Středoškolská technika 2013

Setkání a prezentace prací středoškolských studentů na ČVUT

ČIPOVÝ PŘÍSTUPOVÝ SYSTÉM

Zbyšek Kubát

Střední průmyslová škola elektrotechnická
Ječná 3é, Praha 2 – Nové Město

Vedoucí práce: Ing. Vladimír Beránek

Konzultant: Bc. Štěpán Fučík

Prohlášení

Prohlašuji, že jsem svou práci vypracoval samostatně, použil jsem pouze podklady (literaturu, SW atd.) uvedené v přiloženém seznamu a postup při zpracování a dalším nakládání s prací je v souladu se zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) v platném znění.

V Praze dne 20. 2. 2013
podpis: ……

Poděkování

Děkuji Ing. Vladimírovi Beránkovi a Bc. Štěpánovi Fučíkovi za obětavou pomoc a podnětné připomínky, které mi během práce poskytovali.

Obsah

1 Úvod

Jako téma odborné maturitní práce jsem si vybral projekt *„Návrh a realizace čipové systému otevírání dveří do laboratorních prostor*“.

Starý systém byl nevyhovující z důvodu komplikovaného návratu studenta do laboratoří. Obsahoval telekomunikační systém mezi vstupními dveřmi do učeben laboratoří a kabinetem profesorů a vlastní ovládaní dveří pomocí elektrického otvírače dveří, který musel aktivovat profesor z kabinetu. Časté otevírání dveří studentům rušilo profesory připravující se na výuku. Navíc, při nepřítomnosti profesora v kabinetu nemohl být ani student vpuštěn zpět.

Požadavky na tento projekt byly následující:

- Použití kitu STM32 F100RB … jako hlavní řídící prvek systému.
- Použití školních karet pro identifikaci studenta.
- Praktická aplikace.
- Zachování stávajícího dálkového otevírání z kabinetu
- Snadná aktivace/deaktivace zařízení

2 Obecná realizace problematiky

2.1 Teoretický rozbor

Tato práce vznikla z důvodu nutnosti řešení problému nevyhovujícího systému vstupu studentů do laboratorních prostor.

2.1.1 Popis současného systému

V současné době jsou vstupní dveře do laboratorních prostor opatřeny klikou pouze z vnitřní strany dveří. Toto zabezpečení však komplikuje návrat studenta, který o přestávce opustil laboratoře. Aby byl takový student opětovně vpuštěn, musí použít zvonek do kabinetu profesorů. Ti pak studentovi dveře dálkově otevřou pomocí elektrického otvírače. Ovšem tento současný stav nevyhovuje jak studentům, tak samotným profesorům. Tento systém s sebou přináší značné nevýhody:

- Pro profesora je časté vpouštění studentů tímto způsobem velmi rušivé.
- Pokud v kabinetu nikdo z profesorů není, studentovi nezbývá, než čekat před dveřmi.

2.1.2 Popis nového systému

Cílem této práce je navrhnout, zkonstruovat a nainstalovat čipový systém otevírání dveří, který by odstranil nevýhody současného systému.

Návrh je založen na dvou čtečkách čipových karet, které komunikují s mikroprocesorem. První čtečka je umístěna na vnitřní straně dveří a posílá v podobě elektronických impulzů signál z přiložené čipové karty do paměti procesoru. Při příchodu studenta druhá čtečka, umístěná z venku dveří, načítá signál z přiložené čipové karty do mikroprocesoru, který porovná číslo této karty s čísly karet uloženými v paměti. Pokud se najde shoda čísel, mikroprocesor sepne relé a tím otevře dveře do laboratorních prostor.

2.1.3 Stanovení požadavků čipového systému otevíraní dveří

Na začátku byly stanoveny tyto požadavky:

- **Použití kitu STM32 F100RB** - jako hlavní řídící prvek systému

Využití tohoto kitu bylo požadováno především pro názornou aplikaci těchto mikroprocesorů ostatním studentům, kteří se s nimi učí pracovat (programovat) ve výuce. Navíc je zde možnost v rámci výuky tento systém dále zdokonalovat.

- **Využití školních karet pro identifikaci studenta**

Bylo požadováno využití studentských průkazu ISIC. Jelikož tyto ISIC karty vlastní každý student na škole a zároveň je již škola využívá pro evidenci příchodu/odchodu studentů. Tento systém funguje na základě technologie RIFD.

RFID (**R**adio **F**requency **I**n**D**entification) je metoda identifikace založená na radiové komunikaci mezi čtečkou a identifikačním prvkem – tagem RFID. Čtečka vysílá rádiový signál, tag odpovídá vysíláním svého identifikačního čísla (unikátní identifikátor daného RFID), popř. odesláním obsahu své datové paměti.

- **Praktická realizace**

  Umístění čipového systému na vnitřní straně vstupních dveří do učeben laboratoří. Krabice bude vyrobená z průhledného plexiskla tak, aby si každý student, který přijde do styku s tímto zařízením, mohl prohlédnout hardware zařízení.

- **Zachování stávajícího dálkového otevírání z kabinetu**

  Jelikož tato aplikace vpouští zpátky do laboratorních prostor, pouze studenty, kteří si načtou svoji identifikační kartu z vnitřní strany dveří, je nutné zachovat stávající dálkové otevírání z kabinetu pro vpuštění návštěv a studentů při začátku výuky v laboratořích.

- **Snadná aktivace/deaktivace zařízení**

  Tento požadavek je nutný kvůli bezpečnosti. Je nutné, aby v žádném případě nemohli studenti vstoupit do laboratorních prostor v době, kdy se v prostorách nenachází žádný profesor. Proto začátkem výuky profesoři aktivují zařízení a po skončení výuky jej deaktivují. Jelikož tuto operaci budou profesoři pravidelně provádět, je nezbytné, aby tato aktivace/deaktivace byla jednoduchá.

3 Použité technologie

3.1 Technologie RFID

(Radio **F**requency **I**n**D**entification**)** jedná se o bezkontaktní identifikaci sloužící k přenosu a ukládání dat pomocí elektromagnetických vln. Systémy radiofrekvenční identifikace (RFID) jsou schopny:

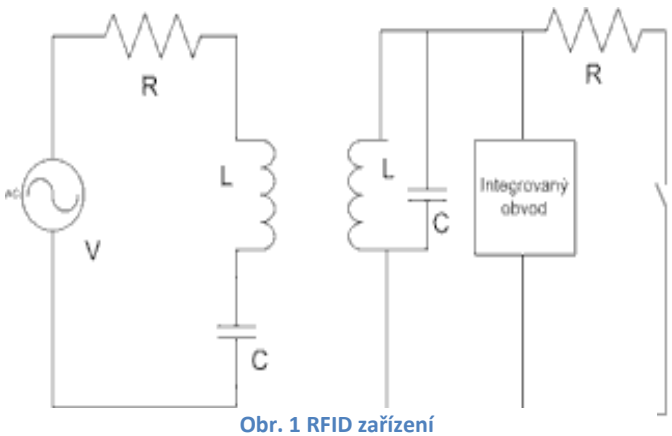
- zaznamenávat
- uchovávat
- poskytovat objektivní informace o objektech v reálném čase

Mezi hlavní výhody RFID patří:

- bezkontaktní povaha technologie, která nevyžaduje pro identifikaci objektu jeho přímou viditelnost, ani přesné polohování
- přenosu dat z čipu nebrání ani špatné optické či atmosférické podmínky
- rychlost čtení
- aktivní technologie pak přináší nové možnosti funkcionality identifikačního procesu

Tuto technologii lze najít v různých odvětvích průmyslu, jako je kontrola výrobních procesů, logistika, dodávky a expedice, v obchodních řetězcích, ale i v identifikaci zvířat, ať už jde o jednotlivé domácí mazlíčky, tak i velké stáda dobytku. RFID systémy najdete rovněž i v automobilovém průmyslu, pivovarnictví (sledování pivních sudů) ve zdravotnictví. Dá se říci, že RFID zvyšuje kvalitu, rozšiřuje možnosti procesu identifikace ve všech oblastech a odvětvích průmyslu, bezpečnosti, dopravy atd.Funkce RFID

RFID je technologie **bezkontaktní identifikace** – k identifikaci (získání identifikačního kódu) není nutné, aby čtečka kódu přišla do přímého kontaktu s identifikátorem (jako je tomu například u čipových či magnetických karet), dokonce nemusí být ani v přímé viditelnosti. Samotné identifikátory jsou jednoduchým elektronickým obvodem (energii pro funkčnost získávají z energie vysílače, tj. snímacího zařízení).



Obr. 1 RFID zařízení

Čtecí zařízení (obr. 1) prostřednictvím antény vysílá periodicky na svém nosném kmitočtu elektromagnetickou vlnu (rádiovou vlnu) do okolí. Objeví-li se ve vhodné vzdálenosti od antény tag, který je naladěn na stejnou frekvenci, je tato vlna přijata anténou tagu. Indukované napětí na anténě tagu, vyvolá střídavý elektrický proud, který je usměrněn a nabíjí kondenzátor v tagu. Uložená energie je použita pro napájení logických a rádiových obvodů tagu. Když napětí na kondenzátoru dosáhne minimální potřebné úrovně, spustí řídící obvody uvnitř tagu a ten začne odesílat odpověď čtecímu

zařízení. Vysílání tagu je realizováno zpravidla pomocí dvoustavové ASK (Amplitude Shifting Key) modulace, která je realizována změnou zakončovací impedance antény transpondéru (anténa je buď přizpůsobena, nebo zakončena nakrátko). Modulace představuje důkladné ovlivňování tří parametrů signálu, a to je výška, frekvence a fáze amplitudy. Analýzou těchto vln kdekoliv v dosahu čtečky můžeme zpětně zrekonstruovat demodulací zprávu vyslanou tagem. Dostatečná energie pro nabití kondenzátoru v transpondéru a schopnost detekovat přijatou odpověď transpondéru čtečkou jsou tak hlavní hardwarové podmínky pro fungování RFID systému. S rostoucí vzdáleností mezi čtečkou a transpondérem postupně klesá kvalita RFID signálu. Narůst šumu v základním signálu vede až k nemožnosti úspěšné detekce přijaté zprávy.

3.1.1 Vznik technologie RFID

Samotná technologie vychází z principu radaru a její historie zasahuje až do 20. let minulého století, kdy se k navigaci letadel se začaly používat rádiové vysílače, tzv. radiomajáky. V roce 1935 skotský elektrotechnik sir R. Watson-Watt zkonstruoval první prakticky použitelný přístroj pro rádiovou detekci letadel pomocí mikrovln. Stal se tak skutečným vynálezcem radaru. Z roku 1939 pochází technologie podobná RFID tzv. IFF (Identification, Friend and Foe (přítel a nepřítel)), používaná za války k odlišení vlastních a nepřátelských letadel.

Vývoj radaru a rádiových komunikačních systémů pokračoval v letech 1950 až 1960, kdy probíhalo testování, a vyvíjely se aplikace, které by mohly být využity v praxi. První aplikace, které byly uvedeny do praxe, byly založeny na jednobitových čipech, které signalizovaly, zda jsou či nejsou funkční. Toto řešení slouží například jako systém proti krádežím v obchodech.

Roku 1970 si nechal Mario Cardullo patentovat vysílací zařízení s pamětí a dalšími funkcemi RFID čipu. První skutečný RFID čip předvedla americká Los Alamos Scientific Laboratory roku 1973. V sedmdesátých letech se na vývoji podílela řada firem, mimo jiné IBM, ComServ a FairChild. Od roku 1980 až 1990 začaly vznikat komerční aplikace (např. bezkontaktní karty, sloužící k identifikaci vstupů do budov, lyžařských vleků, mýtné brány atd.). V devadesátých letech, s vytvořením prvních standardů, nastaly podmínky pro mezinárodní využívání RFID.

3.1.2 Systém RFID

Komponenty RFID systému patří:

- **Transpondér** (RFID tag) je tvořen čipem, což je elektronický paměťový obvod, cívkou či anténou a v případě aktivních nebo semipasivních tagů, je vybaven i vlastním zdrojem energie (baterií). Všechny tyto součásti jsou pak umístěny na vhodně konstruované podložce z plastu nebo papíru.

Obr. 2 Pasivní RFID karta

- **Čtecí zařízení** (obr č.3) tzv. RFID reader (nebo také čtečka), které je tvořena vysílacím/přijímacím obvodem s dekodérem, anténou. V některých případech může být čtečka vybavena i vlastním operačním systémem se základní softwarovou funkcionalitou.

Obr. 3 Čtecí zařízení

- **Řídící software** (middleware)

3.1.3 Frekvence a standarty

Systémy RFID využívají elektromagnetických vln, které pracují na různých vlnových délkách. Pracovní kmitočet je určujícím parametrem pro čtecí dosah a interakci s okolním prostředím. Platí, že čím vyšší frekvence je použita, tím je rychlejší přenos dat a větší vzdálenost na kterou je RFID čtečka schopna komunikovat s RFID tagem. Nevýhodou je však vyšší cena a větší citlivost na přítomnost problematických materiálů (uhlík, kovy a kapaliny), které výrazně ovlivňují šíření rádiových vln. Volba vhodné frekvence je tedy pro konkrétní aplikaci jedna z nejdůležitějších fází návrhu řešení systému RFID.

Existují čtyři hlavní frekvenční pásma pro systémy RFID.

- **LF** (**L**ow **F**requency) 125 - 134 kHz
  Frekvenční pásmo LF má velmi krátkou (téměř kontaktní) čtecí vzdálenost (do cca 20 cm) a nízkou přenosovou rychlost. Tato technologie se využívá převážně v identifikačních průkazech (evidence docházky), v průmyslu k identifikaci komponentů v zařízení během výroby, k identifikacím pivních sudů, na evidenci domácích zvířat atd. Využívá se pasivních tagů.

- **HF** (**H**igh **F**requency) 13,56 MHz
  Toto pásmo má vyšší čtecí vzdálenost než LF (do cca 1 metru). Tento systém využívá opět především pasivních tagů. Má nižší přenosovou rychlost ale poskytuje v přítomnosti kovu a tekutin vysokou spolelivost. Anténa tagu je vyrobena z měděného drátu nebo může být vytištěna vodivým inkoustem na papírovou podložku a doplněná čipem. V této kategorii jsou čipy většinou k dispozici ve variantách RO (Read Only – pouze čtení) nebo RW(Read Write – možnost zápisu) s kapacitou paměti od několika bytů až po kilobyty. Tato technologie se nejčastěji využívá pro knihovní systémy, docházkové systémy, pro identifikační karty (e-peněženky, přístupové systémy).

- **UHF** (Ultra High Frequency) 433, 868 nebo 915 MHz
  UHF pásmo umožňuje přenos informace na vzdálenosti jednotek metrů. Systémy UHF v různých zemích světa mají přiděleny různá frekvenční pásma. U této technologie se využívá standard ISO 18000 určený pro knihovní systémy, docházkové systémy, identifikace palet.

