Univerzita Pardubice
Fakulta elektrotechniky a informatiky

Zámek dveří s ověřením přes LAN

Jiří Černohorský

Bakalářská práce

2019

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: **2015/2016**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Jiří Černohorský**
Osobní číslo:	**I13007**
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 na čip s ověřením proti autentizačnímu serveru přes LAN. V práci je možno využít připraveného řešení z literatury [1].
V teoretické části popište možnosti autentizace zámkového systému a možné způsoby správy oprávněných čipů.
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**

Seznam odborné literatury:

[1] DUMEK, Jakub. Zámek s technologií RFID, Bakalářská práce, Pardubice, 2015, Univerzita Pardubice.
[2] An AVR microcontroller based Ethernet device [online]. USA, [cit. 24. 5. 2010]. Dostupné z URL:
<http://tuxgraphics.org/electronics/200606/article06061.shtml>
[3] ENC28J60 Data Sheet - Stand-Alone Ethernet Controller with SPI Interface, Chandler: Microchip, 2008. 95s., [cit. 24. 5. 2010]. Dostupné z URL:
<http://ww1.microchip.com/downloads/en/DeviceDoc/39662c.pdf>

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

Datum zadání bakalářské práce: **15. prosince 2015**
Termín odevzdání bakalářské práce: **13. května 2016**

Univerzita Pardubice Česká republika

L.S.

prof. Ing. Simeon Karamazov, Dr.
děkan

Ing. Zdeněk Němec, Ph.D.
vedoucí katedry

V Pardubicích dne 31. března 2015

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. 2017

Jiří Černohorský

PODĚKOVÁNÍ

Chtěl bych poděkovat všem, kdo mě provázeli na mé cestě za vzděláním.

ANOTACE

Bakalářská práce se zabývá návrhem a realizací sytému ovládaní dveřního zámku pomocí technologie RFID a autentizací uživatele přes LAN. V teoretické části jsou popsány druhy autentizace a technologie RFID. V praktické části je popsána konstrukce řídící desky elektronické součástky, moduly použité ke konstrukci zařízení, popis kódu řídící jednotky a popis softwaru pro správu čipů.

KLÍČOVÁ SLOVA

RFID, LAN, ENC28j, ATMega328p, Autentizace

TITLE

Door lock with authentication over LAN

ANNOTATION

The bachelor thesis deals with design and implementation of door lock control system using RFID technology and user authentication over LAN. The theoretical part describes the types of authentication and RFID technology. The practical part describes the design of control board, electronic components, modules used for the construction of the device, code and chip management software.

KEYWORDS

RFID, LAN, ENC28j, ATMega328p, Authentication

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM ZKRATEK

PDF	Portable Document Format
LAN	Local Area Network
RFID	Radio frequency identification
GDRP	General Data Protection Regulation
MAC	Media Access Control
IEEE	Institut of Electrical and Electronics Engineers
SPI	Seriál Peripheral Interface
IP	Internet Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
ICMP	Internet Control Message Protokol
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Systém
RTC	Real Time Circuit
HTTP	Hypertext Tranfer Protocol
ID	Identification
LED	Light-Emitting Diode

ÚVOD

Bakalářské práce se zabývá návrhem a realizací zámkového systému s autentizací přes LAN. Cílem je vytvořit systém, který zajistí jednoduchou správu uživatelských přístupů a jednotek. V současné době existuje mnoho způsobů autentizace odvíjejících se od stupně zabezpečení a tím i ceny sytému, proto bude v teoretické části popsaná autentizace jako taková a nejrozšířenější autentizační systémy. Jako porovnávací systém slouží stávající zámkový systému na fakultě elektrotechniky a informatiky Univerzity Pardubice, který vyžaduje fyzickou přítomnost administrátora u čtecího zařízení a nahrání každé přístupové karty do každého čtecího zařízení.

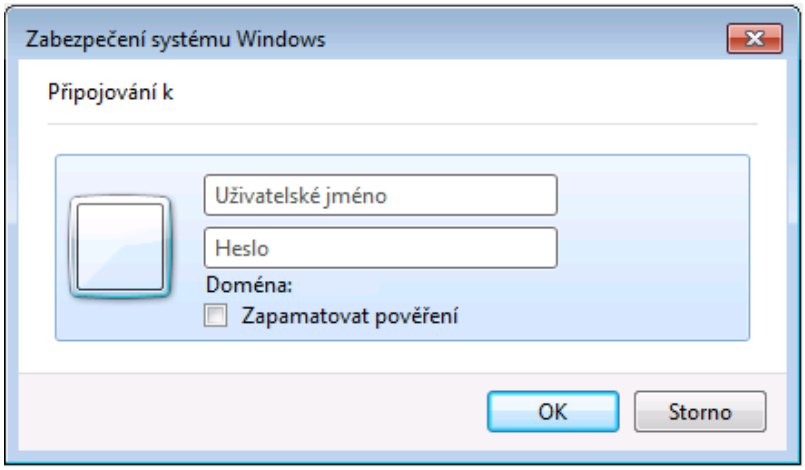
Nový systém by měl změnit způsob zadávání přístupů a jejich správu. Tím umožní efektivnější správu a úsporu času administrátora. Cílem je vytvořit zařízení, které bude připojené do počítačové sítě a bude přenášet data na server, kde bude docházet k vyhodnocování přístupů. Pro snadnější ovládání databáze bude vytvořen program pro správu databáze s grafickým rozhraním a tím odpadne potřeba znalosti jazyka SQL a databázových systémů.

1 AUTENTIZACE

Je proces ověření identity uživatele služby a patří k bezpečnostnímu opatření, které chrání uživatelský účet před zcizením nebo zneužitím. Autentizace je často zaměňována s pojmem autorizace, která neporovnává údaje nebo data o uživateli, ale po úspěšné autentizaci, povolí uživateli např. přístup do místnosti nebo k informacím.

1.1 Faktor „znalost“

Je druh autentizace, při které uživatel zná své přístupové údaje, jako například přihlašovací jméno a heslo, přes které přistupuje do systému. Jedná se o nejjednodušší druh autentizace. Ve většině případů má uživatel možnost zvolit si přístupové údaje sám. Některé dnešní služby už vyžadují heslo odolnější, takže při zadávání uživateli nepovolí vytvořit účet, než splní přednastavené požadavky (kombinace počtu znaků, velká a malá písmena, číslice). Tato metoda je nejvíce využívaná webovými službami.[1]



Obrázek 1: Znalost jména a hesla[1]

1.2 Faktor „vlastnictví“

Při tomto druhu autentizace se využívá speciální, jednoznačně identifikovatelný hardware. Příkladem mohou být čipové karty, autorizované flashdisky, RFID klíčeny nebo karty. Před použitím je nutno hardware přiřadit k uživateli.[1]

[1]Zdroj: Vlastní

Obrázek 2: RFID klíčenka[2]

1.3 Faktor „Biometrie“

Biometrická autentizace využívá automatizované měření fyziologických vlastností lidského těla. Charakteristické vlastnosti mohou být otisk prstu, sken obličeje, oční sítnice atd. Nevýhoda biometrie je, že naměřená data se nikdy na 100% neshodují a systémy tak „odhadují“ na kolik procent jsou data podobná. Další nevýhodou je například zanechávání otisků prstů a jejich možném sejmutí a vytvoření totožné kopie.[1]

1.4 Vícefaktorová

Vícefázová autentizace je kombinací tří výše zmíněných faktorů. Jde o systémy, kde jsou kladeny vyšší nároky na zabezpečení. Příkladem může být platební karta (faktor vlastnictví) a k platební kartě zná uživatel PIN (znalostní faktor). Pokud uživatel nezná nebo nemá všechny potřebné prvky k autentizaci jemu znemožněno užívání služeb. [1]

[2]Zdroj: Vlastní

2 MOŽNOSTI AUTENTIZACE V ZÁMKOVÉM SYSTÉMU

V zámkovém systému můžeme zvolit jakoukoliv možnost autentizace, ale záleží na stupni ochrany uzamčeného prostoru a finanční náročnosti.

2.1 Kódový zámek u dveří

Kódový zámek je jedna z nejjednodušších zařízení na ochranu proti vstupu nepovolaných osob do chráněného prostoru. Nevýhodou sytému je, že zámek má jedno přístupové heslo pro všechny uživatele a není tak možné kontrolovat přístupy oprávněných osob a zabezpečení spoléhá na diskrétnost uživatelů.

2.2 RFID zámky

Tato metoda je v současné době nejrozšířenější metoda kontrolování přístupů do prostor. Existují dva typy přístupových systémů založených na technologii RFID. První systém využívá čteček s interní pamětí, kam administrátor systému musí pomocí svého tagu nahrát tagy uživatelů, kterým uděluje přístup.

Nevýhodou je časová náročnost operace nahrávání tagů, protože se musí nahrát tagy do každé čtečky samostatně. Jiný systém využívá počítačové sítě LAN a software na správu oprávnění čtečky, tím je dosažena efektivní správa systému přístupů a možnost kontroly a ukládání záznamů pohybu osob v hlídaných místnostech. Zranitelnost systému je stále v lidském faktoru, pokud například uživatel ztratí nebo někomu předá svůj čip, i když řešení problému při ztrátě se dá vyřešit velice rychle, pouhým smazáním tagu ze systému.

2.3 Biometrické systémy přístupu

Nejvíce využívanou biometrickou veličinou pro určování uživatele je otisk prstu nebo sken oční sítnice. Metoda kontrolování přístupů do místností má velké náklady na pořízení a proto se využívá při nejvyšším stupni zabezpečení. S příchodem GDPR jsou nyní kladeny velké nároky na zabezpečení a ochranu dat uživatelů, což také zvedá cenu systémů.

3 ELEKTRICKÉ ZÁMKY

Elektrické zámky plní stejnou funkci jako ostatní zámky a to zabezpečení prostotu před vstupem nepovolaných osob nebo ochraně majetku. Rozdíl proti obyčejným zámkům je ve způsobu ovládání.

Mechanické zámky, jak název napovídá, jsou ovládány pomocí mechanické síly, otočením klíče v zámkové vložce. Nevýhodou mechanických zámků ve větších objektech nebo komplexech je počet klíčů, které musí uživatel nosit. Částečně tento problém řeší systémy generálního klíče, ale systémy generálního klíče jsou většinou obtížné na správu a po jejich instalaci není možné změnit „přístupová práva“ bez nutnosti dalších investic.

