UNIVERZITA PARDUBICE
Fakulta elektrotechniky a informatiky

Zámek dveří s ověřením přes LAN

Daniel Opršal

Bakalářská práce
2019

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: **2018/2019**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Daniel Opršal**
Osobní číslo:	**I16035**
Studijní program:	**B2612 Elektrotechnika a informatika**
Studijní obor:	**Komunikační a mikroprocesorová technika**
Název tématu:	**Zámek dveří s ověřením přes LAN**
Zadávající katedra:	**Katedra elektrotechniky**

Zásady pro vypracování:

Cílem práce je realizace zámkového systému s ověřením proti autentizačnímu serveru přes LAN. V teoretické části popište možnosti ověření osob vůči zámkovému systému a možnosti ověření zámkového systému vůči serveru a možné způsoby správy oprávněných čipů, otisků prstů apod. V praktické části navrhněte a realizujte komunikační a ověřovací část včetně softwaru pro správu oprávněných čipů. Ověřte funkci realizovaného systému.

Rozsah grafických prací:

Rozsah pracovní zprávy:

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

Seznam odborné literatury:

[1] DUMEK, Jakub. Zámek s technologií RFID, Bakalářská práce, Pardubice, 2015, Univerzita Pardubice.
[2] ESP8266EX Data Sheet. Espressif, 2018, [cit. 1. 11. 2018]. Dostupné z URL: https://www.espressif.com/sites/default/files/documentation/0a-esp8266ex_datasheet_en.pdf

Vedoucí bakalářské práce: **Ing. Jiří Roleček**
Katedra elektrotechniky

Datum zadání bakalářské práce: **15. října 2018**
Termín odevzdání bakalářské práce: **10. května 2019**

Univerzita Pardubice Česká republika

L.S.

Ing. Zdeněk Němec, Ph.D.
děkan

Ing. Jan Pidanič, Ph.D.
vedoucí katedry

V Pardubicích dne 15. listopadu 2018

Prohlášení autora

Prohlašuji:

Tuto práci jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 9/2012, bude práce zveřejněna v Univerzitní knihovně a prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 10. 5. 2019 Daniel Opršal

Poděkování

Nejprve bych rád poděkoval svému vedoucímu bakalářské práce panu Ing. Jiřímu Rolečkovi za odborné vedení, cenné rady, trpělivost a ochotu, kterou mi v průběhu zpracování bakalářské práce věnoval. Rád bych také poděkoval panu Ing. Pavlu Rozsívalovi za zhotovení desky plošných spojů.

Anotace

Tato bakalářská práce se zabývá návrhem a realizací zámkového systému s ověřením přes LAN. Teoretická část popisuje jednotlivé části zámkového systému a RFID technologii. Praktická část je zaměřena na návrh zařízení a řídícího softwaru.

Klíčová slova

RFID, LAN, NODEMCU, Elektronický zámek

Title

Door lock with authentication over LAN

Annotation

The objective of this bachelor thesis is realization of the door-lock system with authentication over LAN. The theoretical chapter describes parts of the door-lock system and RFID technology. The practical chapter contains device construction and its driving software.

Keywords

RFID, LAN, NODEMCU, Eletronic lock

Obsah

Seznam zkratek

RFID	Radio Frequency identification
LAN	Local area network
Wi-Fi	Wriless fidelity
TAG	Někdy též UID – Unique identifier
GSM	Global system for mobile comunication
ID	Identification

Seznam obrázků

Seznam tabulek

Úvod

Bakalářská práce se zabývá elektronickými zámky s technologií RFID, které se aktuálně těší velké oblibě. Tato technologie je v poslední době nasazována zejména ve velkých objektech jako jsou hotely, rozsáhlé školní budovy a budovy státní sféry, kde dochází k velkému pohybu osob a nachází se zde velký počet prostorů, které je třeba střežit.

V prví kapitole jsou obecně popsány zámkové systémy a možnosti ověření uživatele vůči zámkovému systému.

Druhá kapitola popisuje základní rozdělení zámků a jejich výhody a nevýhody.

Třetí kapitola se zabývá samotnou technologii RFID. Je zde podrobně popsána historie, princip fungování této technologie, druhy čtecích zařízení a RFID transpondérů (čipů). V závěru kapitoly je uvedena tabulka frekvencí pro různé použití a různé technologie.

Ve čtvrté kapitole je podrobně popsán konkrétní návrh elektronického zámku pro přístup do místnosti nebo objektu, kde se jako klíč používá pasivní RFID čip. Jsou zde popsány jednotlivé komponenty včetně jejich parametrů.

Pátá kapitola je věnována ověření funkčnosti zámkového systému.

1 Zámkové systémy

1.1 Historie

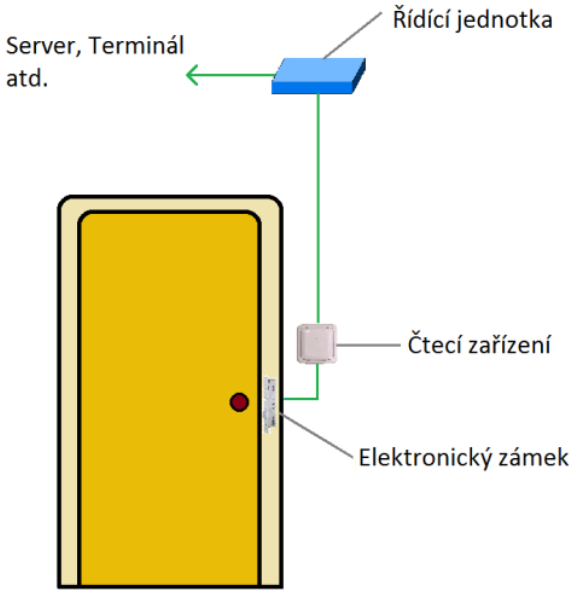
Původ zámku jako mechanické zábrany sahá až do období Babylónu, kde ho potvrdily archeologické nálezy v podobě dřevěných zámků. V období antického Řecka a Říma se již zámky vyráběly také z bronzu. Do 17. století se vyráběly zámky, u kterých šlo klíčem pouze pootočit, ale nešlo klíč vyndat. Zámky nebyly zadlabávané do dveří, byly pouze nasazené na vnitřní straně dveří. [1]

> *Přibližně od poloviny 17. století dochází k revoluci ve výrobě zámků, jejichž mechanismus se rychle zlepšuje. Významnou inovací byl patent Roberta Barrona z r. 1788, jehož zámek byl vybaven stavítky – pákami, které musí klíč zvednout do správné polohy, jinak se závorou nelze pohnout. Barronův vynález dále vylepšil např. Jeremia Chubb a později Robert Yale, který v r.1844 vynalezl cylindrickou vložku – soustavu odpružených stavítek s blokovacími kolíky, která musí zuby klíče nastavit tak, aby bylo možno otočit cylindrem (válcem uvnitř zámku), jehož zub teprve pohybuje závorou. Vzniká tak jednoduchý a subtilní, avšak bezpečný zámek, který poskytuje značnou variabilitu klíčů. [1]*

Během 20. století prošly zámky značným vývojem. Byly použity profilované, dozické a patentní (FAB) klíče. Složitost zámků vzrůstá s vyšším požadavkem na bezpečnost. [1]

1.2 Princip zámkového systému

Tato kapitola popisuje princip zámkového systému, který je na obrázku níže (Obrázek 1). Mezi hlavní výhody elektronických zámkových systémů patří zejména možnost zaznamenání vstupů, a to včetně identifikace osoby, která do místnosti vstoupila. Systém vyčkává do doby, než je přiložena RFID karta ke čtecímu zařízení. Čtecí zařízení poté předá načtený TAG karty řídící jednotce, která na základě svého softwaru vyhodnotí, zda má daný uživatel do místnosti přístup. Pokud je to nezbytné, řídící jednotka se obrátí na server, kde si vyžádá informaci o tom, zda má daný uživatel do dané oblasti přístup. Podle řídící jednotky je pak uživateli přístup do místnosti povolen, nebo zamítnut. Řídící jednotka pak může, je-li to požadováno, na server odesílat informace o tom, kdo a kdy se v místnosti vyskytoval. Systém se skládá z pěti hlavních částí. [2]



Obrázek 1 - Jednoduchý zámkový systém [2]

- **Dveře** – Tvoří mechanickou překážku.
- **Elektronický zámek** – Je mechanickou částí, která po připojení řídícího napětí uvolní dveře.
- **Čtecí zařízení** – Načte jedinečný TAG karty pomocí technologie RFID.
- **Řídící jednotka** – Na základě informace od čtecího zařízení vyhodnocuje, kdy mají být dveře otevřeny. Případě ověří správnost informací vůči serveru.
- **Server** – Vůči serveru probíhá ověřování informací o přístupech do dané místnosti.

1.3 Možností ověření

1.3.1 Osoba vůči zámkovému systému

Možností, jak uživatel provádí svou identifikaci, je mnoho. Jde především o to, aby uživatel předal zámkovému systému jedinečnou identifikaci, díky které bude systémem rozpoznán. Nejčastěji se používají karty s jednoznačným identifikačním číslem UID, někdy též označované jako TAG karty. Mezi další možnosti ověření patří například snímání biometrických údajů, jako jsou otisk prstu, sítnice a duhovky oka. Mezi další prvky identifikace patří zadání hesla na klávesnici, nebo číselné kombinace, kterou by měli znát jen oprávnění uživatelé.

Na základně využívaného druhu identifikace musí být vybráno vhodné čtecí, nebo zadávací zařízení těchto parametrů. Jednotlivé způsoby lze samozřejmě i kombinovat. Příkladem může být uveden zámek otisku prstu v kombinaci se zadáním hesla.

1.3.2 Zámkový systém vůči serveru

Komunikace mezi zámkovým systémem a serverem je řešena bezdrátově, nebo pomocí vodičů. Spojení pomocí vodičů se používá na kratší vzdálenosti (uvnitř budov atd.). K tomuto účelu se využívá nejčastěji UTP kabel.

Pro komunikaci bezdrátovou se pak využívá připojení pomocí Wi-Fi, GSM (síť pro mobilní telefony) nebo radiového přenosu (při kmitočtech 80 MHz, 160MHz, 400MHz). [3]

1.4 Správa oprávněných čipů

V této kapitole jsou zmíněny dva hlavní způsoby, jak se dají spravovat oprávněné čipy. Oprávněné čipy jsou takové čipy, které mají do dané oblasti přístup, a po přiložení ke čtecímu zařízení by mělo dojít k odblokování dveří či jiné překážky. Správa oprávněných čipů se tak dělí na lokální a centrální.