- **MW** (Mikrovlnné vlny) 2,45 nebo 5,8 GHz
  - MW pracuje v blízkosti frekvenčního pásma často používaných Wi-Fi sítí. Charakteristickým znakem této technologie je velká čtecí vzdálenost a vysoká přenosová rychlost, ale s velmi špatným výkonem v přítomnosti kovu a tekutin. Tato frekvence je spjata s aktivními tagy, protože vlastní zdroj energie tagu dokáže zvýšit čtecí vzdálenost až na desítky metrů. Využívají se např. pro identifikace vozidel, pohybujících se předmětů, mýtné systémy a řízení vozového parku

Aby to nebylo tak jednoduché, existují ještě standardy definující komunikační protokol pro přenos dat mezi čtečkou a tagem, ale také pro obsah paměti tagu nebo i zabezpečení informací uložených v tagu. Podrobnosti o kmitočty, přenosové rychlosti, protokoly a kódy jsou definovány v ISO. Zatím to jsou následující normy:

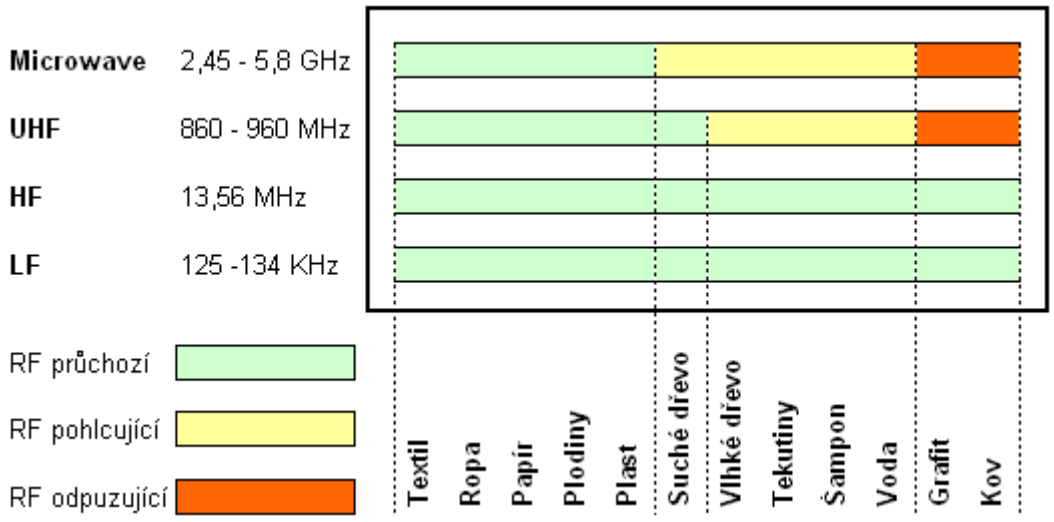
- **ISO 14223** Elektronická identifikace zvířat
- **ISO / IEC 14443** Identifikační karty – pro osobní identifikaci, elektronické jízdenky
- **ISO / IEC 18000-1** identifikace zboží
- **ISO / IEC 18000-2** Informační technologie AIDC - technika, identifikace zboží. Parametry pro komunikaci na frekvencích pod 135 kHz
- **ISO / IEC 18000-3** Informační technologie AIDC – technika. Parametry pro letecké komunikační rozhraní na 13,56 MHz
- **ISO / IEC 18000-4** Informační technologie AIDC technika, identifikace zboží. Parametry pro komunikační rozhraní ve vzduchu na frekvenci 2,45 GHz

- **ISO / IEC 18000-5** Informační technologie AIDC technika, identifikace zboží. Parametry pro letecké komunikační rozhraní na 5,8 GHz
- **ISO / IEC 18000-6** Informační technologie AIDC - technika, identifikace zboží. Parametry pro komunikaci o frekvencích 860 až 930 MHz
- **ISO / IEC 18000-7** Informační technologie AIDC - technika, identifikace zboží. Parametry pro letecké komunikační rozhraní na 433 MHz

3.1.4 Zranitelnost RFID systémů

RFID systémy jsou náchylné k rušení od jiných rádiových systémů. RFID systémy pracující v pásmu LF jsou zvláště zranitelné, protože rádiové signály z jiných komunikačních systémů, působí na téměř stejné frekvenci. Na druhém konci spektra, mikrovlnné systémy jsou nejméně citlivé na rušivé vlivy.

Výkonnost systémů RFID v pásmu HF jsou vzhledem k jejich relativně dlouhé vlnové délce, lépe schopny proniknout do vody, než UHF a MW signály. Signály vysokých frekvenci mají větší šanci být absorbovány v kapalině. Rovněž kov je elektromagnetický reflektor, kterým rádiové signály nemohou proniknout. V důsledku toho kovy nejen brání komunikaci, nacházejí-li se mezi tagem a RFID čtečkou, ale i samotná přítomnosti kovu může mít negativní vliv na fungování systému (dochází k nežádoucím odrazům a tím i vzniku stojatého vlnění). Vysoká frekvenční pásma jsou ovlivněna kovy víc než nižší frekvence pásma (Obr. 4).



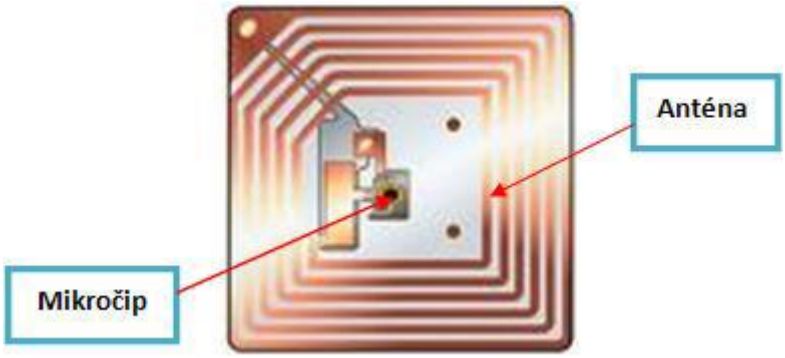
Obr. 4 Interakce systémů RFID se vzorovými materiály

Nevhodné označení plechovky nebo plastové láhve s kapalinou, stejně jako nevhodné umístění antén může znamenat problémy se čtením. Proto se musí dbát na správnou instalaci čteček a na návrh infrastruktury sítě RFID i na způsob umístění RFID tagů (nejčastěji se používá nálepka v kombinaci RFID tagu a čárového kódu – označujeme jako Smart Label). Podmínkou úspěchu je vhodný výběr druhu antén pro čtečku, zvolení jejich počtu a vzájemného rozmístění, popřípadě použití několika čteček na jednom místě pro lepší pokrytí.
Mezi základní kritéria ovlivňující výkonnost systému patří:

- přítomnost problémových materiálů
- nevhodné frekvenční pásmo
- špatné umístění jednotlivých komponenty RFID systému
- rušení jiných zařízení vydávající elektromagnetické vlnění va stejném frekvenčním pásmu (elektromagnetická kompatibilita EMC)
- neporozumění problematice značení objektů pomocí RFID systému

3.1.5 RFID tag

Nosičem informací v **RFID** (**R**adio **F**requency **InD**entification**)** se nazývá RFID tag, jinak také transpondér, jehož význam vznikl sloučením anglických slov transmit - přenos a response - odpověď. Základní funkcí RFID tagu je uložení dat do vnitřní paměti a poskytnutí těchto uložených údajů RFID systému.
Každý tag se skládá z mikročipu a antény (Obr. 5). Samotný čip může být velký pouze 1 mm (dnes i méně). Velikost tagu přímo souvisí s velikostí antény, která je jeho největší součástkou. Obvykle platí, že čím vyšší je použitá frekvence, tím menší může být anténa.



Obr. 5 RFID tag

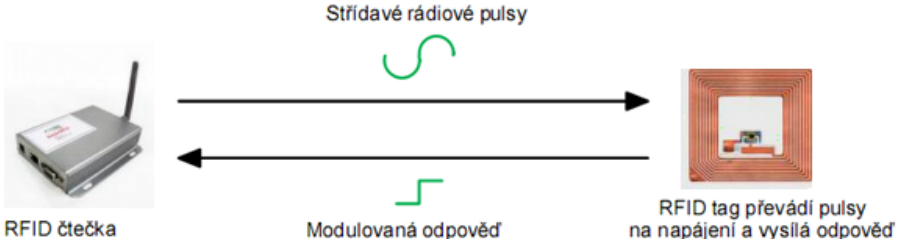
Anténa a čip mohou být zapouzdřeny do PVC karty velikosti kreditní karty, skleněné trubičky (jako subdermální aplikaci značení domácích mazlíčků), nebo nalepení na plochu etikety. Mohou být ale i speciálně zapouzdřeny podle požadavku zákazníka a způsobu použití. Je tak možné vyrobit RFID tagy odolné pro teploty od -40°C do +300°C.

Dělení RFID tagu:

- Pasivní RFID systémy
- Aktivní RFID systémy

Pasivní RFID tag

RFID tag neobsahuje vlastní zdroj energie a je závislý na dodávce energie z antény čtecího zařízení. Čtecí zařízení šíří pomocí antény elektromagnetické pole, které slouží jako zdroj energie pro RFID tag a také jako komunikační kanál ve směru od čtecího zařízení k RFID tagu viz Obr. 6. Primárním účelem nasazení pasivního RFID je identifikace objektů.



Obr. 6 Komunikace mezi pasivním tagem a RFID čtečkou

Aktivní RFID tag

U aktivního RFID nejde pouze o identifikaci předmětů, ale i o další funkce jako například (lokalizaci, měření teploty a podobně). Na rozdíl od pasivního tagu obsahuje vlastní zdroj napájení, který zajišťuje jeho činnost nezávisle na čtecím zařízení. Může obsahovat také snímače pro měření fyzikálních veličin. Často je vybaven optickou nebo akustickou komunikací s uživateli. Jedno z praktických použití je v případech domácího vězení, kdy tento čip komunikuje se čtečkou v místě bydliště či zaměstnání a softwarová aplikace potom analyzuje standardní a nestandardní chování.

Obr. 7 Komunikace mezi aktivním tagem a RFID transceiverem

3.2 NFC

NFC (Near field communication) slouží k bezdrátové komunikaci mezi elektronickými zařízeními na krátkou vzdálenost, obvykle přiblížením zařízení do vzdálenosti jednotek centimetrů. Současné a předpokládané využití této technologie je především v bezkontaktních transakcích, výměně dat či třeba ve zjednodušené konfiguraci zařízení (Wi-Fi). Technologie NFC se především využívá ve vzájemné komunikaci aktivních zařízení s pasivními zařízeními. Pro příklad můžeme uvést vzájemnou komunikaci bezkontaktní karty (pasivní zařízení) a její čtečky (aktivního zařízení). NFC technologie je popisována standardy, které zahrnují několik komunikačních protokolů a formátů popisujících přenášená data. Je založena na standardech RFID zahrnující ISO/IEC 14443 a FeliCa. Tyto standardy jsou definované neziskovou organizací NFC Fórum, jež byla založena v roce 2004 firmami Nokia, Philips a Sony. Nyní tato organizace čítá přes 160 členů, v současné době prosazuje NFC a certifikuje zařízení na shodu s definovanými standardy.

NFC je sada bezdrátových technologií krátkého dosahu, pracující obvykle na vzdálenostech do 4cm. Na nejnižší vrstvě je NFC definováno skupinou standardů bezkontaktních karet, mezi které patří standardy bezkontaktních čipových karet ISO/IEC 14443, JIS X 6319 pod názvem FeliCa a ISO/IEC 15693. První dva zmíněné standardy (ISO/IEC 14443 a JIS X 6319) operují na frekvenci 13,56 MHz a na ISO/IEC rádiovém rozhraní a s obvyklými přenosovými rychlostmi od 106 kbit/s do 424 kbit/s. Výjimkou je standard ISO/IEC 15693, jehož použitelná vzdálenost dosahuje oproti dvěma předchozím standardům vzdálenostem výrazně větším, a to až do vzdálenosti 1,5 metru. S touto vzdáleností však musíme počítat s razantním poklesem přenosových rychlostí, jedná se o rychlosti do 26 kbit/s. Rozšíření standardu pro potřeby technologie NFC je specifikováno pomocí standardů NFCIP, které rozšiřují standard ISO/IEC 14443 o další technické specifikace, jenž definuje komunikaci mezi dvěma NFC zařízeními, a je znám jako ISO/IEC 18092.

3.2.1 Historie

Počátky technologie NFC se datují do doby vzniku technologie RFID. RFID umožňuje čtečce, aby vysílala rádiové vlny k pasivnímu, elektronickému tagu, pro identifikaci, autentizaci a sledování.

- 1983 - první patent byl asociován se zkratkou RFID, který byl přidělen Charlesu Waltonovi.
- 2004 - firmy Nokia, Philips a Sony založily neziskovou organizaci NFC Forum.
- 2006 - Byly vytvořeny počáteční specifikace pro NFC tagy.
- 2006 - Byly vytvořeny specifikace k "SmartPoster" záznamům.

- 2006 - Prvním telefonem podporujícím NFC byla Nokia 6131.
- 2009 - V lednu roku 2009 byly NFC fórem vytvořeny standardy pro přenos kontaktů, URL, iniciaci Bluetooth a další.
- 2010 - Samsung Nexus S: prezentován první Android telefon podporující NFC
- 2011 - Google I/O "How to NFC" demonstruje NFC k zahajování her a sdílení kontaktů, URL, aplikací, videí, a další.
- 2011 - Podpora NFC se stává součástí operačního systému Symbian ve verzi Symbian Anna.
- 2011 - RIM 2011 je první firmou, jejíž zařízení jsou certifikovány pro funkcionalitu MasterCard Paypass, a to firmou MasterCard WorldWide.
- 2012 - V březnu roku 2012 řetězec britských restaurací EAT a firma Everything Everywhere (partner mobilního operátora Orange Mobile) vytvořili první celonárodní kampaň k NFC ve Velké Británii skrze SmartPostery.
- 2012 - Sony uvádí "Smart Tags", které používají NFC technologii pro změnu režimů a profilů na smartphonech Sony.

3.2.2 NFC tagy

NFC tagům se říká pasivní z jednoho jediného důvodu: nevyžadují žádné napájení. To ale není tak úplně pravda, bez energie by samozřejmě nefungovaly, pouze nejsou napájeny přímo. Elektřinu jim totiž dodává například právě telefonem. Tagy využívají stejné technologie jako RFID tag, proto se mohou obejít bez externího napájení. NFC tagy se hlavně liší tím, jaký je v nich použitý čip. Výrobců samotných tagů je sice spousta, ale firem, které umí vyrábět čipy, zas tolik není. V podstatě uslyšíte jen o nizozemské společnosti NXP (odštěpená v roce 2006 od společnosti Philipsu), která dodává čipy téměř všem. Mimochodem společnost má větší tržby, než třeba Nvidia.

Důležitým faktorem je to, že NFC je zpětně kompatibilní s RFID tagy, které odpovídají normě ISO/IEC 14443, a která se ještě dále dělí na typ A a B. Jinak by totiž nekomunikovaly na frekvenci 13,56 MHz, a to je důležitým faktorem pro telefon, který nezvládne jinou frekvenci. Možná už jste tak někdy slyšeli o čipech **Mifare.** MIFARE je vlastněná ochranná známka ze série čipů široce používán v bezkontaktních čipových kartách. Název MIFARE zahrnuje patentované technologie založené na normě ISO / IEC 14443 a frekvenci 13,56 MHz pro bezkontaktní čipové karty, které jsou právě marketingovou značkou společnosti NXP pro RFID tagy. Kromě toho si ale NFC poradí třeba i se standardem od společnosti Sony pojmenovaném FeliCa (JIS X 6319-4), který už do normy ISO/IEC 14443 přijat nebyl. Jde ale o technologii používanou převážně v Japonsku, takže nás to tady v Evropě nemusí až tak trápit.

NFC Forum definovalo čtyři formáty tagů určených už přímo pro NFC. Tři z nich jsou postaveny právě na normě ISO/IEC 14443 a jeden podle FeliCa. Tagy přidávají možnost uzamknutí, takže poté co se do tagu něco zapíšete, nebude už možné jej změnit. To se hodí ve chvíli, kdy jej potřebujete umístit na veřejně přístupné místo. Liší se kapacitou i přenosovými rychlostmi.

