VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV MIKROELEKTRONIKY
DEPARTMENT OF MICROELECTRONICS

DVEŘNÍ ZABEZPEČOVACÍ SYSTÉM
DOOR SECURITY SYSTEM

BAKALÁRSKA PRÁCA
BACHELOR'S THESIS

AUTOR PRÁCE — Andrej Marián Drugda
AUTHOR

VEDÚCI PRÁCE — doc. Ing. Pavel Šteffan, Ph.D
ADVISOR

BRNO 2023

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní program **Mikroelektronika a technologie**

Ústav mikroelektroniky

Student: Andrej Drugda ***ID:*** 230467

Ročník: 3 ***Akademický rok:*** 2022/23

NÁZEV TÉMATU:

Dveřní zabezpečovací systém

POKYNY PRO VYPRACOVÁNÍ:

V rámci bakalářské práce navrhněte a realizujte dveřní zabezpečovací systém EKV. Systém realizujte tak, aby podporoval autentizaci pomocí čteček RFID karet, biometrických znaků otisků prstů a aby umožňoval zadávaní hesla přes klávesnici s možným ovládáním systému. Systém dále musí umožňovat konfigurovatelné připojení dalších periferií jako jsou sirény a magnetické snímače. Při návrhu se zaměřte na vhodné bezpečnostní provedení. Systém zhotovte a na hotovém modelu ověřte jeho funkčnost.

DOPORUČENÁ LITERATURA:

Podle doporučení vedoucího práce

Termín zadání: 6.2.2023 ***Termín odevzdání:*** 1.6.2023

Vedoucí práce: doc. Ing. Pavel Šteffan, Ph.D.

doc. Ing. Pavel Šteffan, Ph.D.
předseda rady studijního programu

UPOZORNĚNÍ:

Autor bakalářské práce nesmí při vytváření bakalářské práce porušit autorská práva třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č.40/2009 Sb.

ABSTRAKT

Táto bakalárska práca sa zaoberá návrhom dverového zabezpečovacieho systému podporujúceho vstup pomocou číselného hesla, RFID čítacej karty a tiež pomocou biometrického overovania odtlačku prstu. Projekt je realizovaný ako názorná ukážka rôznych spôsobov bezpečnostného overenia identity. Nosnou časťou práce je hmotný model dverí, ktorý má poskytnúť vizuálne a prehľadné informácie o možnostiach a prevedení zabezpečovacích systémov. Okrem bezpečnostných prvkov, práca popisuje aj výber a parametre mikrokontroléra, na ktorej je celý systém založený. V práci sú ďalej obsiahnuté aj náležitosti, ako popis funkčnosti systému, zobrazenie blokových schém, hardwarové a softwarové vybavenie či postupné vyhotovenie projektu.

KĽÚČOVÉ SLOVÁ

Zabezpečovací systém, Elektronická kontrola vstupu, Jablotron, Atmel, mikroelektronika a technológie.

ABSTRACT

This bachelor thesis deals with the design of a door security system supporting entry using a numeric password, RFID card reader and also using fingerprint biometric authentication. The whole project is situated as a demonstration of various methods of security identity verification. The main part is a material model of the door, which is intended to provide visual and clear information about the possibilities of security systems. In addition to safety elements, the work also describes the selection and parameters of the microcontroller on which the entire system is based.The work also contains essentials such as a description of the system's functionality, a display of block diagrams, hardware and software equipment, or step-by-step implementation of the project.

KEYWORDS

Security system, Electronic access control, Jablotron, Atmel, microelectronics and technology.

Vysadené pomocou balíčku `thesis` verzie 4.07; `http://latex.feec.vutbr.cz`

DRUGDA, Andrej Marián. *Dveřní zabezpečovací systém*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav mikroelektroniky, 2023, 96 s. Bakalárska práca. Vedúci práce: doc. Ing. Pavel Šteffan, Ph.D

Vyhlásenie autora o pôvodnosti diela

Meno a priezvisko autora:	Andrej Marián Drugda
VUT ID autora:	230467
Typ práce:	Bakalárska práca
Akademický rok:	2022/23
Téma závěrečnej práce:	Dveřní zabezpečovací systém

Vyhlasujem, že svoju záverečnú prácu som vypracoval samostatne pod vedením vedúcej/cého záverečnej práce, s využitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor uvedenej záverečnej práce ďalej vyhlasujem, že v súvislosti s vytvorením tejto záverečnej práce som neporušil autorské práva tretích osôb, najmä som nezasiahol nedovoleným spôsobom do cudzích autorských práv osobnostných a/alebo majetkových a som si plne vedomý následkov porušenia ustanovenia § 11 a nasledujúcich autorského zákona Českej republiky č. 121/2000 Sb., o práve autorskom, o právach súvisiacich s právom autorským a o zmene niektorých zákonov (autorský zákon), v znení neskorších predpisov, vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovenia časti druhej, hlavy VI. diel 4 Trestného zákonníka Českej republiky č. 40/2009 Sb.

Brno ....

podpis autora*

*Autor podpisuje iba v tlačenej verzii.

POĎAKOVANIE

Rád by som sa poďakoval vedúcemu semestrálnej práce pánovi doc. Ing. Pavelovi Šteffanovi, Ph.D. za odborné vedenie, konzultácie, trpezlivosť a podnetné návrhy k práci. Taktiež sa musím poďakovať pánom Ing. Vladimírovi Levkovi Ph.D. a Ing. Petrovi Petrovičovi za materiálnu podporu pri vyhotovovaní práce. Samozrejme jedno veľké Ďakujem patrí aj celej mojej rodine, ktorá bola pre mňa obrovskou podporou počas celého štúdia.

Obsah

Úvod **12**

1 Zabezpečovací systém **13**
1.1 Definícia základných pojmov 13
1.2 Elektronický zabezpečovací systém (EZS) 14
1.2.1 Vývoj pojmu EZS 14
1.2.2 Norma ČSN EN 5013x 16
1.3 Architektúra a štruktúra EZS 16
1.3.1 Popis prvkov EZS 17
1.4 Rozdelenie periférií 19
1.4.1 Detektory (hlásiče) - klasifikácia 20
1.4.2 Detekčný diagram 22
1.4.3 Príklady intrúznych detektorov 23
1.4.4 Informačné zariadenia 28
1.4.5 Akčné zariadenia 30
1.4.6 Ovládacie jednotky 31
1.4.7 Komunikačný systém 33

2 Elektronická kontrola vstupu (EKV) **35**
2.1 Popis implementácie EKV 35
2.1.1 Autorizácia 36
2.1.2 Overenie identity 36
2.2 Spôsoby autentizácie podľa stupňa zabezpečenia 37
2.3 Štruktúra architektúry systému EKV 38
2.3.1 Praktická realizácia systému EKV 39
2.4 Druhy autentizácie 40
2.4.1 Autentizácia heslom 41
2.4.2 Autentizácia preukazom 41
2.4.3 Autentizácia hardwarom 42
2.4.4 Autentizácia biometriou 42

3 Praktická časť **44**
3.1 Požiadavky vyplývajúce zo zadania práce 44
3.2 Postup návrhu: 44
3.2.1 Návrh blokovej schémy systému EKV 44
3.2.2 Výber mikrokontroléra (MCU) 46

3.2.3 Výber kompatibilných periférií a modulov na základe návrhu systému elektronickej kontroly vstupu 51
3.2.4 Návrh elektrickej schémy a DPS 66
3.2.5 Zostrojenie modelu dverí 72
3.2.6 Popis programu a funkcionalita systému 74
3.2.7 Meranie a overenie funkčnosti 80

Závěr **82**

Zoznam symbolov a skratiek **88**

Zoznam príloh **89**

A Schéma zapojenia DPS **91**

B Doska plošných spojov **92**
B.1 Vrchná strana 92
B.2 Spodná strana 93

C Vývojový diagram programu systému **94**
C.1 Hlavné menu 94
C.2 Spôsob autentizácie 95
C.3 Možnosti nastavení 96

Zoznam obrázkov

1.1 Štruktúra architektúry EZS 17
1.2 Príklad viacvrstvovej ochrany[2] 20
1.3 Princíp pasívneho detektora 22
1.4 Princíp aktívneho detektora 22
1.5 A - DO je priestor, B - DO je plocha, C - DO je línia 23
1.6 Jazýčkový magnetický detektor 24
1.7 Guľôčkový magnetický detektor 25
1.8 Princíp pyroelektrického snímača 26
1.9 Lom svetla šošovky, vľavo Fresnelova, vpravo Konvexná 26
1.10 Vnútorná konštrukcia prvkov detektora PIR 27
1.11 Štruktúra twisted nematic displeja. [5] 28
1.12 Účinný dosah sirén v závislosti na úrovni hlasitosti[6] 29
1.13 Elektrický vrátnik IQ eStrike, A5000-A[7] 30
1.15 Princíp detekcie stlačenia klávesy[9] 32
1.16 USART- asynchrónny prenos jedného bajtu. 33
1.17 Prenosový protokol komunikácie I2C 34
1.18 SPI komunikácia 34
2.1 Bloková schéma RFID čítačky a karty 37
2.2 Bloková schéma systému EKV 39
2.3 Hierarchické zoradenie spôsobov autentizácie 43
3.1 Bloková schéma systému EKV 45
3.2 Architektúra mikrokontroléra 46
3.3 ATmega644-20PU[23] 50
3.4 Príklad zdroja 12 V 3 A, APV-35-12[24] 51
3.5 UPS akumulátor Li-pol SWISS ARMS 11,1 V 1200 mAh 25C[25] . . . 52
3.6 Modul pre čítanie a zápis SD karty[26] 52
3.7 RTC IC DS3231 53
3.8 Detektor PIR, HC-SR501[27] 54
3.9 Odchodové tlačidlo [28] 54
3.10 MD otvorenia dverí[29] 55
3.11 Príklad koncového spínača WK320[30] 56
3.12 Piezoelektrická siréna LS-103[31] 56
3.13 PWM signál 57
3.14 Servomotor 9g [32] 58
3.15 Spôsoby zapojenia svoriek 58
3.16 Príklad GSM modulu SIM800L[34] 59
3.17 I2C LCD 20x4 [35] 60

3.18 IIC modul LCM1602,[35] 60
3.19 Maticová klávesnica 4x4[36] 61
3.20 Čítačka MF RC522[37] 62
3.21 Príklad snímača odtlačku prsta AS608[38] 63
3.22 Príklad štandardných GaP LED, 5 mm[39] 63
3.23 RGB LED 64
3.24 ASHATA Ibutton Dallas reader [41] 64
3.25 Pasívny Buzzer 5 V[42] 65
3.26 Napájanie a UPS 67
3.27 Stabilizátory 3,3 V 67
3.28 Doplnkové obvody MCU 68
3.29 TTL spínač pre elektrický zámok 69
3.30 Obvod magnetického detektora 70
3.31 Schéma obvodu RTC 71
3.32 Ilustračné foto hotových dverí 72
3.33 Elektronika systému zasadená do zárubne 73
3.34 Zápis hexadecimálnej hodnoty E5 do shift registra 76
3.35 Funkcie pre zápis a čítanie z EEPORM 76
3.36 Úvodná obrazovka 77
3.37 Autentizovanie biometrikou 78
3.38 Autentizovanie predmetom 78
3.39 Autentizovanie znalosťou 78
3.40 Správa systému 79
3.41 Odber za neutrálnych podmienok 80
3.42 Odber pri zopnutom elektrickom zámku 81
3.43 Minimálne napájacie napätie v kľudovom stave 81
A.1 Elektronická schéma zapojenia systému EKV 91
B.1 Pohľad na vrchnú stranu DPS 92
B.2 Pohľad na spodnú stranu DPS 93
C.1 Prvotná zobrazenie systému 94
C.2 Postup autentizácie 95
C.3 Nastavenia 96

Zoznam tabuliek

1.1 Stupne zabezpečenia objektu 16
1.2 Konkrétne typy jednotlivých detektorov 23
2.1 Nároky na autentizáciu podľa stupňa zabezpečenia[15] 38
2.2 Druhy autentizácie 41
3.1 Parametre vybraných mikrokontrolérov z rady ATmega[21] 49
3.2 Základné parametre mikrokontroléra ATmega644-20PU 50
3.3 Súpis komponentov komunikujúcich cez špecifické rozhranie 65

Úvod

Problematikou uschovania a zabezpečenia vlastného nadobudnutého imania sa človek zaoberá v podstate od počiatku existencie. Či sa jednalo o znehodnotenie alebo odcudzenie majetku, vždy tu bola prirodzená snaha chrániť si svoje vlastníctvo.

V prvých prípadoch (dalo by sa povedať už v dobe kamennej), kedy sa človek začal starať o zábezpeku svojho majetku, sa jednalo skôr o nepriaznivé prírodné vplyvy, ako je potopa, požiar či zemetrasenie. Nevylučujú sa i prípadné škody spôsobené zverou. Na ochranu pred týmito faktormi dlho postačovali mechanické zábrany alebo prístup k vode.

Vývoj doby a človeka je však neustály proces bez možnosti zastavenia. Prejdime teda do aktuálnej doby novoveku [16. storočie až súčasnosť], v ktorej dochádza ku množstvu významných objavov a inovácií v širokom spektre odvetví.

Hlavnou kľúčovou sférou dejín objavovania, v preberanej problematike tejto práce, je elektrická energia. Tá má za následok rozvoj nových technologických možností a zmenu životného štandardu človeka. Zostrojením prvého galvanického článku (1792, A.Volta), objavením spojitosti medzi elektrickým prúdom a magnetizmom (1820, H. Ch. Oersted) či vyjadrením vzťahu medzi prúdom, napätím a odporom (G. S. Ohm, 1826) sa elektrine postupnými krokmi otvárali dvere do sveta. Bolo len otázkou času, kedy si nájde uplatnenie aj v zabezpečovacích systémoch.

Jedným z prvých patentových míľnikov v bezpečnostných systémoch fungujúcich na elektrickú energiu podal američan A. Pope v roku 1853. Jednalo sa o poplašný systém PZS, ktorý spočíval na paralelnom zapojení spínacích kontaktov v oknách a v dverách. Zopnutím niektorého z kontaktov bol uzatvorený obvod s elektrickým zvončekom, ktorý spustil poplach [1]. Na hlavnej myšlienke spínania kontaktov pracujú poplachové systémy dodnes, len s obmenou technologického prevedenia.

Dnešné EZS navyše nesnímajú iba zopnutie kontaktu, ale združujú viacero podsystémov pre celkové zabezpečenie stráženého objektu. Pomocou nich je možné monitorovať strážený priestor prostredníctvom kamier, kontrolovať oprávnenie vstupu osôb do miestnosti alebo eliminovať prípadný vznik požiaru. Väčšinou disponujú viacerými komunikačnými rozhraniami ako sú ethernet, sériová linka alebo bezdrôtovými GSM či bluetooth.

Tento projekt spadá do oblasti Elektronických zabezpečovacích systémov [EZS], konkrétne do podoblasti elektronickej kontroly vstupu [EKV]. Hlavnými cieľmi je vytvoriť model dverového zabezpečovacieho systému spoločne s riadiacou elektronikou a korešpondenčným programom. Chráneným záujmom môže byť konkrétny objekt alebo aj celá strážená miestnosť. Tieto dvere budú slúžiť na demonštráciu variabilných spôsobov autentifikácie pomocou prístupových terminálov.

1 Zabezpečovací systém

Ako z názvu vyplýva, zabezpečovací systém (ZS) je určený ku zaisteniu bezpečnosti. V chránených objektoch (firmy, úrady) sa okrem materiálnych aktív môžeme stretnúť i s nehmotnými. Z toho dôvodu bezpečnosť klasifikujeme do následujúcich typov:

- Administratívna – ochrana aktív v listovej podobe
- Personálna – ochrana založená na personálnych opatreniach
- Elektronická – ochrana elektronických dokumentov
- Fyzická – ochrana hmotných aktív

Pre porozumenie, u nehmotných aktív sa jedná napríklad o osobné alebo citlivé informácie (povesť). Základnými, v praxi bežne používanými prvkami jednoduchého zabezpečenia sú napríklad mreže, vyvýšené plochy, bezpečnostné dvere, zámky či prekážky. Okrem týchto mechanických systémov existujú i *elektronické zabezpečovacie systémy*. O EZS stále rastie záujem a dopyt, nakoľko sú rozšírenou formou zabezpečenia a v dnešnej dobe sú bez nich niektoré aplikácie bezpečnostných systémov nerealizovateľné.

Táto práca združuje všetky typy bezpečnosti v závislosti na spôsobe použitia.

1.1 Definícia základných pojmov

Ešte pred začiatkom oboznámenia s danou problematikou je potrebné definovať pár základných pojmov ohľadom zabezpečovacích systémov:

1. **Aktíva** – Všetky cenné statky.
   - Hmotný majetok (nábytok, elektronika)
   - Nehmotný majetok (informácie, know-how...).
2. **Hrozba** – Akákoľvek možnosť straty aktív.
3. **Ochrana** – Akékoľvek opatrenie, ktoré znižuje veľkosť a množstvo strát aktív.
4. **Riziko** – Miera strát aktív. Môže byť:
   - Kvalitatívna (nízka; stredná; vysoká).
   - Kvantitatívna (strata v tisícoch eur).
5. **Bezpečnosť** – Stav, kedy je úroveň rizík nízka.
6. **Zabezpečenie** – Systém ochrany pre zabezpečenie aktív.
7. **Slabina** – Nedostatočná súčasť zabezpečenia, "diera v systéme".
8. **Incident** – Nežiadúca udalosť / uskutočnenie hrozby.

9. **Autorita** – Správna osoba (majiteľ, orgán), ktorá rozhoduje kto a v akej miere má prístup ku daným aktívam.
10. **Užívateľ** – Lojálna osoba, ktorá získala oprávnenie od autority.
11. **Autorizácia** – Povolenie prístupu užívateľovi zo strany autority. (Vloženie dát do systému)
12. **Autentizácia** – Overenie pravosti užívateľa prostredníctvom systému. (Porovnanie OF s DF).
13. **Útočník** – Osoba, ktorá prevádza neoprávnené aktivity bez udelenia povolenia od autority. Môže sa jednať o neautorizovanú, ale aj o autorizovanú osobu.
14. **Útok** – Incident prevedený útočníkom.
15. **Nehoda** – Incident, ktorý nie je útokom (vytopenie, úder blesku, požiar).[1]

1.2 Elektronický zabezpečovací systém (EZS)

Je v zmysle zastúpenia jednotlivých čiastkových poplachových systémov (PZS, EKV, DVS, EPS) systém určený na zaisťovanie bezpečnosti v kontrolovanej oblasti. Jeho úlohou je vo všeobecnosti detegovať a signalizovať vznik nežiadúcich incidentov. Na zaisťovanie bezpečnosti sa v samotnom dôsledku nemusí podieľať iba elektronický systém, ale použitý môže byť aj ľudský faktor vo forme personálu či iného opatrenia.

Pod pojmom elektronické zabezpečovacie systémy si však ľudia najčastejšie predstavia nejakú zložitú až priam predimenzovanú štruktúru bezpečnostných prvkov, aké možno vidieť v rôznych Hollywoodskych scénach. To ale nie je celkom pravdivá ukážka reality a platí presný opak. Samotný návrh bezpečnostného systému sa zakladá na jednoduchosti a nenápadnosti prevedenia.

