Komunikace v blízkém poli
Near Field Communication

Bc. Jakub Havlíček

Diplomová práce
2015

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2014/2015

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

Jméno a příjmení:	**Bc. Jakub Havlíček**
Osobní číslo:	**A13442**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Počítačové a komunikační systémy**
Forma studia:	**prezenční**
Téma práce:	**Komunikace v blízkém poli**
Téma anglicky:	**Near Field Communications**

Zásady pro vypracování:

1. **Popište technologii RFID.**
2. **Srovnejte jednotlivé metody, které se pro komunikaci v blízkém poli používají, a popište jejich výhody a nevýhody.**
3. **Posuďte možnosti jednotlivých metod používaných v rámci komunikace v blízkém poli.**
4. **V laboratoři elektromagnetické kompatibility změřte spektrum a intenzitu elektromagnetického pole vyzařovaného vzorkem RFID čtečky.**
5. **Na základě naměřených výsledků navrhněte optimalizaci vazební antény měřené RFID čtečky.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **MAYER, Daniel. Aplikovaný elektromagnetizmus: Úvod do makroskopické teorie elektromagnetického pole pro elektrotechnické inženýry. 2. Vyd. České Budějovice: Kopp, 2012, 538 s. ISBN 978-80-7232-436-1.**
2. **MAZÁNEK, Miloš a Pavel PECHAČ. Šíření elektromagnetických vln a antény. 2. Vyd. , Přeprac. Praha: Vydavatelství ČVUT, 2005, 259 s. ISBN 8001030326.**
3. **SVAČINA, Jiří. Elektromagnetická kompatibilita: Principy a poznámky. 1. Vyd. Brno: Vysoké učení technické, 2001, 156 s. ISBN 8021418737.**
4. **GLOVER, Bill a Himanshu BHATT. RFID Essentials. Massachusetts, USA: O'Reilly Media, 2006. ISBN 978-0-596-00944-1.**
5. **WANT, Roy. RFID Explained: Synthesis Lectures on Mobile and Pervasive Computing. California, USA: Morgan and Claypool Publishers, 2006. ISBN 978-1598291087.**
6. **PERIS LOPEZ, Pedro. Security and Trends in Wireless Identification and Sensing Platform Tags: Advancements in RFID. Hershey, Pennsylvania: IGI Global, 2012. ISBN 978-1466619906.**
7. **COSKUN, Vedat, Kerem OK a Busra OZDENIZCI. Near Field Communication (NFC): From Theory to Practice. New York, USA: Wiley, 2012. ISBN 978-1119971092.**

Vedoucí diplomové práce: **Ing. Martin Pospíšilík, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání diplomové práce: **12. ledna 2015**

Termín odevzdání diplomové práce: **15. května 2015**

Ve Zlíně dne 6. února 2015

L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Miroslav Matýsek, Ph.D.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/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 diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/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 diplomovou/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 – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové/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 diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/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 diplomové/bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně 25.5.2015

Horňák
.....
podpis diplomanta

ABSTRAKT

Práce je zaměřena na technologii komunikace mezi zařízeními s využitím tzv. blízkého pole. Typickým zástupcem této technologie je RFID, která bude popsána v rámci teoretické části práce. Dále pak budou v teoretické části popsány podobné technologie, ať už předchůdci RFID čárové kódy nebo další technologie vycházející právě z RFID, například NFC. Práce shrne princip těchto technologií, jejich uplatnění a také bezpečnost. Praktická část práce bude zaměřena na laboratorní měření v laboratoři elektromagnetické kompatibility, přičemž bude kladen důraz na optimalizaci antén RFID čteček, které již byly na UTB FAI vyrobeny.

Klíčová slova: RFID, tag, čtečka, komunikace, frekvence, NFC, bezpečnost, měření, intenzita, spektrum

ABSTRACT

The thesis focuses on the technology of communication between devices using so-called Near Field. A typical representative of this technology is RFID, which will be described in the theoretical part. Furthermore, the theoretical part will describe similar technologies, whether predecessors RFID bar codes or other technology inherent in the RFID, for example NFC. Work will summarize the principle of these technologies, their usage and security. Practical work will be focused on laboratory measurements in the laboratory of electromagnetic compatibility EMC, with an emphasis on optimizing antennas RFID readers that have already been made at TBU FAI.

Keywords: RFID, tag, reader, communication, frequency, NFC, security, measurement, intensity, spectrum

Tímto bych chtěl poděkovat svému vedoucímu panu Ing. Martinu Pospíšilíkovi Ph.D., za ochotu a výpomoc při tvorbě této diplomové práce. Dále pak celé své rodině a přátelům za podporu. A také Univerzitě Tomáše Bati ve Zlíně, která mi umožnila studovat.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

RFID (Radio Frequency Identification – Identifikace na rádiové frekvenci) patří mezi jedny z rychle se rozvíjejících technologií a to zejména kvůli jejímu potenciálu. Tato technologie nalezla a stále nalézá uplatnění v mnoha odvětvích lidské činnosti. Jedná se o celkem starou technologii, avšak pokroky ve výrobě čipů otevřeli této technologii dveře k novým možnostem a uplatněním v různých aplikacích. Pokud bychom chtěli hovořit o možném předchůdci této technologie, pravděpodobně by to byla identifikace pomocí čárových kódů. Tyto dvě technologie lze porovnávat pomocí různých kritérií, avšak jako u kterékoliv technologie, každá má své vlastní výhody i nevýhody. Pokud bychom se naopak zaměřili více na modernější technologie, potom by naši pozornost určitě upoutaly technologie jako Bluetooth či NFC. Právě o NFC technologii se hovoří jako o nástupci RFID. Ale nebudeme předbíhat dobu.

Pokud jde o samotnou technologii RFID, tak tato technologie je založena na bezdrátovém přenosu identifikačního čísla nebo dat prostřednictvím elektromagnetických rádiových vln. Tuto technologii lze úspěšně nasadit a používat v mnoha odvětvích a oblastech, kde je kladen důraz na co nejrychlejší a přesné zpracování informací a okamžitý přenos načtených dat k následnému zpracování. To následně vede ke zvýšení přesnosti, rychlosti a efektivnosti zejména obchodních, logistických, skladových a výrobních procesů.

V teoretické části práce se zaměříme hlavně na popsání technologie RFID, její princip, zařízení, použití, výhody a nevýhody. Poté si popíšeme perspektivní technologii, která zde již také byla zmíněna a to NFC. Opět bude popsán princip této technologie, její použití, výhody a nevýhody a také bude provedeno srovnání s podobnými technologiemi jako například čárové kódy nebo Bluetooth.

Praktická část je zaměřena na laboratorní měření v laboratoři elektromagnetické kompatibility, přičemž bude kladen důraz na optimalizaci antén RFID čteček, které již byly na UTB FAI vyrobeny.

I. TEORETICKÁ ČÁST

1 RFID

Radio Frequency Identification (RFID) by se dala charakterizovat jako bezdrátová technologie, která využívá elektromagnetických polí pro přenos dat a napomáhá nám k identifikaci objektů pomocí rádio-frekvenčních vln. Systémy založené na RFID technologii lze úspěšně používat tam, kde je zapotřebí co nejrychleji a nejpřesněji zpracovat informaci a zvýšit efektivnost procesů. [7] Počátky RFID technologie leží již v 19. století, kdy se značně projevil pokrok v elektromagnetizmu. Mezi průkopníky můžeme zařadit Michaela Faradaye s objevem elektrické indukce nebo třeba také Jamese C. Maxwella, který popsal elektromagnetické rovnice. Ranným předchůdcem RFID byly tzv. systémy detekce objektů. Jeden z prvních patentů na takový systém byl rádiový vysílač pro detekci objektů navržený Johnem L. Bairdem v roce 1926. Jedna z prvních aplikací přímo RFID systému byl tzv. „Identify Friend or Foe“ (IFF) systém, vyvinutý Britským Královským Letectvem, během druhé světové války. IFF umožňovalo pilotům a operátorům, kteří seděli za radarem, automaticky rozlišit přátelské letectvo od nepřátelského pomocí rádio-frekvenčních signálů. Pokud jde o komerční aplikace, systémy RFID lze považovat za instanci automatické identifikace (Auto-ID). Auto-ID systémy v podstatě připojí jméno nebo identifikátor fyzickému objektu a tyto informace jsou poté z objektu sejmuty/přečteny. Tento identifikátor může být reprezentován opticky, elektromagneticky nebo dokonce chemicky. Pravděpodobně nejznámějším auto-ID systémem je Universal Product Code (UPC), který je jednodimenzionální, optický čárový kód, ve kterém jsou zakódovány informace o produktu a značce zboží. Tento systém je celosvětově rozšířený a hojně využívaný (viz kapitola 1.1 Čárové kódy). [8]

Existuje několik metod k jednoznačné identifikaci využívající RFID, ale nejběžnější je uchování EPC kódu (viz kapitola 1.2.2.2 EPC) spolu se sériovým číslem a dalšími důležitými údaji, které umožní rozpoznání a dohledání konkrétního produktu. Na mikročipu, který je připojen k anténě a je zalitý do substrátu, je uložena celá informace. Dohromady tyto složky tvoří tzv. RFID tag (viz kapitola 1.2.2 RFID tagy), který je schopen uloženou informaci vyslat ke čtečce. Ta přemění vyslané rádiové vlny přijaté z RFID tagu na formu, která může být dále zpracována. [9]

1.1 Čárové kódy

Čárový kód již jistě každý z nás někdy v životě viděl (viz Obr. 1). Jedná se o sadu tištěných černých pruhů, které mají definovanou šířku a lze je pomocí laserové čtečky načíst. Jde o prostředek pro automatizovaný sběr dat neboli auto-id. Existují různé typy čárových kódů, dnes se ovšem nejčastěji setkáváme s typem EAN, který na trh přišel již v roce 1976. Mezi další modifikace kódů lze zařadit např. QR kód, kruhový či mozaikový kód. [8]

Obrázek 1 - Ukázka čárového kódu [17]

Princip činnosti čárového kódu je založen na odrazu červeného světla. Tradiční snímače vyzařují červený pruhový paprsek, který je odrážen světlými mezerami v kódu a pohlcován tmavými čarami. Snímač analyzuje rozdíly v reflexi a ty následně přemění na elektrické signály, které odpovídají šířkám čar a mezer. Signály se dále převedou na číslice či písmena, která obsahuje čárový kód. [8] Obsah čárového kódu může být různý, od čísla výrobku, místa uložení až po informace, které Vám dávají pravomoc např. vstoupit do uzavřeného objektu. V dnešní době lze přejít z klasických laserových snímačů na snímače digitální, které pracují jako fotoaparát. Čárový kód se vyfotí nebo se pomocí aplikace a kamery sejme a dekóduje se jeho obsah. [7]

Čárové kódy se používají již pěknou řádku let a nutno říct, že se osvědčily a jsou hojně používané. Kompletní nahrazení čárových kódů technologií RFID se nejspíše v nejbližší době konat nebude a to zejména proto, že mezi hlavní výhody oproti RFID patří stále jejich pořizovací cena, která je u čárových kódů výrazně nižší. Avšak RFID technologie nám nabízí oproti čárovým kódům také několik nesporných výhod. Jako první výhodu lze zmínit právě technologii, na které je RFID založena a to rádiovou komunikaci. Zde odpadá nutnost přímé viditelnosti čárového kódu na snímač (nenarušený kód). U RFID tagů stačí, aby byl v dosahu čtecího pole snímače. A jelikož většina z nás již byla někdy nakupovat v nějakém supermarketu, víme, že produkty s čárovým kódem musíme na pokladně načítat odděleně, což někdy dokáže zabrat hodně času, nemluvě o tom pokud

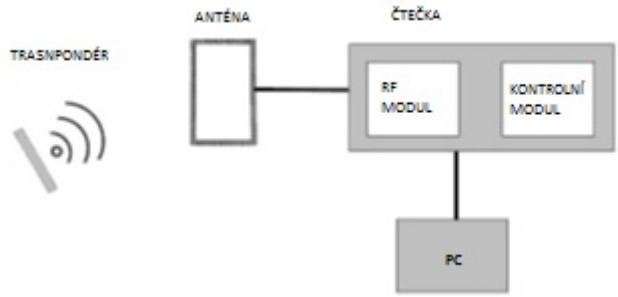
je kód poškozený a nejde načíst. Rádiová komunikace nám umožní načíst větší počet produktů označených RFID čipy zároveň (ve velmi krátkých, po sobě jdoucích intervalech) tudíž odpadá nutnost přímé viditelnosti. Mezi další rozdíly patří větší mechanická odolnost RFID tagů oproti čárovým kódům. Výhody a nevýhody RFID jsou popsány v dalších kapitolách. [7]

1.2 Princip

RFID systémy se skládají ze tří částí ve dvou kombinacích. Stanice (vysílač/přijímač) a anténa jsou obvykle kombinovány jako RFID čtečka. Transpondér (vysílač/respondér) a anténa jsou kombinovány, aby vytvořili RFID tag.

Základní RFID systém se skládá ze tří částí:

- Anténa nebo cívka,
- Transceiver (stanice s dekodérem),
- Transpondér (RF tag) s elektricky naprogramovanou identifikační informací.



Obrázek 2 - RFID systém

RFID systémy obsahují elektronické zařízení tzv. transpondéry nebo tagy a čtecí elektroniku pro komunikaci právě s tagy. Jak je znázorněno na obrázku výše, pokud transpondér (tag) vstoupí do čtecí zóny, jeho data jsou zachycena čtečkou a potom mohou být přenesena pomocí standardních rozhraní to počítače, tiskárny nebo dalších vhodných zařízení. Čtečka vysílá rádiové vlny (rozsah je závislý na použité frekvenci) a pokud tag vstoupí do elektromagnetické zóny čtečky, tak detekuje aktivační signál. Čtečka dekóduje data, která jsou zakódována v integrovaném obvodu tagu a tyto data jsou předána hostitelskému počítači ke zpracování. [29]

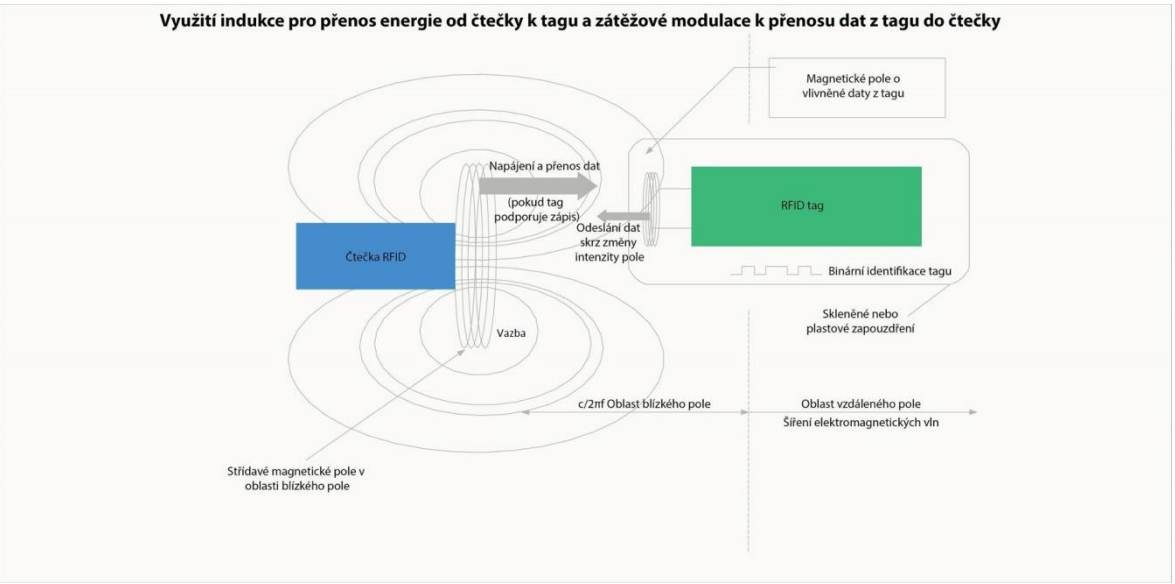
1.2.1 Komunikace

Pro přenos energie z RFID čtečky do RFID tagu existují dva odlišné způsoby. Způsob využívající magnetické indukce a způsob využívající zachycení elektromagnetických vln. Tyto dva způsoby využívají elektromagnetických vlastností spojených s rádio-frekvenční anténou – komunikace v blízkém poli a komunikace ve vzdáleném poli. Oba způsoby mohou přenést dostatek energie ke vzdálenému tagu, aby udrželi jeho provoz. Typicky mezi 10 μW až 1 mW, záleží na typu tagu. Pro srovnání, nominální výkon procesoru Intel XScale spotřebuje přibližně 500 mW a Intel Pentium 4 spotřebuje až 50 W. Prostřednictvím různých modulačních technik, jsou signály v blízkém i vzdáleném poli schopny vysílat a přijímat data. [30]

1.2.1.1 Blízké pole

Faradayův princip magnetické indukce je základem pro spojení čtečky a tagu v blízkém poli. Čtečka prožene velký střídavý proud přes její vedení (cívku) a to má za následek vytvoření magnetického pole. Pokud umístíte tag, který má své vedení (cívku) do tohoto pole, tak se přenese střídavé napětí od čtečky k tagu. Je-li toto napětí přivedeno ke kondenzátoru, kde se nahromadí, pak je toto nahromaděné napětí využito pro aktivaci a napájení tagu. Tagy, které využívají blízké pole, posílají data zpět ke čtečce pomocí zátěžové modulace. Protože jakýkoliv odebíraný proud z cívky tagu navýší jeho vlastní magnetické pole, které bude oponovat magnetickému poli čtečky, tak je vedení čtečky schopné odhalit mírné zvětšení protékajícího proudu. Tento proud je úměrný zatížení působící na vedení tagu. Jedná se o stejný princip jako napájení transformátorů, které lze dnes najít ve většině domácností, i když obvykle primární a sekundární cívky transformátoru jsou spolu úzce navinuty s cílem zajistit efektivní přenos energie. Nicméně, jak magnetické pole zasahuje mimo primární cívku, sekundární cívka může získat část energie na dálku, podobně je tomu tak i mezi čtečkou a tagem. Čtečka pak může obnovit tento signál sledováním změn proudu přes svoje vedení. Existují různé modulace a kódování v závislosti na počtu potřebných ID bitů, rychlosti přenosu dat a dalších redundantních bitů, umístěných v kódu pro odstranění chyb vyplívajících z šumu v komunikačním kanálu. Využití blízkého pole je nejjednodušší přístup k implementaci RFID systémů. Nicméně i komunikace v blízkém poli má jistá fyzikální omezení. Rozsah, pro který můžeme magnetickou indukci použít je dán vztahem $c/2\pi f$, kde c je konstanta (rychlost světla) a f je frekvence. Čím vyšší je frekvence, tím je možná vzdálenost

komunikace v blízkém poli nižší. Dalším omezením je energie, která je dostupná pro indukci, jako funkce vzdálenosti od vedení (cívky) čtečky. Magnetické pole klesá koeficientem $1/r^3$, kde r je vzdálenost mezi tagem a čtečkou, podél středu přímky kolmé na rovinu cívky. Pokud chceme načíst více tagů ve stejný čas, tak každý tag vyžaduje vyšší rychlost přenosu dat a vyšší provozní frekvenci. Tyto omezení vedly k novým návrhům pasivního RFID systému, založenému na komunikaci ve vzdálené poli. [30]