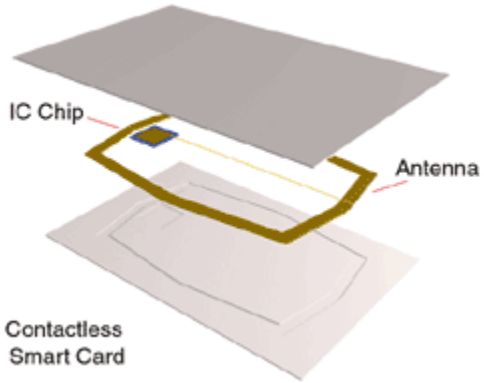
- **Typ 1** je postaven na standardu ISO/IEC 14443 A, je možné jej používat v režimu čtení/zápis nebo jej uzamknout pouze pro čtení. Kapacita tagu je od 96 bajtů až do 2 kilobajtů, přenosová rychlost 106 Kb/s. Výhodou je nízká cena.
- **Typ 2** je shodný s prvním typem, minimální kapacita je ale menší: 48 bajtů.
- **Typ 3** je postaven na japonském standardu FeliCa, ovšem režim čtení/zápis nebo jen čtení se nastavuje už při výrobě. Kapacita je variabilní, teoretický limit je až 1 MB, rychlost je 212 nebo 424 Kb/s. Cena je tentokrát vyšší.
- **Typ 4** je kompatibilní se standardem ISO/IEC 14443 A i B, tag se při výrobě konfiguruje v režimu čtení/zápis nebo pouze čtení. Kapacity jsou už větší a pohybují se v kilobajtech, maximální velikost je 32 kB, rychlost je pak 106 nebo 424 Kb/s.

3.2.3 MIFARE

Tag ze skupiny MIFARE si můžete představit jako takovou bezdrátovou paměťovou kartu. Na rozdíl od nich mají ale výrazně menší kapacitu, rozhodně nečekejte, že byste si na tag mohli uložit třeba film. I ty největší tagy mají kapacitu v jednotkách kilobajtů, takže byste na ně nenahráli ani několikapixelový obrázek.

Za to se tam dá ale uložit třeba webová adresa, vizitka s kontakty, identifikační číslo nebo krátká zpráva. A to už předurčuje, k čemu se čipy ze skupiny MIFARE používají:

- Jízdenky a předplacené kupony pro MHD
- Občanské a řidičské průkazy, pasy
- Docházkové a věrnostní karty
- Klíče, vstupní karty a žetony
- Vizitky
- Reklama



Obr. 11 Pasivní RFID karta

Zařízení se dělí do dvou základních skupin:

- Zařízení s vlastním napájením označujeme jako aktivní zařízení. Navíc díky tomu může být toto zařízení iniciátorem komunikace
- Zařízení bez vlastního napájení označujeme jako pasivní zařízení. Tato zařízení jsou v komunikaci napájena aktivním zařízením. a nemohou iniciovat komunikaci

Určitě by vás napadla celá řada dalších použití. Tag ze skupiny MIFARE si totiž můžete vyrobit i vlastní, čehož využívají některé chytré aplikace. Můžete si tak na čip ze skupiny MIFARE zapsat třeba to, že chcete nastavit budík na sedm hodin ráno. Čip si pak nalepíte na noční stolek, a když na něj telefon večer položíte, ráno vás probudí.

3.2.4 Datový formát NDEF

Když už tag máte, máte několik málo volných bajtů paměti, kam můžete zapsat data. Aby jim ale také rozuměl ten, kdo si je bude číst, NFC Forum zároveň se specifikacemi NFC tagů vytvořilo i nový datový formát NDEF (zkratka NFC Data Exchange Format). NDEF je definicí obecného formátu tagu, pod sebou má ale několik už konkrétních šablon na data. Jde zejména o text a webovou adresu (URI), pak je zde ještě formát Smart Poster, který se bude užívat hlavně v marketingu. Po dotyku se dozvíte bližší informace a telefon může vykonat nějakou akci, například načíst web nebo poslat SMS. Nakonec je tady ještě nezbytný elektronický podpis. U těchto věcí by tak mělo být zaručeno, že i když na tag zapíšete něco z Androidu, bez problémů tag přečte a správně interpretuje třeba i Symbian. Z dosavadních zkušeností se ale dá říct, že to tak funguje i u mnoha dalších formátů, kde se jakési nepsané standardy dodržují. Na druhou stranu, některé proprietární tagy, jako třeba Xperia SmartTags od Sony, v sobě mají pouze unikátní ID a NDEF formát zde nehraje žádnou roli. Právě to je totiž dalším dělícím prvkem tagů. Ty určené přímo pro NFC obvykle dostanete už předformátované do NDEF formátu, ty zaměřené spíš obecně na RFID technologii (například Mifare Classic) si musíte naformátovat ručně.

Proč to všechno? Kromě toho, že je nutností, aby měl tag nějaký standardizovaný formát, se tím ušetří poměrně mnoho dat. Když si vezmete, že běžné tagy mají kapacitu okolo 150 bajtů, každý ušetřený bajt se hodí. V URI adresách se tak ušetří pár pěkných znaků třeba tím, že jsou protokoly předdefinované ve specifikacích a na tagu fyzicky žádné http:// zapsané není.

3.2.5 Co umožňuje technologie NFC

NFC (je zkratka pro **Near Field Communication**). Technologie NFC umožňuje:

- Pomocí technologie NFC můžeme nahradit všechny **klíče**, ať už ty fyzické, tak i ty virtuální. Od *auta,* od *domu,* od *garáže,* 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.

- NFC umožňuje spojení fyzického a virtuálního světa. Představte si, položíte si telefon večer na noční stolek a automaticky se

ztlumí zvuk a nastaví budík. Nebo si v obchodě bez námahy zjistíte kompletní parametry zboží ťuknutím na jeho cenovku.

- *NFC usnadňuje komunikaci m*ezi telefony a počítači (nebo tablety) nebo mezi telefony a příslušenstvím. Stačí dotyk a už máte fotku, kterou jste právě měli na displeji, promítnutou na zdi projektorem. A co třeba připojení bezdrátového headsetu jen tím, že ho prostě přiblížíte k telefonu.

3.2.6 Režim přenosu

Reader/Writer režim

Specifickými režimy pro čtení či zápis dat NFC čteček z tagů jsou režimy reader/writer. Tyto režimy vyhovují rádiovému rozhraní standardů ISO/IEC 14443 typu A, B a schémat FeliCa. V tomto režimu není vyžadována vysoká bezpečnost vzhledem k povaze komunikace, tj. není zde zapotřebí mít bezpečné, zašifrované úložiště dat, tzv. Secure element. Celý proces komunikace spočívá pouze v zápisu nebo čtení dat z/do pasivního čipu, tzv. NFC tagu. NFC tag je v obou případech napájen elektromagnetickým polem iniciátora. Maximální přenosová rychlost v režimu pro zápis je 106 kbit/s.

Příkazy a instrukce k řízení tagů NFC zařízeními jsou realizovány pomocí datového formátu NDEF (Data Exchange Format definuje formát zapouzdření zpráv pro výměnu informací mezi zařízeními respektujícími doporučení NFC fóra, tj. mezi dvěma aktivními NFC zařízeními, nebo aktivním zařízením a zařízením pasivním (tagem). Jedná se o binární formát zpráv, který může být použit k zapouzdření libovolných dat aplikačních protokolů do jedné zprávy.) a parametrů RTD k definici obsahu NDEF záznamů. Použití datového formátu NDEF však není pro aplikace vyžadováno.

3.2.7 Fyzická a linková vrstva NFC

ISO/IEC 14443

Bezkontaktní čipové karty, na nichž je založena technologie NFC, jsou popsány standardem ISO/IEC 1443. Veškeré NFC transakce, jako jsou libovolné přenosy dat mezi účastníky přenosu, jsou realizovány pomocí přenosu energie skrze elektromagnetickou indukci mezi dvěma smyčkovými anténami čipové karty a NFC čtečky (mezi stěžejní komponenty NFC čtečky patří mikrokontrolér a magnetická smyčková anténa pracující na frekvenci 13,56 MHz). V rámci tohoto standardu se běžně užívají pojmy PICC (Proximity Integrated Circuit Card) a PCD (Proximity Coupling Device), které představují zmíněné komponenty v rámci NFC transakce, a to PICC ve formě čipové karty (obsahující čip a smyčkovou anténu) a PCD ve formě NFC čtečky. Společně se standardem ISO/IEC 14443 existují i některé vzájemně kompatibilní standardy, z nichž nejznámější jsou MIFARE, Calypso a FeliCa.

Čipové karty, které se pro tyto podmínky používají, mohou nabývat rozměrů definovanými standardem pro rozměry identifikačních karet a jejich fyzickým vlastnostem, standardem ISO/IEC 7810, jehož nejpoužívanějším rozměrem je formát ID-1. Rozměry tohoto formátu používá většina identifikačních a platebních karet.

Standard ISO/IEC 14443, na němž staví bezkontaktní karty, definuje především základní elementy v komunikaci, základní požadavky, fyzické vlastnosti, maximální vysílací výkony a protokoly pro iniciaci komunikace, antikolizní protokoly a přenosové protokoly. Základní shrnutí tohoto standardu je v níže uvedené tabulce, která popisuje jednotlivé části tohoto standardu.

Část standardu	**Popis standardu**
Část 1 - Fyzikální charakteristiky bezkontaktních čipových karet	Definuje fyzikální charakteristiky bezkontaktních čipových karet a jejich požadavky na ně.
Část 2 - Vysílací výkony a signálové rozhraní	Definuje vysílací výkony, způsob napájení čipu z radiofrekvenčního magnetického pole, signalizační rozhraní, jejich signalizační schémata a typy modulací k oběma typům PICC (pro oba směry komunikace, a to jak pro aktivní a pasivní typ PICC)
Část 3 - Inicializační a antikolizní protokoly	Definuje inicializační a antikolizní protokoly pro oba typy PICC, společně s antikolizními příkazy, odpověďmi, datovými rámci a časováním.

Část 4 - Protokoly pro přenos	Určuje, které protokoly jsou určeny pro vysokoúrovňový přenos dat. Všechny tyto protokoly v rámci této části standardu jsou volitelné.

Standard ISO/IEC 14443 definuje dva typy komunikačních rozhraní, a to typ A a typ B. Jako dodatek k nim existuje rozhraní typu F z Japonského standardu JIS X 6319.

Rozhraní typu A používá ve směru čtečky (PCD) ke kartě (PICC) ASK modulaci se 100% hloubkou, jehož data jsou zakódována pomocí modifikovaného Millerova kódování. V opačném směru komunikace se používá OOK modulace s daty zakódovanými pomocí Manchester kódování. V tomto typu rozhraní se pole vypíná po dobu krátkých intervalů, kdy čtečka přenáší data.

Rozhraní typu B používá ve směru čtečky (PCD) ke kartě (PICC) ASK modulaci s 10% hloubkou, jehož data jsou zakódována pomocí kódování NRZ-L. Komunikace v opačném směru používá BPSK modulaci s daty zakódovanými pomocí NRZ-L.

3.2.8 Případy užití NFC

Platební systémy

Pro platební systémy využívající debetní či kreditní karty a čipové karty (tzv. Smartcards) může být alternativou, či kompletní náhradou, použití NFC technologie. Pro příklad můžeme uvést Google Wallet, který umožňuje zákazníkům uložit si informace o debetní/kreditní kartě do úložiště, tz. Google Wallet. Poté při jakékoli platbě u MasterCard PayPass terminálu můžete využít svůj mobilní telefon podporující NFC pro platební transakce. Německo, Rakousko a Itálie jsou státy, které již vyzkoušely a zavedly NFC jako způsob prodeje jízdenek pro veřejnou dopravu. Čína toto již běžně využívá v autobusech veřejné dopravy a Indie již zavádí pokladny podporující NFC transakce.

Výhody NFC v platebních systémech zahrnují jedny z následujících bodů:

- Vzhledem ke krátkému dosahu technologie NFC jsou transakce bezpečnější.
- Okamžité platby a doručování kupónů pomocí telefonů, podobně, jako je to realizováno pomocí kreditních nebo debetních karet.
- Platba za zboží jen mávnutím telefonu přes NFC čtečku.

Bluetooth a Wi-Fi připojení

Výhody velmi jednoduché konfigurace NFC, byť o nízkých přenosových rychlostech, mohou být využity ke konfiguraci složitějších bezdrátových připojení. Pro příklad můžeme uvést párování zařízení pomocí Bluetooth připojení, v němž při párování bude užito technologie NFC, zatímco pro přenos bude použita technologie Bluetooth. Další alternativou je také konfigurace Wi-Fi připojení (ačkoliv pro tyto případy zde existuje technologie Wi-Fi Protected Setup, která umožňuje také velmi jednoduchou konfiguraci Wi-Fi připojení).

Sociální sítě, kontakty

Další možností, jak využít technologie NFC, jsou situace, při níž se setkávají skupiny lidí. V těchto situacích pomocí technologie NFC může být sdílení kontaktů, fotografií, videí nebo souborů značně jednodušší.

Identifikace

NFC fórum má zájem o to, aby se potenciální NFC zařízení chovala jako elektronické identifikační karty a klíčenky. Vzhledem k tomu, že NFC je bezdrátová technologie krátkého dosahu a podporuje šifrování, tak je její použití mnohem výhodnější, než méně privátní RFID systémy.

3.2.9 Bezpečnostní aspekty NFC

Ačkoliv může být krátký dosah NFC technologie brán za jeden z bezpečnostních aspektů, tak NFC samotné nezabezpečuje komunikaci. V roce 2006 Ernst Haselsteiner a Klemens Breitfuß popsali různé typy útoků a ukázali, jak využít odolnost NFC vůči útokům typu Man-in-the-middle k získání specifického klíče. Zmíněná technika není součástí ISO standardu, NFC nenabízí nějakou ochranu proti odposlechu a může být proto zranitelné vůči modifikaci dat. 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 vícero úrovních: 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.

- **Odposlech** - Pomocí antén můžeme odposlechnout radiofrekvenční signál vysílaný zařízeními. Vzdálenost, z níž je schopen útočník odposlechnout signál, závisí na několika parametrech, a to především na použitém komunikačním režimu, kde u pasivních zařízení, které negenerují své elektromagnetické pole, je odposlech výrazně náročnější. Naopak je tomu u aktivních zařízení, kde odposlech můžeme realizovat i ze vzdálenosti několika metrů (sic jde o opravdu krátké vzdálenosti).
- **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 obtížnější úlohou je modifikace dat takovým způsobem, aby se zdála veškerá komunikace uživatelům jako nenarušená, validní. K modifikaci přenášených dat musí útočník modifikovat jednotlivé bity radiofrekvenčního signálu. Proveditelnost takového útoku (t. j., jestliže je možné změnit hodnotu bitu signálu z 0 na 1 nebo naopak) se vztahuje k hloubce amplitudové modulace. Jestliže jsou data přenesena modifikovaným Millerovým kódováním a hloubka modulace byla 100%, pak pouze některé bity mohou být modifikovány. 100% hloubka modulace nám umožňuje eliminovat pauzy v radiofrekvenčním signálu, ale neumožňuje generovat pauzy, kde pauzy nebyly. Proto pouze bity 1 následované bitem 1 mohou být změněny. Přenosem dat zakódovaných pomocí kódování Manchester s hloubkou modulace 10 % umožňujeme útočníkovi modifikovat data ve všech bitech signálu.