V praxi hrá veľkú rolu samozrejme ekonomická stránka projektu EZS. Tá sa odvíja od ceny chránených aktív a od požiadavky zákazníka na spôsob ochrany. Zložité predimenzovanie systému sťažuje interakciu zo strany užívateľa a pridáva na celkovej cene. Preto je niekedy zbytočné zavádzať bezpečnostné prvky pre aktíva s hodnotou nižšou ako samotný EZS. Z toho dôvodu je aj systém v tejto práci navrhovaný ako modulárny s možnosťou využitia rôznych druhov prístupových terminálov a periférií pre riadenie EKV.[2]

1.2.1 Vývoj pojmu EZS

Do roku 2002 sa (EZS) nazývalo Elektronická zabezpečovacia signalizácia. Neskôr od roku 2002 až do roku 2009 nadobudlo pojem Elektronický zabezpečovací systém. V dnešnej dobe sa elektronické zabezpečovacie systémy nazývajú Poplachové

zabezpečovacie systémy (PZS). Tie sa delia na 3 pododvetvia:

- PZS => IAS – Intruder Alarm System (signalizácia vniknutia)
- PTS => HAS – Hold-Up Alarm System (signalizácia lúpeže alebo zdravotných ťažkostí)
- PZTS => I&HAS – Intruder and Hold-Up Alarm System (kombinácia obidvoch predošlých systémov)[1]

Pohľad na EZS v súčastnosti

Z počiatku sa všetky elektrické zabezpečovacie systémy zakladali prevažne na relé a spínačových obvodoch s priamou reakciou na podnet páchateľa. Na tomto princípe fungoval aj Bostonský EZS od pána Popa. Avšak prevratná zmena nastala v roku 1947 vynájdením polovodičovej súčiastky tranzistora. Obvodové zapojenia mohli byť menšie, výkonnejšie, spoľahlivejšie a požadovali menšie nároky na údržbu. Tranzistor si tak rýchlo našiel uplatnenie v širokom priemyselnom odvetví vrátane zabezpečovacích systémov.

Funkcia a využitie EZS sa môže javiť ako mierne zbytočná, no nie je tomu celkom tak. Bez EZS si niektoré dnes bežné procesy nedokážeme predstaviť. Jednoduchým príkladom je ľubovoľný väčší nákupný reťazec, ktorý využíva na predaj svojich produktov čiarové kódy. Ak by mala všetky zakúpené tovary kontrolovať a účtovať obsluha bolo by to zdĺhavé, neefektívne a pravdepodobne chybové. Ďalším príkladom je aj početnosť ľudí na svete, ktorá pribúda exponenciálnym rastom. Pri aktuálnej populácií 8 mld. obyvateľov by bolo extrémne náročné dokonca priam nemožné bezpečne ustriehnuť všetky internetové operácie ako sú aj bankové prevody atď. Z ďalšieho hľadiska, skôr materiálnej ochrany, nachádza využitie systém EPS pri automatickej detekcií a včasnej eliminácií požiaru.

Využitie EZS je naozaj široké a vplyvom dnešnej chamtivej doby čím ďalej viac žiadúce. Práve na tento druh útoku je zameraná táto bakalárska práca, kedy je nositeľom hrozby samotný človek. Časom si ľudia uvedomili, že na získanie aktív existuje jednoduchšia a rýchlejšia cesta, akou je "krádež". Na ochranu pred týmto druhom hrozby bolo potrebné vymyslieť sofistikovanejšie systémy ako sú len mechanické zábrany, ktoré dokázal človek jednoducho prekonať. Bezpečnostný systém na ochranu pred vlámaním siaha až do roku 1858, kedy E. T. Holmes vyhotovil prvý poplachový zabezpečovací systém v Bostone i v New Yorku pre budovy, v ktorých neustále monitoroval stav [1].

V Českej republike je hlavným predstaviteľom v priemysle EZS svetoznáma 33 ročná firma na zabezpečovacie systémy Jablotron so sídlom v Jablonci nad Nisou. Jej špecializácia sa zameriava na PZS, EKV a DVS pričom sa orientuje len na vývoj vlastnej elektroniky a na výskum nových technológií.

1.2.2 Norma ČSN EN 5013x

Elektronické zabezpečovacie systémy v ČR sa od roku 1997 riadili podla normy ČSN EN 5013x. Z dôvodu inovácií a komplikácie jednotlivých systémov sa na vydávaní noriem uplatňujú rôzne pracovné skupiny.[1]. Norma ČSN EN 5013x štandardizuje (EZS) na nasledujúce odvetvia poplašných systémov:

1. 50130 – Poplachové systémy (PS)
2. 50131 – Poplachové zabezpečovacie a tiesňové systémy (PZTS) podľa novej normy.
3. 50132 – Dohľadné systémy (CCTV)/ uzavretý televízny okruh. Problematiku CCTV postupne preberajú štandardy normy 62676 (DVS) dohľadové video systémy.
4. 50133 – Elektronický systém kontroly vstupu (EKV) => ČSN EN 60839.
5. 50134 – Systém privolania pomoci
6. 50135 – Tiesňové systémy. Norma bola zrušená a prevedená do rady 50131.
7. 50136 – Poplachové prenosové systémy a zariadenia.
8. 50398 – Kombinované a integrované systémy (kombinácia viac druhov poplašných systémov alebo kombinácia s inými systémami)
9. 54 – Elektronická požiarna signalizácia (EPS).[1]

1.3 Architektúra a štruktúra EZS

Základom pri každom návrhu systému EZS je potrebné stanoviť výšku formy ochrany pre primerané zvolenie stupňa zabezpečenia podľa rizika ohrozenia. Podľa normy ČSN EN 50131 sa delí zabezpečenie na 4 stupne:

Tab. 1.1: Stupne zabezpečenia objektu

STUPEŇ	RIZIKO	ZNALOSŤ ÚTOČNÍKA O EZS
1.	Nízke	Malá
2.	Nízke až stredné	Určitá
3.	Stredné až vysoké	Dobrá
4.	Vysoké	Expertná

1. Stupeň – Útočník disponuje len obyčajnými nástrojmi (kameň, páčidlo). Typickým príkladom chráneného objektu je rodinný dom alebo chata uprostred lesa.

2. Stupeň – Útočník disponuje základným sortimentom nástrojov (rebrík, skrutkovače, multimeter) a má určité znalosti o EZS. Chráneným objektom môžu byť kancelárske alebo komerčné budovy.

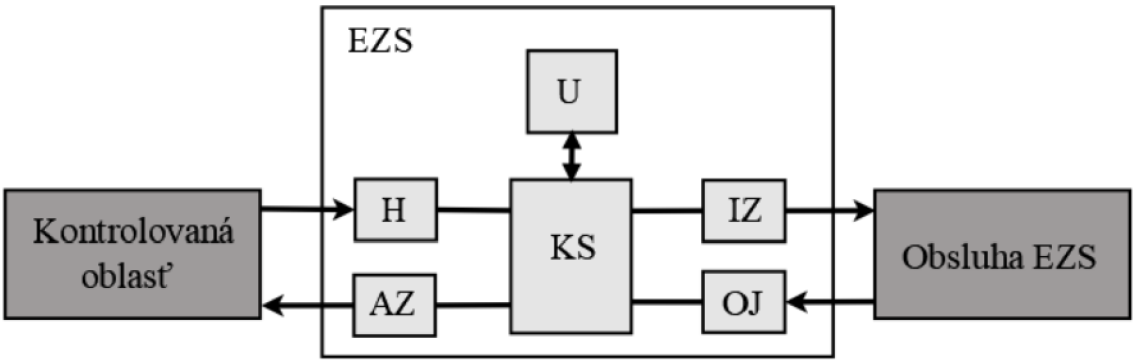
3. Stupeň – Útočník disponuje úplným sortimentom špecializovaných nástrojov (detacher, neodymové magnety, špecializované multimetre). V tomto stupni zabezpečenia sa chránia napríklad banky.

4. Stupeň – Útočník disponuje rovnakým sortimentom ako pri stupni 3, ale navyše má vo vybavení prostriedky na výmenu alebo odrušenie rozhodujúcich prvkov EZS ako sú hlásiče.[2]

Na základe stupňa zabezpečenia môže inštalačný projektant navrhnúť elektronický zabezpečovací systém presne na mieru pre daný chránený objekt. Podmienkou mu je dodržanie stupňa zabezpečenia u všetkých použitých komponentov.

1.3.1 Popis prvkov EZS

Každý elektronický zabezpečovací systém sa skladá z určitých prvkov/komponentov potrebných na jeho fungovanie. Každý prvok a komponenta zohrávajú v navrhovanej architektúre istú úlohu, či už základnú–funkčnú alebo doplnkovú–rozširujúcu. Celková štruktúra systému EZS je vyobrazená na (obrázku č.1.1)



Obr. 1.1: Štruktúra architektúry EZS

1. Ústredňa [U]: Hlavnou riadiacou jednotkou a vôbec hlavou celého bezpečnostného systému je ústredňa. Od nej závisia vlastnosti a možnosti EZS, akými bude disponovať. Jej úlohou je prijímať signály od pripojených periférií, na základe nich vyhodnotiť možný vznik incidentu a následne vykonať podľa programu patričnú akciu. Každá ústredňa je jedinečná a do chránených oblastí sa volí ako prvá na základe parametrov a potenciálneho využitia. Skladá sa zo základnej DPS, záložného zdroja (UPS) pre prípad výpadku sieťového napájacieho napätia, rozširujúcich modulov,

a transformátora na napájanie ústredne. Periférie sa do ústredne pripájajú buď káblovo alebo bezdrôtovo. Ústredňa tiež zohráva v EZS opornú a ochrannú funkciu, kedy chráni všetky v nej uložené komponenty pred vonkajším vplyvmi a zároveň poskytuje komponentom dostatočný priestor pre prehľadné a konštrukčne efektívne rozloženie.

2. Hlásiče [H]: Ich úlohou je snímať aktuálny stav v chránenej oblasti a pravidelne podávať hlásenie ústredni, o možných vznikoch incidentu. Incidentom sa rozumie nielen neautorizované vykonávanie nepovolených úkonov (poplach, sabotáž), ale i vznik nevhodného prostredia v kontrolovanej oblasti, ako je požiar, únik vody či plynu. Na snímanie sa spravidla používajú zmeny vhodných fyzikálnych veličín ako sú teplota, tlak či intenzita hlasitosti. Hlásiče sa podľa spôsobu spracovávania snímaných veličín delia na detektory a senzory:

- Senzor – posiela ústredni alebo obsluhe nameranú hodnotu a tá vyhodnotí príznaky incidentu.
- Detektor – sám spracuje nameranú hodnotu a ústredni zasiela už len hlásenie o vzniku incidentu.

Všetky hlásiče a prvky EZS samozrejme musia podliehať podmienke na splnenie stupňa zabezpečenia objektu. [1]

3. Informačné zariadenia [**IZ**]: Slúžia na podávanie informácií o aktuálnom stave ochrany stráženého objektu alebo na interakciu s užívateľom. Existujú rôzne typy IZ a všetky disponujú špecifickými parametrami na základe, ktorých si autorita zvolí akým spôsobom chce dostávať informácie. V súčastnosti sa pre informačné účely stále viac využíva výpočtová technika (PC, smartphone), čo zjednodušuje správu systému zo strany PCO ako aj užívateľa. Príkladom je prezentovanie poplachu, kedy sa nerozozvučí alarm ale vyšle varovný signál do PCO alebo priamo vybranej bezpečnostnej inštitúcií. Vizuálno - akustické periférie sú však stále využívané vo veľkej miere a väčšinou zohrávajú úlohu doprevádzajúcich IZ.[1]

4. Akčné zariadenia [**AZ**]: Jedná sa o všetky členy vykonávajúce elektromechanickú prácu. Radí sa sem elektrický zámok, osvetlenie, ovládanie žalúzií, protipožiarne vybavenie či rôzne odstrašujúce zariadenia pri útoku (napr.dymostroj). AZ sú riadené prostredníctvom ústredne na základe vopred stanoveného algoritmu, ale najnovšie vznikajú aj bezústredňové AZ, ktorým stačí pripojenie na vstupný terminál.

5. Ovládacie jednotky [**OJ**]: V závislosti na možnostiach ústredni a požiadavkách konkrétnej realizácie EZS je možné do systému implementovať i prídavné

ovládacie jednotky pomocou ktorých je obsluha schopná ovládať rôzne akčné zariadenia. K ovládaniu zabezpečovacieho systému sa používajú klávesnice, dátové výpočtové zariadenia ako PC umiestnený v PCO alebo terajší trend v jednoduchosti prevedenia ovládania systému, pomocou smartphonu.[1]

6. Komunikačný systém [KS] slúži na vzájomné prepojenie ústredne so všetkými komponentami a perifériami pre prenos signálov, hlásení a príkazov. Delenie KS podľa pripájania periférie:

- Káblový – priame prepojenie periférií a ústredni prostredníctvom vodiča (stále prevládajúci typ)
- Bezdrôtový – rádiová komunikácia (Prenosové pásmo 434 a 868 MHz)

V blízkej budúcnosti sa pravdepodobne dostane do popredia trend unifikácie komunikačných systémov a ako vhodným kandidátom pre zvládnutie tejto funkcie sa ukazuje široko používané rozhranie Ethernet.

Rozdelenie podľa dnešnej štandardizácie KS EZS:

1. Systém PZS a EPS:
   - linky pre komunikáciu s hlásičmi (prúdové slučky a zbernice)
   - linky pre spustenie výstražných zariadení (dvoj-stavové slučky)
   - linky pre spojenie s PCO (káblové alebo rádiové spoje)
2. Systém EKV:
   - linky pre komunikáciu s terminálom (zbernica RS-485)
   - linky pre ovládanie akčných členov (holé vodiče + GND)
3. Systém DVI:
   - analógový signál – štandard NTSC/PAL (Koaxiálny kábel)
   - digitálny signál – Ethernet (UTP)[1]

1.4 Rozdelenie periférií

Periférиami možno uvažovať všetky zariadenia alebo moduly, ktoré sa pripájajú na maticovú dosku ústredni (H, IZ, AZ, OJ).

Drôtové/Bezdrôtové

1. <u>Drôtové</u> – Na komunikáciu s ústredňou sa pripájajú pomocou metalických vodičov o stanovenom priereze (zvyčajne $1\,mm^2$).
   Výhody => Lacnejšia varianta periférií; jednoduché prevedenie zapojení (prúdové slučky, zbernice); stabilita spojenia...

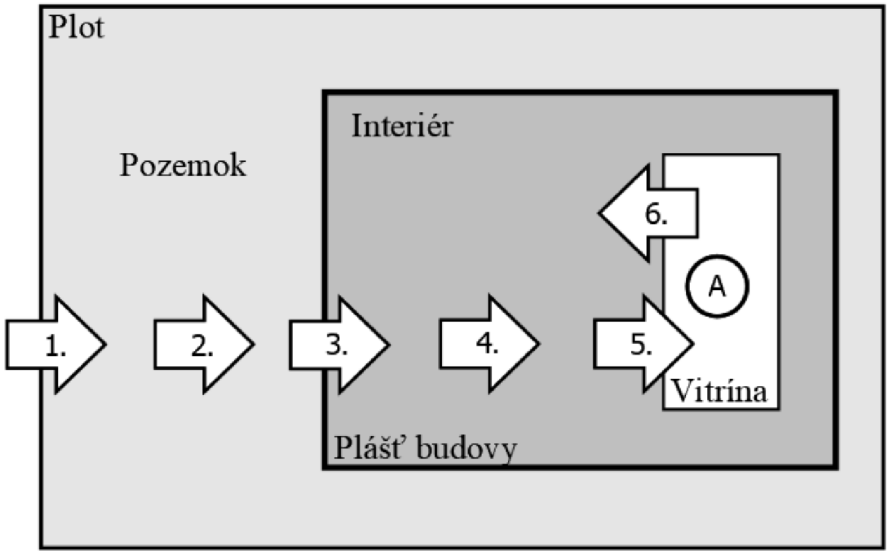
Nevýhody => Nutnosť vedenia káblov ku každému zariadeniu (vzdialenosť obmedzená, s rastúcou vzdialenosťou aj vyššia cena).

2. Bezdrôtové – Na komunikáciu s ústredňou využívajú rádiové pásmo o frekvencií 434 alebo 868 MHz.
   Výhody => Jednoduchšia inštalácia (stačí osadiť a zapnúť); nie je potrebné viesť ku perifériám vodiče; vysoký dosah $\approx 300m$.
   Nevýhody => Menšia stabilita prepojenia s ústredňou; nutné dosadiť rádiový komunikačný modul; náchylnosť na rušenie (ich veľká slabina); potreba zaobstarania batérií pre chod zariadení; vyššia cena oproti bezdrôtovým.

3. Kontaktné – Spravidla sa jedná o vývodové rozširujúce moduly pre ústredňu. Aplikujú sa jednoduchým zasunutím vývodov do vopred pripravených soketov na základnej doske. Komunikácia je okamžitá a stabilná. Umožňujú ústredni rozšírenie drôtových slučkových vstupov alebo pridanie nových komunikačných sfér ako s detektormi, tak i s užívateľmi.

1.4.1 Detektory (hlásiče) - klasifikácia

- intrúzne – [povinné] detegujú neoprávnenú aktivitu osôb.
- požiarne – [voliteľné] detegujú vznik požiaru.
- tiesňové – [voliteľné] detegujú tiesňové situácie.
- substančné – [voliteľné] detegujú nežiadúce látky (únik plynu/vody).



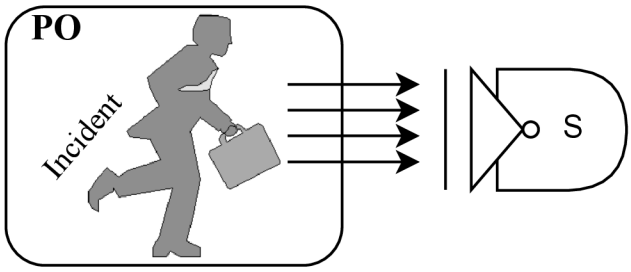
Obr. 1.2: Príklad viacvrstvovej ochrany[2]

Pri detektoroch sa prevažne využíva stratégia viacvrstvovej ochrany. To znamená, že aktíva (A) sú obklopené viacerými líniami prekážok a detektorov. Názorné

zobrazenie jednotlivých ochranných línií je na obrázku č.1.2. V každej línií dokáže EZS detegovať možný vznik incidentu/útoku, pričom v každej sa používa iný typ detektorov na detekciu jeho mechanizmu.
Systém navrhovaný v tejto práci je určený pre ochranné línie 3 alebo 5, kedy je prekážkou plášť budovy, miestnosti alebo objektu.