Elektrické zámky většinou fungují na principu elektromagnetického relé nebo elektromotoru, které při průchodu proudu odblokuje pohyblivou část zámku, která uzamyká dveře a umožní otevření dveří. Elektrický zámek v kombinaci s technologií RFID tvoří kombinaci, která umožní efektivní správu přístupů. Jedna z největších výhod systému je, že při ztrátě přístupového čipu, je možné čip jednoduše vymazat z databáze přístupů, při ztrátě klíče z mechanického klíčového systému je z bezpečnostních důvodů nutno vyměnit celou vložku. Počáteční náklady na pořízení jsou větší, něž u mechanických zámkových systémů.

3.1 Typy elektrických zámků

Elektrické zámky se rozdělují podle konstrukce nebo způsobu blokace.

3.1.1 Klasické elektrické otvírače

Standardní provedení elektrického otvírače je v poloze otevřeno jen po dobu trvání napěťového impulzu, to je pouze po dobu, po kterou je přivedený spínací signál. Další možností je s momentovým kolíkem. K otevření stačí krátký elektrický impulz, kterým se otvírač s momentovým kolíkem odjistí, a tím je v poloze otevřeno, po průchodu dveřmi se vrátí do polohy zavřeno. Další možnost je otevírač s mechanickou blokádou. Ten umožňuje mechanické nastavení páčky do polohy otevřeno nebo zavřeno. V poloze otevřeno je vhodný pro stálý průchod bez použití elektrického impulzu na neomezeně dlouhou dobu.[17]

3.1.2 Samozamykací elektromechanický zámek

Je druh kombinovaného zámku, který po uzavření dveří se zámek automaticky uzamkne, vysune se závora a zablokuje se střelka. Stisknutím aktivované nebo panikové kliky je závora zatažena do těla zámku a následně odblokována střelka. Zámek je vždy možné odemknout cylindrickou vložkou z obou stran dveří nebo stiskem kliky.[17]

3.1.3 Samozamykací elektromotorický zámek

Po příchodu aktivačního signálu je motoricky zatažena závora společně s háky dovnitř zámku a následně odblokována střelka. Zámek je odemčen a dveře je možné otevřít pouhým zatlačením. Po uzavření dveří je zajišťovací střelka společně s hlavní střelkou zatlačena o protiplech do těla zámku a po vyskočení hlavní střelky do zárubně dojde k automatickému vysunutí závory, háků a následnému zablokování střelky. Zámek je uzamčen ve více bodech a je elektromotoricky chráněn proti vysunutí závory a háků mimo zárubeň. Zámek je vždy možné odemknout cylindrickou vložkou z obou stran dveří.[17]

4 RFID

RFID je technologie založená na přenosu identifikačních informací z transpondéru, tvz. RFID tagu, do čtecího zařízení pomocí radiových frekvencí na krátkou vzdálenost. Základní rozdělení technologie RFID je podle typu transpondéru na aktivní a pasivní a podle nosných frekvencí. Technologie si našla využití v mnoha oborech např. zdravotnictví, průmyslu, zabezpečení, obchodu a sportu.[1]

4.1 Dělení podle typu napájení

4.1.1 Pasivní

Pasivní RFID transpondér neboli tag, je integrovaný obvod, připojený k anténě a zabalený do ochranného obalu (nejčastěji plast). Tento obvod sám o sobě nevysílá informace, dokud se nepřiblíží k čtečce, která vysílá elektromagnetické vlnění (energii), na stejné frekvenci na kterou je naladěna anténa transpondéru. Tag využije energii přenesenou za čtecího zařízení k vyslání uložených informací, které jsou poté dále zpracovány podle potřeby. Pasivní technologie RFID je více rozšířená díky malým a levným RIFD tagům s velkou životností, které umožňují širší

využití. Absence baterie má za následek kratší přenosové vzdálenosti a omezení velikosti informace uložené v tagu.[2]

4.1.2 Aktivní

Na rozdíl od pasivního tagu má aktivní tag vlastní napájecí zdroj, který umožňuje velký čtecí dosah a velkou paměť. Aktivní tagy jsou napájeny baterií, která obvykle vydrží 3 až 5 let, ale když baterie dojde, je potřeba vyměnit celý tag. V podstatě existují dva druhy aktivních RFID tagů, nazývané „transponders“ a „beacons“. V systému s „transponders“ je tag aktivní až po zachycení signálu od čtečky systému – teprve potom pošle zpět požadované informace. Tím je tento druh tagů velmi šetrný k baterii, protože šetří její energii ve chvíli, když je tag mimo čtecí dosah.

Aktivní RFID transponders jsou obecně používány v bezpečných přístupových systémech a na místech, kde se vybírají poplatky (např. mýta). V systému, který používá aktivní tag typu „beacon“, vysílá tag určité informace každých 3−5 sekund, bez ohledu na to, zda je, nebo není v čtecím dosahu čtečky systému. Protože jeho čtecí dosah je velký, i několik set metrů, používá se například často v průmyslu těžby a zpracování nafty a plynu. Pokud se sníží vysílaný výkon kvůli úspoře baterie, čtecí dosah se úměrně zmenší.[2]

4.1.3 Poloaktivní

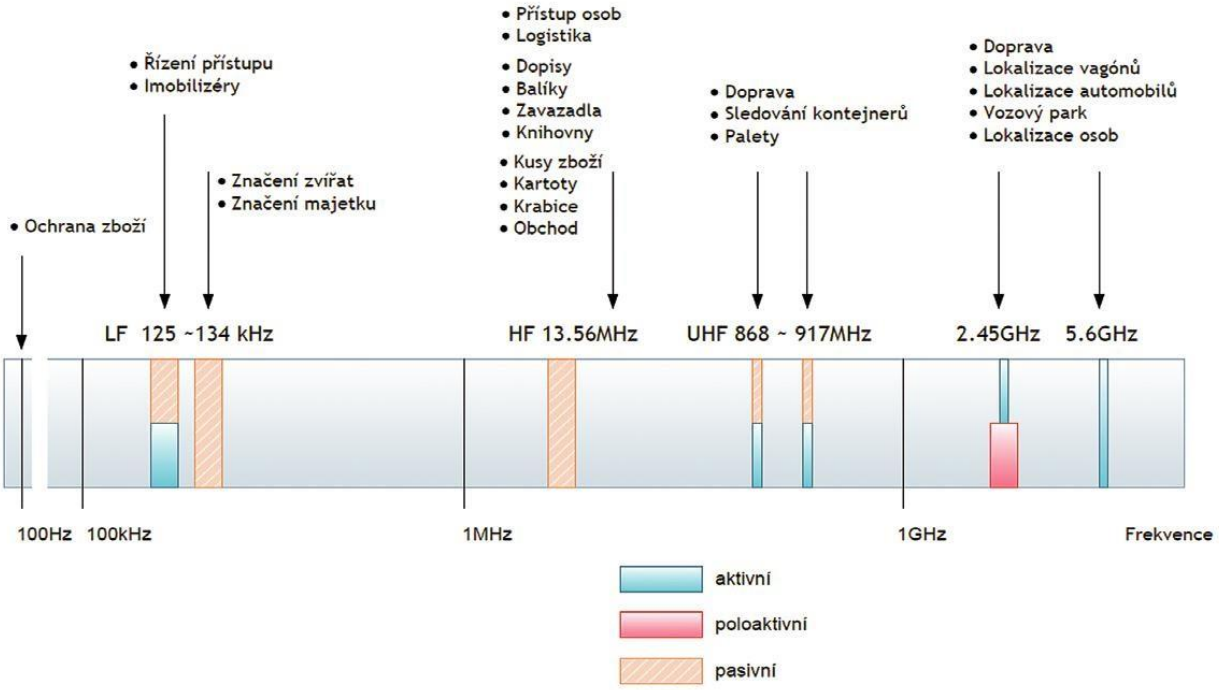
Poloaktivní (semi-pasivní, semi-aktivní) tag představuje skupinu tagů s vlastním zdrojem energie. Komunikuje stejným způsobem jako pasivní tagy a baterii používá pro napájení mikročipu a případných senzorů integrovaných do tagu. Poskytuje možnost čtení na delší čtecí vzdálenosti než pasivní tagy.[12]

4.2 Dělení podle typu paměti

1. **READ ONLY** – transpondér pouze vysílá informace uložené výrobcem
2. **READ AND WRITE** – uživatel má možnost uložit informace do tagu podle aktuální potřeby
3. **READ AND WRITE(částečně)** – uživatel má možnost změnit některé informace v paměti tagu

4.3 Dělení podle nosné frekvence

Systémy RFID můžeme dělit podle nosné frekvence na které přenášejí data mezi čtečkou a tagem. Většina frekvencí jsou standardizované po celém světě. V některých zemích jsou pro RFID vyhrazena i jiná frekvenční pásma. Přehled frekvencí a nejčastějšího využití ukazuje obrázek č.3.