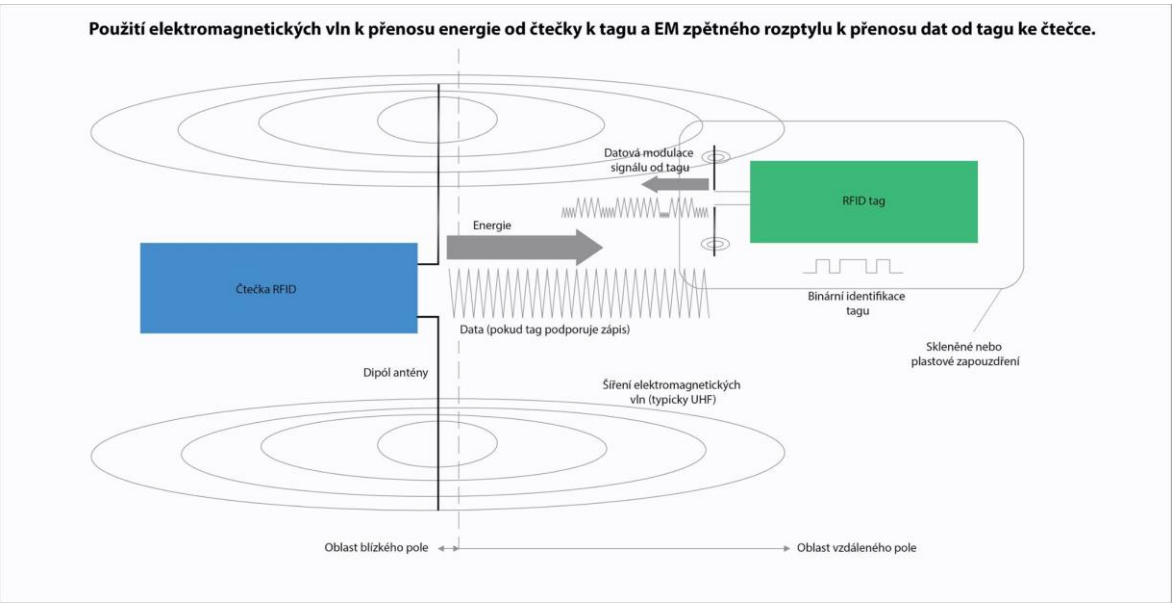


Obrázek 3 - Komunikace v blízkém poli

1.2.1.2 Vzdálené pole

Jedná se o komunikaci založenou na zachytávání emisí elektromagnetických vln šířených z dipólu připojeného ke čtečce. Menší dipól v tagu přijímá tuto energii, jako střídavý potencionální rozdíl, který se vyskytne mezi rameny dipólu. Dioda může tento potenciál propojit do kondenzátoru, což bude mít za následek akumulaci energie, za účelem napájení elektroniky. Pokud je anténa navržena s přesnými rozměry, může být laděna na určité frekvenci a absorbovat většinu energie, která této frekvence dosahuje. Nicméně pokud se na této frekvenci vyskytne impedanční šum, anténa odrazí zpět část energie (jako malé vlny) ke čtečce, která poté může detekovat tuto energii pomocí citlivého rádiového přijímače. Změnou impedance antény může tag odrážet zpět příchozí signál ve vzoru, který kóduje identifikátor tagu. Pro tento účel si můžete v praxi anténu rozladit umístěním tranzistoru napříč jeho dipólu a poté částečným vypínáním a zapínáním. Tagy, které používají principy vzdáleného pole a běžně pracují na frekvenci vyšší než 100 MHz,

operují typicky v ultra-vysokém frekvenčním pásmu (jako je 2,45 GHz). Pod touto frekvencí je doména RFID založených na komunikaci v blízkém poli. Rozsah vzdáleného pole je limitován množstvím energie, která se předá od čtečky k tagu a tím, jak má čtečka citlivý rádiový přijímač pro odražený signál. Skutečný zpětný signál je velmi malý, protože se jedná o výsledek dvou útlumů. První útlum nastává, když elektromagnetické vlny vyzařují od čtečky k tagu. A druhý útlum, když odražená vlna míří zpátky od tagu ke čtečce. Tudíž, návratová energie je $1/r^4$, kde r je opět vzdálenost mezi tagem a čtečkou. Naštěstí, díky Moorovu zákonu a zmenšování velikosti polovodičů při výrobě se energie, která je potřeba k aktivaci a pohánění tagu na dané frekvenci, snižuje (v současné době se jedná o pár microwattů). To znamená, že s moderními polovodiči jsme schopni navrhnout tagy tak, že je lze číst z větší vzdálenosti, než tomu bylo před několika lety. Kromě toho byly vyvinuty laciné rádio přijímače, které mají lepší citlivost. Takže nyní mohou detekovat signály za rozumnou cenu, s výkonem řádově 100 dBm v pásmu 2,4 GHz. Typická čtečka fungující na principu vzdáleného pole je schopna úspěšně komunikovat s tagy na vzdálenost 3 metrů. Některé společnosti dokonce tvrdí, že jejich výrobky mají čtecí dosah až 6 metrů. [30]

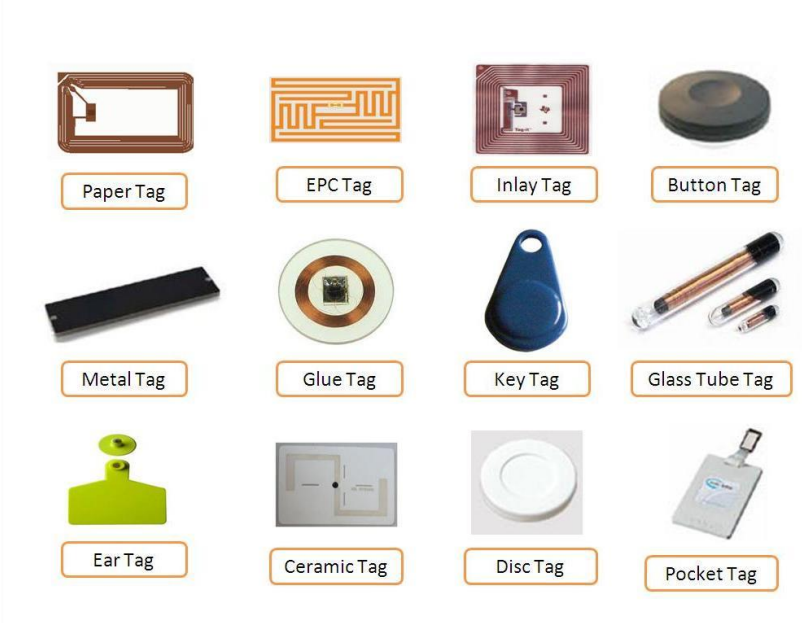


Obrázek 4 - Komunikace ve vzdáleném poli

1.2.2 RFID Tagy

Jak již bylo zmíněno, rádio-frekvenční komunikace je uskutečněna pomocí tzv. tagů (čipů). Jedná se o paměťové médium používané právě v RFID systémech, které je připojeno k objektům. [9] Tag je typicky složen z antény nebo spojovacího prvku a

integrovaného obvodu. Tagů existuje velké množství druhů, které nabízí různé funkce, mají různé zdroje energie a pracují na rozdílných rádiových frekvencích. Dále se tagy mohou lišit materiálem, tvarem, formou a samozřejmě rozměry. Ukázky různých tagů je možno vidět na obrázcích 5, 6, 7, 8. Moderní tagy mají tendenci provádět identifikaci pomocí integrovaného obvodu, který poskytuje úložiště a výpočetní jednotku. Integrované obvody jsou ve výrobním procesu připojeny k anténě ještě předtím, než jsou zapouzdřeny do finálního výrobku.



Obrázek 5 - Ukázky RFID tagů [18]

1.2.2.1 Rozdělení tagů

RFID čipy lze rozdělit do několika základních skupin a to podle možnosti napájení, možnosti zápisu a také podle toho, v jakém frekvenčním pásmu pracují.

a) Podle možnosti napájení

Aktivní: buď jsou připojeny k elektrické síti, nebo obsahují vlastní zdroj napájení. Jsou schopny samy vysílat své identifikace. Jsou složitější a dražší. Používají se pro aktivní lokalizaci. Baterie vydrží cca 1-5 let. Čtecí vzdálenost se udává do 100 metrů. Velikost paměti dosahuje až 100 kb. V praxi nejsou tak používané jako pasivní tagy. [8]

Obrázek 6 - Aktivní tag [19]

Pasivní: vysílač (čtečka-reader) periodicky vysílá pulsy do okolí. Pokud se v blízkosti objeví pasivní RFID čip, využije přijímaný signál k nabití svého napájecího kondenzátoru a odešle odpověď. Podle frekvence na které pracují je dána akční vzdálenost čtení, od 0,5 až 10 metrů. Velikost paměti 64 – 256 bitů. [8] [9]

Obrázek 7 - Pasivní tag [20]

Semi-aktivní: mají baterii, která ovšem slouží pouze k zvýšení dosahu čtení.

Obrázek 8 - Semi-aktivní tag [21]

Typ	Pasivní	Semi-aktivní	Aktivní
Zdroj energie	Příjem RF energie	Baterie	Baterie
Komunikace	Pouze odpověď	Pouze odpověď	Zahájení i odpověď
Dosah	10 m	100 m +	100 m +
Cena	Nejlevnější	Dražší	Nejdražší
Použití	Bezkontaktní karty, identifikace zboží	Elektronické mýtné, sledování palet	Sledování velkých nákladů a chovu hospodářských zvířat

Tabulka 1 - Porovnání vlastností tagů

b) Podle možnosti zápisu

Read Only: pouze pro čtení (sériové číslo zakódované při výrobě tagu).

WORM: jednou zapsatelné (vhodné pro etiketu na zboží).

Read/Write: mnohokrát přepisovatelné.

c) Frekvenční pásma

LF – (125 až 135 KHz) – tagy s nízkofrekvenčním přenosem se vyznačují dosahem do 0,5 m a malou rychlostí komunikace. Jsou vhodné ke čtení přes kapalinu, částečně i přes kov. Jsou použitelné ve vlhkém prostředí.

HF – (13,56 MHz) – tagy s vysokofrekvenčním přenosem se vyznačují dosahem do 1 m a dosahují vyšší komunikační rychlosti než LF tagy. Díky největší rozšířenosti tohoto typu tagů jsou také nejlevnější. Zkrácený dosah u kovů a kapalin.

UHF – (860 až 960 MHz) – tagy s ultra vysokofrekvenčním přenosem mají dosah přibližně 3m. Vyznačují se velkou komunikační rychlostí.

MW – (2,45 a 5,8 GHz) – tagy s mikrovlnnou frekvencí mají dosah až 10 m. Vyznačují se komunikační rychlostí až 2 Mb/s. Složitější konstrukce = dražší provedení. Velký vliv kapalin a kovů na komunikaci.

UWB – (3,1 až 10,6 GHz) – tagy pracující s ultra širokopásmovou frekvencí mají dosah až 200 metrů. Toto frekvenční pásmo je kompatibilní s kapalinami i kovy.

Přehlednější znázornění frekvenčních pásem udává tabulka č. 2.

Rozsah frekvencí	Frekvenční pásmo	Pasivní čtecí vzdálenost
Nízká (LF)	125-135 KHz	10-20 cm
Vysoká (HF)	13,56 MHz	10-20 cm
Ultra-vysoká (UHF)	868-928 MHz	3 m
Mikrovlnná (MW)	2,45 a 5,8 GHz	3 m
Ultra-širokopásmová (UWB)	3,1-10,6 GHz	10 m

Tabulka 2 - Znázornění frekvenčních pásem

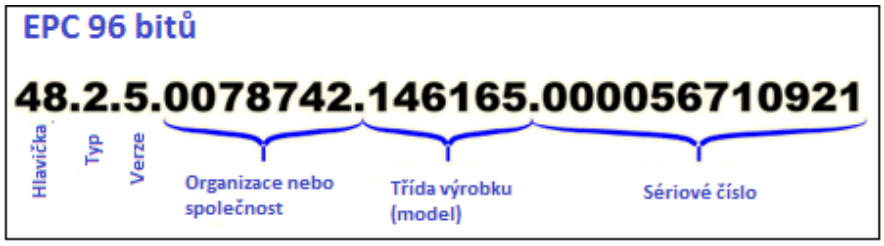
1.2.2.2 EPC

RFID tag v sobě uchovává jedinečné číslo, jednoznačný identifikátor. V současnosti se nejvíce osvědčilo zaznamenání čísla EPC. Zkratka EPC - Electronic Product Code - znamená v překladu elektronický kód produktu a jde o jednoduchý kompaktní kód, který

jednoznačně identifikuje daný tag. Jedná se o sériové číslo zapsané v mikročipu. Tento jedinečný kód obsahuje informaci, kterou RFID tag předává RFID čtečce (readeru). EPC je přidělován a spravován světovou organizací Global Standards (GS1). Struktura kódu EPC umožňuje definovat vedle výrobce nejen název produktu, ale také jeho výrobní číslo konkrétní šarže. To má za následek zajištění rychlé a přesné identifikace dalších údajů, jako je např. datum spotřeby, datum výroby atd. EPC dokáže na rozdíl od jiných kódů, jedinečně identifikovat každou jednotku zboží. Kombinace RFID a EPC představuje účinný nástroj současné moderní automatické identifikace. [11]

8 bitů	Hlavička - velikost, typ, verze EPC	Přiděleno EPC Global
28 bitů	Informace o firmě - definice výrobce (268mil. výrobců)	Přiděleno EPC Global
24 bitů	Třída výrobku - definice druhu produktu (16 mil. tříd)	Přiděleno vedením společnosti
36 bitů	Sériové číslo produktu - definice jednotky zboží (68 mld. čísel)	Přiděleno vedením společnosti

Tabulka 3 - Rozdělení EPC a rozdělení bitů [11]



Obrázek 9 - Rozdělení EPC [16]

1.2.3 RFID Čtečky

Aby RFID čtečky získaly identifikační informace, komunikují s tagem pomocí rádio-frekvenčního kanálu. Podle typu tagu může komunikace probíhat ve formě pingu anebo ve více komplexní formě pomocí multi-round protokolů. V prostředí s hodně tagy může čtečka použít anti-kolizní protokol, aby zajistila, že v komunikaci nedojde ke konfliktu. Anti-kolizní protokol umožní čtečce postupně, ale rychle komunikovat s velkým množstvím tagů. Čtečky obvykle dodávají energii tzv. pasivním tagům pomocí jejich rádio-frekvenčního kanálu a to vede k zahájení komunikace. Existuje mnoho variant čteček, které pracují na různých frekvencích a nabízí různé funkce (kontrola zboží,

přístupu atd.) Mají svoje vyhodnocovací jednotky a interní paměť. Mohou pracovat s rozšiřujícím systémem anebo uchovávat a zpracovávat všechna data lokálně. [29] RFID čtečky mohou být rovněž implementovány do ručních mobilních zařízení, které Vám například umožní rychlé načtení zboží a okamžitou kontrolu skladu pouhým projitím kolem zboží.

Klasická RFID čtečka se skládá z několika základních komponent. Jedná se o frekvenční rozhraní, které je rozděleno na příjem a vysílání. To znamená, že odděluje přenosové cesty. Tato komponenta se stará o generování vysílací energie pro aktivaci tagu a dále pak moduluje či demoduluje přenos signálů právě z tagu. Dále čtečka obsahuje kontrolní systém. Tento kontrolní systém je složen z mikroprocesoru, ASIC modulu pro kryptování a šifrování signálu a ze síťového modulu. Kontrolní systém má za úkol kontrolovat komunikaci s tagem. Dohlíží na šifrování dat, autentizaci a zabraňuje kolizím pomocí anti-kolizního protokolu. Kontrolní systém také kóduje a dekóduje signál a komunikuje se síťovými službami. Další důležitou součástí čtečky je její anténa, pomocí které se vysílá generovaný signál do okolí, nebo také přijímají signály z tagů. Antény mohou být integrované nebo externí. Může být jedna nebo jich čtečka může obsahovat více.

Obrázek 10 - Ukázka RFID čteček [22] [23]

1.3 Použití, výhody a nevýhody

Technologie RFID nalezla uplatnění v mnoha odvětvích. Jedná se o velice zajímavou možnost řešení úloh automatické identifikace. Zde uvádím několik příkladů.

1.3.1 Použití

Logistika:

- Zrychlení procesu příjmu, výdeje, přesunu a inventarizace produktu
- Odstranění chyb obsluhy a zpřesnění celé evidence produktů
- Velká odolnost RFID čipů (vlhkost, teplota, atd.)
- Minimalizace nákladů spojených se značením produktů
- Přesná evidence spotřebitelských jednotek, kartónů, palet
- Opakovaný zápis údajů zboží do čipu během celého logistického pohybu
- Rychlé načtení údajů - není nutná přímá viditelnost označených jednotek

Výroba:

- Přesné řízení toku materiálu ve výrobě (snížení zásob)
- Dohled na správnou kompletaci celku
- Okamžitá informace o stavu výroby
- Možnost zápisu informací do čipu během výroby
- Zpětná dohledatelnost až na úroveň jednotlivých materiálů
- Sledování využití a činností na pracovišti
- Možnost umístit čip natrvalo do výrobku a informace poté využít v distribuci

Evidence majetku:

- Snížení chybovosti při evidenci a inventarizaci majetku
- Možnost zápisu většího množství dat do čipu, např. uložení poslední inventarizace
- Výrazné zrychlení procesu inventarizace majetku
- Finanční úspory v nákladech na obsluhu při inventarizaci

Zdravotnictví:

- Prevence chyb zdravotnického personálu
- Snadné a rychlé zobrazení všech údajů o pacientovi
- Přepisování stavu pacienta

Ochrana majetku:

- Přístupový systém
- Docházkový systém
- Poplachový zabezpečovací systém

- Informační systémy
- Měření a regulace
- Elektrická požární signalizace

Do dalšího odvětví může také patřit zemědělství. Sledování zvířat a jejich diagnostiky, identifikace rostlin nebo je možné uplatnění také ve sportu a hrách. Stopování sportovních událostí, sledování golfových míčků, identifikace herních čipů atd. Jak je vidět, prostor pro uplatnění této technologie je veliký. [29]

1.3.2 Výhody RFID

Na začátku této práce byly zmíněny a lehce porovnány dvě identifikační technologie a to RFID a čárové kódy. Ačkoli je nepravděpodobné, že by RFID v blízké budoucnosti zcela nahradila běžně používané čárové kódy, tak níže je uveden seznam několika nesporných výhod právě RFID technologie, díky kterým nalézá tak hojné uplatnění v praxi. [29] [30]

- Detekce pomocí tagu nevyžaduje zásah člověka, snižuje náklady na zaměstnanost a eliminuje lidské chyby ze sběru dat
- Jelikož není zapotřebí přímé viditelnosti tagu při čtení, umístění je méně omezené
- RFID tagy mají větší čtecí vzdálenost (než čárové kódy)
- Tagy mohou mít možnost čtení/zápisu
- Na RFID tag lze uložit velké objemy dat, navíc má unikátní identifikátor
- Tagy jsou méně citlivé na nepříznivé podmínky (prach, chemikálie, fyzické poškození)
- Lze načíst více tagů současně
- RFID tagy mohou být kombinovány s čidly
- Automatické čtení na několika místech snižuje časové prodlevy a nepřesnosti v soupisu
- Tagy mohou lokálně uložit další informace, distribuovaným ukládáním dat se může zvýšit odolnost proti chybám v celém systému
- Snižuje čas potřebný pro inventury zásob a náklady na obstarávání

1.3.3 Nevýhody – omezení RFID

I když je RFID v dnešní době poměrně využívaná technologie, stále zde existují oblasti, kde maximální využití potenciálu této technologie vyžaduje vylepšení jak po technické, procesní, tak i bezpečnostní stránce. Nicméně na vyřešení těchto omezení neustále pracuje řada odborníků a specialistů. [30]

- **Standardizace** – Existence malého množství norem dává výrobcům svobodu při určování komunikačního protokolu, formátu a kapacitě informací uložených v tagu. Firmy tvoří vlastní řešení a později se může stát, že tato řešení nebudou kompatibilní s ostatními. Proto by se měli stanovit standardy pro komunikační protokoly, používané modulace signálu, rychlosti přenosu dat, kódování dat, kolizní algoritmy atd.
- **Cena** – Cenu lze u RFID brát také jako nevýhodu. I když se cena každým rokem snižuje, stále se u některých méně cenných výrobků vyplatí používat jiné technologie.
- **Kolize** – Pokus o čtení několika tagů najednou může mít za následek vznik kolizního signálu a poté může vést i ke ztrátě dat. Aby se tomu zabránilo, existují tzv. proti-srážkové algoritmy. Samozřejmě cena se s použitím takovýchto algoritmů zvyšuje.
- **Vadné tagy** – Ani výroba tagů není bezporuchová. Stále existuje určité procento výrobků vadných přímo z výroby. Tagy mohou být také poničeny během používání. Takové poškození může vést například k chybě při čtení tagu. Tato chyba pak může být velmi obtížně detekovatelná. Toto se může stát problémem například u načítání mnoha položek, které byly načteny při placení, ale nebylo bráno v potaz selhání či nefunkčnost tagu.
- **Bezpečnost** - Jednou z nejvážnějších otázek z hlediska bezpečnosti u RFID je otázka ochrany soukromí. Tagy jsou aktivní i po tom, co je zboží zakoupeno novým majitelem. Výrobci tvrdí, že lze tag deaktivovat, otázkou ale zůstává, jestli se tak opravdu stane. Když se nad tím zamyslíme, zákazník si koupí zboží, zaplatí platební kartou a tím pádem je jasně asociováno zákazníkovo jméno s vybraným produktem. Dále se dá tato situace využívat k marketingovým účelům. Dalším bezpečnostním problémem může být bezkontaktní čtení tagu. Udávaná čtecí vzdálenost sice není nějak veliká (pár centimetrů), ale za použití speciálního vybavení (mobilní čtečky) může být tag načten i z mnohem větší vzdálenosti.