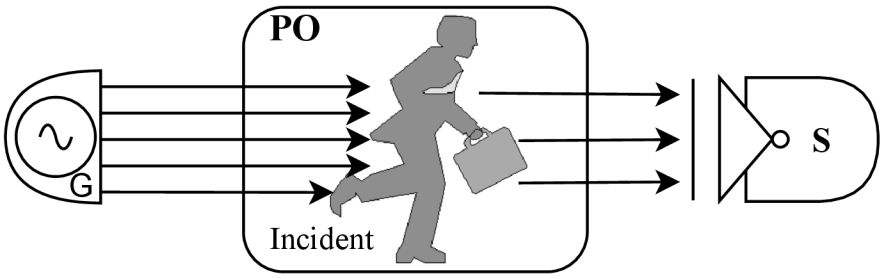
Detektory - delenie:

1. Objektové – Sú určené na detegovanie manipulácie útočníka s objektami. Môže sa jednať o cenné aktíva, ale i prekážky tvoriace bariéru vo vrstvovej ochrane. Ďalšie členenie objektových detektorov:
   - predmetové – určené na detekciu neoprávnenej manipulácie s predmetmi/aktívami.
   - prekážkové – určené na detekciu neoprávneného prekročenia alebo manipulácie s prekážkou.
2. Priestorové – Sú určené na detegovanie útočníka pohybujúceho sa v kontrolovanej oblasti. Tieto detektory fungujú na snímaní fyzikálnych veličín ako sú teplota alebo mikrovlnné vlnenie. Dôležitým pojmom pri priestorových detektoroch je detekčný diagram (obrázok.1.5).[3]
3. Vnútorné – Sú určené pre suché, vnútorné podmienky, čo znamená, že nemusia spĺňať normy pre vonkajšie použitie ($IP44$). Ich cena je rádovo nižšia od vonkajších detektorov, nakoľko nemusia riešiť zložité poveternostné podmienky. Na druhú ranu prípadný incident zachytia až v interiéri stráženého objektu.[3]
4. Vonkajšie – Sú určené pre vonkajšie použitie. Z toho hľadiska sú nadimenzované tak, aby dokázali pracovať za všetkých poveternostných podmienok. Musia zvládať veľký rozsah teplôt, dážď, sneh, hmlisté počasie či silný vietor a navyše k tomu musia čeliť množstvu iných nežiadúcich udalostí, ktoré môžu pôsobiť ako falošné zdroje poplachov (napr. zver, pohyb konárov). Tieto zdroje musia vedieť odfiltrovať, čoho následkom je ich zložitejšie prevedenie a vyššia cena.[3]
5. Pasívne – Využívajú príznaky incidentu priamo ako zdroj meranej veličiny. Rozumie sa tým teplota alebo akustická vlna vybudená od detegovaného objektu. Formálne vyjadrenie aktívnych detektorov možno zapísať v tvare $P = F(I)$. Pričom P je príznak, F je známe ako funkcia a I je incident. Príkladnými pasívnymi detektormi sú napríklad detektor rozbitia skla alebo detektor pohybu PIR. Názorné zobrazenie princípu funkcie pasívneho detektora je na obrázku č.1.3 pričom S => senzor, PO => príznaková oblasť.[3]



Obr. 1.3: Princíp pasívneho detektora

6. Aktívne – Na ich funkciu nestačí len príznak incidentu, ale potrebujú externý generátor ako zdroj budiacej energie pre prijímací senzor detektora. Formálne vyjadrenie vyzerá v tvare $P = F(E, I)$, pričom podobne ako v predošlom prípade P je príznak, F je matematicky funkcia, I je incident plus dodaná je ďalšia zložka E ako budiaca energia od generátora. Táto budiaca energia môže byť napríklad vo forme IR žiarenia. Príkladnými aktívnymi detektormi sú magnetický detektor otvorenia alebo infračervená závora. Názorné zobrazenie princípu funkcie aktívneho detektora je na obrázku č.1.4 pričom S => senzor, PO => príznaková oblasť, G => generátor budiacej energie.[3]



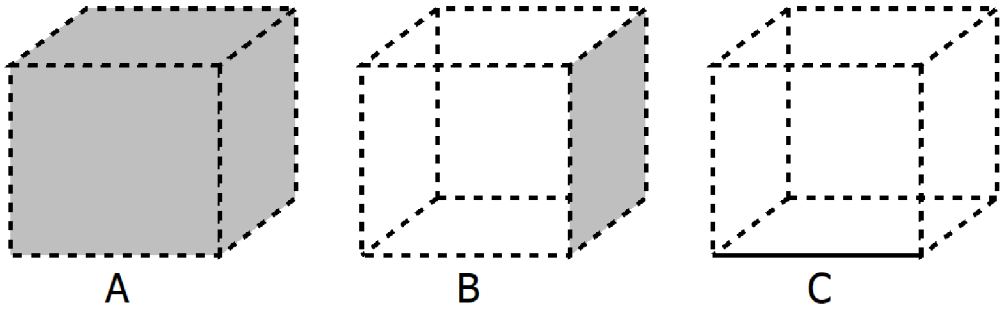
Obr. 1.4: Princíp aktívneho detektora

1.4.2 Detekčný diagram

Definuje akú časť priestoru (detekčnú oblasť – DO) bude daný detektor schopný detegovať. [3] Delenie:

- Objemové (volumetrické detektory) – Ich snímacou oblasťou je trojrozmerná geometrická dimenzia. Ak sa začne niekde v tomto priestore útočník pohybovať, ústredňa vyhlási poplach.

- Hraničné (líniové detektory) – Ich detekčný diagram je v tvare plochy alebo línie (virtuálna hranica), ktorú keď útočník prekročí vyhlási ústredňa poplach.



Obr. 1.5: A - DO je priestor, B - DO je plocha, C - DO je línia

1.4.3 Príklady intrúznych detektorov

Tab. 1.2: Konkrétne typy jednotlivých detektorov

OBJEKTOVÉ DETEKTORY		PRIESTOROVÉ DETEKTORY	
Predmetové	Prekážkové	Objemové	Hraničné
1. Tiažové	1. MD otvorenia	1. PIR	1. IR bariéra
2. Akceleračné	2. GBS, otrasový	2. MW	2. MW bariéra

MW – mikrovlnná, GBS – glass break sensor, IR – infračervený

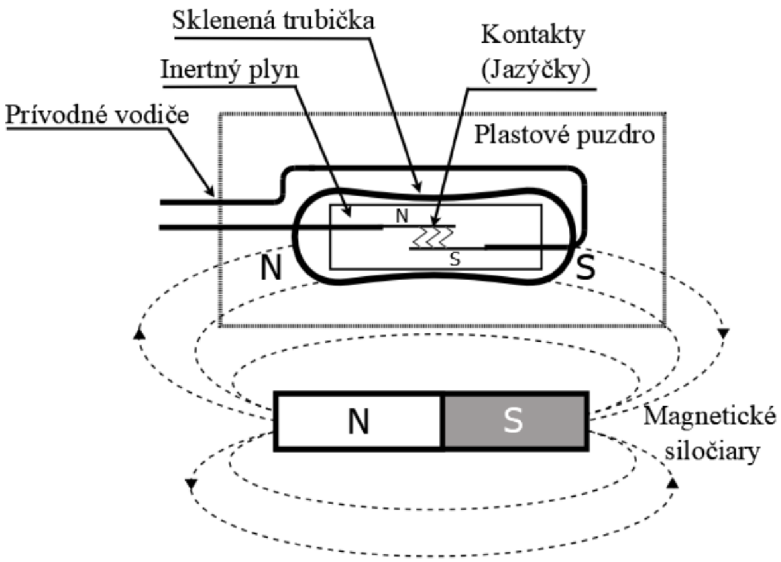
1. Objektový-prekážkový magnetický detektor otvorenia

Magnetické detektory otvorenia (MD) sú určené na detekciu otvorenia akejkoľvek výplne (najčastejšie sa uvažujú dvere, okná) v plášti ochrannej bariéry objektu ako sú vitrína, steny budovy alebo rôzne iné prekážky. Magnetické detektory sú direktné aktívne typy detektorov. Ich vysielačom je permanentný magnet a prijímačom magnetický kontakt. Jedná sa teda o spínač ovládaný magnetickým poľom, ktorý je v kľudovom stave zabezpečenia zatvorený. Vysielač a prijímač sa musia inštalovať do tesnej blízkosti na jedno krídlo otváraného objektu v miestne najrýchlejšieho otvorenia. V prípade dverí je to na koniec krídla, kde už aj pri malom odchýlení dverí dôjde ku oddialeniu prijímača od vysielača, čím zanikne magnetické pole v prijímači, kontakt sa rozpojí a ústredňa vyhlási poplach.

V zabezpečovacích systémoch je magnetický detektor obzvlášť používanou periériou. Inštaluje sa už od 1. stupňa zabezpečenia na obvodové dvere a pri 2. stupni zabezpečenia navyše aj na okná a ostatné otvory. V praxi existujú dve prevedenia magnetických detektorov:

- Jazýčkový [reed switch] – Jeho jadrom sú dva prepružené vodiče z magneticky-mäkkého materiálu na jednom konci sploštené do podoby plochých kontaktov

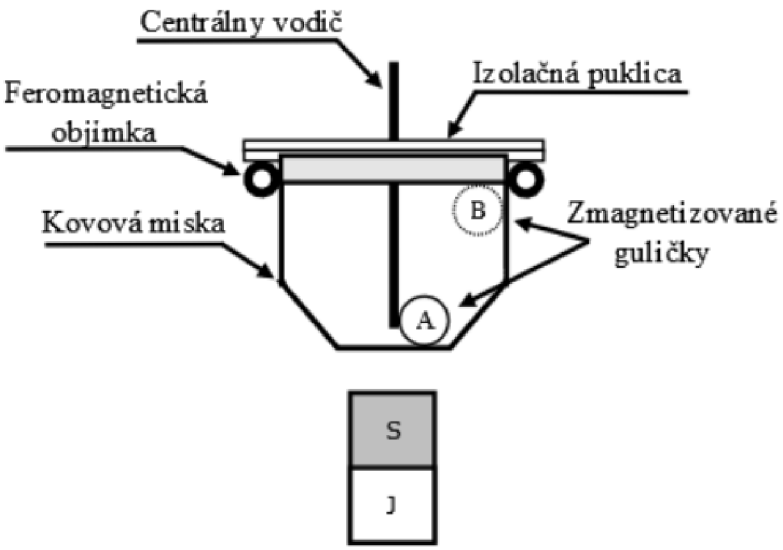
”jazýčkov”. Obidva kontakty sú hermeticky zapúzdrené a zatavené v sklenenej trubičke naplnenej inertným plynom (dusík) na zamedzenie korózií kontaktov. Pre-pruženie jazýčkov kontaktov je zámerné, aby za normálnych okolností, kedy nie je ku prijímaču priložený magnet, boli od seba oddialené a tým kontakt rozpojený**NO** (Normal Open). Po priložení magnetu ku kontaktom sa ich konce skrz prívodné vodiče zmagnetizujú inou polaritou a preto sa ku sebe pritiahnu. Spojí sa tým elektrický kontakt a začne pretekať slučkou prúd. Po následnom oddialení magnetu od kontaktov, magnetické pole zanikne, kontakty sa rozpoja a elektrický prúd prestane tiecť. Tento zánik prúdu zaznamená ústredňa, ktorá vzápätí vyhlási poplach. Vyobrazenie zloženia a princípu fungovania jazýčkového MD (viď. obrázok 1.6).[2]



Obr. 1.6: Jazýčkový magnetický detektor

- Guľôčkový – Je vylepšeným typom magnetického detektoru, ktorý eliminuje prípadné útoky permanentného priloženia magnetu z bočnej strany detektoru. Zatiaľ čo pri jazýčkovom MD bolo jedno z akej strany sa k nemu magnet priloží aby sa kontakty spojili, pri guľôčkovom je prípustná iba jedna strana a to pred detektorom. Guľôčkový MD sa skladá z kovovej misky, zmagnetizovanej guľôčky, feromagnetickej objímky, izolačnej puklici a centrálneho vodiča. Miska tvorí jeden kontakt detektoru a centrálny vodič je kontaktom druhým. Guľôčka potom hrá rolu spínača medzi týmito dvomi kontaktmi. Keď sa priloží magnet na spodnú stranu misky, pritiahne k sebe zmagnetizovanú guličku (viď. guľka A, obrázok 1.7), ktorá prepojí misku s centrálnym vodičom a tým uzavrie prúdovú slučku, ktorou môže pretekať prúd. Pri následnom odobratí

magnetu (otvorenie dverí) spadne gulička naspäť do vnútra misky (viď. guľka B, obrázok1.7) vplyvom gravitácie a magnetickej príťažlivosti feromagnetickej objímky, čím sa rozpojí kontakt a prúd zanikne, čo centrála vyhodnotí ako poplach.[2]



Obr. 1.7: Guľôčkový magnetický detektor

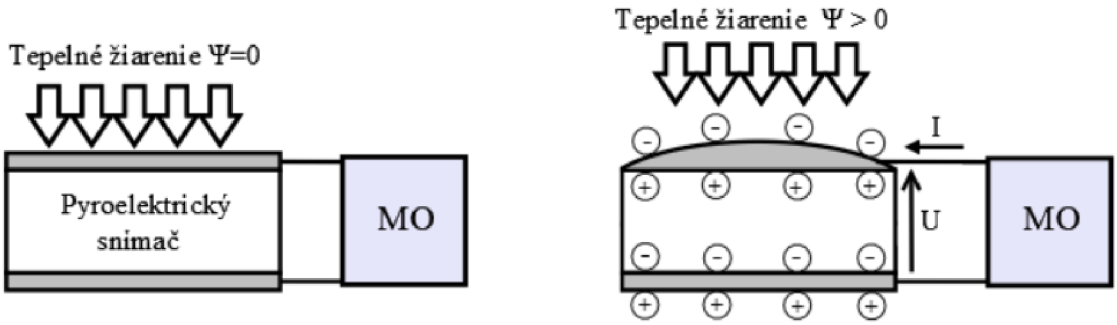
2. Priestorový-objemový pasívny infračervený detektor

PIR (Passive InfraRed) detektor využíva ako budiacu energiu príznak incidentu v podobe infračerveného žiarenie tepelných objektov. Samozrejme nemusí sa jednať len o hmotné objekty. Detektor zachytí všetky teplotné IR zmeny v okolí teplôt $37°C$, čo je približne teplota ľudského tela. Nemal by sa inštalovať v priestoroch so sálajúcim teplým vzduchom napríklad z kúrenia alebo pred iné tepelné zariadenia, aby nedochádzalo ku možnému vzniku falošných poplachov.

Hlavným stavebným prvkom každého detektoru PIR je pyroelektrický snímač (viď. obrázok1.8). Je to tenká doštička s postrannými elektródami citlivá na teplo. Keď na hornú alebo dolnú elektródu pyroelektrického snímača dopadne tepelné žiarenie s intenzitou Ψ, tak sa doštička vplyvom teplotnej rozťažnosti vyduje a vznikne z pyroelektrika elementárny dipól. Tento vznik dipólu zapríčiní, že sa na doštičkách objavia opačne nabité náboje a rozdiel potenciálov týchto nábojov je prezentovaný ako výstupné napätie U [V]. Pokiaľ by sa na doštičku napojil rezistor s odporom R [Ω], začne ním pretekať prúd I, ktorý možno vypočítať z Ohmovho zákona ako: $I = U/R$ [A]. Tento prúd je možné ďalej spracovať v riadiacej logike detektoru na základe čoho sa vyhodnotí vznik incidentu.

V PIR detektoroch je zabudovaný navyše filter, ktorý sa obmedzuje vstupné pásmo dopadajúceho žiarenia v rozmedzí 9,4 až 10 μm, čo je vlnová dĺžka najviac

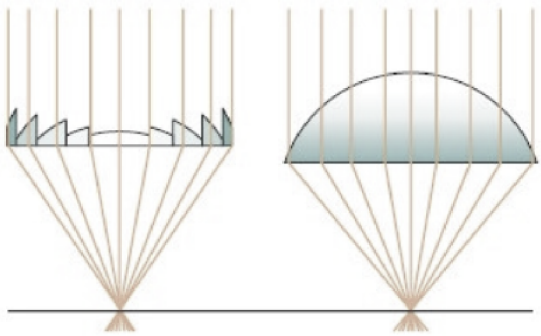
vyžarovaná objektmi s teplotou okolo $37°C$. Z toho bol odvodený názov detektoru PIR, nakoľko žiarenie o tejto vlnovej dĺžke sa radí v spektre elektromagnetického žiarenia už medzi infračervené.



Obr. 1.8: Princíp pyroelektrického snímača

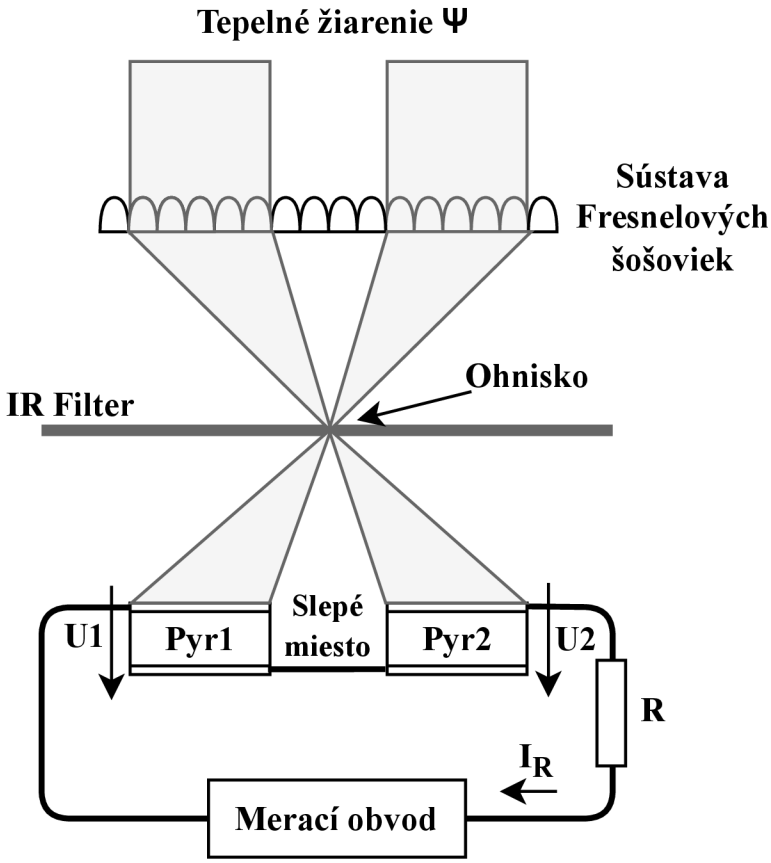
U PIR detektorov sa používajú na snímanie incidentu dva pyroelektrické snímače, ktoré sú zapojené v diferenčnom zapojení, aby sa eliminovali rušenia. Keďže potenciál u obidvoch snímačov rastie priamo úmerne, rozdielové zapojenie sa postará o to, aby sa tieto napäťové úrovne udržiavali v rovnováhe. V prípade detekcie útočníka dôjde ku rozváženiu napäťového pomeru medzi snímačmi, čo detektor vyhodnotí ako incident a pošle ústredni hlásenie. Rozdielovým zapojením sa síce zamedzilo prípadným falošným poplachom, ale zároveň sa zredukovalo zorné pole na detekciu útočníka, keďže tepelné žiarenie od osoby dopadá na obidve doštičky súčasne.

Na vyriešenie tohoto problému sa používajú fyzikálne zákony optiky. Tá dokáže svetlo rozptýliť alebo spojiť v závislosti od jej tvaru a navyše zväčšuje rozhľadový dosah a spoľahlivosť detektorov podobne ako okuliare u človeka. Detektory PIR využívajú sústavu Fresnelových (čit. Frenelových) šošoviek, čo je modifikovaná konvexná spojovacia šošovka (spojka) zborená do seba. Výhodou je jej tenkosť oproti obyčajnej šošovke a teda má menšie straty pri prechode IR žiarenia. Menej používaná je sústava parabolických zrkadiel.



Obr. 1.9: Lom svetla šošovky, vľavo Fresnelova, vpravo Konvexná

Ako vidieť na obrázku 1.9, princíp lomu svetla zostal pri Fresnelovej šošovke rovnaký ako pri konvexnej spojke iba s rozdielom väčšej ohniskovej vzdialenosti. Fresnelové šošovky sa vyrábajú z materiálu PTFE (teflon) a usporadúvajú sa do sústav s rôznym detekčným diagramom. Odlišujú sa vo veľkosti snímacieho uhlu, v dosahu snímania či v počte lalokov (zón snímania). Každá šošovka vytvorí 2 laloky.



Obr. 1.10: Vnútorná konštrukcia prvkov detektora PIR

Z hľadiska praktického využitia sa PIR detektory delia aj na základe použitej šošovky.

- Klasické – detekčný snímací uhol je široký (zvyčajne 120°) s hustým rozložením šikmo sklopených vejárov, čo obmedzuje detekčnú vzdialenosť do cca. 15 m.

- Chodbové – detekčným diagramom sú veľmi úzke ale dlhé vejáre. Rádovo > 40 m. V blízkosti detektoru sú však detekčné vejáre rozložené v širšom uhle.

