Konstrukce systému kontroly vstupu pomocí Arduina

Peter Bitara

Bakalářská práce
2018

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2017/2018

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Peter Bitara**
Osobní číslo:	**A15111**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Konstrukce systému kontroly vstupu pomocí Arduina**
Téma anglicky:	**The Construction of an Access Control System Using an Arduino System**

Zásady pro vypracování:

1. **Vypracujte literární rešerši zaměřenou na systémy kontroly vstupu.**
2. **V rešerši se zaměřte na konstrukci systému kontroly vstupu pro demonstrační a výukové účely.**
3. **Zrealizujte systém kontroly vstupu s RFID čtečkou karet, číselnou klávesnicí a LCD displejem.**
4. **Napište program, který zajistí dvoustupňové ověřování vstupu.**
5. **Naprogramujte simulaci otevření dveří pomocou relé a LED diód.**
6. **Vytvořte vzorovou laboratorní úlohu.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management. Zlín: Radim Bačuvčík – VeRBuM, 2015. ISBN 978-80-87500-57-6.**
2. **MARGOLIS, Michael. Arduino cookbook. 2nd ed. Sebastopol, Calif.: O'Reilly, c2012. ISBN 1449313876.**
3. **BOXALL, John. Arduino workshop: a hands-on introduction with 65 projects. San Francisco: No Starch Press, 2013. ISBN 1593274483.**
4. **PURDUM, Jack J. Beginning C for Arduino: learn C programming for the Arduino. Second Edition. New York: Apress, 2015. ISBN 9781484209400.**
5. **WARREN, John-David, Josh S. ADAMS a Harald MOLLE. Arduino robotics. New York: Apress, 2011, xxiv, 601. Technology in action. ISBN 978-1-4302-3183-7.**

Vedoucí bakalářské práce: **doc. Mgr. Milan Adámek, Ph.D.**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **12. prosince 2017**

Termín odevzdání bakalářské práce: **24. května 2018**

Ve Zlíně dne 12. prosince 2017

doc. Mgr. Milan Adámek, Ph.D.
děkan

L.S.

Ing. Jan Valouch, Ph.D.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové/bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 21.05.2018

.....
podpis diplomanta

ABSTRAKT

Cieľom bakalárskej práce bolo skonštruovať elektronický systém kontroly vstupu s ukladaním dát na SD kartu. V teoretickej časti bakalárskej práce sú v krátkosti popísané elektronické systémy kontroly vstupu. Je načrtnutý pohľad na autentizáciu užívateľov, druhy overovania užívateľov podľa stupňov zabezpečenia a typy elektrických zámkov. V praktickej časti práca popisuje mikropočítač Arduino Mega. Sú popísané druhy pamäti a rozširovacie moduly s ktorými sa pracuje. Následne je opísané, zobrazené hardwarové zapojenie systému, jednoduchý popis funkčnosti programu a jeho overenie. Na záver je načrtnutá laboratórna úloha na konštrukciu elektronického systému kontroly vstupu.

Klíčová slova: Arduino, systém, kontroly, vstupu

ABSTRACT

The aim of the bachelor thesis was to design an electronic access control system with data storage on the SD card. The theoretical part of the bachelor thesis is briefly describing electronic access control systems. There is a sketched look at user authentication, types of user authentication under different security levels and types of electric locks. Arduino Mega is described in the beginning of practical part. There are described types of memory and expansion modules that Arduino works with. The hardware connection of the system is described, a simple description of the program´s functionality and its verification. At the end, there is a sketched laboratory role on the design of the electronic access control system.

Keywords: Arduino, system, control, access

Rád by som poďakoval vedúcemu bakalárskej práce pánovi doc. Mgr. Milanovi Adámkovi, Ph.D. za odborné vedenie a smerovanie v priebehu tvorby bakalárskej práce. Taktiež rodine a priateľke, ktorý mi boli oporou počas štúdia.

OBSAH

ÚVOD

Elektronické systémy kontroly vstupu už nepredstavujú iba otváracie mechanizmy na dvere. Ich integrácia s rozličnými zabezpečovacími systémami zvyšuje bezpečnosť, jednoduchosť a energetickú náročnosť zabezpečovaných objektov. Autentizácia užívateľov napreduje hlavne kvôli technologickému posunu a rýchlejším procesorom, ktoré dokážu spracovať väčšie množstvo informácií. Vďaka tomu je možné využiť presnejšie biometrické snímače. Tie už dokonca nemusia byť umiestnené na prístupovom bode, ale na smartphone, pomocou ktorého sa užívateľ autentizuje.

Technologický vývoj na svete sa za posledných 20 rokov výrazne posunul. Tvorba elektronických systémov kontroly vstupu pripadala iba veľkým firmám s vysokým počtom inžinierov a veľkým kapitálom. Taktiež financie a časová náročnosť vývoja elektronických systémov bola vysoká. Tvorba takýchto systémov bola obyčajnému smrteľníkovi neprístupná. V dnešnej dobe na to však nie je za potreby celý tým inžinierov, ale jeden študent so znalosťou jazyka C a hardwarovým vybavením v hodnote 20€.

Mikropočítače Arduino sú malé a výkonovo postačujúce na konštrukciu elektronického systému kontroly vstupu. Na trhu sa nachádza dostatok modulov, ktoré sa dajú využiť pri ich konštrukcií. Moduly je možné využiť na dvojstupňové overovanie užívateľov, kde v prvom kroku sa užívateľ autentizuje a v druhom autorizuje. Čiže systém zisťuje, či má užívateľ právo vstúpiť do objektu a či je užívateľ tým za koho sa vydáva. Na dvojstupňové overovanie je možné využiť token, znalosť informácie, alebo biometrickú vlastnosť.

I. TEORETICKÁ ČASŤ

1 ELEKTRONICKÉ SYSTÉMY KONTROLY VSTUPU

Elektronické systémy kontroly vstupu (ďalej ESKV) predstavujú jeden z typov poplachových systémov. Obsahujú konštrukčné a organizačné opatrenia, potrebné pre povolenie vstupu entít. Rozhodujú o tom, komu, kde a kedy je povolený prístup. Taktiež musia umožniť odchod z priestorov oprávnením i neoprávneným entitám.

Cieľom implementovania ESKV je zvýšenie bezpečnosti objektu. Môže pracovať samostatne, alebo môže byť integrovaný do druhých systémov. Napríklad poplachové zabezpečovacie a tiesňové systémy, poprípade uzavretý televízny okruh.

Do roku 2016 boli ESKV definované v technickej norme ČSN EN 50133, avšak tá bola dňa 11.6.2016 nahradená normou ČSN EN 60839: Poplachové a elektronické bezpečnostné systémy časť 11-1: Elektronické systémy kontroly vstupu. Táto norma zmenila klasifikáciu zabezpečenia, ktorá vychádzala z tried identifikácie a tried prístupu. V novej norme vychádza z úrovne rizika. Tak isto sa zvýšil rozsah a podrobnosť funkčných požiadavkou. Bola rozšírená i používaná terminológia.

1.1 Autentizácia užívateľov

Autentizácia, alebo identifikácia predstavuje dokázanie, alebo zistenie identity jedného objektu. Je to proces pri ktorom sa porovnávajú vlastnosti jedného objektu s databázou objektov. Autentizácia osôb a predmetov je široko použitá v bezpečnostnom priemysle. Využíva sa najmä pri ESKV. Pri overovaní užívateľa môže preveriť: vlastníctvo predmetu, znalosť určitej informácie, alebo biometrickú charakteristika človeka [1], [2], [3].

1.1.1 Autentizácia tokenom

Je to autentizácia osoby pomocou predmetu (tokenu), ktorý vlastní iba tá určitá osoba. Token by mal byť čo najťažšie kopírovateľný. Výhodou a zároveň nevýhodou tejto metódy je prenositeľnosť tokenu. Preto by táto metóda mala byť vždy doplnená o biometrické overenie, alebo znalosť informácie. V praxi sú používané :

- Magnetické karty – Na magnetickom prúžku je pomocou zmagnetizovania určitých častí nahraný kód, ktorý po načítaní identifikuje užívateľa.
- Kontaktné karty – Na povrchu karty sa nachádza čip. Po priložení na čítačku odošle uložené dáta.

- Pasívne bezkontaktné – Obsahujú kondenzátory, ktoré sa po vložení pri snímač nabijú a následne odošlú dáta.
- Aktívne bezkontaktné – Majú väčšiu vzdialenosť ako pasívne bezkontaktné a obsahujú batériu. Aktívne vysielajú do prostredia dáta.
- RFID – pracujú na podobnom princípe ako pasívne bezkontaktné, ale dokážu uložiť väčšie množstvo dát. Existuje mnoho druhov operujúcich na rôznych frekvenciách, avšak v oblasti bezpečnosti by sa mali využívať karty so šifrovaným prenosom. Šifrovanie môže prebiehať pomocou AES alebo 3DES šifrovania. Toto šifrovanie podporujú napríklad karty MIFARE DESFire [4].
- Mobilné zariadenia – v dnešnej dobe majú vysoký výpočtový výkon a veľký úložný priestor. Postupne by mohli nahradiť bezkontaktne karty. Znížili by sa náklady na výrobu kariet a zvýšila by sa bezpečnosť. V podstate by mobilne zariadenie mohlo fungovať ako dvojfaktorová autentizácia. Napríklad pri iPhone 7 by sa mohla overiť biometrická informácia a heslo. Správnosť daných informácií by vyslala kód pomocou NFC prenosu [5].

1.1.2 Autentizácia znalosťou

Autentizácia znalosťou informácie je najjednoduchší, najstarší a najrozšírenejší spôsob autentizácie užívateľa. Je používaná v bezpečnostných aplikáciách, bankovníctve, informačných technológiách, atď. Pri ESKV sa vyskytuje v podobe 5 až 6 miestneho hesla. Autentizácia užívateľa pomocou znalosti sa využíva pri nízkych stupňoch zabezpečenia a predpokladá sa, že znalosťou informácie disponuje iba jediná osoba. Väčšinou vystupuje ako forma autorizácie pri dvoj a trojfaktorovej verifikácií, kde systém overuje užívateľa, čí je tým za koho sa vydáva [3].

1.1.3 Autentizácia biometriou

Biometria je bezpečný a pohodlný spôsob autentizácie užívateľa. Užívateľ si nemusí pamätať heslo, alebo nosiť zo sebou token. V podstate užívateľ je sám sebou tokenom a zároveň informáciou.

Pri biometrickom overovaní užívateľa rozlišujeme medzi biometrickou verifikáciou a biometrickou identifikáciou. Pri biometrickej verifikácií sa overuje biometrický znak s jedným konkrétnym znakom z databázy. Táto metóda je rýchla, pretože systém nemusí prehľadávať celú databázu, ale porovnáva iba jeden znak. Avšak užívateľ sa musí

identifikovať pomocou tokenu, napríklad karty, hesla, atď. Pri biometrickej identifikácií sa biometrický znak porovnáva s celou databázou. Nevýhodou je rýchlosť overovania, ktorá klesá s väčším počtom užívateľov v databáze.

