VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

BAKALÁŘSKÁ PRÁCE

Brno, 2020 Prokop Tkadlec

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV AUTOMATIZACE A MĚŘICÍ TECHNIKY
DEPARTMENT OF CONTROL AND INSTRUMENTATION

ELEKTROMECHANICKÝ ZÁMEK DVEŘÍ S BIOMETRICKOU ČTEČKOU A NFC
ELECTROMECHANICAL DOOR LOCK WITH BIOMETRIC READER AND NFC

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **Prokop Tkadlec**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Tomáš Benešl**
SUPERVISOR

BRNO 2020

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní program **Automatizační a měřicí technika**

Ústav automatizace a měřicí techniky

Student: Prokop Tkadlec ***ID:*** 205846

Ročník: 3 ***Akademický rok:*** 2019/20

NÁZEV TÉMATU:

Elektromechanický zámek dveří s biometrickou čtečkou a NFC

POKYNY PRO VYPRACOVÁNÍ:

Cílem práce je vytvořit prototyp elektromechanického zámku využívající technologii NFC a biometrii, s možností zabudování do stávajících dveří.

1. Seznamte se s komerčními technologiemi pro zabezpečení vstupu
2. Navrhněte elektromechanickou koncepci systému
3. Navrhněte softwarové vybavení řídicího systému
4. Implementujte a demonstrujte funkčnost
5. Diskutujte dosažené výsledky a zhodnoťte úroveň zabezpečení

DOPORUČENÁ LITERATURA:

Cyber security: analytics, technology and automation, 2015. New York, NY: Springer Berlin Heidelberg. ISBN 978-3319183015.

Termín zadání: 3.2.2020 ***Termín odevzdání:*** 8.6.2020

Vedoucí práce: Ing. Tomáš Benešl

doc. Ing. Václav Jirsík, CSc.
předseda rady studijního programu

ABSTRAKT

Cílem této práce je sestavení prototypu elektromechanického zámku, který bude ovládán za pomocí biometrické složky a NFC. V bakalářské práci jsou představeny a popsány jednotlivé součásti celého prototypu. V další části je ukázán návrh softwarového a hardwarového řešení problému a jeho implementace do připravené fyzické konfigurace. Vytvořený prototyp umožňuje autentizaci uložených otisků prstů a karet, které podporují normu ISO/IEC 15693. Zadání a uložení autorizovaných otisků a karet je možné skrze sériovou komunikaci.

KLÍČOVÁ SLOVA

Elektromechanický zámek, Biometrická čtečka, NFC, zámek, ESP32, Esp-Idf,

ABSTRACT

The aim of this thesis is to prototype an electromechanical lock, that will be controlled by a biometric reader and NFC. In this bachelor's thesis all the individual components of designed prototype are presented and described. The next chapter presents selected software and hardware solutions and their implementation into the prepared physical configuration. The designed prototype enables the authentication of stored fingerprints and cards that support the ISO/IEC 15693 standard. Insertion and saving of authorized fingerprints and cards is possible via serial communication.

KEYWORDS

Electromechanical lock, Biometric scanner, NFC, lock, ESP32, Esp-Idf

TKADLEC, Prokop. *Elektromechanický zámek dveří s biometrickou čtečkou a NFC*. Brno, 2020, 49 s. Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav automatizace a měřicí techniky. Vedoucí práce: Ing. Tomáš Benešl

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Elektromechanický zámek dveří s biometrickou čtečkou a NFC“ jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno 8.6.2020 .....

podpis autora

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu diplomové práce panu Ing. Tomáši Benešlovi za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Obsah

Seznam obrázků

Seznam tabulek

Seznam výpisů

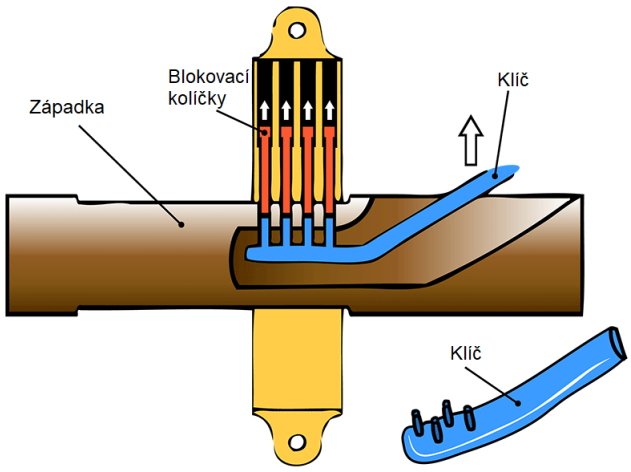
Úvod

S bezpečnostními prvky, které zamezují vstupu do oblastí neoprávněným osobám, se setkáváme již od narození. V dnešní době se stále častěji místo klasických mechanických zámků setkáváme s těmi elektrifikovanými. A proto se tato práce zabývá vytvořením návrhu a následné realizace zabezpečení vstupu s použitím elektromechanického zámku. Cílem je vytvořit vhodné seskupení součástí pro bezproblémovou funkčnost elektromechanického dveřního zámku, který pro své ovládání bude využívat biometrickou složku a komunikaci pomocí NFC-(Near Field Communication).

V této bakalářské práci budou čtenáři seznámeni s jednotlivými částmi navrhovaného zabezpečovacího systému a jeho následné implementace. Možností využití technologií biometrického údaje a NFC k prokázání identity. Kromě popisu dílčích částí bude čtenář krátce seznámen s aktuálními českými normami pro elektromechanické dveřní zámky a možnost fungování jako nouzový nebo panikový východ. Dále budou popsány původní návrhy a to jak hardwarové tak softwarové části. V posledních kapitolách je popsán výsledný způsob implementace a zhodnocení dosažených výsledků zabezpečení.

1 Zabezpečení vstupu

Už od starověku můžeme sledovat snahu člověka ochránit osobní vlastnictví pomocí zámku. Do dnešních dob se toho moc nezměnilo, pořád se snažíme omezit přístup a ochránit tak naše soukromé věci před cizími lidmi. Nejpoužívanějším a velice bezpečným byl a stále je zámek. První snahy o ochranu majetku na principu zámku se objevily již ve starém Egyptě a Mezopotámii 1.1. Vyráběly se z běžně používaných materiálů jako je například dřevo. V dalších letech nezaznamenáme žádný velký skok v bezpečnosti a zámky pouze střídají materiály a zvětšují se.[2, 3]

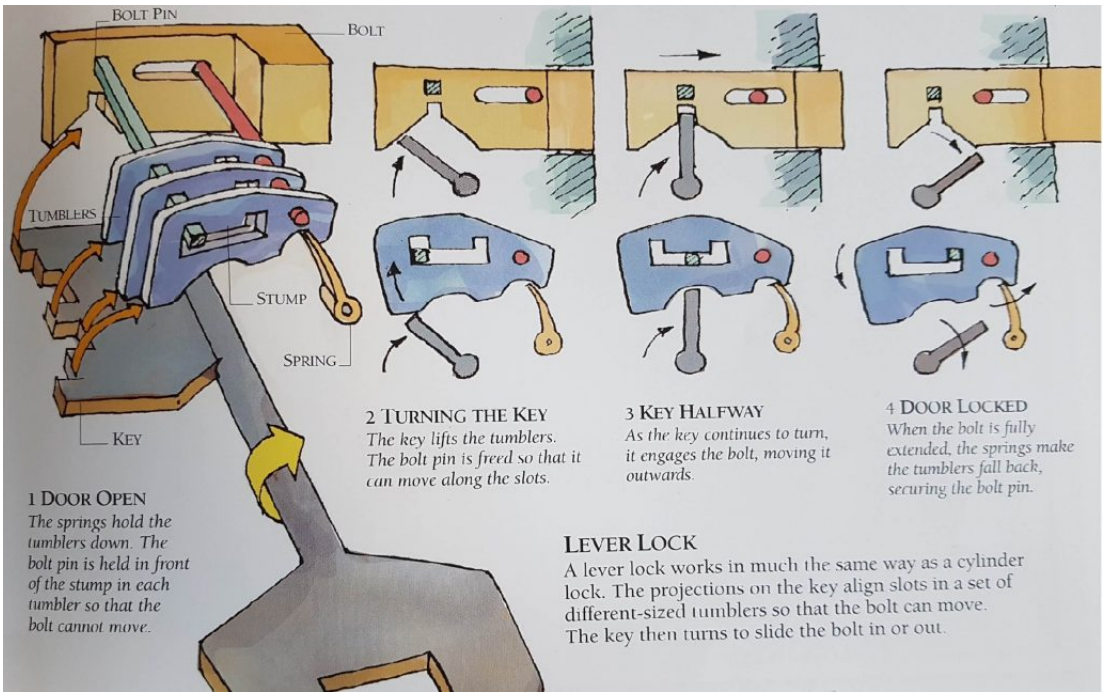


Obr. 1.1: Egyptský dřevěný zámek.

První větší technický porkrok můžeme sledovat až v roce 1778, kdy zámečník Rober Barron patentoval dvojčinný západkový zámek 1.2. Který byl jednoduchý na výrobu, levný a měl velkou variaci klíčů. Tento typ zámku byl dále vylepšován a na jeho obdobném principu se používají některé jednoduché zámky dodnes.[3, 1]

Poslední velký technický pokrok v zabezpečení a konstrukci zámku přišel roku 1844. Pan Linus Yale Sr. patentoval si "čtyřnásobný"bankovní zámek. Kde byly poprvé použity válcové stavítka a otočné jádro. Roku 1865 jeho sy Linus Yale Jr. patentoval zámek který dal základ dnešním cylindrickým vložkám 1.4. Oproti otci dal stavítka do jedné roviny což umožnilo zámek zmenšit a vsadit ho do klasických dveří.[3, 4]

V dnešním světě používáme zámky i v elektronickém světě, kde své soubory zamykáme a vytváříme k nim stále složitější a delší binární klíče.