- Záclonové – detekčný diagram tvoria vertikálne 2 úzke snímacia zóny do dosahu približne 13 m a výške > 3 m. Sú určené na detekciu pokusu útočníka o prechod

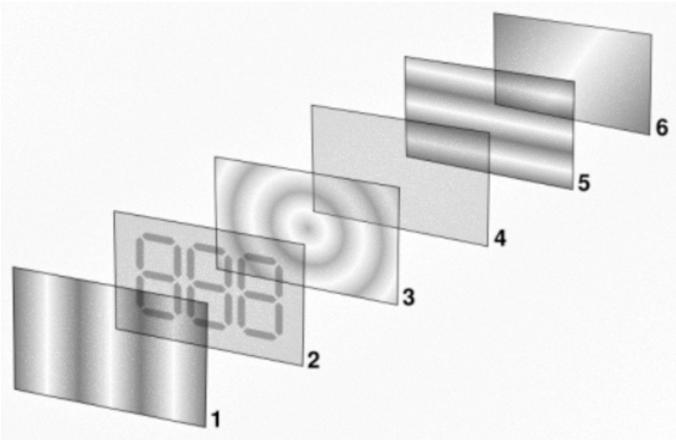
cez strechu či okno.

1.4.4 Informačné zariadenia

LCD displej

Pre vytvorenie textového, grafického rozhrania na interakciu s užívateľom sa používajú dispeleje. Sú to zariadenia na zobrazovanie informácií (text, obrázky) v elektronickej digitálnej podobe. Delia sa podľa spôsobu zobrazovania a použitia napríklad na 7-segmentové, LCD, LED-DOT, OLED a mnohé iné.

Do tejto práce najviac vyhovuje spomedzi vymenovaných, displej LCD.
(z ang. Liquid crystal display) je tenké ploché zobrazovacie zariadenie skladajúce sa z obmedzeného počtu farebných alebo monochromatických pixelov zaradených pred zdrojom svetla (reflektorom) 1.11. Každý pixel LCD displeja sa skladá z molekúl tekutých kryštálov (od toho liquid crystal), uložených medzi dvomi priehľadnými elektródami. Tie sú navyše obalené navzájom kolmými polarizačnými filtrami pre umožnenie priameho priechodu svetla. Po privedení napätia na molekuly tekutých kryštálov sú ich pozície ťahané a stáčané rovnobežne so smerom elektrického poľa, čo znižuje rotáciu vstupného svetla. Pomocou rotácie kryštálov teda možno korigovať svietivosť jednotlivých pixelov.[4]



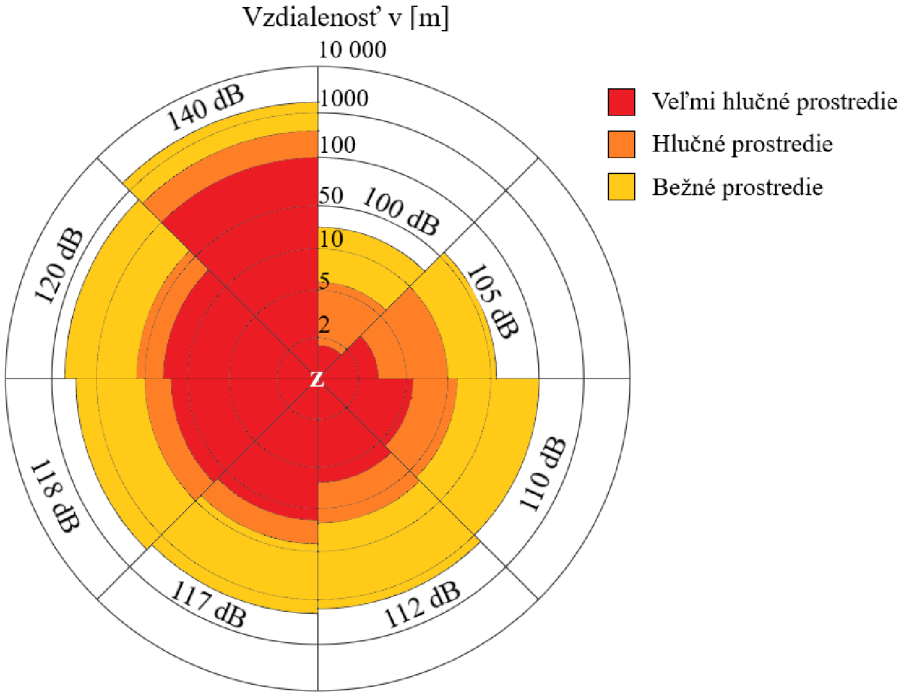
Obr. 1.11: Štruktúra twisted nematic displeja. [5]

1 a 5 => polarizačné filtre, 2 a 4 => substrát s elektródami, 3 => vrstva tekutých krištáľov, 6 => zdroj svetla.

Ich výhodou je nízka spotrebe energie, čo je praktické i pre použitie v aplikáciách z batériového napájania. LCD displeje sa vyrábajú v rôznych veľkostiach (16x2, 20x4) a prevedeniach, najčastejšie už v zabudovaných DPS embedded moduloch, ktoré v sebe zahŕňajú obstarávaciu logiku pre chod displeja.

Siréna

Sirény alebo presnejšie akustické meniče boli vôbec prvým informačným prvkom v EZS. Ich funkciu síce dokonalejšie preberajú novšie periférie, ale z pohľadu notorika sa bez nich zabezpečovací systém nedá predstaviť. V začiatkoch sa pre akustické poplachy využívali klasické elektronické zvonce, ktoré po rozpojení dverového kontaktu spustili vyzváňanie. Pre dnešné účely poplachovej signalizácie sa využívajú piezosirény s variabilnou úrovňou hlasitosti podľa situačného prostredia. Úroveň hlasitosti sa udáva v decibeloch [dB] a určuje akustickú silu (PSL), do akej vzdialenosti bude mať konkrétna siréna dosah (viď. obrázok 1.12 závislosť úrovne hlasitosti na vzdialenosti od zdroja [Z]). Pri výbere treba tiež zohľadniť umiestnenie sirény.



Obr. 1.12: Účinný dosah sirén v závislosti na úrovni hlasitosti[6]

GSM komunikátory

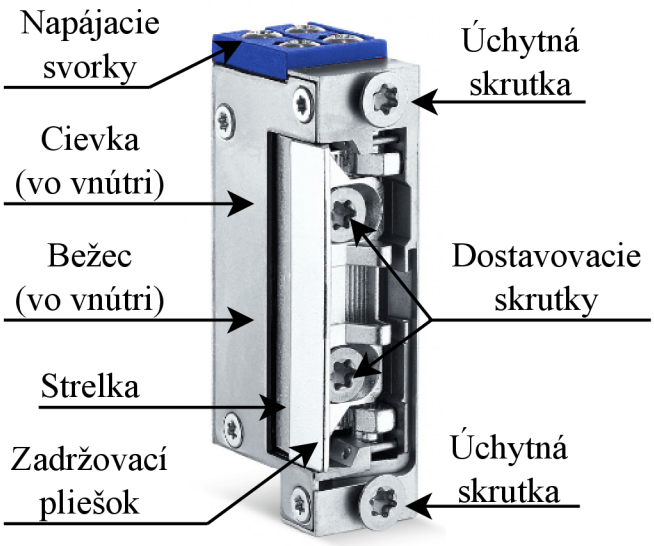
Z franc. (Groupe Spécial Mobile) je GSM najrozšírenejší štandard na svete pre komunikovanie medzi mobilnými telefónmi. Vytvoril ho Európsky ústav pre telekomunikačné normy (ETSI), ktorý mu dal pomenovanie, mobilný systém druhej generácie tiež označovaný ako 2G. Postupom času ho nahradila sieť tretej generácie 3G, štvrtej 4G a najnovšie piatej generácie 5G. Na svoju činnosť systém využíva mnoho prenosových frekvencií. V Európe sa napríklad využívajú 900 MHz a 1800 MHz. GSM sieť sa ďalej delí na 4 frekvenčné pásma, z ktorých každé disponuje istým počtom kanálov a má určené presné frekvencie pre uplink a downlink.

Komunikátory GSM teda ponúkajú možnosť rozšíriť funkcie ústredne o ďalšiu komunikačnú cestu. Základnými rozhodujúcimi parametrami pre výber GSM modulu sú kompatibilita s mikrokontrolérom, pracovné napätie a prenosové pásmo.

1.4.5 Akčné zariadenia

Elektrický zámok

EZ nahradzuje štandardnú pevnú západku v zárubni dverí, do ktorej vchádza strelka zámku. Jeho úlohou je uvolniť túto západku v momente, keď na to ústredňa vyšle povoľovací signál a tým sprístupniť otvorenie dverí. Každý EZ sa skladá z budiacej cievky, strelky, bežca a zadržiavacieho pliešku (viď. obrázok 1.13). Po privedení požadovaného napätia na napájacie svorky EZ sa v cievke naindukuje napätie, ktoré v cievke vyvolá tok prúdu. Ako vieme z Faradayovho indukčného zákona, tok prúdu vo vodiči vyvolá magnetické pole. Z cievky sa tak stane elektromagnet, ktorý spôsobí pritiahnutie bežca. Tento bežec uvolní miesto pre zapadnutie strelky do vnútra EZ. Tým uvoľní zároveň cestu pre zadržiavací pliešok dverového zámku a dvere možno jednoducho otvoriť. EZ sú spoľahlivé a ich využitie je všestranné. Na ich správnu funkciu je potrebné vybaviť EZ spoľahlivým riadiacim obvodom.



Obr. 1.13: Elektrický vrátnik IQ eStrike, A5000-A[7]

1.4.6 Ovládacie jednotky

Klávesnica

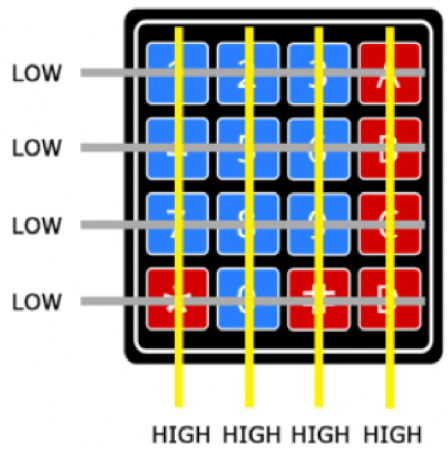
Je univerzálne vstupné zariadenie, ako pre riadenie/správu systému, tak aj pre autentizáciu. Využiť sa dá všade, kde je požiadavka na prehľadné ovládanie viacerých funkcií. Skladá sa zo skupiny tlačidiel dizajnovaných najčastejšie do maticového, štvorcového alebo obdĺžnikového tvaru. Samozrejme je možné dizajn ľubovoľne pozmeniť podľa aplikácie. Na trhu existuje viacero typov klávesníc.[8]

1. **Čiste mechanické klávesnice** – Hlavným prvkom sú mechanické spínače s pružinovým mechanizmom.
2. **Mechanické s penovým prvkom** – Namiesto pružiny využíva penový prvok. Nepoužíva sa (nepočuť stláčanie = neistý stisk kláves).
3. **Mechanické s gumenou membránou** – Pružina a penový prvok nahradený gumou. Takmer všetky lacnejšie PC klávesnice. Dlhá životnosť.
4. **Membránové** – Podobné klávesniciam s gumenou membránou. Klávesy nie sú od seba oddelené. Odolné voči zaneseniu nečistôt. Krátka životnosť (cca. 10 miliónov stlačení).
5. **Magnetické** – Pod klávesami sú umiestnené Hallové sondy na snímanie stlačenia. Pri stlačení klávesy sa jej magnet priblíži k sonde a vzrast magnetického poľa vygeneruje impulz. Môžu byť celkom vodotesné.
6. **Senzorické** – Sú tvorené dvomi kontaktmi blízko pri sebe. Stláčanie sa prevádza priložením vodivého prstu, ktorý prepojí kontakty.
7. **Kapacitné** – Využívajú kapacitu medzi pevnou elektródou a pružnou membránou. Stlačením klávesy prudko vzrastie kapacita, čo je jednoducho merateľné.
8. **Optické** – Stlačenie klávesov môže byť delegované prerušovaním svetelného paprsku vo vnútri klávesnice alebo je celá klávesnica realizovaná premietajúcim laserom.

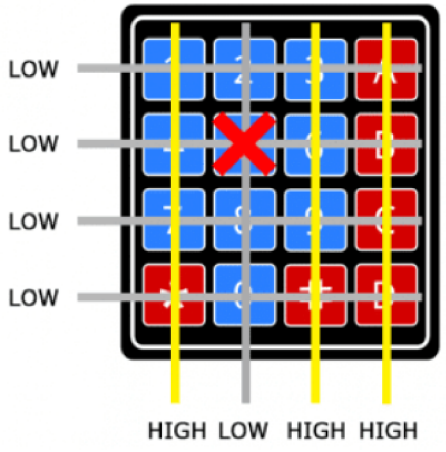
Princíp detekcie stlačenia klávesy:

Uvažujme maticovú klávesnicu 4x4 (viď. obrázok1.15). Jednotlivé riadky a stĺpce maticovej klávesnice tvoria prostredníctvom klávesových prepojení, kontaktnú maticovú sieť. Na jednotlivé riadky a stĺpce sú priamo napojené kontakty, kedy jedna polovica kontaktov (šedé vodiče) je pripojená na riadky klávesnice a druhá polovica kontaktov (žlté vodiče) je pripojená na stĺpce klávesnice. Snímanie stlačenia konkrétnej klávesy sa odohráva v štyroch krokoch:

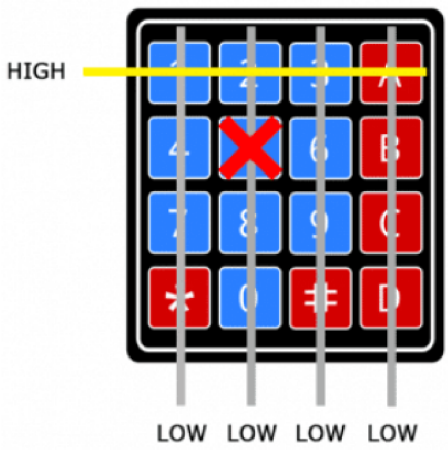
1. Na začiatku detekcie v neutrálnom stave nie je stlačené žiadne tlačidlo. Preto je na vývodoch riadkov pomocou MCU držaná nízka napäťová úroveň (LOW) a na vývodoch stĺpcov snímaná výstupná napäťová úroveň.
2. Keď stlačíme tlačidlo, MCU zaznamená zmenu úrovne jedného vývodu stĺpca na LOW, čo si uloží ako 1. súradnicu. MCU teraz vie, v ktorom stĺpci sa nachádza stlačené tlačidlo.
3. Následne prejde na hľadanie správneho riadku. Postupne bude nastavovať na každý z vývodov riadkov úroveň HIGH a súčasne snímať hodnoty napätia jednotlivých stĺpcoch.
4. Keď zdeteguje na vývode stĺpca úroveň HIGH, proces hľadania sa ukončí a výsledné uložené súradnice predstavujú stlačenú klávesu.



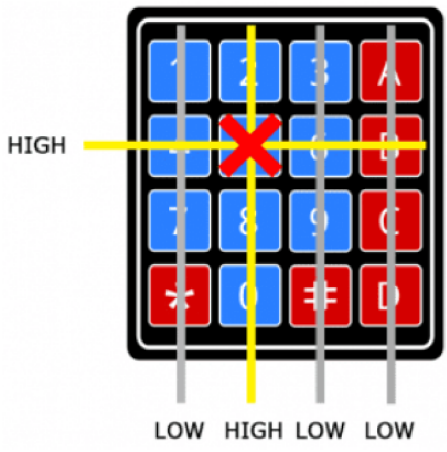
(a) 1.Krok



(b) 2.Krok



(a) 3.Krok



(b) 4.Krok

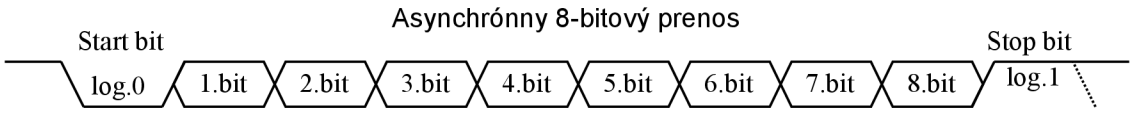
Obr. 1.15: Princíp detekcie stlačenia klávesy[9]

1.4.7 Komunikačný systém

Každý systém a to nie len bezpečnostný musí obsahovať určitý komunikačný systém - spôsob, akou cestou sa budú všetky komponenty a periférie medzi sebou dorozumievať. Základným spôsobom komunikácie je drôtové alebo bezdrôtové prepojenie (kap.1.3.1). Pomocou drôtových prepojení možno snímať a vyhodnocovať úroveň napätia nanajvýš posielať jednoduché digitálne informácie (snímanie stlačenia klávesnice). S príchodom komplexnejších periférií ako sú napríklad čítačky kariet, už obyčajné drôtové spoje nepostačovali. Na komunikáciu s takýmto typom zariadení preto vznikli rôzne komunikačné rozhrania.

USART

Rozhranie USART (z ang. Universal Synchronous / Asynchronous Receiver and Transmitter) je zariadenie pre sériovú komunikáciu. Je ho možné prevádzkovať v synchrónnom (half-duplex) alebo asynchrónnom (full-duplex) režime. Vysielanie a príjem dát prebieha na pinoch označovaných TX (transmit) a RX (receive).



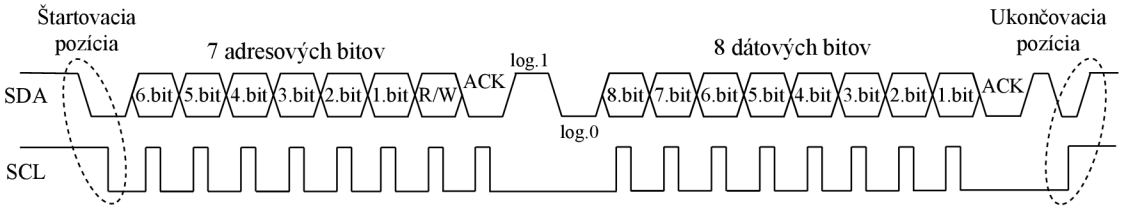
Obr. 1.16: USART- asynchrónny prenos jedného bajtu.

Na začiatku, kým neprebieha komunikácia je signál v kľudovej polohe na úrovni log.1, v TTL typicky 5V alebo 3,3V. Vysielanie sa zaháji zmenou hodnoty signálu na log.0 po dobu jedného bitu (Start bit). Po ňom nasleduje séria ôsmych bitov poslaných postupne od LSB po MSB zakončených Stop bitom s úrovňou log.1. Po poslaní Stop bitu môže ihneď začať prenos ďalšieho bajtu (viď.1.16 čiarkovaná čiara).[10]

TWI

Rozhranie I^2C (z ang.Inter-Integrated Circuit) tiež známe ako IIC, je dvojvodičové rozhranie pre komunikáciu na krátke vzdialenosti medzi MCU a ďalšími modulmi ako napríklad LCD, EEPROM, pamäťové karty. Prenosová rýchlosť sa pohybuje v rozmedzí od 100 kbps až po 5 Mbps. Káždá I2C zbernica pozostáva z dvoch signálov: SDA (Serial Data) a SCL (Serial Clock). Hodinový signál generuje vždy master na zbernici. Komunikácia IIC sa musí držať stanoveného protokolu, aby ju zariadenia na zbernici rozpoznali.[11] Komunikačný prenos správy je rozdelený do dvoch rámcov:

- Adresný rámec (7 bitov)– radič označuje zariadenia, na ktoré sa má správa odosielať
- Dátový rámec (8 bitov)– jeden alebo viac rámcov, ktoré nesú telo správy.