Každý biometrický znak je kombináciou dedičných charakteristík človeka. Tie nie sú závislé na jeho vedomí. Podľa Nation Science and Technology sa rozpoznávanie užívateľa rozdeľuje na biologické a behaviorálne [1], [3], [6].

Biologická biometria

Biologická biometria je založená na jedinečných fyzických znakoch užívateľa. Tieto znaky sa počas života menia len minimálne. Najčastejšie používané sú:

- odtlačok prstu,
- geometria tváre,
- vzorka dúhovky,
- sietnica oka,
- geometria ruky,
- geometria prstu,
- štruktúra žíl na zápästí.

Behaviorálna biometria

Behaviorálna biometria je založená na jedinečných návykoch užívateľa. Tieto návyky získava človek počas celého života. Patrí sem napríklad:

- overovanie hlasom,
- dynamika podpisu,
- dynamika písania na klávesnici [6].

Trendy v biometrií

Smartphony sa v dnešnej dobe stávajú rýchlejšie a výkonnejšie. To dovoľuje implementáciu biometrických čítačiek priamo do zariadení. Napríklad už v roku 2013 bol predstavený iPhone 5s s biometrickým snímačom odtlačku prstu. Od roku 2014 sa biometrické odomykanie smartphonov stáva štandardom vo vyšších triedach a v dnešnej dobe je možné získať smartphone so snímačom odtlačku prstu za ceny od 2000 Kč. To dovoľuje overovanie užívateľa pomocou biometrickej verifikácie na smartphone (token). Čím by sa odstránila nutnosť vybavenia čítačiek ESKV o biometrické snímače, alebo klávesnice. Všetko by

mohlo byť verifikované cez smartphone a čítačka ESKV by iba overovala kód vyslaný zo smartphonu.

V roku 2017 predstavila spoločnosť Apple iPhone X, ktorý podporuje technológia Face ID. Tá používa geometriu tváre, ktorá zvýšila zabezpečenie biometrického overovania pri smartphonoch. Kamera TrueDepth zachytáva údaje z viac ako 30 000 bodov a procesor ich následne porovnáva s uloženým obrazom tváre [7].

1.2 Druhy overenia podľa stupňov zabezpečenia

Druhy overenia podľa normy ČSN EN 60839-11-1 vychádzajú zo stupňov zabezpečenia. Pre každý stupeň zabezpečenia nie je možné využiť všetky druhy overovania. To platí hlavne pri jednofaktorovej autentizácií. Pri dvoj a trojfaktorovej autentizácií je možné využiť všetky druhy overenia na všetky stupne zabezpečenia. Avšak pri nízkych stupňoch zabezpečenia by bola dvoj a trojfaktorová autentizácia príliš nákladná a zbytočná.

Stupne zabezpečenia podľa normy ČSN EN 50131-1:

- nízke,
- nízke až stredné,
- stredné až vysoké,
- vysoké.

Podľa jednotlivých stupňov sa odvíja druh overovania užívateľov. Druhy overenia sú podrobne rozpísané v nasledujúcej tabuľke.

Tab. 1 Druhy overenia užívateľa, podľa stupňa zabezpečenia [2]

	Stupeň 1	Stupeň 2	Stupeň 3	Stupeň 4
Jednofaktorová autentizácia				
PIN – 10 000 kombinácií	Povolené	Zakázané	Zakázané	Zakázané
PIN – 100 000 kombinácií	Povolené	Povolené	Zakázané	Zakázané
Magnetické/bezkontaktné /RFID karty	Povolené	Povolené	Povolené	Povolené
Biometria	Povolené	Povolené	Povolené	Povolené
Dvojfaktorová autentizácia				

Magnetické/bezkontaktné karty + PIN 10 000 kombinácií	Povolené	Povolené	Povolené	Povolené
Biometria + PIN 10 000 kombinácií	Povolené	Povolené	Povolené	Povolené
Biometria + magnetické/bezkontaktné karty	Povolené	Povolené	Povolené	Povolené
Biometria + RFID	Povolené	Povolené	Povolené	Povolené
Trojfaktorová autentizácia				
Biometria + PIN 10 000 + magnetické/bezkontaktné/RFID karty	Povolené	Povolené	Povolené	Povolené

1.3 Druhy otváracích zámkov

Pri navrhovaní ESKV je dôležité brať ohľad na bezpečnosť užívateľov a pracovníkov nachádzajúcich sa v objekte počas kritickej situácie. Dôležitým prvkom ochrany zdravia je voľný pohyb osôb z objektu. Napríklad ak by sa v prípade požiaru vyžadovala autentizácia užívateľa na odchod z objektu, tak by sa zvyšoval čas evakuácie a tým by sa zvyšovalo riziko zranenia užívateľa. Z tohto dôvodu sa na dvere inštalujú elektrické zámky. Tie môžu byť rozdelené na zámky, ktoré sa otvárajú mechanicky a zámky otvárané iným spôsobom. Do mechanicky otváracích zámkov partia:

- elektrifikované zadlabovacie zámky,
- elektrifikovaný panikový hardware,
- samozamykacie zámky,
- elektrifikované cylindrické zámky.

Do ostatných spôsobov spadajú:

- magnetické zámky,
- elektromechanické západky.

1.3.1 Samozamykacie zámky

Na otváranie a zatváranie dverí používajú cievku a elektromagnetické pole, ktoré sa vytvára pri prechode elektrického prúdu. To otvára/zatvára západku dverí, ktorá následne umožňuje/neumožňuje prechod. Prichádzajú v dvoch variantoch:

- pri prechode elektrického prúdu sa zámok otvorí. Ak nastane výpadok elektrickej energie, zámok ostáva zatvorený. Môžu byť využité dva druhy prúdov. Striedavý pri ktorom zámok vydáva bzučiaci zvuk. A priamy pri ktorom je počuť iba klik. Tento typ sa nazýva Fail-secure.
- pri prechode prúdu sa zámok zatvorí. Ak nastane výpadok elektrickej energie, zámok ostáva otvorený. Tento typ sa nazýva Fail-safe [8].

1.3.2 Elektrifikované zadlabovacie zámky

Pracujú na podobnom princípe ako samozamykacie zámky, ale cievka neuzamyká západku dverí, ale mechanizmus, ktorý ju otvára. Napríklad kľučku dverí. Tá je z vonkajšej strany objektu uzavretá a otvorí sa iba v prípade povolenia vstupu. Z vnútornej strany je kľučka „odomknutá“ a dvere je možné otvoriť. Tak isto existujú v dvoch variantoch a to: Fail-safe a Fail-sercure.

1.3.3 Elektrifikovaný panikový hardware

Predstavuje systém otvárania dverí v krízových situáciách. Najčastejší variant tohto systému je v podobe tyče, ktorá je pozdĺž celých dverí. Pri jej zatlačení smerom k dverám, môže nastať niekoľko prípadov:

- okamžité otvorenie s alarmom,
- oneskorené otvorenie (15-30) s alarmom. V prípade požiarneho poplachu okamžité otvorenie,
- kontrolované otvorenie. Panicky zámok je nefunkčný a iba v prípade jeho aktivácie (odomknutia) ho je možné použiť. Pri požiarnom poplachu sa musí automaticky aktivovať. Je väčšinou využívaný v nemocniciach a psychiatriách [9].
- monitorované prepínače. Väčšinou používané na exteriérové, alebo vysoko zabezpečené interiérové dvere. Vo forme tlačidla, alebo západky.
- elektrický otváraná západka. Pri prechode prúdu sa automatický otvorí [10].

1.3.4 Elektrifikované cylindrické zámky

Na zadlabovanie zámku využívajú cievku. Sú malé a nie veľmi odolné. Je to jeden z najmenej bezpečných zámkov na trhu. Sú málo odolné voči útoku hrubou silou. Tak isto existujú dve varianty: Fail-safe a Fail-secure.

1.3.5 Magnetické zámky

Patria medzi najpoužívanejšie typy zámkov. Ich výhodou je všeobecnosť. Je ich možno inštalovať skoro na každé dvere. Avšak nie všade legálne. Rozdeľujú sa na: povrchové a skryté. Pracujú na princípe aplikovania elektrického prúdu na elektromagnet.

1.3.6 Elektromechanický západky

Z vnútra objektu sú vybavené mechanickou pákou na núdzový východ z objektu. Dvere sú vybavené s „sledovačom polohy dverí," ktorý pri zavretí dverí vyšle signál ESKV a ten zámok uzavrie. Takýto systém môže obsahovať jeden až päť západiek pre najvyššiu bezpečnosť [10].

1.4 Výhody použitia systému kontroly vstupu

Hlavnou výhodou implementovania ESKV do poplachového systému je zvýšenie bezpečnosti objektu. Ďalšou obrovskou výhodou je možnosť integrovania ESKV s rôznymi systémami. Následkom čoho môže byť zvýšená bezpečnosť a ochrana pri práci, alebo zníženie nákladov na prevádzku objektu.

1.4.1 Bezpečnosť

ESKV funguje nepretržite (za optimálnych podmienok) 24 hodín denne 7 dní v týždni. Znižuje riziko vstupu nepovolených osôb do objektu a zamedzuje pohybu personálu v nepovolených priestoroch. Pri strate tokenu (karty) je možné jednoducho odstrániť token zo systému a tým zamedziť vstupu osoby s daným tokenom.

1.4.2 Integrácia

Ako technologický vývoj napreduje, otvára sa pre konštruktérov možnosť, využívať TCP/IP protokol a tým vytvárať novú generáciu integrovaných systémov. Tieto systémy sú nazývane „Systém riadenia bezpečnosti informácií" (ISMS – Information Security Managment System). ISMS spája bezpečnostné prvky, bezpečnosť pri práci, manažment budovy a rôzne iné.

Integrácia ESKV s rôznymi systémami zvyšuje zabezpečenie objektu, znižuje energetickú náročnosť objektu, atď. Môžu byť integrované napríklad s:

- dochádzkovým systémom,
- ovládaním výťahov
- uzavretým televíznym okruhom (CCTV),
- poplachovými zabezpečovacími systémami (PZS),
- build managment system (BMS),
- požiarnou ochranou.

Dochádzkový systém

Je kombináciou dochádzkového systému a ESKV. Jeden token (karta) slúži užívateľovi na vstup do objektu a zároveň na zapisovanie dochádzky. Kvôli smernici Európskeho parlamentu a Rady 2003/88/E je nutné oddeliť stanice dochádzkového systému od ESKV.

Ovládanie výťahov

Moderné výťahy si dokážu načítať dáta zo ESKV a podľa toho určiť do ktorého poschodia osoba ide, alebo má prístup. Výťah naloží osobu na jednom poschodí a vyloží na presne určenom. Tým pádom sa zníži pravdepodobnosť pohybu neoprávnených osôb v objekte. Zároveň sa zníži spotreba energie, opotrebovanie výťahu a jeho komponentov.