Lokální správa čipů

Systém funguje zcela nezávisle na ostatních řídicích jednotkách. Žádné řídicí jednotky nekomunikují navzájem, ani s dalšími subjekty (např. servery). Každá řídicí jednotka v systému (např. budově) má ve své paměti uložené tagy karet, které mají oprávnění ke vstupu. Mezi hlavní nevýhody tohoto systému patří poměrně složitý způsob jeho upravování a aplikování změn, kdy pro změnu jednoho uživatele je nutné obejít všechna místa, kam měl dotyčný uživatel přístup a odstranit jeho tag z paměti oprávněných uživatelů. Obdobně je tomu při přidání nového uživatele, nebo změnách v přístupu. Při použití této technologie je podstatná velikost paměti, na které jsou uloženy oprávněné tagy karet. Z tohoto důvodu se tato možnost volí nejčastěji u méně rozsáhlých systémů s malým počtem uživatelů. [4] [2]

Centrální správa čipů

U systému s centrální správou jsou informace o přístupech do daných oblastí uloženy na centrálním místě, dostupném pro všechny řídící jednotky. Každá jednotka se dotazuje centrálního prvku, který vrátí informaci, zda má daný uživatel přístup. Toto řešení

se aplikuje nejčastěji u rozsáhlých komplexů s velkým počtem uživatelů. Jednou z hlavních výhod je snadnost rekonfigurace systému, kde přidaní, odebrání nebo změna přístupových práv zabere minimum času, a vše je možné udělat z jednoho místa. Nevýhoda této technologie spočívá v tom, že v případě výpadku centrálního prvku je celý systém paralyzován. [4] [2]

Hybridní správa čipů

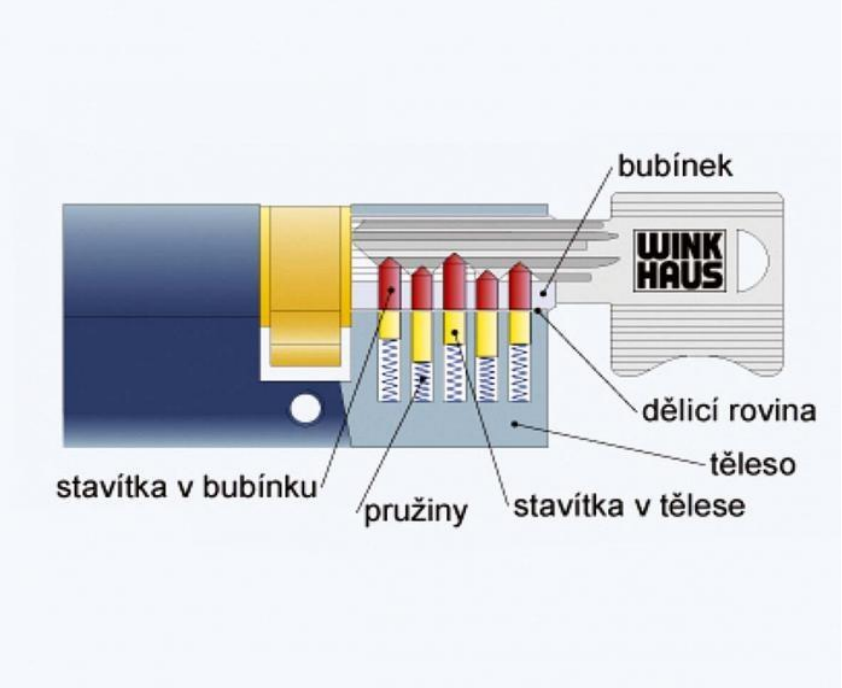
Tento způsob kombinuje výhody předešlých dvou možností. Řídící jednotka se může nejprve podívat do vlastní paměti a v případě, že nenajde shodu, se dotáže centrálního prvku, zda má daný uživatel přístup do dané oblasti. Je tak snadné systém upravovat a zároveň není systém zcela vyřazen výpadkem centrálního prvku. Zda systém používá paměť jen při výpadku centrálního prvku, nebo se dotazuje nejprve vlastní paměti, a teprve poté přistupuje k ověření přes centrální prvek, je již otázkou programu a individuálních potřeb systému.

2 Zámky

Zámky se v dnešní době používají ve zvláště velké míře. Hlavním důvodem použití zámků je zamezení přístupu osobám do určitých prostor. Zámky se rozdělují na mechanické a elektronické. Jejich vlastnosti budou popsány níže.

2.1 Mechanické

Mechanické zámky jsou zámky, které musíme ručně, nebo za pomoci mechanických pomůcek odblokovat. Pro odblokování je nejčastěji využíván klíč. Typů mechanických zámků je nepřeberné množství. Mezi dnes nejpoužívanější zámky patří zámky s cylindrickou vložkou. Princip její funkce je zobrazen níže (Obrázek 2)



Obrázek 2 - Princip funkce cylindrické vložky [5]

Cylindrická vložka má 2 druhy stavítek. Stavítka v bubínku (otočná část klíče) a stavítka v tělese (v nepohyblivé části zámku), kde jsou tato stavítka tlačena proti stavítkům v bubínku pružinkami. Díky tomu, že je každé stavítko jinak dlouhé, musí být na klíči odpovídající profil, při kterém se stavítka bubínku a tělesa dostanou do roviny. Po zasunutí klíče jsou stavítka stlačena do určité polohy. Pokud byl použit nesprávný klíč, stavítka se nedostanou do roviny na úrovni dělící roviny a zámkem nebude možné otočit. Po zasunutí správného klíče jsou stavítka v rovině na úrovni dělící roviny a v tuto chvíli lze otočit klíčem.

Hlavní nevýhodou mechanických zámků je složitá agenda s klíči. Zvláště u rozsáhlých objektů s velkým počtem klíčů a uživatelů. Tento problém pomohl zredukovat generální klíč. Generální klíč je klíč, kterým lze otevřít veškeré dveře v daném komplexu, pro který byl vytvořen. V případě ztráty nebo krádeže takového klíče je nutné vyměnit veškeré zámky v objektu, což bývá velmi nákladné. [5]

2.2 Elektrické

Elektrické zámky se v dnešní době používají stále častěji. Nejčastější použití těchto zámků je ve firmách, hotelových budovách a jiných rozsáhlých objektů s velkým počtem uživatelům, kde dochází k častým změnám osob a jejich oprávnění.

Jedná se o mechanický zámek doplněný o elektrickou část. K otevření dveří není zapotřebí klíče, ale totožnost uživatele, která se ověřuje elektronicky. Ověřování probíhá na základě toho, co člověk zná (PIN nebo heslo) nebo toho, co člověk má (např. identifikační kata), nebo na základě charakteristických znaků daného člověka (biometrické parametry).

Jedním z nejpoužívanějších elektrických zámků je například elektrický otvírač (Obrázek 3). Elektronický otvírač funguje na principu uvolnění západky (nikoliv střelky, jak je tomu u elektrických zámků). Pro uvolnění západky je třeba přivést napětí, typicky 12 - 24 V DC, na zámek. V případě výpadku napájení tak dveře zůstávají zavřené. [6]

Obrázek 3 - Elektrický otvírač [6]

3 RFID

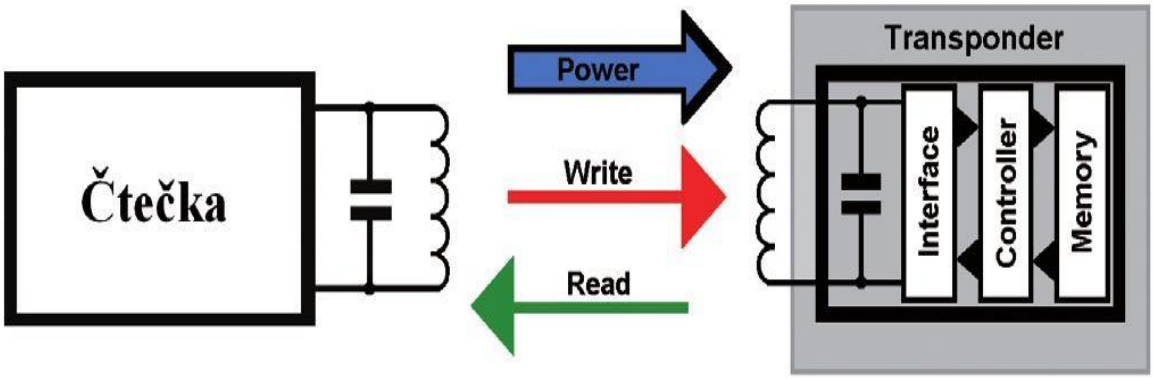
3.1 Historie

Technologie radiové frekvenční identifikace (RFID) byla vynalezena již v roce 1948. Jedno z prvních použití této technologie bylo ve vojenských letadlech jako identifikace, zda se jedná o přátelské či nepřátelské letadlo. Prvního komerčního použití se tato technologie dočkala až roku 1980, kdy se tato technologie začala pomalu rozšiřovat v průmyslu. Průkopníkem této technologie byla firma Wal-Mart, která začala tuto technologii využívat v logistice na označování balíku a zásilek. Postupem času se tato technologie rozšířila do dalších odvětví. RFID se začala využívat například k ochraně zboží, identifikaci zboží ve skladištích a k identifikaci osob pro přístup do střežených prostor. [7]

3.2 Princip RFID

Technologie RFID je založena na principu bezdrátového radiového přenosu dat mezi čtecím zařízením a kartou, nebo čipem obsahujícím jedinečný tag. Tato technologie potřebuje ke své funkci 3 základní prvky. Čtečku RFID karet, RFID transponder (karta s čipem, který obsahuje jedinečný tag, a řídící jednotku, která provádí zpracování přijatých dat od čtečky.

Princip činnosti s pasivním transpondérem je založen na tom, že čtečka nejprve svou anténou vysílá na svém nosném kmitočtu elektromagnetickou vlnu, která vybudí elektromagnetické pole. Jakmile se v elektromagnetickém poli čtečky vyskytne pasivní RFID transponder, tak se v anténě transponderu naindukuje potřebné napětí a nabije se napájecí kondenzátor. Transponder pak odvysílá svá data uložená v paměti (nejčastěji svůj tag). Vysílání transpondéru je zpravidla realizováno pomocí dvoustavové modulace ASK (Amplitude shifting key – což je amplitudová modulace), která je realizována změnou zakončovací impedance (anténa transpondéru je zakončena nakrátko nebo je přizpůsobena). Odrazy vznikající změnou impedance jsou pak detekovány čtečkou a vyhodnoceny jako logické úrovně „0“ a „1“. Princip funkce je zobrazen níže (Obrázek 4). [8]



Obrázek 4 - Princip funkce RFID [8]

3.3 Čtečky

Čtečky jsou zařízení, které umožnují zachytit vysílání pasivního nebo aktivního tagu. Základním faktorem pro správné fungování je předpoklad, že čtečka a transpondér musí pracovat na stejné frekvenci a se stejným protokolem. Jinak nebude čtečka schopna zachytit informace vysílané transpondérem. Čtecí zařízení může pouze číst, nebo může být schopno informace do přikládaných transponderů i zapisovat. Úkolem čtečky tak je zpravidla napájení pasivních transponderů, čtení údajů a jejich zapisování do transponderů, základní filtrace dat, případná detekce chyb.

Základní rozdělení čtecích zařízení je na mobilní a stacionární. Mobilní zařízení se pohybují a transpondéry jsou nepohyblivé. Tuto variantu lze najít například ve skladech, kde je zboží umístěno v regálech a pracovník, který je vybaven mobilní RFID čtečkou, načítá jednotlivé položky ve skladu. Čtečky stacionární jsou umístěné na jednom místě a transpondéry se pohybují. Typickým příkladem může být přístupový systém, kde čtečka je na stabilním místě a transpondér je k ní přikládán. Dalším příkladem může být v logistice statická brána vybavená čtecím zařízením a náklad označený RFID transpondéry, který projíždí bránou.