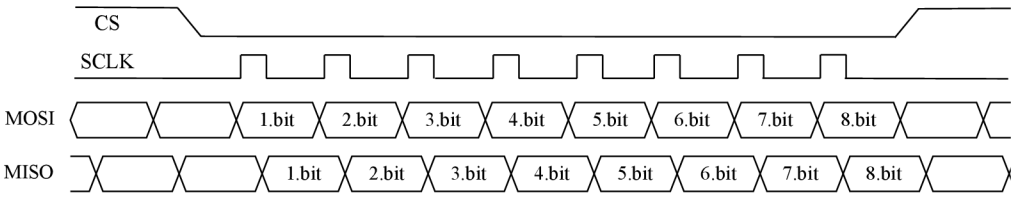
Obr. 1.17: Prenosový protokol komunikácie I2C

Pre zahájenie komunikácie musí najskôr MCU zviesť signál SDA na nízku úroveň a potom začne generovať hodinové impulzy SCL. Ako prvé sa odošlú adresné bity zaradom od MSB pre určenie zariadenia, s ktorým bude komunikácia prebiehať. Za nimi nasleduje bit R/W, ktorý určuje či sa bude jednať o čítanie alebo zápis. Ako posledný z inicializačných bitov sa odošle 9. kontrolný bit NACK / ACK, pre overenie, či sa dáta poslali správne. Po odoslaní rámca adresy sa môžu začať prenášať údaje. Hodinový signál SCL bude pokračovať v generovaní impulzov a SDA pracovať s dátami na základe parametru R/W bitu pre zápis alebo čítanie. Po spracovaní posledného bitu, MCU vygeneruje konečný stav zodvihnutím úrovne SDA na HIGH hneď po tom, ako bude v log.1 aj signál SCL (viď.1.17 čiarkovaná elipsa).[11]

SPI

Rozhranie SPI (z ang.Serial Peripheral Interface) je synchrónne sériové rozhranie využívané pre komunikáciu na krátke vzdialenosti medzi MCU a ostatnými integrovanými obvodmi (pamäťové karty, RFID čítačky). Na zbernici sú zariadenia rozdelené na master (riadi prenášanie dát) a slave (prijíma a spracúva prenášané dáta).

- CS – Chip select pin pre výber periférie na komunikáciu.
- SCLK – Synchronizačný hodinový signál.
- MOSI – (Master Out Slave In) Posielanie dát od mastra.
- MISO – (Master In Slave Out) Príjem dát od slavu.



Obr. 1.18: SPI komunikácia

2 Elektronická kontrola vstupu (EKV)

Po oboznámení so všeobecnou problematikou elektronických zabezpečovacích systémov možno prejsť ku konkrétnej téme zadania danej semestrálnej práce a to ku systému elektronickej kontroly vstupu.

V samotnej podstate sa jedná o systém určený pre zamedzenie vstupu do kontrolovaných miestností pre neoprávnené osoby. Označujú sa tiež skratkou ACS (z ang. Access Control System). V praxi je systém EKV veľmi rozšírený najmä vo firmách, bankách, bytových domoch, školách, ale využitie si našlo i pri výťahoch. Prakticky je možné EKV použiť pri akýchkoľvek uzatvárateľných priechodoch. Nemusí sa jednať práve len o dverové ústrojenstvá. S takým systémom EKV sa možno stretnúť napríklad pri turniketoch na letisku, lyžiarskych strediskách alebo pri automatickej cestnej vjazdovej závorách pre vstup do podzemnej garáže.

Systém EKV vykonáva kontrolu vstupu neustále v reálnom čase bez upustenia pozornosti. Z toho dôvodu predbehol a výrazne pomohol rozšíriť možnosti v strážení vstupu oproti samotnému ľudskému faktoru.

EKV slúži tiež ako náhrada systému jedného kľúča, kedy vo firme pracuje viacero zamestnancov a namiesto vyrábania množstva kľúčov stačí nainštalovať jednorázovo systém EKV. Týmto spôsobom sa dá chrániť aj pre prípadnou stratou kľúčov, čo by mohlo viesť k uskutočneniu útoku. Práve na tento účel bol EKV využívaný do 60. rokov minulého storočia.

Zostavený systém EKV je možné použiť aj ako dochádzkový systém (DS). Ten je určený pre evidenciu príchodu a odchodu zamestnancov, ako aj vyhodnotenie pracovnej doby. Zamestnanci sa evidujú pomocou čítacích kariet alebo iných dokazovacích faktorov. Zaznamenané údaje ďalej slúžia ako mzdový doklad pre mzdový systém a splnenia podmienky zákonníku práce.[12]

V normalizácií spadal systém EKV pod normu ČSN EN 50133–1 od marca 2001 do 11. 6. 2016, kedy ho ju nahradila ČSN EN 60839. [13]

2.1 Popis implementácie EKV

Po stručnom oboznámení so zameraním systému EKV možno prejsť ku stručnému popisu konkrétnych častí objektu pre EKV. Najskôr si definujeme základné pojmy pre nadobudnutie porozumenia hlbšej problematiky.

1. Prekážka – Bariéra, ktorá chráni aktíva pred priamym kontaktom s útočníkom. Na zmocnenie aktív je potrebné cez prekážku preniknúť. (Steny budovy, ploty).

2. Priechod – Diera v prekážke, ktorá umožňuje priamy pohyb do priestoru za prekážkou.
3. Vstup – Priechod opatrený uzatvárateľnou výplňou ako sú dvere.
4. Zóna – Časť kontrolovanej oblasti, po ktorej sa je možnosť voľne pohybovať. Je ohraničená prekážkami (stenami). Jedná sa o miestnosti, ale tiež to môže byť pozemok, či celý strážený komplex.[14]

Elektronická kontrola vstupu je systém určený ku automatizovanému riadeniu vstupu do kontrolovanej oblasti. Avšak chovanie tohoto systému musí podliehať istým nariadeniam "kto sa môže dostať do kontrolovanej oblasti a kto nie". Toto povolenie udeľuje autorita. Od toho je odvodený pojem autorizácia, čo v preklade znamená udelenie práv užívateľovi na využívanie prístupu ku chráneným záujmom alebo do kontrolovanej oblasti.

2.1.1 Autorizácia

Prebieha v pár krokoch, kedy autorita udelí prístupové práva užívateľovi a stanoví mu jeho identifikátor ID. To môže byť unikátne číslo alebo označenie, pod ktorým bude v systéme daná osoba zapísaná. Ďalej musí autorita do systému zasadiť overovací faktor OF a dokazovací faktor DF.

Overovací faktor [OF] sú dáta uložené v systémovej pamäti, s ktorými bude systém EKV porovnávať DF ako znak identifikácie.

Dokazovací faktor [DF] je potom akýkoľvek prostriedok, ktorým užívateľ svoju identitu dokazuje. DF môžu byť v hardwarovej podobe (RFID karta), v podobe znalosti (heslo) alebo biometrickej podobe (odtlačok prsta). Autorita vloží do systému ID a OF užívateľa čím ho autorizovala a užívateľ od tejto doby môže prostredníctvom DF svoje práva využívať. [2]

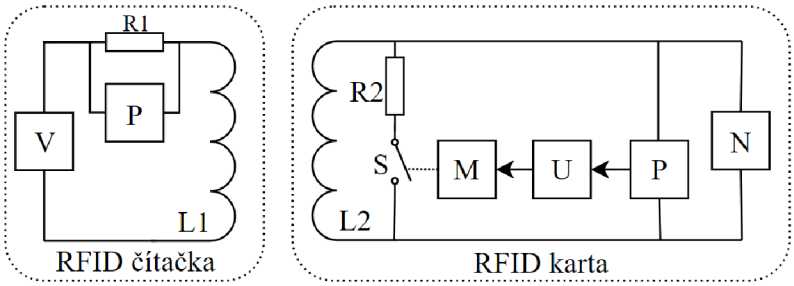
2.1.2 Overenie identity

Ďalej po autorizácií prichádza overenie identity osoby **autentizácia**. Je to hlavný a vo svojej podstate najdôležitejší bod systému EKV, kedy sa overí identita človeka a na základe toho systém povolí prístup do kontrolovanej oblasti. Je nesmierne dôležité, aby overovacie prvky systému boli spoľahlivé a presné, nakoľko ich chybovosť je priamou cestou na vznik incidentu.

Pre overovanie identity v počiatkoch systémov EKV slúžili obslužné klávesnice pre zadanie jedinečného hesla (70. rokov, 20. stor). Neskôr v 80. rokoch boli vymyslené Wiegandové karty, ktoré sú zároveň predchodcami RFID čipových kariet. Ich

slabinou bola ľahká možnosť klonovania. Nahradili ich teda RFID pamäťové karty (viď. obrázok2.1) no bohužiaľ i tieto sa časom stali ľahko klonovateľné. V dnešnej dobe sa na autentizáciu využívajú všestranné prostriedky od čipových kariet cez stále zaužívané klávesnicové zadávanie. Vhodným spôsobom je smartfónové overovanie, ktoré v sebe zahŕňa rovno kombináciu niekoľkých autorizačných protokolov. Smartfony dosahujú vysokých výpočetných výkonov a postupne by mohli nahradiť RFID bezkontaktné karty pomocou prenosu NFC.

Najnovším rozmachom je však overovanie identity prostredníctvom morfologických črtov človeka. Tejto oblasti sa hovorí biometrická autentizácia.



Obr. 2.1: Bloková schéma RFID čítačky a karty

Vysielač [V], prijímač [P], odpor [R], cievka [L], modulátor [M], pamäť [U], napájanie [N], spínač [S].

Princíp funkčnosti kariet RFID (Radio Frequency IDentification)
Vysielač (V) čítacieho terminálu neustále generuje signál o frekvencií 125 kHz do budiacej cievky (L1). Po priblížení obidvoch vynúti karty a čítačky (L1, L2) dôjde ku indukčnej väzbe, čo spôsobí vznik napätia na karte [transformátor]. Toto napätie slúži ako napájacie, ale zároveň pre prenos dát. Teda prenos dát nie je v skutočnosti rádiový ako z názvu vyplýva, ale indukčný. Generovaný signál sa v karte pomocou napájacieho bloku (N) usmerní a poskytne napájanie pre všetky podielové bloky karty. Následne začne modulátor (M) odpájať a pripájať odpor (R2) prostredníctvom spínača (S), čím sa mení generované magnetické pole karty. Tieto zmeny sa odzrkadlia na odpore (R1) čítacieho modulu, čo nasníma prijímač (P). Postupné zmeny napätia na RFID čítačke signalizujú jednotlivé prenášané bity, na základe ktorých čítačka dekóduje dáta WS z pamäti karty (U).

2.2 Spôsoby autentizácie podľa stupňa zabezpečenia

Stupne zabezpečenia vychádzajúce z kapitoly 1.3 sa delia pre systém EKV podľa novej normy ČSN EN 60839–11–1 na jedno, dvoj a troj-faktorové. Počet faktorov

určuje počet prevedený overovacích úkonov potrebných ku autentizácií užívateľa. Pri každom stupni zabezpečenia podľa normy ČSN EN 50131–1 nie je potrebné a ani vždy možné všetky faktory overovania využiť. Pri **vyšších** stupňoch sú **nižšie** faktory nepostačujúce a pri **nižších** stupňoch sú **vyššie** faktory neprimerane nákladné a predimenzované.[2]

Tab. 2.1: Nároky na autentizáciu podľa stupňa zabezpečenia[15]

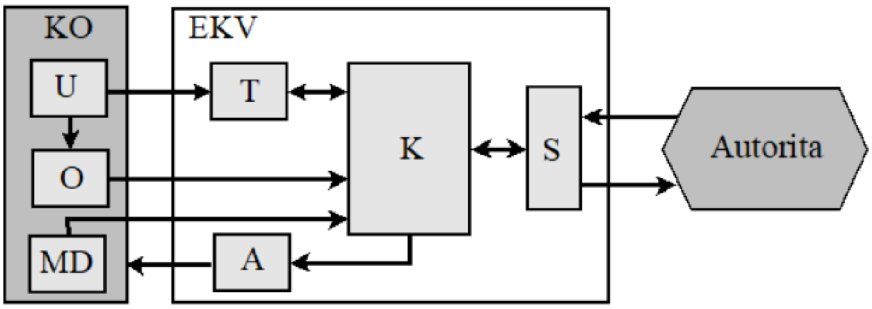
Jednofaktorová autentizácia	1. Stupeň	2. Stupeň	3. Stupeň	4. Stupeň
PIN =>10 000 kombinácií	áno	nie	nie	nie
PIN =>100 000 kombinácií	áno	áno	nie	nie
Magnetické/Bezkontaktné/ RFID karty	áno	áno	áno	áno
Dvojfaktorová autentizácia	——	——	——	——
Magnetické/Bezkontaktné karty + PIN =>10 000 komb.	áno	áno	áno	áno
Biometria + PIN =>10 000 kombinácií	áno	áno	áno	áno
Biometria + Magnetické/Bezkont.kary	áno	áno	áno	áno
Biometria + RFID karty	áno	áno	áno	áno
Trojfaktorová autentizácia	——	——	——	——
Biometria + PIN =>10 000 kombinácií + Magnetic/Bezkont./RFID karty	áno	áno	áno	áno

2.3 Štruktúra architektúry systému EKV

Každý systém EKV sa musí skladať z istých základných prvkov pre jeho možnú realizáciu (viď. obrázok2.2). Tými prvkami sú:

1. Kontrolér (K) – Riadiaca výpočtová logika, ktorá vykonáva všetky rozhodujúce výpočty a riadi systém EKV.
2. Terminál (T) – Zariadenie na prístup k systému zo strany užívateľa (klávesnica, čítačka).
3. Správna jednotka (S) – Slúži na správu systému zo strany autority. Aktualizácia zoznamu OF atď...

4. Ovládacia jednotka (A) – Spravidla elektrické zariadenie na ovládanie vstupov v kontrolovanej oblasti (Elektrický vrátnik)
5. Komunikačná systém (K) – Prepojenie všetkých jednotlivých blokov systému EKV. Väčšinou zbernica (RS-232,RS-485) alebo 2 a viac žilové káblové rozhrania. [14]



Obr. 2.2: Bloková schéma systému EKV

Kontrolér (K) riadi všetky procesy vykonávané v EKV, ako je aj komunikácia medzi zvyšnými prvkami. Keď sa užívateľ (U) autentizuje pomocou terminálu (T) priložením karty alebo zadaním hesla na klávesnici, poputuje jeho DF do kontroléra na porovnanie s databázou OF získanými autorizáciou. Pri potvrdení zhody DF s OF uloženými v pamäti sa preverí či autorita udelila užívateľovi prístupné práva v danom čase. V prípade obidvoch úspešných overení vyšle kontrolér signál do logiky akčného člena (A), ktorá odomkne prístupové dvere a užívateľ môže vstúpiť do stráženej miestnosti. V opačnom prípade ostane vstup uzavretý.

Doplnkovými nepovinnými prvkami systému sú napríklad ešte odchodové tlačítko (O) umiestnené v kontrolovanej miestnosti a magnetický detektor otvorenia dverí (MD). Odchodové tlačítko nachádza využitie v prípade použitia len jedného terminálu pre vstup do kontrolovanej oblasti (KO). Funguje teda ako úspora jedného terminálu, kedy na opustenie miestnosti je potrebné iba stlačiť toto odchodové tlačítko. Takto strážené dvere môžu byť aj v prevedení, kedy majú z jednej strany kľučku a z druhej guľu.

Magnetický detektor (MD) sa používa spravidla na detegovanie otvorenia dverí. Využitie tejto informácie je naozaj všestranné, ako pre získanie informácie o stave dverí, tak i na PZS. [2]

2.3.1 Praktická realizácia systému EKV

V praxi sa z hľadiska ekonomickej a systémovej efektivity, systém EKV realizuje zoskupením viacerých kontrolovaných vstupov do jedného správneho systému. Podľa

zapojenia prvkov a spôsobu riadenia sa systém EKV delí na:

1. **Centralizovaný** – Všetky prvky jednotlivých samostatných strážených vstupov sú riadené jediným kontrolérom. Výhodou je ušetrenie a jednoduchšia inštalácia kábelových rozvodov, nakoľko sa všetky prvky zvyčajne pripájajú ku terminálu a ten následne ku kontroléru pomocou zbernice. Výraznou nevýhodou z pohľadu funkčnosti je labilnosť systému na možné útoky. Stačí, aby vypadol kontrolér alebo komunikačná zbernica a celý systém ostane paralyzovaný. Ďalším nepríjemným faktom je výrazne nižšia prenosová komunikačná rýchlosť, ktorá pri zložitých systémoch môže predĺžiť čas odozvy jednotlivých prvkov systému. V praxi sa preto možno stretnúť častejšie s decentralizovanou formou systému.[2]

2. **Decentralizovaný** – Pri tomto systéme slúži na riadenie kontroly jednotlivých vstupov viacero samostatných kontrolérov, ktoré pracujú nezávisle od seba. Toto prevedenie zlepšuje spoľahlivosť systému, rýchlosť odozvy prvkov i pri zložitejších systémoch a navyše sťažuje prístup útočníka na sabotovanie riadiacej logiky, nakoľko sa môže namotovať priamo do kontrolovanej miestnosti. Jediná nevýhoda je z pohľadu ceny, keďže je potrebné obsiahnuť pre každý kontrolovaný vstup osobitný mikrokontrolér (1 MCU môže riadiť 1 až 2 vstupy).[2]

Z pohľadu historického vývoja sa o riadenie a kontrolu vstupu prvotne staral kontrolér. Najnovším riešením je integrovanie riadiaceho kontroléra priamo do terminálu, ktorý vykonáva všetky autentizačné protokoly a ústredni predáva iba informácie a zhode prípade nových autorizačných dátach.

2.4 Druhy autentizácie

Overením identity alebo inak autentizáciou sa vo všeobecnosti zaoberá kapitola2.1.2. V tejto podkapitole bude delenie a opis konkrétnych druhov autentizácií.

Na základe dokazovacieho faktoru (DF) a nosiča dokazovacieho faktoru (NDF) možno klasifikovať rôzne druhy autentizácie. Nosičom autentizačných prvkov môže byť osoba alebo určitý predmet (viď. Tabuľka 2.2). [2]

Tab. 2.2: Druhy autentizácie

	NDF = osoba	NDF = predmet
DF je rys	Biometrika	Preukaz
DF sú dáta	Heslo	Hardware

2.4.1 Autentizácia heslom

Dalo by sa povedať, že kolískou autentizácie bolo práve zadávanie hesla do terminálu. DF je v tomto prípade jedinečná kombinácia dekadických číslic (4 – 8 miest), ktoré sa nazývajú známou skratkou PIN (Personal Identification Number). Tento PIN udelí autorita užívateľovi, ktorý si musí danú kombináciu zapamätať. Následne pri požiadavke udelenia prístupových práv sa bude musieť žiadateľ preukázať týmto prideleným PIN-om na autentizačnom zariadení (klávesnica). S tým je spojený aj istý nedostatok tejto formy autentizácie a to je, že DF si musí užívateľ zapamätať. To zhoršuje komfort a taktiež zvyšuje pravdepodobnosť zabudnutia hesla. Čo sa týka vyhotovenia, tak ide o najjednoduchšiu automatickú kontrolu vstupu z pohľadu obsluhy aj inštalácie.

2.4.2 Autentizácia preukazom

Jedná sa o preukázanie identity prostredníctvom kartového DF. Karty (preukazy) majú štandardnú veľkosť 85,6 x 53,9 mm (občiansky preukaz, vodičský preukaz, ISIC...). Každý preukaz má podľa majiteľa priradené jedinečné ID pomocou, ktorého sa v systéme užívateľ autentizuje. Preukaz môže zahŕňať jedno, ale aj dvojfaktorovú autentizáciu. V dvojfaktorovom prevedení je na preukaze dotlačená fotografia majiteľa aj s jeho prideleným ID.