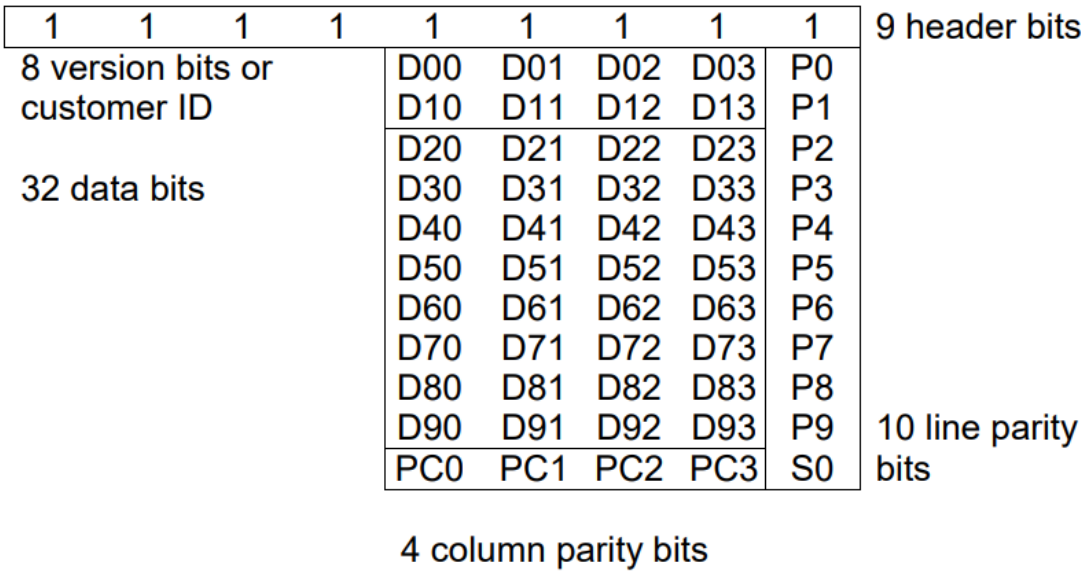
Obrázek 3:Využívané frekvence RFID[3]

4.4 Transpondér EM4100

Aby mohla probíhat komunikace mezi čtečkou a tagem, je nutné znát způsob uložení dat v tagu a v jakém pořadí jsou vysílána. Mnoho výrobců má své vlastní technologie a tagy. Mezi nejčastější používané transpondéry v pásmu 125 kHz patří EM4100. Název tohoto čipu vznikl z názvu výrobce Microelectronic. Transpondéry EM4100 mají CMOS čip s pamětí ROM (Read Only Memory) o velikosti 64 bitů. To znamená že do transpondéru jsou nahrána data od výrobce už při výrobě a poté data není možné dále měnit. Programování čipu se provádí pomocí laserové fixace polysilikonových spojů, aby se na každém uložil jedinečný kód.[4]

[3] Zdroj: [3]

Datový tok začíná hlavičkou obsahující samé bity s hodnotou 1, hlavička má velikost 9 b, tato bitová sekvence slouží čtečce k rozpoznání, že nejde o náhodný signál nebo o signál z jiného zařízení. Následující data jsou rozděleny vždy po skupinách o velikosti 4 b, následovaných jedním paritním bitem. První dvojice nese informaci o výrobním čísle nebo o verzi tagu. Další 4 skupiny jsou nejdůležitější, protože v nich je uložen identifikátor klíčenky. Poslední skupina je sloupcová parita. Poslední bit je označován jako stop bit a má hodnotu 0, pokud by byla hodnota posledního bitu 1, znamenalo by to problém s komunikací a data by nebyla dále zpracovávána. Obrázek č.4 ukazuje výše popsané rozložení vysílaných bitů.



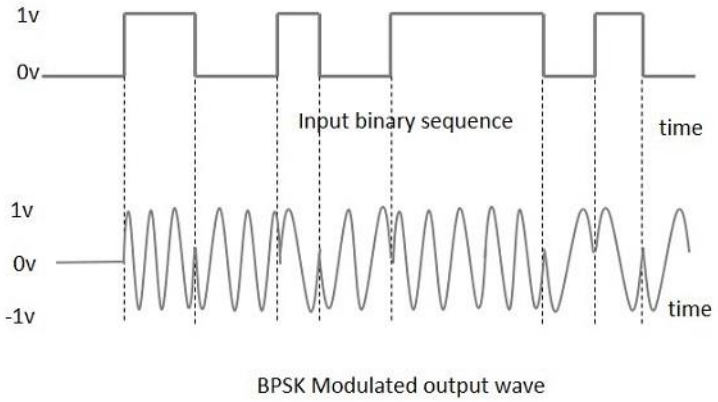
Obrázek 4:Způsob uležení dat v čipu EM4100[4]

4.5 Modulace dat

Data jsou při přenosu modulovaná technikou zvanou PSK, Phase Shift Keying neboli klíčování fázovým posuvem. Metoda PSK je používána pro modulaci digitálních signálů a přenáší informaci pomocí změny fáze signálu. V systémech RFID, s frekvencí od 100Khz do 130KHz, je

[4] Zdroj: [4]

používaná metoda BPSK, nejjednodušší forma PSK. BPSK používá ke klíčování dvě fáze, navzájem posunuté o 180°, díky tomu je odolná proti šumu nebo zkreslení, ale nehodí se pro vyšší přenosové rychlosti. Obrázek č.5 názorně ukazuje princip BPSK. [5]



Obrázek 5:BPSK modulace[5]

5 SPRÁVA JEDNOTEK A ČIPŮ

5.1 Možnosti správy čipů

Pro plné využití potenciálu zařízení, které je připojené do počítačové sítě, je nutné pracovat s daty na síťovém uložišti, aby byl zachován vzdálený přístup a zvýšila se tím efektivita správy přístupů.

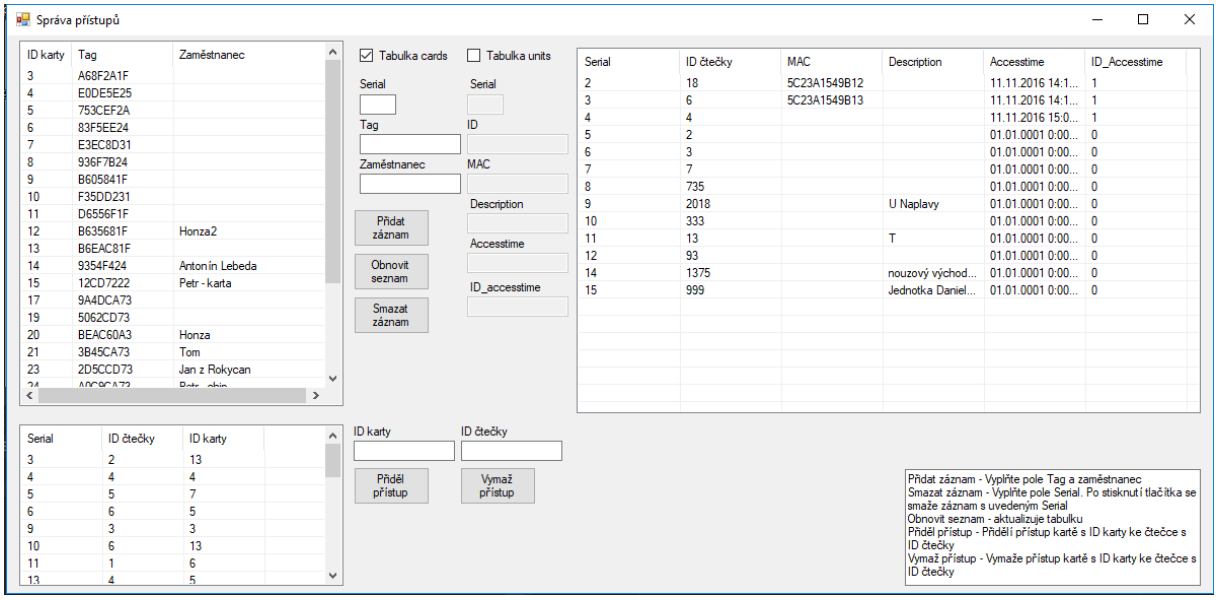
Nejvhodnějším nástrojem pro správu dat je databáze. Existuje několik druhů databázových systémů od různých výrobců. Mezi nejznámější patří: Microsft Access, Oracle, FireBird nebo MySQL. Všechny jmenované databázové programy mají společný dotazovací jazyk SQL (Structured Query Language). Přímé využití některého databázového programu vyžaduje znalost jazyka SQL.

[5] Zdroj: [5]

5.2 Software pro správu jednotek a čipů

Pro účely správy přístupů byla vytvořena aplikace v jazyce C#. Vývoj aplikace probíhal v prostředí Visual Studio 2019. Aplikace je napojená do databáze accesscontrol na serveru mysql.rolda.cz. Grafické rozhraní aplikace se skládá ze dvou listboxů, ve kterých se zobrazují záznamy z databáze. První tabulka jsou data o čipech a uživatelích. Druhá tabulka obsahuje data o čtecích jednotkách. Chechkbox pro výběr tabulky, textová pole pro zadávání hodnot do tabulky a tlačítka pro vykonávání funkcí obnovit tabulku, smazat záznam a přidat záznam.

Ovládání aplikace je popsáno v popisku v pravé spodní části obrazovky. Pro obsluhu tabulky cards je nutné zaškrtnou checbox s názvem tabulka cards, tímto se ovládací tlačítka přepnou do režimu obsluhy tabulky cards, zpřístupní se textová pole pro vyplnění dat do tabulky cards a ostatní textová pole se uzamknou. Stejný princip platí pro zaškrtnutí chechboxu Tabulka Units. Pro přidělení a vymazání přístupů je nutné vyplnit pole ID karty a ID čtečky, podle kterých se zapíše do vazební tabulky v databázi řádek s příslušným ID.



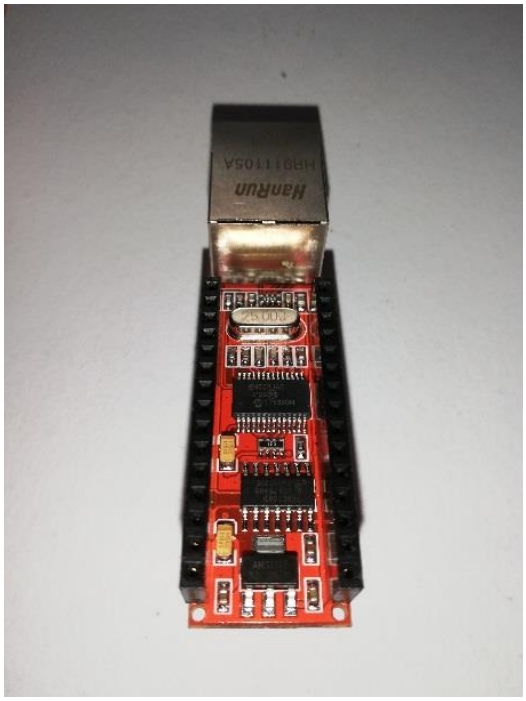
Obrázek 6: Grafické rozhraní programu pro správu databáze[6]

[6] Zdroj: Vlastní

6 MODULY

6.1 Ethernet modul

Komunikace čtečky se serverem přes LAN zajišťuje vývojový kit Arduino Nano ethernet shield V1.0. Jedná se o vývojovou desku, která je osazena konektorem RJ45, regulátorem AMS1117, CMOS čipem 74HCT08D, čipem ENC28j60 a několika dalšími pasivními součástkami.



Obrázek 7:Ethernetnetový modul[7]

6.1.1 ENC28j60

Je samostatný 10BASE-T (standard, který zaručuje přenosovou rychlost 10Mbps na vzdálenost 100 metrů pomocí kroucené dvoulinky) ethernetový radič od společnosti Microchip Technology kompatibilní s normou IEEE 802.3. Shield je osazen čipem v pouzdře 28-SPDIP. Čip se nedodává s MAC adresou, je možné ho využít pro domácí účely a vývoj aplikací v domací LAN

[7] Zdroj: Vlastní

síti (možnost zvolit si vlastní MAC adresu a nezpůsobit tak kolizi MAC adres), při případném komerčním nasazení je nutné MAC adresu zakoupit.

