UNIVERZITA PARDUBICE
Fakulta elektrotechniky a informatiky

ELEKTRONICKÝ PŘÍSTUPOVÝ SYSTÉM

Tomáš Otto

Bakalářská práce
2021

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: 2020/2021

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Tomáš Otto**
Osobní číslo:	**I18310**
Studijní program:	**B2612 Elektrotechnika a informatika**
Studijní obor:	**Řízení procesů**
Téma práce:	**Elektronický přístupový systém**
Zadávající katedra:	**Katedra řízení procesů**

Zásady pro vypracování

Cílem práce je realizace elektronického přístupového systému s ověřením proti autentizačnímu serveru. V teoretické části popište možnosti ověření vůči přístupovému systému a vůči serveru. V praktické části navrhněte a realizujte hardware elektronického přístupového systému a vytvořte webové prostředí pro správu tohoto systému. Ověřte funkci realizovaného systému.

Rozsah pracovní zprávy:
Rozsah grafických prací:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

[1] OPRŠAL, Daniel. Zámek dveří s ověřením přes LAN , Bakalářská práce, Pardubice, 2019, Univerzita Pardubice.
[3] ESP32 Data Sheet. Espressif, 2020, [cit. 1. 12. 2020].
Dostupné z URL: https://www.espressif.com/sites/default/files/documentation/esp32_datasheet_en.pdf

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

Datum zadání bakalářské práce: **27. listopadu 2020**
Termín odevzdání bakalářské práce: **14. května 2021**

L.S.

Ing. Zdeněk Němec, Ph.D.
děkan

Ing. Daniel Honc, Ph.D.
vedoucí katedry

V Pardubicích dne 29. ledna 2021

Prohlášení

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 14. 05. 2021 Tomáš Otto

Poděkování

Rád bych tímto poděkoval vedoucímu práce Ing. Jiřímu Rolečkovi za vstřícný přístup, cenné rady a pomoc při tvorbě této bakalářské práce. Dále bych chtěl poděkovat své rodině a přátelům za podporu během celého studia

V Pardubicích dne 14. 05. 2021 Tomáš Otto

ANOTACE

Práce je věnována problematice elektronického přístupového systému. Systém vyhodnocuje uživatelské RFID transpondéry pomocí řídicí jednotky, která se dotazuje místního serveru. Pomocí daného serveru spravujeme uživatelské karty a vazby mezi kartami a řídicími jednotkami.

KLÍČOVÁ SLOVA

elektronický přístupový systém, RFID, webový server

TITLE

ELECTRONIC ACCESS SYSTEM

ANNOTATION

The work is devoted to the issue of electronic access system. The system evaluates user RFID transponders using a control unit that asks the local server for authorization. We use the given server to manage user cards and links between cards and control units.

KEYWORDS

Electronic access system, RFID, web server

OBSAH

SEZNAM ZKRATEK

HF	High Frequency
IP	Internet Protocol
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
LF	Low Frequency
RFID	Radio Frequency Identification
SPI	Serial Peripheral Interface
SSID	Service Set Identifier
UHF	Ultra High Frequency
UID	Unique Identifier
URL	Uniform Resource Locator
Wi-Fi	Wireless Fidelity

SEZNAM ILUSTRACÍ

SEZNAM TABULEK

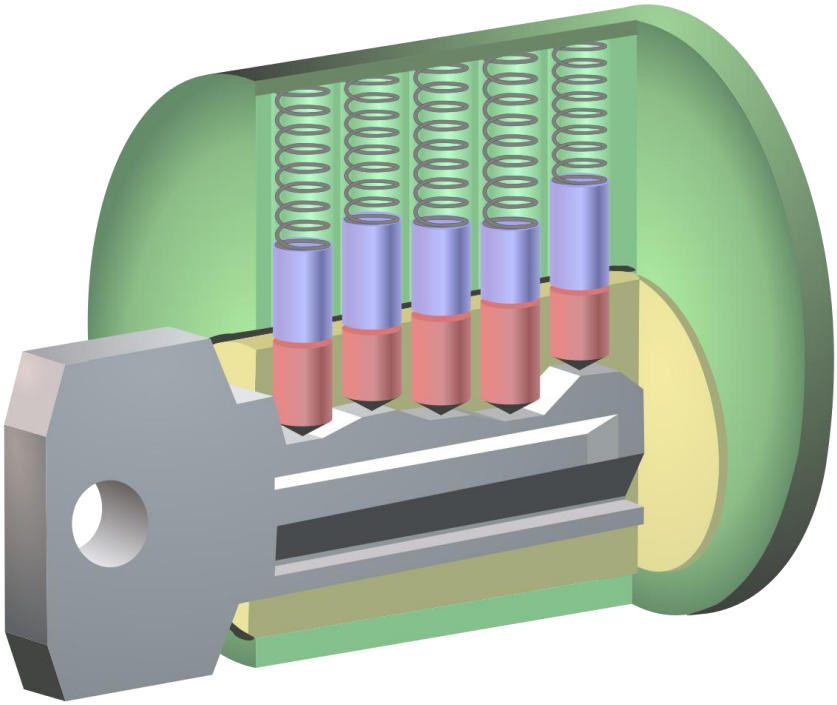
ÚVOD

Bakalářská práce se zabývá funkcionalitou a realizací elektrických zámkových systémů, které jsou využívány převážně v budovách a objektech s rozsáhlým počtem osob a různými prioritami přístupů do různých prostorů. Elektronické zámkové systémy jsou užitečné pro hotelové objekty, rozsáhlé firemní a kancelářské prostory, školní objekty a státní úřady. Výhodou takovýchto systému je převážně centralizace kontroly přístupu a využití moderních technologií pro zabezpečení daných objektů.

1 HISTORIE ZÁMKŮ

1.1 MECHANICKÉ ZÁMKY

Archeologické důkazy prastarých zámkových designů byly objeveny v ruinách hlavního města Asýrie, které byly později využívány v egyptských zámcích. Zámky, ve kterých bylo potřeba specifických klíčů, se začaly objevovat již ve starověkém Římě. Po příchodu průmyslové revoluce na konci 18. století, vývoji precizního inženýrství a standardizace komponentů se zámky a klíče začaly vyrábět s vyšší úrovní preciznosti a sofistikovanosti. Moderní mechanické zámky jsou variantami zámků z této doby, byť s menšími úpravami (Lock and Key, 2021).



Obrázek 1.1 – Kolíkový zámek s klíčem (Lock and Key, 2021)

Běžným designem mechanického zámku je kolíkový systém. Série kolíků znemožňuje odemčení zámku, pokud není vložen klíč se správnou stopou. Klíč vysune kolíky zámku do takové výšky, kdy je umožněno otočení vnitřního válce. Hlavní slabinou daného zámku je možnost vyzkoušet všechny možnosti výšky daných kolíků a po nalezení správné výšky může být daný kolík zajištěn na místě aplikováním rotačního pohybu na vnitřní válec (Lock and Key, 2021).

Přestože se tato slabina vztahuje na kolíkový zámek, ostatní designy zámků trpí podobnými slabinami, které útočník může využít k prolomení zámku a získání přístupu do zabezpečeného prostoru nebo k zabezpečenému majetku.

1.2 ELEKTRONICKÉ ZÁMKY

Elektronická přístupová kontrola se snaží zamezit slabinám běžných mechanických zámků pomocí nahrazení klíče různými identifikačními prvky. Elektronický přístupový systém umožňuje odemčení zámku pouze na základě správnosti hodnot přiložených identifikačních prvků. Zámek takového systému je tvořen elektrickým dveřním systémem, který umožní přístup do místnosti při průchodu elektrického proudu. Daný zámek tak neobsahuje přímé slabiny, kterých může útočník snadno využít, není však odolný proti ostatním typům útoku. Výhodou daného systému je způsob a kontrola daného přístupu. Uživatel může získat přístup na základě jednoduššího identifikačního prvku, který mu umožní přístup do různých objektů. Není zde nutnost nošení velikého množství klíčů pro velké množství zámků. Uživateli stačí, aby si pamatoval heslo, nosil v kapse přístupovou kartu nebo ověřil své biometrické údaje na skeneru (Access control, 2021).

Pokud je přístup odepřen na základě přiložených údajů, uživateli není povolen přístup do objektu. Pokud je uživateli přístup povolen, systém uživatele informuje rozsvícenou LED nebo zvukovým signálem, případně kombinací.