Pri autentizácií napríklad na polícií alebo na vrátnici zabezpečenej budovy bude musieť člen ochranky identifikovať na základe biometrických vlastností zhodu medzi OF a DF v tomto prípade medzi podobnosťou tváre na preukaze a overovanej osoby, prípadne môže požiadať o ďalší dodatočný preukaz pre zníženie možnosti sfalšovania. Ak sa potvrdí, že držiteľ preukazu je jeho skutočným majiteľom, ochranka pomocou zoznamu povolení práv osobám vyhľadá podľa ID povolenie pre vstup danej osoby, na základe čoho žiadateľa do objektu vpustí alebo nie.

Novodobé preukazy v sebe zahŕňajú už aj integrované čipové obvody, čo z nich ale robí čiastočne už hardwarovú autentizáciu.

2.4.3 Autentizácia hardwarom

Keď sa povie slovo hardware, nemyslí sa tým nič iné ako pevné uchopiteľné médium (nejaký predmet) určené v tomto prípade na uchovanie autentizačných dát (DF). Existujú rôzne formy prevedenia týchto médií (kľúčenky, mobily, karty). Všetky tieto pamäťové úložiská pracujú na rovnakom princípe uchovávania takzvaného Wiegandového slova (WS), čo je slovo o dĺžke obvykle 26 bitov, z čoho prvých 8 bitov slúži na identifikovanie organizácie a druhých 16 bitov na definovanie čísla karty. Celkové slovo je doplnené krajnými paritnými bitmi. Z hľadiska malého počtu bitov pre definovanie organizácie (8) sa rozšírilo WS na 34 alebo až 37 bitov. Typickými hardwarovým autentizátormi sú napríklad magnetické, RFID alebo mikroprocesorové karty. Najnovšie pomocou funkcie NFC preberajú túto úlohu i smartfóny.

Výhodou autentizovania pomocou hardwaru je jednoduchosť udelenia autorizačných práv, kedy stačí priložiť nosič (kartu, kľúčenku) o čítačku a priradiť v systéme konkrétne ID. Pri následnom autentizovaní priložením nosiča (DF) o čítačku bude žiadateľ systémom rozpoznaný na základe databázy porovnávacích (OF) a systém vzápätí vyhľadá podľa prideleného ID povoľovacie práva pre vstup. Ďalšou výhodou je taktiež cena. Stačí zaobstarať jeden čítací terminál pre množstvo užívateľov a zvyšné náklady idú len na prístupové karty podľa počtu užívateľov.

Ako každý systém ani tento sa nezaobíde bez slabín. Konkrétne pri čipových NDF je náchylnosť na ľahké kopírovanie a falšovanie. Najbezpečnejšia forma sa teda javí pomocou dnešných smartphonov s funkciou NFC, ale ani to nie je úplne stopercentné.

2.4.4 Autentizácia biometriou

Biometrické autentizovanie je najspoľahlivejšie spomedzi predošlých spomínaných vďaka jej nenapodobiteľným charakterom, keďže každý človek na zemi je jedinečný. Stretávame sa s ňou na dennom poriadku vo svojom mobilnom telefóne, ako i v iných výpočtových technikách. Využitie nachádza aj vo vysoko-strážených oblastiach ako sú banky alebo muničné sklady. Zápletka pri biometrickom identifikovaní nastáva vo vyhotovení vhodných spoľahlivých snímačov daných biometrických veličín, ktorých prevedenie nie je práve najjednoduchšie na technológiu výroby. Nemožno teda vyrobiť 100% presný snímač biometrických črtov. Podľa Nation Science and Technology sa biometrická autentizácia delí na biologickú a behaviorálnu.[2]

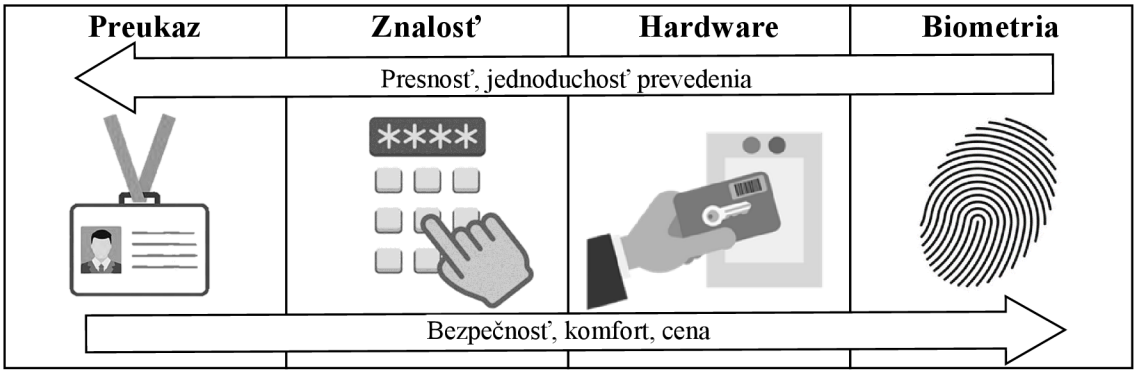
Biologická biometria – sú to jedinečné fyzické črty užívateľa, ktorými disponuje od narodenia. Na overovanie biologickej biometrie sa využívajú DF ako napríklad:

1. Jedinečné odtlačky papilárnych línií prstov
2. Geometria tváre
3. Riečištie/ štruktúra žíl na zápästí a v ruke
4. Sfarbenie dúhovky oka alebo sietenice
5. Geometria celej dlane

Behaviorálna biometria – sú to jedinečné nadobudnuté znalosti užívateľa, ku ktorým navykol počas života. Radia sa ku nim napríklad:

1. Hlasové a rečové schopnosti
2. Štýl podpisu
3. Spôsob chôdze
4. Pásanie na klávesnici

Z predchádzajúceho popisu vyplýva, že každý druh autentizácie má svoje výhody a nevýhody. Či sa jedná o rýchlosť, presnosť, komfortnosť alebo cenu, vždy je rozhodujúca aplikácia, kde bude systém EKV použitý. V dedinskom obchode je nepraktické, aby bol do skladu zavedený biometrický autentizátor, nakoľko je to zbytočné drahé riešenie. Naopak do bankového trezoru použiť iba autentizáciu znalosťou číselného kódu môže byť nedostatočné z pohľadu jednoduchého prekonania. V konečnom dôsledku možno vypísané druhy autentizácie hierarchicky zoradiť podľa ich vlastností. Prehľadné zobrazenie škály autentizátorov je na obrázku.2.3. Priečne hrubé šípky označujú vzostupný rast uvedených parametrov.



Obr. 2.3: Hierarchické zoradenie spôsobov autentizácie

– Navrhovaný systém v tejto práci je decentralizovaný založený na 3-faktorovej autentizácií prostredníctvom biometriky, hesla a hardwaru.

3 Praktická časť

V praktickej časti semestrálnej práce je popísaný návrh a zostrojenie modelu pre systém EKV. Pri návrhu sa vychádza z teoretických poznatkov o zabezpečovacích systémoch a zároveň z blokovej schémy štruktúry EKV (viď. obrázok2.2).

3.1 Požiadavky vyplývajúce zo zadania práce

Navrhovaný systém EKV musí spĺňať:

- Autentizácia pomocou číselného hesla
- Autentizácia pomocou RFID kariet
- Autentizácia pomocou odtlačkov prstov
- Správa systému prostredníctvom klávesnice
- Detekcia otvorenia pomocou MD
- Detekcia pohybu pomocou detektora PIR
- Signalizácia poplachu pomocou sirény
- Vhodné bezpečnostné prevedenie

3.2 Postup návrhu:

1. Návrh blokovej schémy celkového systému EKV.
2. Výber vhodnej riadiacej logiky (mikrokontrolér).
3. Výber kompatibilných periférií a modulov.
4. Návrh elektrickej schémy a DPS.
5. Zostrojenie modelu dverí.
6. Popis programu a funkcionality systému.
7. Meranie a overenie funkčnosti.

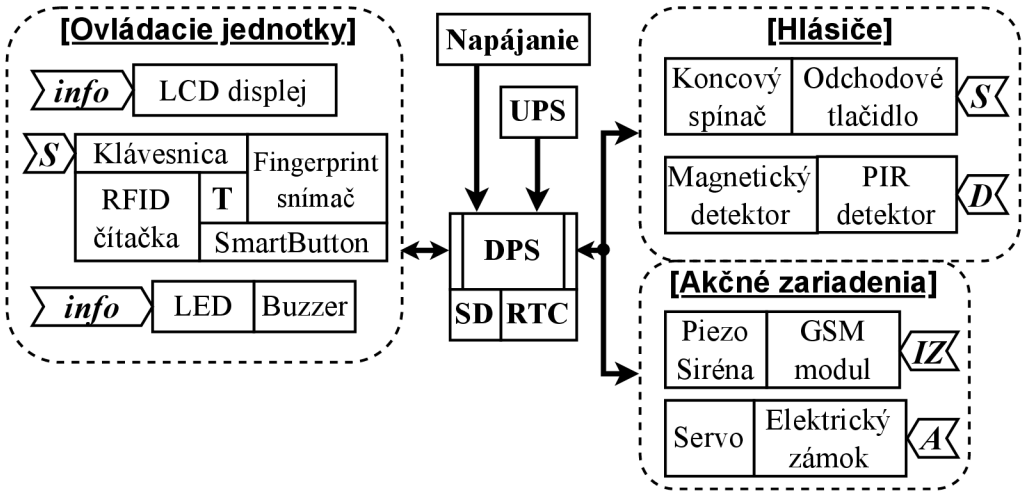
3.2.1 Návrh blokovej schémy systému EKV

Celý navrhovaný systém je rozdelený do štyroch funkčných celkov vychádzajúcich zo základnej teórie EZS (viď. obrázok3.1). Každá skupina prvkov je označená globálnym pomenovaním a zároveň konkretizačným štítkom.

1. **Ústredňa** – Predstavuje štruktúrovane-združený embedded systém hlavnej dosky plošných spojov (DPS) s integrovaným prvkom RTC pre meranie aktuálneho času, SD kartou pre ukladanie dát a osadeným MCU. Na doske sú

realizované všetky jednoduché, pomocné, elektrické obvody pre fungovanie systému ako napríklad stabilizátory napätia, spínacie tranzistorové obvody či vyvedené svorkovnice pre pripojenie periférií. Samozrejme je v ústredni zahrnuté aj napájanie so záložným zdrojom UPS v prípade výpadku sieťového napätia. Hlavná DPS prepojuje periférie a moduly medzi sebou prostredníctvom zberníc a zabezpečuje tak komunikáciu medzi nimi.

2. **Ovládacie jednotky** – Ovládacími jednotkami sa rozumejú všetky periférie určené na interakciu medzi autoritou/užívateľom so systémom. Sú v nich zahrnuté všetky prístupové terminály [T] a informačné zariadenia [info] pre obdržanie akusticko-vizuálnej spätnej väzby. Zároveň je podľa zadania terminálová klávesnica použitá aj ako správny prvok [S] pre ovládanie systému. Všetky OJ sú pripájané na ústredňu pomocou viačžilových vodičov (IDE kábel,jumper wire).
3. **Hlásiče** – Hlásiče sa delia na dve podskupiny. Prvá podskupina [S] označuje mechanické spínače pre kontrolu stavu uzamknutia dverí a stavu odchodového tlačidla. V druhej podskupine [D] sa jedná o detektory nakoľko podávajú ústredni priamo hlásenie o vzniku incidentu, buď to otvorením dverí (MD) alebo pohybom osôb v nepovolenej oblasti (PIR).
4. **Akčné zariadenia** – Sú to všetky členy, ktoré sa podieľajú na vykonávaní mechanickej, akustickej alebo vizuálnej práce zo strany systému. Aj keď sú všetky členy zahrnuté v jednej skupine, ich funkcia je celkom odlišná. Preto sú rozdelené na ďalšie dve podskupiny a to konkrétne na informačné zariadenia [IZ] a akčné členy [A]. IZ sú poplašné ústrojenstvá určené na signalizáciu vzniku incidentu. Akčné členy naopak vykonávajú iba mechanicku činnú prácu potrebnú pre chod systému.

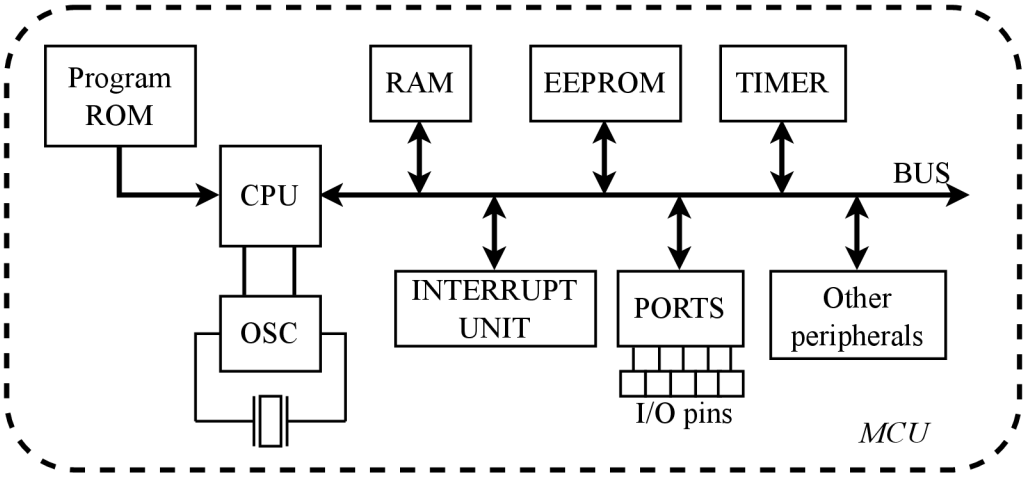


Obr. 3.1: Bloková schéma systému EKV

3.2.2 Výber mikrokontroléra (MCU)

Prečo je vhodný práve mikrokontrolér? Narozdiel od mikroprocesoru (μP), ktorý je len integrovaným obvodom s doplneným radičom pamäte, má MCU všetky postranné doplnkové prvky ako sú pamäte, RAM, EEPROM, počítadlá či komunikačné rozhrania integrované priamo na jednom čipe (viď.obrázok 3.2). Výhodou je teda potreba použitia menšieho počtu externých komponentov, ktoré by sme v prípade μP museli dodať. Aj keď je síce μP rýchlejší a jeho využitie je univerzálnejšie než MCU, v dnešnej dobe nie je problém z existujúcich rád mikrokontrolérov vybrať ten správny s potrebnými parametrami pre špecializovanú aplikáciu, navyše keď je ich cena častokrát nižšia.[16]

Na trhu exituje mnoho typov mikrokontrolérov od rôznych výrobcov a patričných rodín. Odlišujú sa v množstve parametrov na základe čoho sa odvíja ich patričné využitie. Medzi kľúčové rozdiely patrí: výkon, spotreba, taktovacia frekvencia, veľkosť pamäte, veľkosť puzdra, počet vývodov, druhy komunikačných rozhraní, cena.



Obr. 3.2: Architektúra mikrokontroléra

Architektúra AVR

Pre objasnenie preberanej problematiky je potreba definovať pár základných pojmov:

1. **Harvardská architektúra** – Pamäť pre program a dáta je oddelená. Údaj zapísaný do pamäti není možné chápať ako inštrukciu. Výhodou je zvýšenie bezpečnosti programovania a zvýšenie výpočtového výkonu.
2. **Von Neumannová architektúra** – Pamäť pre program a dáta je spoločná. Hrozí prepísanie programu sebou samým.

3. **RISC** – Reduced Instruction Set Computer (mikropočítač s obmedzenou sadou inštrukcií). Je to architektúra procesorov s priamočiarym vykonávaním pomerne jednoduchých inštrukcií.
4. **CISC** – Complex Instruction Set Computer (mikropočítač s rozsiahlou sadou pomerne zložitých funkcií). Je to μP architektúra kde sa inštrukcie vykonávajú ako viaceré operácie kódu v jednom takte procesora.
5. **RAM** – Random Access Memory. Umožňuje informácie z pamäti čítať tak ako do nej zapisovať.
6. **ROM** – Read-Only Memory. Do tejto pamäti sa nedajú dáta počas bežného prevozu ukladať, je možné ich len čítať. Rozlišujeme dve špeciálny druhy ROM pamätí:
   - EPROM (Erasable and Programmable ROM). Je zmazateľná ultrafialovým žiarením a programovateľná pomocou špeciálneho programátoru.
   - EEPROM (Electrically Erasable PROM). Tiež sa označuje ako E^2PROM. Špeciálnym programátorom je možné pamäť vymazať i spätne naprogramovať. Pamäť FLASH je práve špeciálnym typom E^2PROM pamäte.
7. **RS-232** – sériová linka využívaná ako komunikačné rozhranie pre PC. Dáta sú vysielané postupne po sérií. Využíva na to dátové signály RX, TX.
8. **USB** (Universal Serial Bus) – Univerzálna sériová zbernica. Nahradzuje takmer všetky používané prepojenia skoršej doby pre bežné druhy periférií (tlačiarne, myšky, klávesnice...). Je to zbernica s jediným typom Master. Dáta sa prenášajú v paketoch o šírke 8 a potom 256 bajtov. Vďaka jej univerzálnosti a stálemu vývoju (príchod USB-C, Plug&play) je možnosť, že by sa stala celosvetovou jedinou normou v prenosových rozhraniach. [17]

Mikrokontroléry AVR od firmy ATMEL sú nizkopríkonové MCU založené na AVR modifikovanej harvadskej RISC architektúre. Veľa AVR mikrokontrolérov disponuje integrovanými ADC, PWM a rôznymi druhmi komunikačných rozhraní napríklad USART, SPI, I2C, CAN, USB atď.

Programová pamäť: je tvorená zabudovanou Flash, ktorej kapacita sa pohybuje v rozmedzí 500 B až 128 kB v závislosti od série AVR (tiny, mega, Dx). Flash je programovateľná buď klasickým paralelným programátorom alebo pomocou rozhrania SPI a má obmedzený počet preprogramovaní cca. 1000 cyklov.

Dátová pamäť je buď typu RAM o veľkosti (64 B – 16 kB) alebo EEPROM s kapacitou od 64 B do 4 kB. Počet preprogramovaní dátovej pamäti je o čosi vyšší a to 100 000 cyklov.[18, 19]

Radenie čipov od firmy ATMEL z rady AVR

Mikrokontroléry z rady AVR sú na trhu od roku 1996 kedy ich vývojárom bola firma ATMEL. V roku 2016 bola ale odkúpená spoločnosťou Mikrochip Technology, pod ktorou teraz vystupuje. Rodina čipov z rady AVR sa kategorizuje podľa parametrov do nasledujúcich základných skupín.