Vzdálenost pro čtení a zápis se zvyšuje spolu s frekvencí. Neplatí ovšem, že při určité frekvenci je čtecí vzdálenost konstantní. Čtecí vzdálenost je ovlivněna řadou faktorů. Mezi hlavní faktory ovlivňující čtecí vzdálenost patří prostředí (voda, kovy), velikost antén (čtečky i tagu) a také poloha transponderu vůči čtečce. Maximální čtecí vzdálenost udávaná výrobci je tak zpravidla udávána za ideálních podmínek. Při návrhu takového systému je tedy třeba počítat s určitou rezervou a ideálně funkčnost odzkoušet v reálném

čase na konkrétním místě. V případě, že čtecí zařízení umí i zapisovat, je třeba brát v potaz maximální zapisovací vzdálenost, ta je zpravidla výrazně menší než čtecí vzdálenost. Pro správou funkci takové čtečky je zapotřebí umístit čtecí zařízení do vzdálenosti umožňující bezpečný zápis do transpondéru. [9] [10]

Obrázek 5 - Čtečka RFID [11]

3.4 Čipy (transpondéry)

Čipy jsou základním prvkem RFID technologie. Obsahují informaci, kterou chceme zjistit (identifikaci daného objektu) a skládají se z těchto částí:

Anténa – Anténa slouží pro komunikaci čipu s čtecím zařízením a obráceně. Definuje radiofrekvenční charakteristiky. U pasivních čipů slouží také k získání potřebné energie pro aktivaci procesoru. Proto se za anténou většinou nachází ještě nabíjecí kondenzátor, který uchovává energii a s ní následně napájí procesor po dobu nezbytnou na odeslání dat, nebo vykonání jiných instrukcí.

Procesor – Zajišťuje čtení z paměti, zápis do paměti a odesílání dat zpět čtecímu zařízení.

Paměť – Na paměť čipu se ukládají informace, které jsou poté předány čtecímu zařízení. Více v kapitole 3.4.1.

Baterie – Baterie se nachází pouze u čipů aktivních a semipasivních.

Základní rozdělení čipů je na aktivní, pasivní a semipasivní čipy. Každý z těchto druhů má specifické vlastnosti a různé způsoby použití, které jsou podrobněji popsány níže. [2] [8]

Aktivní čipy:

Aktivní čipy jsou čipy, které obsahují vlastní napájení (baterii). Tyto čipy jsou oproti pasivním neustále aktivní a mohou vysílají své informace do okolí nepřetržitě. Nepotřebují tedy jako pasivní čipy přítomnost čtecího zařízení. Díky přítomnosti vlastní baterie je možné doplnit k transpondéru některé senzory, díky kterým je pak možné zaznamenávat další hodnoty a ukládat je do paměti. Mezi nejpoužívanější senzory se řadí senzory teploty, otřesů a vlhkosti. Tyto hodnoty mohu být v pravidelných intervalech snímány a ukládány do paměti čipu. Uložené hodnoty slouží poté pro případnou kontrolu, jak bylo s daným výrobkem nakládáno a v jakých podmínkách byl přepravován (využívá se zejména při převozu aut nebo potravin umístěných v chladících boxech).

Za výhodu těchto čipů lze považovat jejich zvýšený dosah, který činí až řády stovek metrů. Dosah těchto čipů se odvíjí od použitého typu baterie a frekvence.

Nevýhodou těchto čipů je jejich životnost, která je díky baterii většinou 3 až 5 let a oproti čipům pasivním jsou dražší. Jejich použití tedy není tak časté jako u pasivních čipů, neboť jsou složitější a dražší.

Používají se nejčastěji pro aktivní lokalizaci, díky své možnosti neustále vysílat do okolí svá data. Dalšími případy použití nalezneme v logistice při transportech velkých kontejnerů a v automobilovém průmyslu. [9] [2]

Pasivní čipy:

Jedná se o čipy, které nejsou vybaveny vlastím napájením. Energie se získává z elektromagnetického pole čtečky, která nabije napájecí kondenzátor umístěný v transpondéru a poté dojde k odvysílání vlastních dat. Z tohoto důvodu čip vysílá svá data pouze, pokud je v přítomnosti čtecího zařízení. Pasivní čipy obsahují minimum součástí,

tvoří je anténa, napájecí kondenzátor, paměť a procesor, díky čemu jsou velmi levné a mají velmi dlouho životnost, jsou téměř nezničitelné.

Mezi hlavní výhody patří velmi nízká cena a dlouhá životnost.

Z důvodů absence baterie mají nižší dosah, který činí 3 cm až 3 m v závislosti na použité frekvenci (podrobnosti naleznete v kapitole 3.5).

Tyto čipy se nejčastěji používají pro řízení přístupu osob do objektů, jejich evidenci v docházkových systémech, a také k identifikaci zboží, jako nástupce čárových kódů. [9] [2]

Obrázek 6 - Pasivní čip [12]

Semipasivní čipy:

Jedná se o pasivní čipy, které jsou vybaveny baterií, která však neslouží pro napájení čipu. Baterií jsou napájeny snímače, které ukládají své informace do paměti čipu a při přiložení ke čtecímu zařízení jsou tyto informace spolu s identifikačním číslem odeslány čtecímu zařízení. [2]

3.4.1 Paměť čipů

Velikost pamětí se liší podle účelu použití. Velikost pamětí čipů RFID se pohybuje od 4B do 8kB. U aktivních čipů může paměť dosahovat i hodnot vyšších.

Kromě prostého uložení existuje ještě celá řada dalších možností, jako jsou například šifrování uložených dat, ochrana proti přepsání, zakódování dat, jejich zpřístupnění po zadání pinu atd. [14]

Paměti se dělí na tyto tři základní kategorie:

Read-Only – Tato paměť je, jak už její název napovídá, pouze ke čtení. Tento druh paměti nese většinou pouze unikátní identifikační číslo, které je do paměti nahráno již ve výrobě a nelze jej měnit. Nejčastěji se používá v přístupových systémech, nebo pro elektronickou ochranu zboží.

Read-Write – Tento druh umožnuje opakované přepsání dat jak výrobcem, tak zákazníkem. Jedná se o nejdražší typ. Velikost paměti u aktivních čipů se může dostat až na hodnotu 2 MB. Do této paměti se většinou ukládá krom identifikačního čísla i celá řada dalších informací.

Write Once.Read Mandy – Tento typ paměti je stejný jako Read-Only s tím rozdílem, že paměť lze jednou přepsat. Poté, co se provede zápis do paměti, se již paměť chová jako klasická Read-Only paměť. [12]

3.5 Frekvenční pásmo

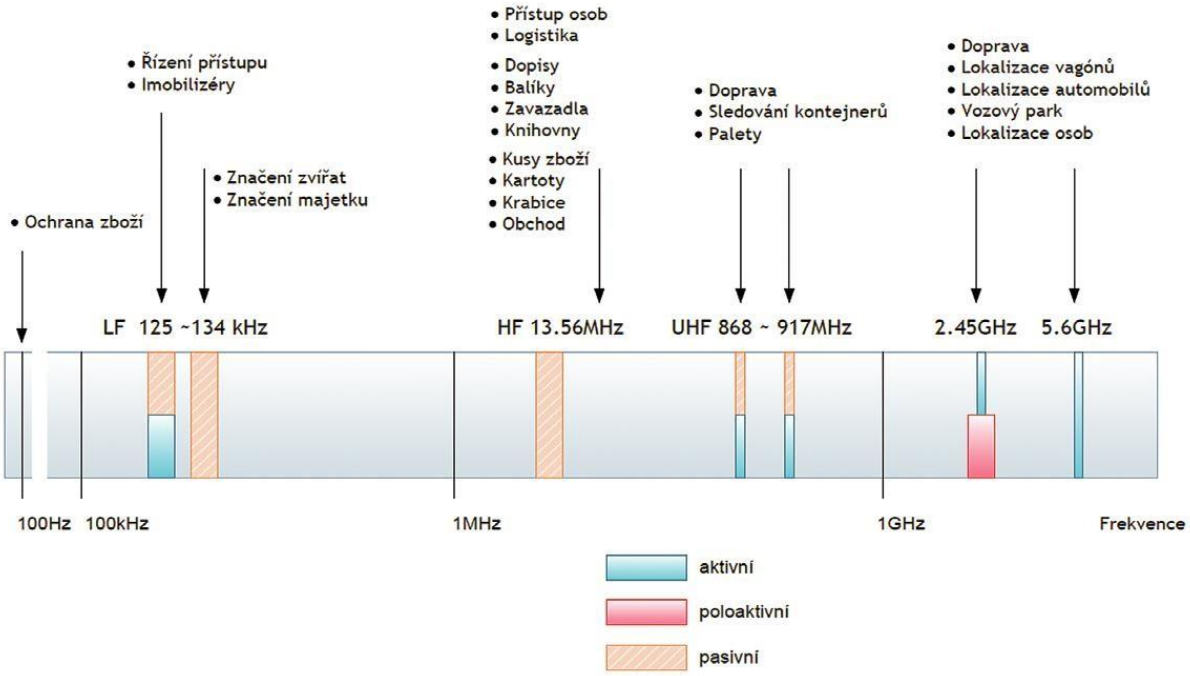
Od použité komunikační frekvence se odvíjí to, jaký bude dosah, přenosová rychlost, míra spolehlivosti přenosu v určitém prostředí a také velikost celého transpondéru. Od zvolené frekvence se odvíjí velikost antény - čím nižší je frekvence, tím větší musí být anténa. Při překročení frekvence 100 MHz se mění typ antény z cívky na dipólovou anténu.

Základní rozdělení frekvencí je na nízkofrekvenční (125–134 kHz), vysokofrekvenční (13,56MHz), ultrafrekvenční (860–960MHz) a mirkovlné (2,4 GHz). [15]

Tabulka 1 - Frekvence RFID a jejich vlastnosti [15]

Komunikační frekvence	Čtecí dosah	Výhody	Nevýhody	Použití
125 – 134 kHz	Do 0,5 m	Větší odolnost proti rušení, možnost upevnění v blízkosti tekutin a na kovové podložce.	Malý čtecí dosah a nízká komunikační rychlost, velká anténa.	Kontrola přístupu, identifikace zvířat, ochrana zboží.
13,56 MHz	Do 1 m	Menší rozměry antény, větší komunikační rychlost, větší čtecí dosah, nejvíce rozšířené, celosvětově standardizovaná frekvence.	Kovové podložky a voda významně snižují čtecí dosah a ruší komunikaci.	Chytré karty, bezkontaktní placení, označování zavazadel při přepravě, záznam a přenos naměřených dat, sledování palet a beden při přepravě a ve skladech.
860 – 960 MHz	Do 10 m	Možnost i vzdáleného čtení - indentifikace průjezdem brány, velká přenosová rychlost = možná větší kapacita paměti RFID tagu, dipólová anténa, levná výroba.	Nemožnost čtení přes kapaliny a na kovových podložkách, celosvětově nejednotná frekvence, problémy s odrazem od okolních kovových konstrukcí.	Současná identifikace více zabalených produktů, elektronické mýtné, parkovací karty, sledování toku vratných obalů, sledování palet při přepravě a ve skladech.
2,4 GHz	Desítky metrů	Vysoká přenosová rychlost až 2 Mb/s malé rozměry dipólové antény.	Drahá a složitá konstrukce, velký vliv rušení (kovu, kapalin apod.).	Elektronické mýtné, identifikace zavazadel při letecké přepravě, bezdrátový záznam a přenos dat v reálném čase.