1.3 ZPŮSOB ÚTOKU A OPATŘENÍ

Přesto, že elektronický systém eliminuje slabiny, kterým čelí mechanické zámky. Útočník může otevřít schránku elektronického systému a přiložit vlastní zdroj napětí na elektrický zámek, čímž otevře dveře bez nutnosti přikládat transpondér. Můžeme zabránit otevření schránky pomocí antivandal systému. Magnetický senzor je umístěný uvnitř schránky v blízkosti magnetického pole permanentního magnetu. Pokud dojde k otevření schránky nelegitimním způsobem, magnet se vzdálí od magnetického senzoru a daný senzor začne vést elektrický proud. Řídicí jednotka tento proud zachytí a spustí varovný systém a také zaznamená otevření schránky na server (Access control, 2021).

Útočník však může mít znalost o tomto antivandal systému a může k tělu elektronického systému přiložit vlastní permanentní magnet. Pokud však přiloží své vlastní napětí a otevře zámek, může magnetický senzor na dveřním zámku zaznamenat dané otevření. Pokud přístup nebyl povolen řídicí jednotkou, bude aktivován varovný systém. Magnetický senzor se bude nacházet na vnitřní straně dveří, což znemožní útočníkovi tento magnetický senzor ošálit.

1.4 ÚTOK NA RFID PŘÍSTUPOVÝ SYSTÉM

Moderním způsobem přístupu do elektronického zámku jsou RFID čipy, které obsahují unikátní identifikátory. Pokud útočník nalezne unikátní identifikátory čipů od osob s přístupem do objektu, může jejich identifikátory zkopírovat a přepsat unikátní identifikátory na vlastním RFID čipu pomocí specializovaného zařízení. Útočník může tyto unikátní identifikátory získat přímo, naskenováním karet zaměstnanců ve chvíli, kdy nedávají pozor. Druhý způsob je nepřímý, kdy útočník může do těla elektronického systému vložit vlastní zařízení, které bude číst výstup ze čtecího zařízení. Může tak získat větší množství karet, časy jejich použití a ostatní informace, které může využít k útoku (PETERSEN, 2020).

Přestože útočník může využít této slabiny, jeho útok bude zaznamenán na serveru. Každý přístup do objektu je zaznamenán, společnost nebo bezpečnostní složky mohou získat znalost o osobách, byť falešných, které o daný přístup požádaly pomocí svého čipu a zjistit, který přístup byl legitimní.

Tomuto útoku je možno zabránit pomocí časového omezení přístupu. Každá karta tak může získat přístup v povoleném čase (např. přes pracovní dobu) nebo pouze v povolené dny (např. pouze přes pracovní týden).

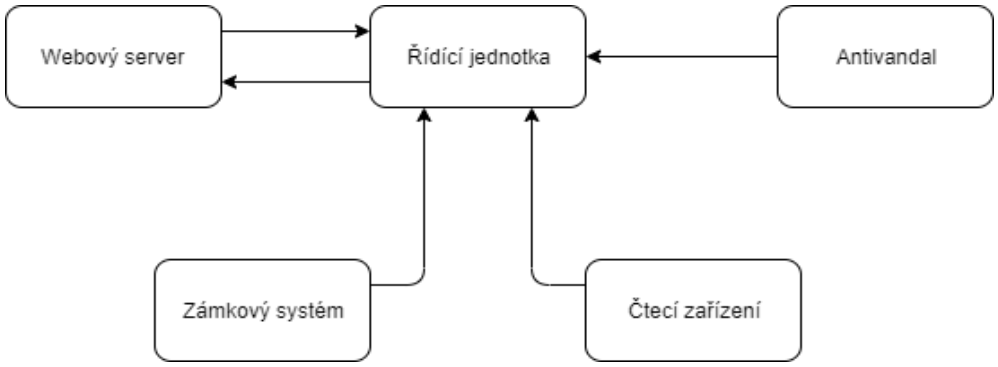
2 TEORETICKÁ REALIZACE

2.1 ZÁKLADNÍ POPIS

Základním stavebním prvkem elektronického přístupového systému je řídicí jednotka, která zpracovává data ze čtecího zařízení, kontroluje antivandal systém, dotazuje se serveru na oprávnění přístupu a řídí vstupní napětí na elektrický zámek pomocí tranzistoru. Pro dotazování na server je nutné, aby řídicí jednotka měla schopnost přihlásit se k místní síti.

Čtecí zařízení slouží pro přiložení uživatelského RFID čipu. Data z RFID čipu jsou zpracována specializovaným modulem, který tato data přenese na vstup řídicí jednotky.

Zámkový systém je běžný, komerčně dostupný elektronický zámek. Napětí uvolní zámek, což umožní uživateli otevřít dveře. Většina zámkových systémů funguje na 12 V stejnosměrného napětí, které můžeme do zámkového systému dodávat pomocí stejného zdroje, který využíváme pro napájení řídicí jednotky.



Obrázek 2.1 – Diagram elektronického systému

Server se nachází na stejné síti, jako řídicí jednotka. Webový server obsahuje veškeré uživatelské karty a identifikátory řídicích jednotek, stejně tak jako databázi vazeb, které obsahují povolené kombinace. Uživatel může data na tomto serveru upravovat pomocí internetového prohlížeče.

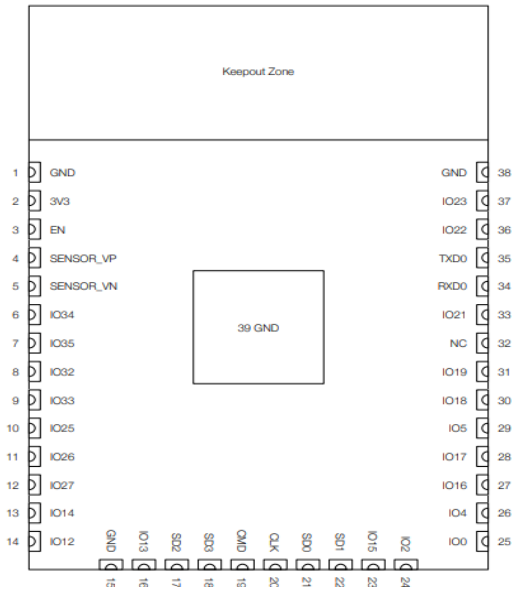
2.2 ŘÍDICÍ JEDNOTKA

Základním stavebním prvkem je řídicí jednotka, která řídí veškeré periferie elektronického přístupového systému. Základní funkcí, kterou musí řídicí jednotka mít, je schopnost připojit se na místní internetovou síť a vytvořit přístupový bod pro uživatele.

Pro řídicí jednotku využijeme modul ESP32-WROOM-32, který má schopnost připojit se k místní síti. Danou funkci využijeme pro dotazování se na server. Přístupový bod využijeme pro vytvoření webového serveru na daném modulu, pomocí kterého budeme moci ovlivňovat

hodnoty řídicí jednotky. Dané hodnoty jsou SSID a heslo místní sítě, IP adresa webového serveru s uživatelskými daty a možnost vytvoření hesla pro danou řídicí jednotku.

ESP32-WROOM-32 má funkční napětí mezi 3,0 V až 3,6 V. Průměrný proudový odběr modulu je 80 mA. Přestože modul obsahuje takzvaný “deep sleep” mód, který omezuje funkcionalitu modulu, nemůžeme daný mód využít, protože modul musí být vždy dostupný pro zpracování karet a přístupového bodu. Dané energetické nároky vyžadují napájení ze sítě pomocí transformátoru (ESP32–WROOM32: Datasheet, 2021).



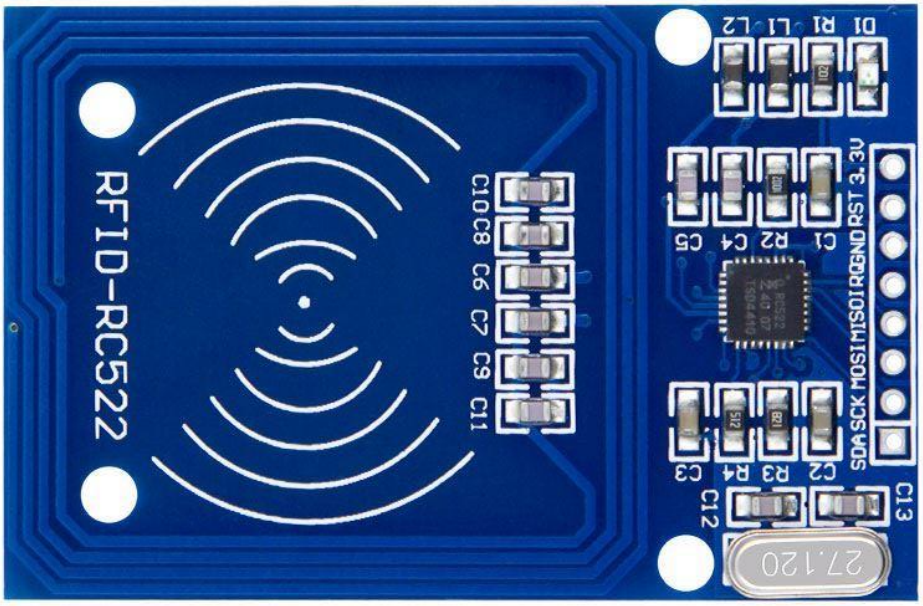
Obrázek 2.2 – ESP32-WROOM-32
(ESP32–WROOM32: Datasheet, 2021)

2.3 ČTECÍ ZAŘÍZENÍ

Pro čtení RFID čipů potřebujeme specializované zařízení. Pro danou funkci využijeme modul RFID-RC522, který obsahuje čip MFRC522. Čip je vysoce integrovaný prvek pro bezkontaktní komunikaci na 13,56 MHz. Modul nám umožňuje komunikovat s ISO/IEC 14443 A/MIFARE transpondéry bez nutnosti dalších obvodů. Čtečka může komunikovat s řídicí jednotkou pomocí čtyř pinů SPI.