Komunikace s řídícím procesorem je dosažena pomocí rozhraní SPI. Maximální frekvenci čipu udává výrobce jako 25MHz a je na desce realizována krystalovým oscilátorem (vysoká stabilita), dále je připojen konektor RJ45 s integrovanými pulsními transformátory (modulace a demodulace signálu).[8]

6.1.2 Regulátor AMS1117

Čip ENC28j60 vyžaduje napájecí napětí v rozmezí 3,1V až 3,6V, typicky 3,3V. Jelikož je ethernetový shield napájen přímo z vývojové desky arduino nano, která vyžaduje napájecí napětí 5V, je na desce přítomný regulátor AMS 1117, který se stará o udržení stabilního napětí 3,3V. AMS 1117 je řada nastavitelných a fixních napěťových regulátorů, které jsou navrženy pro odebíraný proud až 1A. Na desce je regulátor AMS1117-3.3 v pouzdře SOT-223. Pro správnou regulaci a stabilizace napětí je potřeba vstupní napětí na regulátoru 4.8V, z důvodu napěťového poklesu na regulátoru o cca 1,3V.

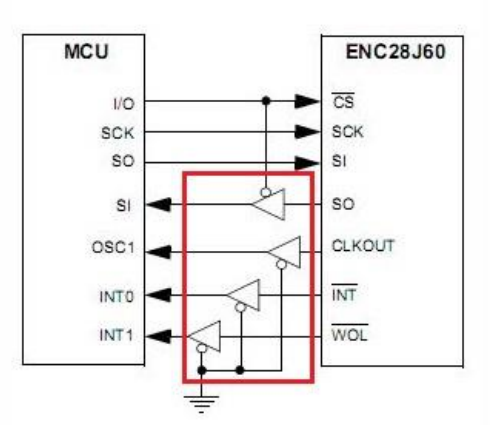
V datasheetu výrobce uvádí hodnotu tepelného odporu pouzdra SOT-223, v závislosti na způsobu připevnění, na 46 °C/W až 90°C/W. Provozní teplota čipu je -40°C až 125°C. Při napájecím napětí 3,3V a odběru čipu ENC28j60 180mA je výkon regulátoru podle vzorce:

$$P = U * I = 3{,}3 * (180 * 10^{-3}) = 0{,}594W$$

Z rovnice vychází, že i při zvolení nevhodného způsobu připevnění regulátoru (bez kovové plošky pro odvod tepla) nehrozí přehřátí čipu a jeho zničení.[9]

6.1.3 74HCT08D

74HCT08D je vysokorychlostní CMOS hradlo se čtyřmi dvouvstupovými hradly AND. Čip obsahuje výstupní buffer a díky tomu je vysoce imunní vůči šumu a má stabilní výstup. Na vývojové desce slouží ke konverzi určitých signálů z napěťové logiky 5V (ATMega) na 3,3V (ENC28j60). [10]



Obrázek 8:Blokové schéma 74HCT08D[8]

6.2 HZ-1050

Čtení RFID tagů zajišťuje modul HZ-1050. Modul čtecího zařízení se skládá z mikroprocesoru ATMega 8A AU 1348, operačního zesilovače LM358 PHZY, který zajištuje fázovou modulaci signálu, antény a několika pasivních součástek.

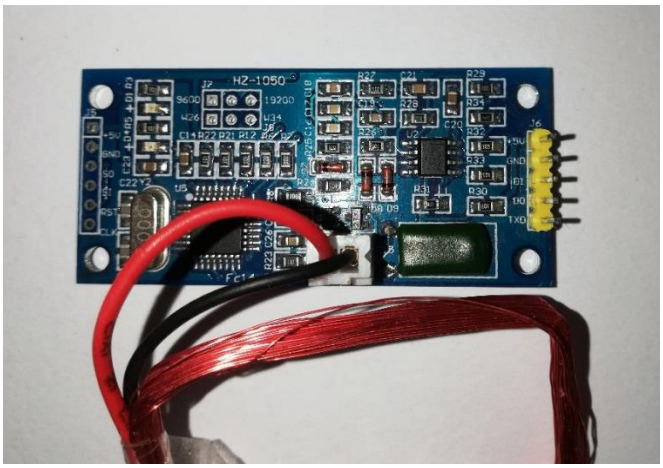
6.2.1 Popis modulu HZ-1050

Pro naprogramování procesoru jsou na desce vyvedeny vývody 5V, GND, SO, SI, RST a CLK. Pro čtení tagů jsou na desce vývody 5V, GND, D1, D0 a TXD. Dále je možné pomocí propojek volit přenosovou rychlost 9600 Bd nebo 19200 Bd a verzi protokolu Wiegand W26 nebo W34. Pro naši aplikaci využijeme sériovou linku, resp. jen pin TXD a vývody 5V a GND pro napájení modulu a čtení po sériové lince přes pin TXD.[11]

Nevýhodou modulu je nedostatek informací od výrobce, absence technického listu a popis kódu mikroprocesoru.

Tento RFID modul pracuje s RFID tagy na frekvenci 125kHz. Frekvence byla zvolena z důvodu ceny a shodnosti s frekvencí čipových karet, které jsou používány na Fakultě elektrotechniky a informatiky Univerzity Pardubice.

[8] Zdroj: [10]



Obrázek 9:Čtecí modul HZ-1050[9]

7 POPIS KÓDU ŘÍDÍCÍ JEDNOTKY

7.1 Použité knihovny

```
#include <SPI.h>
#include <UIPEthernet.h>
#include <TextFinder.h>
#include <EEPROM.h>
#include <avr/pgmspace.h>
#include <UIPServer.h>
#include <UIPClient.h>
#include <SoftwareSerial.h>
#include <virtuabotixRTC.h>
```

Obrázek 10:Použité knihovny[10]

V kódu jsou použity následující knihovny

SPI.h – je knihovna pro komunikování mikroprocesoru s ostatními periferiemi pomocí SPI (Seriál Peripheral Interface). SPI je synchronní sérioví protokol, umožňující komunikaci na krátké vzdálenosti pro několik zařízení, z nichž je jedno nazývané Master (řídící) a ostatní Slave (periferie). Jsou zapotřebí čtyři datové sběrnice: MISO (Master In Slave OUT), MOSI (Master

[9] Zdroj: Vlastní
[10] Zdroj: Vlastní

Out Slave In), SCK (Seriál Clock) a SS (Slave select) nebo CS (Chip select). Sběrnice SS a CS jsou totožné, jde jen o jiné pojmenování.

UIPEthernet.h – knihovna zajišťující ethernetovou komunikaci pro čip ENC28J60. Knihovna podporuje TCP a UDP spojení, ARP, ICMP, DHCP a DNS. Knihovny IUPServer a UIPClient jsou podknihovny UIPEthernet.[6]

TextFinder.h - TextFinder je knihovna pro extrahování informací z datového toku. Byla využita pro nalezení konkrétních polí a získání řetězců nebo číselných hodnot. Lze jej také použít se sériovými daty.

EEPROM.h – knihovna umožňující práci s pamětí EEPROM (Nonvolatilní paměť, která uložené data uchová i po odpojení napájení). Využívané funkce knihovny jsou ukládání (write()), čtení (read()).

Pgmspace.h – knihovna umožňující ukládání dat do paměti FLASH (Nonvolatilní paměť sloužící k uložení neměnících se dat, jako například program procesu nebo neměnná data).

SoftwareSerial.h - hardwarové zařízení Arduina má vestavěnou podporu pro sériovou komunikaci pouze na pinech 0 a 1. Knihovna SoftwareSerial byla vyvinuta tak, aby umožňovala sériovou komunikaci na jiných digitálních pinech Arduina, pomocí softwaru pro replikaci funkčnosti (odtud název "SoftwareSerial"). Je možné mít více sériových portů s rychlostí až 115200 bps. Parametr umožňuje invertovanou signalizaci pro zařízení, která tento protokol vyžadují.

virtualboxRTC.h – knihovna umožňující komunikaci mikroprocesoru s RTC (Real time circuit) DS1302.[7]

7.2 Deklarace proměnných

mac – proměnná ve které je uložena MAC adresa čtečky

ID_Unit – identifikační číslo čtecí jednotky

ip – IP adresa čtečky

subnet – maska podsítě

gateway – Výchozí brána sítě

dnsserver – adresa DNS serveru

Proměnné i,a,e, pomocna - jsou pomocné proměnné využívané pro výpočty v průběhu programu

c – je proměnná využívaná pro ukládání jednotlivých znaků při práci s textem

pocitadlo_znaku, **priznak** – proměnná využívaná pro určování pořadí znaků příchozí odpovědi na http požadavek

ID_karta – pole proměnných deklarované pro uložený dat o přiloženém tagu

SoftwareSerial – inicializace pinů procesoru pro simulování sériové komunikace se čtečkou RFID karet

EthernetServer –inicializace ethernetového serveru a poslouchaní na portu 80

vituabotixRTC – inicializace pinů určených pro komunikace mikroprocesoru s obvodem RTC

poradiKarty – proměnná určení počtu uložených karet

denZapsani, mesicZapsani – proměnné do kterých ukládá obvod RTC DS 1302 informace o datu přiložení a zapsání čtečky

pocetPovolenychDni – slouží k uchování informace o počtu dní, které mohou uplynout od posledního průchodu dveřmi od výpadku komunikace se serverem.

pocetPovolenychKaret – počet karet které se mají ukládat do paměti EEPROM

casOtevreniDveri – určuje čas po který jsou dveře otevřené

V programu jsou dále deklarovány lokální proměnné dle potřeby.