- **Přepojovaný útok** - Přepojované útoky jsou možné i na NFC zařízeních, jelikož tato technologie zahrnuje protokoly ISO/IEC 14443, které jsou na tyto útoky náchylné. V tomto typu útoku musí útočník přeposílat požadavky čtečky k oběti a poté vracet tyto odpovědi v reálném čase zpět, aby mohl úspěšně předstírat, že je čipová Smart karta oběti. Tyto útoky jsou podobné útokům Man-in-the-Middle.
- **Ztráta majetku** - Ztráta NFC RFID karty umožní nálezci pracovat s telefonem obvykle jako s jednofaktorovou autentizační entitou. Mobilní telefony chráněné PIN kódem jsou zařízení s jednofaktorovou autentizací. Možnost jak zabránit zneužití dat při ztrátě zařízení je možnost rozšířit tento typ zabezpečení o další nezávislý bezdrátový autentizační faktor, tj. další typ autentizace.
- **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.

3.2.10 Komunikační protokoly

V dnešní době, kdy se zvyšují nároky na ochranu soukromí a stým spojenou i ochranu osobních údajů jsou kladeny stále větší požadavky na zajištění aplikací a systémů, které přicházejí do styku s těmito údaji. Přístupový systém je jeden z mnoha systémů, kde je možné setkat se s takovými informacemi. S rozvojem nových technologií přicházejí nové možnosti a způsoby překonání používaných k zajištění ochrany osobních informací. Proto je logické, že jsou kladeny stále větší požadavky a nároky na funkčnost a zajištění všech částí systému. Nejzranitelnější prvkem přístupového systému jsou ty, se kterými přicházíme nejčastěji do kontaktu. Tedy čtečky identifikačních prvků, nebo biometrické údaje a samozřejmě jednotlivé identifikační prvky. Čtečky identifikačních prvků se nejčastěji setkávají se čtečkami přístupových karet, které se liší typem technologií čtení karet, zpracování údajů z karet a způsobem posíláním zpracovaných dat do přístupových panelů, nebo na server. Podle těchto kritérií se dělí čtečky na různé typy, kde každý má své výhody a nevýhody v oblasti zabezpečení osobních údajů. Jednou z těchto kategorií tvoří čtečky, které používají wiegand efekt. Tyto čtečky nejsou až tak rozšířené na Evropském trhu v porovnání s ostatními čtečkami, jako v USA odkud pocházejí. Tyto typy jsou však nahrazovány bezkontaktními čtečkami karet, kde identifikační karty mají určitou paměť a tedy je jejich možné využití kromě i v přístupu i v jiných systémech (např. stravovací systémy). Slovo wiegand se postupem času zažívalo pro používání v různých aplikacích, ale nejčastěji se vyskytuje v souvislosti s přístupovými systémy.

Může jít o už zmiňované čtečky wiegand karet a přístupové karty, které používají fyzikální princip Wiegand efektu pro získávání dat z karty, dále rozhraní pro komunikaci čtečky mezi přístupovým panelem, nebo protokolem na posílání dat po tomto rozhraní a podobně.

4 RFID čtečka (reader)

RFID reader (RFID čtečka) působí jako most mezi RFID tagem a řídícím počítačem. Vlastní RFID čtečky jsou v podstatě malé počítače, které se skládají se tří částí. Jedné nebo více antén, které mohou být integrované nebo externí. Rádiového rozhraní, které je zodpovědné za modulaci, demodulaci, přenos a příjem rádiového signálu. Vzhledem k vysoce citlivým požadavkům, RFID reader mají často oddělené cesty pro příjem a vysílání. Hlavním prvkem řídící jednotky je mikroprocesor, jehož úkolem je zpracovat data přicházející ze čtecího zařízení. K mikroprocesoru jsou připojeny pomocné obvody, díky nimž může mikroprocesor komunikovat jak se čtecím zařízením, tak s PC. Na trhu existuje trhu rozsáhlá paleta čtecích/zapisovacích jednotek, které plní několik základních funkcí.

- Dodávat energií pasivním tagům.
- Přečtení údajů, které obsahuje RFID tag.
- Zapsání dat do tagu (v případě Read-Write Tagů).
- Přenos dat z a do řídícího počítače.
- Popř. základní filtrace dat nebo ovládání integrovaných vstupně/výstupních obvodů).

Kromě plnění výše uvedených základních funkcí, je schopna složitější RFID čtečka provádět další důležité funkce:

- Provádění antikolizních opatření k zajištění RW komunikace s mnoha tagy najednou.
- Ověřování tagů, aby se zabránilo podvodům nebo neoprávněnému přístupu k systému, šifrování, ochrany dat.

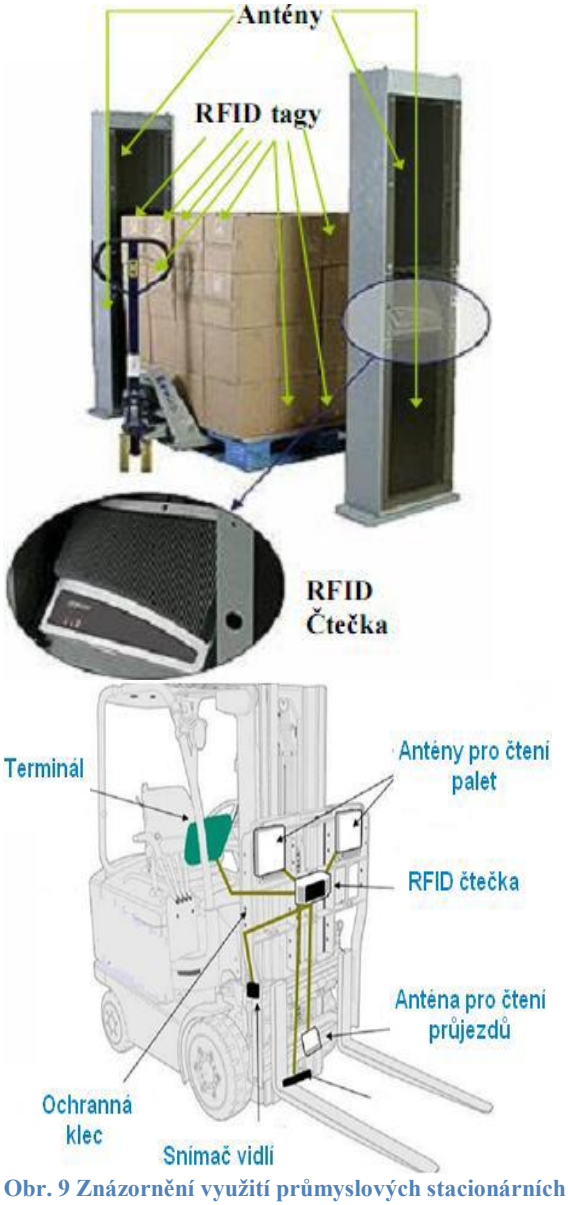
Dělení RFID čteček:

A podle toho je členíme na stacionární a mobilní a čtečky s poduškovými anténami, s bránovými anténami (jednostranné a dvoustranné) a tunelové jednotky s uspořádáním dvou horizontálních a dvou vertikálních antén.

Stacionární čtečky

Jsou pevně vestavěné v určeném identifikačním bodu například vstup do skladu, začátek dopravníku, stůl na přípravu produktů (Obr. 8).

Obr. 8 Stacionární RFID čtečka



Obr. 9 Znázornění využití průmyslových stacionárních RFID čteček

Mobilní čtečky

Jsou k dispozici jako zařízení pro držení v ruce. Mohou být použity bez kabelu s dokovací stanicí k odesílání či nahrávání údajů, (je možné je použít i pro průmyslové čtení na výrobních linkách), nebo s kabelem přes sériové datové rozhraní

k osobnímu počítači. U ručních RFID čteček existují i zařízení schopná hybridního použití, která mohou jak snímat čárový kód, tak číst RFID tag a zapisovat do něho (Obr. 10).

Obr. 10 Ruční RFID čtečka

4.1 Aplikační oblasti RFID systémů

RFID systémy lze uplatnit v mnoha odvětvích obchodu, výroby, zdravotnictví, nebo službách. V následujících odstavcích jsou popsány jedny z možných a nejčastějších aplikací RFID systémů.

- **Hlídání pohybu zboží**
  Nejjednodušší využití RFID ve kterém se uplatí dokonce **jednobitové** RFID identifikátory. Na vstupu do skladu/obchodu stačí umístit čtečku, stejně tak jako na výstupu. A pak už jenom stačí hlídat, zda něco s RFID neprochází. V praxi můžete podobné systémy najít v mnoha obchodech.
- **Docházkové systémy**
  RFID systémy se velmi často uplatňují ve firmách – umožňují nejenom evidovat docházku, ale také slouží jako „elektronické klíče“. Osobní „magnetické“ karty vybavené identifikací pracovníka se ve spojení s docházkovým systémem snadno postarají o oprávnění vstupu do určitých míst a stejně tak dokáží evidovat příchody a odchody.
- **Stravovací systémy a předplatní systémy**
  Propojení osobních „magnetických“ karet s účetním systémem jídelny (nebo třeba plaveckého bazénu či fitness centra) je ideální. Osobní „magnetická“ karta je prakticky nezničitelná (pro plavecký bazén může být navíc vyhotovena jako náramek z

plastu). Informační systém poskytovatele služby potom eviduje stav účtu návštěvníka (a umožňuje mu například „dobíjet“ kartu potřebnými peněžitými částkami). Protože odpadá nutnost kontaktu identifikátoru (s kartou například stačí projít dveřmi vybavenými anténou), odpadají i fronty a zbytečné zdržování.

- **Plně elektronické pokladny v obchodech**
  Jakkoliv je použití čárového kódu na zboží obrovským ulehčením (pro zákazníka i pokladní), může jít RFID ještě dál. V ideálním případě zjistí pokladní kompletní obsah nákupního košíku najednou a bez jeho vyložení. Pokud si dobře všímáte času a úsilí nutného na odbavení jednoho nákupního košíku u pokladny v současnosti, musí vám být více než jasné, jak by se celý postup zjednodušil.
- **Skladová či výrobní evidence**
  Podobně jako u pokladny (v podstatě výstup ze skladu) je možné RFID nasadit pro skladovou evidenci. Naskladnění kompletní palety či kontejneru je potom také otázkou několik minut (stačí načíst všechny identifikátory). Stejně tak je možné například automaticky evidovat části vyráběného zboží. Díky RFID mohou existovat regály v obchodech, které samy upozorní na nedostatek určitého zboží. Stačí, aby regál byl vybaven snímačem a propojen s počítačem.
- **Sledování pohybu zboží či strojů**
  Stroje (automobily, čistící či transportní stroje) vybavené RFID identifikátory mohou být nepřetržitě sledovány. Přijímače umístěné v podlaze to zajistí snadno a automaticky. Zpětně, za předpokladu ovladatelnosti strojů bezdrátově, je možné stroje řídit.
- **Identifikace jako taková**
  - RFID se může používat pro označování zvířat (obdoba psích známek), poštovních zásilek, leteckých zásilek či čehokoliv dalšího u čeho je potřeba rychlé a jednoznačné identifikace. RFID naleznete i v imobilizérech – klíče od automobilu vybavené RFID spárované s elektronikou automobilu.
  - S identifikační schopností RFID čipů se ovšem může počítat i pro využití místo osobních dokladů. Představa označkování člověka RFID čipem je sice poněkud divoká, ale pouze budoucnost ukáže jak hodně.
  - Identifikovat lze (a je potřeba) ale řadu dalších věcí. Praktické využití RFID může být například v knihovnách či video/dvd půjčovnách.
- **Inteligentní lednička**
  Proč nevybavit ledničku RFID čtečkou? Vaše lednička by potom „věděla“ co obsahuje. Dokázala vám říct, i zda vaše mléko není zrovna ve stavu nepoživatelném. A případně i poradit, co vlastně můžete uvařit k večeři.

5 Čtečky karet v přístupových systémech

Jedná se o fyzické zařízení, které přijímají informace od identifikačního média a mají za úkol tuto informaci bezpečně přečíst a dekódovat. Čtečky karet se liší mezi sebou množstvím faktorů od základních technických parametrů (velikostí, tvarem, napájení, pracovní teplota, čtecí vzdálenost, čtecí médium, apod.) Dále je to schopnost odolávat externím vlivům počasí, vandalismus, teplotě atd.

Čtečky dělíme na:

- **Autonomní systém:** ten se skládají z několika prvků a vytvářejí tím celý systém v jednom zařízení. Skládají se s databáze, řídícího prvku, čtečky karet, často i klávesnicí, dveřního kontaktu, odchodového tlačítka a relé výstupů na zámek a alarm. Mají omezenou kapacitu uživatelů a většinou neobsahují paměť událostí. Při těchto typech systémů se informace získávají z karty, ukládá v paměti čtečky, kde se následně porovnává s databází. Při shodě získané údaje z karty a údajů v databázi následně řídící prvek vydá povel k povolení přístupu. Při nezjištění shody přístup zamítne. Používají se pro jednoduchý vstup, kde není potřeba kontrolovat pohyb zaměstnanců apod.
- **On-line systémy**: čtečky získanou informaci neověřují, ale posílají na přístupový modul, kde probíhá identifikace. Komunikace může probíhat přes sběrnice RS232, RS485, TCP/IP, Wifi, Wiegand apod. Tento typ čteček je nejrozšířenější a používá se všude, kde je třeba zabezpečit přístup do objektu na určité bezpečnostní úrovni.

5.1.1 Komunikační protokol Wiegand

Každá přístupová karta obsahuje informace (čísla). Když je karta v dosahu čtečky karet, tyto informace (čísla) jsou jí posílány. Nicméně, čtečka karet potřebuje vědět, jak jsou jednotlivé informace zasílané a jak organizované (co znamenají). Toto je známé jako formát karty. (Př.: pokud je soubor čísel 026523258, vypovídací hodnota a informace o tomto čísle je téměř nulová. Ale když víme, že první dvě čísla je telefonní předvolba, pak se jedná o telefonní číslo 6523258 s předvolbou 02). Potom znalost formátu dokáže dekódovat kartu. Formát karty určuje, co jednotlivé bity znamenají a jak se používají. Počet bitů je různý. V minulosti se nejčastěji používal 26 bitový formát a stále je jeden z nejrozšířenějších. Tento formát obsahuje dva paritní bity, 6 tzv. facility bitů a 16 bitů s číslem karty.

Následně vznikaly nové formáty s různou bitovou délkou (28, 33, 37, 48, 50 bitů apod.). Různé formáty mají jiné uspořádání bitů. Z tohoto důvodu bude čtečka karet přijímat informace pouze s formátem, kterému bude rozumět.

5.1.2 Paritní bit

Při komunikaci mezi kartou, čtečkou karet nebo serverem, může vzniknout situace, že nepřijdou správné hodnoty přenášených bitů. Při takové chybě odmítne přístup karty, která měla byt přijata a naopak karta, která měla byt odmítnuta je přijatá. Proto se vkládá určitý počet bitů, které slouží pro kontrolu jako detektor chyby. Při sériových přenosech se používá tzv. paritní bit. Výhodou tohoto zabezpečení je jednoduchost v řešení kodérů a dekodérů, malá nadbytečnost a možnost zabezpečení libovolně dlouhé skupiny prvků. Každý k - prvkový soubor se doplní jedním zabezpečovacím prvkem tak, aby počet prvků log 1 byl sudý nebo lichý. Pak se jedná buď o sudou, nebo lichou paritu. Pro sudou paritu platí, že součet všech prvků v kódu včetně Společného je 0:

$c1 + c2 + c3 + c4 + c5 + p = 0$

Pro lichou paritu je postup stejný, ale součet je roven 1.