Obr. 1.2: Ukázka funkce západkového zámku.

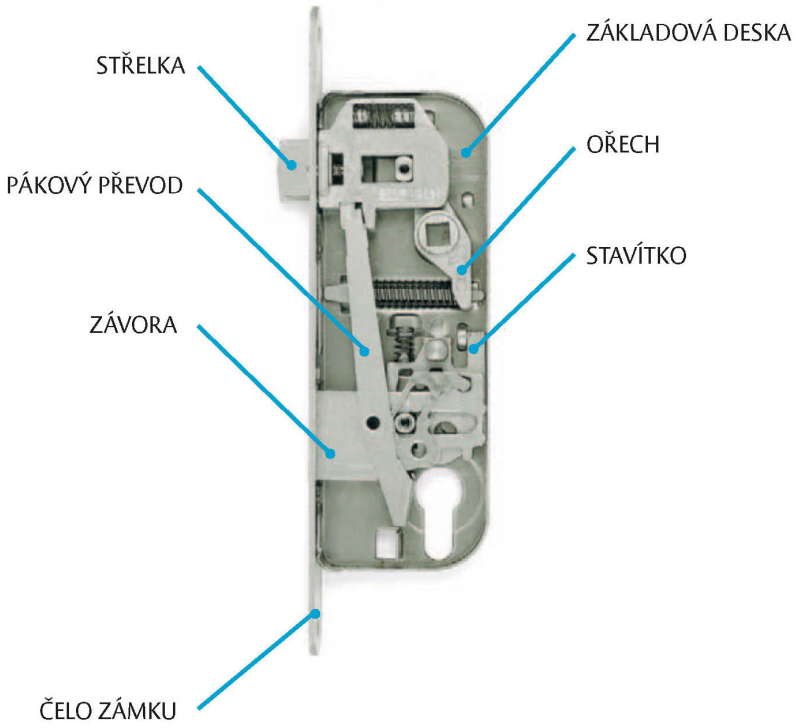
1.1 Druhy zámků

Zámky můžeme rozdělit do dvou skupin, mechanické a elektrické. Mechanické zámky známe již od dob starých egypťanů, zatím co ty elektrické jsou výsadou posledního půl století.

1.1.1 Mechanické zámky

S mechanickými zámky se můžeme v běžném světě setkat prakticky dennodenně a to jak v podobě klasického zámku u dveří, tak třeba zámku na kolo,zapalování v autě nebo tak formou visacího zámku. Dveřní mechanismy můžeme rozdělit podle typu otvírání na:[1]

- zástrčku - otevírá se ručně, posuvem ze strany na stranu, může sloužit jako doplněk k zámku či jako samostatné zabezpečení málo otvíraných prostor
- západku - otevírá se klikou, západka ,která je ovládaná klikou nebo v některých případech i klíčem udržuje dveře v zavřeném stavu v některých případech se můžeme setkat se střelkou
- závora - otevírá se pomocí klíče, jde o kovový kvádr(viz.1.3), který vlivem otáčení klíčem zajíždí do protiplechu umístěném naproti v dveřní zárubni. Závora má více poloh tzv. západů zpravidla dva.

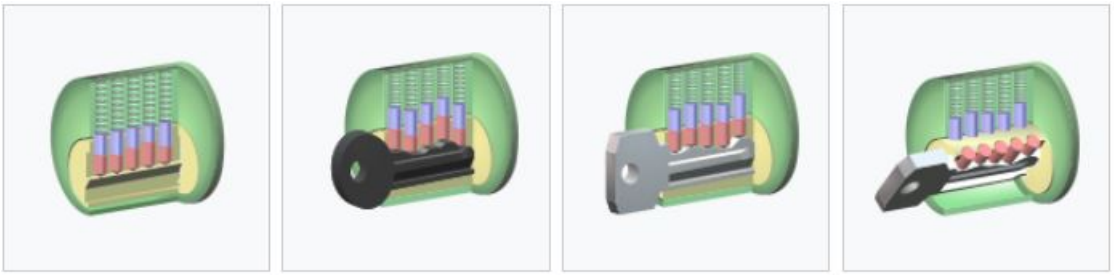


Obr. 1.3: Popis částí mechanického zámku

U dnešních zámků se až na výjimky výhradně setkáme s cylindrickou vložkou. Tento mechanismus je ve své podstatě jednoduchý, viz Obr. 1.4, uvnitř válcového jádra se nacházejí dvě řady různě dlouhých stavítek a blokovacích kolíků. Když je do zámku zasunut správný klíč, válečky se vyrovnají a je možné zámkem otočit, zároveň hrot klíče vysune spojku,která spojí vložku se zubem, který následným otáčením pohybuje se závorou a tím odemyká nebo zamyká. Pokud by se uvnitř nacházel špatně tvarovaný klíč, bude jeho otáčení bránit buďto stavítko nebo blokovací váleček. Dalším bezpečnostním prvkem je výřez, do kterého se klíč zasouvá, pokud drážky nesouhlasí s výřezem vložky, klíč do ní nestrčíme. [1, 4]

1.1.2 Elektrické zámky

Tyto zámky zažívají v poslední době velký boom. Díky moderním technologiím jako NFC, otiskům prstů či rozpoznávání obličeje a možnosti jejich připojení na kontrolér a následnou komunikaci se zámkem. Již se nemusíme omezovat na nutnost nosit u sebe fyzicky klíč, kterým bychom zámek otevřeli. Zjednodušuje se tak i možnost rychlého přidělení povolení pro vstup osobám do určitého oddělení. V současnosti rozlišujeme tři druhy: [1]



Obr. 1.4: V první části můžeme vidět vložku bez klíče, v další části je vložený špatný klíč, v předposlední části je vložen správný klíč a v poslední části můžeme vidět pootočení jádrem.

- Elektrický zámek - zámek ovládaný pouze elektrickým signálem
- Elektromotorický zámek - elektrický signál sepne motor, který otevře dveře
- Elektromechanický zámek - elektrický signál aktivuje vnější kliku

Elektrický zámek

Nejednoduší typ elektrického zámku, který se více objevuje pod názvem elektrický otvírač. Je tomu proto, že poskytuje minimální zabezpečení a žádnou výraznou ochranu proti jeho zničení. Dveře je možné otevřít po dobu kdy je přiveden elektrický signál. Tento typ se využívá hlavně u dveří s velkým počtem průchodů, běžně se používají pro oddělení pracoviš uvnitř podniků.

Obr. 1.5: Elektrický otevírač

Elektromotorický zámek

Tento typ zámků se skládá z klasického mechanického mechanismu a elektrického motoru, který ovládá závoru celého zámku. Díky tomu se dá zámek otevřít pouze vnitřní klikou, klíčem z obou stran přes klasickou vložku anebo zámek se také odemkne pokud dostane signál z kontroléru. Z vnější části dveří je namontována místo kliky koule, protože zámek se otevře pomocí motoru a stačí tak jen za dveře potáhnout.

Elektromechanický zámek

U tohoto typu se setkáváme také s mechanickou částí. Dveře vypadají na první pohled jako klasické, jelikož mají na obou stranách kliku. Jak název napovídá zámek již neobsahuje elektrický motor nýbrž pouze mechanismus, který spojuje hranol kliky se závorou. Vnější klika tudíž pracuje takzvaně naprázdno, dokud nedostane elektrický signál z kontroléru. Dveře lze také otevřít pomocí klíče přes vložku nebo vnitřní klikou, která funguje pořád.

2 Mechanická konstrukce nového zařízení nebo použití zařízení na trhu

2.1 Teoretická konstrukce

Konstrukce elektromechanického zámku se ve své podstatě liší od běžného mechanického zámku pouze děleným čtyřbokým hranolem. Oproti mechanickému zámku je nutné tedy zajistit, aby se vnější klikou dal po příchozím signálu zámek otevřít. Taková to funkce by mohla být řešena třeba posuvnou zarážkou v ořechu zámku, která by se po příchozím signálu vysunula do protější části a tím by se daly otevřít dveře.

2.2 Rozložení na trhu

Na českém trhu se v současnosti nacházejí dva velcí výrobci elektromechanických a elektromotorických zámku. A jsou to Assa Abloy a ERBI. Firma Assa Abloy vznikla roku 1994 sloučením dvou společností švédské Assa a finské Abloy. Od té doby je jedním z předních dodavatelů přístupových systémů a ESZ - (elektronické systémy zabezpečení). Společnost se dělí do tří regionálních divizí a dvou globálních. Nás zajímá divize EMEA, která vyrábí a prodává mechanické,elektromechanické a elektromotorické zámky, také vložky, bezpečnostní dveře a kování. Od roku 2008 spadá do divize i česká FAB, s.r.o.. Roku 1992 vznikla firma BERA, která si vybudovala svou pověst a značku na českém trhu a po sedmnácti letech byla začleněna do společnosti Assa Abloy. Začlenění však nenaplnilo očekávání původního majitele, který se proto rozhodl založit společnost ERBI a vybudovat si znovu své místo na trhu. Firma vyrábí mechanické a elektromechanické bezpečnostní a střelkové zámky, silové zámky a skříňkové. [15, 16]

2.3 Výběr zámku

Při výběru zámku jsem se musel rozhodnou zda vyrobím zámek vlastní nebo použiji již vyráběný produkt na trhu. Rozhodl jsem se použít jíž vyráběný zámek. Při výběru jsem se rozhodoval mezi firmami Assa Abloy a ERBI, kde jsem nakonec zvolil firmu ERBI pro její nižší cenu a výběr s dostatečně různých typů. Konkrétně jsem pak zvolil zámek s označením SAM EL B 7255. Jedná se o samozamykací zámek s funkcí Fail secure - Vnější klika je aktivní po přivedení proudu., bez zvukové signalizace. [16]

3 ČSN Normy

V následující kapitole popíšu české technické normy, které se zabývají určováním bezpečnosti a kvality elektromechanických zámků, panikových dveřních uzávěrů a nouzových dveřních uzávěrů.