7.3 Funkce setup()

```
void setup()
{
  pinMode(6, OUTPUT);
  pinMode(7, OUTPUT);
  pinMode(8, OUTPUT);
  pinMode(9, OUTPUT);
  Serial.begin(9600);
  RFID.begin(9600);
  ShieldSetup ();
  delay(1000);
  server.begin();
}
```

Obrázek 11:Funkce setup()[11]

Funkce setup se volá při startu programu a je volána pouze jednou. Příkazem pinMode nastavíme digitální piny procesoru 6,7,8 a 9 jako výstupní piny. Pomocí těchto pinů ovládáme indikační LED a spínáme tranzistor, který ovládá dveřní zámek. Příkaz Seriál.begin(9600) zapne sériovou komunikaci o rychlosti 9600b. RFID. Begin(9600) zapne emulovanou sériovou komunikaci pomocí knihovny SoftwareSerial. Příkaz ShieldSetup() vyvolá funkci, která nastaví ethernetové parametry zařízení (IP, MAC, atd.). Příkazem server.begin() zapneme funkci serveru na zařízení, díky tomu je možné měnit parametry čtecího zařízení v internetovém prohlížeči.

7.4 Funkce ShieldSetup()

Při vyvolání funkce ShieldSetup dojde k nastavení pinu T na hodnotu 1, tímto příkazem rozsvítíme oranžovou led, která indikuje přípravu jednotky. Čip ENC28j60 má zabudovanou podporu DHCP serveru. Pokud na síti máme aktivní DHCP server, vyzkoušíme, zda nám budou přiděleny parametry automaticky. Podmínkou if (ethernet.begin(mac)==0) získáme parametry sítě z DHCP. Pokud je podmínkou vrácena hodnota 1, znamená to úspěšné navázaní spojení s DHCP serverem a přidělení síťových parametrů.

[11] Zdroj: Vlastní

Program dále pokračuje kontrolou prvního spuštění. Kontrola prvního spuštění programu je kontrola místa v paměti EEPROM na adrese 0, pokud je na pozici nula uloženo číslo 92, znamená to, že program už běžel a mají se načíst parametry (Unit_ID, poradiKarty, pocetPovolenychDni, pocetPovolenychKaret a casOtevreniDveri) uložené v paměti EEPROM, pokud tomu tak není program načte hodnoty z proměnných deklarovaných na začátku programu. Obsazení paměti EEPROM je ukázáno v tabulce č.1.

Paměťová buňka	Data
0	Kontrola prvního spuštění
1	ID jednotky
2	ID jednotky
3	IP adresa
4	IP adresa
5	IP adresa
6	IP adresa
7	Maska podsítě
8	Maska podsítě
9	Maska podsítě
10	Maska podsítě
11	Výchozí brána
12	Výchozí brána
13	Výchozí brána
14	Výchozí brána
15	Počet povolených dní
16	Čas otevření dveří
17	Počet povolených karet
18	Nevyužito
19	Nevyužito
20	Pořadí karty

Tabulka 1: Rozložení paměti EEPROM

Pokud spojení s DHCP serverem není k dispozici, dojde ke kontrole prvního spuštění, pokud program nebyl spuštěn, nastaví se parametry sítě podle deklarovaných parametrů na začátku programu, pokud byl program dříve spuštěn, parametry se nastaví podle dat uložených v paměti

EEPROM. Na konci funkce dojde k nastavení pinu 7 na hodnotu 0 a oranžová LED zhasne, poté je na 1s nastaven pin 8 na hodnotu 1 a svítí zelená LED indikující konec nastavování čtečky.

7.5 Změna parametrů čtečky

Změnitelné parametry:

- ID čtečky
- IP adresa
- Maska sítě
- Výchozí brána
- Počet povolených dní
- Počet uložených karet
- Interval otevření dveří

Pro změnu parametrů čtečky je nutné v internetovém prohlížeči vytvořit http request ve tvaru „192.168.1.158/setup“, jako příklad jsem uvedl vymyšlenou IP adresu, pro přístup do nastavovacího rozhraní je nutné uvést skutečnou IP adresu čtečky. Pro zachycení příchozího požadavku je v programu zapnut server příkazem server.available().

Pokud je zachycen příchozí požadavek na spojení, je podmínka if (client) splněna a přechází se do těla podmínky. Příkazem Text finder finder (client) vytvoříme instanci pro datový tok client. Dokud není spojení ukončeno a pokud je klient dostupný, hledáme tři části textového streamu: GET, setup a SBM. Pokud v http požadavku najdeme všechny tři zmiňované texty, dostaneme se do těla podmínky if (finder.findUntil("SBM", "\n\r")). V této části hledáme text DT, kterým jsou označeny hodnoty v html kódu. Pokud najdeme spojení DT, je do proměnné val uložen následující znak, který značí pořadové číslo hledané hodnoty.

Následující část kódu porovnává hodnotu val a ukládá nalezené hodnoty do proměnných. Po načtení všech hodnot jsou následně uložena do paměti EEPROM a provede se zápis prvního spuštění programu. Při splnění podmínek GET a setup je vytvořen http response, který pošle prohlížeči potřebná data k sestavení html stránky. Po odeslání všech dat se přeruší smyčka while (client.connected) příkazem break a dojde k zastavení komunikace klienta se serverem.

7.6 Načtení karty

```
while (RFID.available())
{
  a = RFID.read();
  ID_karta[e] = a;
  e = e + 1;
}
```

Obrázek 12:Načtení karty[12]

Načtení karty probíhá tak, že sledujeme, zda se neobjeví sériová komunikace na portu 6. Pokud jsou dostupná data, čteme a ukládáme do pole ID_Karta na pozici 1-4. Čtečka HZ-1050 posílá již data zkontrolovaná a zbavená pro nás redundantních informací (startovací sekvence, stop bit, parita). Jako pomocnou proměnnou pro dočasné uložení dat používáme proměnnou a.

7.7 Kontrola uložených karet

Na začátku bloku jsou deklarovány pomocné lokální proměnné ulozenaKartaNalezena a datumExpirace. Jako předběžná kontrola správného načtení karty slouží počítadlo e. Pokud je počítadlo rovno čtyřem, předpokládáme že přenos proběhl v pořádku a můžeme se přesunout k další kontrole. Následně je prohledávána paměť EEPROM a hledá se shoda mezi uloženou hodnotou v paměti a v poli ID_Karty. Pokud je nalezena shoda, zvýší se hodnota proměnné ulozenaKartaNalezena o 1. Dosáhne-li hodnota proměnné ulozenaKartaNalezena=4, znamená to, že jsme našli kartu v paměti a v dalším kroku se určí její platnost.

Platnost karty ověříme díky obvodu reálného času, který udržuje aktuální čas i po odpojení napájení díky vlastní 3V baterii, a tak může i po delším výpadku napájení a nefunkčnosti serveru určit datum. Nejdříve příkazem mxRTC.updateTime() získáme z DS1302 aktuální datum. Problém při odečtu dvou dní může nastat na přelomu měsíce a při odečítání dnů by mohlo dojít k výsledku se zápornými hodnotami, proto pokud je aktuální měsíc větší než měsíc zapsání, dochází k přepočtu měsíce na dny.

Vzorec pro přepočet data:

$$pomocna = \Big(\big((1 - mesicZapsani) * 30\big) + myRTC.dayofmonth\Big) - denZapsani$$

[12] Zdroj: Vlastní

Do hodnoty pomocna je uložen rozdíl čísel myRTC.dayofmonth a denZapsani. Pomocna je porovnána s pocetPovolenychDni. Pokud je pomocna menší, je nastaven datumExpirace na hodnotu true. Další podmínka vyhodnocuje oprávnění přístupu na základě parametru ulozena-KartaNalezena a datumExpirace, pokud jsou obě podmínky splněny, je rozsvícena zelená LED a je sepnut tranzistor na dobu určenou v proměnné casOtevreniDveri.

7.8 http request

Pokud není splněna podmínka na data expirace a karta nebyla nalezena v paměti zařízení, je vytvořen http požadavek na server accesscontrol.rolda.cz na portu 80. Požadavek vypadá takto:

http://accesscontrol.rolda.cz/checkaccess.php?id_unit=1375&tag=01F70D6

```
client.print("GET /checkaccess.php?id_unit=");
client.print(ID_Unit[0], HEX);
client.print(ID_Unit[1], HEX);
client.print("&tag=");
client.print(ID_karta[0], HEX);
client.print(ID_karta[1], HEX);
client.print(ID_karta[2], HEX);
client.print(ID_karta[3], HEX);
client.println(" HTTP 1.0");
client.println("Host: accesscontrol.rolda.cz");
client.println("Connection: close");
client.println();
```

Obrázek 13:Vytvoření HTTP požadavku[13]

V http požadavku se mění pouze id_unit, v případě že je vícero čtecích zařízení, a tag.

Po odeslání požadavku a dokud je spojení aktivní prohledáváme příchozí odpověď znak po znaku. Http response zasílá stejnou sadu znaků, jen s jedním rozdílem, že v těle odpovědi odesílá 1 nebo 0 podle toho, zda najde kartu v databázi nebo ne. V http response se hledaný znak (1 nebo 0) nachází po znaku male l, v ASCII l=108. V odpovědi se nachází dva znaky l.V první podmínce if(c==108) zvedáme pocitadlo_znaku o 1 a v případě dosažení hodnoty pocitadlo_znaku=2, musíme přeskočit 6 pozic znaků, podmínka if(pocitadlo_znaku ==2)(priznak+=1), abychom se dostali k hledaným rozhodovacím znakům 0 nebo 1. Poté nám už jen stačí určit podle ASCII tabulky, jaký znak jsme dostali, 0 = 48 a 1 = 49, a podle toho

[13]Zdroj: Vlastní

rozhodnout o přístupu do místnosti. Pokud je odpověď serveru 0 nic se neděje, pokud 1, čtečka si uloží kartu do paměti EEPROM.

7.9 Uložení ID karty

```
poradiKarty ++;
if(poradiKarty<pocetPovolenychKaret)
{
EEPROM.write(20, poradiKarty);

if (poradiKarty <= 10)
{
  for (int i = 0; i < 4; i++)
  {
    EEPROM.write(((poradiKarty + 1) * 10) + i + 1, ID_karta[i]);
  }
  myRTC.updateTime();
  EEPROM.write(((poradiKarty + 1) * 10) + 5, myRTC.dayofmonth);
  EEPROM.write(((poradiKarty + 1) * 10) + 6, myRTC.month );
}
```

Obrázek 14: Uložení karty[14]

Proces ukládání karty začíná po úspěšné autentizace karty oproti serveru. Prvním krokem je zvýšení hodnoty poradiKarty o 1 a kontroluje se, zda počet uložených karet nepřesáhl počet povolených karet. Poté se uloží poradiKarty do paměti EEPROM aby nedošlo ke ztrátě dat při výpadku napájení. Data jsou ukládána na pozice podle ukázkové tabulky č.2.