Na modulu využíváme veškeré piny kromě pinu IRQ, který se využívá pro informování mikrokontroléru na příchod transpondéru do blízkosti čtecího zařízení. Piny VCC a GND jsou pro napájení modulu samotného. Pin RST se využívá pro resetování modulu. Piny MISO a MOSI se využívají pro datový přenos ze čtecího zařízení. SDA pin je sériový input, který slouží pro SPI komunikaci. SCK pin slouží jako zdroj hodinového signálu pro modul.

Při komunikaci se modul chová jako slave, přičemž řídicí jednotka se chová jako master. Master musí pro jednotku generovat hodinový signál na pin SCK. Komunikace z MFRC522 pro mastera se provádí na pinu MISO (MFRC522, 2016).



Obrázek 2.3 – Modul RFID-RC522
(Modul RFID-RC522 13,56MHz s klíčenkou a kartou, Nedatováno)

MOSI pin na zařízení zasílá adresy, ze kterých chce číst a MISO zpět posílá data. Tato data jsou v řídicím zařízení uložena do objektu mfrc522, který obsahuje objekt uid. Upravené hodnoty pole pomocí logického posunu doleva jsou pak sečteny. Výsledkem je unikátní identifikátor karty. Hodnoty UID a ostatní data výrobce transpondéru jsou uložena v prvním bloku nultého sektoru (MFRC522, 2016).

Line	Byte 0	Byte 1	Byte 2	To	Byte n	Byte n + 1
MOSI	address 0	address 1	address 2	...	address n	00
MISO	X[1]	data 0	data 1	...	data n – 1	data n

[1] X = Do not care.

Obrázek 2.4 – Čtení n bajtů ze čtecího zařízení (MFRC522, 2016).

2.4 ZÁMKOVÝ SYSTÉM

Elektrické zámkové systémy fungují na několika principech a designech. Většina těchto zámkových systémů funguje na 12 V stejnosměrného napětí. Dané napětí můžeme dodávat ze zdroje, kterým napájíme řídicí jednotku a kontrolovat dané napětí pomocí tranzistoru.

Obrázek 2.5 – Elektronický zámek BeFo Klasik
(Elektrický otvírač BeFo Klasik, Nedatováno)

2.5 ANTIVANDAL SYSTÉM

Pro antivandal systém využíváme jednoduchý magnetický přepínač. Magnetické pole je v tomto případě vytvořené permanentním magnetem. Magnetické pole přerušuje kontakt v daném přepínači a nedovoluje průchod proudu. Pokud se však magnetické pole vzdálí od magnetického přepínače, dojde k uzavření obvodu a průchodu proudu. Daný proud je přiveden na kontrolní pin řídicí jednotky, která tento proud vyhodnotí jako nelegitimní otevření těla přístupového systému.

Obrázek 2.6 – Magnetický kontakt KSK1C90-1520
(Reed Contact SPDT 0,25A 3W AW15-20, Nedatováno)

Stejný magnetický přepínač využíváme také pro kontrolu otevření dveří. Magnetický senzor je vyveden ze zařízení pomocí svorkovnice a bude uložen do elektronického zámku. Pokud jsou dveře otevřeny, permanentní magnet se vzdálí od magnetického senzoru, což způsobí průchod proudu, který bude zaznamenán na vstupním pinu řídicí jednotky.

Využíváme dva magnetické přepínače pro zajištění větší bezpečnosti. Pokud útočník dokáže překonat magnetický přepínač v těle zařízení a pomocí vlastního zdroje napětí nebo pomocí přemostění na zámek přivede požadované napětí, otevření dveří v daném případě způsobí aktivaci magnetického senzoru na dveřním zámku, ke kterému útočník nemůže přistoupit. Pokud byl permanentní magnet z blízkosti tohoto senzoru oddálen bez autorizace řídicím zařízením, způsobí to varování na serveru.

2.6 WEBOVÝ SERVER

Webový server obsahuje veškeré uživatelské transpondéry, identifikátory řídicích jednotek a vazby mezi těmito prvky. Webový server je vytvořen pomocí vývojového prostředí WampServer, který nám dovoluje vytvářet webové aplikace pomocí PHP a dovoluje nám spravovat MySQL databáze.

Uživatel oprávněný k práci na tomto serveru může vkládat nebo mazat prvky z těchto databází, vytvářet nové vazby nebo mazat vazby již nevyužívané. Pro administrativní a bezpečnostní důvody nejsou prvky ani vazby z databáze mazány, pouze deaktivovány. Společnost tak může získat přístup k již nefunkčním prvkům a získat informace o dané kartě nebo vazbě.

3 RFID

3.1 HISTORIE

Rádiově-frekvenční identifikační systém se poprvé začal využívat za druhé světové války, kdy spojenecké a německé letectvo využívalo danou technologii pro identifikaci vlastních nebo nepřátelských letadel (RFID, 2021).

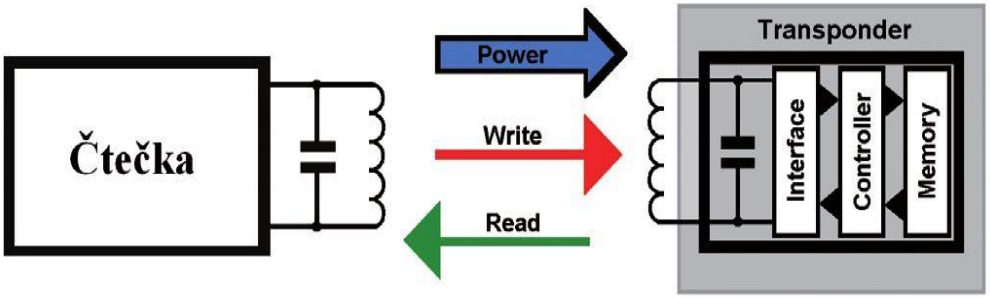
Technologie byla také využita americkou vládou. Ministerstvo energie potřebovalo způsob kontroly nukleárního materiálu. Řešením bylo nainstalovat transpondéry na nákladní vozidla přenášející nukleární materiál, které by mohly být přečteny okamžitě u brány (RFID, 2021).

RFID technologie se v dnešní době využívá pro sledování položek téměř v každém odvětví. Hlavní výhodou nad běžnými čárovými kódy je větší množství přenášených dat. (RFID, 2021)

3.2 PRINCIP

Čtecí zařízení do své blízkosti zasílá elektromagnetické vlny o určité frekvenci. Pokud se v blízkosti daného elektromagnetického pole nachází RFID transpondér, naindukuje se na něm potřebné napětí, kterým se nabije napájecí kondenzátor. Transpondér následně vysílá data uložena ve své paměti zpět na čtecí zařízení (RFID, 2021).

Transpondéry mohou být aktivní a pasivní. Aktivní transpondéry využívají vlastní zdroj energie pro přenos dat. Pasivní transpondéry získávají potřebné napětí z elektromagnetických vln čtecího zařízení. Pasivní transpondéry jsou v dnešní době mnohem více využívané. Mají nízkou výrobní cenu a dlouhou životnost (RFID, 2021).



Obrázek 3.1 – Princip funkce RFID (OPRŠAL, 2019)

3.3 FREKVENCE

Technologie RFID funguje na specifických frekvencích, které mají různé výhody a nevýhody a ovlivňují nejen výkonnost a velikost transpondérů, ale také cenu daných transpondérů a čtecích zařízení.

Nižší frekvence mají nižší hodnotu energie, což znamená, že data přenášejí pomaleji a na menší vzdálenost. Jejich výhodou je však tolerance proti fyzickým překážkám a také proti menšímu množství kovů, které mohou ovlivnit tyto elektromagnetické vlny.