$c1 + c2 + c3 + c4 + c5 + p = 1$

Použitím parity se původní k - prvkový kód změní na (k+1). Tímto je možné detekovat lichý počet chyb. Sudý počet chyb nemůže být samozřejmě rozpoznán. Většinou se používá jeden paritní bit na 7, 12 bitů a na poslání menšího počtu bitů, se počítá s maximálně s jednou chybou, což stačí na rozpoznání paritním bitem. Přijímací strana poté provede stejný výpočet, a porovnáním vyhodnotí, zda přenos byl správný.

5.1.3 Wiegand 26

Tento formát se stal nejpoužívanějším formátem při přístupových systémech a nazývá se též otevřený formát, který se tím stal široce využívaným standardem. Z toho důvodu jsou schopny skoro všechny přístupové systémy od různých výrobců akceptovat tento 26 bitový formát. Z toho vzniklo i označení WIEGAND 26.

Protokol se skládá z 8 bitů facility code, 16 bitů dat karty (card identification code) a dvou paritních bitů. Prvních 8 bitů (facility code)určuje nejčastěji výrobce čipu (tagu). Pro data karty je tedy vyčleněno 16 bitů, což je 65 535 jednoznačných karet. Celkově v tomto formátu může být vytvořeno až 16 711 425 jednoznačných karet, aniž by se některá opakovala. Protokol obsahuje 2 paritní bity MSB a LSB. Paritní bit MSB (sudá parita) slouží pro kontrolu prvních 12 bitů a ostatních 12 bitů kontroluje.

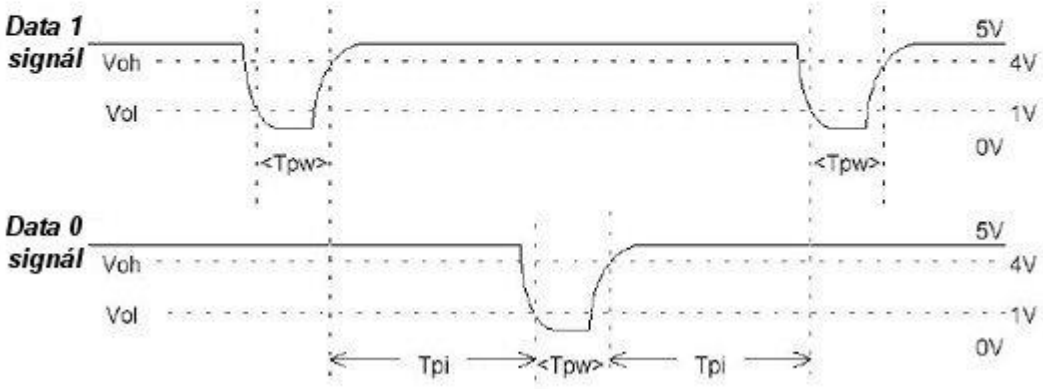
5.1.4 Čtečky karet využívající Wiegand protokol

Wiegand protokol je používán většinou pro komunikaci mezi čtečkami karet a přístupovými moduly. Pro jednoduchost přenosu dat a možnost propojení čtečky karet s modulem na relativně dlouhou vzdálenost je využíván hlavně v průmyslu.

Přenos dat je řešen pomocí dvou datových vodičů a GND. Datové vodiče se většinou označují DATA 0 a DATA 1 (někdy též DATA Low a DATA High). Při připojení čtečky k terminálu jsou označené vodiče takto: zelený vodič pro DATA 0, bílý vodič pro DATA 1 a černý vodič pro GND. Při připojení čtečky karet se též indikuje stav led diody čtečky, který je označen hnědým vodičem.

Komunikace probíhá sekvenčně, což znamená, že bity se přenášejí postupně za sebou. Protokol má jednoduchou časovou synchronizaci. Přenos probíhá tak, že pokud na čtečce není žádná aktivita na DATA 0 (DATA Low) a DATA 1 (DATA High) se přivádí napětí o hodnotě 5V. Pokud se má přenést bit s hodnotou 1, napětí na DATA 1 (DATA High) se přiblíží k nule na definovanou dobu ale napětí na DATA 0 (DATA Low) se nemění. Doba impulsu trvá obvykle 50 us pokud je dodržený protokol. Pokud se přenáší bit s hodnotou 0, napětí na DATA 0 (DATA Low) klesne k nule a napětí na DATA 1 zůstává stejné. Interval mezi dvěma impulsy trvá 2 ms, pokud je dodržený protokol.

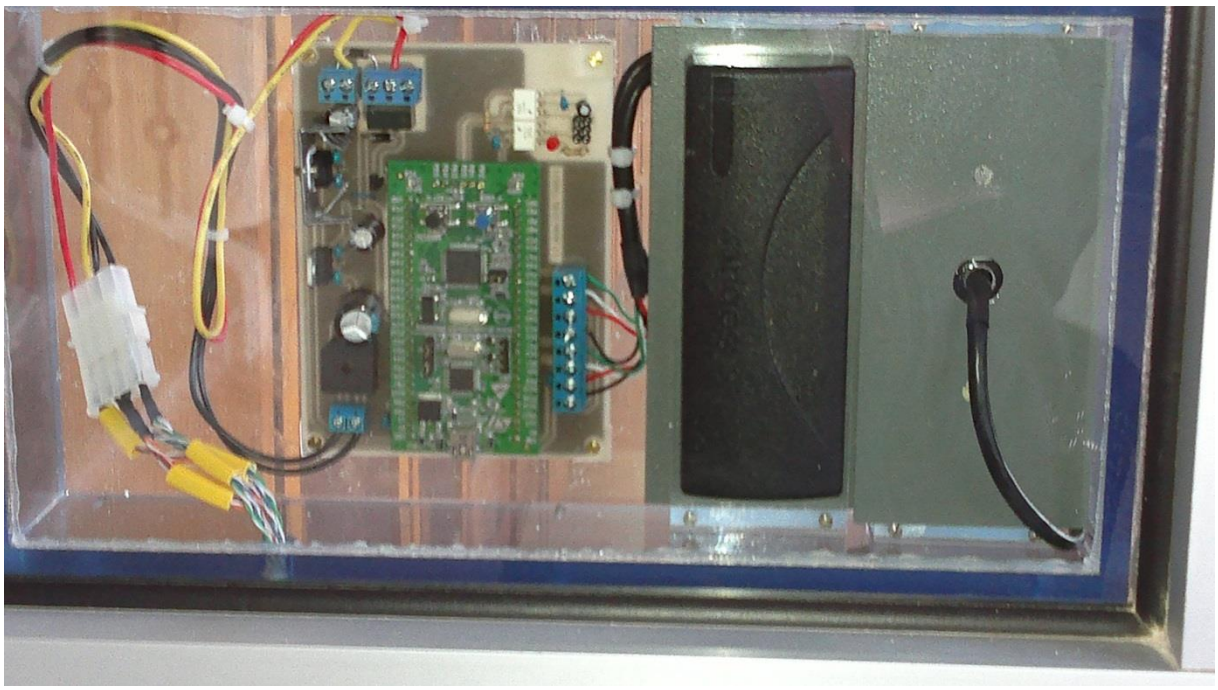
Symbol	*Popis*	*Typické doby trvání*
Tpw	***Doba pulsu***	50µs
Tpi	***Doba pausy***	2ms



Obr. 12. Časová synchronizace protokolu Wiegand

6 Vlastní realizace zařízení

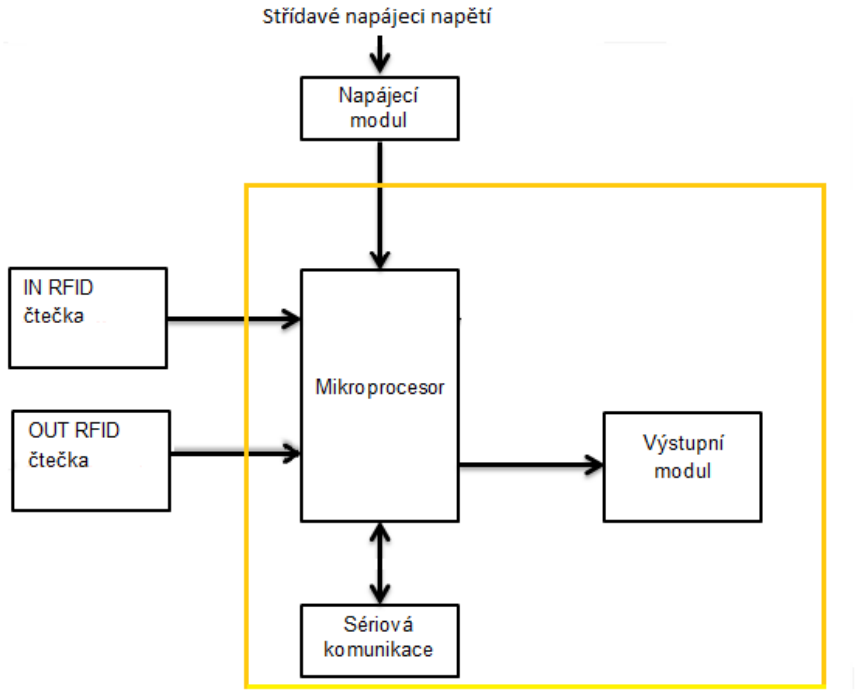
Realizace spočívá ve využití dvou RFID čteček, které posílají řídícímu prvku systému identifikační číslo ISIC karty (MIFARE). Komunikace mezi RFID čtečkami a řídícím prvkem systému je realizovaná přes komunikační protokol Wiegand 26. Řídicí systém je tvořen kitem STM32 F100RB, který je společně s napájecím modulem a výstupním modulem osazení na plošném spoji. Plošný spoj se čtečkami je uzavřen v průhledné krabici z plexiskla. Celé zařízení je přilepené vedle vstupních dveří do laboratorních prostor.



6.1 Hardware

6.1.1 Blokové schéma

Zde ve školních dílnách pan Bárta podle mého návrhu vytvořil plošný spoj. Plošný spoj jsem navrhoval kvůli odblokování dveří, jelikož plošný spoj je osazen nejen mikroprocesorem a napěťovým stabilizátorů, ale především výstupním modulem. Který se skládá z tranzistoru, který ovládá relé. Relé se rozepne a tím odmagnetizuje magnet, který přitahuje dveře k rámu.

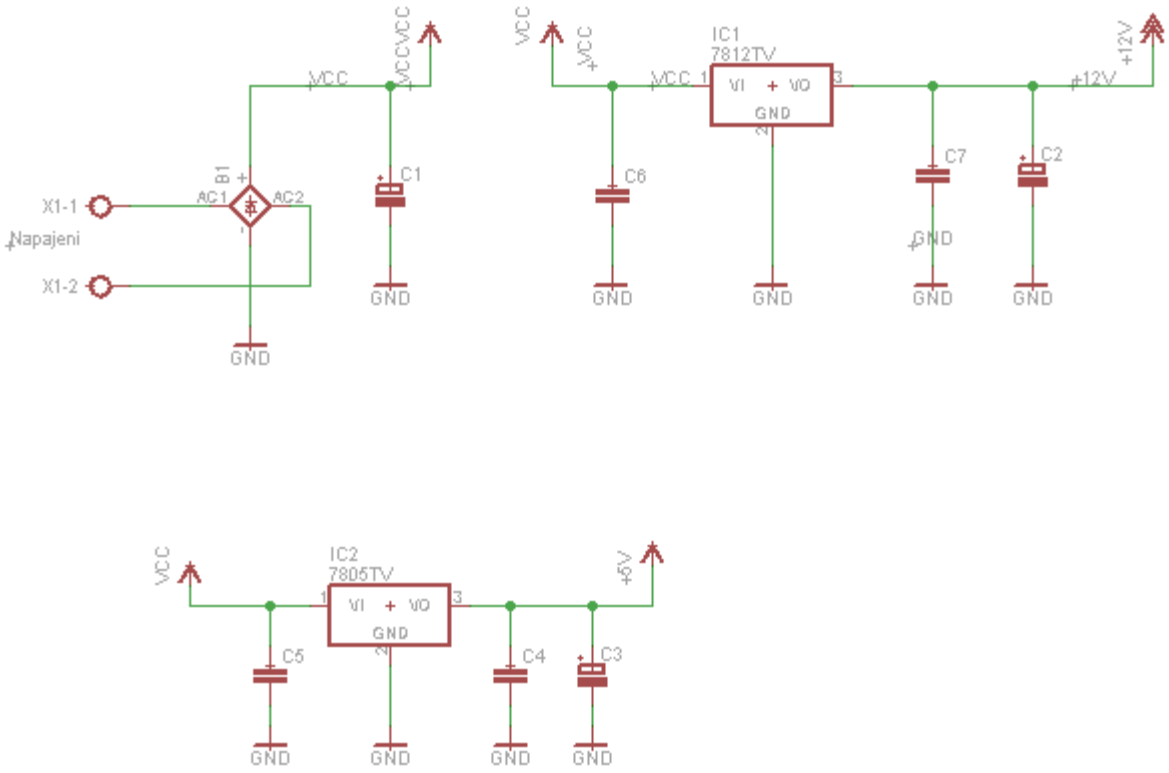


6.1.2 Modul - Napájení

Zařízení je napájeno vstupním napětím 15V. Napětí 15V je z důvodu zatížení, aby při otevírání dveří mi napětí nekleslo pod 12V.Které je posléze stabilizováno do napěťových úrovní:

- 12 V (napájení výstupní modul a RFID čtečky)
- 5 V (napájen řídící prvek systému)

Zařízení má svoje stabilizátory napětí 12V, kterým v tomto případě je napájení vstupu a výstupu. 5V stabilizátorem napájím mikroprocesor.

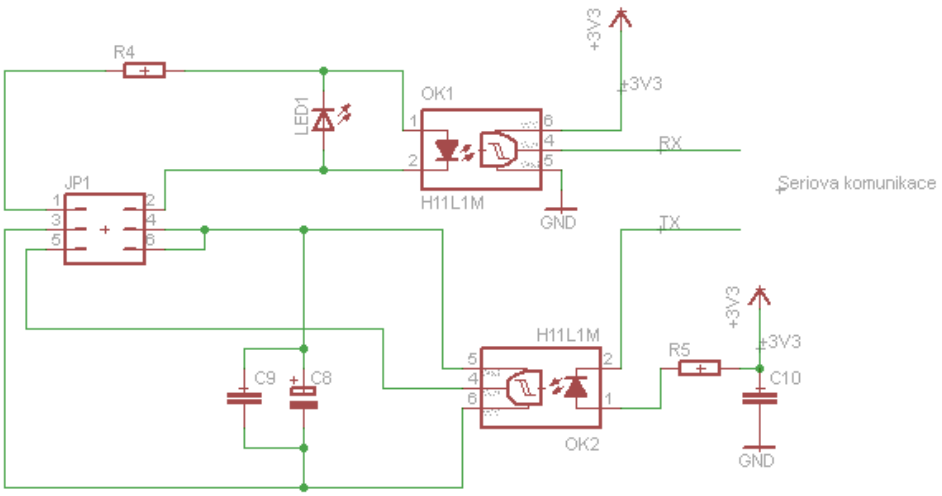


6.1.3 Modul – Sériová komunikace

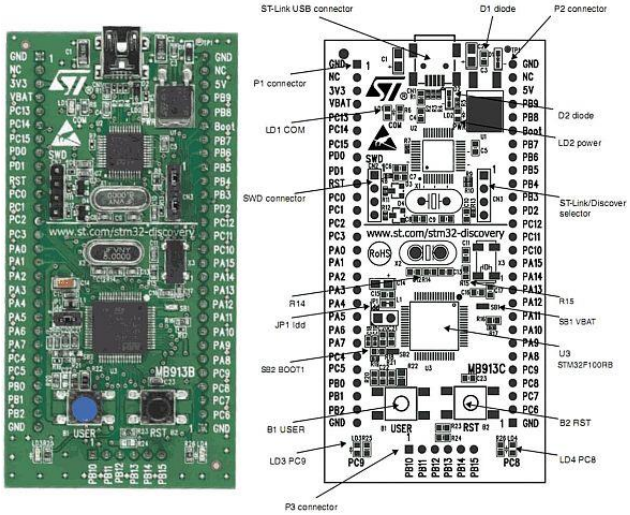
Modul – Sériová komunikace je připraven pro přenos a přijímaní čísel karet do zařízení. Jelikož se počítá v budoucnu s evidencí odchodu a příchodu do učeben laboratoří.

