EAS systémem je společně se znalostí právního výkladu ustanovení o zadržení základním předpokladem k úspěchu při řešení majetkové trestné činnosti v obchodních řetězcích.

7.2.3 Návod na postup při zadržení

Nepoctivý zákazník prochází detekčním rámem. Nezaplacené zboží ukryl pod kabát nebo do příruční tašky. Vzhledem k situaci vyhlašuje radio-frekvenční systém poplach. Bezpečnostní pracovník v uniformě se nachází za čtecí bránou u východu z prodejny, signalizaci zaregistroval a je připraven zakročit. Jak má správně postupovat, aby neporušil zákon a zároveň zamezil odcizení zboží?

Prvním krokem k úspěchu je zaujmutí strategické pozice. Ostraha se musí před zákazníka postavit bez jakéhokoli fyzického kontaktu tak, aby zákazník nemohl pokračovat v přímočarém pohybu, aby musel zpomalit a případně ostrahu obejít. Dalším krokem je navázání komunikace. S pachatelem se musí pracovat. Cílem ostrahy je přesvědčit se o tom, zda podezřelý spáchal trestnou činnost, nebo se jedná jen o falešný poplach. Jak danou osobu vhodně oslovit? V tuto chvíli se nabízí zjistit, zda podezřelý zákazník nakupoval. Mohl nakupovat u nás, ale i v jiném obchodě, kde mají podobný či stejný anténní systém. Neodstraněná bezpečnostní etiketa by reagovala poplachem v obou případech. Nakupoval jste u nás? Nakupoval jste v poslední době v jiném obchodu? Máte účtenku? Otázky jsou jasné, snaží se ověřit či vyvrátit falešný poplach, který nedopatřením obsluhy u pokladny může snadno nastat. Méně častou variantou falešného poplachu může být technická chybovost nasazené RF technologie související s elektromagnetickými reflektory. Podle potřeby může položit ostraha otázku i tímto směrem. Nemáte u sebe klíče nebo jiný kovový předmět? Ve všech případech je primárním účelem pachatele zastavit a

přimět ke konverzaci. Následuje snaha ovlivnit podezřelého tak, aby prošel opět detekčním rámem směrem do obchodu, ideálně ho oddělit od tašky, abychom zjistili, zda spustil alarm on (schovávaný předmět se nachází na těle někde pod bundou či jinou částí oděvu) nebo příruční taška, kterou drží v ruce. V tomto kroku lze při komunikaci s podezřelou osobou opět využít chybovosti a odkázat na chybu vzniklou na pokladně. Půjdete se mnou? Na pokladně vám bezpečnostní etiketu odstraní! U pokladen se přesvědčíme o krádeži nebo falešném poplachu. Pokud dotyčná osoba tímto způsobem s pracovníkem ostrahy spolupracuje, jedná se opravdu o chybu ze strany obchodu ať už ze strany personálu na pokladně nebo technického selhání systému, nebo se jedná o nezkušeného zloděje, který byl při krádeži přistižen. V jiných případech může ostraha narazit na zkušené či znalé zloděje, kteří na vyhlášený poplach ani položené otázky reagovat nebudou. Fyzická ostraha většinou hlídá výstup z prodejny u pokladen, a proto jen velmi těžko může vidět trestnou činnost, krádež, která se uvnitř obchodu odehrála. Příslušník SBS je ve většině případů odkázaný pouze na anténní systém, a jelikož nemá pravomoci Policie ČR, nemůže pouze na základě vyhlášené signalizace zasáhnout a podezřelou osobu zadržet. Pokud dotyčná osoba nespolupracuje, nemá ostraha v rámci zákona právo osobu nijak obtěžovat. V PKB je možné RF systém naplno využít pouze v případě kontroly personálu daného podniku.