21	22	23	24	25	26
ID_karta[1]	ID_karta[2]	ID_karta[3]	ID_karta[4]	Den	Mesíc

Tabulka 2: Schéma ukládaní záznamu o kartě

Vzorec pro vypočet indexu paměti:

$$index = \big((poradiKarty + 1) * 10\big) + 1 + i$$

Volná místa v paměti se mohou využít pro zvětšení kapacity uložených karet nebo pro ukládání dodatečných informací o čtečce.

[14] Zdroj: Vlastní

8 KONSTRUKCE ŘÍDÍCÍ JEDNOTKY

8.1 Popis hlavních komponent

V této části jsou popsány hlavní komponenty řídící desky.

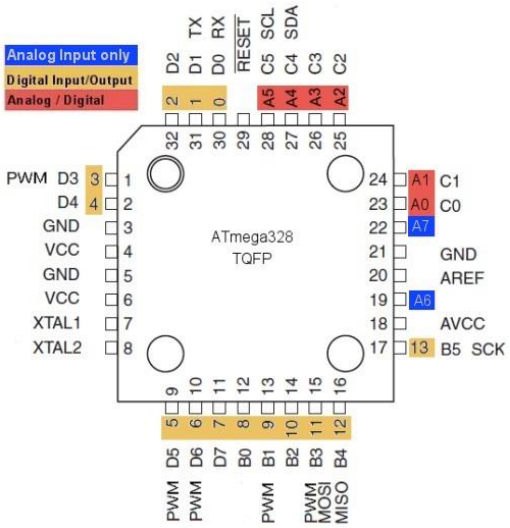
8.1.1 ATMega328P AU

Řídící čip je mikroprocesor ATMega328P AU od firmy Atmel. Mikroprocesor je z důvodu úspory místa na desce v pouzdře TQFP (Thin Quad Flat Package). Písmeno P je kódové označení pro technologii PicoPower. Technologie PicoPower umožňuje mikroporocesoru pracovat s nejnižším výkonem se spotřebou 650nA s RTC a 100nA v režimu Power Down.[13]

Parametry ATMega328P AU

- 8 bitový
- 32KB Flash
- 1KB EEPROM
- 2KB SRAM
- 2x 8b časovač/čítač
- 1x 16 časovač/čítač
- 8 kanálový ADC s rozlišením 10 bitů
- SPI
- 23 programovatelných I/O
- Operační napětí 4.5-5.5V pro frekvenci 0-20MHz
- Pracovní teplota v rozmezí -40 – 85℃

Pracovní takt procesoru byl zvolen 16MHz. Z důvodu vývoje projektu na vývojové desce Arduino Nano bylo nutné dodržet rozvržení pinů procesoru na řídící desce jako na vývojové desce (obrázek č. 14). Na čip byl pomocí programátoru Atmel ICE a vývojového prostředí Atmel Studio 7 nahrán bootloader, což je zavaděč samotného programu, který umožňuje nahrání programu přes vývojové prostředí Arduino IDE. Samotný program je do řídící jednotky nahrán pomocí převodníku USB na UART s čipem FT232.



Obrázek 15:ATMega328 rozložení pinů[15]

8.1.2 Regulátor LM7805DT

Je regulátor s fixním výstupním napětím 5V. Z důvodu co největší miniaturizace projetu bylo použito pouzdro SOT-223 (DPAK). Součástka dokáže dodat proud o velikosti až 1A a je chráněna proti přetížení vnitřním obvodem pro limitaci proudu a tepelným obvodem pro kontrolu teploty. Zapojení regulátoru bylo provedeno podle schématu, které doporučuje výrobce součástky. Oproti doporučenému zapojení je na výstup navíc připojen elektrolytický kondenzátor pro zlepšení kvality výstupního napětí.[15]

8.1.3 RTC DS1302

Mikroprocesor ATMega328P není vybaven interním RTC a z důvodu potřeby sledování času bylo nutné obvod reálného času přidat. Z důvodu dostupnosti byl zvolen obvod DS1302. Čip je v pouzdře DIP8. Hodiny reálného času počítající sekundy, minuty, hodiny, den v měsíci, měsíc, den v týdnu, rok včetně přestupných roků až do roku 2100. Obvod můžeme napájet napětím od 2V do 5,5V. DS1302 uchovává informace v paměti RAM.

Propojení DS1302 s mikroprocesorem je zjednodušeno užitím synchronního sériového přenosu. Pro komunikaci s hodinami/pamětí jsou použity pouze tři vodiče: CE, I/O (data) a SCLK (časovač). Data mohou být přenesena z hodin nebo paměti buď po jednom bajtu, nebo až 31

[15] Zdroj[14]

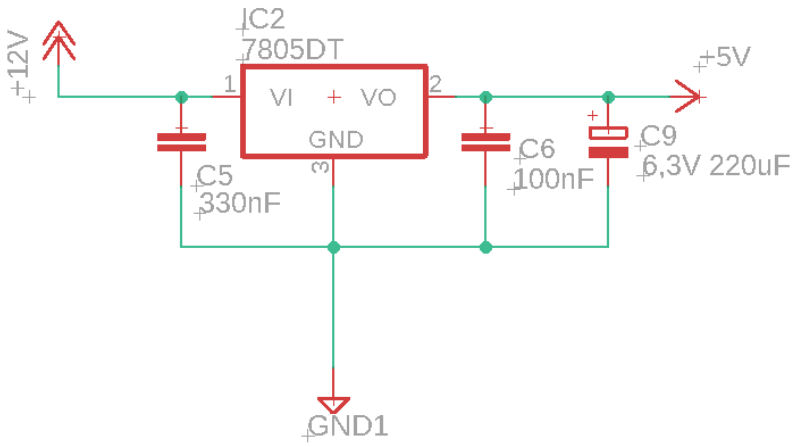
bajtů v burst modu. DS1302 je navržen pro velmi malou spotřebu a udržení dat při příkonu menším než 1µW.

DS1302 využívá externí krystal 32.768kHz. Oscilační obvod k funkčnosti nevyžaduje žádné další kondenzátory, jako je tomu u mikroprocesoru.[16]

8.1.4 Tranzistor BCP-5510

Tranzistor BCP-5510 je NPN tranzistor v pouzdře SOT223. Tento tranzistor byl vybrán z důvodu potřeby spínat napětí 12V pomocí pinu mikroprocesoru, tedy pomocí 5V. Napětí tranzistoru může dosáhnout hodnoty až 60V. Tranzistor je stavěn na kolektorový proud 1A a špičkový proud může být 2A. Maximální proud do báze tranzistoru může být 100mA a špičkový až 200mA. Hodnota bázového rezistoru byla zvolena 1k2Ω. Proud do báze bude tedy omezen na 5mA.

8.2 Schéma napájení modulu



Obrázek 13:Schéma napájení[16]

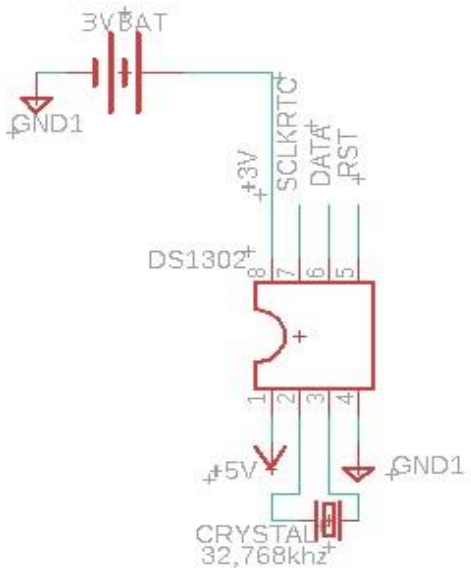
Na řídící desku je přivedeno napětí 12V. Napětí 12V se využívá pro otevření zámkového systému. Pro ostatní komponenty na desce je napětí 12V příliš velké, proto je na desce umístěn

[16] Zdroj: Vlastní

regulátor napětí 7805. Pro vyhlazení stabilizovaného napětí a ochraně obvodu před kolísáním napětí jsou u vstupu a výstupu stabilizátoru umístěny kondenzátory C5, C6 a C9. Hodnoty kondenzátorů byly vybrání podle doporučení výrobce z technického listu.

8.3 Schéma obvodu reálného času

Pro získání času přístupu uživatele je na řídící jednotce umístěn obvod reálného neboli RTC. Vývod 1,4 a 8 slouží pro napájení čipu. Při normálním provozu je čip napájen 5V (vývod 1), ale při ztrátě napájecího napětí je schopen udržet aktuální čas a datum díky 3V baterii CR2032 (Vývod 8). Vývody 2 a 3 Slouží k připojení externího krystalového oscilátoru s frekvencí 32,768KHz. Vývody 7,6 a 5 slouží k přenosu dat a řízení obvodu RTC.



Obrázek 14:Schéma RTC obvodu[17]

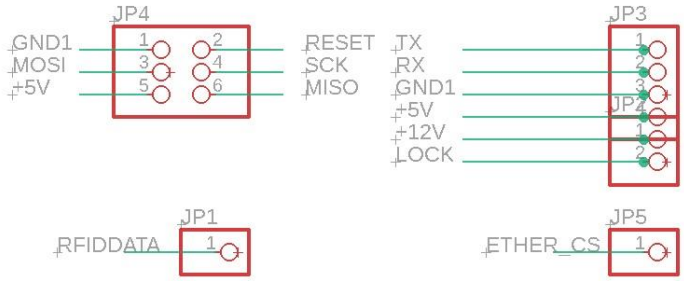
8.4 Vývody

Pro účely programování, napájení a komunikaci řídící desky s ostatními moduly jsou na řídící desce tři sekce vývodů. Na první patici jsou vývody pro napájení modulu 5V a GND, Vývody MISO, MOSI, SCK a RESET slouží k nahrání bootloaderu do procesoru ATMega 328p a následně k připojení ethernetového modulu. Na druhé patici jsou vyvedeny piny mikroprocesoru

[17] Zdroj: Vlastní

RX a TX, které slouží k nahrání programu. Piny 5V a GND1 napájí druhý modul, čtečku HZ-1050. Vývod 12V slouží k přivedení napětí na desku. Pin LOCK otevírá elektrický zámek.

Třetí sekce je samotný vývod z mikroprocesoru, na který přichází za čtecího zařízení data o přiloženém čipu.