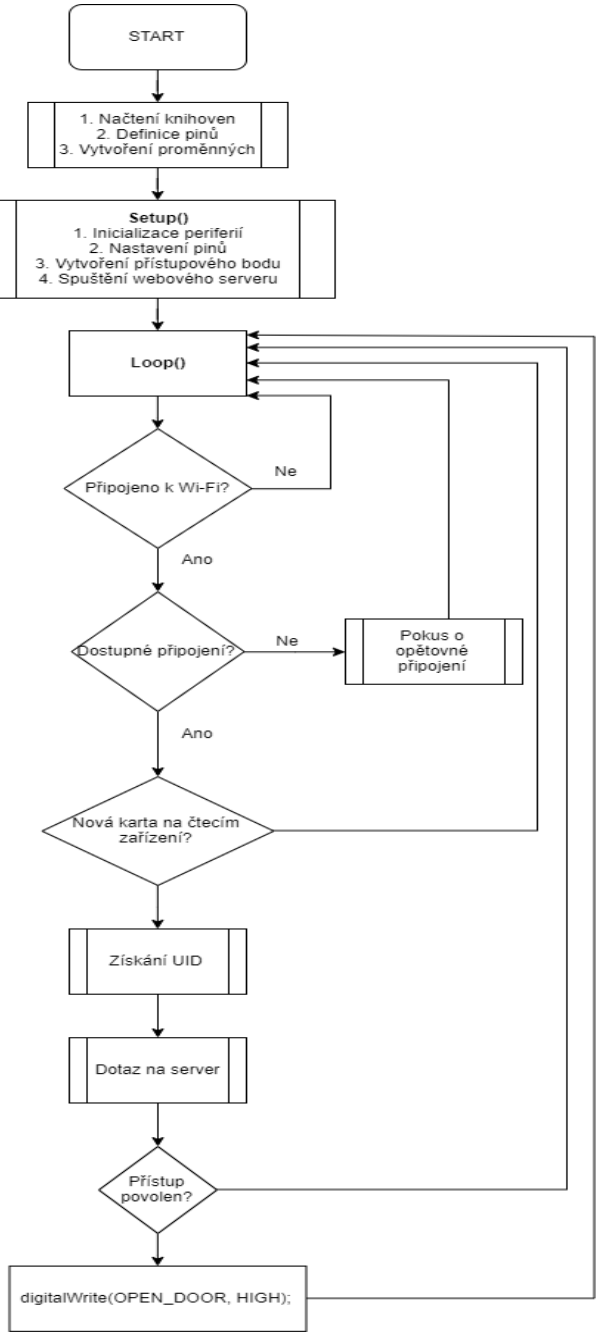
Vyšší frekvence mají vyšší hodnotu energie a můžou se tak využívat na větší vzdálenosti s větším množstvím přenesených dat. Může být využit paprsek, což nám umožní lokalizovat transpondér v trojrozměrném prostoru. Nevýhodou je snadné zastavení těchto paprsků, vliv vln na lidské zdraví, nemožnost vidět za roh nebo skrze objekty, přes které může člověk vidět bez problémů (DAS, 2016).

Tabulka 3.1 – Frekvence RFID a porovnání (DAS, 2016)

<table>
<tr><th>Frekvence</th><th>Využití</th><th>Kladné vlastnosti</th><th>Záporné vlastnosti</th></tr>
<tr><td>125-135 KHz</td><td>Pivní barely, plynové lahve, pneumatiky</td><td>Možnost vidět za roh a skrze většinu materiálu, levná elektronika</td><td rowspan="2">Dosah okolo 1 m (signál rychle ztrácí energii), pomalý datový přenos</td></tr>
<tr><td>13,56 MHz</td><td rowspan="3">Dopravní prostředky, knihovny, bankovky, bezpečnostní přístup, letadlová doprava</td><td>dosah 1 m, tolerance na kov a kapaliny, standardizace</td></tr>
<tr><td>UHF</td><td>Největší dosah</td><td rowspan="2">Jednoduché odstínění nebo absorpce signálů, zdravotní problémy s povoleným mikrovlnným zářením, drahá čtečka</td></tr>
<tr><td>GHz</td><td>Dlouhý dosah, vysoký datový přenos, nejlevnější transpondér</td></tr>
</table>

4 SOFTWARE

Tato kapitola pojednává o programu, který běží na řídicí jednotce. Program pro řídicí jednotku zajišťuje velké množství funkcí, od správy přístupového bodu, kontroly přístupu a čtení antivandal systému. Program byl napsán v jazyce C ve vývojovém prostředí Arduino IDE 1.18.13.



Obrázek 4.1 – Diagram programu

4.1 NASTAVENÍ ŘÍDICÍ JEDNOTKY

Na začátku programu nastavíme důležité hodnoty a piny řídicí jednotky pro vstup a výstup, čímž kontrolujeme LED a antivandal systém, stejně jako tranzistor pro elektrický zámek. Vstupní piny pro antivandal systém a dveřní magnet jsou také nastaveny na interní pull-down rezistor pro zajištění jasné LOW hodnoty, když dané magnetické přepínače nevodí proud.

Je zde nastaven Wi-Fi modul řídicí jednotky na tzv. WIFI_AP_STA mód. Daný mód nám umožní připojit se na místní síť a spravovat přístupový bod ve stejnou chvíli (ESPRESSIF, ©2016-2021).

Nastavujeme zde knihovnu pro SPI, pomocí které budeme získávat informace z dat ze čtecího zařízení stejně jako nastavení pinů, které budou zodpovědné za přenos samotných dat ze čtecího zařízení.

Nastavujeme zde také webový server na přístupovém bodě, pomocí kterého kontrolujeme řídicí jednotku. Vkládáme do serveru několik URL, které chceme uživateli ukázat. Také zde vkládáme chybovou stránku v případě, že uživatel udělá chybu v zadávání URL.

4.2 PROGRAM

Prvním krokem programu je kontrola antivandal systému. Pokud je na pinu hodnota proudu, kterou modul chápe jako logickou 1, je na webový server zasláno varování, které se zapíše do záznamového systému serveru. Pro zaslání varování musí mít modul nastavenou hodnotu IP daného serveru. Zároveň je zablokováno čtení karty.

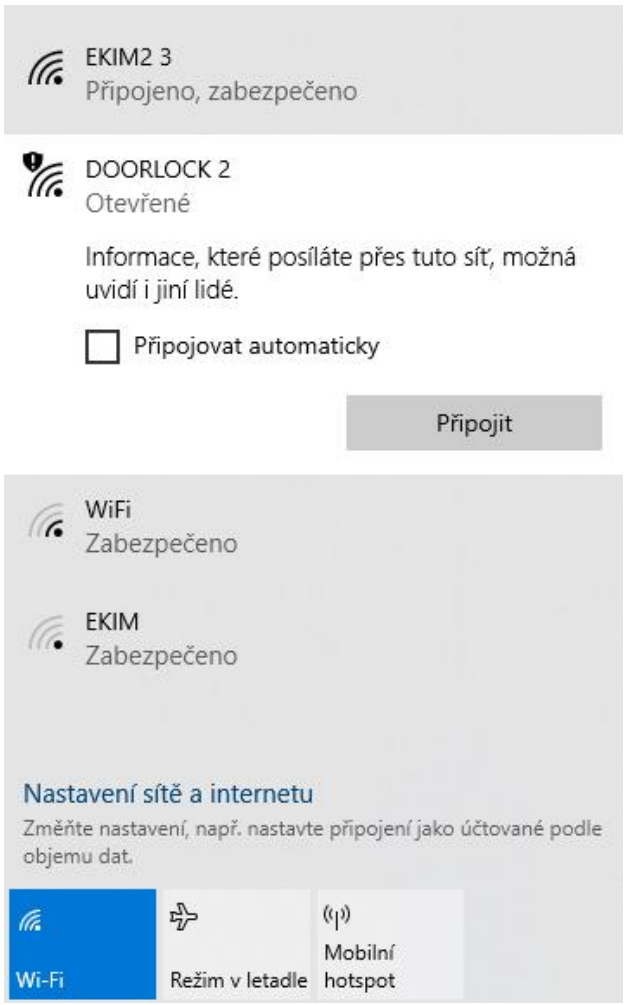
Dále je spravován server na přístupovém bodu, který je kontrolován pomocí specializované knihovny WebServer. Knihovna čeká na uživatelské akce a adekvátně na ně reaguje.

Smyčka vyčkává do přihlášení k místní síti pomocí uživatelského vstupu. Dokud není řídicí jednotka připojena k místní síti, nereaguje na výstup čtecího zařízení. Pokud je řídicí jednotka přihlášena, informuje o tom uživatele zeleně rozsvícenou LED. V opačném případě, kdy by řídicí jednotka měla být přihlášena k Wi-Fi, ale není, informuje o tom uživatele červenou LED a bude se opětovně pokoušet přihlásit k naposledy nastavené Wi-Fi.