Uzavretý televízny systém

Integrovanie ESKV a CCTV má výhodu v doplnení ESKV o obrazovú informáciu. Pri povolení/zamietnutí vstupu môže kamera zaznamenať užívateľa, s presným časovým údajom (ktorý zaznamenal ESKV) a uložiť ho na úložisko. Záznam môže byť následne analyzovaný a páchateľ zaznamenaný. Zamedzuje i požičiavaniu kariet medzi zamestnancami.

Poplachový zabezpečovací systém

Pri integrácií ESKV a PZS nie je nutné zastražovať/odstražovať systém pomocou klávesnice PZS, užívateľ to môže vykonať u prístupového bodu ESKV. Taktiež systém ESKV môže upozorňovať užívateľa pri zastražení na osoby, ktoré sa ešte nachádzajú v objekte. Pri zastražení môže PZS zablokovať ESKV, aby osoba nenarušila priestor v čase zastražovania. Tieto opatrenia prispievaniu k zníženiu počtu planých poplachov.

Build Managment System

Integrácia BMS a ESKV napomáha k zníženiu energetickej spotreby objektu. BMS môže ovládať svetla, kúrenie, klimatizáciu, ventiláciu, atď. Tieto funkcie môžu byť po opustení budovy automaticky vypnuté. Poprípade pri nižšom počte zamestnancov v objekte obmedzené. A tým znížená energetická náročnosť budovy.

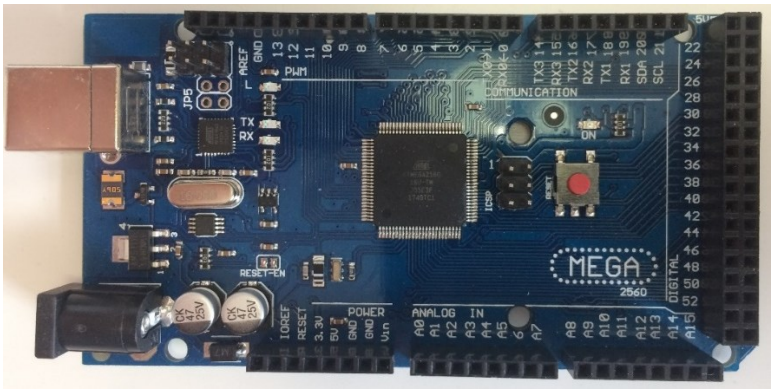
Požiarna ochrana

V prípade požiaru by došlo k automatickému otvoreniu únikových dverí. Pomocou ESKV by bolo možné zistiť, kde sa naposledy nachádzali pracovníci, ktorý sa nedostavili na evakuačné miesto. Následne by táto informácia bola podaná zasahujúcim zložkám [12].

II. PRAKTICKÁ ČASŤ

2 MIKROPOČÍTAČ ARDUINO

Mikropočítač Arduino vznikol v roku 2005. Vymyslel ho profesor Massimo Banzi a David Cuartielles, ktorý hľadali lacný spôsob pre tvorbu mikropočítačových prototypov. Mikropočítače, ktoré sa nachádzali na trhu boli drahé a zložité na používanie. Preto sa rozhodli vytvoriť mikropočítač, ktorý by mohli využiť študenti vo svojich projektoch. Ich hlavným zámerom bolo vytvoriť mikropočítač nízkej cenovej kategórie, ktorý by si mohol dovoliť každý študent. Vývojový team sa rozhodol vydať Arduino pod open source hardware licenciou. Každý môže Arduino vyrábať, modifikovať a distribuovať. To spôsobilo rýchlejší vývoj platformy a širokú distribúciu [14]. Zujímavosťou je, že názov Arduino je podľa lokálneho pohostinstva, ktoré navštevovali študenti a členovia inštitútu [13].



Obr. 1 Ardiuno Mega

Mikropočítač Arduino obsahuje procesor, pamäť, vstupy/výstupy často nazývané GPIO (General Purpose Input Output, preložené ako vstupy a výstupy všeobecného použitia), napájací jack a programovací USB port. Základné špecifikácie mikroprocesoru sú uvedené v tabuľke Tab. 2. Používa mikroprocesor od firmy Atmel. Konkrétne pri mikropočítači Arduino Mega je to ATmega2560 [15], [16].

Tab. 2: Základné údaje o mikroprocesory ATmega2560 [16], [17]

Operatívne napätie	5 V
Vstupné napätie	7 – 12 V
Pamäť Flash	256 KB
Pamäť SRAM	8 KB

Pamäť EEPROM	4 KB
Taktovanie	16 MHz
Počet analógových pinov	16
Počet digitálnych pinov	54

Programovanie Arduina

Arduino Intergrated Development Enviroment, alebo v skrate Arduino IDE je program, ktorý sa používa na programovanie a komunikáciu s mikropočítačmi Arduino. Tento program obsahuje textový editor pre písanie kódu, textovú konzolu pre komunikáciu s Arduinom a textovú oblasť pre vypisovanie chýb v programe [17].

Pri nahrávaní programu na Arduino sa využíva bootloader umiestnený na mikroprocesory ATmega16U2, ktorý dovoľuje nahrávať program bez dodatočného hardwaru.

2.1 Typy komunikácie

Na to aby mikropočítač Arduino dokázal komunikovať s modulmi potrebuje dátovú zbernicu. Arduino využíva hlavne dátovú zbernicu Inter-Integrated Circuit bus (I^2C) a Peripheral Interface (SPI).

2.1.1 Sériová komunikácia I^2C

Tento štandard vyvinula spoločnosť Philips na komunikáciu medzi zariadeniami. Využíva dva vodiče a to SDA - dátový a SCL - hodinový. Na Arduino Mega sú umiestnené, SDA - 20, SCL- 21.

Využíva sedembitovú adresu, na ktorú je možné zapojiť až 128 zariadení. V adresnom rozsahu 0 až 127. Arduino predstavuje master zariadenie a ostatné pripojené sú slave (otroci). Taktiež je možné zapojiť viac rovnakých modulov (napríklad LCD s I^2C), avšak daný modul musí podporovať možnosť zapojenia na rôzne adresy. Rýchlosť prenosu sa pohybuje od 100 Kbit / sec až 3,4 Mbit / sec [18].

2.1.2 Sériová komunikácia SPI

Na rozdiel od I^2C komunikácie dokáže sériová komunikácia SPI, vysielať i prijímať dáta v jednu dobu. Avšak využíva väčší počet vodičov. Na komunikáciu medzi zariadeniami sa využívajú štyri vodiče:

- MOSI – Master Out Slave In,
- MISO – Master In Slave Out,
- SCK – Clock,
- SS – Slave select.

U Arduino Mega sa nachádzajú na pinoch 50 ,51 ,52, 53. Pri pridávaní viacerých slave zariadení je možné využiť tie isté MISO, MOSI a SCK vodiče. Avšak každý slave musí mať vlastný SS vodič.

V programe musí byť SS pin nastavený ako výstup a hodnota HIGH. Pri inicializácií komunikácie s master zariadením (Arduino) sa hodnota mení na LOW. Túto zmenu master zaznamená a začne komunikovať so slave zariadením [14].

2.2 Typy pamäte

Na to aby mikropočítač mohol fungovať potrebuje pamäť. V pamäti sa nachádza aktuálny program a premenné (dáta), s ktorými program pracuje. Tieto pamäte sa volajú Flash a SRAM pamäť. Na ukladanie hodnôt môže užívateľ využiť pamäť EEPROM, ktorá sa nachádza priamo na mikropočítači. Avšak je silne obmedzená na počte čítaní a zápisov, čo nemusí zodpovedať každej aplikácií. Ak užívateľ potrebuje pamäť, ktorá má čítať a zapisovať dáta niekoľko rokov, môže využiť SD kartu.

2.2.1 Flash pamäť

Pri napísaní a nahratí programu na Arduino, sa program uloží do pamäte Flash. Táto pamäť je nevolatilná, čiže po odpojení Arduina z napájania, sa pamäť nevymaže. Flash pamäť obmedzuje veľkosť programu, ktorý môže byť na ňu nahraný. Pri mikropočítači Arduino Mega má užívateľ k dispozícií 248 KB pamäte. Jej veľkosť je pôvodne 256 KB, ale bootloader využíva 8 KB pamäte.

2.2.2 Static Random Access Memory

Ukladajú sa do nej premenné, ktoré využíva program. Je volatilná a jej obsah sa vymaže po odpojení Arduina z napájacej siete. Mikropočítač Arduino Mega má k dispozícií 8 KB SRAM pamäte [19].

2.2.3 Pamäť EEPROM

Electrically Erasable Programmable Read-Only Memory, v preklade elektricky zmazateľná, pamäť ROM. Je to bytovo adresovateľná pamäť. Čiže je možné na jednu adresu uložiť maximálnu hodnotu 255. Táto pamäť, podobne ako Flash pamäť sa pri vypnutí Arduina nevymaže a hodnoty zostanú uložené. Na mikropočítači Arduino Mega je veľkosť tejto pamäte 4096 bytov [20].

Nevýhodou je rýchlosť čítania a zápisu, ktorá je o niečo pomalšia ako pri Flash pamäti. Ďalšou nevýhodou je obmedzený počet zápisov a čítaní z pamäti, ktorý je stanovený na 100 000. Po presiahnutí tohto počtu sa pamäť stáva nespoľahlivou a jej funkčnosť môže vypovedať kedykoľvek. Preto by sa do pamäte mali ukladať iba nastavenia systému, ktoré sa prečítajú jeden krát a následne sa uložia do pamäte SRAM [19].

Systém by mohol byť postavený iba s EEPROM pamäťou, ale jeho funkčnosť by netrvala dlho. Ak by sa na systéme nachádzalo 10 kariet a každý užívateľ by denne použil systém dva krát, nefunkčnosť pamäte by mohla nastať už po 400 dňoch používania. Počet dní rapídne klesá so zvyšujúcim sa počtom užívateľov. Pri 20 užívateľoch môže nastať nefunkčnosť pamäte už po 140 dňoch.

2.2.4 Secure Digital

Štandard Secure Digita (SD) bol predstavený v roku 1999 spoločnosťami SanDisk, Panasonic a Toshiba. Od vtedy sa stal celosvetovým štandardom. SD je nevolatilná pamäť navrhnutá pre prenosné zariadenia. Jej životnosť je približne 100 000 zápisových cyklov. Jeden cyklus predstavuje zápis dát o veľkosti karty. Čiže ak má karta 8 GB, tak na jeden zápis je potreba 8 GB dát [21].

2.3 Moduly

Keďže mikroprocesor reaguje a kontroluje iba elektrické signály, je nutné na prácu s okolím inštalovať moduly. Tieto moduly konvertujú fyzické signály z okolitého prostredia na signál elektrický, ktorý môže mikroprocesor ďalej spracovávať a vyhodnocovať [22].