Přehled používaných frekvencí je zobrazen na obrázku 7.



Obrázek 7 - Přehled používaných frekvencí [8]

4 Praktická realizace

V této kapitole bude popsáno, jak byl řešen návrh konkrétního funkčního zařízení pro ovládání přístupu v budově. Přístupový systém se skládá z více součástí. Tyto jednotlivé součásti budou popsány v následujících kapitolách.

Hardware pro jedny dveře se skládá z řídící jednotky, čtecího zařízení, napájení a elektronického zámku. Tento hardware bude aplikován u všech dveří v objektu, kde bude vyžadováno elektronické otevírání dveří pomocí RFID karet. V celém přístupovém systému je tak několik řídících jednotek, které o sobě navzájem „nevědí“ a neprovádí spolu žádnou komunikaci. Každá řídící jednotka se stará jen sama o sebe a případné dotazy směřuje na databázi přes LAN. Čtecí zařízení bude popsáno podrobněji v kapitole 4.1.2. Vývojový kit vyhodnocuje příchozí data a provádí řízení celého systému včetně komunikace s uživatelem pomocí třech barevných diod, které slouží pro signalizaci určitých stavů. Systém má hybridní charakter, což znamená, že některá data bude mít systém uložen v paměti na každé řídící jednotce a zbytek dat, která se nebudou v daném okamžiku nacházet v paměti řídící jednoty, bude ověřovat vůči serveru pomocí připojení přes Wi-Fi. Systém pracuje na 125 kHz, což je totožná frekvence, na které jsou stávající studentské a zaměstnanecké karty. Dojde tak ke změně hardwaru i softwaru, ale nebude třeba měnit jednotlivé identifikační karty, což by znamenalo vyšší náklady a administrativně náročný proces. Napájení je popsáno v kapitole 4.2.

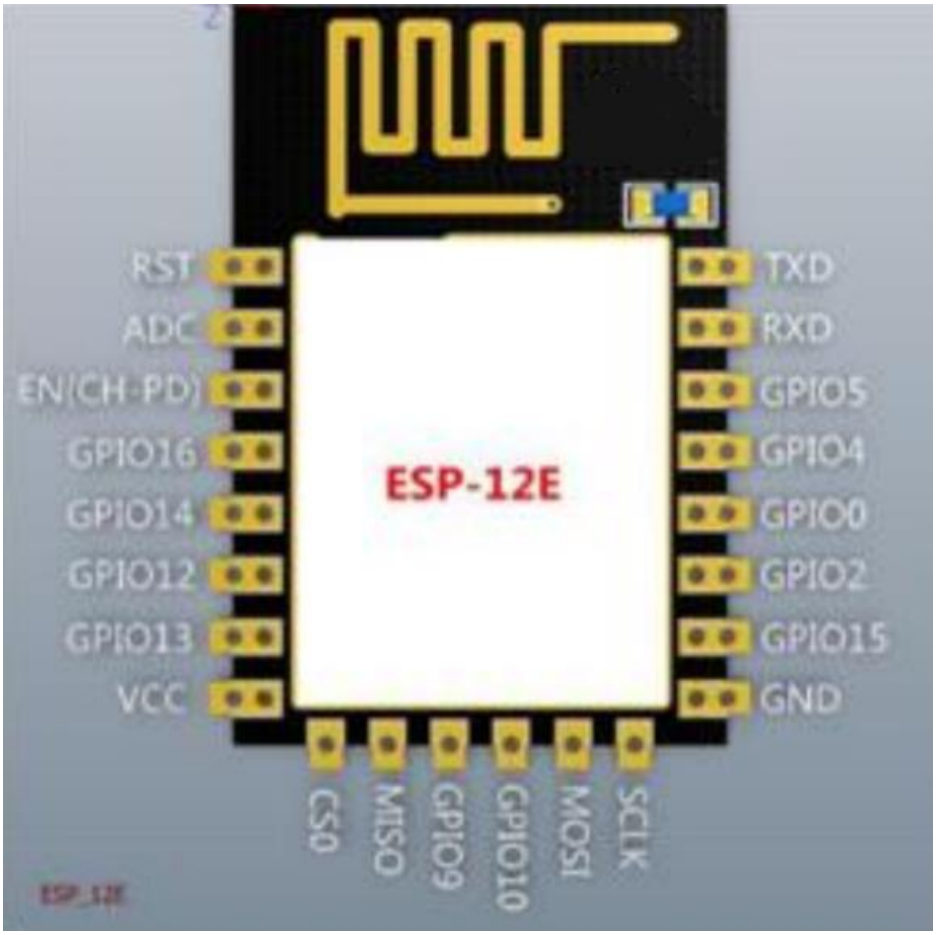
4.1 Zvolené komponenty

V této kapitole budou popsány jednotlivé komponenty, které byly použity pro realizaci vybraného přístupového systému.

4.1.1 Použitý Wi-Fi modul

Pro toto konkrétní řešení byl vybrán Wi-Fi modul ESP-12E s procesorem ESP8266. Hlavním důvodem pro zvolení tohoto modulu byla jeho možnost komunikace přes Wi-Fi a také fakt, že tímto modulem je osazena vývojová deska nodeMCU, která bude použita. Více informací o vývojové desce naleznete v kapitole 4.1.2.

Procesor ESP8266 od firmy Espressif Systems je 32 bitovým procesorem.



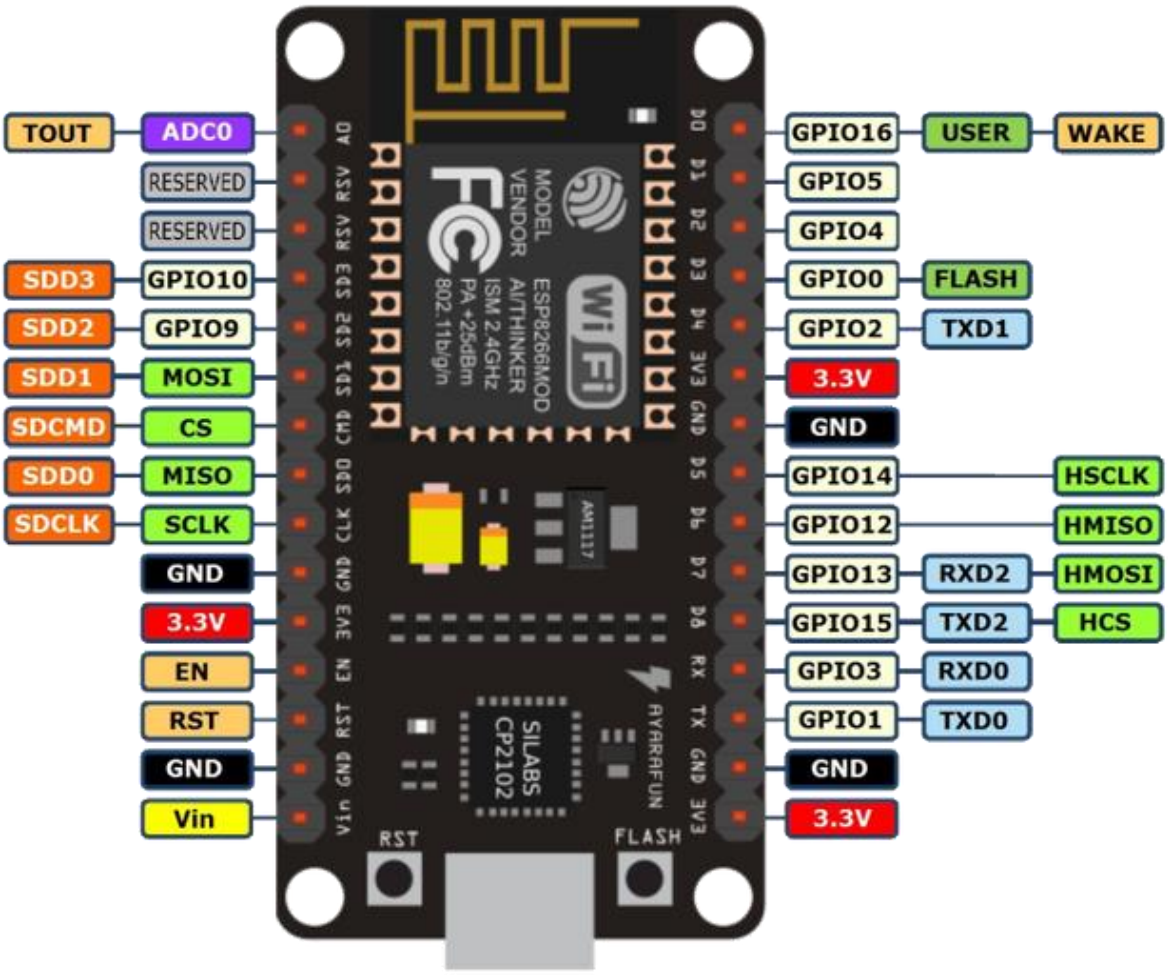
Obrázek 8 - ESP-12E piny [16]

Vlastnosti modulu: [16]

- 32 bitový procesor Tensilica L106
- 4 MB externí flash paměti
- 11 digitálně vstupně výstupních pinů, z nichž používáme D2, D4, D5, D6, D7
- Napájení 3,3 V

4.1.2 Vývojová deska

Jako vývojová deska byla zvolena nodeMCU, jejíž hlavní částí je již zmíněný modul ESP-12E s čipem ESP8266. V prostředí arduino IDE byla vytvořena podpora pro tuto desku. Veškeré vývody ESP8266 jsou na desce vyvedeny na dvě pin lišty. Deska má na všech I/O pinech přerušení, PWM, I2C a 1-Wire, mimo pin D0. Deska je osazena konektorem USB Micro s připojeným UART převodníkem. Díky tomu je možné desku připojit přes USB k počítači. Použitý převodník je CP2102. Deska je napájena přes USB konektor nebo přivedením 5 V na pin Vin. [17]

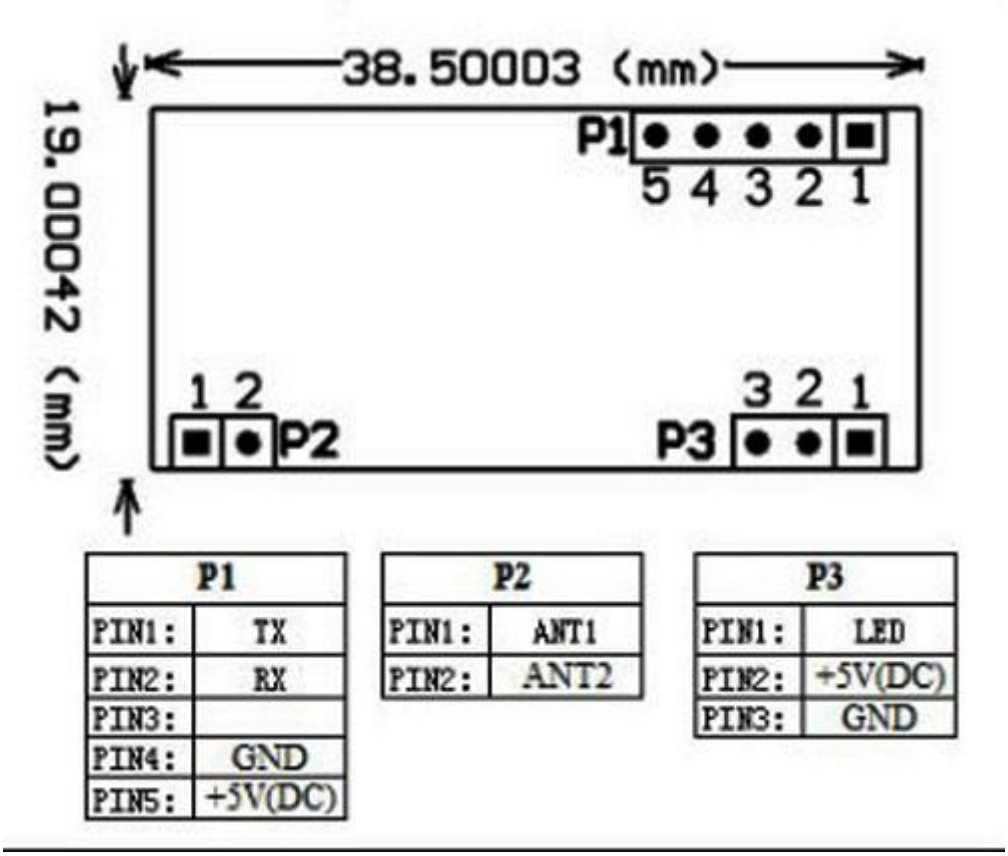


Obrázek 9 - Vývojová deska nodeMCU [17]

Rozdíl mezi verzemi 2 a 3 je ve velikosti desky (verze 2 je menší) a v použitém převodníku.