1. AT90 – Táto rada sa už nevyrába. Náhradou za ňu je rada ATtiny alebo ATmega.
2. ATtiny – Využívajú sa v jednoduchých malých aplikáciách, v ktorých môžu plniť doplnkovú alebo náhradnú zložku za iné integrované obvody. Vyrábajú sa v drvivej väčšine v 8 vývodovom prevedení.
3. ATmega – Sú to výkonové mikrokontroléry s rozhraním JTAG a integrovanou väčšou pamäťou flash a RAM.
4. ATxmega – Disponujú zvýšeným výkonom oproti štandardu a podporujú kryptografiu.
5. ATmega pre špeciálne operácie – Radia sa sem čipy ATmega so špeciálnymi periférami ako LCD kontroléry, USB kontroléry, PWM atď.
6. FP SLIC – Kombinácia AVR s FPGA. Obvod FPGA sa skladá z 5 000 až 40 000 hradiel. Jadro AVR za to môže bežať na frekvencií až 50 MHz.
7. 32 bitové AVR – Mirkopočítače s rozšírením pre spracovanie audia a videa. Prvotne mala 32bit-ová rada konkurovať architektúre ARM no ATMEL radšej rovno súbežne vyrábal procesory s jadrom ARM. [20]

Zohľadnenie rady mikrokontroléra:

Vzhľadom na veľké zameranie návrhu systému, sa rada ATtiny nebude uvažovať a tak isto ani AT90 z dôvodu ukončenia výroby. Návrh bude orientovaný smerom na μP techniku teda hradlá FP SLIC tiež možno vylúčiť. Jedná sa o bezpečnostný systém EKV kedy bude mikrokontrolér riadiť periférie digitálnym signálom o hodnotách log.0/log.1 maximálne signálom PWM a komunikačnými rozhraniami SPI,I2C. Príliš veľký výstupný výkon od MCU nebude požadovaný čo vylučuje radu xmega. V tejto práci sa nerieši systém DVS teda nebude potrebné ani signlové spracovanie audia/videa.

Vyraďovacou metódou z predošlého zoznamu sa výber okresal na výsledný typ MCU rady ATmega.

Konkrétne typy mikrokontrolérov rady ATmega

Pre prehľadné spracovanie parametrov sa využije štruktúrovanie údajov do tabuľky (viď. tabuľka 3.1). Všetky typy mirkokontrolérov v sebe zahŕňajú rozhrania v projekte potrebné I^2C, SPI a USART, čiže sa v tabuľke nebudú uvádzať nakoľko by

ponúkali zbytočne opakujúcu sa informáciu. Zároveň číslo v označení púzdra odkazuje na počet vývodov preto ani táto informácia nemá samostatnú kolónku.

Tab. 3.1: Parametre vybraných mikrokontrolérov z rady ATmega[21]

MCU	Prac.nap.	Frekv.	Flash	E^2PROM	Puzdro	Cena
ATmega48	2,7 až 5,5 V	20 MHz	4 kB	512 B	DIP28	99 Kč
ATmega644	2,7 až 5,5 V	20 MHz	64 kB	2 kB	DIP40	135 Kč
ATmega16L	2,7 až 5,5 V	8 MHz	16 kB	512 B	DIP40	155 Kč
ATmega8A	2,7 až 5,5 V	16 MHz	8 kB	512 B	DIP28	159 Kč
ATmega168P	2,7 až 5,5 V	20 MHz	16 kB	512 B	DIP28	169 Kč
ATmega88A	1,8–5,5 V	20 MHz	8 kB	512 B	TQFP32	269 Kč
ATmega328P	1,8–5,5 V	20 MHz	32 kB	1 kB	PDIP28	325 Kč
ATmega2560	4,5–5,5 V	16 MHz	256 kB	4 kB	TQFP100	1290 Kč

Údaje sú platné ku dňu 27.1.2023.
Z vpísaných parametrov možno vidieť jasné rozdiely v pracovnom kmitočte, obnose pamäti, veľkostí púzdra či výške ceny. Zámerne je tabuľka zoradená vzostupne podľa ceny pretože tá v dnešnej dobe kedy je celkový dopyt po mikrokontroléroch obmedzený hrá značnú rolu.

Pre aplikáciu akou je tento elektronický systém, je výber MCU rozhodujúci pre nasledujúci vývoj. Ideálna varianta by mala disponovať potrebným množstvom výstupných pinov, veľkou dátovou a programovou pamäťou , potrebnými komunikačnými rozhraniami a samozrejme primeranou cenou. Z vybraných druhov MCU preto treba znovu vyraďovacou metódou vybrať ten najadekvátnejší.

ATmega48, ATmega8A, ATmega88A – Malá pamäť pre program.
ATmega16L – Nízka taktovacie frekvencia.
ATmega168P, ATmega328P – Malý počet I/O pinov

Vo finále ostal výber medzi dvomi mikrokontrolérmi ATmega644 a ATmega2560. Obidva dominujú pozitívnymi parametrami v iných oblastiach. Pri ATmege644 je to širší rozsah napájacieho napätia, vyššia taktovacia frekvencia a cena. ATmega2560 pre zmenu disponuje vyšším počtom I/O pinov, objemom pamäte Flash a EEPROM no na úkor vyššej ceny. Parametrické výhody medzi nimi sú teda presne v pomere 50/50 no vzhľadom k nepotrebnosti takého mnohého počtu I/O pinov ako aj pamäte a samozrejme rozhodujúcej výšky ceny (takmer 10x lacnejší než ATmega2560) je spomedzi nich vybraný pre riadiacu funkciu systému EKV, MCU **ATmega644**.

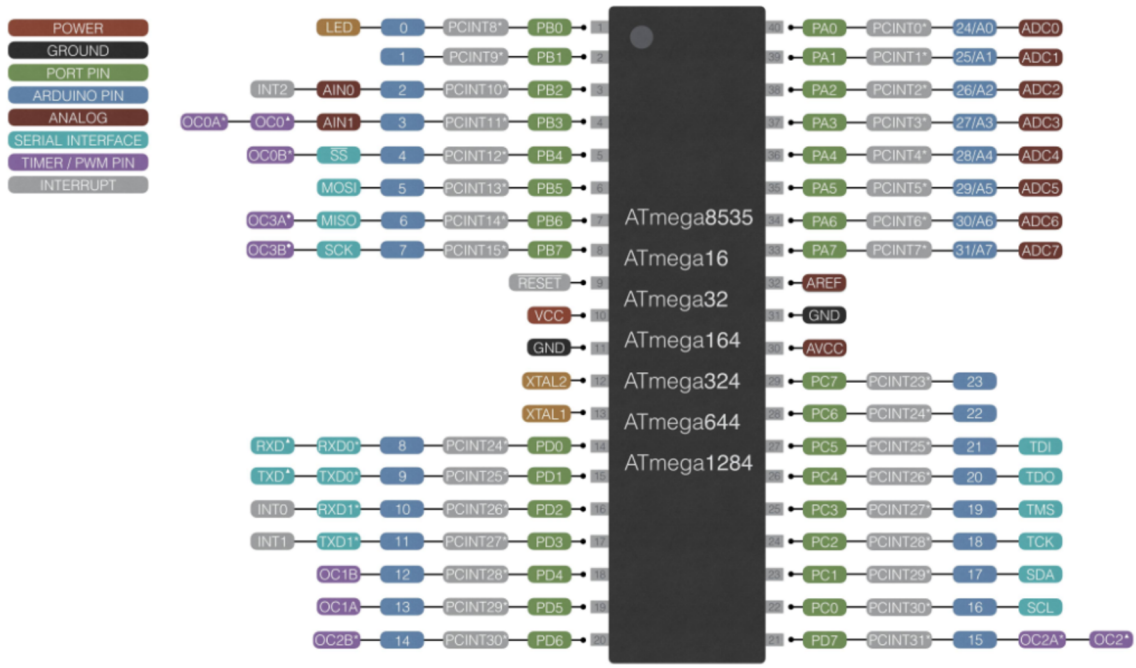
ATmega644-20PU

Pre túto prácu bol zvolený mikrokontrolér od osvečenej firmy ATMEL z rady AVR **ATmega644-20PU** pre jeho vyhovujúce parametre a taktiež v tejto dobe z hľadiska ceny a dostupnosti na trhu.

Jedná sa o jednočipový 8-bitový CMOS mikrokontrolér. Spôsobom vykonávania inštrukcií v jednom hodinovom cykle dosahuje MCU priepustnosť blížiacu sa 1 MIPS na 1 MHz. Je opatrený stredným počtom vývodov, ktoré sa dajú využívať k priamemu ovládaniu. Meno MCU rady ATmega povýšila implementácia do známej Talianskej vývojovej platformy Arduino UNO, ktorá vznika v roku 2005 a veľmi rýchlo sa ujala na celom svete. ATmega644-20PU sa vyrába v prevedení THT [DIP40] ale dostupná je aj v SMD verzií [TQFP44]. Názorná ukážka typu puzdra použitého v tejto práci a zároveň popis vývodov (viď. obrázok 3.3) [22]

Tab. 3.2: Základné parametre mikrokontroléra ATmega644-20PU

FLASH	EEPROM	RAM	I/O	TIMER	ADC	Nap.	Rozhranie
64 kB	2 KB	4 kB	32	3	8	2,7 - 5,5 V	USART, SPI, I2C



Obr. 3.3: ATmega644-20PU[23]

3.2.3 Výber kompatibilných periférií a modulov na základe návrhu systému elektronickej kontroly vstupu

Táto sekcia praktickej časti sa zameriava na popis všetkých použitých periférií v navrhovanom systéme. Výber periférií sa riadi podľa jednotlivých blokov blokového diagramu (viď. obrázok3.1)

Ústredňa

1. Napájací zdroj.
2. UPS
3. DPS – návrhu sa venuje samostatná kapitola
4. SD karta
5. RTC
6. Mikrokontrolér – už vybratý. Podrobný opis v kapitole 3.2.2.

Napájací zdroj

Od napájacieho zdroja sa požaduje aby bol schopný dotovať celú ústredňu energiou spoločne aj so všetkými pripojenými prvkami. Jednoduchým spočítaním odberov prúdu jednotlivých periférií sme dostali výsledný prúdový odber 2,5 A. Z dôvodu rezervy je zdroj dimenzovaný na 3 A. Zdroj musí byť taktiež prispôsobený na Európske sieťové napätie 230 V/50 Hz a na výstupe musí disponovať napätím 12 V. Nižšie úrovne napätí pre napájanie zvyšných komponentov sa budú riešiť prostredníctvom stabilizátorov na základnej doske ústredni. Zdroj by mal mať taktiež prijateľné rozmery a hmotnosť. Požadované vyššie parametre spĺňa pulzný zdroj APV-35-12, 35W, IN 230 V AC, OUT 12 V DC.

Obr. 3.4: Príklad zdroja 12 V 3 A, APV-35-12[24]

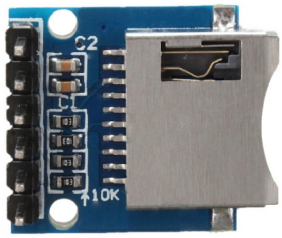
UPS

Neprerušiteľný zdroj energie. Slúži na udržanie behu ústredne po výpadku sieťového napájania. Na túto činnosť sa využívajú gélové, olovené, elektrolitové či lítiové batérie upravené pre špecializované použitie (extrémne vysoko-rýchlostné aplikácie,dlhá životnosť). V tomto návrhu sa použije Lithium-polymerový akumulátor, ktorý disponuje možnosťou vysokej dodávky energie a zároveň netrpí pamäťovým efektom. Na trhu je ešte relatívne novým typom elektrického uchovávania energie ale vzhľadom na jeho parametre (nízka hmotnosť,vysoká kapacita, minimálne straty samovybíjaním) je ideálnym adeptom pre tento projekt. Využíva sa napríklad v RC modeloch a v množstve iných aplikácií kde sa ráta s vyšším odberom prúdu. Batéria pre UPS musí na výstupe poskytnúť napätie približne 12 V a prúd 3 A s dostatočnou kapacitou pre dlhú výdrž chodu ústredne po výpadku sieťového napätia.

Obr. 3.5: UPS akumulátor Li-pol SWISS ARMS 11,1 V 1200 mAh 25C[25]

SD-karta

(Z ang.Secure Digital) je elektronické zariadenie pre ukladanie dát. Využívaná je v širokom okruhu elektronických spotrebičov ako sú notebooky, mobily, fotoaparáty, prehrávače atď. Je založená na pamäti Flash EEPROM. Z počiatku bola vyrobená ako náhrada HDD z rozmerových dôvodov. Dnešné SD karty dosahujú dostatočných kapacít pre využitie na rýchle ukladanie množstva dát. Práve pre veľkosť kapacity a minimálne rozmery vyhovuje pre ukladanie dát v tomto systéme práve SD-karta. Na čítanie a zápis je ale potrebné osadiť do ústredni modul kompatibilný s MCU(3.6).



Obr. 3.6: Modul pre čítanie a zápis SD karty[26]

Konkrétny modul je určený pre mikro SD karty a disponuje komunikačným rozhraním SPI. Je kompatibilný s akýmkoľvek MCU rady AVR a podporuje čítanie-/zápis formátov FAT16 a FAT32.[26]

RTC

(Z ang.Real Time Clock) je RTC elektronické zariadenie pre meranie reálneho času. Interné časovače a počítadlá v mikrokontroléroch sú prevažne vždy energeticky závislé. To znamená, že pre prácu ako aj na uchovávanie dát potrebujú stály prísun elektrickej energie. Výnimkou je interná pamäť EEPROM, ktorá uchováva uložené dáta aj po odpojení napájania, avšak s nimi nie je schopná nijak pracovať. V prípade počítania reálneho času je potrebné aby bežal tento proces neustále aj po resete či odpojení napájania. K tomu sa využívajú špecializované počítadlá reálneho času RTC s pripojenou malou batériou, ktorá dodáva elektrickú energiu aj po vypnutí systému. Pre tento systém bol zvolený integrovaný obvod DS3231 s externou gombíkovou batériou CR2032 a prídavnou pamäťou EEPROM AT24C32 pre ukladanie dát a adresáciu komunikácie pomocou rozhrania I2C.

Obr. 3.7: RTC IC DS3231

Hlásiče

1. Detektor PIR
2. Odchodové tlačidlo
3. Magnetický detektor otvorenia
4. Koncový spínač

Detektor pohybu PIR

Funkcionalita detektoru PIR je opísaná v kapitole 1.4.3. Detektor v tomto navrhovanom systéme bude slúžiť čiste na snímanie priestoru okolia dverí. Nebude potreba sa zameriavať na chodby, stropy či vzdialenejšie objekty. Dôvodom je zameranie práce

na systém EKV, kedy nejde o zabezpečenie celého objektu ale iba dverí, takže stačí keď bude detektor snímať prechod cez ne. Samozrejme prípadnému postrannému detegovaniu sa nezabraňuje. Ideálnou variantou detektora pre tento druh aplikácie je HC-SR501. Jedná sa o univerzálny PIR modul kompatibilný s AVR MCU, snímacím dosahom 7 metrov a uhlom snímania 110°. Pracuje na napätí (3 až 20 V) pri ktorom má odber prúdu $< 60\ \mu A$ čiže je prevádzkovateľný aj z baterky. Modul na základe detekcie vysiela digitálny signál o úrovni 0/3,3 V. Jeho obrovskou výhodou sú jeho malé rozmery, teda má prirodzené dobré maskovanie a navyše sa dá zabudovať do rámu dverí. Na module je možné pomocou dvoch potenciometrov nastaviť dobu detekcie a intenzitu snímania (efektívny dosah).

Obr. 3.8: Detektor PIR, HC-SR501[27]

Odchodové tlačidlo

Slúži na uvedomenie ústredni o požiadavku opustenia stráženej miestnosti. Využíva sa v mnohých systémoch EKV, kde nie je prítomné dvojterminálové riešenie z obidvoch strán dverí. V samotnej podstate nahrádza odchodový terminál, kedy stačí pri odchode stlačiť tlačidlo a systém vám dovolí opustiť miestnosť bez spustenia alarmu. Na túto funkciu je možné využiť akékoľvek mechanické tlačidlo. Často sú k dispozícií rôzne dizajnové prevedenia (viď.3.9).

Obr. 3.9: Odchodové tlačidlo [28]

Magnetický detektor otvorenia dverí

Podrobnou problematikou MD detektorov sa zaoberá kapitola 1.4.3. Magnetický detektor nie je nijak špecificky náročná periféria na vyžadované parametre systému. Je to obyčajný mechanický kontakt spínaný magnetickým poľom čo znamená, že je kompatibilný s akýmkoľvek systémom alebo zariadením. Rozdeľujú sa len na základe formy spínacieho kontaktu (jazýčkový, guľôčkový) a cesty prenosu (drôtové, bezdrôtové). Pre tento návrh sa použije drôtové prevedenie MD nakoľko drôtové prevedenia periférií zvyšujú spoľahlivosť a rýchlosť reakcie systému.

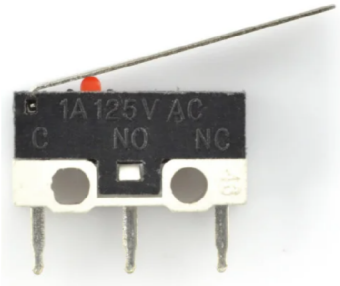
Obr. 3.10: MD otvorenia dverí[29]

Koncový spínač

Slangovo "Koncák"sa využíva na signalizovanie uzamknutia dverí. V prípade kedy máme možnosť dvere uzamknúť i mechanickým kľúčom, je výhodné tento stav snímať hneď z pár praktických dôvodov.

1. Systém bude vedieť, že nikto v miestnosti nie je a môže prejsť do úsporného režimu = menšia spotreba.
2. Systém týmto gestom dostane automatické povolanie ku stráženiu. V prípade vyrazenia dverí spustí poplach.
3. Možnosť zistiť na diaľku či sa ešte niekto nachádza v kontrolovanej miestnosti. Tento bod možno realizovať aj pomocou PIR detektoru ale iba pokiaľ by sa osoba v miestnosti pohybovala v blízkostí dverí.

Koncové spínače sa skladajú z páky a väčšinou troch kontaktov, z ktorých dva slúžia ako prepínacie (NC,NO) a jeden je spoločný (C)(viď. obrázok3.11). Parametricky sa vyrábajú na vysoké napätia a prúdy v rádoch stovky voltov a jednotky ampérov.



Obr. 3.11: Príklad koncového spínača WK320[30]

Akčné zariadenia

1. Piezo siréna
2. Servo
3. Elektrický zámok
4. GSM modul

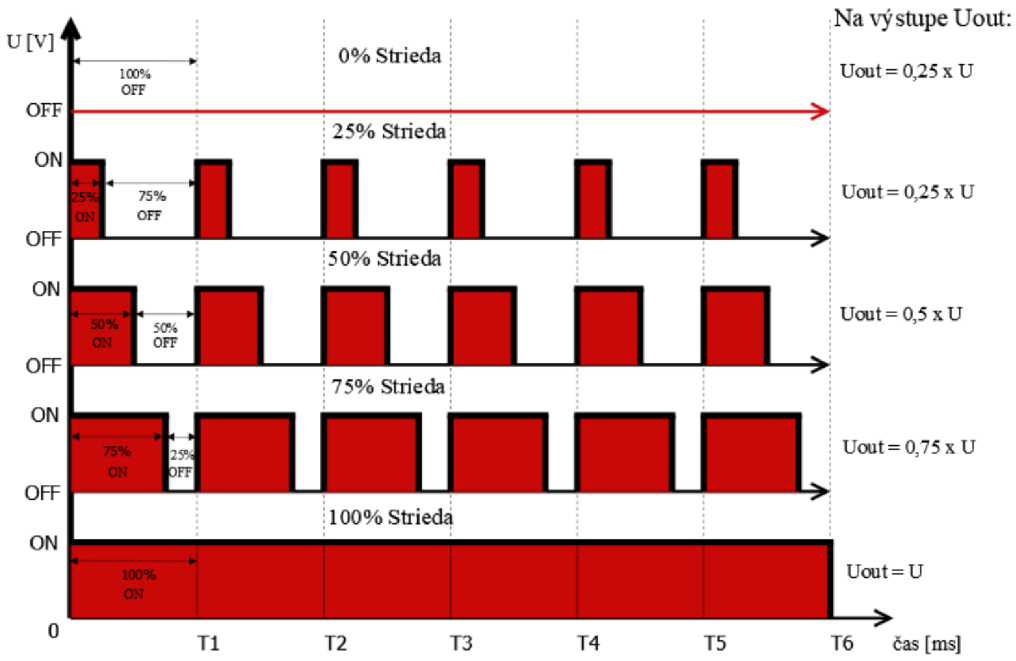
Piezo siréna

Pre tento návrh vyhovuje klasická interiérová siréna so zabudovaným blikačom, konkrétne LS-103 (obr.3.12). Pracovné napätie sirény sa hýbe v rozmedzí 11 až 14 V pri odbere prúdu 280 mA. Jej vysoký akustický výkon 105 dB je realizovaný prostredníctvom 3-vývodovej súčiastky zvanej Alarm boost. Jedná sa o transformátor s dvomi vinutiami a vyvedeným stredom. Pri napájaní z 12 V sa na jeho výstupe generuje napätie okolo 22 V AC. Výstupné napätie z alarm boostu je priamo pripojené na piezoelktrikum. To kmitá na amplitúdé 22 V o frekvencií generovanej alarm čipom AC3Y305. Dosah sirény sa pohybuje v okolí 50 m (viď. efektívny dosah sirén1.12).