Vstupy a výstupy

Arduino Mega obsahuje 54 digitálnych vstupov/výstupov, 16 analógových vstupov/výstupov, 5 uzemňovacích vstupov, 4 napájacie výstupy, napájací jack a programovací USB vstup. Digitálne vstupy/výstupy sú schopné rozlišovať medzi hodnotou

0 a 1. Môžu byť nastavené ako INPUT, alebo OUTPUT. Ak sú nastavené ako INPUT, sledujú hodnotu na vstupe. Ak ako OUTPUT vysielajú danú hodnotu ako výstup.

Analógové vstupy/výstupy dokážu rozlišovať medzi hodnotou 0 až 255, kde 0 je logická 0 a 255 je logická 1. V prípade potreby môžu byť naprogramované aj ako digitálne vstupy/výstupy. V prípade potreby je možné nastaviť digitálne a analógové ako napájacie piny (5V), ak je ich hodnota nastavená na HIGH.

2.3.1 Arduino Data Logger Shield

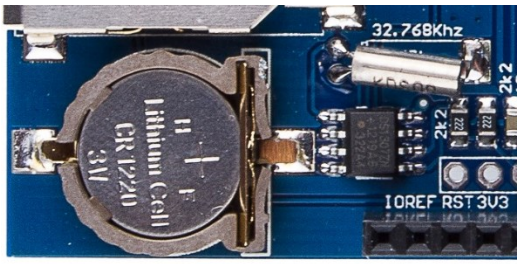
Shieldy sú rozširovacie moduly, ktoré sa dajú nasunúť na Arduino a tak rozšíriť funkčnosť Arduina. Pri používaní shieldov je nutné dbať na rovnaké rozmiestnenie jednotlivých pinov. Väčšina shieldov má rozmiestnenie pinov ako Arduino Uno. Preto pri práci s Arduino Mega je potreba poprepájať niektoré piny. Napríklad piny pre I^2C a SPI komunikáciu. Shieldy môžu obsahovať slot na SD kartu, Eternetovú komunikáciu, GPS modul, alebo aj relé spínače [14].

Čítačka SD kariet

Umožňuje Arduinu komunikáciu s externou SD kartou. Shield umožňuje čítanie i zápis na SD karty s formátovaním FAT 16, FAT 32. Komunikáciu medzi Arduinom a SD kartou zabezpečuje SPI sériová komunikácia [23].

Počítadlo reálneho času DS1307

Počítadlo reálneho času (Real Time Counter, ďalej RTC) ds 1307 používa externý 32.768 kHz quartzový kryštál na výpočet reálneho času. Nachádza sa na Arduino Data Logger Shielde. S Arduinom komunikuje pomocou I^2C komunikácie. Nevýhodou externého oscilátoru je citlivosť na teplotné podmienky. To znamená, že sa hodiny môžu posunúť o 5 minút mesačne [25].



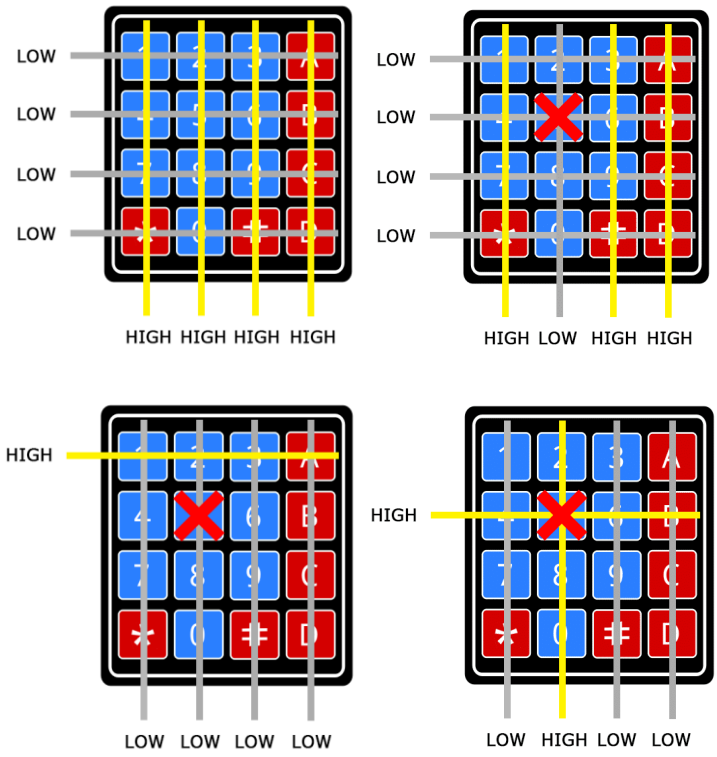
Obr. 2 DS1307 umiestnený na data logger shielde [26], upravil Bitara 2018

2.3.2 Klávesnica

Pokiaľ je nutné zadávať do Arduina číselný vstup a nie je možné využiť počítač, môže sa využiť numerická klávesnica. Jedna z výhod používania klávesnice je nízka obsadenosť pinov. Využíva iba sedem pinov na dvanásť tlačidiel. Stlačenie tlačidla určuje pomocou techniky culumn scanning.

Column scanning

Touto technikou je možné určiť stlačenie určitej klávesy. Ak nie je stlačené žiadne tlačidlo, tak stĺpce majú hodnotu HIGH a riadky LOW (*Obr. 3 vľavo hore*). Po stlačení tlačidla sa hodnota v stĺpci zmení z HIGH na LOW. Tento stĺpec si Arduino uloží. (*Obr. 3 vpravo hore*). Arduino vie v ktorom stĺpci sa stlačené tlačidlo nachádza, avšak nepozná riadok. Ten zistí prepísaním všetkých hodnôt na LOW a postupným zapínaním riadkov na HIGH (*Obr. 3 vľavo dole*). Ak sa na stĺpci objavy hodnota HIGH, znamená to že riadok je správny a tlačidlo sa nachádza v danom riadku (*Obr. 3 vpravo dole*) [27].



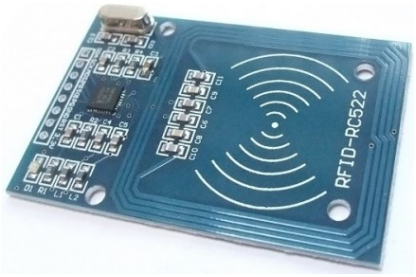
Obr. 3 Culumn scanning [33]

2.3.3 Čítačka kariet RFID-RC522

Tieto čítačky kariet sú lacné a široko dostupné. Dokážu čítať a zapisovať UID karty. Používajú SPI protokol pre komunikáciou medzi Arduinom, ale podporujú i I2C a UART

protokol. Avšak tieto protokoly ešte nie sú implementované v knihovne. Pre komunikáciu s kartami používajú elektromagnetické pole s frekvenciou 13.56 MHz [29].

Ich nevýhodou je zabezpečenie. Problém je medzi komunikáciou karty a čítačky. Tá totižto používa kryptovanie komunikácie Crypto1. Toto kryptovanie bolo prelomené a publikované v roku 2008 výskumnou skupinou z Radboud University. Vďaka tomu je útočník schopný dekryptovať zachytenú komunikáciu medzi kartou a čítačkou. Následne môže vytvoriť vlastnú kartu s rovnakým UID [30].

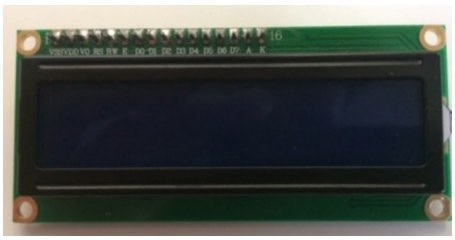


Obr. 4 Čítačka RFID kariet RC522 [31]

2.3.4 Liquid crystal display s I2C modulom

LCD displeje predstavujú grafický výstup mikropočítača. Dokážu zobraziť alfanumerické a špeciálne znaky. Diakritiku však nie. Avšak v prípade potreby si užívateľ môže vytvoriť vlastný znak s diakritikou. V obchodoch sa vyskytujú v rôznych veľkostiach a s rôznym rozlíšením. Ich rozlíšenie sa uvádza ako počet stĺpcov a riadkov. Niektoré displeje dovoľujú zmenu farby podsvietenia a písmen [14].

Nevýhodou je vysoká obsadenosť GPIO pinov. Displej totižto využíva 6 GPIO pinov, VCC a GND pin. Preto sa väčšinou tieto displeje predávajú s I^2C modulom, ktorý tento počet redukuje [32].



Obr. 5 LCD displej s rozlíšením 16x2 znakov

I^2C modul

Hlavnou úlohou I^2C modulu je zníženie počtu GPIO pinov. Ten sa z pôvodných 6 zníži na 2, a to: SDA – dátovy pin a SCL – časový pin (clock line). V prípade potreby je možné na

I^2C zbernicu zapojiť až 8 displejov. To vďaka adresovateľnosti displejov. Ich adresy sa nastavujú pomocou skratovania pinov A0 až A2 (*Obr. 6* pod modrým potenciometrom) [33].

Obr. 6 LCD displej s I^2C modulom

2.3.5 Relé

„Je to elektromagnetický spínač, ktorý pomocou malého vstupného elektrického prúdu dokáže spínať omnoho väčší elektrický prúd na výstupe.“. Pomocou vstupného napätia 5V z Arduina je schopné spínať obvody s napätím 115-250*V* AC a 28-30*V* DC pri prúde 10 *A* (tieto špecifikácie sa vzťahujú ku relé SRD-05VDC-SL-C) [34].

2.3.6 Elektroluminiscenčná dióda

Elektroluminiscenčná dióda (Light Emiting Diode), je polovodičová súčiastka obsahujúca PN prechod, ktorý emituje optické žiarenie, ak ním preteká dostatočný prúd. Je umiestnená priamo na relé a svieti iba v prípade zopnutého stavu, teda signalizuje otvorenie dverí [35].

2.4 Konštrukcia a schéma systému kontroly vstupu

Hlavným stavebným prvkom je mikropočítač Arduino Mega s procesorom ATmega2560. Na Arduino je nasunutý shield s SD kartou a RTC. K nemu sú pripojené moduly pre prácu a komunikáciu s užívateľom. Na shield je pripájaná čítačka RFID kariet, kvôli zníženiu počtu vodičov a úspore miesta. Pomocou vodičov je pripojená klávesnica, displej a spínacie relé.

Komunikácia s modulmi

Arduino komunikuje s modulmi pomocou I^2C a SPI sériovej komunikácie. Konkrétne RFID čítačka a SD kartový modul používa SPI komunikáciu. Počítadlo reálneho času a LCD displej komunikujú pomocou I^2C komunikácie.

Čítačka RFID kariet a SD kartový modul používajú spoločné vodiče. Rozdielny je iba SS pin. Na Arduino Data Logger Shielde je pin 10 pevne pripájaný k SD karte a nejde zmeniť. Pre RFID čítačku kariet je možnosť vybrať ktorýkoľvek voľný pin. Bol zvolený pin 8. Medzi MOSI vodičmi SD modulu a RFID čítačky sa nachádza 220 Ω rezistor.