4.1.3 Čtecí zařízení a protokol EM4100

Pro čtení čipů byl zvolen modul RDM6300, který je osazen čipem s implementovaným protokolem EM4100 se schopností číst studentské a zaměstnanecké karty. Celé zařízení pracuje na frekvenci 125 kHz a je schopno číst nízkofrekvenční karty s pamětí Read-only, což odpovídá uvedeným kartám, které mají aktuálně všichni studenti a zaměstnanci Univerzity Pardubice. Zařízení není určeno pro zápis, umí pouze číst data.



P1	
PIN1:	TX
PIN2:	RX
PIN3:	
PIN4:	GND
PIN5:	+5V(DC)

P2	
PIN1:	ANT1
PIN2:	ANT2

P3	
PIN1:	LED
PIN2:	+5V(DC)
PIN3:	GND

Obrázek 10 - RDM6300 piny [18]

Pro aktuální potřeby postačí zapojit napájení na P1 (piny 5 a 4), data (pin 1) a anténu čtečky na P2 (piny 1 a 2).

Obrázek 11 - Použité čtecí zařízení RDM6300 [18]

Specifikace čtečky: [19]

- Kmitočet: 125 kHz
- Napájení: 5 V
- Pouze pro čtení karet (Protokol EM4100)
- Rychlost: 9600 Bd
- Dosah: 20 až 50 mm
- Odběr: <50 mA
- Rozhraní: UART, který používáme

Čtečka zpracuje přijatá data (Obrázek 12), která pak odesílá po sériové lince (14 byte) ve formátu 1B start byte, 2B jsou typ tagu, 8B identifikační číslo – tag, 2B kontrolní součet, 1B stop byte.

Obrázek 12 - Data odesílaná čtecím zařízením [20]

Protokol EM4100

Aby bylo možné správně načíst data z RFID transponderu, musí čtečka vědět, v jakém formátu jsou data uložena a mít protokol pro jejich extrahování. Nejrozšířenějším protokolem je protokol EM4100 od firmy EM Microelectronic. Transpondéry kompatibilní s EM4100 mají Read-Only pamět o velikosti 64 b. Data jsou do paměti nahrána již od výrobce a již je nelze měnit. Formát dat je zobrazen na obrázku 13.

1	1	1	1	1	1	1	1	1	9 bit header bits, all 1's
8 bit version number or customer ID.				D00	D01	D02	D03	P0	
				D04	D05	D06	D07	P1	
				D08	D09	D10	D11	P2	Each group of 4 bits
				D12	D13	D14	D15	P3	is followed by an Even
32 Data Bits				D16	D17	D18	D19	P4	parity bit
				D20	D21	D22	D23	P5	
				D24	D25	D26	D27	P6	
				D28	D29	D30	D31	P7	
				D32	D33	D34	D35	P8	
				D36	D37	D38	D39	P9	
4 column Parity bits				PC0	PC1	PC2	PC3	S0	1 stop bit (0)

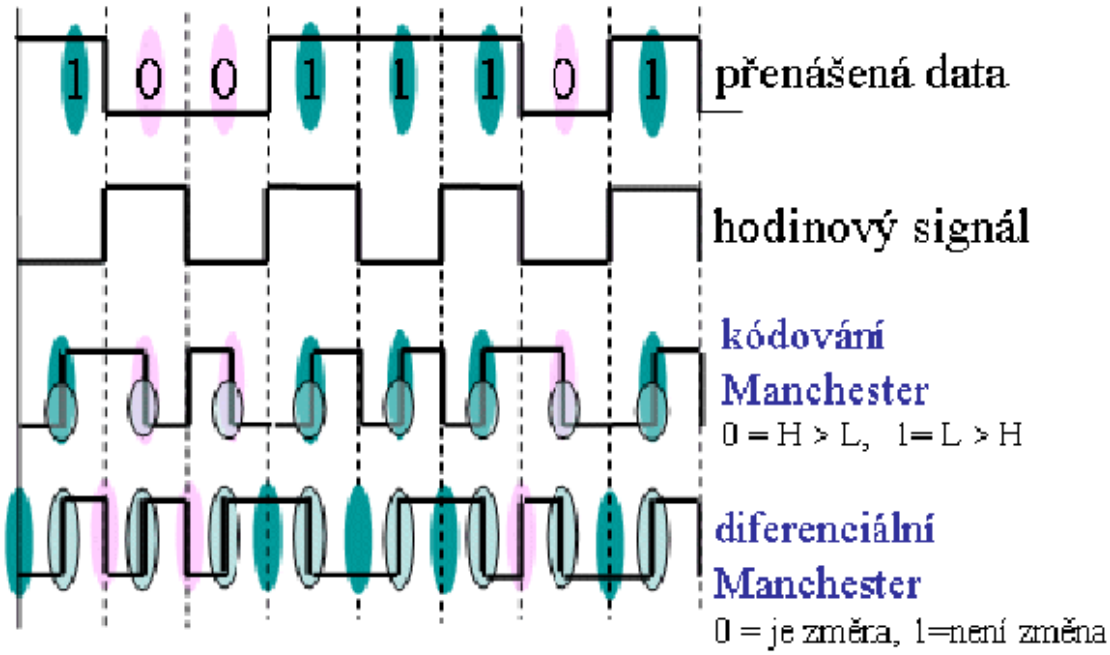
Obrázek 13 - Formát dat EM4100 [21]

Jak je z obrázku patrné, data jsou rozdělena do pěti skupin. Prvních 9b je záhlaví, které slouží jako indikace začátku řetězce. Následuje deset skupin po čtyřech bitech dat (D00 až D39), které jsou vždy zakončeny paritou řádku. V bitech D00 až D07 je uložena verze

tagu, pak následuje samotný tag (D08 až D39). Po sekvenci dat následuje 4b sloupcové parity a jeden stop bit. Máme tedy záhlaví, data, parita (P0 až P9), sloupcová parita (PC0 až PC3) a stop bit (S0)

Po vložení karty do blízkosti čtečky dojde k nabití napájecího kondenzátoru v transpondéru a ten začne vysílat. Po správném přečtení startovací části začne čtečka číst data (10 x 4 + 1 parita). Nakonec je transpondérem odeslaná sekvence čtyř paritních bitů a jednoho ukončovacího bitu. Transpondér vysílá, dokud nedojde k vybití kondenzátoru. [21]

Informace se z RFID transpondéru přenáší do čtecího zařízení pomocí modulace nosného signálu. Možností kódování je více, u protokolu EM4100 se ovšem nejčastěji používá kódování manchester (Obrázek 14).



Obrázek 14 - Kódování manchester [22]

U kódování manchester se „užitečná“ informace přenáší uprostřed bitového intervalu. Jestliže je změna signálu z nízké hodnoty na vysokou, pak to značí log. 1. Při změně signálu z vysoké hodnoty na nízkou je reprezentována log. 0. [22]

4.1.4 Elektronický zámek

Pro otevírání dveří bude použit elektrický otvírač 511 Standard. Zámek má mechanickou odolnost proti vylomení 590 kg. Zámek se nachází v poloze otevřeno jen po dobu, kdy je

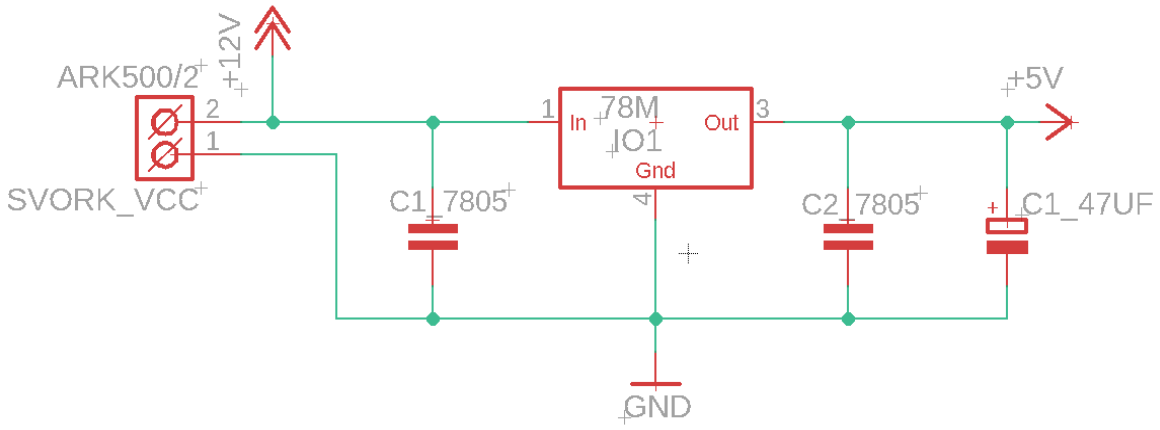
na něj přivedeno napětí. Mimo tuto dobu jsou dveře zavřeny. Zámek je univerzální pro pravé i levé dveře. [18]

Obrázek 15 - Elektrický otvírač FAB klasik 511 [18]

- Odběr cívek: 12 V DC, 600 mA
- Maximální doba otevření je 60 s
- Doba otevření při oprávněném přístupu je 2 s