Pokud se na čtecím zařízení objeví nová karta, je z dat získán unikátní identifikátor, pomocí kterého se ptáme na server s uživatelskými daty. Pokud tělo stránky obsahuje znak “1”, přístup je povolen. V opačném případě, pokud se nikde v těle stránky nevyskytuje znak “1”, přístup je odepřen.

4.3 WEBSERVER NA PŘÍSTUPOVÉM BODĚ

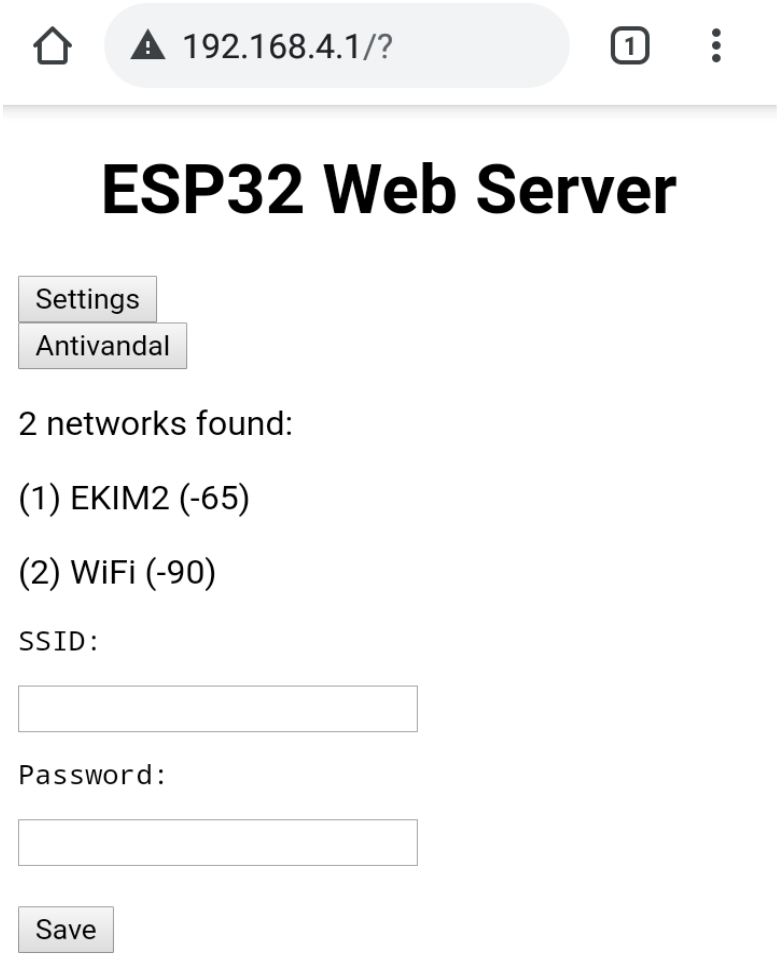
Pomocí web serveru na přístupovém bodě můžeme kontrolovat vnitřní data řídicí jednotky. Řídicí jednotka pro přístupový bod vytváří pokaždé stejné IP 192.168.4.1. Pokud se pomocí zařízení s přístupem na internet přihlásíme na tento přístupový bod, můžeme tuto IP adresu zadat do internetového prohlížeče. Daný server je vytvořen pomocí knihovny WebServer (WebServer, 2021).



Obrázek 4.2 – DOORLOCK v nabídce Wi-Fi

Na adrese „192.168.4.1“ se nachází hlavní stránka webového serveru. Jsou zde nabídnuta dvě pole pro vyplnění, jedno pro SSID dané sítě a druhé pro heslo. Uživateli jsou také poskytnuté informace o tom, které sítě může řídicí jednotka najít a jakou sílu daný signál má.

Na adrese „192.168.4.1/settings“ se nachází nastavení řídicí jednotky pro uživatele. Uživatel zde může nastavit IP serveru, na který se bude řídicí jednotka dotazovat nebo nastavit heslo pro přístupový bod. Změna hesla způsobí restart přístupového bodu.



Obrázek 4.3 – stránka pro vkládání hodnot Wi-Fi sítě

Na adrese „192.168.4.1/antivandal“ se nachází možnost aktivovat nebo deaktivovat antivandal systém, což nám umožní otevřít tělo přístupového systému pro jeho správu. Otevření těla je uloženo do záznamové databáze, není však bráno jako varování.

4.4 WI-FI PŘIHLÁŠENÍ

Po zadání SSID a hesla je řídicí jednotka připojena na internet a následně operuje s tím, že by měla být přihlášena k Wi-Fi. Přihlášení k Wi-Fi není vždy okamžité, může se tak stát, že kdybychom zadali špatné hodnoty, program by se zasekl do nekonečné smyčky. Přihlášení k Wi-Fi je tak omezeno na 15 vteřin. Pokud nedošlo k přihlášení do té doby, je pokus zrušen. Uživatel může po neúspěšném pokusu zadat hodnoty znova.

Pokud řídicí jednotka nemá žádný Wi-Fi signál, přestože by měla být připojena k síti, dochází tak k nekonečnému pokusu o opětovné připojení. Pokusy o připojení se střídají se správou serveru a nedojde tak ke znecitlivění webové serveru na přístupovém bodu.

4.5 KOMUNIKACE POMOCÍ KNIHOVEN MFRC522 A SPI

Na začátku programu musíme zahrnout knihovny MFRC522 a SPI, definovat piny ESP32, které budou připojeny ke čtecímu zařízení a vytvořit instanci MFRC522 objektu (MFRC522, 2021) (SPI, 2021).

```
#include <SPI.h>
#include <MFRC522.h>

#define RST_PIN 22
#define SS_PIN   5

MFRC522 mfrc522(SS_PIN, RST_PIN);
```

Obrázek 4.4 – Vytvoření MFRC522 čtecího objektu

Dále musíme v části setup inicializovat sériovou komunikaci a MFRC522. PCD znamená proximity coupling device (bezdotykové spojovací zařízení).

```
SPI.begin();
mfrc522.PCD_Init();
```

Obrázek 4.5 – Inicializace komunikace

V části loop musíme zjistit, jestli je v blízkosti čtecího zařízení transpondér a zvolit jednu z daných karet ke čtení. Pokud karta není v blízkosti, ukončíme danou smyčku a započneme novou (MFRC522, 2021).

```
if (!mfrc522.PICC_IsNewCardPresent())
{
  return;
}

if(!mfrc522.PICC_ReadCardSerial())
{
  return;
}
```

Obrázek 4.6 – Zjišťováni přítomnosti karty

Pokud byla karta v blízkosti a byla zvolena pomocí funkce, uloží se její informace do proměnné mfrc522, ze které pak můžeme pomocí funkce GetUID získat unikátní identifikátor ze zaslaných dat vnitřní paměti transpondéru.

4.6 ZÍSKÁNÍ UID RFID TRANSPONDÉRU

Získání unikátního identifikátoru z paměti karty není složité. Z pole hodnot UID je získána číselná hodnota, kterou můžeme následně přeložit na hexadecimální řetězec. Používáme posunutí bitů doleva pro zachování jejich hodnoty v celém řetězci. Pokud by nebyly upraveny, jejich hodnoty by byly o několik řádů menší a výsledný unikátní identifikátor by měl špatnou hodnotu (MFRC522, 2021).

```
unsigned long GetUID()
{
  unsigned long hex;
  hex  = mfrc522.uid.uidByte[0] << 24;
  hex += mfrc522.uid.uidByte[1] << 16;
  hex += mfrc522.uid.uidByte[2] <<  8;
  hex += mfrc522.uid.uidByte[3];

  return hex;
}
```

Obrázek 4.7 – Získání unikátního identifikátoru

4.7 DOTAZOVÁNÍ NA SERVER

Dotazování na server není složité. Využíváme HTTPClient knihovnu, pomocí které můžeme zasílat dotazy na dané webové servery. Vstupem do funkce je unikátní identifikátor karty (MCEWEN, 2015).

```
String GetResponseFromServer(unsigned long uid)
{
  if(databaseIP == NULL)
  {
    return "error";
  }

  String page = "http://" + databaseIP + "/check_access.php?card_tag=" + String(uid, HEX) + "&door_tag=" + door_tag;
  client.begin(page);
  int httpCode = client.GET();

  if(httpCode > 0)
  {
    String payload = client.getString();
    Serial.println(payload);
    return payload;
  }
  else
  {
    Serial.println("Error on HTTP request");
    return "error";
  }
}
```

Obrázek 4.8 – Komunikace s autorizačním serverem

Pokud nemáme nastavenou hodnotu IP daného serveru, dotázání je zrušeno. Dále je vytvořen řetězec pomocí daného IP, hodnoty unikátního identifikátoru karty jako hexadecimálního řetězce a identifikátorů dveří, uložené ve vnitřní paměti.