ZÁVĚR

Zkratku RFID používáme jako výraz definující technologie, které využívají rádiové vlny k automatické identifikaci objektů. Identifikace na rádiové frekvenci je po čárovém kódu další generace identifikátorů navržených k bezkontaktní identifikaci předmětů, popřípadě osob. RFID technologii lze aplikovat v mnoha oblastech lidské činnosti včetně průmyslu komerční bezpečnosti. Jednou z technologií fungujících na bázi rádiové identifikace využívaných v bezpečnostním průmyslu je anténní systém EAS, který je zaměřen na ochranu zboží v obchodních řetězcích. Je technologicky jednoduchý, administrativně a organizačně nenáročný.

Elektronický systém ochrany zboží (EAS) je využíván jako nezastupitelný pomocník pro identifikaci úmyslně či neúmyslně nezaplaceného zboží zákazníkem a současně je klíčovým prvkem v rámci prevence samotného předcházení vzniku těchto situací. Při aplikaci elektronického systém ochrany zboží (EAS) se v praxi neobejdeme bez využití lidského faktoru, který se společně s tímto systémovým opatřením musí podílet na výstupní kontrole.

Občasné potíže v průmyslu komerční bezpečnosti činí chybovost systémů v podobě falešných poplachů. Z tohoto důvodu pracovník SBS či jiná pověřená osoba nemůže jednoznačně zadržet podezřelou osobu označenou automatickou signalizací. Při kontrole osob podezřelých musí pracovník SBS postupovat vždy podle zákonem definovaného ustanovení o zadržení, viz § 76 odst. 2 trestního řádu. Pouze v rámci režimové ochrany, jenž je nejúčinnějším bezpečnostním opatřením proti vnitřnímu způsobu rozkrádání zaměstnanci, může zaměstnavatel dle zákoníku práce účinně provádět preventivní osobní prohlídky zaměstnanců s využitím elektronického systému ochrany.

Přestože jsme doposud zaznamenali markantní vývoj v oblasti technologií na principu rádiové identifikace, i v rámci dalšího rozvoje se dá očekávat např. eliminace falešných poplachů, jejichž přínos může směřovat k širšímu využívání ustanovení o zadržení v oblasti průmyslu komerční bezpečnosti.

ZÁVĚR V ANGLIČTINĚ

The abbreviation RFID is used to define a technology which uses radio transmission waves to identify objects automatically. The identification through radio frequency is after the barcode method the next generation of surveillance systems designed for a contactless identification of objects and persons. RFID technology can be applied in many fields of human activity including industrial trade and business safety measure. One of the technologies of radiowave identification used in the security business is the aerial system EAS securing articles of commerce in stores. It provides easy technology and is undemanding of both administration and organization.

The electronic system of security (EAS) is used as an unreplacable helper to identify articles of commerce which were intentally or unintentially not paid for by the customer. The EAS system cannot be applied without the use of human assistance and has to follow the rules within the defined borders of basic human rights and freedom.

Occasional difficulties in the field of commercial security are caused by the system resulting in false alarms. For that reason a member of SBS cannot stop and take hold of the suspicious person detected by the automatic signalization. The employee of SBS can only act according to the law defined order of taking hold of a suspect. Only in terms of internal regime security the employer can make use of personal searching's of the employees with the help of the electronic security system.

Although we have registered a significant development in technology of radio wave identification we can expect as a result of further research the elimination of false alarms which would lead to a wider use of the system in the field of commercial security.

SEZNAM POUŽITÉ LITERATURY

Monografické publikace:

[1] LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti I*. Vyd. 3. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010, 81 s. ISBN 978-80-7318-889-4 (BROž.).

[2] LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti II*. Vyd. 2. Zlín: Univerzita Tomáše Bati ve Zlíně, 2007, 123 s. ISBN 978-80-7318-631-9 (BROž.).

[3] IVANKA, Ján. *Systemizace bezpečnostního průmyslu I*. Vyd. 3. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009, 123 s. ISBN 978-80-7318-850-4 (BROž.).

[4] IVANKA, Ján. *Mechanické zábranné systémy*. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010, 151 s. ISBN 978-80-7318-910-5 (BROž.).