3.1 Norma ČSN EN 14846

Požadavky a zkušební metody pro elektromechanicky ovládané zámky a zapadací plechy. Norma se zaměřuje na pevnost, bezpečnost životnost a funkčnost elektrických a elektronických součástí pro všechny typy elektromechanických zámků a zapadacích plechů.[20]

3.1.1 Požadavky

Mezi všeobecné požadavky patří absence nebezpečných látek anebo jejich uvolňování a nutnost otevírací doby na obou koncích nesmí přesáhnout 3s. Dále se kontroluje použití v zatížení jako jsou odolnost proti bočnímu zatížení střelky, moment síly pro ovládání neodpružené závory, pevnost pro běžnou činnost střelky a omezení, odolnost proti momentu síly na uzamykatelný ořech zámku.[20]
Životnost se dělí do tříd podle počtu cyklů, po kterých bude ještě zámek funkční:

Tab. 3.1: Požadavky na životnost zámku

Třída	Činnost střelky	Neodpružená závora ovládaná ručně	Neodpružená závora ovládaná automaticky	Neodpružená závora ovládaná elektricky
A,F	50 000	10 000	50 000	50 000
B,G,L,R,W	100 000	25 000	100 000	100 000
C,H,M,S,X	200 000	50 000	200 000	200 000

Pokud existuje zdvojená funkce (např. ruční ovládání zvenku a elektrické zevnitř) ,musí být pro ověření použity dva rozdílné zkušební vzorky.

Mezi další kritéria patří hmotnost dveří pro které se bude moci zámek použít, zavírací síla nutná pro zavření nebo také vhodnost pro použití v protipožárních či protikouřových dveřích. Kontroluje se také odolnost proti korozi, teplotě a vlhkosti. Na závěr se ověřují elektrické funkce, jako je ukazatel stavu (otevřeno, zamčeno, lze otevřít), nebo elektrická manipulace [20]:

- Ochrana proti poklesu napětí

- Ochrana proti účinkům přestřižených kabelů
- Ochrana proti účinkům manipulace s dráty
- Odolnost proti vyzařovanému elektromagnetickému poli
- Odolnost proti elektrostatickému výboji

3.1.2 Klasifikace

Rozdělujeme na devět znaků, kde každý znak charakterizovaný číslem nebo písmenem odpovídá testované vlastnosti.[20]

1. Kategorie použití
    - Třída 1: pro místa s velkou pečlivostí o udržování a malou šancí na nesprávné používání např. bytové dveře
    - Třída 2: pro místa s pečlivostí o udržování a možnou šancí nesprávného používání např. kancelářské dveře
    - Třída 3: pro místa s malou pečlivostí o udržování, vysokou šancí nesprávného používání např. veřejné vchody pozn. nutnost splnění pro panikové a nouzové únikové systémy
2. Životnost a zatížení střelky

Tab. 3.2: Rozdělení tříd podle počtu zvládnutých cyklů a zatížení střelky

Třída	Počet cyklů	Zatížení střelky
A	50 000	bez zatížení
B	100 000	bez zatížení
C	200 000	bez zatížení
F	50 000	10 N
G	100 000	10 N
H	200 000	10 N
L	100 000	25 N
M	200 000	25 N
R	100 000	50 N
S	200 000	50 N
W	100 000	120 N
X	200 000	120 N
Y	200 000	250 N

3. Hmotnost dveří a zavírací síla - rozdělení do sedmi tříd podle hmotnosti do 100kg,200kg a nad 200kg a podle zavírací síly 50,25 a 15 N.
4. Vhodnost použití pro protipožární/protikouřové dveře - rozděleno do sedmi tříd:

- 0 - nevhodné
- A - vhodné
- B - S klasifikační dobou od 15 min
- C - S klasifikační dobou od 30 min
- D - S klasifikační dobou od 60 min
- E - S klasifikační dobou od 90 min
- F - S klasifikační dobou od 120 min a výš

5. Bezpečnost při používání - bez požadavků pozn. nutné pro panikové a únikové dveřní systémy
6. Odolnost proti korozi,teplotě a vlhkosti - rozděleno do 15 tříd
7. Bezpečnost a odolnost proti odvrtání - Je rozdělena do tříd od 1 do 7, určuje se podle již neplatné normy
8. Bezpečnost elektrické funkce
    - Třída 0: bez požadavku
    - Třída 1: ukazatel stavu
9. Bezpečnost elektrické manipulace
    - Třída 0: bez ochrany
    - Třída 1: odolnost pouze proti elektrostatickému výboji
    - Třída 2: všechny ochrany a odolnosti kromě manipulace s dráty
    - Třída 3: kompletní ochrany a odolnosti

3.2 ČSN EN 179

Norma definuje požadavky a zkušební metody pro nouzové dveřní uzávěry ovládané klikou nebo zařízením s tlačnou plochou.

3.2.1 Požadavky

Požadavky na navrhování dveřního nouzového uzávěru jakou jsou funkce uvolnění, konstrukce kliky popř. tlačné plochy, odolnost proti korozi, nutnost zaoblit nechráněné rohy, rozsahy teplot ve kterých dveřní uzávěr stále pracuje v mezích běžných sil nutných k otevření, pozici instalace kliky popř. tlačné plochy na dveře nebo také dostupnou mezeru mezi ovládacím prvkem a čelní plochou dveří.[18]

3.2.2 Zkušební metody

Dále jsou v normě uvedeny a popsány všechny zkušební testy a metody testující výše uvedené požadavky, kterými musí zkoušený dveřní uzávěr projít s akceptovatelnými výsledky. Výsledky testů se dále klasifikují do 10 znaků. Kde každý znak

symbolizovaný číslicí nebo písmenem označuje testovanou vlastnost a její výsledek. Konec normy je věnován povinným a nepovinným označováním platné normy, jména produktu, roku výroby, atd. přímo na výrobku nebo v dokumentaci.[18]

3.3 ČSN EN 1125

Norma definuje požadavky a zkušební metody pro panikové dveřní uzávěry ovládané horizontálním madlem. Je zde kladen důraz hlavně na zvládání panických událostí před nátlakem a odolností proti vnějším vlivům.[18]

3.3.1 Požadavky a zkušební metody

V požadavcích a následných testech se setkáváme s velice podobnými nároky jako u ČSN EN 179. Rozdíly oproti předchozí normě je že se tady ještě zkouší test na uvolnění dveří při jejich zatížení. A hlavní důraz je kladen na jednoduché otevření mladistvými, staršími a nemohoucími. Naopak na bezpečnost není kladen takový důraz a její úroveň je minimální.[18]

3.4 ČSN EN 13637

Tato norma definuje požadavky a zkušební metody pro elektricky řízené únikové systémy.

3.4.1 Požadavky

Požadavky na tyto zařízení záleží na složení celého mechanismu, pokud jeho úniková část obsahuje technicky nezávislé komponenty odkazuje se norma na normy EN 179 a EN 1125. Na druhou stranu systémy podle EN 13637 mohou zahrnovat technicky závislé části s elektrickou nebo mechanickou spoluúčastí na bezpečnostní funkci, jako je například spouštěcí prvek v ovládacím prvku. Dále je norma podobná normám EN 1125 a EN 179, kde má stejné požadavky a odkazuje se na ně, obsahuje další požadavky a to zejména na elektrickou část dalo by se říci na čistě elektrické zámky. Ty se pak zejména vztahují na výpadky napětí, vstupní signál poplachového systému, časové prodlevy nebo požadavky na únikové tlačítka.[19]

3.4.2 Zkušební metody

Norma dále uvádí pečlivě popsané testy a jejich provádění pro různé typy únikových systémů. Testy prověřují všechny nutné požadavky a přesně definují kriteria

přijatelnosti. Výsledek se dále klasifikuje do 11 znaků, kde znak odpovídá jednomu z prováděných testů.[19]

4 Biometrické čtečky

Biometrický údaj je takový, který je jedinečný pro každého člověka např. oční duhovka. V dnešní době se takovéto údaje často využívají jako přídavné zabezpečení, které zjednodušuje identifikaci. Každý člověk má tak svůj vlastní, nezaměnitelný a nepřenositelný klíč, kterým se dá identifikovat.V dnešní době se využívá hlavně čteček otisku prstů. Běžně se již používají u notebooků, mobilních telefonů či bezpečnostních zámků. V počátcích byla tato technologie drahá a taky ne příliš bezpečná, s postupujícími technologiemi výroby se však ceny a velikosti snímačů zmenšovaly a díky novým principů se zvětšila i jejich bezpečnost. Principů, na kterých může taková čtečka fungovat je více, já zde uvedu ty nejvíce známe a používané :