Pokud je odpověď serveru větší než 0, je navrácena hodnota těla, pomocí které se rozhodujeme o přístupu. Pokud je hodnota menší nebo rovna 0, je navrácena hodnota “error” a přístup je automaticky zamítnut. Daná hodnota mohla nastat z důvodů výpadku sítě nebo selhání serveru.

4.8 ROZHODOVÁNÍ O PŘÍSTUPU

Program z navrácené hodnoty řetězce těla rozhoduje o otevření dveřního zámku. Pokud řetězec obsahuje znak “1” na jakékoliv pozici, jsou dveře otevřeny. Může nastat situace, kdy server navrátí také řetězec se znaky “0”, protože karta a řídicí jednotka může být propojena na různá časová omezení, která neodpovídají aktuálnímu času.

```
uid = GetUID();
if (uid != -1) // GetUID returns -1 if the card could not be read
{
  String response = GetResponseFromServer(uid);
  if (response.indexOf("1") >= 0)
  {
    digitalWrite(ACCESS_YES, HIGH);
    digitalWrite(ACCESS_NO, LOW);

    digitalWrite(OPEN_DOOR, HIGH);
  }
  else
  {
    digitalWrite(ACCESS_YES, LOW);
    digitalWrite(ACCESS_NO, HIGH);
  }
```

Obrázek 4.9 – Rozhodování o přístupu

5 SERVER

Přístupový systém pro správu uživatelských RFID transpondérů je napsán v jazyce PHP. Webový server také musí podporovat MySQL k čemuž je využito vývojové prostředí WAMP (Windows, Apache, MySQL, PHP).

Webový server obsahuje hlavní stránku, na kterém je uživateli vypsána databáze se záznamy změn a pokusů o přístup a možnost zobrazit další databáze. První databáze je cards, která uchovává hodnoty unikátního identifikátoru a jména zaměstnance. Další databáze je doors, která obsahuje identifikátory a popis řídicích jednotek. Poslední databáze je relations, která obsahuje vztahy mezi transpondéry a řídicími jednotkami společně s časovým omezením.

5.1 KONTROLA PŘÍSTUPU

Pro kontrolu přístupu je využit soubor check_access. Nejprve musíme získat přístup do dané databáze, který získáme pomocí funkce mysqli_connect. Vstupními hodnotami dané funkce jsou název serveru, uživatelské jméno, heslo a název databáze (PHP Notes for Professionals, 2019).

```php
<?php
        $dbServername = "localhost";
        $dbUsername = "root";
        $dbPassword = "";
        $dbName = "door_master";

        $conn = mysqli_connect($dbServername, $dbUsername, $dbPassword, $dbName);
?>
```

Obrázek 5.1 – Komunikace s databází

Následně z databází cards a doors jsou získány sériové hodnoty v závislosti na datech, které zasíláme na tento server z řídicí jednotky. Proměnné card_tag a door_tag jsou získány z URL. Využíváme funkci mysqli_query, jejíž vstupními hodnotami je připojená databáze a text kódu, který se má provést (PHP Notes for Professionals, 2019).

```php
$card_tag = $_GET['card_tag'];
$sql = "SELECT serial FROM cards WHERE tag = '$card_tag' AND active = true";
$result_card = mysqli_query($conn, $sql);

$door_tag = $_GET['door_tag'];
$sql = "SELECT serial FROM doors WHERE door_tag = '$door_tag' AND active = true";
$result_door = mysqli_query($conn, $sql);
```

Obrázek 5.2 – Získání dat z databáze podle zaslaných identifikátorů

Ze zadaných databází je následně získáno sériové číslo daných prvků databáze. Sériové číslo využíváme jako cizí klíč v databází vazeb, podle kterých následně můžeme najít veškeré vazby obsahující tyto hodnoty. Pokud je jedna z těchto výsledných databází prázdná, je navrácena hodnota “0”.

```
$id_card = mysqli_fetch_assoc($result_card)['serial'];
$id_door = mysqli_fetch_assoc($result_door)['serial'];
$sql = "SELECT * FROM relations WHERE card_id = '$id_card' AND door_id = '$id_door' AND active = true";
$result = mysqli_query($conn, $sql);
```

Obrázek 5.3 – Získání prvků z databáze vazeb

Zde opět platí, že pokud je množství vrácených řádků nulové, je zpět okamžitě poslána hodnota “0”. Vyplývá z toho totiž, že mezi zadanou kartou a řídicí jednotkou neexistuje žádná vazba, která by zároveň byla aktivní. Funkce mysqli_fetch_assoc nám z řádku databáze navrátí hodnotu daného sloupce (PHP Notes for Professionals, 2019).

```
if(!mysqli_num_rows($result_card) > 0)
{
        $sql = "INSERT INTO logs (day_date, description) VALUES (CURRENT_TIMESTAMP(),
                'Access denied, no card with tag $card_tag in the database!');";
        mysqli_query($conn, $sql);
        echo "0";
}
else if(!mysqli_num_rows($result_door) > 0)
{
        $sql = "INSERT INTO logs (day_date, description) VALUES (CURRENT_TIMESTAMP(),
                'Access denied, no door with tag $door_tag in the database!');";
        mysqli_query($conn, $sql);
        echo "0";
}
else if(!mysqli_num_rows($result) > 0)
{
        $sql = "INSERT INTO logs (day_date, description) VALUES (CURRENT_TIMESTAMP(),
                'Access denied, no relationship between card $card_tag and door $door_tag!');";
        mysqli_query($conn, $sql);
        echo "0";
}
```

Obrázek 5.4 – Prvotní porovnání výstupů

Nyní musíme zkontrolovat každou vazbu, která nám byla navrácena a jestli alespoň jedna z nich splňuje časové podmínky.

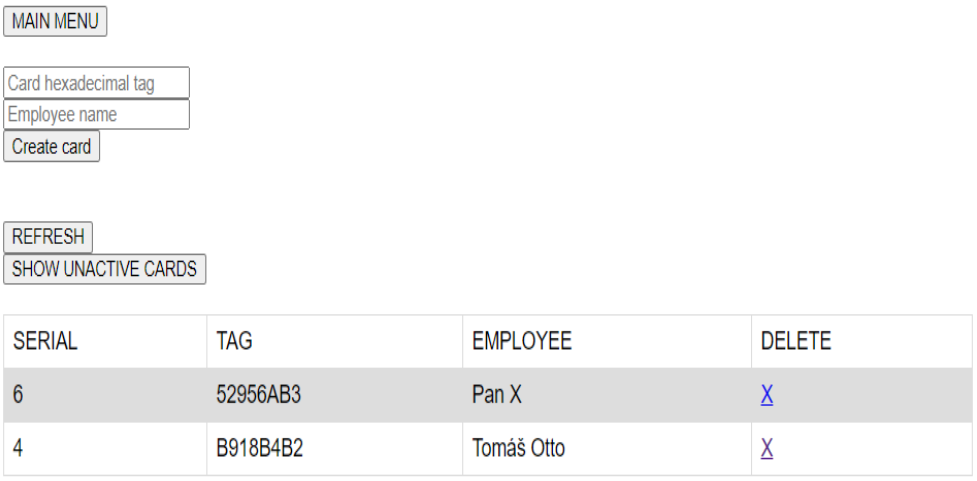
První větvení je závislé na splnění časového omezení. Aktuální čas dne musí být větší než hodnota start_at a zároveň musí být menší než hodnota end_at. Časová hodnota musí být upravena na místní časové pásmo. Další větvení kontroluje aktuální den týdne a kontroluje, jestli daný řádek databáze obsahuje hodnotu “1” ve sloupci reprezentující daný den. Větvení pro kontrolu dne je celkově 7, pro každý den v týdnu.

```
while($row = mysqli_fetch_assoc($result))
{
        if(date('H:i', time()) > $row['start_at'] && date('H:i', time()) < $row['end_at'])
        {
                if(date("D") == "Mon" && $row['monday'] == 1)
                {
                        $sql = "INSERT INTO logs (day_date, description) VALUES (CURRENT_TIMESTAMP(),
                                'Access granted to card $card_tag at door $door_tag');";
                        mysqli_query($conn, $sql);
                        echo "1";
                }
                else if(date("D") == "Tue" && $row['tuesday'] == 1)
                {
                        $sql = "INSERT INTO logs (day_date, description) VALUES (CURRENT_TIMESTAMP(),
                                'Access granted to card $card_tag at door $door_tag');";
                        mysqli_query($conn, $sql);
                        echo "1";
                }
                //
                //
                //
                //
                else
                {
                        echo "0";
                }
        }
        else
        {
                echo "0";
        }
```