Nikdo tak nepostřehne, že informace z Vašeho RFID tagu byly přečteny a odcizeny. Mezi další problém lze zařadit nezabezpečenou komunikaci mezi tagem a čtečkou. Komunikace založená na systému dotaz-odpověď. Samozřejmostí jsou dnes tagy, které podporují šifrování (symetrický šifrovací klíč, asymetrická kryptografie). Ovšem tyto bezpečnostní opatření se projeví na rychlosti, spotřebě, složitosti a ceně jednotlivých tagů. Dalším bezpečnostním rizikem jsou samozřejmě hackerské útoky na RFID systémy. Tyto útoky využívají slabinu systému, kde se technika RFID používá. Infikovaný tag totiž využije slabá místa softwaru, který ovládá čtečku a poté virusem nakazí celý systém. Velký důraz je také kladen na ochranu osobních informací. [6] [29]

2 NFC

Podle Mezinárodní Telekomunikační Unie existuje v dnešní době asi šest miliard mobilních telefonů, což dělá skoro jeden telefon pro každého člověka na planetě. Tyto zařízení se každým dnem stávají stále více a více populární a užitečnější s velmi rychle se rozvíjejícími vylepšeními a velkým množstvím funkcí. Jednou z nejvíce ožehavou funkcí zavedenou do mobilních zařízení je NFC, které umožňuje chytrým telefonům rychle a bezpečně komunikovat s jinými telefony nebo nenapájenými zařízeními. [31]

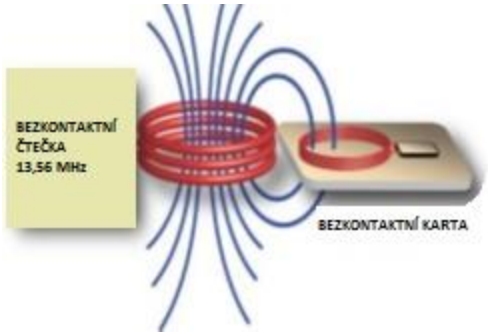
Near Field Communication (NFC), česky lze přeložit jako komunikace v blízkém poli, je modulární technologie rádiové bezdrátové komunikace, která probíhá ve velmi krátkých vzdálenostech (v řádu jednotek centimetrů). Přenos dat je uskutečněn na frekvenci 13,56 MHz pomocí elektromagnetické indukce. [1] Dá se říci, že NFC se vyvinulo z technologie RFID. V roce 2003 bylo NFC schváleno jako ISO/IEC standard. O rok později byla založena asociace NFC Forum. Jedná se o neziskové sdružení vývojářů, výrobců, finančních institucí atd., které bylo založeno společnostmi Nokia, Sony a Phillips. [2]

Obrázek 11 - NFC Forum logo [12]

V letech 2007/2008 proběhlo prvních pár pokusů o uvedení této technologie, ale bohužel neúspěšně. Dalo by se říct, že tuto technologii nastartovali až masově prodávané mobilní telefony právě s implementovanou NFC technologií. Od roku 2011 bylo pořádáno mnoho konferencí, kde výrobci předváděli originální možnosti implementace technologie NFC a spustili se první projekty plateb přes NFC. [1] [10]

NFC je technologie navržená tak, že vychází z RFID a umožňuje více komplexní výměnu dat mezi účastníky/objekty. NFC také umožňuje čtení některých pasivních RFID tagů. Umožňuje také zápis dat do určitých RFID tagů pomocí standardního formátu, nezávisle na typu tagu. Může také komunikovat s jinými zařízeními (NFC) v obousměrném, duplexním režimu. Zařízení s touto technologií si mohou vyměňovat informace o vlastních funkcích. Například můžete spojit svůj telefon s rádiem, takže se tyto zařízení navzájem identifikují a zjistí, že obě podporují Wi-Fi. Poté telefon začne vysílat (streamovat) audio do rádia přes Wi-Fi. Proč telefon nevysílá audio přes NFC? Ze

dvou důvodů. Za prvé, NFC připojení je záměrně krátkého dosahu, obecně do 10 cm. To umožňuje zařízením mít nízkou spotřebu energie a také nebude docházet k rušení ostatními zařízeními. Za druhé, relativně nízká rychlost přenosu dat v porovnání s Wi-Fi, Bluetooth a dalšími komunikačními protokoly. NFC nebylo navrženo pro vysokorychlostní komunikace. Tato technologie je pro komunikaci na malou vzdálenost, krátké zprávy a výměnu pověření (přihlašovacích údajů, identifikátorů). Zajímavostí na NFC je to, že umožnuje zahájit komunikaci bez nutnosti výměny hesel, párování a dalšími složitými kroky, které se objevují u ostatních protokolů. To znamená, že pokud si chcete s někým vyměnit informace, např. adresu, telefonní číslo, obrázek, stačí pouze přiložit telefony k sobě, kliknout na displej a je to. Na NFC může být nahlíženo jako rozšíření RFID technologie. NFC také pracuje s inicializačním a cílovým zařízení. Nicméně, může dělat víc než jen vyměňovat jedinečné identifikátory a číst nebo zapisovat do cílového zařízení. Nejzajímavější rozdíl mezi těmito dvěma technologiemi je ten, že cílová zařízení NFC jsou většinou programovatelná, např. mobilní telefony. To znamená, že místo pouze doručování statických dat z paměti, může zařízení NFC generovat skutečně jedineční obsah pro každou výměnu dat a doručit ji zpět k inicializačnímu zařízení. Například pokud používáte NFC pro výměnu adres mezi dvěma telefony, NFC zařízení může být naprogramováno tak, aby poskytlo pouze limitované informace, pokud s tímto zařízením ještě nikdy předtím nekomunikovalo.



Obrázek 12 - Indiktivní vazba [24]

Komunikace v blízkém poli je založena na induktivní vazbě. Na jejímž principu si předávají energii a data na vzdálenost několika centimetrů. NFC zařízení sdílejí základní technologii s (13,56 MHz) RFID tagy a bezkontaktními čipovými kartami, ale mají řadu klíčových doplňkových funkcí.

2.1 Režimy přenosu

K dispozici jsou tři provozní režimy, Reader/Writer (Čtení/Zápis), Peer-to-Peer, a Card Emulation (emulace karty). Režim pro čtení/zápis umožňuje jednomu NFC zařízení-mobilního telefonu, výměnu dat s jedním NFC tagem. Režim peer-to-peer umožňuje, aby si dvě NFC zařízení vyměnily data mezi sebou. V režimu emulace karet, může být použito NFC zařízení jako čipová karta v interakci se čtečkou NFC. Každý operační mód má jinou technickou infrastrukturu, a také i jiné výhody pro uživatele. [24]

2.1.1 Reader/Writer

Proces komunikace spočívá pouze v zápisu/čtení z nebo do NFC tagu, který je napájen elektromagnetickým polem iniciátora. Tento režim přenosu neklade důraz na vysokou bezpečnost vzhledem k povaze komunikace. Pro zápis v tomto režimu je maximální přenosová rychlost 106 kbit/s.

NFC zařízení se chová jako čtečka pro tagy jako jsou bezkontaktní karty a RFID tagy. Detekuje tag bezprostředně v blízkosti pomocí mechanismu zabraňujícímu kolizím. Aplikace v NFC zařízení může číst data z detekovaného tagu nebo do tohoto tagu i zapisovat pomocí režimu pro čtení/zápis. Tento režim je proto dále rozdělen pouze na čtení a pouze na zápis. V čtecím modu čte iniciátor data z NFC tagu, ve kterém jsou již uložena požadovaná data. Kromě dat se tag skládá také z programu, který je odesílá zpět iniciátorovi. V modu pro zápis funguje NFC zařízení (mobilní telefon) jako iniciátor a zapisuje data do tagu. Pokud tag již předtím obsahuje nějaká data, tak tyto data budou přepsána. Některé algoritmy mohou být navrženy i tak, že se již existující data budou pouze aktualizovat – doplňovat. [24]

Aplikace:

V reálné aplikaci tohoto režimu zaujímá dominantní postavení pojem Smart Poster (inteligentní plakát). Tento termín se vztahuje k reklamním materiálům nebo plakátům, kterým jsou vybaveny NFC tagy. Tyto tagy mohou obsahovat různé typy dat, jako jsou například URL adresy, kupóny, SMS službu atd. Dalšími odvětvími pro aplikaci režimu čtení/zápis je tzv. Remote Marketing and Shopping (vzdálený marketing a nakupování) nebo také použití v sociálních sítích, sdílení polohy a informací o místech.

2.1.2 Peer-to-Peer (P2P)

Režim P2P umožňuje dvěma NFC zařízením výměnu informací, jako je například záznam kontaktu, textové zprávy či obrázku. Má dvě standardizované možnosti, NFCIP-1 a LLCP. První zmíněný využívá modelu iniciátor-cíl jehož zařízení jsou definovány před spuštěním komunikace. Nicméně tato zařízení jsou identická i pro LLCP komunikaci. Po inicializačním handshaku je pomocí aplikace, která běží v aplikační vrstvě, provedeno rozhodnutí. V tomto režimu jsou obě zařízení během komunikace aktivní a to na základě energie dodávané z mobilního telefonu. Data jsou odesílána v obousměrném polo-duplexním kanálu, což znamená, že pokud jedno zařízení právě vysílá, druhé musí jenom naslouchat a mělo by začít přenášet data až poté, co první přenos dokončí. Komunikace probíhá s maximální přenosovou rychlostí dosahující 424 kbit/s.

Aplikace:

Výměna dat - v mobilním zařízení mohou být bezpečně uloženy citlivé informace, které mohou být vyměňovány s jinými autorizovanými lidmi, právě za použití režimu P2P. Vzhledem k faktu, že komunikace probíhá na vzdálenost pouze několika centimetrů, se uživatelé s použitím NFC budou při sdílení soukromých a důležitých dat cítit bezpečněji. Pokud ale bude kladen důraz na vyšší úroveň bezpečnosti, bude potřeba poskytnout další bezpečnostní opatření.

Převod peněz – Dva uživatelé si mohou vyměňovat peníze mezi peněženkami, které jsou uloženy v jejich mobilních NFC zařízeních. Dárky, kupóny a vstupenky mohou být stejně tak realizovány jako výměnné objekty.

Počet aplikací vyvinutých pro použití P2P modu je zatím menší než u ostatních režimů. Hlavní uplatnění nalézá pro párování zařízení, sítí a přenos souborů. Jako možné implementace tohoto režimu lze vyjmenovat párování Bluetooth zařízení, výměnu vizitek, poznávání nových přátel na sociálních sítích atd. Jako příklad uveďme dva obchodní partnery, kteří si navzájem vymění vizitky/kontakty tím, že k sobě přiloží svoje mobilní telefony. Další populární využití je pro předání připojení jiné standardní technologii. NFC připojení lze použít k nastavení Bluetooth párování nebo Wi-Fi. [24]

2.1.3 Card emulation

Režim card emulation umožňuje mobilním telefonům (nebo jiným NFC zařízením) fungovat jako bezkontaktní čipová karta. Mobilní zařízení v sobě může dokonce uchovávat

více aplikací bezkontaktních karet. Mobilní telefon se v tomto případě chová jako pasivní NFC čip standardu ISO/IEC 14443. Jakmile dojde ke kontaktu s NFC čtečkou s tímto čipem v telefonu, tak NFC čtečka zahájí komunikaci. Hlavními příklady emulovaných bezkontaktních čipových karet jsou kreditní karty, debetní karty, věrnostní karty, dále pak karty dopravní, přístupové a různé průkazy. Režim emulace karty pouze odstraňuje nutnost mít a nosit kartu stále u sebe. Po většinu času u sebe lidé stejně nosí mobilní telefony, což je pro NFC technologii značné plus. [24] Dá se očekávat, že v blízké budoucnosti budou lidé nosit u sebe zapnutý mobilní telefon s NFC nejen pro jeho klasické funkce (telefonování, SMS, e-maily atd.), ale také pro vykonávání každodenních funkcí. Všechny platební karty, klíče, lístky atd. bude možné vložit do mobilních telefonů. Proto bude existovat více příležitostí k integraci každodenních úkolů pouze do jednoho NFC podporujícího zařízení.

V tomto provozním režimu zapnuté NFC zařízení negeneruje své vlastní radiové pole, ale NFC čtečka ho vytváří za něj. V současné době podporovanými komunikačními rozhraními jsou IEC 14443 typu A, typu B a FeliCa. Tento režim se stává hojně využívaným, neboť umožňuje placení a je v souladu se stávající infrastrukturou čipových karet. [3]

Aplikace:

Platby – Existují různé typy platebních NFC aplikací. Není pochyb o tom, že nejdůležitější a nejvýraznější platebními aplikacemi jsou kreditní a debetní karty, jejichž aktivace a použití může být spuštěno NFC čtečkou. Existují i jiné možnosti pro NFC platby, jako je ukládání a používání poukázek, dárkových karet, balíčků atd.

Věrnostní programy – věrnostní body lze získat na různých platebních místech a později mohou být použity k opětovnému nákupu nebo k získání jakéhosi bonusu např. v podobě dárku. Také kupóny a vouchery, které jsou stažené prostřednictvím inteligentních plakátů za použití již zmiňovaného režimu čtení/zápis mohou být dále využívány tímto pracovním režimem.

Jízdenky – Příklady použití jízdenek a tiketů mohou být implementovány v mnoha formách. Uživatel může uchovávat různé druhy lístků, tiketů, jízdenek jako například lístek do divadla nebo do kina. Jízdenku do autobusu, vlaku či dokonce letenku. Tyto lístky potom mohou být použity u vstupních bran, turniketů, v MHD apod. Samozřejmě se pro tento typ/režim NFC zařízení nachází velmi široké uplatnění v každodenním životě.

Kontrola přístupu – Aplikace pro kontrolu a přístup umožňuje uživatelům NFC zařízeních uchovávat jejich údaje k přístupům právě v těchto NFC zařízeních (mobilních telefonech). Jako příklad použití lze zmínit elektronické klíčenky, ať už od domu nebo od automobilů, zabezpečených objektů či hotelových pokojů. Zajímavým příkladem může být přijetí hosta do hotelu. Host si může hotel objednat předem a bude mu zaslán elektronický klíč, tudíž nemusí ztrácet čas zapisováním se a trávením času na hotelové recepci a může přejít rovnou do svého předem objednaného pokoje, který si otevře pomocí svého mobilního telefonu podporující NFC technologii. [24]

2.2 NDEF

Výměna dat mezi NFC zařízeními a tagy je formována za použitím tzv. NDEF (NFC Data Exchange Format). Jedná se o jedno z klíčových vylepšení, které NFC přidává klasickému RFID. NDEF je standardizovaná specifikace formátu dat prostřednictvím organizace NFC Forum, který se používá k popsání, jakým způsobem se bude kódovat do NFC tagu, nebo jak má být provedena výměna data mezi dvěma aktivními NFC zařízeními. Drtivá většina NFC mobilních zařízeních (čtečky, telefony, tablety atd.), podporuje čtení NDEF zpráv z NFC tagů. Všechny typy činností NDEF mohou být zakódovány na všech typech NFC čipů a NFC čteček. Nicméně z důvodu požadavků na velikost dat a omezení paměti NFC čipu je nejlepší zvolit NFC čip, který bude znát typ dat, které se budou kódovat. Na základní úrovni obsahuje NDEF záznam dvě složky. První složkou jsou použitá data a druhou složkou je typ záznamu, který slouží k roztřízení právě použitých dat. Dohromady tyto dvě složky představují souhrn akcí a opatření, která mají být přijata zařízením, pokud se zaktivuje NFC tag. NDEF podporuje poměrně omezenou sadu akcí. Složitější akce mohou být prováděny pomocí specializovaného softwaru. Výhodou použití NDEF je, že tento software nemusí být přímou součástí zařízení. Všechny NDEF zprávy obsahují jeden nebo více záznamů. Každý záznam je určitého typu, unikátního identifikátoru, délky a dat. Existuje několik typů NDEF záznamů. Lze kombinovat i více záznamů najednou. [28]

Textový záznam – tento typ obsahuje jakýkoliv textový řetězec znaků, který chcete poslat. Textová zpráva obvykle neobsahuje instrukce pro cílové zařízení. Zprávy také obsahují metadata indukující jazyk a kódování (UTF-8 atd.).

Síťové adresy – tento typ obsahuje síťové adresy. Cílové NDEF zařízení, které obdrží záznam s odkazem, očekává předání tohoto záznamu aplikaci, která tento záznam dokáže zobrazit. Většinou se jedná o webový prohlížeč.

Smart Posters – typ obsahující data, které se dají připojit k plakátu a slouží pro zobrazení více informací. Může obsahovat jak odkazy, tak další data jako jsou například textové zprávy. Cílové zařízení, které obdrží smart poster záznam může otevřít webový prohlížeč, SMS nebo e-mail aplikaci a přeposlat ji dále. Záleží na obsahu záznamu.

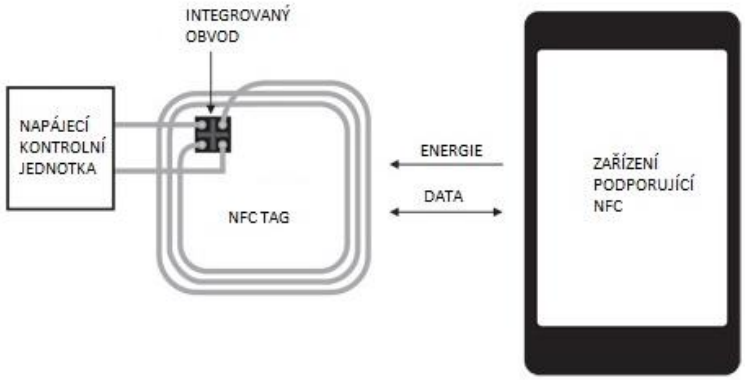
Podpisy – typ záznamu, který nám dává důvěryhodnou informaci o původu dat.