Počítadlo reálneho času a LCD displej sú pripojené na zbernicu, ktorá vyžaduje iba dva vodiče. Komunikujú s Arduinom pomocou I^2C komunikácie.

Klávesnica je pripojená na Arduino Data Logger Shield a to cez piny číslo: 2,3,4,5,6,7. Jeden vodič je pripojený na Arduino Mega a to na pine 22. Bol presunutý zo shieldu z dôvodu obsadenosti pinov. Na 8 a 9 sa nachádzajú vodiče pre RFID čítačku kariet.

Na grafickej schéme nie sú zvýraznené pripojenia medzi shieldom a Arduinom. Grafická schéma zapojenia je zobrazená v prílohe č. 1. Schéma zapojenia je zobrazená v prílohe č. 2.

3 FUNKČNOSŤ SYSTÉMU

Program sa skladá z dvoch častí. V prvej časti (setup) program kontroluje nastavenia systému. Kontroluje dostupnosť Master karty, ktorá je potrebná pre ďalšie nastavovanie systému. Taktiež kontroluje funkčnosť počítadla reálneho času. Po skontrolovaní a prípadnom nastavení prechádza do druhej časti programu (loop). Tu kontroluje správnosť priloženej karty a následne zadaného hesla. Rozpoznáva rozdiel medzi Master kartou a užívateľskou kartou a následne rozhoduje o povolení vstupu do nastavení, alebo objektu. Taktiež vytvára záznam o povolených a zamietnutých vstupoch do objektu. Záznam ukladá do zložiek jednotlivých kariet.

Celý kód programu je možné vidieť v prílohe č. 3.

3.1 Dvojstupňové overovanie užívateľov

Dvojstupňové overovanie užívateľov je zabezpečené pomocou tokenu (RFID karty) a znalosti informácie (PIN kód). Takéto overovanie zabezpečí autentizáciu a autorizáciu užívateľa. Avšak nemôže zabezpečiť požičiavanie kariet a vyzrádzanie hesiel.

Program najskôr porovná priloženú kartu a všetky uložené karty. Až po potvrdení priloženej karty je od užívateľa vyžadované heslo. To je následne porovnávané s užívateľským vstupom. Ak sa tento vstup rovná s uloženým heslom, program vyhodnotí zhodu a povolí užívateľovi vstup do objektu.

Ak sa karta nezhoduje s uloženými kartami, alebo heslo sa nezhoduje s načítanou kartou, tak program vyhodnotí zlý vstup a zablokuje program na 5 sekúnd.

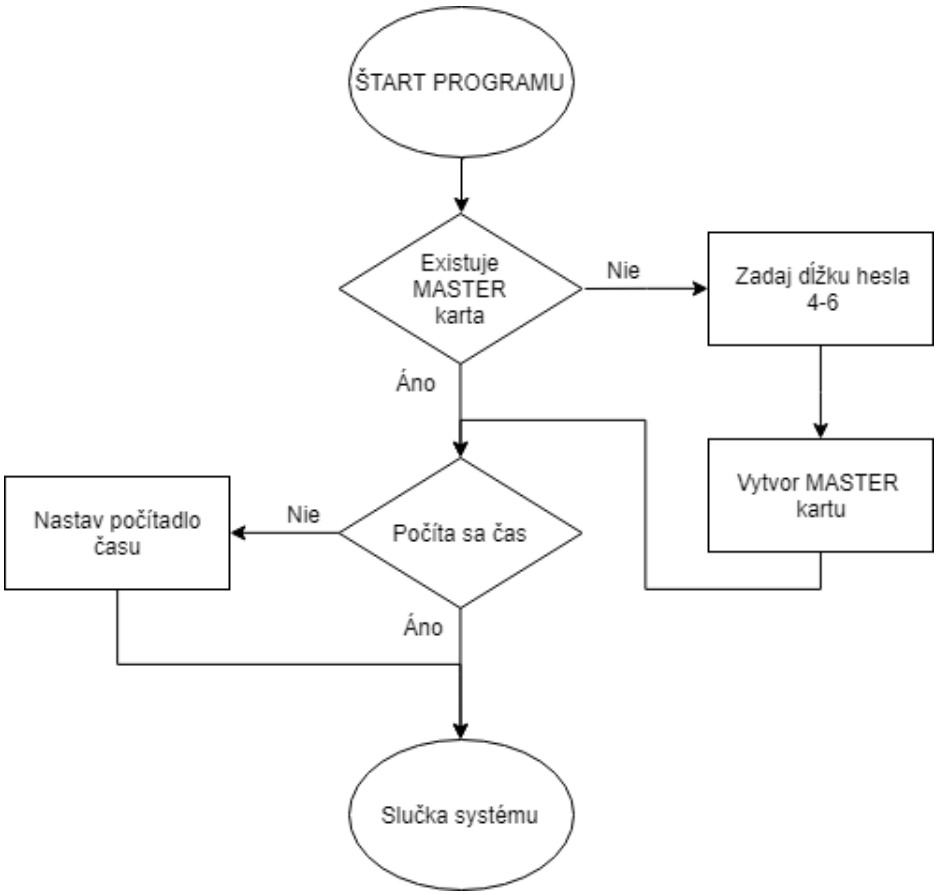
3.2 Štart systému

Pri prvom spustení systému program skontroluje dostupnosť administrátora (Master). Ak Master karta nie je uložená, znamená to že systém nebol nakonfigurovaný. Užívateľ musí zadať dĺžku hesla v rozmedzí 4-6 znakov. Dĺžku hesla je možné meniť iba pri nastavovaní nového systému. Je to opatrenie, aby sa v systéme nenachádzali karty s inou dĺžkou hesla, ako je nastavená v systéme. Po zadaní dĺžky je užívateľ vyzvaný na vytvorenie Master karty. Tú užívateľ vytvorí priložením karty a zadaním nového hesla.

Po uložení program kontroluje nastavenie dátumu a času. Ak ešte nebol nastavený, tak vstúpi do nastavení dátumu a času. Na displeji sa vypíše presný formát zadávania. Užívateľ

následne zvolí dátum a čas pomocou klávesnice. Posledné stlačené tlačidlo sa zobrazí na displej.

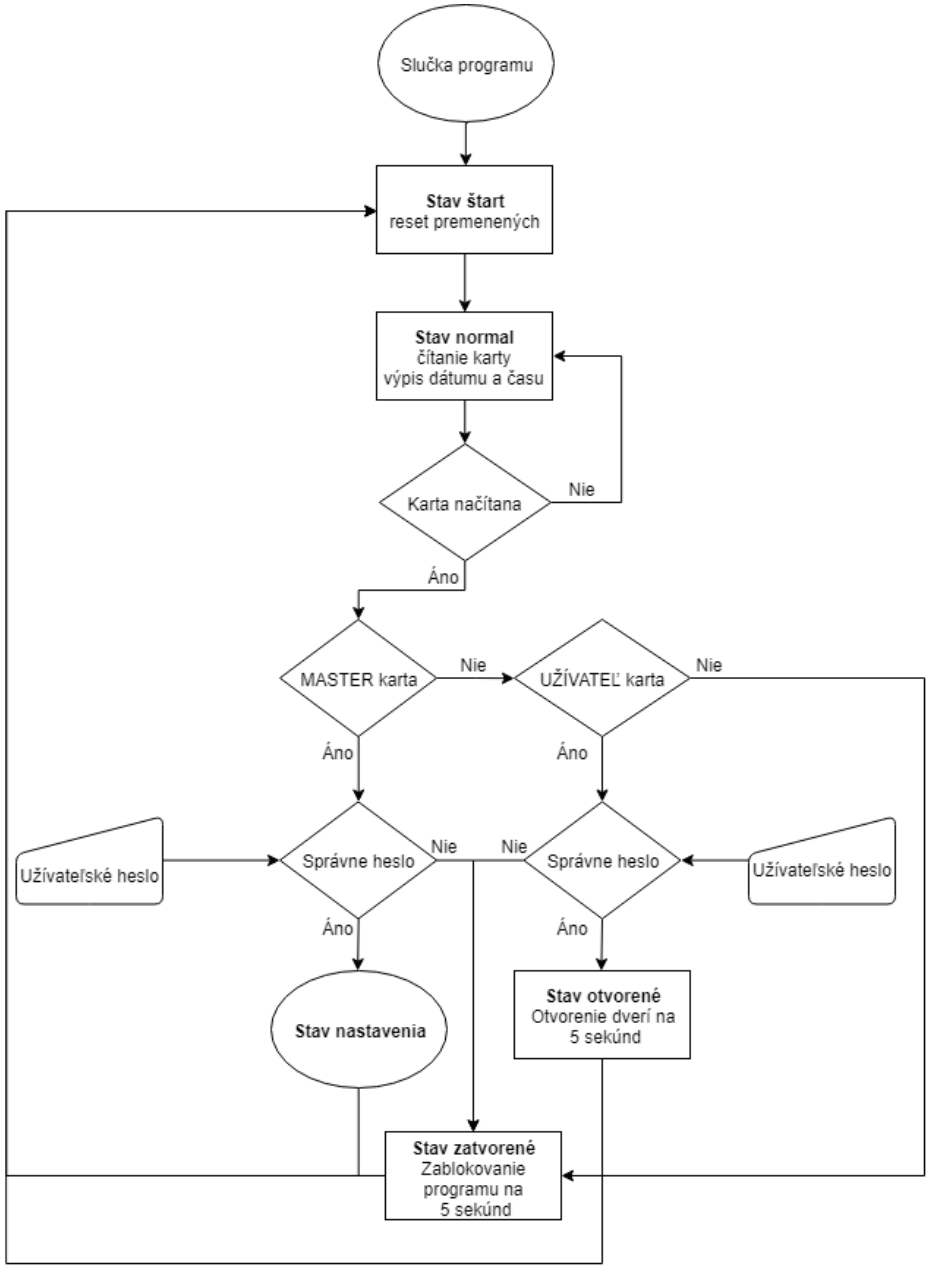
Nastavenie času je možné iba po úplnom vypnutí napájania pre RTC. Následne stačí zapnúť systém a program zistí, že dátum a čas nie sú nastavené.



Obr. 7 Vývojový diagram pre štart programu

3.3 Slučka programu

Slučka programu je tvorená príkazom switch. Switch tvorí celkovo šesť jednotlivých stavov. Prvý stav „start“ prepisuje premenne na počiatočné stavy, rozopína relé a čistí displej. Po vykonaní program prechádza do stavu „normal“. V stave „normal“ program vypisuje na displej aktuálny čas a dátum. Zároveň je aktívna čítačka RFID kariet, ktorá čaká na priloženie karty. Po priložení karty program prechádza do stavu „karta nacitana“, kde kontroluje autentizáciu užívateľa. Podľa umiestnenia karty a hesla následne prechádza do stavov „nastavenia, otvorene, zatvorené“. Po ukončení týchto stavov sa program vracia späť do stavu „start“. Detailnejší popis jednotlivých častí programu sa nachádza nižšie a vývojový diagram je zobrazený na *Obr. 8*.