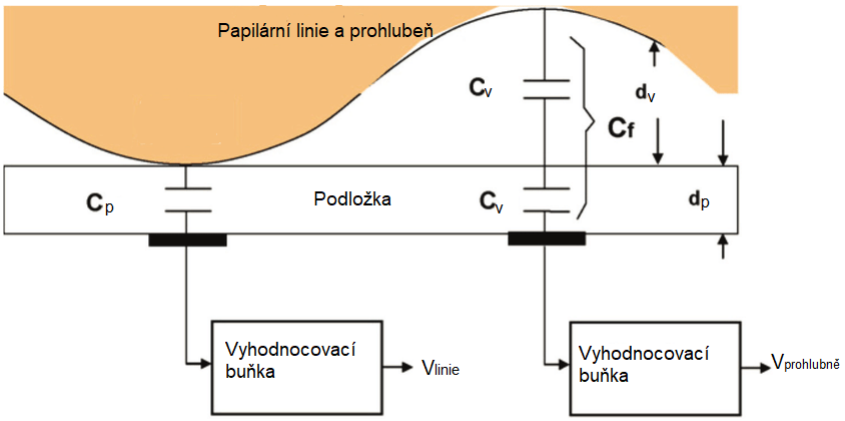
- Optický
- Kapacitní
- Ultrazvukový
- Multispektrální

Optický princip

Tento princip je ze všech uvedených nejstarší, využívá různý odraz světla. Funkce je jednoduchá, na začátku se zdrojem světla vyšle paprsek který se na dotykovém povrchu buď odrazí zpět(papilární linie) nebo pohltí(prohlubeň). Odražené světlo je pak pomocí snímacího čipu vyhodnoceno a je vytvořen obraz otisku. Z principu vyplývají vysoké nároky na rozlišení, dynamický rozsah a další parametry, které snižují šanci na vyhodnocení obrazu. Nevýhodou tohoto principu bylo zpočátku jednoduchost ošálení vyhodnocení, pomocí kvalitní fotografie prstu, nevýhodou jsou i větší rozměry, které znesnadňují implementaci do menších zařízení, mezi další patří možnost špatného vyhodnocení pokud je prst znečištěný nebo poškozený. Výhodou je odolnost vůči poškození statickým výbojem. [13, 14]

Kapacitní princip

Jak název napovídá princip vychází ze změny kapacity mezi deskami. Jednu desku tvoří plocha snímače a druhou snímaný prst. Deska snímače je rozdělena na mnoho jednotlivých částí, kde každá část má vlastní elektrodu a tím i vlastní kapacitu. Ta je určena tím zda se v části nachází papilární linie nebo prohlubeň. Z obrázku 4.1 je patrné, že tam kde je papilární linie je dochází ke změně kapacity, a tam kde je prohlubeň zůstává kapacita relativně nezměněna. Mezi hlavní výhody patří malé rozměry, jednoduchost, s vyšší počtem kondenzátorů vyšší kvalita otisku tím pádem vyšší bezpečnost. Také je zde vyšší bezpečnost než u předchozího optického. Nevýhodou byla zpočátku vysoká cena, která díky moderním výrobním technologiím

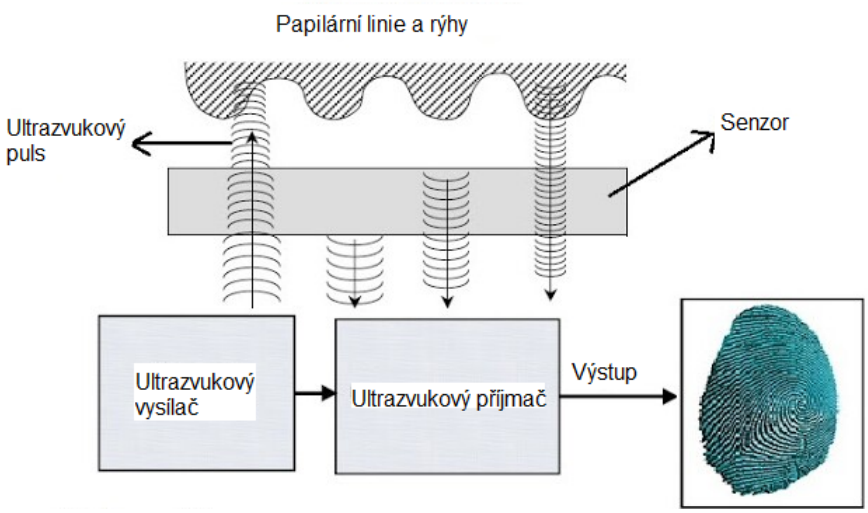


Obr. 4.1: Princip kapacitní čtečky otisku prstů.

již není vysoká, dalším problémem je náchylnost k poškození statickým výbojem. [12, 13, 14]

Ultrazvukový

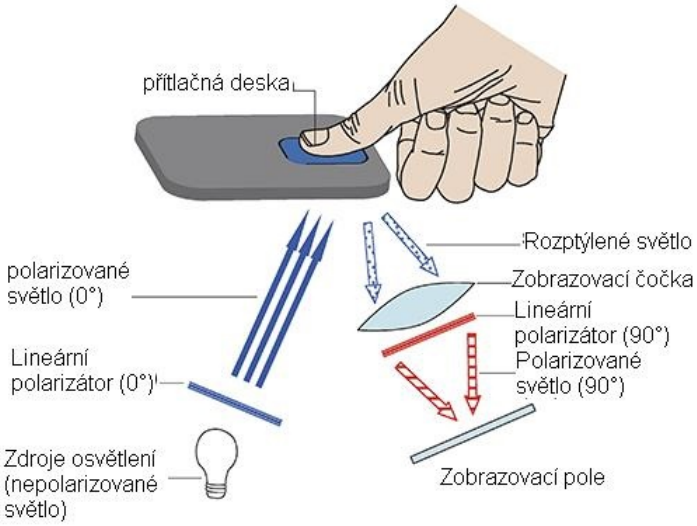
U tohoto typu se porovnává čas mezi vysláním a přijetím odražené vlny. Zjednodušeně můžeme říct, že vlna odražená od papilár bude přijata dřív než vlna odražená od prohlubně. Snímač obsahuje vysílač a přijímač. Pro kvalitní obraz prstu je nutné aby snímač několikrát zopakoval celý proces. Jeho výhody jsou vysoká kvalita obrazu a snímání znečištěných, suchých či vlhkých prstů. Mezi nevýhody patří delší čas snímání a vyšší cena. [12, 14]



Obr. 4.2: Princip ultrazvukové čtečky.

Multispektrální

Princip tohoto snímače spočívá v osvětlování prstu paprsky o různé vlnové délce. Ty prostupují vnějšími vrstvami kůže a odrážejí se od těch vnitřních, což zaručuje mnohem více informací oproti ostatním metodám. Výhody jsou velká kvalita obrazu, odolnost vůči nečistotám a poraněním prstu, vysoká úroveň bezpečnosti. Nevýhodou je vysoká cena. [13]



Obr. 4.3: Princip multispektrálního snímače.

4.1 Výběr biometrické čtečky

Při výběru čtečky otisku prstů jsem se musel řídit potřebami zadané úlohy. Po prvním průzkumu trhu kde jsem se řídil hlavně cenou čtečky, jsem vybral čtyři čtečky Grow R502, Grow R501, Grow R300 a Grow R302 u kterých jsem porovnával další parametry. Mezi prvotní parametr kromě ceny patřil také počet uložitelných otisků, kde počet nad 200 otisků byl zbytečně vysoký pro tuto úlohu. Při bližším porovnání výše uvedených čteček jsem zjistil, že některé parametry mají stejné a proto jsem je mohl vyloučit, mezi takové parametry patřilo rozhraní, které je UART, vyhodnocovací čip, konektor, kapacitní princip snímání nebo shodné rozlišení 508 DPI. Po vyškrtnutí těchto položek jsem se přesunul na porovnávání celkových rozměru, rozměrů snímací plochy a jejich poměrů. Z toho srovnání jsem vyšel s výsledkem

Tab. 4.1: Výhody a nevýhody jednotlivých druhů biometrických čteček

Princip čtečky	Výhody	Nevýhody
Optický	Odolnost proti statickému výboji	Velké rozměry Menší úroveň bezpečnosti Důraz na kvalitu snímacího čipu Nepřesný při znečištění prstu
Kapacitní	Malé rozměry Jednoduchost Vysoká kvalita	Náchylnost k poškození statickým nábojem
Ultrazvukový	Vysoká kvalita Rozpoznání znečištěných nebo poškozených prstů	Delší čas snímání Vyšší cena Vyšší cena
Multispektrální	Vysoká kvalita Správné rozpoznání znečištěném či poraněném prstu Vysoká bezpečnost	Vysoká cena

dvou čteček a to Grow R502 a Grow R501, které jsou obě kulaté. Vybral jsem je protože prostorově zabírají méně místa a proto bude jednodušší je implementovat do kování zámku. Poslední dvě zmíněné čtečky se liší pouze v napájecím pracovním napětí, pracovním proudu a průměru. Grow R501 má pracovní napětí DC 4,2-6V a pracovní proud 42mA, pro Grow R502 to byly následující hodnoty DC 3,3V a 18mA. Vybral jsem si Grow R502, jelikož jeho pracovní napětí je stejné jako jeden z napěťových výstupů mého kontroléru a také jsou jeho rozměry menší než Grow R501.