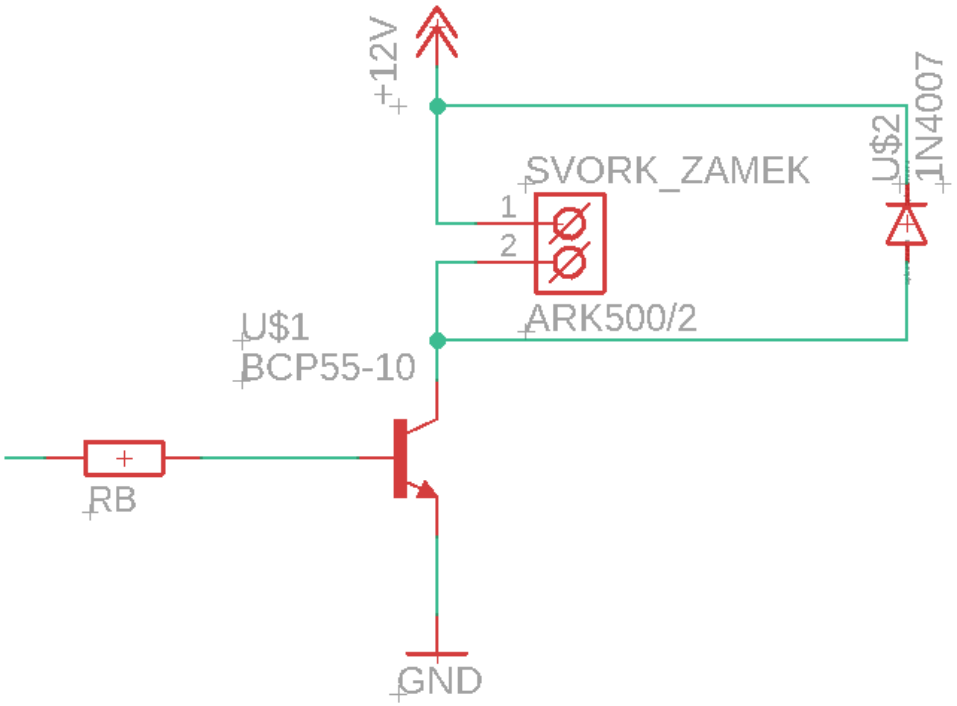
4.2 Napájení

Napájení bude realizováno připojením vodičů 12 V DC, které jsou v místech montáže zámku již vyvedeny. Pro napájení čtecího zařízení a vývojové desky nodeMCU je použito stabilizované napětí 5 V pomocí stabilizátoru 7805. Schéma zapojení je uvedeno na obrázku níže (Obrázek 16). Celkové schéma zapojení je uvedeno v příloze A.



Obrázek 16 - Zapojení stabilizátoru

Samotná deska nodeMCU není schopna dodat tak velký proud, který je potřebný k otevření zámku (600 mA), maximální možný proud na GPIO pinech je pouze 12 mA. Z tohoto důvodu je spínání zámku řešeno pomocí tranzistoru BCP55 zapojeného jako spínač. Do báze tranzistoru tak je připojen výstup GPIO z nodeMCU, kterým se tranzistor spíná.



Obrázek 17 - Zapojení tranzistoru

Dioda je v zapojení z důvodu eliminace napěťové špičky, kterou vyvolá cívka uvnitř zámku při rozepnutí obvodu. Zámek pro své otevření potřebuje 600 mA, z tohoto důvodu

byl zvolen tranzistor BCP 55-10, který má maximální proud I_c roven 1 A. Hodnota odporu báze R_B byla vypočítána podle následujícího postupu.

$$I_{Bmin} = \frac{I_C}{h21E} = \frac{0,6}{63} = 9,52\ mA$$

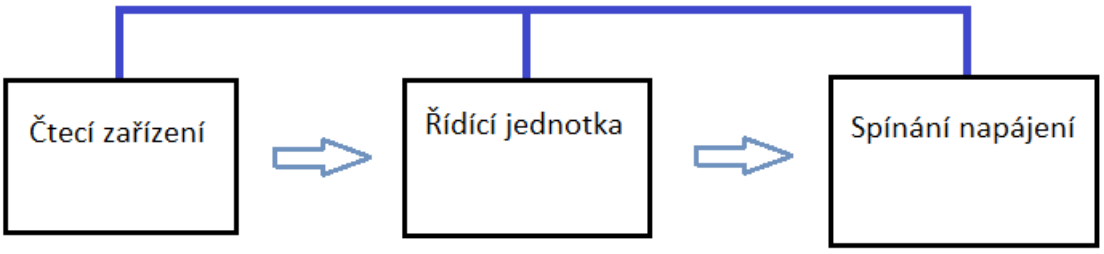
- I_{Bmin} je minimální proud báze pro sepnutí zámku
- I_C je proud kolektorem
- h21E je proudový zesilovací činitel (zjistíme v datasheetu a bereme nejnižší hodnotu)

Odpor báze se pak vypočte:

$$R_B = \frac{U_0 - U_{BE}}{I_B} = \frac{3,3 - 0,6}{10\ mA} = 270\Omega$$

- R_B je odpor báze
- U_0 je napětí přivedené z pinu desky nodeMCU
- U_{BE} je napětí báze emitor
- I_B je proud báze

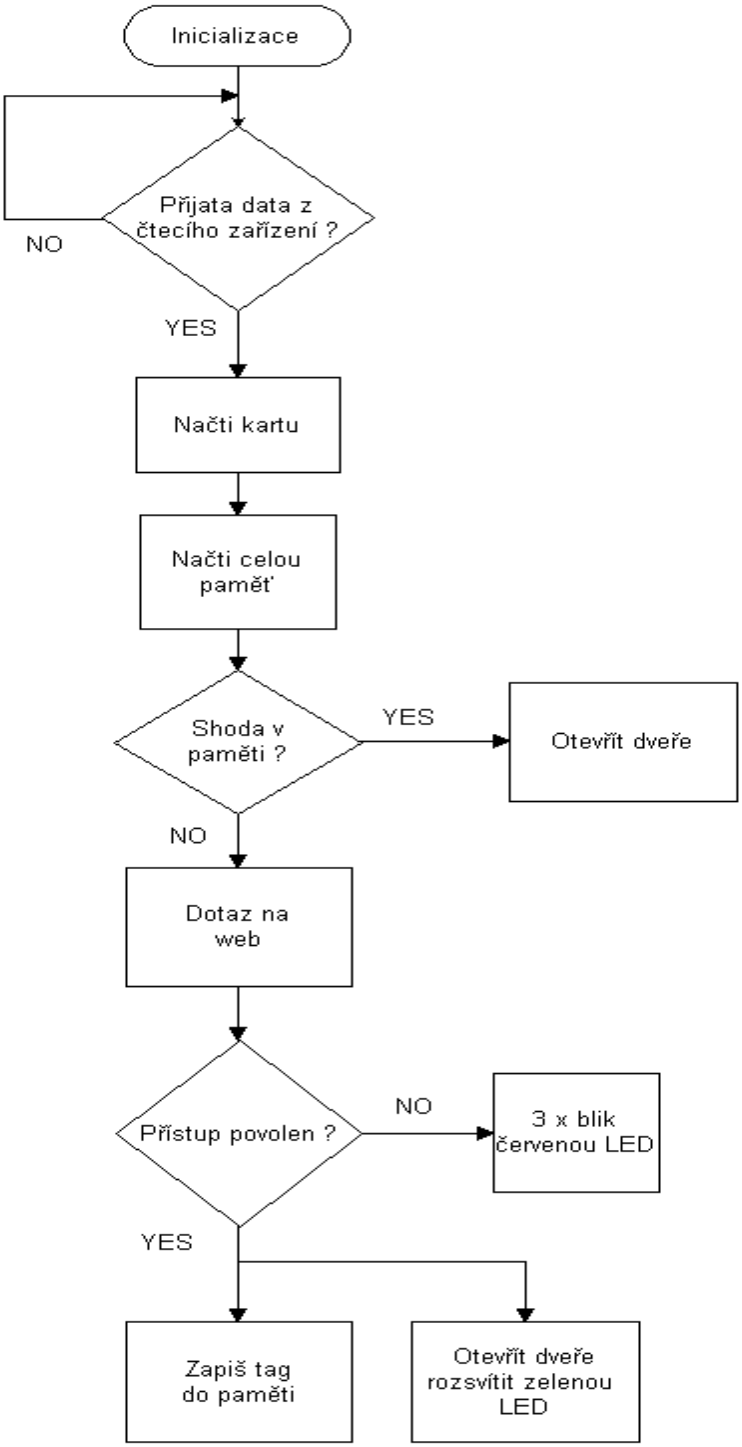
4.3 Blokové schéma zapojení



Obrázek 18 - Blokové schéma zapojení

5 Software

Software je napsán v jazyce Wiring v programu Arduino IDE 1.8.7. Vývojový diagram (Obrázek 19) byl navrhnut v programu Diagram Designer.1.29.3.



Obrázek 19 - Vývojový diagram

Program lze rozdělit na několik hlavních částí. Do těchto částí patří jednotlivé funkce jako jsou načti kartu, načti celou paměť, najdi shodu, dotaz na web, zapiš na paměť a připojení Wi-Fi. Ostatní část kódu pak tvoří inicializace a podmínky.

Načti kartu – V této funkci se do proměnné uloží všech 14 B z čtečky, které se následně ořízou tak, aby zbyl samotný osmibajtový tag. Následně dojde k převodu tagu z datového typu char na datový typ string. Tento string funkce vrátí pomocí příkazu return.

Načti celou paměť – V této funkci je vytvořena proměnná typu char, do které je načtena celá paměť pomocí příkazu EEPROM.read(i), který je umístěn ve smyčce for. Poté je proměnná převedena na datový typ string, který je funkcí vrácen pomocí příkazu return.

Najdi shodu – Tato funkce slouží k vyhledávání v textu. Pomocí příkazu indexof, který prochází celou paměť, která byla uložena do proměnné typu string. V paměti se program snaží najít shodu s tagem, který byl získán z funkce načti kartu. Najde-li program shodu, uloží do proměnné, kterou následně vrací pomocí příkazu return log. 1, pokud shodu nenajde, uloží do proměnné log. 0.

Dotaz na web – Pokud dojde k zavolání této funkce, tak dojde k sestavení dotazu, který je následně odeslán pomocí funkce client.print(dotaz). Poté program vyčkává na odpověď, která je uložena do proměnné typu string. V odpovědi se nachází log. 1, nebo log. 0 v závislosti na tom, zda daná karta přístup má či ne.

Připojení Wi-Fi – V této funkci dojde k připojení Wi-Fi pomocí příkazu wifi.begin, příklad této funkce je zobrazen na obrázku 20.

Zapiš na paměť – Dojde-li k zavolání této funkce, dojde k ověření adresy, na kterou jsou data ukládána, aby nedošlo k jejímu přetečení. Po ověření přetečení adresy se po znacích uloží tag do paměti na aktuální adresu.