Obr. 8 Vývojový diagram pre slučku systému

3.3.1 Stav start

Prvý stav switchu. Má za úlohu resetovať premennú nastavenia (určuje či užívateľ už bol v nastaveniach, alebo nie), vypínať relé výstup a resetovať výpis displeju. Program automaticky pokračuje do ďalšej časti.

3.3.2 Stav normal

Program sa pýta RTC modulu na aktuálny čas a vypisuje ho na LCD displej. Zároveň je aktívna čítačka RFID kariet, ktorá zisťuje prítomnosť priloženej karty. Program je zacyklený

až do priloženia karty. Po priložení karty sa jej UID uloží do pamäte Arduina program pokračuje ďalej.

3.3.3 Stav karta načítaná

Program má uložené UID karty, ale neviem či má karta povolený vstup. Program teda prechádza zložky na SD karte, aby zistil jej prístupové práva. Ako prvú prejde MASTER zložku. Ak sa tu karta nachádza vráti zhodu karty. Taktiež prepíše premennú *master*, ktorá určuje Master kartu. Ak sa načítaná karta nezhoduje so žiadnou kartou v zložke MASTER, program prechádza do zložky KARTY. Postup je následne rovnaký až na premennú *master*, ktorá ostáva nezmenená.

Pri kartách, ktoré sa v systéme nachádzajú si program vyžiada heslo. Každý užívateľ má tri pokusy na zadanie správneho hesla. V prípade neúspechu program prejde do stavu „zatvorené“. Pri úspešnom zadaní hesla program prechádza do stavu „nastavenia, otvorené“ v závislosti na premennej *master*.

Pri známej karte program automaticky zapisuje záznam. Tento záznam tvorí presný čas vstupu, počet pokusov pri zadávaní hesla a či bol vstup povolený [*viď. kapitola 3.4*].

3.3.4 Stav nastavenia

Do tohto stavu sa dostane užívateľ s pomocou Master karty. V nastaveniach je možné pridávať, odstraňovať karty, meniť počet Master kariet a otvárať dvere (*Obr. 9*).

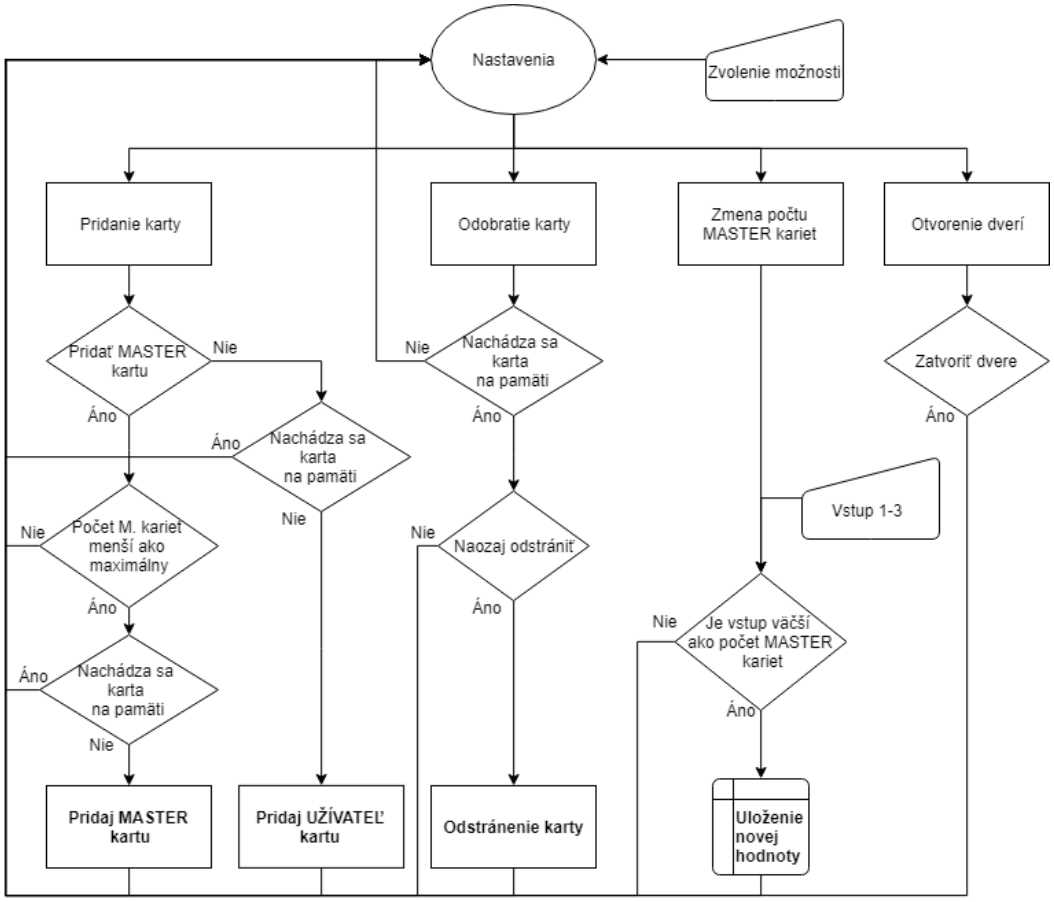
Pri pridávaní karty sa program opýta, či chce užívateľ pridať Master kartu. Pri zvolení Master karty, program skontroluje maximálny počet Master kariet. Ak je aktuálny počet rovný maximálnemu, tak program vypíše chybovú hlášku a vráti sa do nastavení. V prípade nižšieho počtu program pokračuje ďalej. Program následne vyžiada od užívateľa priloženie karty. Túto kartu porovná s uloženými kartami. Ak sa karta už nachádza na SD karte vypíše chybovú hlášku a vráti sa do nastavení. Ak sa nenachádza v systéme, pustí užívateľa k zadávaniu hesla. Následne sa karta uloží a program sa vráti do nastavení.

Odstraňovanie karty prebieha podobným spôsobom. Po priložení karty program skontroluje, či sa karta v systéme nachádza. Ak sa nenachádza vypíše chybovú hlášku a vráti sa do nastavení. Ak sa karta v systéme nachádza opýta sa užívateľa, či chce kartu naozaj odstrániť. Po potvrdení sa karta odstráni aj so zápisom. Následne sa vráti do nastavení.

Zmenu počtu Master kariet je možné vykonať iba v prípade, ak je aktuálny počet Master kariet menší, ako počet ktorý zadáva užívateľ. Čiže ak sa v systéme nachádzajú dve Master karty, užívateľ nemôže zmeniť počet Master kariet na nižší ako dva. Po zadaní správneho maximálneho počtu Master kariet je užívateľ informovaný o zmene prostredníctvom výpisu na LCD displej. Zároveň program prepíše hodnotu v EEPROM pamäti.

Otváranie dverí cez nastavenia je jednoduché a užívateľský priaznivé. Po stlačení tlačidla program automatický otvorí dvere a informuje užívateľa prostredníctvom displeju. Tie zostávajú otvorené, pokiaľ užívateľ nestlačí klávesu „*“. Následne program prejde späť do nastavení a dvere sa zavrú.

V každom kroku sa užívateľ môže vrátiť späť do nastavení. Pri prikladaní karty, zadávaní hesla a nového počtu Master kariet. Toto opatrenie je zavedené kvôli tomu, aby sa v prípade pomýlenia užívateľa nemusel vykonávať celý program. Napríklad ak by chcel užívateľ odstrániť kartu, ale nedopatrením by zvolil pridanie karty. Musel by pridať novú kartu a následne odstrániť obidve. Z nastavení sa užívateľ môže dostať znakom „*“. Program následne prejde do stavu „start“.



Obr. 9 Vývojový diagram pre nastavenia

3.3.5 Stav otvorene

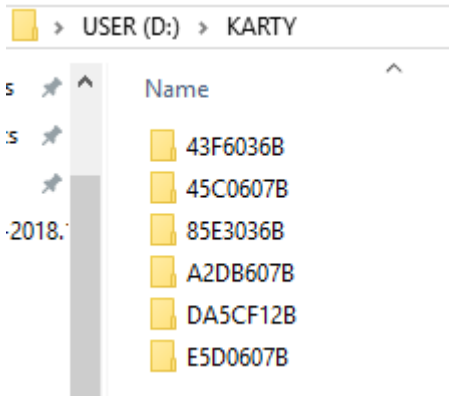
V prípade autentizácie užívateľa program povolí vstup a zopne magnetické relé po dobu piatich sekúnd. Povolený vstup je tak isto vypísaný na LCD displej. Následne program prejde na začiatok programu do stavu „start“.

3.3.6 Stav zatvorene

Tento stav nastane vždy, keď je priložená nesprávna karta, keď je zadané nesprávne heslo a keď je ukončené zadávanie hesla. Program vypíše na displej hlášku „Prístup zamietnutý“ a zablokuje sa na päť sekúnd. Je to opatrenie voči útoku hrubou silou, kde by sa útočník snažil uhádnuť heslo. Program sa následne vráti do stavu „start“.

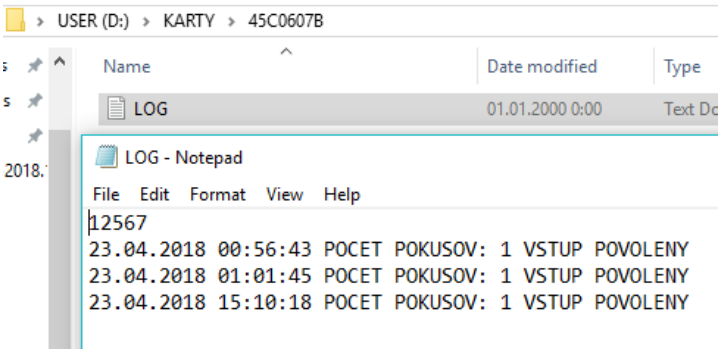
3.4 Formát ukladania kariet a záznamov

Pri prvom spustení systému sa na karte vytvoria dve zložky. Prvá je MASTER, kam sa ukladajú Master karty. Sem sa uloží aj prvá Master karta, ktorá bola vytvorená pri nastavovaní systému. Druhá je KARTY, kam sa ukladajú karty a zatiaľ je prázdna. Pri pridávaní kariet sa vytvárajú zložky. Ich umiestnenie závisí od výberu užívateľa. Každá karta má na SD karte svoju vlastnú zložku. Názov zložky je v tvare hexadecimálneho čísla. Číslo predstavuje jedinečné identifikačné číslo karty (*Obr. 10*).