Funkce modulu:

- Galvanické oddělení
- Převodník úrovní napětí
- Přímé připojení RS-232



6.1.4 Modul –mikroprocesorového kitu



Obr. č. 13 STM32 F100RB

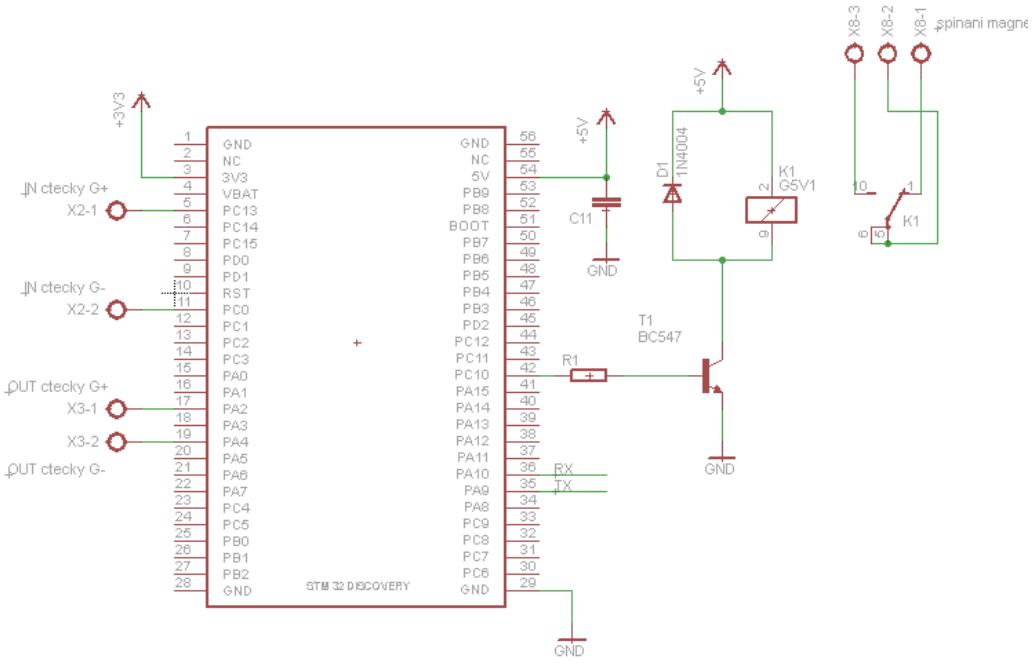
Kit se skládá:

- ARM čip STM32F103C8T6 (který se nachází v horní části kitu)
- Mikrořadič typu STM32F100RB (je vlastní Value Line, který se nachází v dolní části kitu)
  - Obsahuje 128kB Flash a 8kB RAM paměť
- Obsahuje 4 LED, z toho 2 LED slouží pro ST-Link část, kde jedna signalizuje napájení (z USB konektoru) a druhá komunikaci prostřednictvím SWD. Další dvě LED jsou připojeny k Value Line mcu (barva zelená=PC9 a modrá=PC8).

Po obou delších stranách má kit 2 x 28 pinů a na příčné straně ještě 6 pinů.

6.1.5 Modul - Relé

Na relé se může připojit libovolné zařízení, které může mikroprocesor na základě programu ovládat (zapínat nebo vypínat). Například: zvonek, elektrický motor, žárovku, zámek, atd. Zařízení se může napájet přímo ze zařízení a to napětím 12V.



6.1.6 Použité čtečky:

Bezdotyková čtečka pro vnitřní i venkovní použití s výstupním formátem Wiegand 26 bit.

Typ modulu: bezdotyková čtečka
Čtecí dosah: 6 cm
Kompatibilita: Přístupové nebo docházkové systémy s rozhraním Wiegand 26 bit
Výstupní formát Wiegand: 26 bit
Autorizace: karta
Napájení: 10,5 - 13,5 V=
Proudový odběr: max. 60 mA
Optická signalizace: LED dioda červená/zelená
Audio signalizace: ano, bzučák
Délka přívodního vodiče: 90 cm
Provedení: plast
Barva: černá

6.2 Software

Nejdůležitější bylo v programu vytvořit metodu pro dekódování komunikačního protokolu Wiegand 26. Neexistovaly žádné knihovny, které by tuto komunikaci a dekódování protokolu Wiegand 26 řešily. Dekódování

komunikace čteček s procesorem provádí přímo v programech přerušení. Pro každou čtečku je využito jiné přerušení od dvou různých vstupů. V paměti mikroprocesoru jsem si vyhradil paměť pro uložení 1000 identifikačních čísel karet, do které přistupuji pomocí pole. Tato paměť se při deaktivaci (vypnutí) mikroprocesoru smaže, čím je zabráněno vstupu studenta do učeben laboratoří bez přítomnosti profesora. Pro časování je využito časovače, který ovlivňuje dobu, po kterou jsou dveře odblokovány. Zajišťuje blikání diody (indikace funkce zařízení) a pokud dojde k chybě načtení karty, vymaže vstupní buffer. V příloze č.3 Zdrojový kód je obsažen celý okomentovaný zdrojový kód programu.

6.2.1 Přerušení ze vstupní čtečky

Student při opuštění laboratorních prostor přiloží svoji ISIC kartu na IN čtečku. V tento moment čtečka vysílání signály do procesoru. Na jeho vstupy je nastaven přerušovací systém. Mikroprocesor tak přijímá elektronické impulsy z datových vodičů čtečky a dekóduje je. Mikroprocesor si počítá, kolikrát mu přijdou elektronické impulsy z datových vodičů (pro správný přenos si musí mikroprocesor zaznamenat 26 impulsů). Zároveň si tyto elektronické impulsy z datových vodičů převádí na číslo v desítkové soustavě. Po dosažení 26 impulsů si toto číslo uloží do paměti. Viz Příloha č. 1 Vývojový diagram – obsluha přerušení z vstupní čtečky

6.2.2 Z výstupní čtečky

Student při návratu do laboratorních prostor si přiloží svoji ISIC kartu na OUT čtečku. Čtečka přes datové vodiče vyšle v podobě elektronických impulsu do mikroprocesoru unikátní identifikační číslo ISIC karty. Dekódování probíhá jako u první čtečky. Při správném přenosu se toto číslo ISIC karty porovná s ostatními čísly ISIC karet uloženými v paměti mikroprocesoru. Jestliže, dojde ke shodě čísel, sepne relé. Viz Příloha č. 2 Vývojový diagram – obsluha přerušení z výstupní čtečky.

7 Rozšíření systému do budoucna

1. Rozšíření tohoto systému o databázi studentů, která vyřeší automatické vpuštění oprávněného studenta do laboratoří. Databáze bude obsahovat všechny karty studentů rozdělených podle tříd a rozvrhu výuky. Řídicí jednotka pak dle rozvrhu hodin bude povolovat přístup pouze studentům, kteří mají právě vyučovací hodinu.
2. Použití RFID čteček s delším dosahem pohodlnější načítání karet (pouhým přiblížením ke dveřím, a to i přes oděv studenta)
3. Vytvoření vlastního tagu pro mobilní telefony. Telefon by pak nahradil samotnou kartu.
4. Rozšíření čipového systému i pro profesorský sbor. Systému by umožnil pro učitelské karty kdykoliv vstup do laboratoří.
5. Vytvoření dlouhodobého projektu, který se bude zabývat instalací tohoto systému po celé budově. Projekt by přinesl následující dvě výhody:

a. Pro studenty teoretické a praktické dovednosti o technologii bezkontaktní identifikace.
b. Pro školu vytvoření kompletního přístupového systému po celé budově.

8 Závěr

Cílem této práce bylo navrhnout nový čipový systém pro návrat studenta do učeben laboratoří.

Můj čipový systém otevírání dveří vyřešil komplikovaný návrat studenta do laboratoří. Studenta vpouští automaticky díky načtení karty do řídící jednotky při odchodu a studenta opět vpustí při návratu. Systém funguje zcela automaticky bez nutné přítomnosti profesorů. Můj systém předčil mé očekávání, i přesto je možné tento systém dále zdokonalovat jak jsem již navrhnul.

Během realizace jsem získal potřebné teoretické a praktické zkušenosti o technologii bezkontaktní identifikace. Pro správnou funkci systému jsem musel vyřešit několik zásadních problémů. Nejtěžší z těchto problému bylo vytvoření metody pro dekódování komunikačního protokolu Wiegand 26. Tyto nabrané zkušenosti se budu snažit uplatnit i v budoucnu.

Nový přístupový systém obsahuje dvě čtečky, řídící jednotku, vlastní ovládání dveří a napájení. Díky levné pořizovací ceně jednotlivých komponentů systému není finančně náročný.

Můj systém může být aplikován i v jiných institucích, kde krátkodobé opuštění zaměstnance/studenta nebude vyžadovat obsluhu dveří.

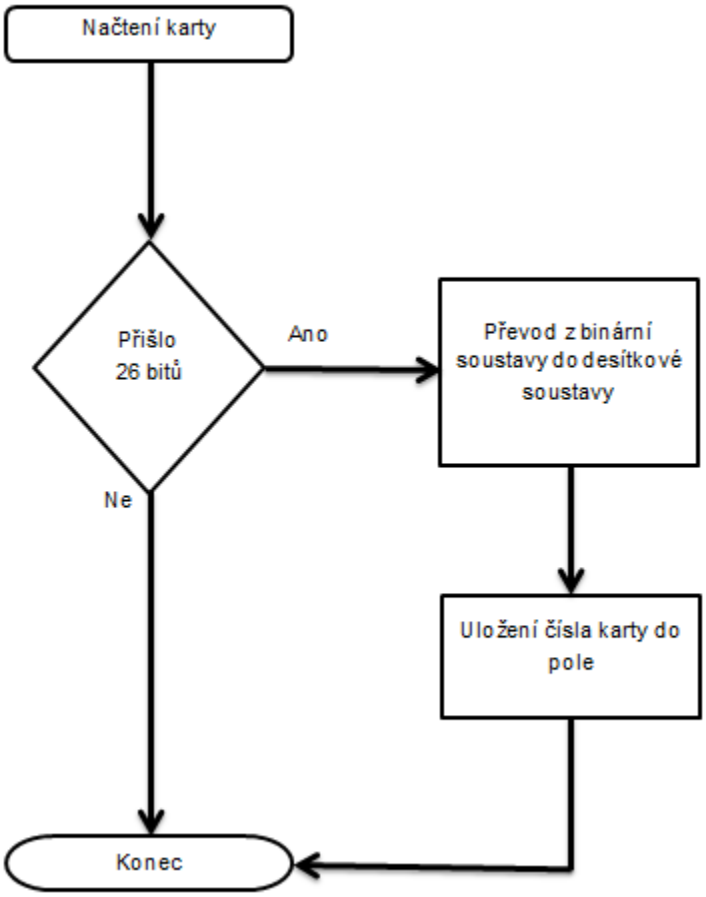
Systém byl v laboratořích nainstalován, úspěšně otestován a je plně funkční.

9 Použitá literatura

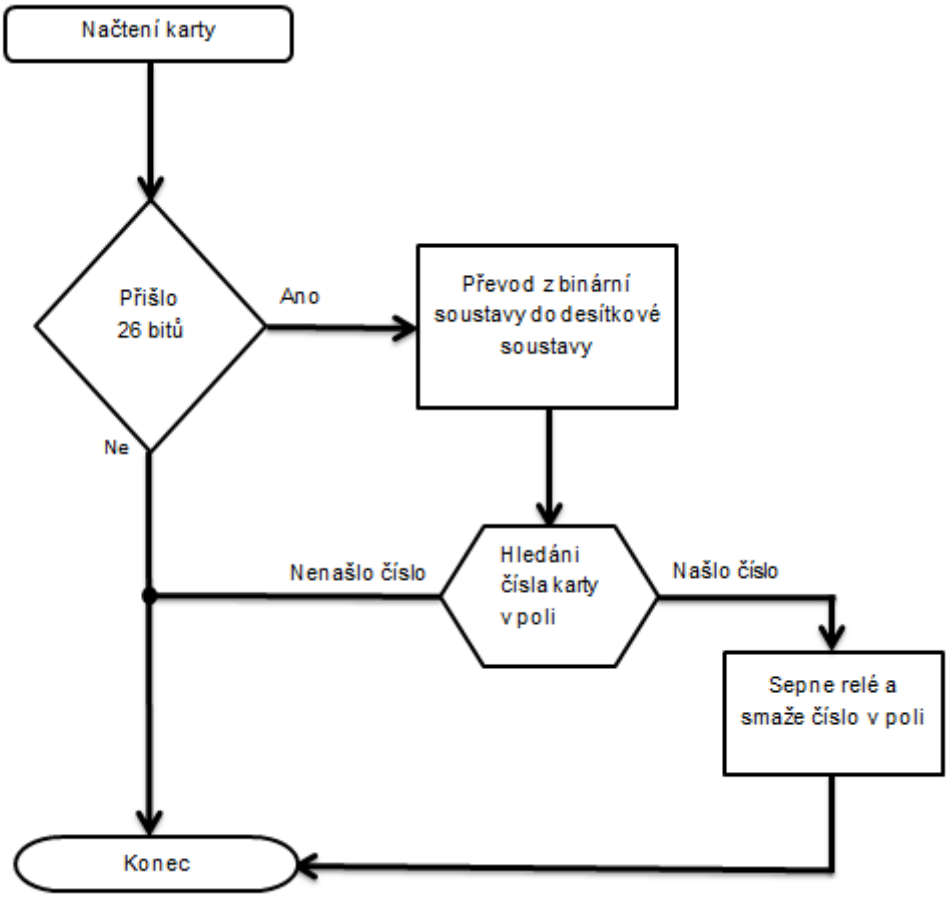
1. Near Field Communication. *Wikipedia* [online]. [cit. 2013-02-22]. Dostupné z: http://cs.wikipedia.org/wiki/NFC
2. RFID. *Wikipedia* [online]. [cit. 2013-02-22]. Dostupné z: http://cs.wikipedia.org/wiki/RFID
3. Protokol Wiegand: řešení jeho čtení. *Dhservis* [online]. [cit. 2013-02-22]. Dostupné z: http://www.dhservis.cz/dalsi_1/wiegand.htm
4. RFID. *Automa* [online]. [cit. 2013-02-22]. Dostupné z: http://www.odbornecasopisy.cz/index.php?
5. MEZINÁRODNÍ LABORATOŘ PRO VÝZKUM RFID TECHNOLOGIE NA VŠB-TUO OSTRAVA: RFID. *Automa* [online]. [cit. 2013-02-22]. Dostupné z: http://rfid.vsb.cz/cs/okruhy/uvod/
6. Nearfield: co je nfc. *Automa* [online]. [cit. 2013-02-22]. Dostupné z: http://nearfield.cz/co-je-nfc