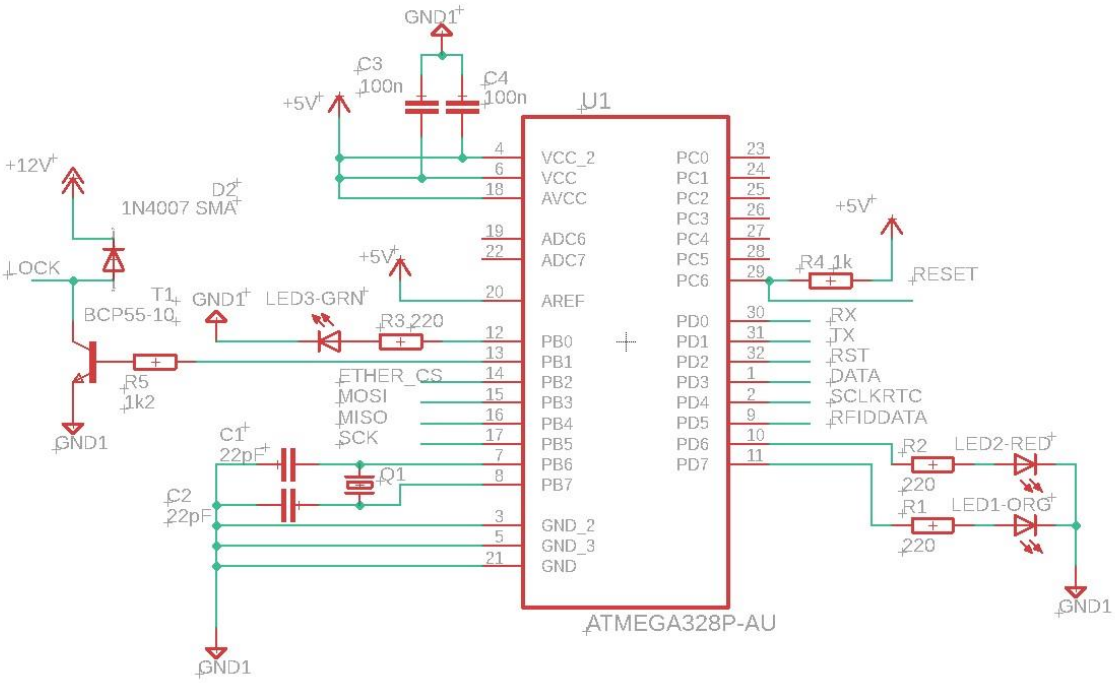


Obrázek 15:Vývody řídící desky[18]

8.5 Schéma zapojení mikroprocesoru

Hlavním komponentem na řídící desce je čip ATMega328P-AU. Vývody napájecího napětí jsou opatřeny kondenzátory, pro případ zakolísání vstupního napětí. Pin 7 a 8 slouží k připojení externího krystalového oscilátoru s frekvencí 16MHz, pro správnou funkčnost oscilátoru jsou mezi jeho vývody a zem připojeny keramické kondenzátory C1 a C2 s kapacitou 22pF. Pin 13 je připojen přes rezistor s odporem 1k2Ω k bázi tranzistoru BCP5510, který slouží k otevření elektrického zámku. Tranzistor je v zapojení se společným emitorem. Jelikož je zámek induktivní zátěž (cívky) je do obvodu zapojena dioda 1N4007, která chrání obvod před možným naindukovaným napětím, které by mohlo zničit tranzistor nebo celou řídící elektroniku. Piny 10, 11 a 12 jsou indikační diody. Do série s diodami jsou zapojeny rezistory s odporem 220Ω, které omezují protékající proud na hodnotu bezpečnou pro LED. Funkce ostatních pinů byla vysvětlena v kapitole Vývody.

[18] Zdroj: Vlastní



Obrázek 16:Schéma zapojení mikroprocesoru[19]

[19] Zdroj: Vlastní

ZÁVĚR

Cílem práce bylo vytvořit zámkový systém s identifikací přes LAN. V teoretické části byla popsána autentizace, nejčastější autentizační metody, elektrické zámky a technologie RFID, která byla vybrána jako jedna z nejrozšířenějších, finančně dostupných a spolehlivých technologií, používaná pro zámkové a přístupové systémy. Prototyp zařízení byl postaven na platformě Arduino. Srdcem prototypu byla vývojová deska Arduino Nano, ke které byl připojen ethernetový modul (připojení zařízení do sítě LAN), RFID modul HZ 1050 (čtení RFID karet) a RTC DS1302 (obvod reálného času).

Program čtecího zařízení byl naprogramován v programu Arduino IDE. Parametry čtecího zařízení je možné nastavovat pomocí internetového prohlížeče. Čtecí zařízení má dva režimy, online a offline. V režimu online je při přiložení čipu ke čtecí jednotce prohledána paměť čtečky a porovnává se databáze uložených karet. Pokud je nalezena shoda a počet dní od posledního průchodu přiloženého čipu není větší než nastavený počet povolených dnů, je umožněn přístup do dveří a je zaznamenán průchod do paměti s aktuálním datem. Není-li však v paměti shoda nebo je počet dní od posledního průchodu vetší než povolený počet dní, je zaslán požadavek na server s číslem čtečky a přiloženým čipem, kde se porovná s databází uložených čipů a vyhodnotí se povolení ke vstupu. Kladné vyhodnocení přístupu je zaznamenáno do paměti čtečky. Offline režim porovnává pouze data uložené v paměti čtečky a nezasílá požadavky na server.

Pro správu databáze se čtečkami a uživatelskými čipy byla vytvořena aplikace s grafickým rozhraním, která se ovládá pomocí několika ovládacích prvků a není tak potřeba znalosti jazyka SQL a databázových systémů. Aplikace byla vyvíjena ve vývojovém prostředí Visual Studio v jazyku C#.

Řídící deska systému byla navržena v programu EAGLE. Deska obsahuje mikroprocesor ATMega 328p AU, který řídí chod zařízení a komunikuje s připojenými periferiemi. K napájení desky je potřeba napětí 12V, které je využito pro otevření zámku. Zámek je otevírán přes tranzistor BCP5510. Napětí pro procesor je regulováno na 5V stabilizátorem 7805. Na desce je patice pro umístění RTC obvodu DS1302 a patice pro 3V baterii, která udržuje v chodu obvod DS1302 při ztrátě napájecího napětí.

POUŽITÁ LITERATURA

[1] Autentizace. In: Wikipedia: the free encyclopedia[online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2019-04-28]. Dostupné z: https://cs.wikipedia.org/wiki/Autentizace

[2] KLAUZ, Milan. Jaký je rozdíl mezi aktivním a pasivním RFID?. DPS [online]. 2017, 2017(5), 6-7 [cit. 2019-04-23]. ISSN 1805-5044. Dostupné z: https://www.dps-az.cz/vyvoj/id:53208/jaky-je-rozdil-mezi-aktivnim-a-pasivnim-rfid-

[3] VOJTĚCH, Lukáš. Frekvence používané různými aplikacemi RFID. In: DPS [online]. Liberec: CADware, 2011 [cit. 2019-04-23]. Dostupné z: https://www.dps-az.cz/zajimavosti/id:10415/rfid-transpondery-pohled-pod-kuzi

[4] Em Microelectronic - Marin SA [online katalogavý list]. EM4100. © 2004 [2019-04-28]. Dostupné z: http://www.smartstripe.com/wp-content/uploads/2012/10/EM4100.pdf

[5] Tutorials Point. In: Tutorials Point [online]. Telangana: Tutorials Point, ©2019 [cit. 2019-04-28]. Dostupné z: https://www.tutorialspoint.com/digital_communication/digital_communication_phase_shift_keying.htm

[6] ANDRÁSSY, Juraj. UIPEthernet. Github [online]. San Francisco: Github, 2019 [cit. 2019-04-28]. Dostupné z: https://github.com/UIPEthernet/UIPEthernet

[7] Libraries. Arduino [online]. Boston: Arduino, ©2019 [cit. 2019-04-28]. Dostupné z: https://www.arduino.cc/en/reference/libraries

[8] Microship technology Inc. [online katalogový list]. ENC28J60. ©2008[cit. 2019-04-28]. Dostupné z: http://ww1.microchip.com/downloads/en/devicedoc/39662c.pdf

[9] Advanced Monolithic Systems Inc. [online katalogový list]. AMS117. ©2007. [cit. 2019-04-28]. Dostupné z: http://www.advanced-monolithic.com/pdf/ds1117.pdf

[10] Toshiba Corparation [online katalogový list]. 74HCT08D. ©2016[cit. 2019-04-28]. Dostupné z: https://toshiba.semicon-storage.com/info/docget.jsp?did=37143&prodName=74HCT08D

[11] GAMMON, Nick. RFID reader - HZ-1050. Gammon Software Solution [online]. -: Gammon Software Solution, 2015 [cit. 2019-04-28]. Dostupné z: http://www.gammon.com.au/forum/?id=12849

[12] Technologie radiofrekvenční identifikace. RFID-EPC.cz [online]. Praha: GS1 Czech Republic, ©2016 [cit. 2019-04-29]. Dostupné z: https://www.rfid-epc.cz/co-je-rfid/technologie

[13] Atmel Corporation [online katalogový list]. ATMega48/88/168/328. ©2009. [cit. 2019-05-02]. Dostupné z: https://www.sparkfun.com/datasheets/Components/SMD/ATMega328.pdf

[14] Arduino ATmega328 Pinout. In: HobbyTronics Ltd [online]. Wilberfoss: HobbyTronics, ©2019 [cit. 2019-05-02]. Dostupné z: http://www.hobbytronics.co.uk/arduino-atmega328-pinout