Obr. 10 Spôsob ukladania kariet na SD kartu

V každej zložke je uložený zápis pre danú kartu (log.txt). Na prvom riadku zápisu sa nachádza heslo od danej karty. Následné riadky tvoria záznamy povolených a zamietnutých vstupov. Záznam pozostáva z presného dátumu a času, počtu pokusov a povolenia, alebo zamietnutia vstupu (*Obr. 11)*. Počet pokusov predstavuje počet pokusov pri zadávaní hesla.



Obr. 11 Zápis karty užívateľa

4 OVERENIE FUNKČNOSTI PROGRAMU

Overenie funkčnosti programu prebiehalo na nenastavenom systéme. V systéme bola vložená prázdna karta a vyresetované počítadlo reálneho času. Skúškou prešiel celý program. Od počiatočných nastavovaní, cez pridávanie/odstraňovanie karty, nastavovanie počtu Master kariet, otváranie dverí pomocou Master karty, až po otváranie dverí užívateľskou kartou.

Pri prvom spustení systému sa na displeji zobrazila správa „Konfigurácia systému“ (*Obr. 12*). Programu chvíľu trvá než sa spustí. To je spôsobene veľkým počtom knihovien, ktoré sú potrebná na komunikáciu s modulmi.

Obr. 12 Konfigurácia systému

Program následne prešiel do počiatočných nastavení. Vyžadoval zadanie dĺžky hesla v rozmedzí 4-6 (*Obr. 13*), kde pri inom čísle, ako je stanovený rozsah zobrazil správnu „neplatný vstup“. Po stlačení správneho čísla sa na displej zobrazilo dané číslo.

Obr. 13 Nastavovanie dĺžky hesla

Po zadefinovaní dĺžky hesla sa program presunul na vytváranie Master karty (*Obr. 14*). Vyzval na priloženie karty a následne na zadanie hesla (*Obr. 18*). Po stlačení klávesy sa na displeji zobrazil znak „*“. Zadávanie hesla sa automaticky ukončilo po dosiahnutí dĺžky hesla.

Obr. 14 Vytváranie Master karty

Ďalším krokom v konfigurácií systému je nastavenie dátumu a času (*Obr. 15*). To prebieha v dvoch krokoch. Ako prvé program vyžaduje zadanie dátumu. Dátum sa zadáva v tvare:

rok, mesiac, deň (*Obr. 16*). Na displej sa vypisuje posledné stlačené tlačidlo. Vstupy sú ošetrené a napríklad nie je možné zadať väčší počet dní, ako má daný mesiac.

Obr. 15 Nastavenie dátumu a času

Po nastavení dátumu program prechádza na nastavenie času. Formát nastavenia času je v tvare: hodina, minúta, sekunda. Zadávanie je rovnaké ako pri nastavení dátumu.

Obr. 16 Nastavenie dátumu

Po úspešnom nakonfigurovaní zariadenia program vypisuje na displej aktuálny dátum a čas (*Obr. 17*). Čas vypisuje vždy aktuálny a mení sa každú sekundu.

Obr. 17 Úvodná obrazovka programu

Po priložení vytvorenej Master karty si program vyžiadal zadanie hesla (*Obr. 18*). Pri stlačený tlačidla sa na displeji zobrazí znak „*“. Heslo sa automaticky porovná po dosiahnutí nastavenej dĺžky hesla.

Obr. 18 Výzva užívateľa na zadanie hesla

Pri zadaní špatného hesla sa na displej vypíše chybová hláška so zostávajúcim počtom pokusov. Ak je heslo zadané tri krát špatne, program sa zablokuje a na displej sa vypíše správa (*Obr. 33*).

Obr. 19 Chybová hláška pri špatnom hesle

Po zadaní správneho hesla systém privíta Mastra (*Obr. 20*) a vstúpi do nastavení. Následne sa zobrazí prvá strana nastavení (*Obr. 21*).

Obr. 20 Úvodná obrazovka pri vstupe do nastavení

Na prvej strane sa zobrazí na výber pridanie a odstránenie karty. Po stlačení tlačidla „#“ systém zobrazil druhú stranu nastavení. Na prvú stranu sa následne dostáva tlačidlom „#“.

Obr. 21 Prvá strana nastavení

Na druhej strane je na výber: zmena počtu Master kariet, otvorenie dverí. Programu nezáleží na ktorej strane nastavení sa nachádza, po celý čas môže užívateľ vybrať všetky možnosti.

Obr. 22 Druha strana nastavení

Po stlačení čísla štyri sa dvere automaticky otvorili (*Obr. 23*). Zostávajú otvorené až do stlačenie klávesy „*“. Stlačením tlačidla sa zatvoria dvere a zobrazí sa druhá strana nastavení.

Obr. 23 Otvorenie dverí cez nastavenia

Pri stlačení čísla jedna sa program opýta, či chce užívateľ pridať Master kartu (*Obr. 24*). Po zvolení tlačidla jeden, program pridáva Master kartu. Po zvolení tlačidla dva, program pridáva užívateľskú kartu.

Obr. 24 Pridávanie kariet

Ak užívateľ pridáva Master kartu a maximálny počet Master kariet je nízky, dostane upozornenie, že už bol dosiahnutý maximálny počet Master kariet (*Obr. 25*).

Obr. 25 Chybová hláška pri pridávaní Master karty

Pri dostatočnom počte voľných Master kariet, alebo pri pridávaní užívateľskej karty sa na displej vypíše potvrdzovacia hláška. Tá potvrdí uloženie karty (*Obr. 26*).

Obr. 26 Potvrdzovacia správa pri pridávaní karty

Pri odstraňovaní karty sa program opýta užívateľa, či si je istý odstránením priloženej karty. Užívateľ musí potvrdiť odstránenie stlačením klávesy jeden.

Obr. 27 Vyžiadanie potvrdenia pri odstraňovaní karty

Po úspešnom odstránení karty je užívateľ informovaný pomocou výpisu na displej (*Obr. 28*). Karta a jej záznam boli nenávratne vymazané.

Obr. 28 Potvrdenie po odstránení karty

Pri zvolení zmeny počtu Master kariet sa na displej zobrazí aktuálny počet Master kariet (*Obr. 29*).

Obr. 29 Zobrazenie aktuálneho počtu Master kariet

Následne je užívateľ informovaný o maximálnom počte Master kariet (*Obr. 30*). Program čaká na užívateľský vstup.

Obr. 30 Informácia o maximálnom počte Master kariet

Po zadaní nového počtu Master kariet, je užívateľ informovaný pomocou displeju (*Obr. 31*).

Obr. 31 Nový počet Master kariet

Po odchode z nastavení sa zobrazí úvodná obrazovka (*Obr. 17*). Po priložení užívateľskej karty a zadaní dobrého hesla sa zoplo relé a displej zobrazil informáciu o otvorení dverí (*Obr. 32*). Rozsvietila sa LED dióda umiestnená na relé.

Obr. 32 Povolenie prístupu

Po priložení užívateľskej karty, ale zadaní špatného hesla bol prístup zamietnutý. Relé zostalo rozopnuté a displej informoval užívateľa o zamietnutom prístupe (*Obr. 33*). Program sa vrátil do úvodnej obrazovky po uplynutí piatich sekúnd.

Obr. 33 Zamietnutie prístupu

5 ZADANIE LABORATÓRNEJ ÚLOHY

1. Vytvorte jednoduchý systém kontroly vstupu.
2. Pri konštrukcií použite Arduino Uno a dve LED diódy (červená, zelená).
3. Nakonfigurujte dve užívateľské úrovne. Master a užívateľ.
4. Autentizácia užívateľov bude prebiehať pomocou štvormiestneho hesla.
5. Heslo Master užívateľa bude nakonfigurované priamo v kóde.
6. Heslá užívateľov bude môcť pridať Master. Užívateľské hesla sa budú ukladať do pamäti EEPROM.
7. Komunikácia s Masterom a overovanie užívateľov bude prebiehať cez počítač pomocou seriálovej komunikácie.
8. Signalizácia povoleného a zamietnutého stavu bude prevedená pomocou LED diód.
9. Pri testovaní kódu vždy zavolajte učiteľa, ktorý skontroluje zacyklene kódu. Zacyklenie by spôsobilo zničenie pamäti EEPROM !!
10. Za optimalizáciu čítaní a zápisov na pamäť EEPROM budú udeľované plusové body.

ZÁVER

Cieľom bakalárskej práce bola konštrukcia elektronického systému kontroly vstupu s dvojstupňovým overovaním užívateľa. Systém je postavený na platforme Arduino. Mikropočítač Arduino bol rozšírený o moduly: LCD displej, čítačka SD kariet, počítadlo reálneho času, čítačka RFID kariet a relé. Tieto moduly a program tvoria funkčný a jednoducho ovládateľný systém. Každá informácia je vypisovaná na LCD displeji a na každú akciu je užívateľ vyzvaný.

Systém je vhodný do malých podnikov s nízkym počtom prístupových dverí. V závislosti na veľkosti vloženej karty dokáže uchovávať dostatočný počet užívateľov. Uložené údaje je následne možné spracovávať na počítači. Napríklad vo forme dochádzky (Excel).

Program je pre užívateľa nenáročný na používanie. Každý krok, ktorý má urobiť je grafický zobrazený na LCD displeji. Zároveň sú ošetrené vstupy, aby užívateľ nezacyklil program.

Aby systém mohol fungovať ako reálny produkt, je nutné vymeniť RFID čítačku kariet. Tú je možne nahradiť za Adafruit PN532, ktorá podporuje čítanie kariet Desfire. Tie majú kryptovanie komunikácie 3DES, alebo AES. Táto čítačka podporuje aj NFC komunikáciu, ktorá by sa dala využiť pri komunikácií so smartphonom. Overovanie užívateľa by potom mohlo prebiehať, len pomocou smartphonu. Systém by overoval token (smarphone) a biometrickú vlastnosť človeka (odtlačok prstu, geometriu tváre, atď.).

Systém by mohol pracovať aj ako ústredňa. Má dostatok pamäte a GPIO. Taktiež je možné systém vylepšiť na integrovaný, a to nahradením SD modulu za Ethernet modul. Komunikácia by následne prebiehala zo serverom, kde by mohli byť integrované ostatné systémy.

ZOZNAM POUŽITEJ LITERATÚRY

[1] RAK, Roman, Václav MATYÁŠ a Zdeněk ŘÍHA. *Biometrie a identita člověka*. Praha: Grada Publishing, 2008. ISBN 8024723655.

[2] BRITHIS SECURITY INDUSTRY ASSOCIATION. *A specifier´s guide to access control systems*[online]. In: . s. 58 [cit. 2018-05-13]. Dostupné z: https://www.bsia.co.uk/Portals/4/Publications/132-specifiers-guide-access-control-systems[1].pdf

[3] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management*. Zlín: Radim Bačuvčík - VeRBuM, 2015. ISBN 9788087500576.