5 NFC

Zkratkou NFC - Near Field Communication, popisujeme bezdrátovou komunikaci podle standardů ISO/EIC 1892. Přenos probíhá na standardizované frekvenci 13,56 MHz. Technologie jako taková není uzpůsobena velkému přenosu dat, její standardní přenosové rychlosti jsou 106kbit/s, 212 kbit/s a 424 kbit/s. Oproti starší technologii RFID -Radio Frequency Identification má sice NFC kratší dosah, avšak má obousměrnou komunikaci. V současné době se NFC používá hlavně pro rychlý přenos objemově malých dat a slouží tak pro identifikaci předmětů, nastavení zařízení nebo rychlejší párování složitějších komunikací jakou je Wi-fi nebo Bluetooth. [5, 6, 7]

5.1 Historie NFC

Počátky NFC se datují do roku 2004, kdy firmy Sony, Nokia a NXP Semiconductors, zakládají neziskovou organizaci NFC Forum pro tvorbu standartu NFC komunikace. V roce 2006 přichází na svět první NFC tag, také byl na trh uveden první mobilní telefon (Nokia 6131) podporující tuto technologii. Roku 2011 Google demonstruje možnost sdílení kontaktů, URL a dalších informací pomocí NFC, díky tomuto kroku se tato technologie dostává do podvědomí veřejnosti. V roce 2013 firmy Samsung a Visa oznamují spolupráci pro rozvoj plateb mobilním telefonem, v témž roce přichází nová bezpečnostní autentizace založená na NFC. [6, 10]

5.2 Princip funkčnosti

Technologie funguje na principu magnetické indukce. Zdroj signálu kolem sebe generuje elektromagnetické pole, pokud je druhé zařízení v tomto poli vytvoří se magnetická vazba se zdrojem. Vlastní komunikace se realizuje modulací magnetického pole. Ve smyslu napájení rozlišujeme dvě zařízení: **Aktivní** a **Pasivní** a druhy komunikací mezi nimi. [7, 8]

Z tabulky 5.1 je patrné, že pro přenos dat je nutné aby alespoň jedno zařízení bylo aktivní. U druhé a třetí komunikace rozlišujeme tok informací.

5.2.1 Aktivní zařízení

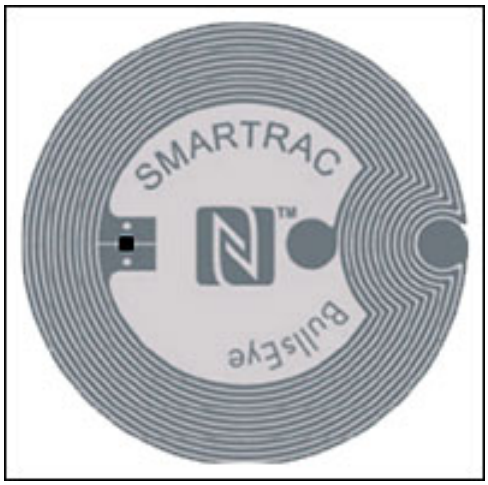
Aktivní zařízení je takové, které má vlastní zdroj energie, čili může vytvářet elektromagnetické pole, kterým pomocí indukce napájí pasivní zařízení a zajišťuje s ním komunikaci. Takovým zařízením může být NFC čtečka nebo chytré zařízení s podporou NFC. [7]

Tab. 5.1: Popis NFC komunikace pro kombinace aktivního a pasivního zařízení

Zařízení A	Zařízení B	EM Pole	Druh komunikace	Popis
Aktivní	Aktivní	Generují obě zařízení	Aktivní	Komunikace probíhá obousměrně, podle potřeby se mění zdroj signálu
Aktivní	Pasivní	Generuje zařízení A	Pasivní	Zdrojem je zařízení A
Pasivní	Aktivní	Generuje zařízení B	Pasivní	Zdrojem je zařízení B

5.2.2 Pasivní zařízení

Pasivní je takové zařízení, které vlastní zdroj energie nemá. Potřebnou energii pro komunikaci získá přes magnetickou indukci od aktivního zařízení. Po získání energie může díky své konstrukci toto zařízení zpětně poslat aktivnímu zařízení informace uložené v paměti. Nejběžnější pasivním zařízením jsou tzv. „tagy“, které se mohou použít jako náhrada čárových kódů. Tyto zařízení jsou velice jednoduché, na substrátu se nachází pouze čip, který je složen z více částí zajišťujících obsluhu komunikace a paměťový blok a anténa. Jelikož tagy jako takové nemají mnoho paměti, tvoří čip zanedbatelnou část celého tagu a celková velikost se odvíjí od velikosti antény jejíž plocha musí být dostatečně velká pro zajištění komunikace. Takovéto zařízení se již běžně používají v kartách, různých čipech nebo ve formě nálepek. [7]



Obr. 5.1: Ukázka NFC tagu

Vyráběné tagy mohou nabývat různých tvarů a velikostí. Nejčastěji je však po-

tkáme v kulatém tvaru. Aby tag fungoval správně, musí být umístěn na nekovovém povrchu. V současné době NFC Forum definovalo čtyři typy NFC tagů v závislosti na velikosti jejich paměti, zabezpečení, přenosové rychlosti a standardu který používají, viz. 5.2

Tab. 5.2: Popis jednotlivých typů tagů

Halo	Typ 1	Typ 2	Typ 3	Typ 4
Použitý standart	ISO/IEC 14443 Typ A	ISO/IEC 1444 Typ A	FeliCa	ISO/IEC 14443 Typ A,B
Název čipu	Topaz	MIFARE	FeliCa	DESFire, SmartMX-JCOP
Velikost paměti	do 1kB	do 2kB	do 1MB	do 64kB
Přenosová rychlost	106kbit/s	106kbit/s	212kbit/s	424kbit/s
Zabezpečení	16 nebo 32 bitový podpis	nezabezpečeno	16 nebo 32 bitový podpis	volitelně
Cena	nízká	nízká	vysoká	průměrná až vysoká
Použití	jednoúčelové	jednoúčelové	flexibilní	flexibilní

Díky výše uvedené tabulce lze podle potřeb úlohy jednoduše zvolit potřebný druh NFC tagu.[5, 10]

5.3 Druhy přenosu

V následujících oddílech budou stručně popsány druhy komunikace.

5.3.1 Reader/Writer

Označuje komunikaci mezi aktivním zařízením a NFC tagem, jejíž cílem je zápis nebo čtení dat z/do NFC tagu. Po celou dobu komunikace je tag napájen elektromagnetickým polem aktivního zařízení. [8]

5.3.2 Card emulation

Jedná se o speciální přenos dat, při kterém se jedno zařízení chová jako pasivní NFC tag, nejběžněji to bývá chytrý mobilní telefon podporující NFC aplikace. Při přiložení takovéhoto zařízení k aktivní čtečce se napodobuje platba bezkontaktní kartou. Tento přenos umožňuje systému chovat se podle standardu ISO/IEC 14443 [8]

5.3.3 Peer-to-Peer

Jedná se o oboustrannou komunikaci dvou aktivních zařízení, které si takto mohou vyměňovat data. ((Popsat technologii. výběr logiky,napsat o videu.... druhy použití... jak jsem to vyřešil s anténou)) [8]

5.4 Formát NDEF

NDEF - NFC Data Exchange Format, jde o binárně zapouzdřenou zprávu, mezi dvěma zařízeními. Zapouzdřená data mohou být libovolná. Každá zpráva se realizuje jedním či více NDEF záznamem. Každý záznam obsahuje tři složky

- Velikost dat - reprezentuje pole uložených dat v bytech. Pole má označení PAYLOAD_LENGHT a zabírá prvních 8B záznamu.
- Typ dat - určuje typ přenášených dat, příslušný typ se ukládá do pole TNF - Type Name Format.
- Volitelný identifikátor - obsahuje identifikátor URI, kterým je možné linkovat data mezi sebou.

[5, 11]

5.5 Vlastní realizace

Při realizaci části úlohy spojené s NFC jsem musel vyřešit dva problémy. Ten první byl výběr kontroléru, který bude řešit samotnou komunikaci pomocí NFC. Druhý problém spočíval ve vytvoření homogenního elektromagnetického pole v prostoru dveří nebo v horší případě pouze kolem kliky.

5.5.1 Výběr modulu

Při výběru modulu pro řízení komunikace jsem se řídil hlavně recenzemi a zkušenostmi ostatních na diskuzních fórech a ve videích. Z předběžného výběru několika kandidátů jsem nakonec vybral modul s označením: PN5180. [9]

5.5.2 Řešení antény

NFC antény nejsou řešeny jako klasické antény, jelikož je pracovní frekvence NFC 13.56 MHz vyplývá nám z toho že délka jedné vlny je 22 metrů, to znamená že kdybychom chtěli udělat klasickou dipólovou anténu měli bychom zařízení o délce 11 metrů. Což není proveditelné. Proto se tyto antény koncipují jako cívka. V zásadě se jedná o dlouhou cívku vytvořenou na ohebném substrátu. Tyto poznatky mě vedou pro sestavení dvěma možnostem koncepce antény u této problematiky. První návrh

by spočíval v rozmístění cívek s dostatečným počtem závitů po obvodu zárubní dveří. Druhá spočívá ve vytvoření dostatečně výkoné cívky, která by se nalepila mezi výplň a desku dveří. Tato teorie není však použitelná pro všechny typy dveří.