10 Přílohy

10.1 Příloha č. 1 – Vývojový diagram – Obsluha přerušení ze vstupní čtečky



10.2 Příloha č.2 - Vývojový diagram – Obsluha přerušení z výstupní čtečky



10.3 Příloha č. 3 – Zdrojový kód

Inicializace včetně přerušení

```
#include "stm32f10x.h"

//Deklarace proměnných
TIM_TimeBaseInitTypeDef  TIM_TimeBaseStructure;
TIM_OCInitTypeDef  TIM_OCInitStructure;
__IO uint16_t CCR1_Val = 6826;
__IO uint16_t CCR2_Val = 6826;
__IO uint16_t CCR3_Val = 6826;
__IO uint16_t CCR4_Val = 6826;
uint16_t PrescalerValue = 0;

//protypy funkci
void RCC_Configuration(void);
void GPIO_Configuration(void);
void NVIC_Configuration(void);
void EXTI_Configuration(void);
void Timer_Configuration(void);

int main (void)
{
 //volani funkce RCC
 RCC_Configuration();
 //volani funkce NVIC
 NVIC_Configuration();
 //volani funkce GPIO
 GPIO_Configuration();
 //volani funkce EXTI
 EXTI_Configuration();
 //volani funkce Timer
 Timer_Configuration();
 while (1);
}

void Timer_Configuration(void)
{

 //Nastaveni hodnoty v Prescalu
 PrescalerValue = (uint16_t) (SystemCoreClock / 120) - 1;

 //Konfigurace TIME-BASE
 TIM_TimeBaseStructure.TIM_Period = 65535;
 TIM_TimeBaseStructure.TIM_Prescaler = 0;
 TIM_TimeBaseStructure.TIM_ClockDivision = 0;
 TIM_TimeBaseStructure.TIM_CounterMode = TIM_CounterMode_Up;

 TIM_TimeBaseInit(TIM2, &TIM_TimeBaseStructure);

 //Konfigurace Prescaler
 TIM_PrescalerConfig(TIM2,                                    PrescalerValue,
TIM_PSCReloadMode_Immediate);

 //Konfigurace výstupu: Kanal 1
 TIM_OCInitStructure.TIM_OCMode = TIM_OCMode_Timing;
 TIM_OCInitStructure.TIM_OutputState = TIM_OutputState_Enable;
 TIM_OCInitStructure.TIM_Pulse = CCR1_Val;
 TIM_OCInitStructure.TIM_OCPolarity = TIM_OCPolarity_High;
```

```
  TIM_OC1Init(TIM2, &TIM_OCInitStructure);

  TIM_OC1PreloadConfig(TIM2, TIM_OCPreload_Disable);

  //Konfigurace výstupu: Kanal 2
  TIM_OCInitStructure.TIM_OutputState = TIM_OutputState_Enable;
  TIM_OCInitStructure.TIM_Pulse = CCR2_Val;

  TIM_OC2Init(TIM2, &TIM_OCInitStructure);

  TIM_OC2PreloadConfig(TIM2, TIM_OCPreload_Disable);

  //Konfigurace výstupu: Kanal 3
  TIM_OCInitStructure.TIM_OutputState = TIM_OutputState_Enable;
  TIM_OCInitStructure.TIM_Pulse = CCR3_Val;

  TIM_OC3Init(TIM2, &TIM_OCInitStructure);

  TIM_OC3PreloadConfig(TIM2, TIM_OCPreload_Disable);

  //Konfigurace výstupu: Kanal 4
  TIM_OCInitStructure.TIM_OutputState = TIM_OutputState_Enable;
  TIM_OCInitStructure.TIM_Pulse = CCR4_Val;

  TIM_OC4Init(TIM2, &TIM_OCInitStructure);

  TIM_OC4PreloadConfig(TIM2, TIM_OCPreload_Disable);

  //Povoleni přerušení
  TIM_ITConfig(TIM2,  TIM_IT_CC1  |  TIM_IT_CC2  |  TIM_IT_CC3  |
TIM_IT_CC4, ENABLE);

  //Povoleni COUNTER
  TIM_Cmd(TIM2, ENABLE);


}

void RCC_Configuration(void)
{
  //PCLK1 = HCLK/4
  RCC_PCLK1Config(RCC_HCLK_Div4);
  //TIM2 hodiny povoleni
  RCC_APB1PeriphClockCmd(RCC_APB1Periph_TIM2, ENABLE);
  RCC_APB2PeriphClockCmd(RCC_APB2Periph_GPIOC,         ENABLE);
            //Zapnuti brany C (hodinového signalu)
  RCC_APB2PeriphClockCmd(RCC_APB2Periph_GPIOA,         ENABLE);
            //Zapnuti brany A (hodinového signalu)
  RCC_APB2PeriphClockCmd(RCC_APB2Periph_AFIO, ENABLE);
//Zapnuti brany Alternate function I/O
  RCC_APB2PeriphClockCmd(RCC_APB2Periph_GPIOB,         ENABLE);
//Zapnuti brany B (hodinového signalu)
}

void GPIO_Configuration(void)
{
  GPIO_InitTypeDef GPIO_InitStructure;
//_____________________________________________________________
_____________________________________________________________
```

```
  GPIO_InitStructure.GPIO_Pin = GPIO_Pin_10;
  GPIO_InitStructure.GPIO_Mode = GPIO_Mode_Out_PP;          //RELE
  GPIO_InitStructure.GPIO_Speed = GPIO_Speed_50MHz;
          //Nastavení rychlosti vystupniho pinu
  GPIO_Init(GPIOC, &GPIO_InitStructure);

//_____________________________________________________________
_____________________________________________________________
__
 //Zelena LED-dioda
  GPIO_InitStructure.GPIO_Pin = GPIO_Pin_9;
          //Nadefinovani parametru pinu 9
  GPIO_InitStructure.GPIO_Mode = GPIO_Mode_Out_PP;
          //Nastavení pinu jako výstup push/pull
  GPIO_InitStructure.GPIO_Speed = GPIO_Speed_50MHz;
          //Nastavení rychlosti vystupniho pinu
  GPIO_Init(GPIOC, &GPIO_InitStructure);
//Modra LED-dioda
  GPIO_InitStructure.GPIO_Pin = GPIO_Pin_8;
          //Nadefinovani parametru pinu 8
  GPIO_InitStructure.GPIO_Mode = GPIO_Mode_Out_PP;
          //Nastavení pinu jako výstup push/pull
  GPIO_InitStructure.GPIO_Speed = GPIO_Speed_50MHz;
          //Nastavení rychlosti vystupniho pinu
  GPIO_Init(GPIOC, &GPIO_InitStructure);
          //Inicializace portu s parametry uloznymi v datove strukture

  GPIO_InitStructure.GPIO_Pin = GPIO_Pin_13;
          //Nadefinovani parametru pinu 13
  GPIO_InitStructure.GPIO_Mode = GPIO_Mode_IN_FLOATING;
//Nastavení pinu jako vstup bez push/pull rezistoru
  GPIO_Init(GPIOC, &GPIO_InitStructure);                    //Inicializace
portu s parametry uloznymi v datove strukture
  GPIO_EXTILineConfig (GPIO_PortSourceGPIOC,GPIO_PinSource13);

  GPIO_InitStructure.GPIO_Pin = GPIO_Pin_4;
//Nadefinovani parametru pinu 4
  GPIO_InitStructure.GPIO_Mode = GPIO_Mode_IN_FLOATING;
//Nastavení pinu jako vstup bez push/pull rezistoru
  GPIO_Init(GPIOC, &GPIO_InitStructure);
//Inicializace portu s parametry uloznymi v datove strukture
  GPIO_EXTILineConfig (GPIO_PortSourceGPIOA,GPIO_PinSource4);

  GPIO_InitStructure.GPIO_Pin = GPIO_Pin_2;
//Nadefinovani parametru pinu 2
  GPIO_InitStructure.GPIO_Mode = GPIO_Mode_IN_FLOATING;
//Nastavení pinu jako vstup bez push/pull rezistoru
  GPIO_Init(GPIOA, &GPIO_InitStructure);
//Inicializace portu s parametry uloznymi v datove strukture
  GPIO_EXTILineConfig (GPIO_PortSourceGPIOA,GPIO_PinSource2);

  GPIO_InitStructure.GPIO_Pin = GPIO_Pin_0;
//Nadefinovani parametru pinu 6
  GPIO_InitStructure.GPIO_Mode = GPIO_Mode_IN_FLOATING;
//Nastavení pinu jako vstup bez push/pull rezistoru
  GPIO_Init(GPIOC, &GPIO_InitStructure);
//Inicializace portu s parametry uloznymi v datove strukture
  GPIO_EXTILineConfig (GPIO_PortSourceGPIOC,GPIO_PinSource0);
}
```

```
void NVIC_Configuration(void)
{
  NVIC_InitTypeDef NVIC_InitStructure;

  //Povolení globalniho přerušení
  NVIC_InitStructure.NVIC_IRQChannel = TIM2_IRQn;
  NVIC_InitStructure.NVIC_IRQChannelPreemptionPriority = 0;
  NVIC_InitStructure.NVIC_IRQChannelSubPriority = 1;
  NVIC_InitStructure.NVIC_IRQChannelCmd = ENABLE;
  NVIC_Init(&NVIC_InitStructure);

  NVIC_InitStructure.NVIC_IRQChannel = EXTI15_10_IRQn;
  NVIC_InitStructure.NVIC_IRQChannelPreemptionPriority = 0x00;
  NVIC_InitStructure.NVIC_IRQChannelSubPriority = 0x0F;
  NVIC_InitStructure.NVIC_IRQChannelCmd = ENABLE;
  NVIC_Init(&NVIC_InitStructure);

  NVIC_InitStructure.NVIC_IRQChannel = EXTI4_IRQn;
  NVIC_InitStructure.NVIC_IRQChannelPreemptionPriority = 0x00;
  NVIC_InitStructure.NVIC_IRQChannelSubPriority = 0x0F;
  NVIC_InitStructure.NVIC_IRQChannelCmd = ENABLE;
  NVIC_Init(&NVIC_InitStructure);

  NVIC_InitStructure.NVIC_IRQChannel = EXTI2_IRQn;
  NVIC_InitStructure.NVIC_IRQChannelPreemptionPriority = 0x00;
  NVIC_InitStructure.NVIC_IRQChannelSubPriority = 0x0F;
  NVIC_InitStructure.NVIC_IRQChannelCmd = ENABLE;
  NVIC_Init(&NVIC_InitStructure);

  NVIC_InitStructure.NVIC_IRQChannel = EXTI0_IRQn;
  NVIC_InitStructure.NVIC_IRQChannelPreemptionPriority = 0x00;
  NVIC_InitStructure.NVIC_IRQChannelSubPriority = 0x0F;
  NVIC_InitStructure.NVIC_IRQChannelCmd = ENABLE;
  NVIC_Init(&NVIC_InitStructure);
}

void EXTI_Configuration(void)
{
  EXTI_InitTypeDef EXTI_InitStructure;

  EXTI_InitStructure.EXTI_LineCmd=ENABLE;
  EXTI_InitStructure.EXTI_Mode=EXTI_Mode_Interrupt;
  EXTI_InitStructure.EXTI_Trigger=EXTI_Trigger_Falling;
  EXTI_InitStructure.EXTI_Line=EXTI_Line13;
  EXTI_Init(&EXTI_InitStructure);

  EXTI_InitStructure.EXTI_LineCmd=ENABLE;
  EXTI_InitStructure.EXTI_Mode=EXTI_Mode_Interrupt;
  EXTI_InitStructure.EXTI_Trigger=EXTI_Trigger_Falling;
  EXTI_InitStructure.EXTI_Line=EXTI_Line4;
  EXTI_Init(&EXTI_InitStructure);


  EXTI_InitStructure.EXTI_LineCmd=ENABLE;
  EXTI_InitStructure.EXTI_Mode=EXTI_Mode_Interrupt;
  EXTI_InitStructure.EXTI_Trigger=EXTI_Trigger_Falling;
  EXTI_InitStructure.EXTI_Line=EXTI_Line2;
  EXTI_Init(&EXTI_InitStructure);

  EXTI_InitStructure.EXTI_LineCmd=ENABLE;
```

```
  EXTI_InitStructure.EXTI_Mode=EXTI_Mode_Interrupt;
  EXTI_InitStructure.EXTI_Trigger=EXTI_Trigger_Falling;
  EXTI_InitStructure.EXTI_Line=EXTI_Line0;
  EXTI_Init(&EXTI_InitStructure);
}

void assert_failed(uint8_t* file, uint32_t line)
{
  while (1)
  {}
}
```