[5] Trestní předpisy: trestní zákon, trestní řád, výkon trestu odnětí svobody, výkon vazby, Probační a mediační služba, peněžitá pomoc obětem trestné činnosti, Rejstřík trestů, soudnictví ve věcech mládeže, zajištění majetku, amnestie : přestupky : zákon o přestupcích, paušální částka nákladů řízení : podle stavu k 7.11.2005. Ostrava: Sagit, 2005, 368 s. Úplné znění, č. 498. ISBN 80-720-8501-8.

Internetové zdroje:

[6] RFID portál, co je RFID? [online]. [cit. 2012-04-16]. Dostupné z WWW: <http://www.rfidportal.cz/index.php?page=rfid_obecne>

[7] Combitrading, jak pracuje systém RFID? [online]. [cit. 2012-04-16]. Dostupné z WWW: <http://www.combitrading.cz/technologie/jak-pracuje-rfid.html>

[8] Combitrading, druhy a typy čárového kódu [online]. [cit. 2012-04-16]. Dostupné z WWW: <http://www.combitrading.cz/technologie/druhy-a-typy-caroveho-kodu.html>

[9] New-rfid-concept.com [online]. [cit. 2012-04-16]. Dostupné z WWW: <http://new-rfid-concept.com/rfid_and_nfc.html>

[10] Barco [online]. [cit. 2012-04-16]. Dostupné z WWW: <http://www.barco.cz/?id=produkty&sel=27>

[11] Přednáška Základy informatiky ze dne 15. 1. 2011

[12] Wikipedie, Otevřená encyklopedie, Sinus [online]. c2012 [citováno 16. 04. 2012]. Dostupné z WWW: <http://cs.wikipedia.org/w/index.php?title=Sinus&oldid=7973216>

[13] Přednáška Ing. R. Drgy ze dne 17. 12. 2011

[14] Retailtheftprevention [online]. [cit. 2012-04-16]. Dostupné z WWW: <http://www.retailtheftprevention.com/how_stuff_works.html>

[15] Slovakalarms [online]. [cit. 2012-04-16]. Dostupné z WWW: <http://www.slovakalarms.sk/system-quickpower/i-2958.html>

[16] Acsystems [online]. [cit. 2012-04-16]. Dostupné z WWW: <http://acsystems.cz/eshop-produkt/rf_systemy/rf_etikety_82mhz/cz>

[17] Barco [online]. [cit. 2012-04-16]. Dostupné z WWW: <http://www.barco.cz/?id=produkty&sel=15#138>

[18] Acsystems [online]. [cit. 2012-04-16]. Dostupné z WWW: <http://acsystems.cz/eshop-produkt/rf_systemy/detacher__uvolovac_pevnych_etiket/cz>

[19] Acsystems [online]. [cit. 2012-04-16]. Dostupné z WWW: <http://acsystems.cz/eshop-produkt/rf_systemy/deaktivator_rf_samolepek/cz>

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACS	Access Control Systems
AUTO ID	Automatická identifikace
CCTV	Closed Circuit Television
EAN	European Article Numbering
EAS	Electronic Article Surveillance
EKV	Elektronická kontrola vstupu
EMC	Elektromagnetická kompatibilita
EMI	Elektromagnetická interference
EMS	Elektromagnetická susceptibilita
EPC	Electronic Product Code
GS	Global Standards
HF	High Frequency
LAN	Local Area Network
LF	Low Frequency
MW	Microwave
PKB	Průmysl komerční bezpečnosti
PZS	Poplachový zabezpečovací systém
RF	Radio-frekvenční systémy
RFID	Radio Frequency Identification
RO	Read Only
RTF	Reader Talks First
RTLS	Real-time Location Service
RW	Read Write
SBS	Soukromá bezpečnostní služba

TTF	Tags Talk First
UHF	Ultra High Frequency
Wi-Fi	Bezdrátová síť
WORM	Write Once Read Many

SEZNAM OBRÁZKŮ

SEZNAM TABULEK