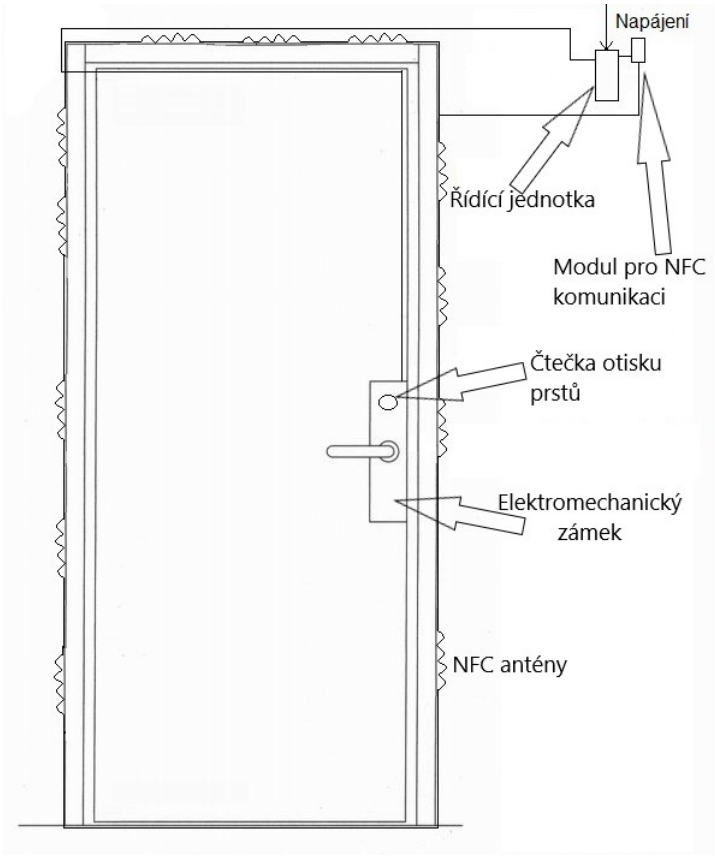
6 Řídící jednotka

Řídící mikrokontrolér je srdcem celého systému, který zpracovává veškerá přijatá data a odesílá signál pro sepnutí vnější kliky. Při jeho výběru jsem si musel určit kritéria, kterými se budu řídit. Hlavním rozhodovacím kritériem byly rozměry desky a implementace softwaru. Vybíral jsem ze tří variant modelů Arduino, ESP32 a Raspberry Pi. Poslední jmenovaný jsem po chvíli vyřadil protože pro zadání je zbytečně výkonný a rozměrově velký. Po srovnání zbylých dvou modelů, které se co do možností rozměrů k poměru dostatečnému výkonu a počtu pinů tak i ceně, sobě vyrovnávaly jsem si vybral variantu ESP díky lepší implementaci kódu.

Vybraný mikrokontrolér disponuje čipem ESP-32 s řadičem CP2102. Frekvence čipu je 240 MHz a disponuje 4MB flash paměti.

7 Návrh hardwarového řešení

Z vybraných součástek popsaných v předchozích kapitolách jsem vytvořil předběžný grafický návrh viz.7.1. Z návrhu je patrné, že čtečka otisku prstů je situována do dveřního kování nad prostor kliky. Napájení zámku a komunikace čtečky je vyvedeno kolem pantů až k řídící jednotce. Kolem rámu dveří můžeme vidět rozmístěné anténu, která má za úkol zajistit dostatečně silné pole pro optimální čtecí vzdálenost NFC karty nebo tagu. Mimo dveřní rám je potom umístěna řídící jednotka s modulem NFC.



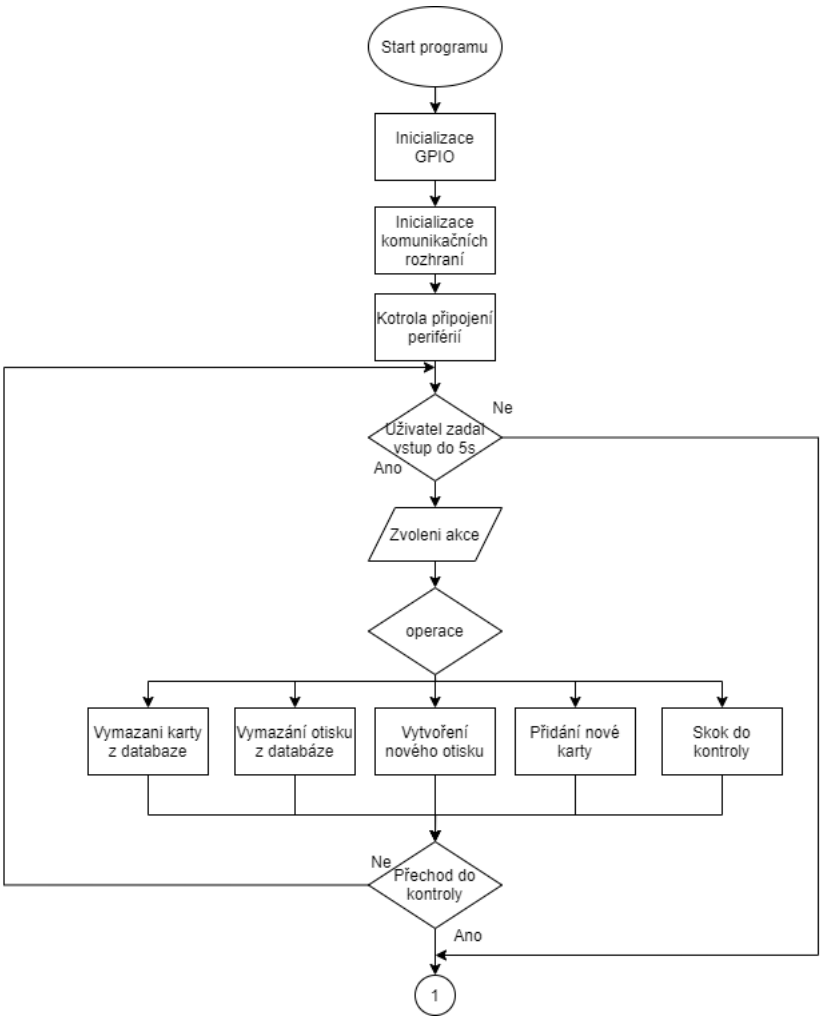
Obr. 7.1: Jednoduché schéma celkového návrhu.

8 Návrh programového řešení

V této kapitole se dále rozepíši o návrhu sowftwaru řídícího systému.

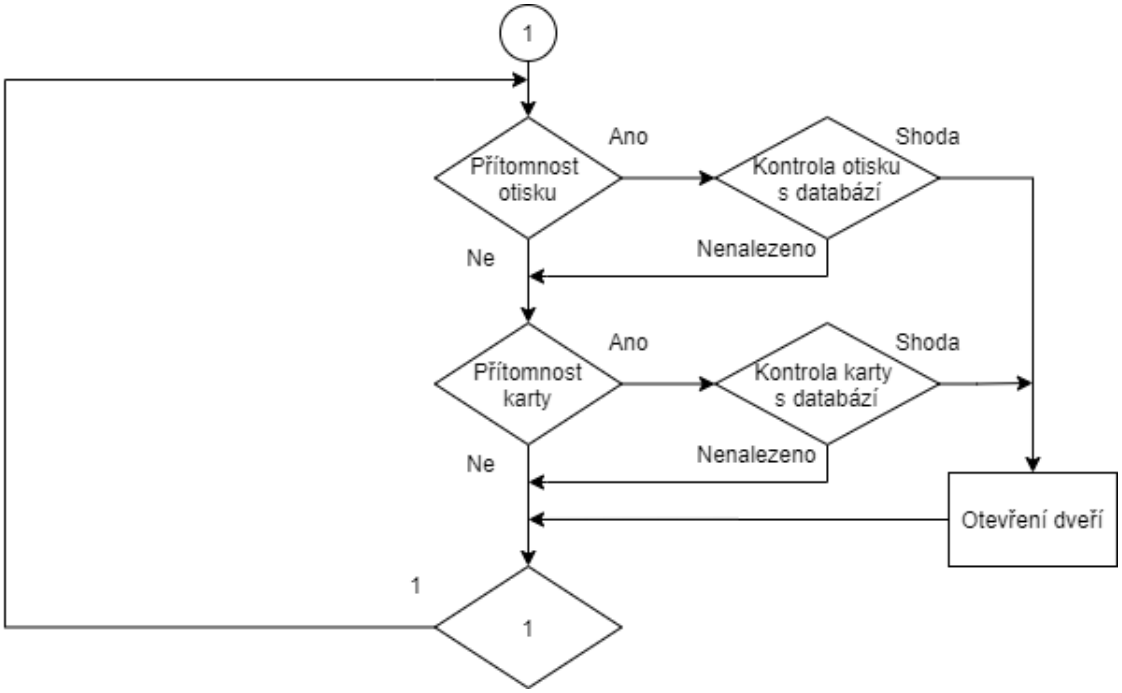
8.1 Hlavní program

Při návrhu jsem kladl hlavní důraz na jednoduchost a rychlost celého programu. Tomu jsem přizpůsobil i tvorbu vývojového diagramu který jsem rozdělil na dvě části. V první části se řeší inicializace a kontrola periferií. Následována možností uživatele zvolit příkaz pokud chce odstranit nebo přidat kartu nebo otisk prstu. Pokud tak neučiní do určité doby program sám přejde do druhé části programu.



Obr. 8.1: Vývojový diagram main funkce první část hlavního programu

Druhá část programu je navržena tak aby neustále kontrolovala možné příchozí vstupy a to buď karty anebo přiložený prst. Pokud je vstup rozeznán a přiřazen ke známé hodnotě v paměti, je sepnut výstup, který ovládá relé a následně je možné otevřít dveře.



Obr. 8.2: Vývojový diagram nekonečné smyčky druhá část hlavního programu

9 Implementace a Demonstrace

Tato kapitola se zabývá implementací vytvořeného softwaru do připraveného hardwaru a následné testování funkčnosti.

9.1 Implementace

Pro programování mikrokontroléru ESP32 jsou oficiálně výrobcem udávané vývojové frameworky Arduino a ESP-IDF, které podporují vývoj programu v programovacích jazycích C/C++.