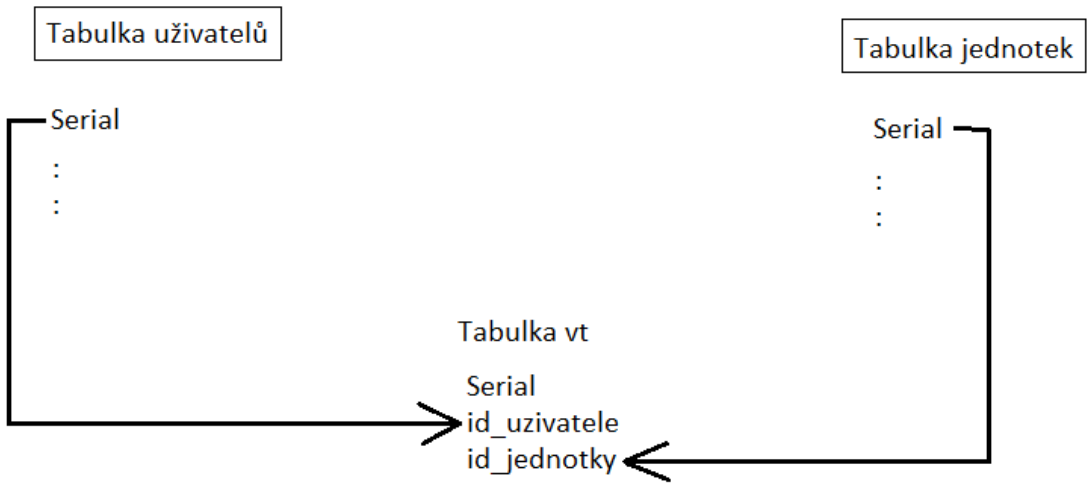
Vzorový příklad kódu, pomocí něhož je možno zprovoznit Wi-Fi (Obrázek 20).

```
#include <ESP8266WiFi.h>

//Proměnné pro připojení
const char* ssid = "NÁZEV WIFI";
const char* password = "HESLO";

void setup()
{
  WiFi.begin(ssid, password); //přihlášení na wifi
}

void loop()
{

}
```

Obrázek 20 - Ukázka kódu pro připojení k Wi-Fi

5.1 Správa přístupového systému

Software pro správu oprávněných čipů je napsán v jazyce php. Požadavkem pro správné fungování je nakonfigurovaný webový server s podporou mysql a php (běžně označováno jako LAMP). Celý kód je rozdělen do 3 souborů. Prvním je config.php, kde je definováno jméno databázového serveru, dále název databáze (v našem případě **accesscontrol**), přihlašovací jméno a heslo pro přístup do databáze. V druhém souboru checkaccess.php je pak kód, který odpovídá na dotazy od jednotek. Nejprve dojde k připojení pomocí příkazu mysql_connect (hostname, username, password, název databáze). Poté se vybírá id jednotky a id uživatele z tabulky vt (vazební tabulka). Najde-li shodu na jednom řádku (dané id jednotky se nalézá na stejném řádku jako id uživatele který má přiřazený tag), pak je odeslána log. 1 pomocí příkazu echo. Tabulka vt je tabulka, kde jsou spojeny jednotlivé id uživatelů a jednotek ke kterým mají přístup. Sloupec **serial** je číslo, které se automaticky inkrementuje o jedničku s přidáním dalšího záznamu, zároveň je unikátní v dané tabulce, tj. po smazání některého záznamu už jeho původní hodnota serial nebude použita. Jak vypadá tabulka vt je zobrazeno na obrázku níže (Obrázek 21).



Obrázek 21 - Vt tabulka

Definování jednotek, uživatelů a jejich přístupů je řešen ve skriptu index.php formou jednoduchých formulářů na adrese http://accesscontrol.rolda.cz. Kód skriptu je rozdělen do několika hlavních funkcí. Mezi hlavní funkce pak patří přidání jednotky, odebrání jednotky, přidání uživatele, odebrání uživatele a nastavení oprávnění přístupu pro jednotlivé uživatele (editace).

Přidání jednotky – Zde jsou zadány parametry popis a id. Ty jsou následně odeslány a uloženy do tabulky jednotek.

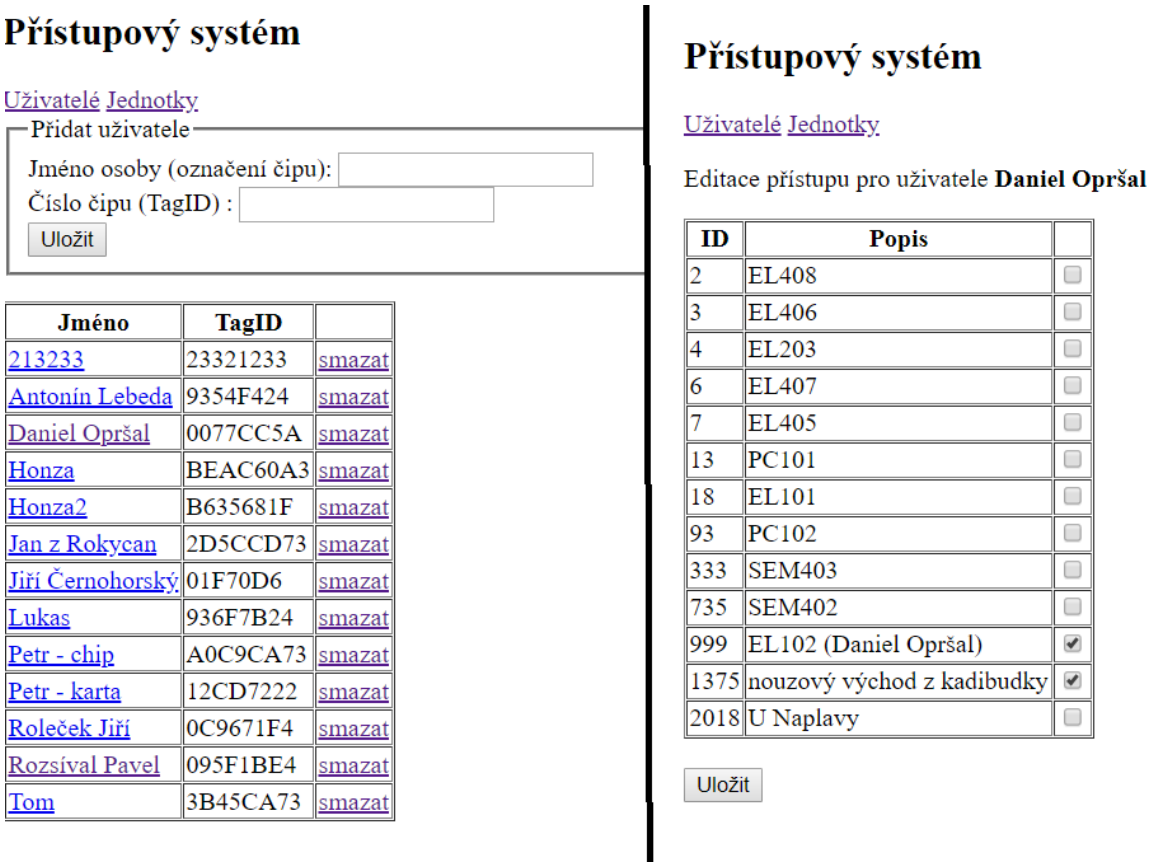
Mazání jednotky – Pokud se v adresním řádku nachází menu = „jednotky“, tak program ví, že se nachází v tabulce s jednotkami, a pokud dojde ke stisknutí smazat dojde k odeslání příkazu, který smaže z tabulky jednotek řádek, ve kterém se nachází daná jednotka. Řádek je označen číslem serial. Poté program smaže veškeré záznamy ve vt tabulce, které obsahují dané id jednotky.

Přidání uživatele – pokud jsou zadány parametry jméno a čip a dojde k jejich odeslání, tak dojde k uložení těchto hodnot do tabulky uživatelů na řádek odpovídající aktuálnímu serial.

Odebrání uživatele – Pokud se v adresním řádku nachází menu = „“, tak program pozná, že se nachází v tabulce uživatelů. Pokud dojde ke stisknutí smazat, pak se odešle příkaz,

který smaže v tabulce uživatelů daného uživatele. Poté dojde ke smazaní všech záznamů v tabulce vt, které obsahují tagID přiřazený ke konkrétnímu uživateli.

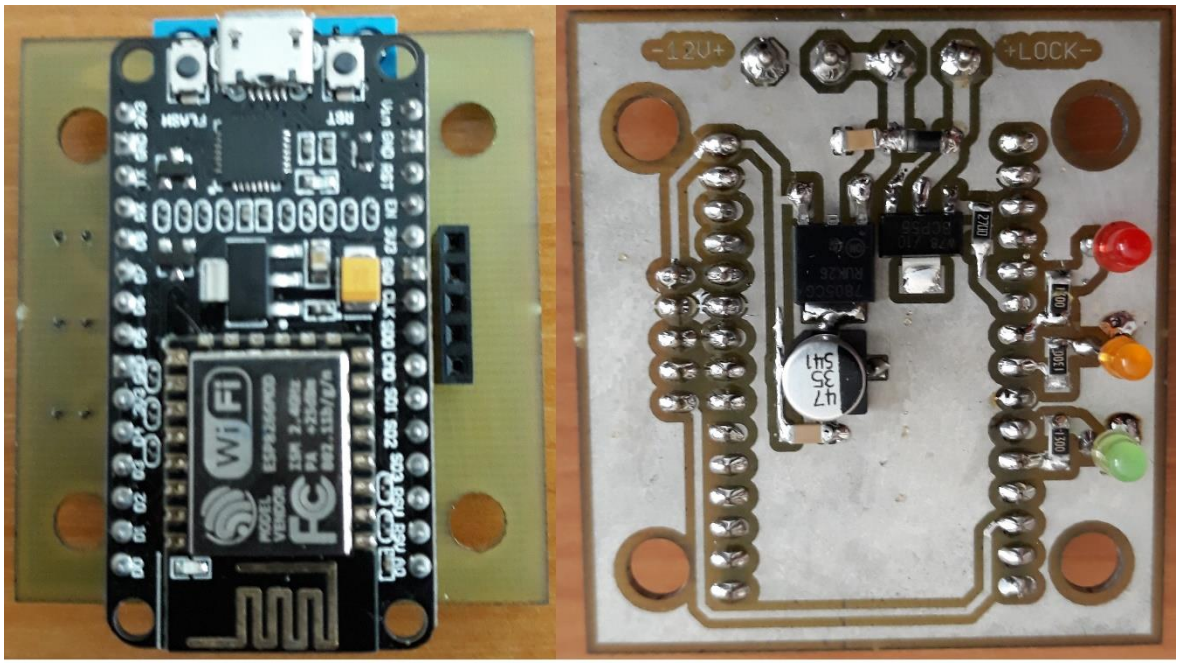
Správa oprávněných přístupů – V tabulce uživatelů je možno otevřít konkrétního uživatele a přiřadit zde přístupy k jednotlivým dveřím pomocí zaškrtávacích polí.



Obrázek 22 - Správa oprávněných přístupů

6 Ověření funkčnosti

Finální zařízení je zobrazeno na obrázku 23.



Obrázek 23 - Fotografie výsledného produktu

Celé zařízení po připojení k napájení funguje dle očekávání. Zelená led dioda svítí, jestliže je připojena Wi-Fi. Oranžová led dioda svítí, jestliže je přiložena karta a svítí po celou dobu vyhodnocování. Červenou led diodou jsou indikovány dva stavy. Zamítnutí přístupu je indikováno tím, že třikrát blikne červená led dioda. Povolený přístup je indikován rozsvícením červené led diody po dobu otevření zámku (v našem případě 2 s). Chybový stav je indikován všemi zhasnutými led diodami.

Závěr

Cílem práce bylo navrhnout a realizovat zámkový systém s ověřením přes LAN. Zámkový systém po přiložení karty správně vyhodnotí, zda má nebo nemá karta přístup, k tomu využívá vlastní paměť, nebo se dotazuje serveru.

V teoretické části byl popsán princip fungování RFID technologie, možnosti a způsoby ověřování osob vůči zámkovému systému nebo serveru. Pro správu oprávněných čipů byl napsán jednoduchý software, ve kterém může uživatel měnit přístupová práva jednotlivým uživatelům a zároveň přidávat nebo mazat jednotlivé uživatele a jednotky.