2.3 NFC tagy

NFC tagy obsahují data a jsou typicky pouze pro čtení, ale existují i přepisovatelné. Jejich výrobci je mohou šifrovat nebo používat specifikace poskytnuté organizací NFC Forum. Tagy mohou být bezpečným úložištěm soukromých dat. Jako jsou například PIN kódy, kontakty, informace o debetních a kreditních kartách a další typy soukromých a důvěrných dat. Jsou definovány 4 typy tagů s různými schopnostmi, přenosovými rychlostmi, velikostí pamětí, bezpečností atd. Níže uvedená tabulka uvádí obecný přehled jednotlivých typů tagů. [10]

	Typ 1	**Typ 2**	**Typ 3**	**Typ 4**
Standard	ISO/IEC 14443 Typ A	ISO/IEC 14443 Typ A	FeliCa	ISO/IEC 14443 Typ A, Typ B
Název čipu	Topaz	MIFARE	FeliCa	DESFire, SmartMX-JCOP
Přenosová rychlost	106 kbit/s	106 kbit/s	212 kbit/s	424 kbit/s
Paměť	do 1 kB	do 2 kB	do 1 MB	do 64 kB
Zabezpečení	16 nebo 32bitový digitální podpis	Nezabezpečeno	16 nebo 32bitový digitální podpis	Volitelně
Cena	Nízká	Nízká	Vysoká	Průměrná až vysoká
Užití	Jednoúčelové tagy	Jednoúčelové tagy	Flexibilní tagy s širokými možnostmi užití	Flexibilní tagy s širokými možnostmi užití

Tabulka 4 - Porovnání vlastností NFC tagů [10]



Obrázek 13 - Popis NFC tagu [13]

2.4 NFC vs. čárové kódy

NFC tag a reprezentant čárových kódů QR kód plní v podstatě stejnou funkci a to, že skladují malé množství informací, například webovou adresu (URL) nebo ID. Avšak tuto funkci oba dva provádějí velmi odlišnými způsoby. [26] Čárové kódy a QR kódy jsou používány zejména pro skladové účely již od 70. let 20. století. Jedná se o univerzální prostředek pro řízení zásob a v dnešní době jsou všudypřítomné a univerzální.

Uživatelská zkušenost: U mobilních telefonů vybavených technologií NFC je použití NFC velmi jednoduchou záležitostí. Stačí si telefon takřka jen vybalit z krabice, zapnout, a pokud máte zapnutou i funkci NFC, tak jednoduše přiložíte svůj telefon k NFC tagu a stisknutím obrazovky/displeje telefonu se Vám automaticky spustí příkaz z NFC tagu. U QR kódů mobilní telefony vyžadují instalaci aplikace, aby mohli s QR kódy pracovat. Abyste mohli naskenovat QR kódu, musíte první spustit aplikaci a potom nasměrovat vaši kameru tak, aby byla schopná přečíst QR kód. [27]

Cena: Pokud se zaměříme na cenovou relaci u těchto dvou technologií, tak ta hovoří v prospěch právě QR kódů. Jelikož NFC tagy jsou nyní k dispozici zhruba za 0,30 $/ks a to jen při objednávce 1000 kusů. QR kódy stojí pouze to, co stojí tisk a proto pokud máme tiskárnu, tak nás nemusí skoro vůbec nic. [27]

Velikost: Z hlediska velikosti se NFC tagy pohybují typicky v rozmezí 1 až 2 centimetry a jsou velmi úzké zhruba 0,015 milimetrů. Na druhou stranu u QR musíme zajistit správné, bezchybné naskenování a přečtení, proto musí být větší jak 2 x 2 cm. [27]

Integrace produktů: NFC tagy lze tak jako RFID tagy skenovat bez přímé viditelnosti a tak mohou být integrovány v produktech viditelně nebo i neviditelně. Oproti tomu QR kódy, stejně tak jako obyčejné čárové kódy musí být vytištěné na každý produkt zvlášť a u skenování je nutná přímá viditelnost kódu. [27]

Tisk a přizpůsobení: Na NFC tagy je možné natisknout cokoliv jakoukoliv barvou a to jim dává právě tu vlastnost, že mohou být skryté jak na tištěných médiích, tak v produktech. Jak již bylo zmíněno, tak QR kódy musí být viditelné, aby byla zachována jejich výkonnost, a to znamená, že je zde velmi malá možnost úprav při tisku a na produktech. [27]

Dostupnost v mobilních telefonech: Od května 2013 je NFC k dispozici ve všech mobilních telefonech od 9 z 10 hlavních světových výrobců. Odhaduje se masové rozšíření této technologie do všech mobilních telefonů. QR kódy mohou být použity na všech existujících chytrých telefonech, samozřejmě stěžejním prvkem je kamera. [27]

Programování: NFC tagy jsou snadno kódovatelné za použití mobilních aplikací, které jsou k dispozici pro telefony podporující tuto technologii. Tyto tagy lze také přepisovat. QR kódy lze tvořit i programovat zdarma, klidně online. Existuje na to široký rozsah webových stránek. [27]

Bezpečnost: QR ani čárové kódy nám nenabízí žádnou možnost zabezpečení, oproti tomu NFC tagy mají fixní výrobní ID a některé specializované tagy mohou podporovat šifrování a tím skrývají data, která jsou v tagu uložena. [27]

2.5 NFC vs. Bluetooth

NFC a Bluetooth jsou rádiové technologie krátkého dosahu. Podle technických detailů, které jsou uvedeny níže, NFC operuje na nižších přenosových rychlostech. Ovšem jednoznačnou výhodou NFC oproti Bluetooth je ta, že ke svému provozu potřebuje výrazně méně energie a odpadá zde nutnost zdlouhavého párování zařízení. [10]

Ve srovnání se standardním Bluetooth je konfigurace NFC je výrazně rychlejší. Spojení je mezi dvěma zařízeními provedeno automaticky (méně než 1 sekunda), nikoliv manuální konfigurací. Maximální přenosové rychlosti NFC (424 kbit/s) jsou nižší, než u standardu Bluetooth V2.1 (2.1 Mbit/s). Za jeden z bezpečnostních prvků lze považovat maximální dosah u technologie NFC, který je menší než 10 cm. Výrazně tak snižuje

možnosti zachytávání provozu okolními zařízeními. Ve srovnání s Bluetooth, je NFC kompatibilní s existující pasivní RFID infrastrukturou (13.56 MHz, ISO/IEC 18000-3). [10]

Pro snadné porovnání technologií NFC a Bluetooth byla vytvořena následující tabulka.

	NFC	BT v2.1	BT v4.0
Kompatibilita s pasivním RFID	Ano (ISO 18000-3)	Ne (pouze aktivně)	Ne (pouze aktivně)
Tvůrce standardu	ISO/IEC	Bluetooth SIG	Bluetooth SIG
Norma	ISO 13157	IEEE 802.15.1	IEEE 802.15.1
Typ sítě	P2P	WPAN	WPAN
Kryptografie	ne s RFID	Možná	Možná
Dosah	< 0,2 m	~10 m (třída 2)	~100 m (třída 3)
Frekvence	13,56 MHz	2,4-2,5 GHz	2,4-2,5 GHz
Rychlost přenosu	424 kbit/s	2,1 Mbit/s	~200 kbit/s
Čas pro sestavení přenosu	< 0,1 s	< 6 s	< 1 s
Spotřeba energie	< 15 mA	Závislé na třídě	< 15 mA

Tabulka 5 - NFC vs. Bluetooth [10]

2.6 Použití, využití NFC

Přestože je NFC poměrně mladá technologie, její využitelnost prakticky den ode dne stoupá a její potenciál do budoucna je obrovský a jak se říká – naprogramovat se dá v zásadě všechno.

Velmi praktické a zřejmě nejdiskutovanější využití NFC je tzv. peněženka v telefonu. Mezi nejpoužívanější aplikace v tomto směru patří Google Wallet a O2 Wallet. Ty vám umožní správu platebních karet včetně uživatelské agendy a to přímo ve vašem telefonu. [4] Velmi diskutovaným tématem je samozřejmě bezpečnost plateb pomocí mobilního telefonu. Ta je zajištěna 4místným PIN kódem, který je nutný při každém spuštění platební aplikace. U plateb nad 500 Kč je navíc potřeba zadání autorizačního Pass Code. [5]

Obrázek 14 - NFC platba [5]

Se zaplaceným účtem v obchodě potenciál NFC rozhodně nekončí. V současné době už se dá NFC využívat jako jízdenka MHD, průkaz do knihovny či stravovací průkaz. Díky této technologie je uživatel schopný mít všechny tyto průkazy, jízdenky a kupóny na jednom místě a to ve svém mobilním telefonu a pomocí NFC je využívat a uplatňovat. [3] [5]

NFC může nahradit všechny klíče, ať už ty fyzické, tak i ty virtuální. Od auta, garáže, domu, ale třeba i pro přihlášení k počítači. A teď situace ze života: Potřebujete někomu něco nechat v autě. Bez klíčů se do něj ale nedostane, a když mu klíče půjčíte, může si odvézt rovnou celé auto. Díky NFC ale pošlete klíč jen s omezenou platností, který dovolí nanejvýš na pět minut otevřít kufr, ale nedovolí nastartovat. A pak z telefonu nenávratně zmizí. [5]

Otevírání domovních (a jiných) dveří je možné již dnes. Vše co k tomu potřebujete je zabezpečovací systém a aplikaci pro jeho správu, která bude tuto technologii podporovat. Odpadá tak nutnost nošení různých klíčů, přístupových karet, čipů či zadávání přístupových kódů. [5]

Další případy možného užití NFC

- Vzájemná konfigurace Bluetooth a Wi-Fi zařízení
- Přístup do bezdrátové počítačové sítě zabezpečené technologií WPS
- Bezdrátové příslušenství bez nutnosti dobíjení
- Elektronický klíč, například k vašemu PC
- Občanský průkaz, řidičský průkaz, pas
- Klíčky od vozu a jiných dopravních prostředků
- Elektronické vizitky
- Zvířecí známky

Obrázek 15 - NFC psí známka [2]

Jak již bylo mnohokrát avizováno, budoucnost NFC se jeví jako velmi slibná. Obrovský potenciál umožňující nahradit velké množství věcí z našeho života a integrovat je do jednoho místa je velice lákavá vize. Toho jsou si vědomi také přední světoví výrobci elektroniky a tak se s touto technologií setkáváme čím dál častěji.

Obrázek 16 - Použití NFC [14]

2.7 Bezpečnost

Ačkoliv může být krátký dosah NFC technologie brán jako jeden z bezpečnostních aspektů, tak NFC samotné komunikaci nezabezpečuje.

Aplikace využívající NFC proto musí použít kryptografické protokoly vyšších vrstev (např. SSL) k vytvoření zabezpečeného kanálu. Zajištění bezpečnosti přenášených dat skrze NFC proto vyžaduje spolupráci na více úrovních: [10]

- Výrobci hardware, kteří budou chtít zabezpečit NFC zařízení silnou kryptografií a autentizačními protokoly
- Zákazníci, kteří budou chtít zabezpečit jejich zařízení a data různými typy zámků, hesly či antiviry
- Výrobci softwaru a subjekty poskytující bezkontaktní transakce, kteří budou chtít zabezpečit své systémy proti spywaru a malwaru před nákazou systémů.

2.7.1 Typy útoků

Odposlech – Stejně jako u RFID lze pomocí antén odposlechnout rádio-frekvenční signál vysílaný zařízeními. U pasivních NFC zařízení je odposlech ztížen malou komunikační vzdáleností. Naopak u aktivních zařízení lze odposlech realizovat i ze vzdálenosti pár metrů. [10]

Modifikace dat - Je relativně jednoduché narušovat přenášená data pomocí RFID rušičky. Neexistuje zatím žádná možnost, jak zabránit takovému typu útoku. Detekce takového útoku je ale možná, jelikož NFC zařízení během přenosu kontrolují své okolní elektromagnetické pole. Výrazně složitější je pak útok, u kterého by se zdála komunikace jako nenarušená. [10]

Přepojovaný útok – Tento typ útoku je podobný útoku Man-in-the-Middle. Útočník musí přeposílat požadavky čtečky k oběti a poté vracet tyto odpovědi v reálném čase zpět, aby mohl úspěšně předstírat, že je čipová Smart karta oběti. Přepojované útoky jsou možné i na NFC zařízeních, jelikož tato technologie zahrnuje protokoly ISO/IEC 14443, které jsou na tyto útoky náchylné. [10]

Ztráta majetku - Ztráta telefonu, který používá NFC služby umožní nálezci pracovat s telefonem obvykle jako s jedno-faktorovou autentizační entitou. Mobilní telefony chráněné PIN kódem jsou zařízení s jedno-faktorovou autentizací. Proto možností, jak nálezci zneužití zabránit, je použít další typ autentizace, nejenom PIN kód v telefonu. [10]

Přerušení spojení - Otevřené spojení k zabezpečeným funkcím NFC nebo jejich datům, je chráněno intervalem, jehož kanál se uzavírá tehdy, jestliže na něm není aktivita. Útoky však mohou nastat v případech, kdy zařízení, opouštějící kanál, jej neuzavře a tak potenciální útočník může navázat z původního umístění zařízení. Další autentizační faktor by takovým případům mohl zabránit. [10]

II. PRAKTICKÁ ČÁST

3 MĚŘENÍ

Měření praktické části této práce proběhlo v laboratoři elektromagnetické kompatibility na fakultě aplikované informatiky ve Zlíně. V rámci praktické části bylo změřeno spektrum a intenzita elektromagnetického pole vyzařovaného vzorkem RFID čtečky, která mi byla poskytnuta na fakultě. K samotnému měření jsem využil několik přístrojů, jejichž seznam uvádím níže.

3.1 Měření v elektromagnetických stíněných prostorech

„Elektromagnetická kompatibilita (EMC) je definována jako schopnost zařízení, systému či přístroje vykazovat správnou činnost i v prostředí, v němž působí jiné zdroje elektromagnetických signálů (přírodní či umělé), a naopak svou vlastní elektromagnetickou činností nepřípustně neovlivňovat své okolí, tj. Nevyzařovat signály, jež by byly rušivé pro jiná zařízení.“ [34]

Jedním z největších problémů při měření na otevřeném prostranství je nežádoucí přítomnost vnějších rušivých elektromagnetických polí. Signály blízkých rozhlasových a televizních vysílačů a převaděčů, radiolokátorů, mnoha různých radiokomunikačních služeb včetně mobilních telefonů a pagerů mohou v místě zkušebního stanoviště vyvolat nepřípustně vysoké intenzity pole, které nejen že nejsou hluboko pod úrovní měřeného vyzařování zkoušeného objektu, ale mohou je dokonce úplně překrýt a tím měření na některých kmitočtech zcela znemožnit. Tento stav je přitom s rostoucí hustotou radiokomunikačních a telekomunikačních služeb stále častější. Aby měřicí anténa nepřijímala vnější rušivé signály, to jest, aby přijímala jen rušivé signály pocházející od zkoušeného zařízení, doporučuje se tato měření provádět v tzv. elektromagneticky stíněných prostorách (komorách). Stíněná komora je vytvořena jako uzavřený prostor nejčastěji z desek ocelových plechů, který zajišťuje dostatečnou elektromagnetickou těsnost, a to včetně dveří, větracích a přívodních otvorů apod. Kvalitní stíněná komora musí zajišťovat útlum pro vnější signály na úrovni 100 – 120 dB. Na konstrukci kvalitní stíněné komory pro měření rušivých signálů jsou kladeny i další požadavky. Komora musí především mít dostatečně velké rozměry, které v ní umožní realizovat zkušební stanoviště s půdorysným eliptickým tvarem. Rovněž výška stíněné komory musí umožňovat nastavitelnost měřicích antén až do úrovně 4 m. Profesionální stíněné komory EMC pro anténní měření tak svými obvyklými rozměry např. 20 x 10 x 10 m i většími jsou spíše

stíněnými halami. Jen v takto rozměrných stíněných halách lze však realizovat nezkreslená a reprodukovatelná anténní měření rušivého vyzařování.

Absorpční materiály, z nichž je vytvářeno obložení stěn bezodrazových komor, přeměňují energii dopadající elektromagnetické vlny na teplo, a to s využitím buď dielektrických, nebo magnetických ztrát. V současné době se většinou dává přednost dielektrickým ztrátovým materiálům, neboť magnetické materiály jsou příliš těžké a také drahé. Hodnoty relativní permitivity ε_r by měly být nízké, aby se svými dielektrickými vlastnostmi co nejvíce blížily vlastnostem vzduchu (volného prostoru). Používají se proto zejména různé tvrzené pěnové materiály z polystyrénu, polypropylénu či polyuretanu, které se sytí elektrovodivými či grafitovými plnidly různé hustoty. Stupněm tohoto sycení lze tak účinně regulovat zejména ztrátové parametry výsledného materiálu. Kromě elektricky vhodných vlastností jsou dalšími výhodami těchto materiálů jejich nízká hmotnost, snadná mechanická opracovatelnost a snadné spojování lepením. Vhodnou technologií sycení lze přitom dosáhnout vysokou homogennost a reprodukovatelnost vlastností výsledného materiálu. Materiály lze obvykle použít do poměrně vysokých teplot (90 až 160 °C), a tím pro pohlcování vysokých intenzit elektrického pole (až 200 V/m), případně vysokých hustot výkonu (až 100 W/m^2). Materiály jsou většinou nevznětlivé, tj. v případě požáru jen doutnají, ale nehoří plamenem.

V současné době nejrozšířenější způsob realizace absorpčních obkladů je pomocí prvků, které mají tvar jehlanu či kužele zhotovených opět z polystyrenu či polyuretanu s grafitovou impregnací. Lineárně se rozšiřující průřez jednotlivých jehlanů realizuje impedanční transformátor, který bezodrazově převádí impedanci volného prostoru na hrotech jehlanů na velmi nízkou impedanci prostoru zcela zaplněného absorbérem v zadní části jehlanu. Stejně tak se postupně zvyšují ztráty absorpčního obkladu, takže maximální pohlcení energie dopadající vlny nastává až v zadní části absorbéru. Bezodrazovost vstupu celého absorpčního obkladu se někdy dále zlepšuje tím, že hroty jehlanů mají menší sycení grafitem (a tedy menší ztráty) než jejich zadní široké části. Délka transformační části absorbéru (výška jehlanu) musí být minimálně *λ/4* na nejnižším pracovním kmitočtu. Pro nejnižší kmitočet měřených signálů EMI 30 MHz by tento požadavek znamenal délku 2,5 m, pro minimální kmitočet 100 MHz je teoretická potřebná výška jehlanu 75 cm. Tyto rozměry však současně znamenají, že na vysokých kmitočtech (např. 1000 MHz) činí výška celého absorbéru již několikanásobek vlnové délky λ a bezodrazovost takového absorpčního obkladu na vysokých kmitočtech je tak velmi dokonalá.

Pyramidální konstrukce absorbéru s sebou přináší ještě další výhodnou vlastnost. Jelikož vlna dopadající na plochu absorpčního obkladu vstupuje mezi jednotlivé absorpční jehlany a je na jejich povrchu částečně odrážena. Vlivem zkosení jehlanů se však tyto odražené vlny nevracejí přímo zpět do prostoru, ale směřují do sousedního jehlanu. Zde se opět částečně odrazí a celý děj se opakuje. Odražená vlna se tedy vrací zpět do vnitřního prostoru komory až po několika částečných odrazech od absorpčních jehlanů. Protože při každém odrazu se část energie vlny absorbuje a jen část se odrazí, je celková energie odražené vlny po vícenásobném odrazu výrazně menší. Počet dílčích odrazů přitom závisí zejména na vrcholovém úhlu jehlanů, který se u praktických konstrukcí pohybuje kolem 25°. Tímto mechanismem se tak dále zlepšují bezodrazové vlastnosti celého absorbéru.