Obsluha přerušení

```
/**

******************************************************************************
  * @file    Project/STM32F10x_StdPeriph_Template/stm32f10x_it.c
  * @author  MCD Application Team
  * @version V3.5.0
  * @date    08-April-2011
  * @brief   Main Interrupt Service Routines.
  *          This file provides template for all exceptions handler and
  *          peripherals interrupt service routine.

******************************************************************************
  * @attention
  *
  * THE PRESENT FIRMWARE WHICH IS FOR GUIDANCE ONLY AIMS AT PROVIDING CUSTOMERS
  * WITH CODING INFORMATION REGARDING THEIR PRODUCTS IN ORDER FOR THEM TO SAVE
  * TIME. AS A RESULT, STMICROELECTRONICS SHALL NOT BE HELD LIABLE FOR ANY
  * DIRECT, INDIRECT OR CONSEQUENTIAL DAMAGES WITH RESPECT TO ANY CLAIMS ARISING
  * FROM THE CONTENT OF SUCH FIRMWARE AND/OR THE USE MADE BY CUSTOMERS OF THE
  * CODING INFORMATION CONTAINED HEREIN IN CONNECTION WITH THEIR PRODUCTS.
  *
  *                <h2><center>&copy; COPYRIGHT 2011 STMicroelectronics</center></h2>

******************************************************************************
  */

/* Includes ------------------------------------------------------------------*/
#include "stm32f10x_it.h"

/** @addtogroup STM32F10x_StdPeriph_Template
  * @{
  */

/* Private typedef -----------------------------------------------------------*/
/* Private define ------------------------------------------------------------*/
/* Private macro -------------------------------------------------------------*/
/* Private variables ---------------------------------------------------------*/
```

```
int pole[1000];
int i=0;
int kontrola=0;
int prom=0;
int prom1=0;
int key=0;
int key1=0;
int des=67108864;
int des1=67108864;
uint16_t capture = 0;
extern __IO uint16_t CCR1_Val;
extern __IO uint16_t CCR2_Val;
extern __IO uint16_t CCR3_Val;
extern __IO uint16_t CCR4_Val;

/* Private function prototypes -----------------------------------------------*/
/* Private functions ---------------------------------------------------------*/

/******************************************************************************/
/*            Cortex-M3 Processor Exceptions Handlers                         */
/******************************************************************************/

/**
  * @brief  This function handles NMI exception.
  * @param  None
  * @retval None
  */
void NMI_Handler(void)
{
}

/**
  * @brief  This function handles Hard Fault exception.
  * @param  None
  * @retval None
  */
void HardFault_Handler(void)
{
  /* Go to infinite loop when Hard Fault exception occurs */
  while (1)
  {
  }
}

/**
  * @brief  This function handles Memory Manage exception.
  * @param  None
  * @retval None
  */
void MemManage_Handler(void)
{
  /* Go to infinite loop when Memory Manage exception occurs */
  while (1)
  {
  }
}

/**
```

```
  * @brief  This function handles Bus Fault exception.
  * @param  None
  * @retval None
  */
void BusFault_Handler(void)
{
  /* Go to infinite loop when Bus Fault exception occurs */
  while (1)
  {
  }
}

/**
  * @brief  This function handles Usage Fault exception.
  * @param  None
  * @retval None
  */
void UsageFault_Handler(void)
{
  /* Go to infinite loop when Usage Fault exception occurs */
  while (1)
  {
  }
}

/**
  * @brief  This function handles SVCall exception.
  * @param  None
  * @retval None
  */
void SVC_Handler(void)
{
}

/**
  * @brief  This function handles Debug Monitor exception.
  * @param  None
  * @retval None
  */
void DebugMon_Handler(void)
{
}

/**
  * @brief  This function handles PendSVC exception.
  * @param  None
  * @retval None
  */
void PendSV_Handler(void)
{
}

/**
  * @brief  This function handles SysTick Handler.
  * @param  None
  * @retval None
  */
void SysTick_Handler(void)
{
}
```

```
/******************************************************************************/
/*            STM32F10x Peripherals Interrupt Handlers                        */
/*  Add here the Interrupt Handler for the used peripheral(s) (PPP), for the  */
/*  available peripheral interrupt handler's name please refer to the startup */
/*  file (startup_stm32f10x_xx.s).                                            */
/******************************************************************************/

/**
  * @brief  This function handles PPP interrupt request.
  * @param  None
  * @retval None
  */
/*void PPP_IRQHandler(void)
{
}*/

/**
  * @}
  */
//-------------------------------------------------------------------------------------------------
void EXTI15_10_IRQHandler(void) //Skupinové preruseni na pinech 10, 11, 12, 13, 14, 15
{

  if(GPIO_ReadInputDataBit(GPIOC,GPIO_Pin_13)==  FALSE)  //Prichazi log.0 na pin 13 brany C
  {

    prom++; //Pocitam kolik signalu mi prislo z pinu 13, na kterém je zapojen signal G+ ze ctecky
    //prevod do 10 soustavy
    key=key+des;  //do key zapisuji tvz. cisla cipove karty ISICu na jednotlivych pozicich
    des=des/2;  //delim dvema coz znamena ze snizuji o pozici, na kterou si zapisu cislo, ktere mi prijde ze signalu G+ ctecky
  }

  if(prom==26)
  {
     //pokud mi prijde dohromady 26 signalu skladajici z signalu G+ ze ctecky zapisu do pole key (key mi reprezentuje cislo cipove karty ISICu)

     pole[i]=key;
     i++;
     GPIO_SetBits(  GPIOC,GPIO_Pin_9);//zde  pro  kontrolu  rozsvitím zelenou diodu
     // kontrola přetečení
     if (i==1000)
     {
          i=0;
     }

     //vracení původních hodnot
     key=0;
     des=67108864;
     prom=0;
```

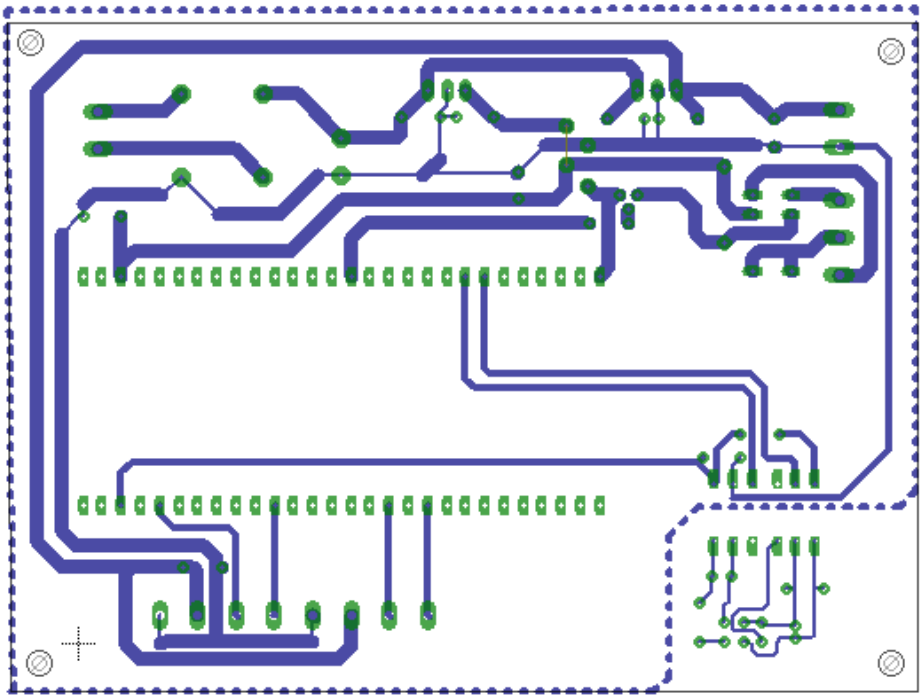
```
  }

  EXTI_ClearITPendingBit(EXTI_Line13);

  }
//-------------------------------------------------------------------------------------------
-------------------------------
void EXTI0_IRQHandler(void) //Preruseni z pinu 0
{
   if(GPIO_ReadInputDataBit(GPIOC,GPIO_Pin_0)== FALSE)    //Prichazi
log.0 na pin 0 brany C
  {
     prom++;  //Pocitam kolik signalu mi prislo z pinu 0, na kterém je zapojen
signal G- ze ctecky
    des=des/2;//delim dvema coz znamena ze snizuji o pozici, na kterou si
zapisu cislo, ktere mi prijde ze signalu G+ ctecky

  }
  if(prom==26)
  {
     //pokud mi prijde dohromady 26 signalu skladajici z signalu G+ a G- ze
ctecky zapisu do pole key (key mi reprezentuje cislo cipove karty ISICu)

     pole[i]=key;
     i++;
     GPIO_SetBits(  GPIOC,GPIO_Pin_9);//zde  pro  kontrolu  rozsvitím
zelenou diodu
     // kontrola přetečení
     if (i==1000)
     {
           i=0;
     }

     //vracení původních hodnot
     key=0;
     des=67108864;
     prom=0;

  }

  EXTI_ClearITPendingBit(EXTI_Line0);

  }
//-------------------------------------------------------------------------------------------
-------------------------------
void EXTI2_IRQHandler(void) //Preruseni z pinu 2
{
  if(GPIO_ReadInputDataBit(GPIOA,GPIO_Pin_2)==                FALSE)
        //Prichazi log.0 na pin 2 brany A
  {
     prom1++; //Pocitam kolik signalu mi prislo z pinu 2, na kterém je
zapojen signal G+ ze ctecky
     //prevod do 10 soustavy
     key1=key1+des1;     //do key zapisuji tvz. cisla cipove karty ISICu na
jednotlivych pozicich
     des1=des1/2;  //delim dvema coz znamena ze snizuji o pozici, na kterou
si zapisu cislo, ktere mi prijde ze signalu G+ ctecky
  }

  if(prom1==26)
```

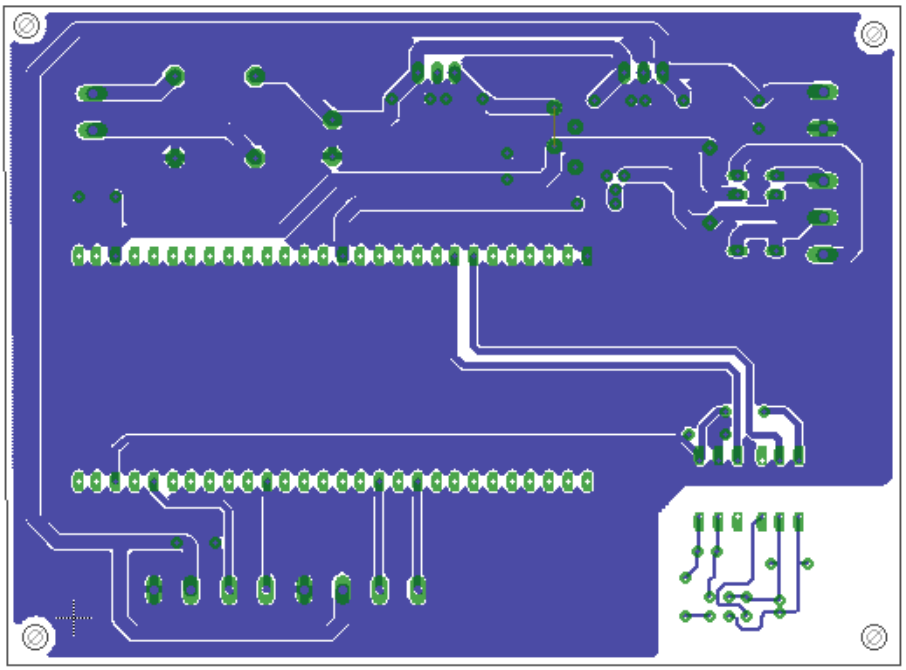
```
  {
      //pokud mi prijde dohromady 26 signalu skladajici z signalu G+ a G- ze
ctecky hledam cislo cipove karty ISICu v poli
      for(kontrola=0;kontrola<1000;kontrola++)
            {
              if(pole[kontrola]==key1)
              {
           // Hledani bylo uspesne
                pole[kontrola]=0;          //vymazani cisla cipove karty ISICu v poli

                GPIO_SetBits( GPIOC,GPIO_Pin_8);//Pro prehlednost rozsviceni
modre diody
                GPIO_SetBits( GPIOC,GPIO_Pin_10);//Sepnuti rele

              }
             }
       //vracení původních hodnot
       key1=0;
              des1=67108864;
       prom1=0;
   }

   EXTI_ClearITPendingBit(EXTI_Line2);

}
//-----------------------------------------------------------------------------------------
---------------------------------
void EXTI4_IRQHandler(void)//Preruseni z pinu 4
{
  if(GPIO_ReadInputDataBit(GPIOA,GPIO_Pin_4)==    FALSE)    //Prichazi
log.0 na pin 4 brany A
  {

      prom1++;//Pocitam kolik signalu mi prislo z pinu 4, na kterém je zapojen
signal G- ze ctecky
      des1=des1/2;//delim dvema coz znamena ze snizuji o pozici, na kterou si
zapisu cislo, ktere mi prijde ze signalu G+ ctecky
  }
  if(prom1==26)
  {
      //pokud mi prijde dohromady 26 signalu skladajici z signalu G+ a G- ze
ctecky hledam cislo cipove karty ISICu v poli
      for(kontrola=0;kontrola<1000;kontrola++)
            {
              if(pole[kontrola]==key1)
              {
               // Hledani bylo uspesne
                pole[kontrola]=0;//vymazani  cisla  cipove  karty  ISICu  v  poli

                GPIO_SetBits( GPIOC,GPIO_Pin_8);//Pro prehlednost rozsviceni
modre diody
                GPIO_SetBits( GPIOC,GPIO_Pin_10);//Sepnuti rele

              }
             }

       //vracení původních hodnot
       key1=0;
            des1=67108864;
       prom1=0;
```

```
    }

    EXTI_ClearITPendingBit(EXTI_Line4);

}
//-------------------------------------------------------------------------------------
-------------------------------
void TIM2_IRQHandler(void)
{
  if (TIM_GetITStatus(TIM2, TIM_IT_CC1) != RESET)
  {
    TIM_ClearITPendingBit(TIM2, TIM_IT_CC1);
    GPIO_ResetBits( GPIOC,GPIO_Pin_8);//zhasnuti zelene diody
    GPIO_ResetBits( GPIOC,GPIO_Pin_9);//zhasnuti modre diody
    GPIO_ResetBits( GPIOC,GPIO_Pin_10);//LOG. 0 PRO RELE
    capture = TIM_GetCapture1(TIM2);
    TIM_SetCompare1(TIM2, capture + CCR1_Val);
  }
  else if (TIM_GetITStatus(TIM2, TIM_IT_CC2) != RESET)
  {
    TIM_ClearITPendingBit(TIM2, TIM_IT_CC2);
    capture = TIM_GetCapture2(TIM2);
    TIM_SetCompare2(TIM2, capture + CCR2_Val);
  }
  else if (TIM_GetITStatus(TIM2, TIM_IT_CC3) != RESET)
  {
    TIM_ClearITPendingBit(TIM2, TIM_IT_CC3);
  }
  else
  {
    TIM_ClearITPendingBit(TIM2, TIM_IT_CC4); }
  }




/******************* (C) COPYRIGHT 2011 STMicroelectronics
*****END OF FILE****/
```

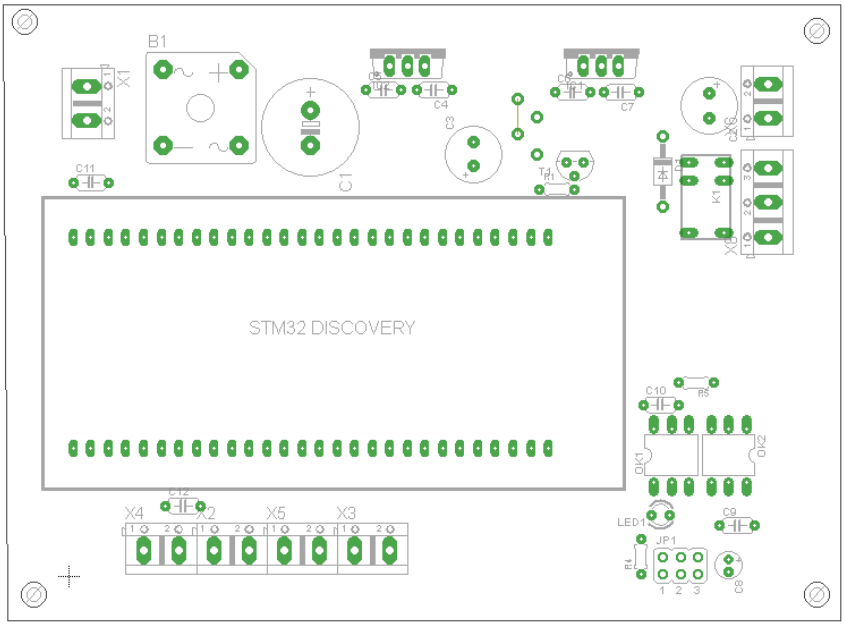
10.4 Příloha č.4 – Plošný spoj

10.4.1 Návrh plošného spoje





10.4.2 Osazník



Part	Value
C1	CE 1000u/35VT JAM-TK 12,5x20 RM5 BULK E5-13
C2	CE 220u/25V JAM-SK 8x11,5 RM3,5 BULK E3,5-8
C3	CE 220u/25V JAM-SK 8x11,5 RM3,5 BULK E3,5-8
C4	CK 100N/100V X7R
C5	CK 100N/100V X7R
C6	CK 100N/100V X7R
C7	CK 100N/100V X7R
C8	CE 10u/16VT HIT-E5R 4x5 RM1,5 BULK E1,8-4
C9	CK 100N/100V X7R
C10	CK 100N/100V X7R
C11	CK 100N/100V X7R
C12	CK 100N/100V X7R
D1	1N4004
IC1	7812TV
IC2	7805TV
JP1	JP3Q jumper
K1	G5V1
OK1	H11L1M
OK2	H11L1M
R1	RRU 4K7
R4	RRU 1K
R5	RRU 330R
T1	BC547