9.1.1 Arduino

Arduino IDE je open-source program pro práci ve frameworku arduino, který původně sloužil pro programování mikrokontroléry ATMega od firmy Atmel. Toto prostředí je pro svou jednoduchost využíváno hlavně začínajícími nebo nezkušenými programátory pro jednoduché programy. Díky veliké popularitě je volně ke stažení mnoho knihoven. Jednotlivé programy v tomto prostředí jsou realizovány z funkcí setup(), která se provede jednou na začátku, a loop(), která se opakovaně volá. Díky této struktuře programu je snadné porozumění programu.

9.1.2 ESP-IDF

Tento framework vyvíjený přímo výrobcem mikrokontroléru ESP32 a ESP8266 a to firmou Espressif Systems. Obsahuje velkou zásobu napsaných knihoven a umožňuje přidat i knihovny napsané pro Arduino, s tím ,že musí Arduino přidat jako komponenta, což má za následek zvýšení velikosti souboru. Pro sestavení programu se používá program Make a skripty napsané v jazyce Python.

9.1.3 PlatformIO

PlatformIO je mezi plaformový nástroj na vytváření programů pro embedded aplikace. V současné době umožňuje psát v 20 různých frameworcích pro více jak 800 desek různých výrobců. Obsahuje všechny potřebné optimalizační a debugovací nástroje. Výhodou je možnost jednoduchého stažení knihoven například z git repozitáře.

9.1.4 Vlastní implementace

K implementování programu do připraveného hardwaru jsem používal Visual Studio Code s rozšířením PlatformIO. Program jsem psal ve frameworku ESP-IDF a platformě Espressif 32. Program je napsaná v jazyce C++. Výsledné zařízení se skládá mikrokontroléru, čtečky otisku prstů a NFC čtečky.
Struktura zdrojových souborů a jejich použití:

- R502.h
  - Obsahuje konstanty pro ovládání čtečky otisku prstů
  - Deklaruje třídu R502
  - Obsahuje hlavičky metod které slouží ke komunikaci a řízení čtečky otisků prstů
- NFCReader.h
  - Obsahuje konstanty pro ovládání NFC čtečky
  - Deklaruje třídu NFCReader
  - Obsahuje hlavičky metod sloužících ke komunikaci a řízení NFC čtečky
- iso15693.h
  - Deklaruje třídu iso15693
  - Obsahuje hlavičky metod sloužící ke komunikaci pomocí normy ISO/IEC 15693
- main.cpp
  - Počátek programu
  - Obsahuje konstanty pro inicializaci programu
  - Obsahuje funkce pro základní setup programu a inicializaci komunikací
  - Také se zde nachází funkce na načtení karet dvou norem a funkce na porovnání načtené karty s uloženými kartami

Při vytváření zdrojového kódu pro třídu iso15693 jsem se malou měrou inspiroval Githubovým repozitářem uživatele ATrappmann. [25]

9.2 Demonstrace

V následující podkapitolách přesněji popíšu chování implementovaného programu.

9.2.1 Hlavní program

Na začátku programu se provede inicializace vstupů a nastavení komunikace UART - (Universal asynchronous receiver-transmitter) a SPI - (Serial Peripheral Interface). Oproti návrhu popsanému v kapitole 8, přechází program po inicializaci rovnou do kontrolní smyčky. V té se nyní nachází kontrola vstupů a možnost přidat nebo

odebrat otisk prstu nebo kartu pomocí čtyř znakových kódů. Pro zadání těchto kódů se musí uživatel dostat nejprve do speciálního módu tím, že zmáčkne klávesu „i“ a poté zadat správné čtyřmístné heslo. Přehled znakových kódů:

- help - Vypíše ostatní kódy a jejich krátký popis
- nwfp - Přidá nový otisk do knihovny
- dcfp - Odebere zadaný počet otisků z knihovny
- clfp - Vymaže celou knihovnu otisků

9.2.2 Kontrola otisku

Tato část kódu je na začátku podmíněna přítomností prstu na čtečce. Ten se kontroluje pomocí výstupu IRQ ze senzoru čtečky. Po kontrole přítomnosti se prst naskenuje, uloží do bufferu a začne se porovnávat s celou knihovnou. Pokud je nalezena shoda vystup funkce vrátí potvrzovací kód a je sepnut výstup.

Výpis 9.1: Kód kontroly otisku prstu

```
if(gpio_get_level(IRQ) == 0){
            uint8_t a;
            fpreader.genImage();
            fpreader.imgtoChar(1);
            a = fpreader.searchLibrary(1,0,199);
            if( a == 0){
                gpio_set_level(OUT, 1);
                vTaskDelay(4000 / portTICK_PERIOD_MS);
                gpio_set_level(OUT, 0);
            }
            else if(a == 0x01)
                printf("error␣receiving␣package\n");
            else if(a == 0x09)
                printf("Zadna␣shoda\n");
            else
                printf("Jiny␣error\n");
        }
```

9.2.3 Kontrola karty

Kontrola přítomnosti karet se skládá z volání jednotlivých funkcí pro určitou normu karty. Pokud čtečka najde kartu vyčte její ID, které následně pošle do funkce karty, která přijaté ID z kontroluje s databází uložených karet. Jeli nalezena shoda obě dvě funkce vrátí hodnotu true a výstup se sepne. V ukázce kódu 9.2, vidíme volání

kontroly pro normu ISO/IEC 15693.

Výpis 9.2: Volání funkce pro kontrolu karet ISO/IEC 15693

```
if(isa15693(iso15693(NFC, NSS, RST, BUSY), false) == true){
            printf("Zapnuta␣LEDKA\n");
            gpio_set_level(OUT, 1);
            vTaskDelay(4000 / portTICK_PERIOD_MS);
            gpio_set_level(OUT, 0);
        }
```

10 Zabezpečení

Tato kapitola se bude zaobírat slovním zhodnocením úrovně zabezpečení vytvořeného prototypu.

10.1 Hardwarová část

Úroveň zabezpečení fyzické části spočívá na dvou parametrech. Prvním z nich je použitý zámek, kde posuzujeme výrobcem udávané splněné normy(viz.3) a v nich dosažené třídy odolnosti. Druhým parametrem je rozmístění a umístění jednotlivých periférií a řídícího čipu. Ten pak porovnáváme s šancí možného útočníka dostat se k zařízení a následně do zařízení, kde by mohl změnit nastavení nebo přeprogramovat celou řídící jednotku. Vhodnou

10.2 Softwarová část

Komunikace mikrokontroléru s připojenými perifériemi je pro každou čtečku založena na jiném protokolu. V případě čtečky otisků prstů je to komunikace pomocí sběrnice UART, ta se skládá posílané data skládají z menších rámců ,které se skládají ze start bitu, zvoleného počtu datových bitů (většinou 8-bitů) a stop bitu, který oznamuje ukončení rámce.Tento komunikační protokol zajišťuje detekci chyb jako je chyba rámce nebo chyba parity který odhalí chybu v posílaném rámci. U použité čtečky otisku prstů má rámec formát 10 bitů, 8 datových, 1 stop bit a nemá definovanou žádnou paritu. Jistým zakláním typem zabezpečení u tohoto konkrétního použití může být dodržení přesného formátu posílaných dat. Kde data musí být posílána jako „little endian“ a být strukturována podle pokynů výrobce.

Komunikace se čtečkou NFC probíhá pomocí sběrnice SPI ta komunikuje pomocí čtyř vodičů těmi jsou MOSI-(Master Out, Slave In) a MISO -(Master In, Slave Out) sloužící k přenosu dat, CLK - (Hodinový signál) pro řízení a země, která slouží na srovnání potenciálů obou zařízení. Na sběrnici je jeden master, který řídí komunikaci a jeden nebo více zařízení v modů slave, které odpovídají. Díky své jednoduchosti sběrnice němá žádné zabezpečení proti útočníkovi a tak jedinou možností je šifrování posílaných dat. V tomto případě tento způsob použít nelze, protože výrobce přesně udává v jakém tvaru je nutné data posílat.

U obou výše zmíněných komunikací se čtečkami je zabezpečení komunikací prakticky žádné a to hlavně z toho důvodu, že výrobce v dokumentaci přesně udává formát přijímaných a odeslaných dat a fakt že tyto dokumentace jsou volně ke stažení

na stránkách výrobce.

Zabezpečení případu kdy chce komunikovat vyšší zařízení(např. PC) s mikrokontrolérem a kupříkladu přidat nový otisk prstu, musí nejdříve zadat čtyřmístné heslo než bude moct zadat příkazový kód.

11 Zhodnocení výsledků

Díky novým poznatkům při procesu implementace jsem se odchýlil od původních hardwarových a softwarových návrhů. U druhého zmíněného návrhu je to především přesunutí smyčky operací pro uživatele do smyčky kontroly. Kvůli neplánovanému krizovému stavu v České republice byl v elektromechanický zámek po domluvě s vedoucím nahrazen signalizační LED, která dostatečně postačuje pro demonstraci.

Vytvořený prototyp je schopný rozpoznat přiložení otisku a jeho následnou kontrolu se svou databází. Také umožňuje číst karty které splňují normu ISO/IEC 15693 a porovnat je s povolenými kartami uloženými v paměti. Proces nahrávání nového otisku prstů je umožněn a kontrolován po sériové lince, kde vypisovanými hláškami uživatele informuje o procesu nahrávání. Ukládání seznamu karet je realizováno přes sériové rozhraní.