V praktické části byl popsán postup pro návrh konkrétního řešení, které bude využito v prostorách Univerzity Pardubice. Na DPS je čtecí zařízení a jednotka upevněna v pin lištách. Toto řešení bylo zvoleno pro snadnou výměnu jednotlivých komponent. Možností, jak systém rozšířit je více. Jednou z možností vylepšení by bylo přidání dalších snímačů (klávesnice, snímač otisku prstů a dalších biometrických údajů). Pro tuto variantu by bylo vhodné přidání externího úložiště (například SD karty). Další možností je ukládat informace o času a datu průchodu.

Literatura

[1] Zámek (zařízení). In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001 [cit. 2019-03-10]. Dostupné z: https://cs.wikipedia.org/wiki/Z%C3%A1mek_(za%C5%99%C3%ADzen%C3%AD)

[2] DUMEK, Jakub. *Zámek s technologií RFID*. Pardubice, 2015. Bakalářská práce. Univerzita Pardubice.

[3] HARWOT, Lubomír. *Pult centralizované ochrany*. Praha, 2016.

[4] KOLAJA, Martin. *Využití přístupových systémů v průmyslu komerční bezpečnosti*. Zlín, 2006. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně. Vedoucí práce Kindl, Jiří.

[5] Princip funkce cylindrické vložky. In: *Bezpečnostní cylindrické vložky Winkhaus* [online]. Winkhaus, 2008 [cit. 2019-03-28]. Dostupné z: https://imaterialy.dumabyt.cz/rubriky/clanky/bezpecnostni-cylindricke-vlozky-winkhaus_101090.html

[6] Elektrický zámek s nerezovým štítkem ELC12D6. In: *Elektrický zámek s nerezovým štítkem ELC12D6* [online]. Tfe elektronika, b.r. [cit. 2019-03-28]. Dostupné z: https://www.tfe.cz/elektricky-zamek-s-nerezovym-stitkem-elc12d6.htm

[7] AN OVERVIEW OF RFID TECHNOLOGY. *AN OVERVIEW OF RFID TECHNOLOGY* [online]. DataFlows Dimensions, 2011 [cit. 2019-03-28]. Dostupné z: http://www.dataflows.com/RFID_Overview.shtml

[8] VOJTĚCH, Lukáš. RFID transpondéry – pohled pod kůži. *RFID transpondéry – pohled pod kůži* [online]. Praha, 2011 [cit. 2019-03-29]. Dostupné z: https://www.dps-az.cz/zajimavosti/id:10415/rfid-transpondery-pohled-pod-kuzi

[9] LUKÁŠ GARGULÁK, Lukáš. *RFID a jeho využití v zabezpečovacích a informačních systémech*. Zlín, 2012. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně. Vedoucí práce František Hruška.

[10] HERŠTUS, Michal. RFID principy fungování a možnosti využití. *Udrzbapodniku.cz* [online]. Praha 5: Point.X, 2014 [cit. 2019-04-03]. Dostupné z: http://udrzbapodniku.cz/hlavni-menu/artykuly/artykul/article/rfid-principy-fungovani-a-moznosti-vyuziti/

[11] Kódová klávesnice a RFID čtečka s tlačítkem zvonku SA-0109, 125 kHz. In: *Eletur.cz* [online]. Eletur.cz, 2011 [cit. 2019-04-04]. Dostupné z: https://eletur.cz/rfid-pin-pristupova-klavesnice-sa-0109?gclid=EAIaIQobChMIwP2Cgfm04QIVCqaaCh3ZAQ0KEAQYBiABEgLojvD_BwE

[12] ŘEZNÍČKOVÁ, Lenka. *RFID*. Pardubice, 2009. Bakalářská práce. Univerzita Pardubice.

[13] RFID karta. In: *Nejdochazka.cz* [online]. Praha 1: NejDochazka.cz, 2014 [cit. 2019-04-04]. Dostupné z: https://eshop.nejdochazka.cz/dochazkove-a-pristupove-systemy/30-rfid-karta.html?gclid=EAIaIQobChMIh6a8wfa04QIVlkMYCh25oAJoEAQYAiABEgJKzvD_BwE

[14] Technologie RFID. *Technologie RFID* [online]. Bystřice nad Pernštejnem: Smart-TEC, b.r. [cit. 2019-03-30]. Dostupné z: https://www.smart-tec.com/cs/auto-id-svet/technologie-rfid

[15] VOJÁČEK, Antonín. Používané RFID frekvence a jejich vliv na čtení a zápis tagu. *Automatizace.HW.cz* [online]. Praha 4: HW server, 2015 [cit. 2019-03-30]. Dostupné z: https://automatizace.hw.cz/komponenty-prumyslove-sbernice-a-komunikace/vice-i-mene-bezne-rfid-frekvence-a-jejich-vliv-na-vlastnosti-tagu.html

[16] ESP-12E WiFi Module. *Ai-thinker.com* [online]. Shenzhen Anxinke Technology, 2015 [cit. 2019-04-05]. Dostupné z: https://www.kloppenborg.net/images/blog/esp8266/esp8266-esp12e-specs.pdf?fbclid=IwAR397VBMDpmmHUXQf2ioJUzHjCC2LjHxRnYi567LG5zNJkqIIbt6EP1NNQY

[17] IoT ESP8266 Lua NodeMcu Amica CP2102 WIFI modul. *Laskarduino.cz* [online]. Rychnov nad Kněžnou: Arduino, 2018 [cit. 2019-04-06]. Dostupné z: https://laskarduino.cz/vyvojove-desky/230310-iot-esp8266-lua-nodemcu-amica-cp2102-wifi-modul.html

[18] RFID ČTEČKA S ANTÉNOU 125KHZ EM4100 RDM6300. *Laskarduino.cz* [online]. Rychnov nad Kněžnou: Arduino, 2019 [cit. 2019-04-07]. Dostupné z: https://laskarduino.cz/prenos-dat-bezdratovy/230154-rfid-ctecka-s-antenou-125k-em4100-rdm6300.html

[19] RDM630 Specification. *Elty.pl* [online]. elty, b.r. [cit. 2019-04-07]. Dostupné z: https://elty.pl/upload/download/RFID/RDM630-Spec.pdf

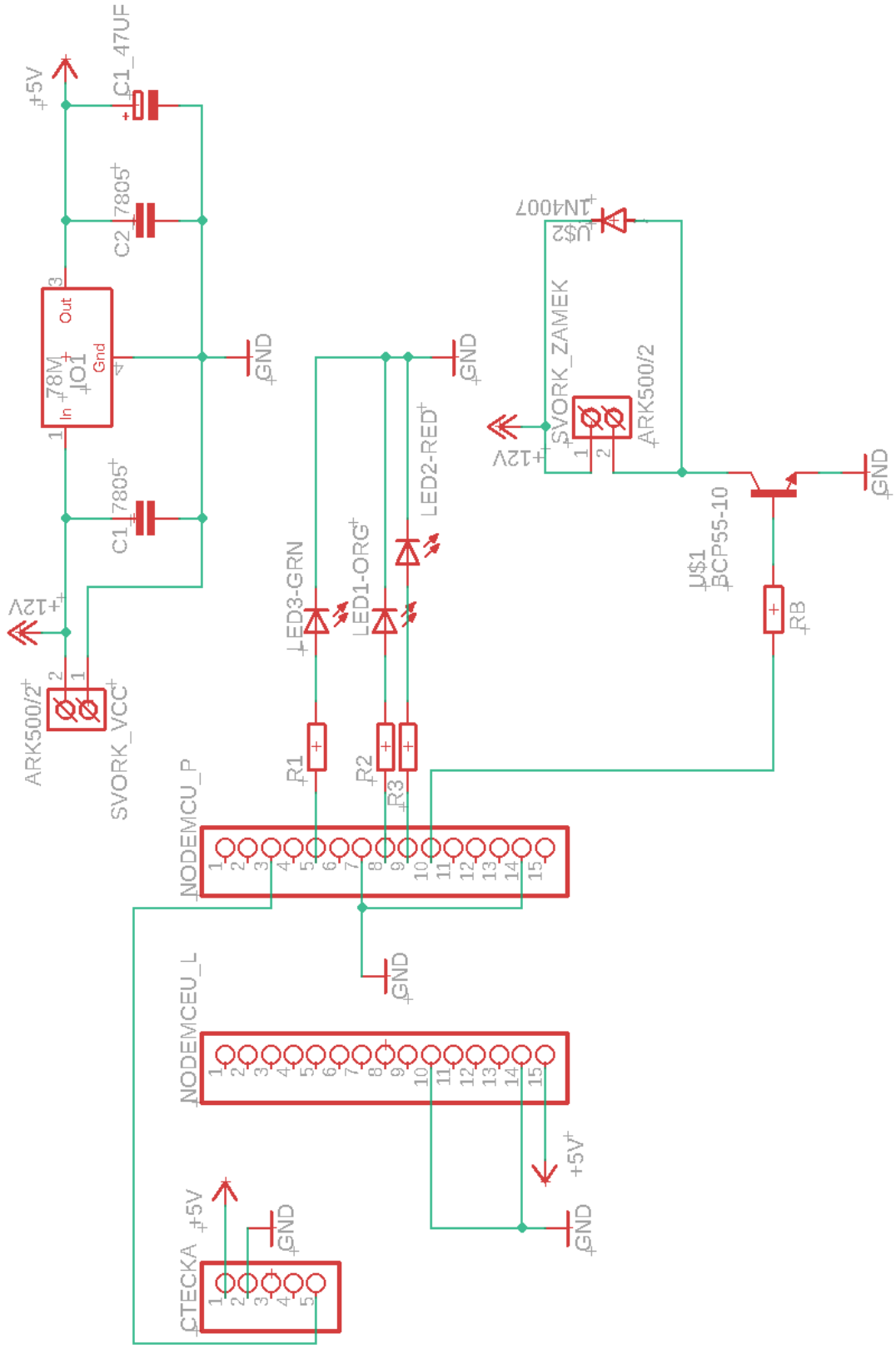
[20] SCHOEFFLER, Michael. Arduino-Tutorial: How to use the RDM630/RDM6300 RFID reader. *Mschoeffler.de* [online]. mschoeffler, 2018 [cit. 2019-04-07]. Dostupné z: https://www.mschoeffler.de/2018/01/05/arduino-tutorial-how-to-use-the-rdm630-rdm6300-rfid-reader/

[21] EM4100 Protocol description. *Priority1design.com* [online]. Melbourne: priority1design, 2007 [cit. 2019-04-07]. Dostupné z: http://www.priority1design.com.au/em4100_protocol.html

[22] PETERKA, Jiří. Báječný svět počítačových sítí. *Earchiv.cz* [online]. earchiv.cz, 2015 [cit. 2019-04-10]. Dostupné z: http://www.earchiv.cz/b05/b1100001.php3

[23] FAB BeFo KLASIK 511MB - elektrický otvírač dveří. *Entryshop.cz* [online]. Praha 10: Entryshop, 2019 [cit. 2019-04-06]. Dostupné z: https://www.entryshop.cz/fab-klasik/fab-befo-klasik-511mb-elektricky-otvirac-dveri/

Příloha A – Schéma zapojení



Příloha B – Návrh desky plošných spojů