Obrázek 5.5 – Porovnání časových omezení

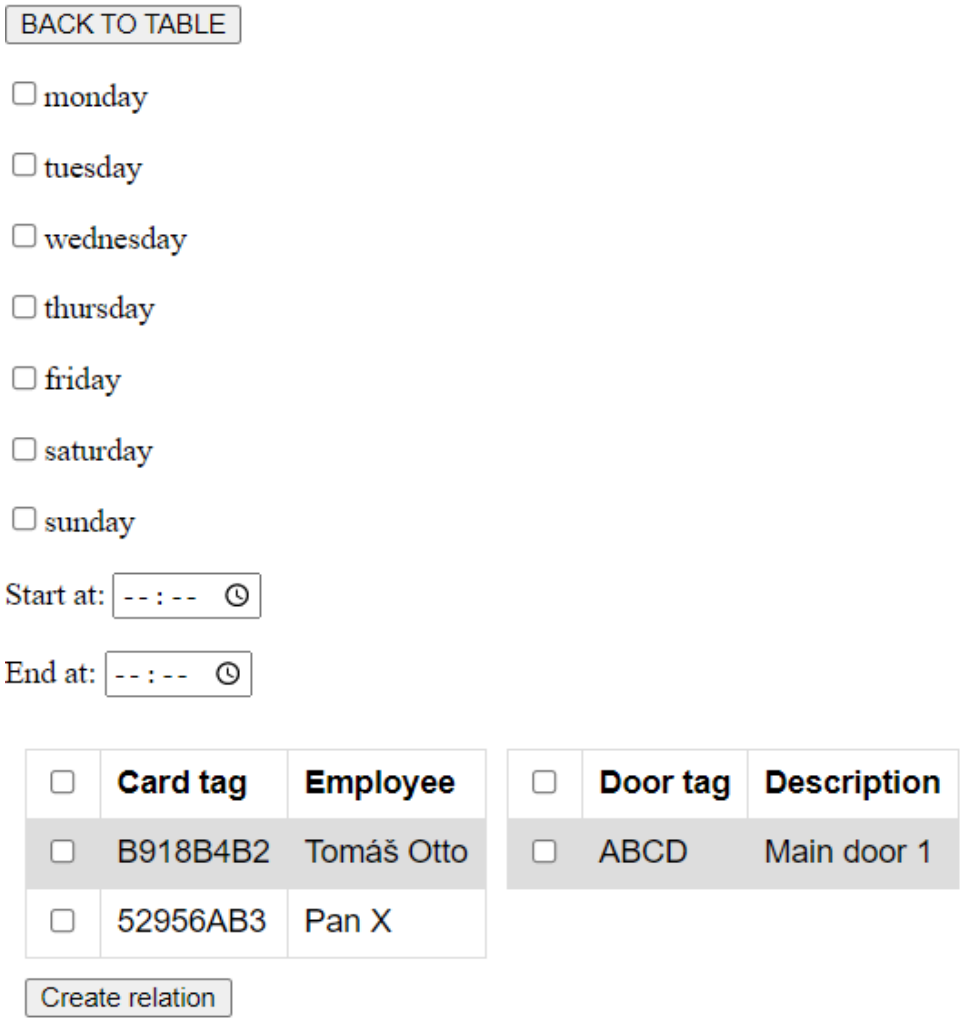
5.2 TVORBA A MAZÁNÍ HODNOT

V případě karet a řídicích jednotek je tvorba hodnot jednodušší. Uživatel zadá požadované hodnoty do vstupního pole a vytvoří danou hodnotu pomocí tlačítkového prvku. Podmínkami tvorby je unikátnost dveřních nebo RFID identifikátorů. V případě, že uživatel zadá stejnou hodnotu znovu, prvek není přidán. Není totiž povoleno, aby jednu kartu vlastnilo více osob, nebo aby dvě řídicí jednotky měly stejný identifikátor. Zamezuje se tak konfliktům při přístupu.



Obrázek 5.6 – Přidání a mazání karet

Hodnota z této databáze nemůže být skutečně nikdy smazána pomocí daného webového serveru. Funkce “DELETE” pouze deaktivuje danou kartu, ale daný řádek bude v databázi zachován. Nebude se s daným prvkem pracovat při kontrole přístupu a není na něj dbáno, pokud vytváříme řádek se stejnou hodnotou karty. Hodnoty nejsou mazány z administrativních a bezpečnostních důvodů.



Obrázek 5.7 – Přidání nové vazby

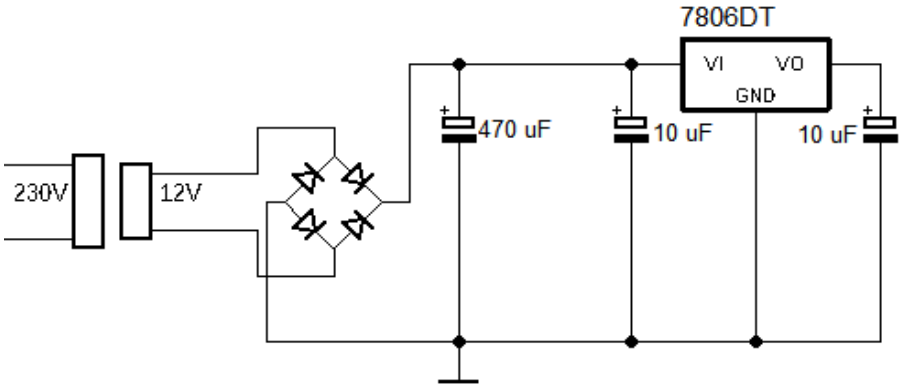
Uživatel zde může nastavit, které karty a řídicí jednotky mezi sebou budou propojeny. Může zde také nastavit, ve které dny toto spojení bude platit (např. pouze na pracovní týden) a také na čas dne (např. pouze na pracovní dobu). Podmínkou je, že hodnota start_at je menší než end_at. Pro každou zvolenou kartu a pro každou zvolenou řídicí jednotku je vytvořen vlastní řádek v databázi vazeb. Uživatel tak může vytvořit několik karet se stejným časovým omezením najednou bez nutnosti vytvářet každou vazbu zvlášť.

6 FYZICKÉ ZAPOJENÍ

6.1 NAPÁJENÍ

Zařízení je napájeno z elektrické sítě. Musíme tak změnit 230 V střídavého napětí na 3,3 V stejnosměrného napětí. Musíme taky dodávat 12 V stejnosměrného napětí na elektrický zámek. Využijeme tak transformátor, pomocí kterého změníme 230 V AC na 12 V AC. Na výstupu sekundární cívky využijeme Graetzův můstek pro usměrnění tohoto střídavého napětí. Za tímto můstkem se nachází polarizovaný kondenzátor pro omezení stavu, kdy napětí prochází nulou. Vytvořili jsme tak zhruba 12 V stejnosměrného napětí.

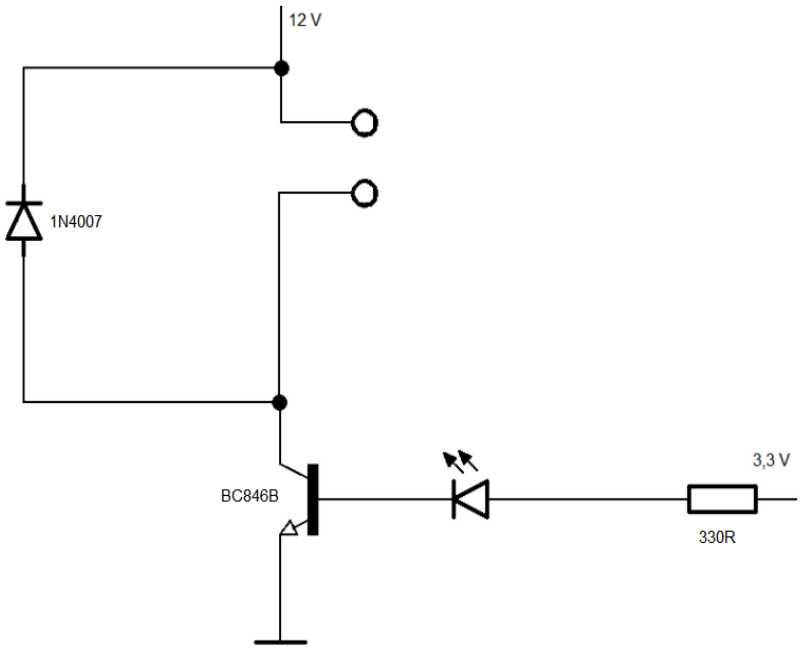
Za kondenzátorem C1 se nachází stabilizátor napětí, jehož výstup je stabilních 3,3 V bez závislosti na velikosti vstupního napětí. Dané napětí pak přivádíme na řídicí jednotku, čtecí zařízení a na vstup magnetického přepínače, který využíváme jako antivandal systém.