[4] Mifare. In: *Wikipedia: the free encyclopedia*[online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2018-05-13]. Dostupné z: https://en.wikipedia.org/wiki/MIFARE

[5] VERNER, Philip. Hot access control trends. *SecuriteNews*[online]. 2017 [cit. 2018-05-13]. Dostupné z: https://www.bsia.co.uk/home/securitenews/2017/march/cem-systems-look-at-hot-access-control-trends-for.aspx#

[6] ŠČUREK, Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi*. VŠB TU Otrava, 2008.

[7] Pokročilá technológia funkcie Face ID. *Apple*[online]. 2018 [cit. 2018-05-13]. Dostupné z: https://support.apple.com/sk-sk/HT208108

[8] Electric strike. In: *Wikipedia: the free encyclopedia*[online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2018-05-13]. Dostupné z: https://en.wikipedia.org/wiki/Electric_strike

[9] GREENE, Lori. Delayed Egress vs. Controlled Egress. *IDigHardware* [online]. 2015 [cit. 2018-05-13]. Dostupné z: http://idighardware.com/2015/10/decoded-delayed-egress-vs-controlled-egress/

[10] ALLEGION. *Electrified options for panic hardware* [online]. 2016, , 2 [cit. 2018-05-13]. Dostupné z: https://us.allegion.com/content/dam/allegion-us-2/web-documents-2/Article/Electrified_Options_for_Panic_Hardware_111352.pdf

[11] NORMAN, Thomas L. *Electronic access control*. Waltham, MA: Butterworth-Heinemann, c2012. ISBN 9780123820280.

[12] BRITISH SECURITY INDUSTRY ASSOCIACION. *A guide to integrated securyte managment systems*[online]. 2017, (2), 11 [cit. 2018-05-13]. Dostupné z:

https://www.bsia.co.uk/Portals/4/Publications/203-integrated-security-management-systems.pdf

[13] EVANS, Martin, Joshua NOBLE a Jordan HOCHENBAUM. *Arduino in action*. Shelter Island, N.Y.: London: Oreilly & Associates, 2013. ISBN 9781617290244.

[14] BOXALL, John. *Arduino workshop: a hands-on introduction with 65 projects*. San Francisco: No Starch Press, 2013. ISBN 9781593274481.

[15] SMITH, Alan. *Intruduction to Arduino*. CreateSpace Independent Publishing Platform, 2011. ISBN 978-1463698348.

[16] Arduino Mega 2560 Rev3. *Arduino store* [online]. [cit. 2018-05-13]. Dostupné z: https://store.arduino.cc/arduino-mega-2560-rev3

[17] Arduino Software (IDE). *Arduino* [online]. 2015.09.07 [cit. 2018-05-13]. Dostupné z: https://www.arduino.cc/en/Guide/Environment

[18] MALÝ, Martin. *Hradla, volty, jednočipy*. 1. Praha: CZ.NIC, 2017. ISBN 978-80-88168-26-3.

[19] PURDUM, Jack J. *Beginning C for Arduino*. New York: Distributed to the book trade worldwide by Springer Science+Business Media, 2012. Technology in action series. ISBN 9781430247760.

[20] EVANS, Brian. *Beginning Arduino programming*. New York: Apress, 2011. ISBN 9781430237785.

[21] Secure Digital. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2018-05-13]. Dostupné z: https://en.wikipedia.org/wiki/Secure_Digital

[22] MARGOLIS, Michael. *Arduino cookbook*. 2nd ed. Sebastopol, Calif.: O'Reilly, c2012. ISBN 9781449313876.

[23] ECLIPSERA. *Arduino Data Logger Shield* [online]. In: . 2016, s. 5 [cit. 2018-05-13].

[24] MAXIM INTEGRATED PRODUCTS. *DS1307 64 x 8, Serial, I2C Real-Time Clock* [online]. , 14 [cit. 2018-05-14]. Dostupné z: https://datasheets.maximintegrated.com/en/ds/DS1307.pdf

[25] HANDL, Antonín. *Tutoriál - Užívání hodin reĺneho času DS1307 a DS3231 s arduinem* [online]. In: . 2015 [cit. 2018-05-13]. Dostupné z: https://arduino.cz/tutorial-uzivani-hodin-realneho-casu-ds1307-a-ds3231-s-arduinem/

[26] Arduino Data Logger Shield. In: *ELAB PEERS*[online]. [cit. 2018-05-13]. Dostupné z: https://www.elabpeers.com/arduino-data-logger.html

[27] VODA, Zbyšek. *Průvodce světem Arduina*. Bučovice: Martin Stříž, 2015. ISBN 9788087106907.

[28] PRAVEEN. Interfacing hex keypad to arduino. *Circuitstoday* [online]. 2014 [cit. 2018-05-13]. Dostupné z: http://www.circuitstoday.com/interfacing-hex-keypad-to-arduino

[29] Mifare MFRC522 RFID Reader/Writer. *Playground arduino* [online]. 2014 [cit. 2018-05-13]. Dostupné z: https://playground.arduino.cc/Learning/MFRC522

[30] Arduino RFID Library for MFRC522. *Github*[online]. 2018 [cit. 2018-05-13]. Dostupné z: https://github.com/miguelbalboa/rfid

[31] RC522 RFID Module 13.56MHz. *Hobbytronics*[online]. [cit. 2018-05-13]. Dostupné z: http://www.hobbytronics.co.uk/mfrc522-reader

[32] M, Ľuboš. LCD displej. *Navody arduino* [online]. 2016 [cit. 2018-05-13]. Dostupné z: http://navody.arduino-shop.cz/zaciname-s-arduinem/lcd-displej.html

[33] LANGE, Alex. *I2C Communication with an Arduino*[online]. 2015 [cit. 2018-05-13]. Dostupné z: http://navody.arduino-shop.cz/zaciname-s-arduinem/lcd-displej.html

[34] Saddam. Arduino Relay Control Tutorial. *CirciutDigest* [online]. [cit. 2018-05-14]. Dostupné z: https://circuitdigest.com/microcontroller-projects/arduino-relay-control

[35] DVORÁČEK, Vladimír. Světelné zdroje - světelné diody. *Světlo* [online]. maj 2009, , 4 [cit. 2018-05-14]. Dostupné z: http://www.odbornecasopisy.cz/res/pdf/39810.pdf

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

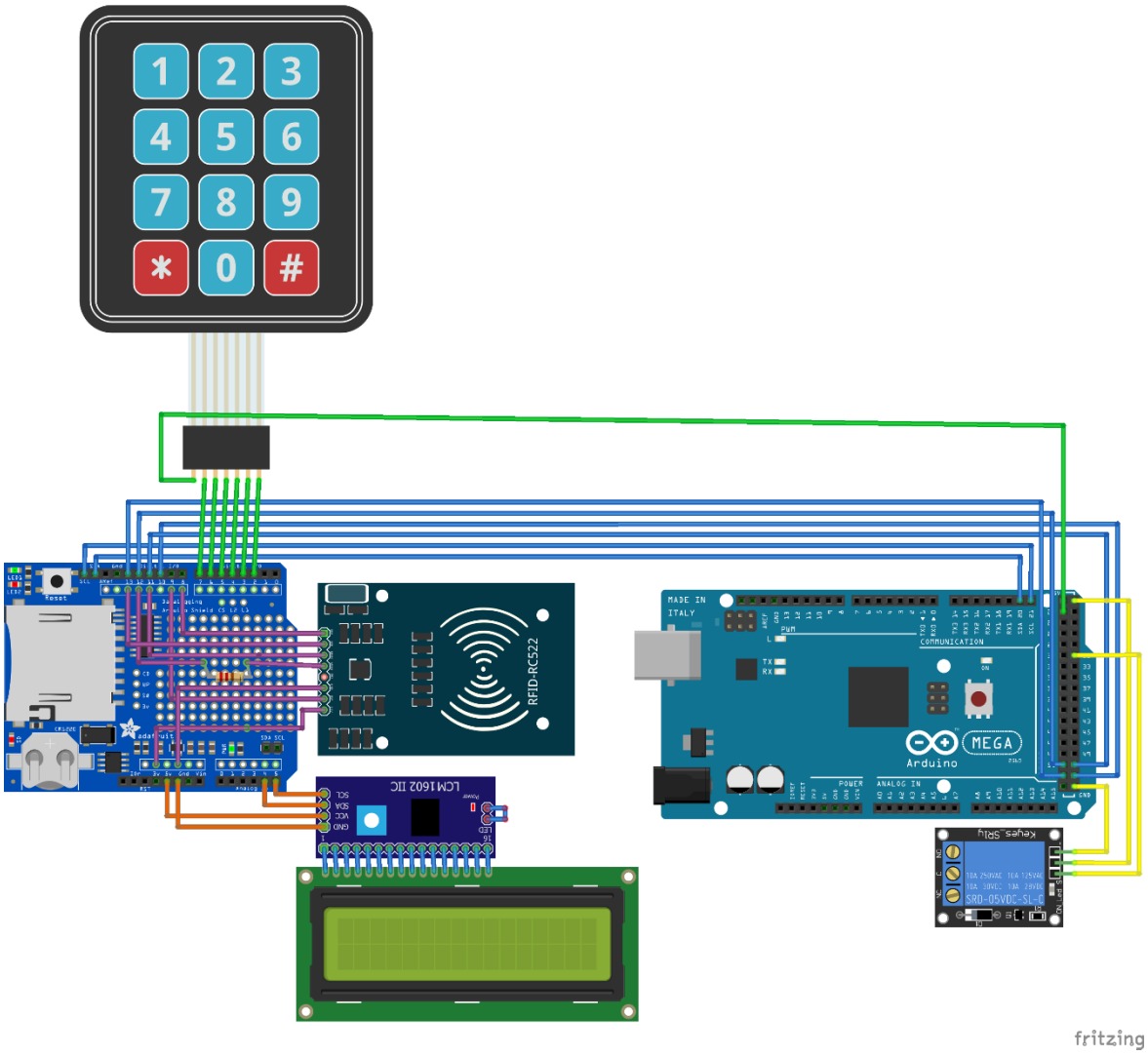
ESKV	Elektronický systém kontroly vstupu
RFID	Radio Frequecy Identification
NFC	Near Field Communication
AES	Advanced Encryption Standard
3DES	Tripple Data Encryption Standard
CCTV	Uzavretý televízny okruh
PZS	Poplachový zabezpečovací systém
BMS	Build Managment System
GPIO	Global Purpose Input Output
USB	Universal Serial Bus
IDE	Intergrated Development Enviroment
SPI	Serial Peripheral Interface
I^2C	Inter Integrated Circuit
LCD	Liquid Crystal Display
SRAM	Static Random Access Memory
EEPROM	Electrically Erasable Programmable Read-Only Memory
SD	Secure Digital
GPS	Global Positioning System
RTC	Real Time Clock
UID	Unique Identifier
LED	Light-Emitting Diode

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

ZOZNAM PRÍLOH

PRÍLOHA P I: GRAFICKÁ SCHÉMA ZAPOJENIA



PRÍLOHA P II: SCHÉMA ZAPOJENIA