Závěr

V této bakalářské práci byly popsány technologie získávání biometrického údaje prstu a NFC. V příslušné kapitole popisuji výhody a nevýhody různých způsobu čtení otisku prstů a jejich vlastnosti. Kapitola o NFC pojednává o historii této technologie, principy její funkčnosti a věnuje se i jednoduchému popisu používaných standardů. Část práce byla věnována českým technickým normám specifikujícím požadavky a testování panikových, nouzových a elektromechanických zámků. Dále byly vytvořeny a popsány návrhy koncepce prototypu a to jak hardwarové tak softwarové části. Z těchto návrhů byl poté implementován a demonstrován funkční prototyp. Ten se skládá z vybraných součástek čtečky otisků prstů Grow R502, integrovaného obvodu pro bezkontaktní komunikaci s kompatibilitou pro NFC PN5180 a řídící jednotky s čipem ESP32. V posledních dvou kapitolách jsem slovně ohodnotil úroveň zabezpečení a zhodnotil výsledky snažení.

Při vypracovávání této práce byla vyložena snaha na její jednoduchost tak aby ji pochopil čtenář, který se touto problematikou nezabývá. Při psaní zdrojových kódu jsem se pokoušel co nejvíce zjednodušit funkce a popsat proměnné tak aby i méně zkušeným programátorům bylo jasné co daná funkce nebo proměnná dělá a jakou má funkci v kódu.

Tato práce pro mě byla obohacením, jak pro vývoj aplikací, tak pro rozšíření znalostí v oblasti nového hardwaru a jeho použití. Blíže jsem pochopil fungování použitých komunikací UART a SPI a jejich využití. Seznámil jsem se s technologiemi rozpoznávání otisku prstů a NFC, s jejich vlastnostmi a možnosti různého způsobu získávání informací. Při práci jsem musel nastudovat různorodé materiály. K tomu jsem využil příslušné dokumentace, ale musel jsem nahlédnou i do vnitřních kódů knihoven abych lépe pochopil jejich fungování.

Literatura

[1] Zámek (zařízení). In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2019-12-30]. Dostupné z: <https://cs.wikipedia.org/wiki/Zámek_(zařízení)<

[2] Něco málo z historie zámkařství [online]. Brno: Novelo, [cit. 2019-12-31]. Dostupné z: <https://www.novelobrno.cz/odborne-clanky/neco-malo-z-historie-zamkarstvi.htm<

[3] BOUŠE, Richard. Technologický postup výroby bezpečnostního klíče [online]. Brno, 2016 [cit. 2019-12-025]. Dostupné z: <http://hdl.handle.net/11012/60264<. Bakalářská práce. Vysoké učení technické v Brně. Fakulta strojního inženýrství. Ústav strojírenské technologie. Vedoucí práce Milan Kalivoda.

[4] Lock and key. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2020-01-01]. Dostupné z: <https://en.wikipedia.org/wiki/Lock_and_key<

[5] ČERNÝ, Tomáš. Nástroj pro vlastní tvorbu NFC štítků na platformě Android [online]. Brno, 2013 [cit. 2020-01-01]. Dostupné z: <http://hdl.handle.net/11012/55064<. Bakalářská práce. Vysoké učení technické v Brně. Fakulta informačních technologií. Ústav počítačové grafiky a multimédií. Vedoucí práce Lukáš Maršík.

[6] VÍTEK, Petr. Senzorový systém s NFC komunikačním rozhraním [online]. Zlín, 2016 [cit. 2019-12-28]. Dostupné z: <https://docplayer.cz/31658886-Senzorovy-system-s-nfc-komunikacnim-rozhranim-bc-petr-vitek.html<. Diplomová práce. Univerzita Tomáše Bati ve Zlíně. Fakulta aplikované informatiky. Vedoucí práce Ing. Tomáš Dulík,Ph.D.

[7] SIKORA, Radoslav. Systém pro bezdrátovou identifikaci na bázi NFC [online]. Ostrava, 2015 [cit. 2020-01-05]. Dostupné z: <http://hdl.handle.net/10084/109337<. Bakalářská práce. Vysoká škola báňská - Technická univerzita Ostrava.

[8] Technologie NFC v 7 bodech. SOS electronic [online]. SOS electronic, 2019 [cit. 2020-01-03]. Dostupné z: <https://www.soselectronic.cz/articles/no-name/technologie-nfc-v-7-bodech-2281<

[9] RFID Roundup! In: Youtube [online]. 2018-12-05 [cit. 2019-12-20]. Dostupné z: <https://www.youtube.com/watch?v=98GXrixOM4c&list=WL&index=33&t=1037s<. Kanál uživatele Playful Technology

[10] Near Field Communication. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2020-01-03]. Dostupné z: <https://cs.wikipedia.org/wiki/Near_Field_Communication<

[11] NFC Data Exchange Format. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2020-01-03]. Dostupné z: <https://cs.wikipedia.org/wiki/NFC_Data_Exchange_Format<

[12] How fingerprint scanners work: optical, capacitive, and ultrasonic variants explained [online]. Robert Triggs, 2019 [cit. 2020-01-02]. Dostupné z: <https://www.androidauthority.com/how-fingerprint-scanners-work-670934/<

[13] Biometrie otisku prstu. ABBAS [online]. Brno: ABBAS, 2011- [cit. 2020-01-02]. Dostupné z: <http://www.biometricke-ctecky.cz/biometriky/otisk-prstu/<

[14] MORAVEC, Petr. Čtečky otisku prstů pod drobnohledem – jak fungují? Mobilizujeme [online]. Mobilizujeme, 2007-, 2016-02-20 [cit. 2020-01-02]. Dostupné z: <https://mobilizujeme.cz/clanky/ctecky-otisku-prstu-pod-drobnohledem-jak-funguji<

[15] Assa Abloy [online]. [cit. 2.1.2020].Dostupné z: <https://www.assaabloy.cz/cs/local/cz/<.

[16] Erbi [online]. movisio [cit. 2.1.2020]. Dostupné z: <https://www.erbi.cz/cs<.

[17] ČSN EN 1125. Stavební kování - Panikové dveřní uzávěry ovládané horizontálním madlem pro používání na únikových cestách - Požadavky a zkušební metody. Praha: Český normalizační institut, 2008, 52 s. Třídící znak 166236.

[18] ČSN EN 179. Stavební kování - Nouzové dveřní uzávěry ovládané klikou nebo zařízením s tlačnou plochou pro používání na únikových cestách - Požadavky a zkušební metody. Praha: Český normalizační institut, 2008, 52 s. Třídící znak 166237.

[19] ČSN EN 13637. Stavební kování - Elektricky řízené únikové systémy pro použití na únikových cestách - Požadavky a zkušební metody. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2015, 130 s. Třídící znak 166239.

[20] ČSN EN 14846. Stavební kování - Zámky a střelkové zámky - Elektromechanicky ovládané zámky a zapadací plechy - Požadavky a zkušební metody. Praha: Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví, 2009, 36 s. Třídící znak 165192.

[21] Esp-Idf dokumentace [online]. 2019 [cit. 2020-06-07]. Dostupné z: <https://docs.espressif.com/projects/esp-idf/en/latest/esp32/index.html<.

[22] PN5180A0xx/C1/C2: High-performance multi-protocol full NFC frontend, supporting all NFC Forum modes [online]. In: . 2018 [cit. 2020-06-07]. Dostupné z: <https://www.nxp.com/docs/en/data-sheet/PN5180A0XX-C1-C2.pdf<.

[23] R502 Fingerprint Module: User manual [online]. In: . 2019 [cit. 2020-06-07]. Dostupné z: <https://www.dropbox.com/sh/epucei8lmoz7xpp/AAAmon04b1DiSOeh1q4nAhzAa?dl=0&preview=R502+fingerprint+module+user+manual-V1.2.pdf<.

[24] Read the Docs Template Documentation: Release v3.0.8-30-gf3704f027 [online]. In: . Espressif Systems, 2019 [cit. 2020-06-07]. Dostupné z: <https://readthedocs.com/projects/espressif-esp-idf/downloads/pdf/release-v3.0/<.

[25] PN5180-Library [online]. In: . 2020 [cit. 2020-06-08]. Dostupné z: <https://github.com/ATrappmann/PN5180-Library<.

[26] ČSN ISO/IEC 15693-1. Karty a bezpečnostní zařízení pro osobní identifikaci - Bezkontaktní objekty s vazbou na dálku - Část 1: Fyzikální charakteristiky. 3. Praha: Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví, 2019, 12 s.

Seznam symbolů, veličin a zkratek

DSP	číslicové zpracování signálů – Digital Signal Processing
f_{vz}	vzorkovací kmitočet
NFC	Near Field Communication
ESZ	elektronické systémy zabezpečení
RFID	Radio Frequency Identification
NDEF	NFC Data Exchange Format
Fail secure	Vnější klika je aktivní po přivedení proudu.
UART	Universal asynchronous receiver-transmitter
SPI	Serial Peripheral Interface
MOSI	Master Out, Slave In
MISO	Master In, Slave Out
CLK	Hodinový signál

Seznam příloh

A Obsah přiloženého CD

- / ..... kořenový adresář přiloženého CD
  - Bakalářská práce ..... Složka s bakalářskou prací
    - Bakalářská práce.pdf
  - Software.zip ..... Zazipované programové soubory
    - .vscode
      - c_cpp_properties
      - extensions
      - launch
      - settings
    - include ..... Hlavičkové soubory
      - iso15693
      - NFCReader
      - R502
      - README
    - lib
      - README
    - src ..... Zdrojové soubory
      - CMakeList
      - iso15693
      - main
      - NFCReader
      - R502
    - test
      - README
    - gitignore
    - travis.yml
    - CMakeLists
    - platformio .3 sdkconfig