Bezodrazové absorpční komory představují v současné technice EMC téměř ideální měřicí a testovací prostor. Ve své konstrukci obvykle kombinují pyramidální a ploché absorbéry, když se na několikavrstvý plochý absorbér umisťují absorpční jehlany. Absorpční haly se realizují jako částečně nebo plně bezodrazové. Částečně bezodrazová hala nebo komora (Semi-anechoic Room) je taková, v níž jsou absorpčním materiálem obloženy všechny stěny a strop, nikoli však podlaha. Hala tak simuluje volné měřicí prostranství včetně odrazů od zemní roviny. V plně bezodrazové hale – komoře (Anechoic Room) jsou absorpčním materiálem obloženy všechny stěny, strop i podlaha a hala simuluje volný neomezený prostor. Konstrukce kvalitní bezodrazové haly je technologicky velmi náročná. Jejím základem je realizace perfektního elektromagneticky stíněného prostoru včetně dokonalého ošetření všech možných vstupů a výstupů elektromagnetického rušení. Na tuto kovovou konstrukci jsou pak upevňovány absorpční obklady o příslušných rozměrech pro požadované kmitočtové pásmo měření. Absorpčními materiály jsou samozřejmě obloženy rovněž všechny dveře a další větrací či jiné průchody a otvory. Pro obložení podlahy v plně bezodrazové hale se buď využívají jenom ploché, mechanicky zpevněné absorbéry (často na bázi feritových materiálů), nebo je nutno pyramidální absorbéry na podlaze vyztužit či překlenout laminátovými můstky, které lze v některých případech po instalaci měřicího zařízení před vlastním měřením z haly odstranit. Základní praktickou nevýhodou bezodrazových komor jakožto ideálního měřicího prostoru je jejich velmi vysoká cena daná zejména pořizovací cenou absorpčních obkladů. Cena 1 m^2 širokopásmového pyramidálního obkladového absorpčního materiálu totiž činí 30 – 350 $, záleží na velikosti jehlanů. Dalším problémem při stavbě absorpčních komor je jejich velký potřebný objem ve srovnání s objemem pouhých

stíněných komor či volných prostranství. To je dáno především potřebnou výškou absorpčních jehlanů pro požadované kmitočtové pásmo měření v komoře.

Ve stíněných bezodrazových komorách je žádoucí provádět nejen anténní měření rušivých elektromagnetických polí, ale i všechny ostatní způsoby měření rušivých signálů – napětí, proudů či výkonů. [34]

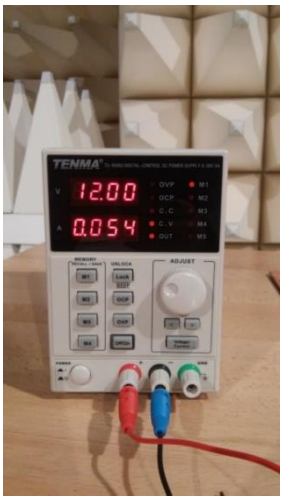
Obrázek 17 - Semi-anechoická komora UTB

3.2 Použité přístroje

Zdroj napětí

Typ: TENMA 72-10480

Specifikace: Rozsah napětí (0-30 V), rozsah proudu (0-3 A), digitální, rozlišení (10 mV/1 mA), nízko-šumový, CV/CC režim konstantní napětí a proudu, OCP (ochrana proti přetížení) a OVP (ochrana proti přepětí) režim konstantní ochrany, funkce vypnutí paměti, funkce zámku klávesnice



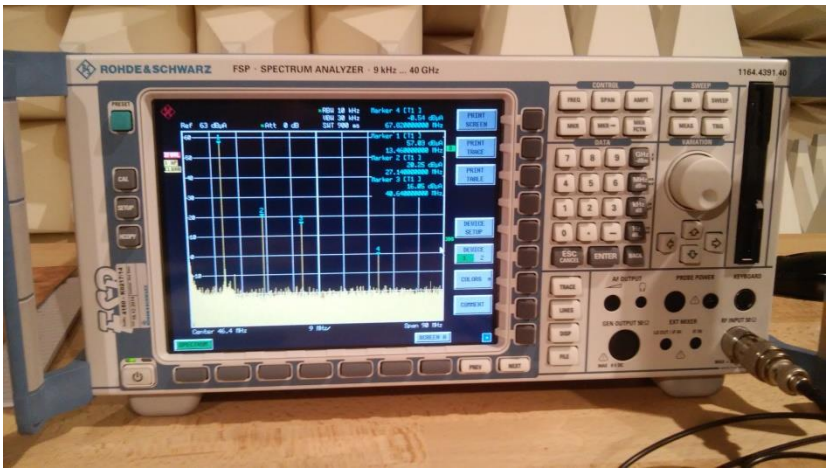
Obrázek 18 - Připojený zdroj napětí

Spektrální analyzátor:

K měření elektromagnetické interference se v posledních letech více a více používá typ přístroje, zvaný spektrální analyzátor. Jeho základní předností je rychlé vizuální zobrazení měřeného rušivého spektra na displeji a tím získání celkového přehledu o elektromagnetickém rušení v daném kmitočtovém pásmu. Kvalitní spektrální analyzátory pro měření elektromagnetické interference však musí také splňovat všechny hlavní požadavky normy ČSN CISPR 16-1 kladené na měřicí přijímače, zejména šířku propustného pásma, vstupní impedanci, impulzní odezvu, selektivitu, účinnost stínění a další. Jelikož spektrální analyzátory jsou většinou širokopásmové, to znamená, že nejsou vybaveny vstupním preselektromer, tak jako měřicí přijímače, nedosahují zdaleka tak velkého dynamického rozsahu měření. Také jejich citlivost je běžně nižší než citlivost u měřicích přijímačů. Tím dochází ke zkreslení až znehodnocení výsledků měření zejména impulzního rušení. Přední světoví výrobci elektronické měřicí techniky se v poslední době snaží kombinovat výhodné vlastnosti jak měřicích přijímačů, tak spektrálních analyzátorů. Tím pádem vznikají vysoce kvalitní měřicí přijímače s rozmítáním kmitočtu a přesným zobrazením celého kmitočtového spektra, nebo naopak spektrální analyzátory vybavené vstupním vysokofrekvenčním preselektorem schopné pracovat na diskrétních kmitočtech s vlastnostmi plnohodnotného měřicího přijímače. Uvedené přístroje tak představují špičku současné širokopásmové vysokofrekvenční měřicí techniky, navíc plně využívají možností číslicového zpracování a počítačové analýzy, archivace a zpracování měřených dat.

Přístroj: Rohde & Schwarz FSP

Parametry: Frekvenční rozsah (9 kHz – 40 GHz), rozlišení frekvence (0,01 Hz), maximální odchylka (0,1%), 8,4“ barevný displej s rozlišením 640 x 480 pixelů.

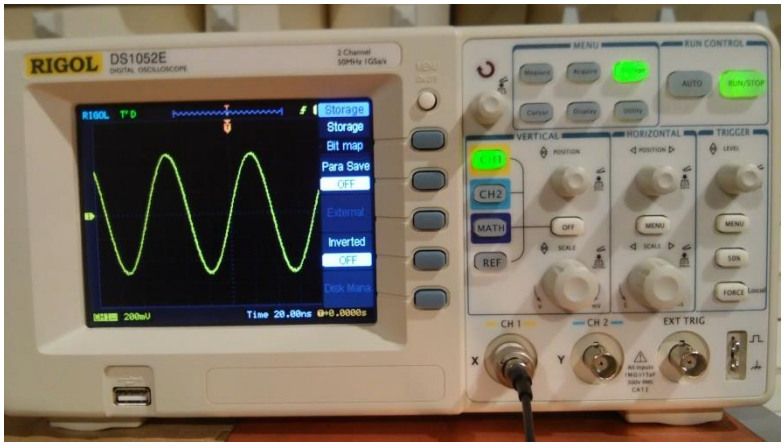


Obrázek 19 - Spektrální analyzátor

Osciloskop

Přístroj: RIGOL DS1052E

Parametry: Duální analogové kanály, maximální šířka pásma 100MHz, maximální vzorkovací frekvence v reálném čase 1GSa/s, 5,6“ LCD displej,



Obrázek 20 - Osciloskop

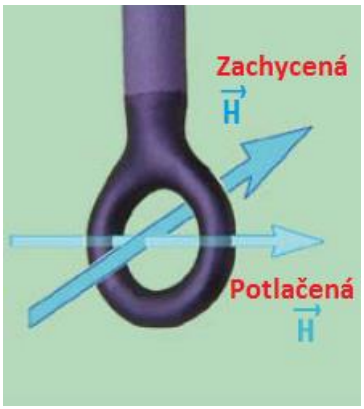
Sonda

Přístroj: RS H-50-1

Parametry: Smyčka o průměru 1cm, frekvenční rozsah 10-3000 MHz.

Obrázek 21 - Měřící sonda RS H-50-1

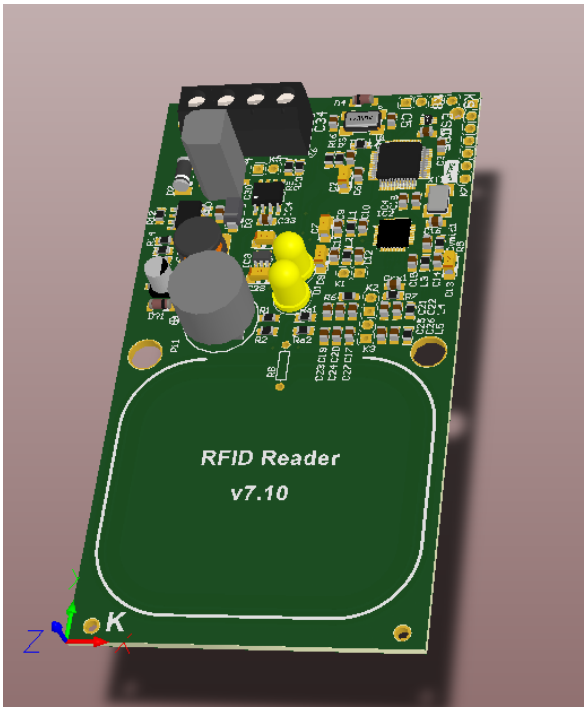
Tuto sondu lze snadno použít pro měření blízkého elektromagnetického pole, a je ideální pro měření vysokých frekvencí do 2,5 GHz. Sonda H50-1 je určena pro měření H parametru. Může být použita k rychlé identifikaci potenciálních zdrojů vyzařování nebo prováděných emisí.



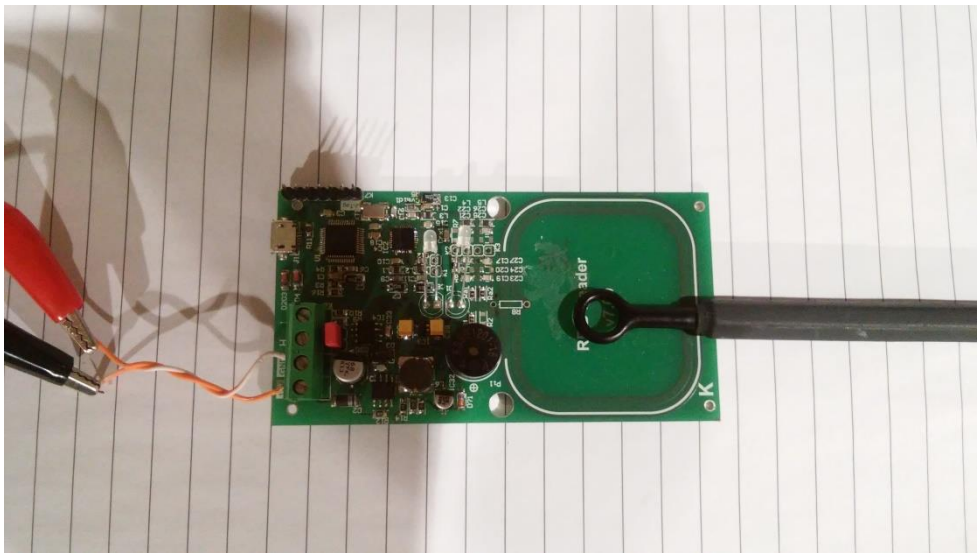
Obrázek 22 - zachycení/potlačení intenzity EM pole sondou

RFID čtečka

Tato čtečka byla vyvinuta v rámci smluvního výzkumu v embedded laboratoři na FAI. Co se obsahu týče, tak celá čtečka je řízena mikropočítačem STM32F303CB. Srdcem RFID části je čip MFRC523 od výrobce NXP, a anténa vycházela z referenčních designů dostupných k tomuto čipu. Celá čtečka je napájená spínaným zdrojem na bázi MC34063, který vstupní napětí transformuje na 5V, které se následně lineárním stabilizátorem převádí na 3V3. Dvojí napájení je nutné z důvodů CAN trancieveru. Čtečka je schopná komunikovat pomocí CAN sběrnice a využívá vlastního zabezpečeného protokolu. Poslední verze čtečky obsahuje i USB rozhraní.



Obrázek 23 - Vizualizace měřené čtečky



Obrázek 24 - RFID čtečka

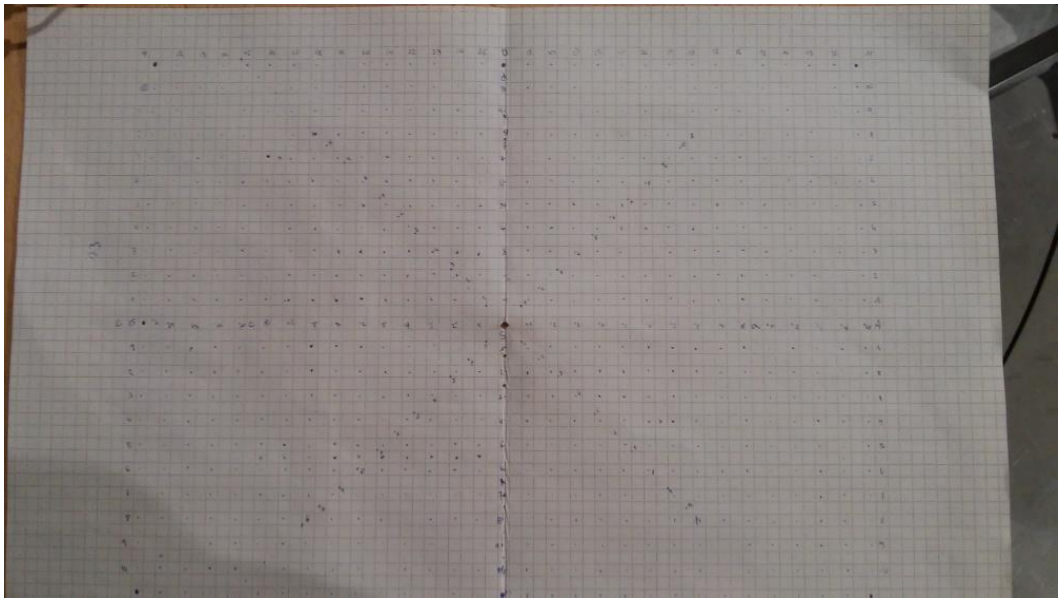
Povrchy

Druhá část měření probíhala se stejnou RFID čtečkou, jenom s tím rozdílem, že čtečka byla umístěna na kovovou podložku, která je zobrazena na obrázku č. 25.

Obrázek 25 - Kovový plech

3.3 Popis měření

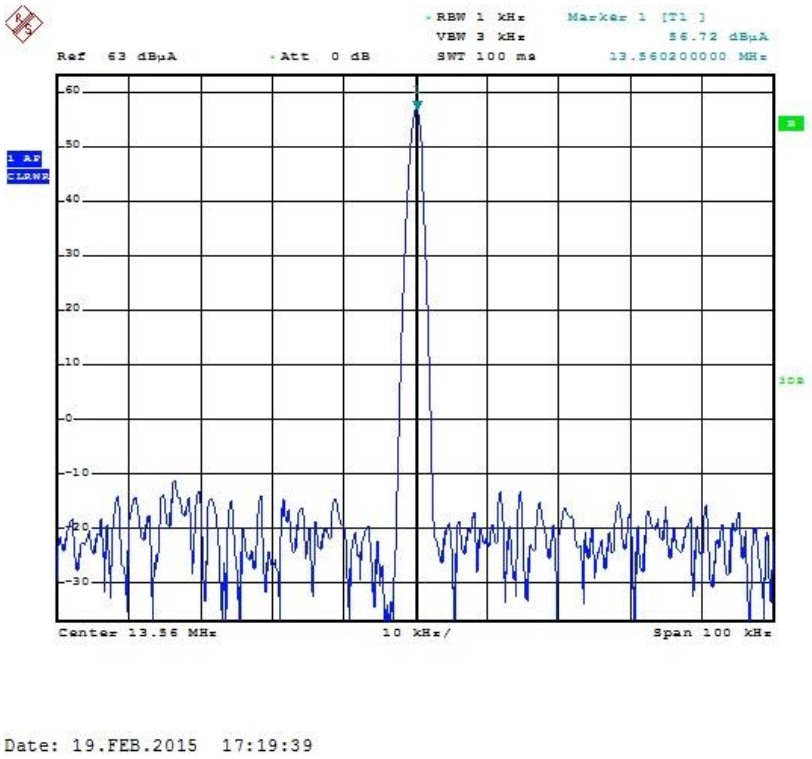
Jak již bylo zmíněno, měření probíhalo v laboratoři elektromagnetické kompatibility na Fakultě Aplikované Informatiky ve Zlíně. Úkolem bylo změřit spektrum a intenzitu elektromagnetického pole vyzařovaného vzorkem RFID čtečky. Vzorek RFID čtečky byl vyvinut v rámci smluvního výzkumu v embedded laboratoři na FAI. RFID čtečku jsem připojil ke zdroji TENMA 72-10480. Napětí bylo nastaveno na 12 V a protékající proud byl 0,054 A. Jakmile byla čtečka napájena, bylo od její antény vyzařováno elektromagnetické pole. Intenzita tohoto pole byla snímána sondou RS H-50-1, která byla připojena pomocí BNC konektorů ke spektrálnímu analyzátoru Rohde & Schwarz FSP a později také k osciloskopu RIGOL DS1052E. Hodnoty snímané sondou byly zaznamenávány po 1 cm na čtverečkovaný papír zhruba ve vzdálenostech 15 cm od středu vazební antény RFID čtečky. Lze vidět na obrázku č. 26. Počet naměřených hodnot byl okolo 650 a všechny hodnoty lze nalézt v přílohách č. PI., PII. Naměřené hodnoty byly ukládány do programu Microsoft Excel, který mi později umožnil vytvořit grafy vyzařovací charakteristiky antény v RFID čtečce. Toto měření proběhlo dvakrát. Jednou byla čtečka položena pouze na dřevěném stole a podruhé jsem pod čtečku vložil kovovou podložku, která vyzařované pole čtečky ztlumila.



Obrázek 26 - Mapování pole čtečky na čtverečkovaný papír

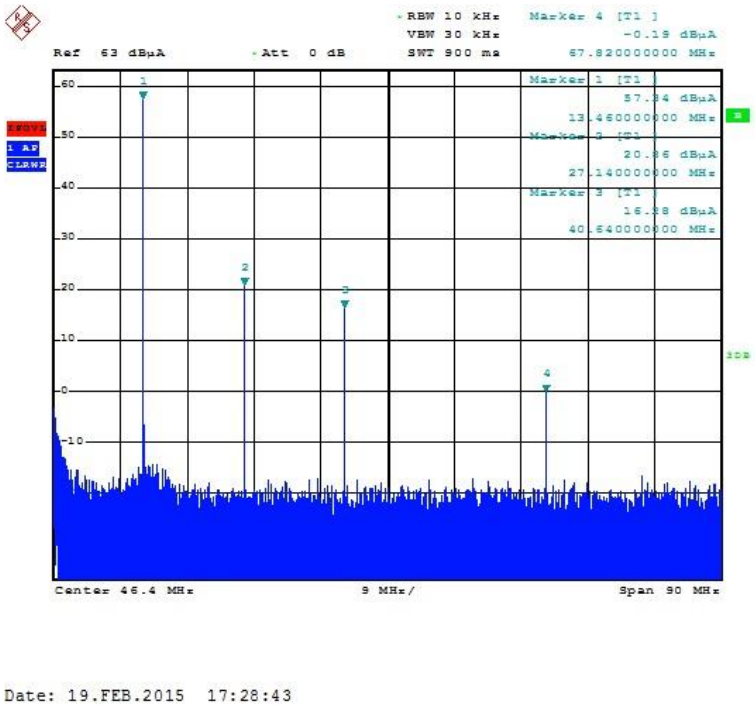
3.4 Naměřené hodnoty

Naměřené hodnoty intenzity magnetického pole čtečky byly zaznamenány do programu MS Excel, viz příloha PI a PII.