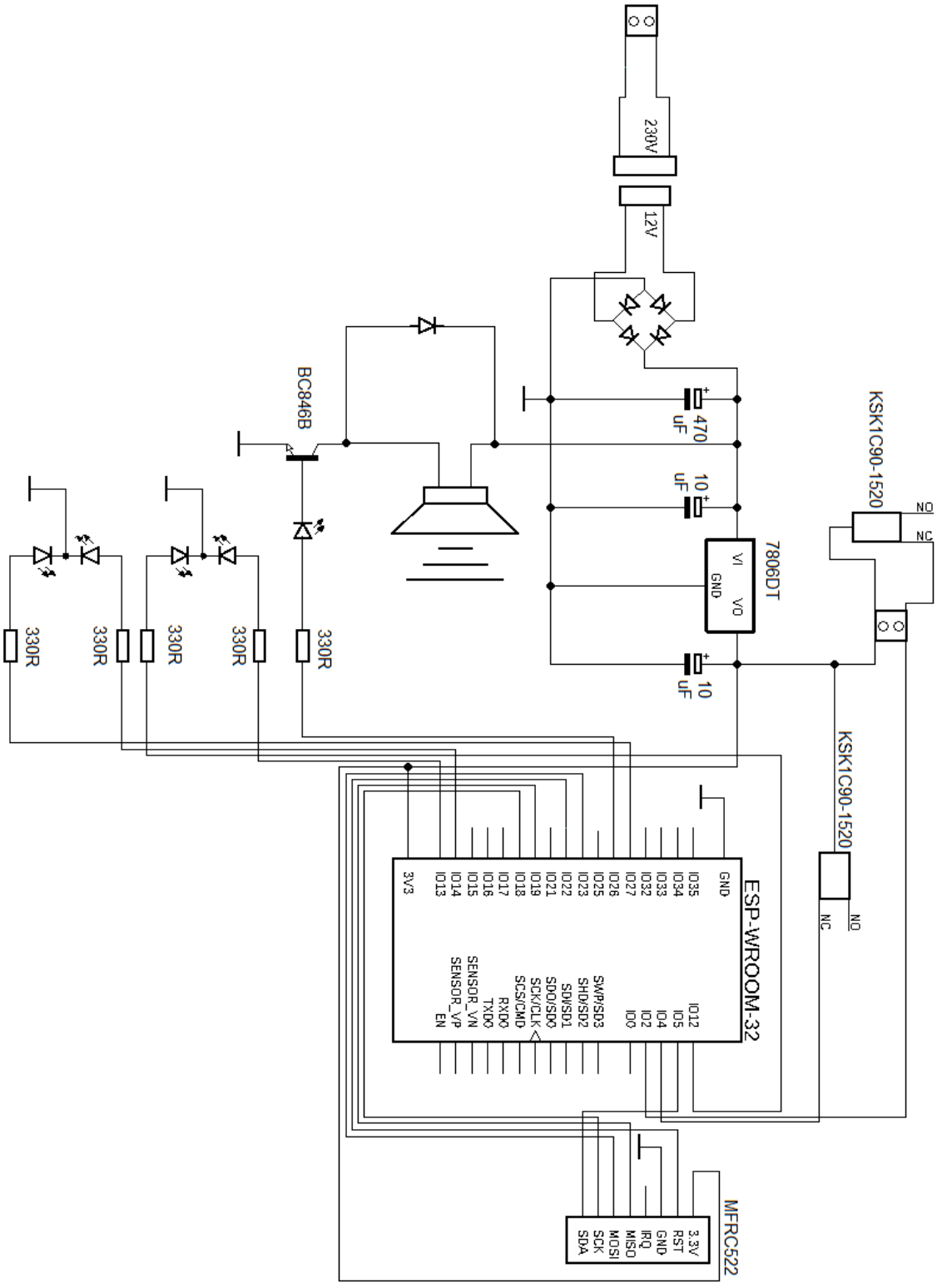
Obrázek 6.1 – Schéma zdroje napětí

6.2 ELEKTRONICKÝ ZÁMEK

Elektronický zámek funguje na 12 V stejnosměrného napětí. Proud je řízen unipolárním tranzistorem, jehož báze je připojena na pin řídicí jednotky. Dioda v opačném směru napětí se zde nachází z důvodů eliminace napěťové špičky. 12 V pro napájení elektronického zámku získáme za prvním tranzistorem zdroje napětí.



Obrázek 6.2 – Schéma elektronického zámku



Obrázek 6.3 – Schéma zařízení

7 ZÁVĚR

Cíle práce byly úspěšně splněny a zařízení pracuje dle zadaných požadavků. Práce poskytuje snadné propojení mezi zámkovým systémem a internetovým serverem, které se může využít v celé řadě oblastí.

Práce může být pro zvýšení bezpečnosti zajištěna dvoustupňovým přístupovým systémem, kde se pro ověření vstupu využívají dvě formy zabezpečení.

POUŽITÁ LITERATURA

Access control. Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001, 2021 [cit. 2021-5-06]. Dostupné z: https://en.wikipedia.org/wiki/Access_control

DAS, R. RFID Frequency bands [online]. IDTechEx, 2006 [cit. 2021-5-6]. Dostupné z: https://www.idtechex.com/fr/research-article/rfid-frequency-bands/40

Elektrický otvírač BeFo Klasik. [online]. 4lock [Cit. 2021-04-15]. Dostupné z: https://4lock.cz/elektricky-otvirac-befo-klasik-antivandal-standardni-5-12v-ac-dc-511

ESP32–WROOM32: Datasheet [online]. Espressif Systems, 2021 [cit. 2021-5-6]. Dostupné z: https://www.espressif.com/sites/default/files/documentation/esp32-wroom-32_datasheet_en.pdf

ESPRESSIF. Wi-Fi. Espressif [online]. Espressif Systems, ©2016-2021 [cit. 2021-05-06]. Dostupné z: https://docs.espressif.com/projects/esp-idf/en/latest/esp32/api-reference/network/esp_wifi.html

GoalKicker. PHP Notes for Professionals. [online] GoalKicker. 2019. [Cit. 2021-04-12]. Dostupné z: https://books.goalkicker.com/PHPBook/

Lock and key. Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001, 2021 [cit. 2021-5-6]. Dostupné z: https://en.wikipedia.org/wiki/Lock_and_key

MCEWEN Adrian. HttpClient. GitHub [online]. GitHub. 2015 [Cit. 2021-04-08]. Dostupné z: https://github.com/amcewen/HttpClient

MFRC522 [online]. NXP Semiconductors, 2016 [cit. 2021-5-6]. Dostupné z: https://www.nxp.com/docs/en/data-sheet/MFRC522.pdf

MFRC522, Arduino [online]. 2021 [Cit. 2021-04-08] Dostupné z: https://www.arduino.cc/reference/en/libraries/mfrc522/

Modul RFID-RC522 13,56MHz s klíčenkou a kartou. [online] Hadex [Cit. 2021-04-15]. Dostupné z: https://www.hadex.cz/m490-modul-rfid-rc522-1356mhz-s-klicenkou-a-kartou/

OPRŠAL, Daniel. Zámek dveří s ověřením přes LAN, Bakalářská práce, Pardubice, 2019, Univerzita Pardubice.

PETERSEN, T. RFID CARD SECURITY AND ATTACKS [online]. Sikich LLP, 2020 [cit. 2021-5-6]. Dostupné z: https://www.sikich.com/insight/rfid-card-security-attacks-and-prevention/

Reed Contact SPDT 0,25A 3W AW15-20. [online] Elektronik Lavpris [Cit. 2021-04-15]. Dostupné z: https://elektronik-lavpris.dk/p88837/ksk1c90-1520-reed-contact-spdt-025a-3w-aw15-20/

RFID. Wikipedia: the free encyclopedia [online]. San Francisco: Wikimedia Foundation, 2001, 2021 [cit. 2021-05-06]. Dostupné z: https://en.wikipedia.org/wiki/Radio-frequency_identification

SPI, Arduino [online]. 2019 [Cit. 2021-04-08]. Dostupné z: https://www.arduino.cc/en/reference/SPI

WebServer, Arduino [online]. 2021 [Cit. 2021-04-08] Dostupné z: https://github.com/espressif/arduino-esp32/tree/master/libraries/WebServer

PŘÍLOHY

Příloha A – CD

Příloha A

Příloha k bakalářské práci

Elektronický přístupový systém

Tomáš Otto

CD

OBSAH

1. Text bakalářské práce ve formátu PDF
2. Úplný zdrojový kód programu pro ESP32-WROOM-32
3. Úplný zdrojový kód pro přístupový server
4. Schéma zapojení a návrh desky plošného spoje