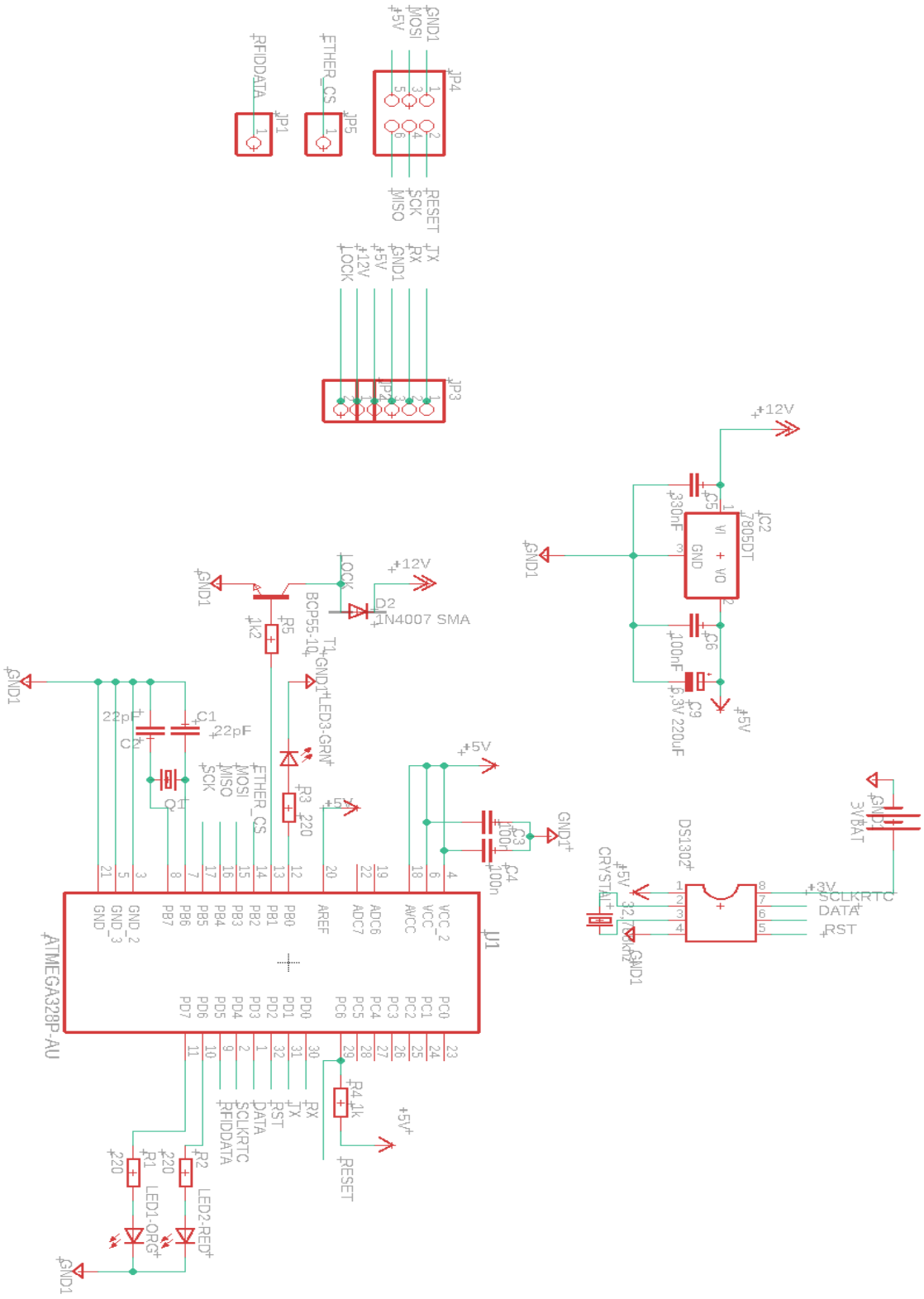
[15] Texas Instruments Incorporated [online katalogový list]. LM340, LM340A and LM7805 Family Wide VIN 1.5-A Fixed Voltage Regulators. ©2016 [cit. 2019-05-02]. Dostupné z: http://www.ti.com/lit/ds/symlink/lm340.pdf

[16] Maxim Integrated Products [online katalogový list]. DS1302 Trickle-Charge Timekeeping Chip. © 2015 [cit. 2019-05-02]. Dostupné z: http://www.farnell.com/datasheets/1904443.pdf?_ga=2.45024356.1704758577.1556782426-59484569.1550579487

[17] Elektrické zámky a jiné typy otvíračů. *K.V.H.* [online]. Praha: K.V.H., ©2019 [cit. 2019-05-02]. Dostupné z: http://www.kvh.cz/domovni-dorozumivaci-systemy-dds/elektricke-zamky-a-jine-typy-otviracu

PŘÍLOHY

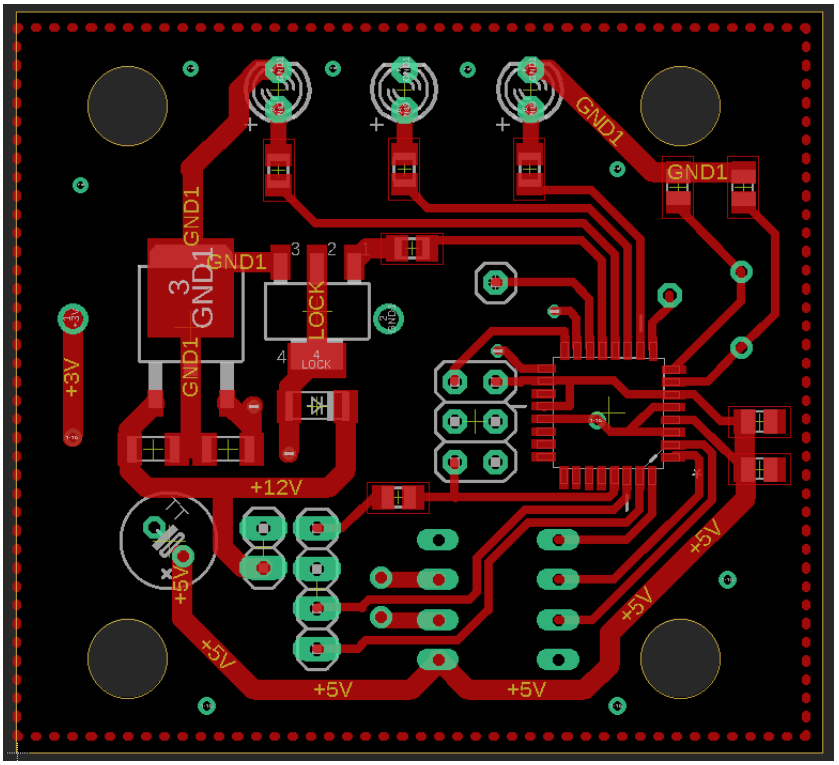
PŘÍLOHA A – SCHÉMA ZAPOJENÍ ŘÍDÍCÍ JEDNOTKY

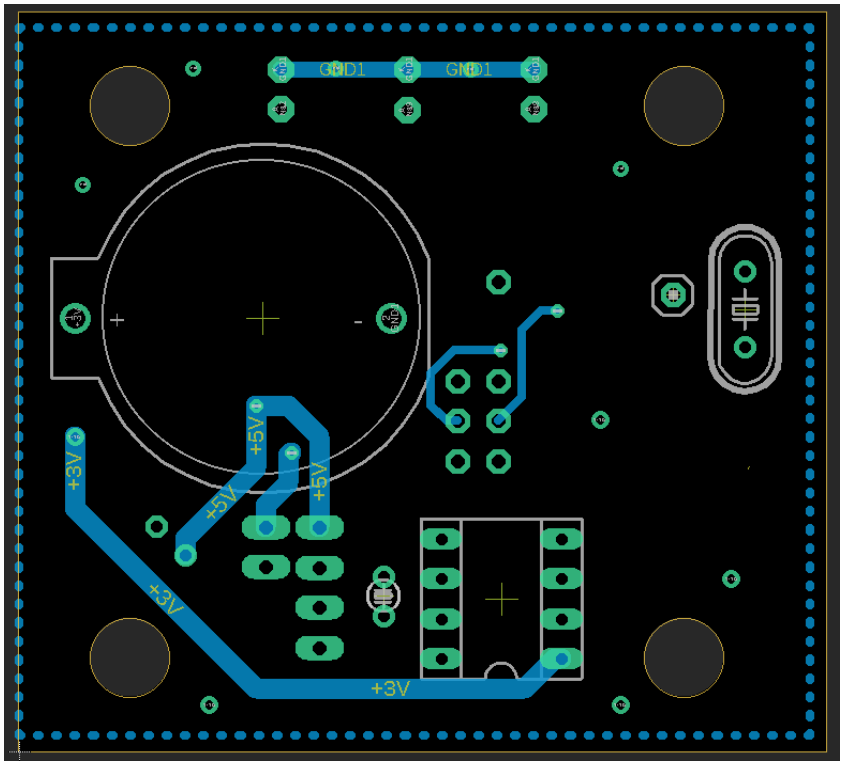


PŘÍLOHA B – SEZNAM SOUČÁSTEK

C1	22pF	C-EUC0805
C2	22pF	C-EUC0805
C3	100nF	C-EUC0805
C4	100nF	C-EUC0805
C5	330nF	C-EUC1206K
C6	100nF	C-EUC1206K
C9	220uF	CPOL
Q2	32,768khz	CRYSTALTC26V
D2	1N4007	CGRM4007-G
IC2	7805DT	TO252(DPAK)
LED1	ORG	LED3MM
LED2	RED	LED3MM
LED3	GRN	LED3MM
Q1	16MHz	CRYSTALHC49S
R1	220Ω	R-EU_M0805
R2	220Ω	R-EU_M0805
R3	220Ω	R-EU_M0805
R4	1kΩ	R-EU_R0805
R5	1k2 Ω	R-EU_M0805
T1	BCP55-10	NPNSOT223
U2	DS1302	DIL8S
U1	ATMEGA328P-AU	TQPF
3VBAT	BATTERY-20MM_PTH	BATTCOM_20MM_PTH

PŘÍLOHA C – NÁVRH DPS ŘÍDÍCÍ JEDNOTKY





PŘÍLOHA D – OBSAH CD

- BP_Cernohorsky_2019_KodRidiciJednotky (DIR)
  - BP_Cernohorsky_2019_KodRidiciJednotky.ino

- BP_Cernohorsky_2019_SchemaEAGLE (DIR)
  - BP-schema.b##
  - BP-schema.b#
  - BP-schema.brd
  - BP-schema.s#1
  - BP-schema.s#2
  - BP-schema.sch
  - BP-schema.txt

- BP_Cernohorsky_2019_SpravaPristupuC# (DIR)
  - vs (DIR)
  - App.config
  - bin (DIR)
  - BP_spravapristupu.csproj
  - BP_spravapristupu.sln
  - Form1.cs
  - Form1.Designer.cs
  - Form1.resx
  - obj (DIR)
  - Program.cs (DIR)
  - Properties (DIR)

- CernohorskyJ_RFIDZamek_JR_2019.pdf

PŘÍLOHA E – FOTOGRAFIE ŘÍDÍCÍ JEDNOTKY