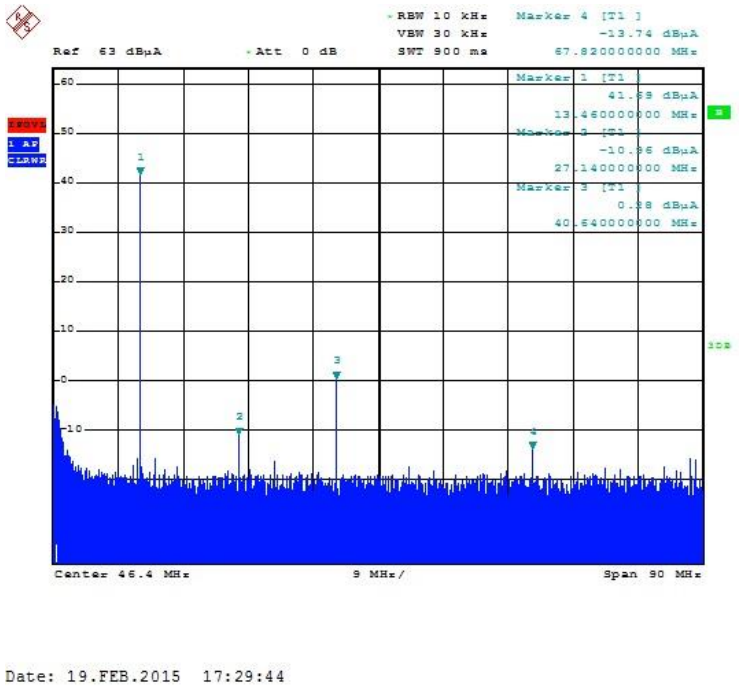
Obrázek 27 - Hodnota intenzity ve středu antény na frekvenci 13,56 MHz.

Obrázek č. 27 byl pořízen spektrálním analyzátorem a znázorňuje, že čtečka vysílala pouze nosnou frekvenci, na které bylo měřeno a to frekvenci 13,56 MHz. Na obrázku je vidět naměřené spektrum. Ve skutečnosti se jedná pouze o jednu spektrální čáru. Když to spektrální analyzátor měří a vykresluje, tak používá sadu filtrů a různé algoritmy. Tím je přesnost vždy určitým způsobem omezená. Z obrázku jde tedy vidět, že vysílá pouze na 13,56 MHz a jedná se o signál, který byl měřen. Čtečka byla defaultně nastavena tak, aby v podstatě neposílala informace a aby posílala pouze nosnou frekvenci. To z toho důvodu, aby se na ní dalo měřit. Pokud se podíváme na nastavení přístroje, tak span je nastaven na 100 kHz. Tímto nám spektrální analyzátor zobrazí na displeji okno o velikosti dané frekvence, tudíž 100 kHz, to znamená, že je viditelná část mezi 13,46 až 13,66 MHz. Mezi další nastavované parametry, které můžete vidět na obrázku, patří SWT a RWB. SWT neboli sweep time (rozmítání), byl nastaven na 100 ms. Jedná se o dobu, za jakou projede spektrum od začátku, až do konce. RBW je šířka pásma, nastavená na 1 kHz a je to šířka, se kterou bereme výsek frekvence, jelikož graf je složen z kHz segmentů. Hodnotu VBW neboli video bandwith si přístroj dopočítává sám. Na spektrálním analyzátoru byl nastaven tzv. marker, který nám sejmul naměřenou hodnotu 56,72 dBμA. Marker na obrázku značí malý modrý trojúhelník na vrcholu signálu. Tato hodnota byla naměřena sondou, která byla umístěna na střed RFID čtečky a její antény. Jedná se o nejvyšší naměřenou hodnotu intenzity elektromagnetického pole vyzařovanou právě měřenou čtečkou.



Obrázek 28 - Hodnoty harmonických frekvencí čtečky bez kovové podložky

Na obrázku č. 28 je vidět, že zde byl nastaven span 90 MHz a jak je vidět, střed je na 46,4 MHz. Opět zde můžeme vypozorovat tzv. markery, nyní jsou tam hned čtyři. Marker č. 1 nám zobrazuje velikost intenzity elektromagnetického pole na frekvenci 13,46 MHz a to 57,34 dBµA. Jedná se vlastně o obdobu z obrázku č. 27. Ostatní vytyčené markery nám znázorňují vyšší harmonické frekvence, tvar signálu a zkreslení. Naměřená hodnota markeru č. 2 s takřka dvojnásobnou frekvencí, než u předchozího markeru a to 27,14 MHz, je 20.86 dBµA. Marker č. 3 nám udává třetí harmonickou frekvenci, která činí 40.64 MHz a naměřenou hodnotu intenzity 16,28 dBµA. Marker č. 4 na čtvrté harmonické frekvenci 67,82 MHz ukazuje hodnotu -0,19 dBµA. Z tohoto vyplívá, že se jedná o skoro čisté sinusové zobrazení. Je zde vidět mírná deformace sinusovky, ale to je pravděpodobně způsobeno měřicím přístrojem, v tomhle případě spektrálním analyzátorem, který nedokáže vygenerovat sinusové zobrazení tak, aby tam žádné zkreslení nebylo.



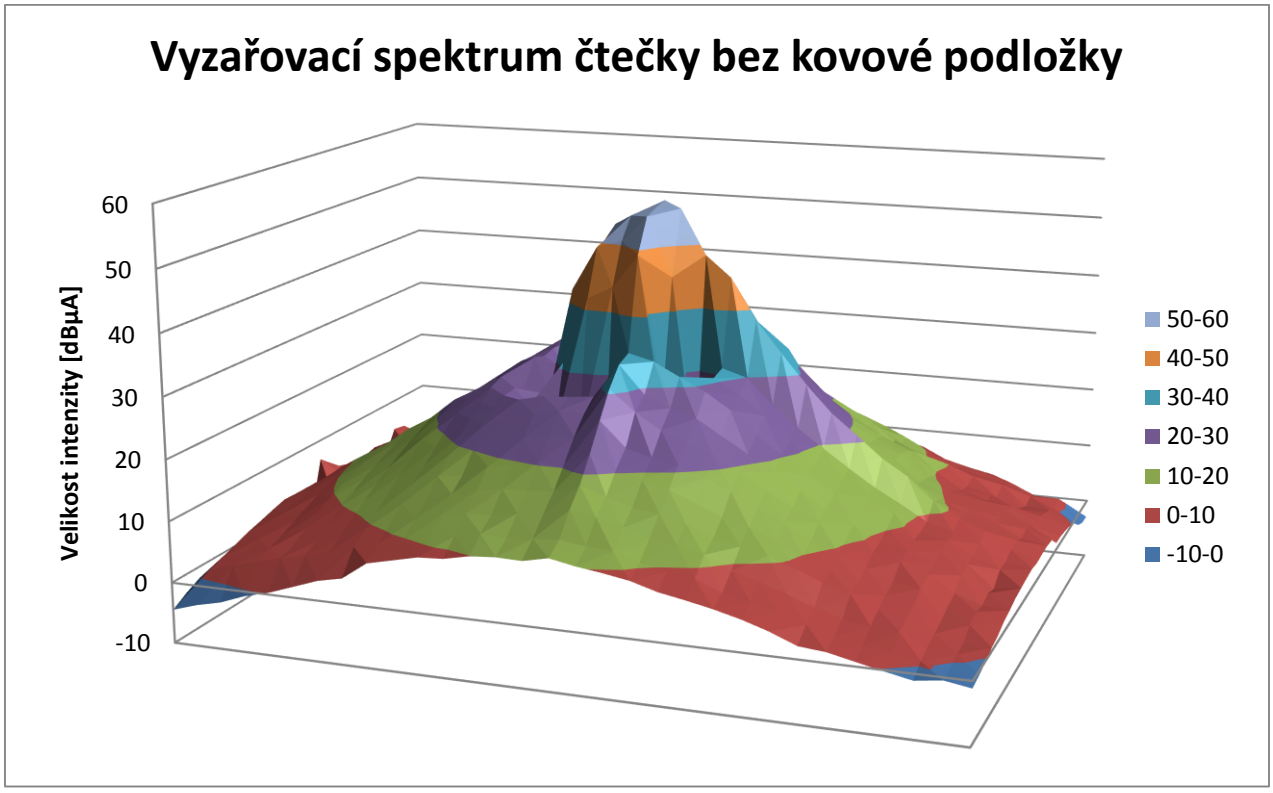
Obrázek 29 - Hodnoty harmonických frekvencí čtečky s kovovou podložkou

Když porovnáme obrázek č. 29 s obrázkem č. 28, tak vidíme, že zkreslení signálu bylo na obrázku č. 29 menší. To způsobila přítomnost kovové podložky. Signál byl výrazně zeslaben. A to z hodnoty 57,34 dBµA na hodnotu 41,69 dBµA, kterou nám opět zobrazuje marker č. 1. Co se týče ostatních markerů na druhé, třetí a čtvrté harmonické frekvenci, tak marker č. 2 naměřil na frekvenci 27,14 MHz hodnotu -10,96 dBµA. Marker č. 3 na frekvenci 40,64 MHz naměřil hodnotu intenzity 0,28 dBµA. A marker č. 4 na čtvrté harmonické frekvenci 67,82 MHz ukázal hodnotu -13,74 dBµA. Můžete si všimnout, že na obrázků č. 28 převažuje druhá harmonická frekvence a třetí harmonická frekvence je níže. Opět je tato změna způsobena kovovou deskou, kterou byla čtečka zatížena a musela dodávat větší proud. Když byla čtečka zatížena, tak klesla amplituda (druhá harmonická frekvence), ale vyrostla třetí harmonická frekvence, která odpovídá ostrým hranám sinusovky. Z toho vyplívá, že když se projevilo zatížení zesilovače, tak se změnil poměr harmonických frekvencí.

3.5 Dosažené výsledky

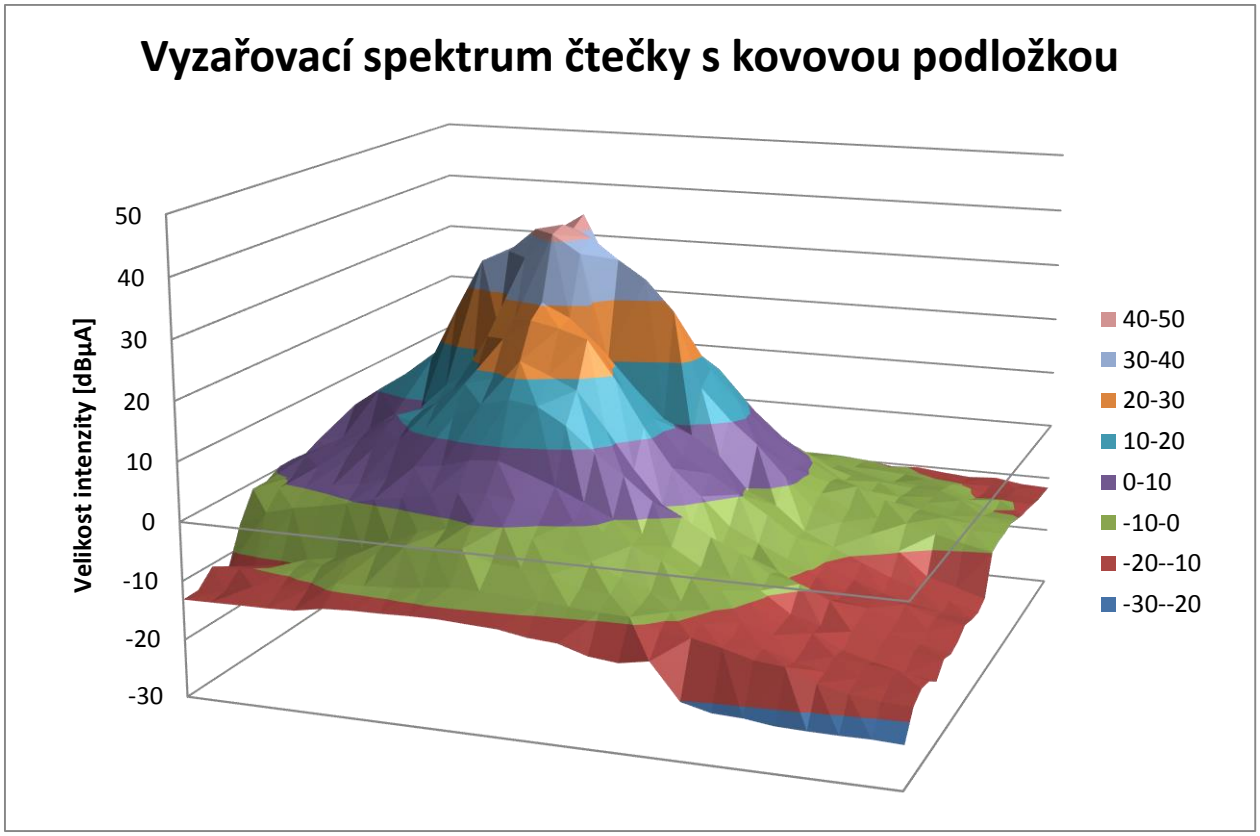
Jak již bylo zmíněno, měření probíhalo ve dvou hlavních fázích. První fáze byla taková, že se měřila intenzita elektromagnetického pole vyzařovaného RFID čtečkou. V druhé fázi se také měřila intenzita elektromagnetického pole čtečky, ale s použitím

kovové podložky, na které byla čtečka umístěna. Z naměřených hodnot první varianty byl vytvořen graf č. 1. Z druhé varianty potom graf č. 2. Jako další byla měřena velikost intenzity vyzařovacího spektra čtečky kolmo od středu její antény až do vzdálenosti 14 cm. Tyto naměřené hodnoty popisuje graf č. 3.



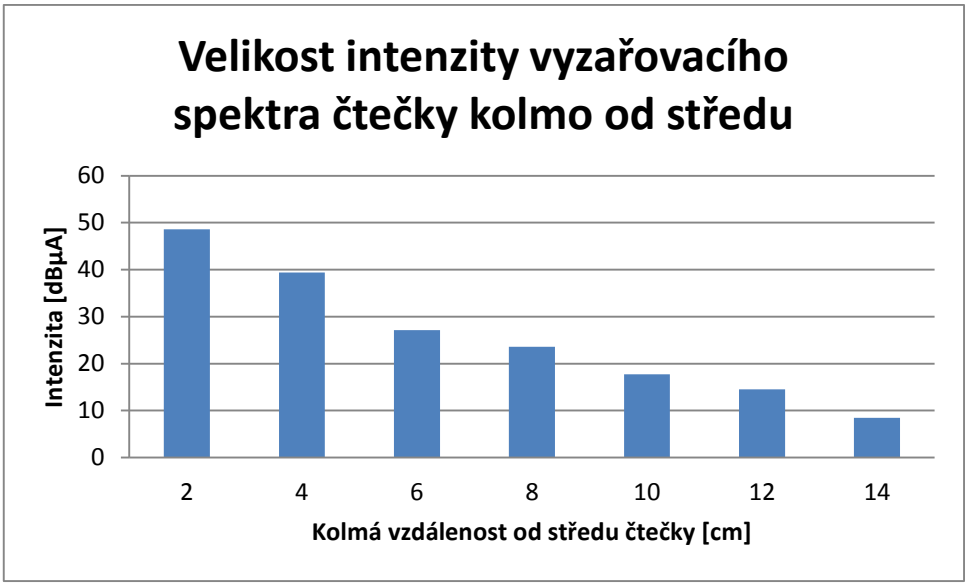
Obrázek 30 - Graf 1 - Vyzařovací spektrum čtečky bez kovové podložky

Z grafu č. 1 lze vyčíst, že naměřené hodnoty byly v rozmezí od cca -4 do 56 dBµA ve vzdálenosti od středu čtečky od středu čtečky 0-15 cm. Nejnižší naměřená hodnota byla -4,48 dBµA a nejvyšší 56,07 dBµA. Z grafu je dále vidět, že spektrum je rovnoměrně rozložené a nejsou v něm žádné velké výkyvy. Možná až na lehký propad hodnot, který mohl být způsobený ostatními prvky RFID čtečky. Z toho lze usuzovat, že vyzařovací spektrum bylo narušeno právě prvky a obvody, které jsou součástí čtečky, ale na vyzařovací vliv antény to nemělo markantní vliv.



Obrázek 31- Graf 2 - Vyzařovací spektrum čteky s kovovou podložkou

Graf č. 2 nám znázorňuje spektrum naměřených hodnot elektromagnetické intenzity, která byla měřena v okolí RFID čtečky až do vzdálenosti 15 cm. Navíc oproti grafu č. 1 jsou hodnoty měřeny se čtečkou, která byla položena na kovové podložce. Z grafu č. 2 lze vyčíst, že vyzařovací spektrum je také rozloženo rovnoměrně. Minimální naměřená hodnota činí – 22,58 dBµA, maximální naměřená hodnota pak 42,02 dBµA. Když porovnáme graf č. 1 s grafem č. 2, tak lze vidět úbytek, který by způsoben právě kovovou deskou.



Obrázek 32 – Graf 3 - Velikost intenzity kolmo od středu antény

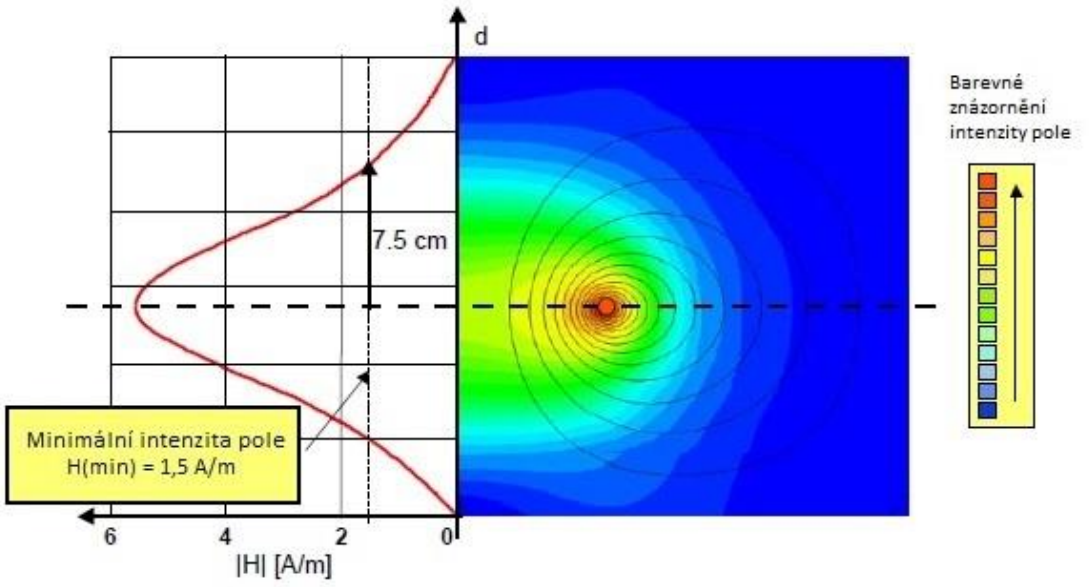
Graf č. 3 nám znázorňuje velikosti naměřené intenzity vzhledem k vzdálenosti kolmo od středu čtečky. Je vidět, že se jedná o víceméně rovnoměrné úbytky hodnot.

4 NÁVRH OPTIMALIZACE

Prvním předpokladem pro toto měření bylo to, že vazební anténa je umístěna na desce RFID čtečky, která je konfigurována nesymetricky. To znamená, že na jedné straně desky je umístěna anténa a na druhé straně jsou umístěny elektrické obvody a další prvky, které jsou součástí čtečky. Tak by se měla projevit přítomnost těchto prvků v blízkosti antény a tato přítomnost by měla vychylovat elektromagnetické pole vysílané RFID čtečkou.

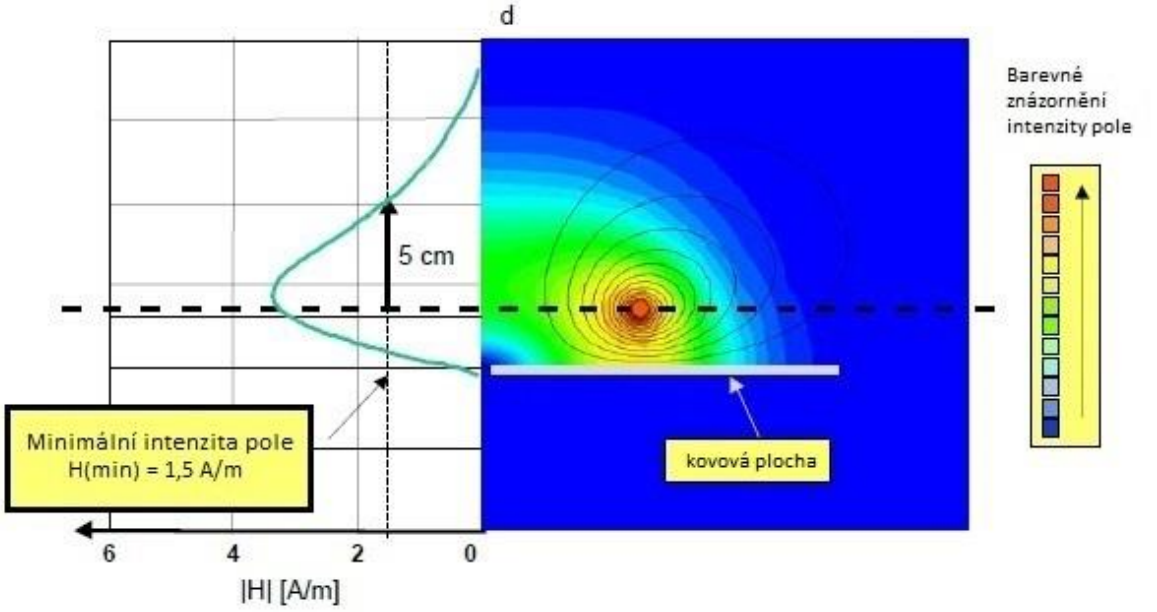
4.1 Feritové stínění

Výhodou feritu je v našem případě to, že dokáže stínit anténu před vlivem kovu. Kovová plocha může být součástí krytu přístroje nebo zařízení, které je připojeno velmi blízko k anténě. Je-li kov umístěn velmi blízko k anténě, střídavé magnetické pole vytváří v kovu rušivé proudy. Tyto rušivé proudy absorbují energii a vedou k rozladění antény vlivem snížené indukčnosti a činitele jakosti. Proto je nutné, aby byla anténa stíněna feritem pro správnou funkčnost v blízkém kovové prostředí. Pro zjednodušení simulace byla použita kruhová anténa. Simulace ukazuje rozložení pole antény. Obrázek č. 33 ukazuje dvourozměrné magnetické pole kruhové antény. Pravá část ukazuje rozložení pole. Nejvyšší intenzita pole je tvořena v oblasti cívky. Levá část zobrazuje velikost pole intenzity H přes vzdálenost *d*. Minimální intenzita magnetického pole H_{min} = 1,5 A/m, jak je definováno v normě ISO/IEC 14443 a je označena svislou tečkovanou čarou. Stínící účinek feritu silně závisí na materiálu a potom také na vzdálenosti mezi anténou a ovlivňujícím materiálem. Stínící účinek může být zanedbatelný, pokud je anténa velmi blízko rušivého materiálu (kov, baterie) a ferit má nízkou propustnost (permeabilitu).



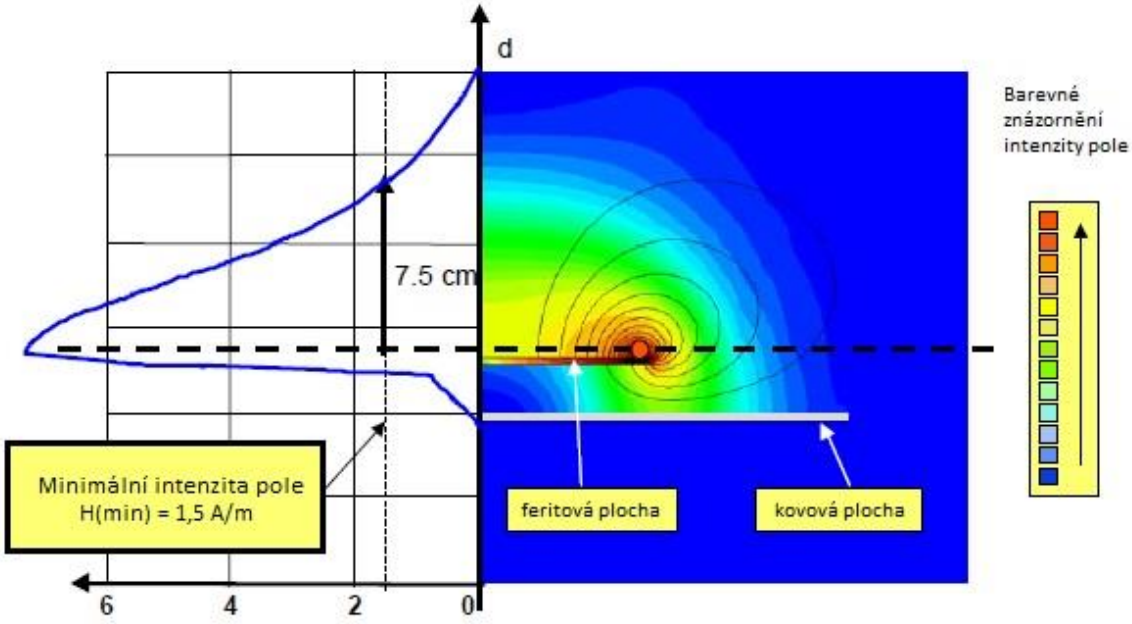
Obrázek 33 - Magnetické rozložení pole antény [25]

Obrázek č. 34 ukazuje rozložení pole antény, avšak s kovovou plochou v blízkosti antény. Velikost intenzity magnetického pole se ve srovnání s narušeným polem snížila. To vede ke snížení provozní vzdálenosti.



Obrázek 34 - Rozložení pole antény s kovovou plochou [25]

Obrázek č. 35 znázorňuje feritovou plochu, která je umístěna mezi kovovou plochu a cívku antény. Intenzita pole velmi blízko feritové plochy se zvyšuje, ale zvýšení intenzity nemusí nutně vést ke zvýšení provozní vzdálenosti.



Obrázek 35 - Rozložení pole s kovovou i feritovou plochou [25]

Simulace ukazuje, že použití feritu snižuje generované vířivé proudy v kovové ploše. Ferit generuje další složku pole, která vede k fixnímu rozladění antény. [25]

4.2 Optimalizace vazební antény

Po úspěšném měření intenzity vyzařovaného elektromagnetického pole RFID čtečky a dalších naměřených hodnotách, byly pro lepší znázornění vytvořeny grafy a také zachyceny obrázky, screenshoty z měřících přístrojů. Tyto hodnoty, grafy a obrázky byly prozkoumány a na jejich základě měla být navrhnouta optimalizace vazební antény měřené RFID čtečky. Jak již bylo zmíněno, vycházel jsem z předpokladu, že vazební anténa umístěna na měřeném vzorku RFID čtečky je konfigurována nesymetricky. A že by prvky, které jsou umístěny na druhé straně RFID čtečky v blízkosti antény, měly vychylovat elektromagnetické pole, které čtečka vysílá. Provedené měření ale tento předpoklad vyvrátilo. Naměřené hodnoty a grafy ukázaly, že pole vyzařované RFID čtečkou není žádným velkým způsobem deformované a je téměř rovnoměrné. Proto lze konstatovat, že u měřené RFID čtečky, která byla vyvinuta v rámci smluvního výzkumu v embedded laboratoři na FAI, nemusí probíhat žádná optimalizace vazební antény, s cílem omezit rušení elektromagnetického pole, vysílané právě vazební anténou. Jelikož měřená čtečka ještě nebyla opatřena žádným krytem, bylo by potřeba při návrhu nové krabičky počítat s tím, že čtečka vyzařuje kolmo po svojí ose.

ZÁVĚR

V této diplomové práci byly popsány technologie jako RFID, čárové kódy a NFC. Všechny tyto technologie mají svá uplatnění a podle mého názoru se v blízké době nechystá kompletní náhrada jednou technologií za další. Dalo by se říci, že RFID technologie se dá použít tam, kde jsou praktické nedostatky u čárových kódů. To stejné by mohlo platit u NFC a RFID technologií.

Jak již bylo zmíněno, technologie jako RFID a NFC mají v sobě velký potenciál na využití v reálném světě. Již nyní nám usnadňují život a myslím, že v budoucnu budou tyto technologie stále více a více používané. V poslední řadě proběhla zmínka o bezpečnosti. Ano, tyto technologie nalezly praktické využití a uplatnění v reálném světě, ovšem mějme na paměti, že s každou novou technologií přichází i jistá bezpečnostní rizika, na které je třeba brát ohled. Rozhodně tím nechci říct, že tyto technologie jsou nebezpečné a neměli by se používat, to ne. Ovšem každý uživatel, by si měl být vědom, jaká možná rizika hrozí u používání těchto technologií.

Co si týká praktické části této diplomové práce, tak proběhlo laboratorní měření v laboratoři elektromagnetické kompatibility na Fakultě Aplikované Informatiky ve Zlíně. Byla změřena intenzita elektromagnetického pole a spektrum vyzařovaného vzorku RFID čtečky, která byla v předchozích letech vyrobena právě na FAI. Na základě těchto naměřených výsledků měla být provedena optimalizace vazební antény měřené RFID čtečky. První předpoklad byl takový, že vazební anténa je umístěna na desce čtečky, která je konfigurována nesymetricky. To by znamenalo, že ostatní prvky umístěné na desce čtečky by svou přítomností měly vychylovat elektromagnetické pole vysílané vazební anténou.

Z naměřených výsledků, grafů a obrázků však bylo patrné, že pole vyzařované RFID čtečkou není žádným velkým způsobem deformované a je rovnoměrné. Proto lze konstatovat, že u měřené RFID čtečky nemusí probíhat žádná optimalizace vazební antény s cílem omezit rušení elektromagnetického pole, vysílané právě vazební anténou. Jelikož měřená čtečka ještě nebyla opatřena žádným krytem, bylo by potřeba při návrhu nové krabičky počítat s tím, že čtečka vyzařuje kolmo po svojí ose. V rámci práce jsem si osvojil systematický přístup ke svěřenému technickému úkolu a práci se specializovaným vybavením laboratoře.

ZÁVĚR V ANGLIČTINĚ

In this thesis were described technology as RFID, barcodes and NFC. All these technologies have their use and in my opinion, in the near future is not going to happen that one technology will replace the other. You could say that RFID technology can be used where there are practical gaps in the barcode. The same could be true for NFC and RFID.

As mentioned above, technologies such as RFID and NFC have in themselves a great potential for use in the real world. Our lives are already easier because of these technologies and I think that in the future will be these technologies more and more used. Lastly was mentioned safety and security. Yes, these technologies have found practical use, application, however, bear in mind that with every new technology comes a certain security risks that need to be kept in mind and taken care of. Certainly, I did not mean to say that these technologies are dangerous and should be avoided, not at all. However, each user should be aware of these risks and possibilities with the use of these new technologies.

In concern of the practical part of this thesis, the laboratory measurements took place in the laboratory of electromagnetic compatibility at the Faculty of Applied Informatics in Zlin. The intensity of the electromagnetic field and spectrum was measured, emitted by a sample of the RFID reader, which in previous years was made at FAI. Based on these measured results, I had to suggest to optimalization of the antenna coupler of the measured RFID reader. The first assumption was that the coupling antenna is located on the RFID reader board that is configured asymmetrically. This would mean that other elements on the readers board by its presence should deflect the electromagnetic field emitted by RFID reader antenna coupler.

However, from the measured results, graphs and images, was evident that the field emitted by RFID reader is not deformed in any big way and it is, more or less evenly. Therefore we can say that in the measured RFID reader there is no need to optimize the antenna coupling, in order to reduce interference of the electromagnetic field emitted by the antenna coupler. As the measured reader has not yet been fitted with cover box, it would be good before designing the box, to count with the fact that the reader radiates vertically along its axis. In this work I learned a systematic approach to the entrusted technical task and how to work with specialized laboratory equipment.

SEZNAM POUŽITÉ LITERATURY

[1] Co je to NFC a co umí?. *Nearfield* [online]. 2012 [cit. 2014-11-30]. Dostupné z: http://nearfield.cz/co-je-nfc

[2] Nfctech. NÁPRSTEK, Miloslav. *Nfctech* [online]. 2014-24-03 [cit. 2014-11-30]. Dostupné z: http://www.nfctech.cz/

[3] Nfctech: CO JE NFC? INFORMACE O TECHNOLOGII NFC (NEAR FIELD COMMUNICATION). NÁPRSTEK, Miloslav.*Nfctech* [online]. 2011-11-25 [cit. 2014-11-30]. Dostupné z: http://www.nfctech.cz/co-je-near-field-communication-nfc/

[4] Nearfield. In: KORB, Kryštof. *Nearfield: NFC tagy: co jsou vlastně zač a jak fungují?* [online]. 2012-03-15 [cit. 2014-11-30]. Dostupné z: http://nearfield.cz/clanky/nfc-tagy-co-jsou-vlastne-zac-a-jak-funguji-5

[5] KOVAŘÍK, David. NFC – prozkoumejte využití technologie budoucnosti (vědecké okénko). *Mobilizujeme* [online]. 2012-04-29, č. 1 [cit. 2014-11-30]. Dostupné z: http://mobilizujeme.cz/clanky/nfc-prozkoumejte-vyuziti-technologie-budoucnosti-vedecke-okenko/

[6] DOKOUPIL, Aleš. RFID z pohledu bezpečnosti. *Automa* [online]. 2009, č. 1 [cit. 2014-11-30]. Dostupné z: automa.cz/res/pdf/39331.pdf

[7] BĚLÍČEK, Vlastimil. *Využití RFID při vyčítání informací o zboží* [online]. Zlín, 2012 [cit. 2014-11-30]. Dostupné z: theses.cz/id/sbwk8v/. Bakalářská práce. UTB Zlín. Vedoucí práce Ing. Jiří Pálka, Ph.D.

[8] KRATOCHVÍL, Vít. *Využití RFID v průmyslu komerční bezpečnosti* [online]. Zlín, 2013 [cit. 2014-11-30]. Dostupné z: https://theses.cz/id/qivr76/. Bakalářská práce. UTB Zlín. Vedoucí práce doc. Mgr. Milan Adámek, Ph.D.

[9] Radio-frequency identification. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-, 2014-11-23 [cit. 2014-11-30]. Dostupné z: http://en.wikipedia.org/wiki/Radio-frequency_identification

[10] Near Field Communication. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-, 2014-11-06 [cit. 2014-11-30]. Dostupné z: http://cs.wikipedia.org/wiki/Near_Field_Communication

[11] POLÁK, David. *Zabezpečení zboží RFID technologiemi* [online]. Zlín, 2012 [cit. 2014-11-30]. Dostupné z: https://theses.cz/id/icamvq/?furl=%2Fid%2Ficamvq%2F;lang=en. Bakalářská práce. UTB Zlín. Vedoucí práce JUDr. Jiří Kameník.

[12] NFC Tag Logos And Icons. In: *Rapidnfc* [online]. 2014 [cit. 2014-11-30]. Dostupné z: http://rapidnfc.com/nfc_tag_logos

[13] NXP begins shipping NFC tags that can wake up a host device. In: *Nearfieldcommunication* [online]. 2013 [cit. 2014-11-30]. Dostupné z: http://www.nearfieldcommunication.com/tag/nfc-tags/page/2/

[14] NFC helps you stay in touch with your customers. *Starkrfid* [online]. 2013 [cit. 2014-11-30]. Dostupné z:http://www.starkrfid.com/rfid-products/nfc/

[15] MATTHEW PIERSON, RYAN. Should You Be Worried About RFID Skimming?. *Lockergnome* [online]. 2012 [cit. 2014-11-30]. Dostupné z: http://www.lockergnome.com/news/2012/06/01/rfid-skimming/

[16] Quick Introduction to RFID. *Polygait* [online]. 2012 [cit. 2014-11-30]. Dostupné z:http://www.polygait.calpoly.edu/tutorial.htm

[17] *Books.fs.vsb: ČÁROVÝ KÓD EAN-13* [online]. 2010 [cit. 2014-11-30]. Dostupné z:http://books.fs.vsb.cz/ZaklInfSbirka/TEOROZ/TEOROZ.HTML

[18] *RFID tags: RFID Tags For Solar Module India*. 2014. Coresonant [online]. [cit. 2015-05-13]. Dostupné z: http://www.coresonant.com/html/rfid-tags-for-solar-module-india.html

[19] *RealTime ID: Passive and Active tags. 2005. Realtimeid* [online]. [cit. 2015-05-13]. Dostupné z: http://www.realtimeid.com/technology.htm

[20] *Passive & Active RFID. 2006. Wirelessvisionme* [online]. [cit. 2015-05-13]. Dostupné z: http://www.wirelessvisionme.com/products-solutions/technologies/passive-active-rfid/

[21] *CADAMURO, Mirco. 2011. CAEN RFID. Veryfields [online]. (1) [cit. 2015-05-15]. Dostupné z: http://www.veryfields.net/caen-rfid-offers-semi-passive-gen-2-rfid-tags-and-development-kits-for-cold-chain-monitoring-applications*

[22] *Mobile and Ubiquitous Compuing. 2013. Department of Computer Science and Information Systems [online]. [cit. 2015-05-15]. Dostupné z: http://www.dcs.bbk.ac.uk/~gr/muc/2013/7_rfidbasics.pdf*

[23] *MC9090-Z. 2015. Motorolasolutions* [online]. [cit. 2015-05-13]. Dostupné z: https://portal.motorolasolutions.com/Support/US-EN/Mobile+Networks+RFID+and+BarCode+Scanners/RFID+Products/MC9090-Z%20RFID_US-EN

[24] *A Review on the Operating Modes of Near Field Communication. 2012. Ijeat* [online]. [cit. 2015-05-13]. Dostupné z: http://www.ijeat.org/attachments/File/v2i2/B0956112212.pdf

[25] *Antenna design guide. 2010. NXP* [online]. [cit. 2015-05-13]. Dostupné z: http://eng.utah.edu/~mlewis/ref/NFC/AN1445.pdf

[26] NFC Tags vs QR Codes: How to Make the Right Choice. 2013. *Rapid NFC* [online]. [cit. 2015-05-13]. Dostupné z: http://rapidnfc.com/blog/73/nfc_tags_vs_qr_codes_how_to_make_right_choice

[27] 5 Reasons why NFC will never replace the barcode. 2012. *Scandit* [online]. [cit. 2015-05-13]. Dostupné z: http://www.scandit.com/2012/04/24/5-reasons-why-nfc-will-never-replace-the-barcode/

[28] About the NDEF Format. 2012. *Adafruit* [online]. [cit. 2015-05-13]. Dostupné z: https://learn.adafruit.com/adafruit-pn532-rfid-nfc/ndef

[29] A. WEIS, Stephen. 2010. RFID (Radio Frequency Identification): Principles and Applications. *Rfid-article.pdf* [online]. (1) [cit. 2015-05-13]. Dostupné z: http://www.eecs.harvard.edu/cs199r/readings/rfid-article.pdf

[30] KAUR, Mandeep, Manjeet SANDHU, Neeraj MOHAN a Parvinder S. SANDHU. 2011. RFID Technology Principles, Advantages, Limitations & Its Applications. *306-E794.pdf* [online]. (3) [cit. 2015-05-13]. Dostupné z: http://www.ijcee.org/papers/306-E794.pdf

[31] MITCHELL, Simon. 2011. Near Field Communication. *Matchbyte* [online]. [cit. 2015-05-13]. Dostupné z: http://www.matchbyte.com/images/download/near-field-communication.pdf

[32] MAYER, Daniel. Aplikovaný elektromagnetizmus: Úvod do makroskopické teorie elektromagnetického pole pro elektrotechnické inženýry. 2. Vyd. České Budějovice: Kopp, 2012, 538 s. ISBN 978-80-7232-436-1.

[33] MAZÁNEK, Miloš a Pavel PECHAČ. Šíření elektromagnetických vln a antény. 2. Vyd. , Přeprac. Praha: Vydavatelství ČVUT, 2005, 259 s. ISBN 8001030326.

[34] SVAČINA, Jiří. Elektromagnetická kompatibilita: Principy a poznámky. 1. Vyd. Brno: Vysoké učení technické, 2001, 156 s. ISBN 8021418737.

[35] GLOVER, Bill a Himanshu BHATT. RFID Essentials. Massachusetts, USA: O'Reilly Media, 2006. ISBN 978-0-596-00944-1.

[36] WANT, Roy. RFID Explained: Synthesis Lectures on Mobile and Pervasive Computing. California, USA: Morgan and Claypool Publishers, 2006. ISBN 978-1598291087.

[37] PERIS LOPEZ, Pedro. Security and Trends in Wireless Identification and Sensing Platform Tags: Advancements in RFID. Hershey, Pennsylvania: IGI Global, 2012. ISBN 978-1466619906.

[38] COSKUN, Vedat, Kerem OK a Busra OZDENIZCI. Near Field Communication (NFC): From Theory to Practice. New York, USA: Wiley, 2012. ISBN 978-1119971092.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ASIC	Application Specific Integrated Circuit
CAN	Controller Area Network
CC	Constant Current
CV	Constant Voltage
EAN	European Article Number
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EPC	Electronic Product Code
FAI	Fakulta Aplikované Informatiky
HF	High Frequency
IFF	Identify Friend or Foe
LCD	Liquid Crystal Display
LF	Low Frequency
LLCP	Logical Link Control Protocol
MHD	Městská Hromadná Doprava
MW	Microwave
NDEF	NFC Data Exchange Format
NFC	Near Field Communication
NFCIP-1	Near Field Communication Interface and Protocol
OCP	Over Current Protection
OVP	Overload Protection
P2P	Peer-to-Peer
PIN	Personal Identification Number
QR	Quick Response

RF	Radio Frequency
RFID	Radio Frequency Identification
SMS	Short Message Service
SSL	Secure Sockets Layer
UHF	Ultra High Frequency
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTB	Univerzita Tomáše Bati
UTF	Universal Coded Character Set + Transformation Format
UWB	Ultra Wideband
UPC	Universal Product Code
Wi-Fi	Wireless Fidelity
WPS	Wireless Provisioning Services

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: NAMĚŘENÉ HODNOTY (BEZ PODLOŽKY)

	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	D	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	
11	-4,48	-3,22	-2,28	-0,76	0,29	1,72	3,19	4,65	6,24	7,88	8,82	9,06	9,94	10,25	10,14	11,03	10,24	9,67	8,97	7,75	6,99	6,12	5,05	3,72	2,02	1,65	0,71	-0,2	-1,05	-0,46	-1,12	11
11	-4,48	-3,22	-2,28	-0,76	0,29	1,72	3,19	4,65	6,24	7,88	8,82	9,06	9,94	10,25	10,14	11,03	10,24	9,67	8,97	7,75	6,99	6,12	5,05	3,72	2,02	1,65	0,71	-0,2	-1,05	-0,46	-1,12	11
10	-3,01	1,18	2,42	3,56	4,52	5,4	6,56	7,82	8,89	9,81	10,67	11,42	12,18	11,94	12,3	12,62	12,05	11,78	10,48	9,67	8,91	7,18	6,36	5,2	3,89	2,61	1,77	1,15	0,37	-0,42	-0,72	10
9	-1,83	2,05	3,22	4,46	5,34	6,65	7,95	9,52	10,62	11,92	13	13,68	13,85	14,6	14,89	16,06	15,25	14,12	12,93	12,27	11,3	9,34	8,02	6,7	5,09	3,8	3,2	2,9	1,08	0,47	-0,21	9
8	-1,63	2,79	4,26	5,52	6,91	8,19	9,51	11,12	12,72	13,83	15,16	16,2	16,82	17,01	17,34	18,73	17,3	16,09	15,51	14,32	12,58	11,76	10,8	9,26	7,56	6,33	4,38	3,43	1,65	0,59	0,54	8
7	-0,44	3,74	5,14	6,55	8,41	9,92	11,38	13,08	14,95	16,48	17,04	18,83	19,54	20,34	20,38	21,5	20,4	19,22	18,14	16,36	14,65	13,47	11,75	9,91	8,17	6,57	5,2	4,28	2,35	2,14	0,93	7
6	0,12	4,38	6,15	7,5	9,58	11,02	12,8	14,71	16,64	18,77	20,14	21,39	22,6	23,24	23,7	26,72	22,73	21,62	20,85	19,21	17,44	15,27	13,32	11,09	9,48	7,5	5,94	5,43	3,21	2,77	1,72	6
5	0,82	5,09	6,81	8,61	10,62	12,26	14,33	16,38	18,5	20,86	22,95	24,27	25,56	26,43	26,28	30,7	27,39	24,81	23,27	21,58	19,25	16,97	14,56	12,66	10,32	8,76	7,8	6,28	3,82	2,3	2,12	5
4	1,28	5,72	7,46	9,34	11,4	13,3	15,45	18,5	20,45	22,79	24,71	26,51	27,44	27,67	28,11	33,6	29,11	27,32	26,07	23,52	21,1	18,87	16,03	13,51	11,52	9,48	8,24	6,73	5,32	2,96	2,65	4
3	1,58	5,6	7,94	9,92	12,25	14,23	16,63	19,44	22,01	24,04	25,76	24,48	19,91	18,91	11,52	34,3	33,48	31,33	29,32	26,7	23,07	20,18	17,85	15,05	12,54	10,19	8,7	7,37	5,73	2,26	2,88	3
2	-2,32	4,92	8,17	10,34	12,78	15,12	17,61	20,85	23,48	25,78	26,06	13,4	30,94	41,84	43,94	49,3	26,6	25,67	30,54	28,1	25,15	21,7	18,24	15,73	13,56	11,35	8,63	7,83	5,67	4,02	3,1	2
1	-3,68	4,25	8,39	10,86	13,32	16,32	18,58	21,98	24,24	26,59	25,26	24,32	42,23	49,37	50,62	54,79	45,3	19,5	31,17	29,93	25,91	22,43	19,47	16,61	13,91	11,62	9,15	7,96	6,56	3,88	3,26	1
C15	-2,9	1,9	6,31	8,23	11,17	14,11	16,8	20,02	22,28	26,11	29,3	28,2	33,6	49,7	54,02	55,56	55,66	48,38	45,01	38,42	33,4	28,57	24,25	20,97	17,55	14,96	11,4	8,95	7,29	4,62	3,01	A
1	6,63	4,3	6,78	10,02	12,63	15,47	18,36	21,55	24,47	27,36	28,6	19,13	45,47	51,7	52,3	56,07	50,9	19,58	36,15	35,7	33,12	24,32	21,12	17,9	15,35	12,5	10,4	8,42	6,7	4,97	3,15	1
2	4,08	3,76	8,5	10,41	13,3	15,16	18,51	21,39	24,33	27,15	29,05	21,07	41,3	49,46	51,02	54,6	49,12	33,66	37,3	32,66	28,08	23,95	20,87	17,3	15,12	11,7	9,82	8,14	6,19	3,95	3,2	2
3	1,52	4,58	7,82	9,97	11,9	15,07	17,9	21,05	23,6	27,04	29,83	30,81	22,26	34,7	39,6	30,52	40,01	37,8	35,7	31,9	27,2	23,21	20,13	17,19	15,02	11,2	9,26	7,63	5,9	4,35	2,95	3
4	1,38	3,88	7,71	9,67	12,03	14,83	16,95	19,76	22,08	25,15	29,04	31,82	30,2	33,56	32,6	41,35	37,12	36,8	33,76	28,51	25,53	21,7	18,89	16,43	14,43	10,34	8,47	7,12	5,55	3,62	1,16	4
5	0,78	5,23	7,12	9,03	10,72	13,32	16,2	18,7	21,7	24,67	26,58	28,54	28,98	29,77	31,3	35,4	31,74	29,46	26,3	23,23	20,63	17,95	15,3	13,31	13,22	9,8	7,3	5,94	5,32	3,39	1,1	5
6	0,91	4,64	6,55	8,21	9,81	12,05	14,4	16,53	18,71	20,83	23,01	25,08	26,11	27,33	27,5	30,21	28,02	27,72	25,9	23,5	21,12	18,8	16,6	13,65	11,7	10,55	6,78	5,66	3,62	2,85	0,82	6
7	0,28	3,13	5,73	7,45	8,67	10,82	12,56	14,82	16,7	19,05	20,83	22,83	24,3	24,8	25,53	25,3	24,95	23,94	22,48	20,27	18,55	16,63	14,53	12,02	10,2	8,62	7,43	4,07	2,68	2,3	0,35	7
8	4,63	2,62	5,07	7,85	7,77	9,25	10,78	13,25	15,11	17,09	18,06	19,3	21,15	22,13	22,5	21,82	20,94	20,23	19,12	17,88	16,73	15,48	13,24	11,9	9,52	7,45	6,32	5,15	1,73	1,5	-0,42	8
9	4,22	2,71	3,12	5,27	6,03	9,17	10,05	11,65	13,41	14,74	16,34	18,01	18,53	19,63	20,04	18,35	18,9	18,3	17,83	16,14	15,1	13,95	12,24	9,47	8,04	6,18	4,94	3,92	2,33	0,52	-1,95	9
10	-0,38	0,63	1,88	0,83	5,42	6,92	7,63	9,76	10,64	12,87	14,21	14,82	16,25	16,78	16,52	15,2	16,4	15,7	15,14	13,62	12,72	11,5	9,63	6,66	6,51	5,26	4,3	3,12	1,26	1,09	-2,81	10
11	-1,32	-1,03	-0,15	5,3	3,5	5,13	5,9	7,35	8,7	10,52	11,48	12,56	14,03	14,15	14,88	12,55	13,7	13,45	12,37	11,32	10,4	9,55	7,92	7,03	5,02	3,98	3,12	0,32	-0,46	-1,2	-2,92	11
11	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	D	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	11

PŘÍLOHA P II: NAMĚŘENÉ HODNOTY (S PODLOŽKOU)

	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	B	D	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	
11	-14,36	-14,23	-13,9	-13,75	-13,62	-13,33	-13,12	-13,05	-12,96	-12,91	-12,74	-11,87	-11,6	-11,54	-11,37	-11,35	-11,6	-11,82	-12,63	-12,98	-14,52	-15,05	-14,13	-20,14	-21,36	-21,55	-22,2	-22,35	-22,41	-22,36	-22,58	11
10	-15,03	-14,72	-14,55	-14,38	-13,63	-13,18	-13,03	-12,58	-11,36	-11,24	-10,64	-9,17	-9,03	-8,79	-8,22	-7,63	-7,66	-7,94	-8,21	-8,62	-8,93	-9,08	-10,85	-11,36	-12,4	-13,79	-14,28	-16,32	-17,39	-18,06	-18,27	10
9	-14,87	-13,54	-13,05	-12,47	-12,01	-11,15	-10,45	-10,22	-9,78	-9,36	-8,2	-6,15	-4,98	-3,29	-3,03	-2,7	-4,56	-4,84	-5,38	-7,13	-7,52	-8,11	-9,16	-9,87	-11,24	-12,96	-14,84	-15,39	-15,94	-16,33	-17,56	9
8	-15,33	-14,62	-14,21	-13,74	-12,76	-12,62	-12,96	-11,31	-10,63	-9,12	-8,32	-6,41	-4,25	-2,36	-1,28	0,53	3,12	1,41	-2,85	-4,16	-5,3	-8,11	-9,16	-9,87	-11,24	-12,96	-14,84	-15,39	-15,94	-16,33	-17,56	8
7	-12,54	-11,91	-10,43	-9,35	-8,14	-7,06	-5,97	-3,41	-2,16	-1,32	-0,32	0,84	1,83	2,77	3,4	3,8	3,12	1,41	0,63	-0,85	-2,41	-4,36	-6,79	-8,23	-10,34	-12,76	-13,65	-15,92	-17,31	-18,52	-19,32	7
6	-11,2	-9,52	-8,12	-6,71	-4,59	-2,67	-1,07	-0,52	0,12	0,94	1,64	3,15	5,54	6,23	7,61	B	6,34	4,51	2,33	0,14	-1,94	-3,52	-6,41	-7,62	-9,25	-12,63	-13,97	-14,39	-15,75	-16,8	-17,25	6
5	-10,98	-8,54	-8,31	-5,12	-3,28	-2,09	-1,05	0,26	2,54	3,94	6,31	8,45	10,91	13,22	15,82	17,06	16,36	13,52	9,43	6,04	2,15	0,14	-2,84	-4,95	-7,98	-9,14	-11,34	-13,93	-15,66	-16,96	-18,06	5
4	-12,25	-10,19	-8,35	-5,16	-3,09	-1,18	0,32	2,65	4,34	6,13	8,62	10,56	14,3	17,85	19,08	22,52	20,51	18,34	12,39	5,81	0,26	-2,94	-6,32	-8,84	-9,1	-11,95	-12,76	-13,59	-15,31	-16,32	-17,51	4
3	-12,56	-11,08	-9,92	-7,14	-5,22	-2,84	0,38	2,67	5,3	7,24	9,94	11,33	14,31	18,94	24,85	28,36	27,3	25,84	19,36	11,74	5,21	0,84	-3,82	-6,22	-8,45	-10,78	-12,66	-13,97	-14,05	-15,62	-16,34	3
2	-11,58	-10,35	-9,31	-6,07	-4,52	-2,63	0,15	1,55	3,93	5,24	8,21	10,99	14,1	23,85	27,12	30,39	28,12	23,94	16,27	11,05	6,04	3,45	0,29	-2,74	-6,12	-10,13	-12,46	-14,15	-15,53	-16,42	-17,05	2
1	-9,42	-8,56	-6,44	-5,21	-3,57	-1,75	1,35	2,38	3,84	7,35	8,13	13,41	16,45	24,32	36,84	41,16	38,14	20,16	15,56	10,86	8,41	5,14	-0,35	-2,43	-6,42	-8,75	-10,86	-12,98	-14,53	-15,88	-17,39	1
C15	-13,36	-12,5	-10,78	-7,16	-3,34	-1,87	0,85	7,1	10,45	13,53	16,43	25,89	34,82	36,84	40,96	42,02	40,13	36,58	33,46	28,32	15,46	10,48	6,42	1,32	-3,76	-5,74	-7,42	-9,82	-13,74	-15,12	-16,48	A
1	-7,21	-6,87	-5,36	-4,19	-2,15	0,23	2,35	5,39	9,46	12,47	17,74	26,25	32,56	37,14	38,89	40,57	37,34	28,13	24,15	22,13	17,56	12,4	5,53	1,43	-2,56	-4,79	-5,82	-6,34	-7,74	-8,89	-9,87	1
2	-6,94	-5,12	-4,21	-3,46	-2,18	-1,59	0,56	3,78	6,94	10,57	13,53	19,34	25,78	30,44	36,62	42,2	32,86	26,46	23,14	19,56	16,53	10,53	5,23	0,65	-1,85	-2,12	-4,06	-5,94	-6,23	-7,98	-9,42	2
3	-4,65	-4,01	-2,46	-2,13	-1,85	-1,06	0,88	2,43	4,15	7,91	12,38	17,86	21,35	27,43	34,15	36,85	25,23	23,56	21,46	16,2	13,43	8,34	4,13	0,34	-2,46	-4,16	-6,52	-6,58	-7,34	-8,31	-9,43	3
4	-2,16	-1,98	-1,46	-1,53	-1,09	-0,56	0,18	1,53	2,96	4,26	6,35	8,16	12,56	21,46	29,48	32,8	30,14	25,13	18,51	13,56	9,42	3,03	0,94	-1,25	-4,15	-5,76	-6,15	-6,85	-7,65	-8,15	-9,12	4
5	-3,25	-3,1	-2,52	-2,13	-1,77	-1,2	-0,87	1,34	2,56	4,12	7,13	9,43	13,59	18,23	25,86	30,15	23,15	20,18	10,58	8,21	2,53	0,84	-0,21	-3,84	-4,62	-5,19	-6,87	-6,97	-7,19	-9,13	-9,77	5
6	-4,12	-4,1	-3,21	-2,84	-1,65	-1,02	-0,94	0,17	1,05	2,94	4,13	8,13	10,45	13,68	20,47	24,16	20,16	12,13	8,64	3,42	0,23	-2,15	-3,59	-4,92	-5,35	-6,31	-7,16	-7,16	-8,45	-10,08	-10,34	6
7	-4,15	-3,12	-2,88	-2,45	-2,06	-1,24	-1,42	-0,98	-0,45	0,19	2,15	1,52	3,35	5,23	7,45	13,25	7,24	3,12	1,34	0,17	-2,94	-3,48	-4,31	-5,84	-6,85	-7,97	-7,98	-7,96	-9,61	-9,36	-10,64	7
8	-4,85	-4,31	-4,13	-3,84	-3,42	-3,18	-2,89	-2,65	-2,14	-1,87	-1,05	0,89	2,16	1,52	0,56	-0,23	-3,15	-2,98	-2,48	-3,18	-4,97	-5,75	-6,57	-7,66	-7,21	-8,64	-8,16	-8,64	-10,56	-10,56	-11,05	8
9	-5,1	-5,02	-5,18	-5,02	-4,68	-4,04	-3,64	-3,43	-2,5	-2,43	-4,53	-4,1	-2,45	-2,14	-1,53	-3,19	-5,43	-4,96	-4,35	-6,33	-6,04	-7,21	-7,68	-8,84	-8,62	-9,02	-9,64	-9,85	-10,98	-11,05	-11,53	9
10	-6,86	-6,31	-6,16	-5,26	-5,19	-4,95	-5,31	-4,19	-4,97	-5,76	-5,91	-6,03	-6,15	-5,44	-6,2	-6,56	-6,81	-6,21	-7,15	-7,58	-7,95	-8,34	-8,16	-9,21	-9,42	-9,85	-10,41	-10,85	-11,09	-11,15	-11,67	10
11	-7,38	-6,98	-7,18	-7,16	-7,01	-6,13	-6,87	-7,19	-7,09	-6,45	-5,94	-6,67	-6,13	-6,78	-7,54	-8,14	-8,24	-8,65	-8,15	-9,42	-9,57	-9,24	-9,35	-9,76	-10,52	-10,26	-10,79	-11,2	-10,89	-11,63	-11,86	11
	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	B	D	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	