Obr. 3.12: Piezoelektrická siréna LS-103[31]

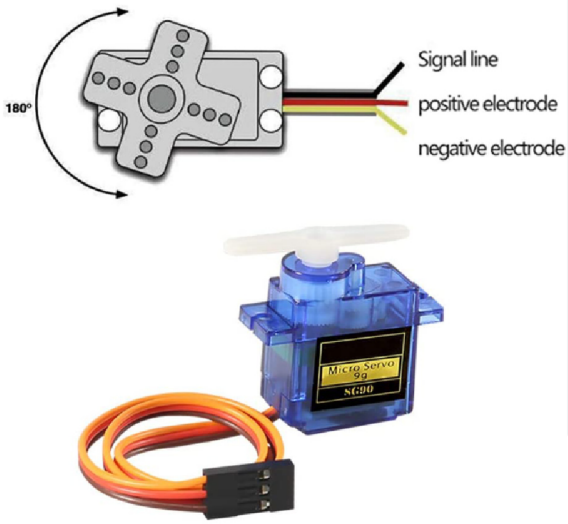
Servomotor

Servomotor je zariadenie pre vykonávanie mechanickej motorickej práce nahrádzajúcej človeka. Existujú rôzne druhy podľa premeny energie ako napríklad parné, hydraulické, pneumatické no v praxi sú najviac využívané elektrické servá. Taktiež sa delia podľa spôsobu vykonávanie pohybu na pozičné alebo rotačné. V tejto práci bude servo zohrávať rolu výsuvného ústrojenstva pre vysúvanie a zasúvanie snímača odtlačkov prstov. Pre túto úlohu vyhovuje pozičné elektrické servo 9g (obr.3.14) s otočným uhlom 180°, bežne používané v malých RC modeloch. Princíp riadenia serva spočíva na signále PWM.



Obr. 3.13: PWM signál

PWM: (Z ang.Pulse Width Modulation) Šírková modulácia impulzu je modulácia periodického signálu zmenou striedy. Pravidelne sa striedajúca vysoká a nízka úroveň (HIGH, LOW) v stanovených periódach T, zapríčiní vznik strednej efektívnej zložky, ktorú je možné využiť ako regulačný signál. Pre lepšie predstavenie by bolo v praxi názorným príkladom rýchle zapínanie a vypínanie stolovej lampy. Čím rýchlejšie by ste ju zapínali a vypínali, tým viac sa bude javiť, že svieti a opačne. Pri PWM modulácií nevznikajú zbytočné tepelné straty na záťaži, nakoľko sa na výstupe pravidelne striedajú iba krajné hodnoty. Nevýhodu je však možný vznik vysokofrekvenčného rušenia vzniknuté spínacím režimom.

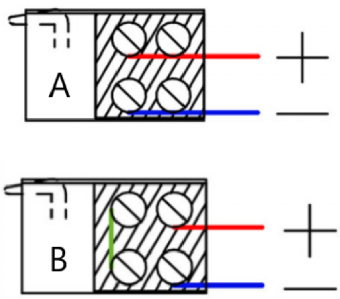


Obr. 3.14: Servomotor 9g [32]

Elektrický zámok EZ

Použitý EZ v navrhovanom systéme EKV bude od Nemeckej firmy GEZE (viď.obrázok1.13). Jedná sa o dvojcievkové prevedenie vrátnika schopné pracovať na striedavý aj na jednosmerný prúd. Prídržná sila pliešku činí 5000 N. Vrátnik je navyše možný prevádzkovať v dvoch režimoch podľa spôsobu zapojenia.[33]. V tejto práci je elektrický zámok prevádzkovaný v jednocievkovom zapojení.

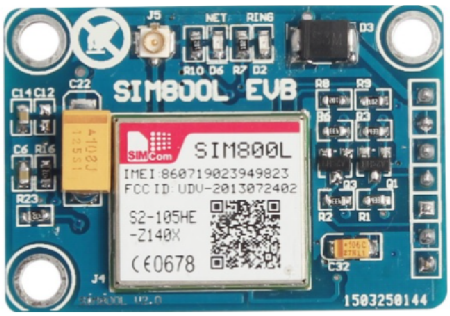
- 2.cievky (obrázok 3.15-A):
  Krátkodobé zaťaženie (max.1 min) 12-24 V AC/DC
  Dlhodobé zaťaženie 12 V AC/DC
  Prúdový odber 0,3 A.
- 1.cievka (obrázok 3.15-B):
  Krátkodobé zaťaženie (max.1 min) 6-12 V AC/DC
  Dlhodobé zaťaženie 6 V AC/DC
  Prúdový odber 0,5 A.



Obr. 3.15: Spôsoby zapojenia svoriek

GSM modul

V zabezpečovacích systémoch je stále množstvo otvorených dverí pre inovácie a hľadanie nových možností ako systémy vyrábať bezpečnejšie a spoľahlivejšie. Jednou z najmladších vychytávok, dnes už samozrejmé, je systémové implementovanie výpočtovej techniky. Ovládanie pomocou smartphonu alebo kontrola stráženej oblasti prostredníctvom programu na PC v PCO je pravidelnou funkciou každého kvalitného EZS. Preto ani navrhovaný systém EKV v tejto práci nezaostáva a disponuje možnosťou pripojenia na mobilnú sieť GSM. Na komunikáciu po sieti GSM sa využíva modul SIM800L, ktorý podporuje posielanie správ typu SMS, MMS aj e-mail. Jeho pracovné napätie je v 5 V a odber prúdu pri pripájania na sieť môže stúpnuť aj na 2 A. Dokáže komunikovať po prenosových frekvenciách (850 MHz, 900 MHz, 1800 MHz, 1900 MHz) čo značí, že môže v ČR komunikovať prostredníctvom siete 2G a 4G/LTE. Komunikácia s MCU prebieha po sériovej linke UART pomocou AT konzolových príkazov dohľadateľných v priručných manuáloch.[34]



Obr. 3.16: Príklad GSM modulu SIM800L[34]

Ovládacie jednotky

1. LCD displej
2. Klávesnica
3. RFID čítačka
4. Snímač odtlačkov prstov
5. Signalizačné LED
6. Smartbutton
7. Bzučiak (Buzzer)

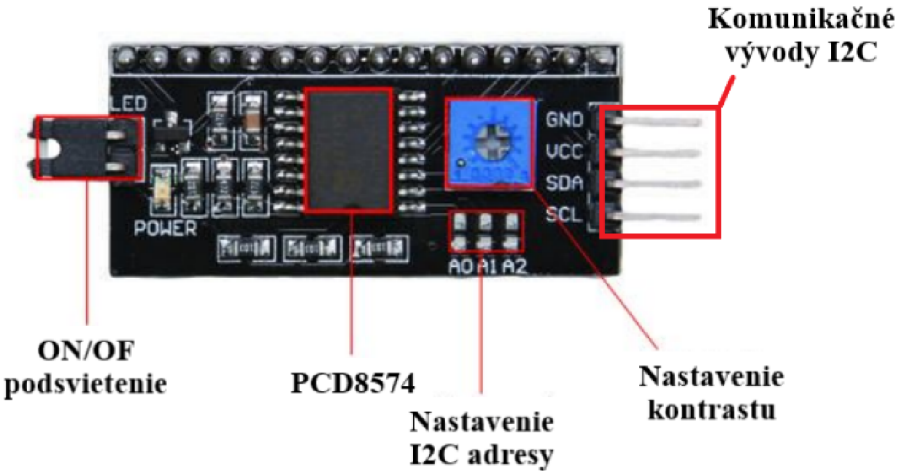
LCD

Základom prehľadného spracovania a ovládania systému je vhodné voľba zobrazovacieho zariadenia. Túto podmienku spĺňa štandardné prevedenie LCD displeja (viď.obrázok 3.17) o veľkosti 20x4 znakov s modrým podsvietením. Nakoľko sme

u vybraného MCU obmedzený počtom riadiacich pinov, nemožno si dovoliť využiť všetky iba na riadenie displeja. Alternatívnou cestou pre výpis je použitie rozširujúceho modulu LCM1602(viď.obrázok 3.18), vďaka ktorému je možné s displejom komunikovať cez rozhranie I^2C. Jeho napájacie napätie je 5 V a rozmerovo [98x60x20 mm] sa radí medzi väčšie displeje čo je obetou za väčšiu zobrazovaciu plochu.

Obr. 3.17: I2C LCD 20x4 [35]

Modul LCM1602 IIC je adresovateľný. To znamená, že je možné komunikovať po jednej zbernici (2 káble) s viacerými displejmi zároveň. Na začiatku je adresa modulu nastavená na hodnotu 0x27. Túto adresu možno zmeniť pomocou kombinácie prepojok na padoch A0, A1, A2 (viď.obrázok 3.18 Nastavenie I2C). Pokiaľ není vytvorená prepojka medzi kontaktami padov, je logická hodnota padu log.1. Ak je prepojka realizovaná tak sa logický stav padu zmení na log.0.



Obr. 3.18: IIC modul LCM1602,[35]

Klávesnica

V tomto návrhu bude systém schopný prostredníctvom klávesnice vykonávať okrem základných autentizačných operácií aj rôzne ďalšie postranné týkajúce sa správy

systému. Preto je potrebné dimenzovať klávesnicu na bohatší sortiment tlačidiel ako len ten základný pre prípadné ďalšie funkcie a na prehľadnejšie ovládanie.

V dnešnej dobe na autentizáciu heslom slúžia celé autonómne sety s vlastnou riadiacou logikou, v ktorých je častokrát zahrnutá aj čítačka kariet. Tento autonómny systém sám vyhodnocuje zhodu DF = OF a ústredni zasiela už len informácie o prípadných akciách terminálu. Z hľadiska návrhu vlastného systému sa tento projekt bude uberať straším spôsobom autentizovania, kedy klávesnica zasiela DF priamo ústredni, ktorá sa postará o porovnanie DF z databázou OF, na základe ktorej vyhodnotí zhodu a udelí resp. neudelí prístup žiadateľovi do chránenej oblasti.

Najvhodnejšou variantov pre tento projekt je klávesnica mechanická s gumenou membránou vzhľadom ku nízkej cene, dlhej životnosti a dobrej spoľahlivosti. Maloprojektové maticové klávesnice pre terminálové využitie sa vyrábajú vo veľkostiach 3x4, 4x4 alebo 5x4 klávesov. Pre tento systém postačí 16 klávesová verzia 4x4. Kontaktný odpor jednotlivých kláves je 500 Ω s odozvou na stlačenie 1 ms.

Obr. 3.19: Maticová klávesnica 4x4[36]

RFID čítačka kariet

RFID karty sa na autentizáciu v systémoch EKV začali používať ako náhrada Wiegandových kariet, ktorých nevýhodou bola ľahká falšovateľnosť. Jedná sa o nizkokapacitné pamäťové rozhranie s bezdrôtovou komunikáciou. Prenos medzi čítačkou a kartou sa realizuje v pásme 125 kHz alebo 13,56 MHz vo vzájomnej blízkosti niekoľkých centimetrov. Rozdiel v kmitočtovom pásme pramení od spôsobu prevedenia čítacieho zariadenia a kontaktnej karty. Požiadavky na čítačku RFID kariet v tomto systéme sú:

1. Vhodné komunikačné rozhranie,
2. Kompaktná veľkosť,
3. Spoľahlivá a bezpečná funkčnosť.

Spomínané parametre spĺňa RFID modul s integrovanou anténou MF RC522, ktorý je v prevedení podľa štandardu ISO/IEC 14443 A/MIFARE a NTAG. Na čítanie kariet sa využíva kmitočt 13,56 MHz čiže je uspôsobený pre mikroprocesorové karty. Je to bezpečnejšia varianta od klasických RFID kariet nakoľko je založená na symetrickej kryptografii. To znamená, že okrem overovania DF = OF, zdieľajú čítačka s kartou spoločnú tajnú hodnotu K (takzvaný "kľúč"), bez ktorého nie je čítačka schopná inú kartu prečítať. Komunikácia s mikrokontrolérom je zabezpečená prostredníctvom rozhrania SPI (signály MOSI,MISO). Je prevádzkovaný na pracovnom napätí 3,3 V , pri ktorom má odber prúdu 13 až 26 mA.

Obr. 3.20: Čítačka MF RC522[37]

Snímač odtlačkov prstov

Najúčinnejšou formou nenapodobiteľného autentizovania sú ľudské morfologické črty (farba očí, farba vlasov, výška, tvar prstov a papilárnych línií). Tým sa ale nevylučuje, že aj tento spôsob autentizácie nemôže byť sfalšovateľný. V praxi sa ku snímaniu ľudskej biometrie využívajú rôzne druhy snímačov uspôsobených pre konkrétnu oblasť. Jedným z najpoužívanejších snímačov biometrií je práve v tomto projekte zahrnutý, snímač odtlačkov prstov.

Každý človek je jedinečný a tak i jeho odtlačky prstov. Jednotlivé odlišnosti v papilárnych líniách prstov, sú snímače schopné detegovať. Pre správnu funkciu v systéme je pre snímač odtlačkov prstov potrebné dostatočné vysoké rozlíšenie snímacieho prvku. Pre tento projekt je zo širokej škály senzorov vybraný optický fingerprint senzor modul AS608 (obr.3.21) s možnosťou sériovej komunikácie pomocou rozhrania UART. Pracovné napätie snímača je 3,3 V pri maximálnom prúdovom odbere < 60 mA. Disponuje taktiež veľmi dobrým rozlíšením 500 dpi. Snímač v sebe zahrňuje vlastnú integrovanú TTL logiku pre vyhodnocovanie odtlačkov a pamäť na dočasné uloženie nasnímaného obrázka.

Obr. 3.21: Príklad snímača odtlačku prsta AS608[38]

Signalizačné LED diódy

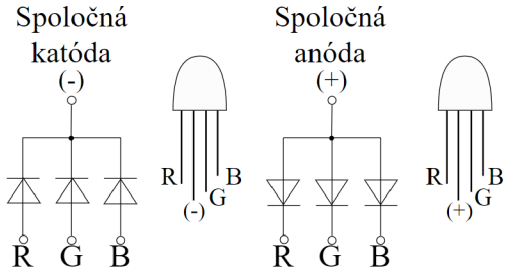
LED použité v práci slúžia na signalizáciu rôznych skutočností. Znázorňujú vznik incidentu, otvorenie či zamknutie dverí atď. Z praktického hľadiska nemajú hlbší význam. Dopĺňajú iba estetickú a interakčnú funkciu pre užívateľa. Ich výber podliehal len rozmerovým kritériám. Pre tieto účely boli zvolené štandardné, GaAs (Gálium-Arzenit) 5 mm LED. Ich pracovné napätie je v rozmedzí 1,8 až 3,2 V (záleží na farbe). Vďaka ich malej spotrebe iba 20 mA sú vhodné i do aplikácií napájaných z batériových zdrojov.

Obr. 3.22: Príklad štandardných GaP LED, 5 mm[39]

Mierna modulácia LED však prišla z dôvodu šetrenia miesta v oblasti terminálov kde bolo treba signalizovať viac ako jeden stav. Jedná sa napríklad o rozsvietenie zelenej farby pri zadaní správneho hesla a naopak červenej pri nesprávnom. Na prevedenie viacerých farieb pomocou jednej LED slúžia RGB LED (Red,Green,Blue). Miešanie farieb je regulované intenzitou svietivosti jednotlivých farebných tónov. Tie sa ovládanú priloženým napätím na diódu v priepustnom smere. Každá farba má však inú škálu spínacieho napätia pri maximálnom prúdovom odbere 20 mA. Preto je potrebné pred každú LED správne nadimenzovať rezistor. RGB diódy sa navyše delia na dva typy podľa spôsobu zapojenia. Jeden so spoločnou anódou a druhý so spoločnou katódou.

1. Napätie v priepustnom smere (Červená): 1,79 V
2. Napätie v priepustnom smere (Zelená): 2,32 V
3. Napätie v priepustnom smere (Modrá): 2,57 V

(a) Reálna RGB LED dióda[40]



(b) Typy prevedení RGB LED

Obr. 3.23: RGB LED

Smartbutton

Jedným z neobvyklých spôsobov autentizovania v systémoch EKV môže byť aj prostredníctvom takzvaného šikovného tlačidla (obr.3.24). Smartbutton alebo Ibutton je RFID komunikátor založený na rovnakom princípe ako čipové karty s rozdielom komunikačnej frekvencie (125 kHz). Do toho systému je dosadený iba ako názorný príklad ďalšieho spôsobu autentizácie bežne používanej v praxi napríklad pri vstupe do panelákov. Komunikácia prebieha pomocou rozhrania onewire kedy sa dáta prenášajú len po jednom kábli. Každý RFID gombík nesie v sebe vopred definovanú adresu v hexadecimálnom tvare, ktorú je MCU schopný rozpoznať pomocou knižníc pridelených ku snímaču. Pracovné napätie Smartbutton čítačky je 5 V pri odbere prúdu 20 mA.

Obr. 3.24: ASHATA Ibutton Dallas reader [41]

Bzučiak

Bzučiak alebo inak Buzzer je malý druh piezoelektrického meniča založeného na opačnom piezoelektrickom jave, premeny elektrickej energie na mechanické kmity.
Aktívny je schopný generovať zvukový signál ihneď po privedení napájacieho napätia. Najčastejšie sa vyrábajú varianty schopné generovať monotónny tón o frekvencií 2 kHz. Využitie nachádza v aplikáciách kde je potreba signalizovať poruchu bez špeciálnych zvukových efektov (napr. PC)
Pasívny potrebuje na rozdiel od aktívneho vonkajší vstupný generátor striedavého signálu pre rozvybrovanie piezoelektrika. Ich bonusom je schopnosť generovať viac rôznych tónov na základe vstupnej frekvencie nosného signálu. Práve tento typ buzzeru je vhodný do tohoto navrhovaného systému kde jeho úlohou bude doplniť interakčné užívateľské prostredie terminálov o škálu zvukových efektov (napr. pípanie klávesnice pri stláčaní kláves). Pracovné napätie pasívneho buzzera je v rozmedzí 3,5 – 5 V pri odbere prúdu do 32 mA.

Obr. 3.25: Pasívny Buzzer 5 V[42]

Tab. 3.3: Súpis komponentov komunikujúcich cez špecifické rozhranie

Periféria	+3,3 V	+5 V	+12 V	DIGI I/O	Rozhranie
Smartbutton	nie	áno	nie	áno	onewire
Servo	nie	áno	nie	áno	PWM
SD	áno	nie	nie	áno	SPI
RFID	áno	nie	nie	áno 5x	SPI
GSM	nie	áno	nie	áno	UART
Snímač odtlačku	áno	nie	nie	áno	UART
LCD	nie	áno	nie	áno	I^2C SCL,SDA
RTC	nie	áno	nie	áno	I^2C SCL,SDA

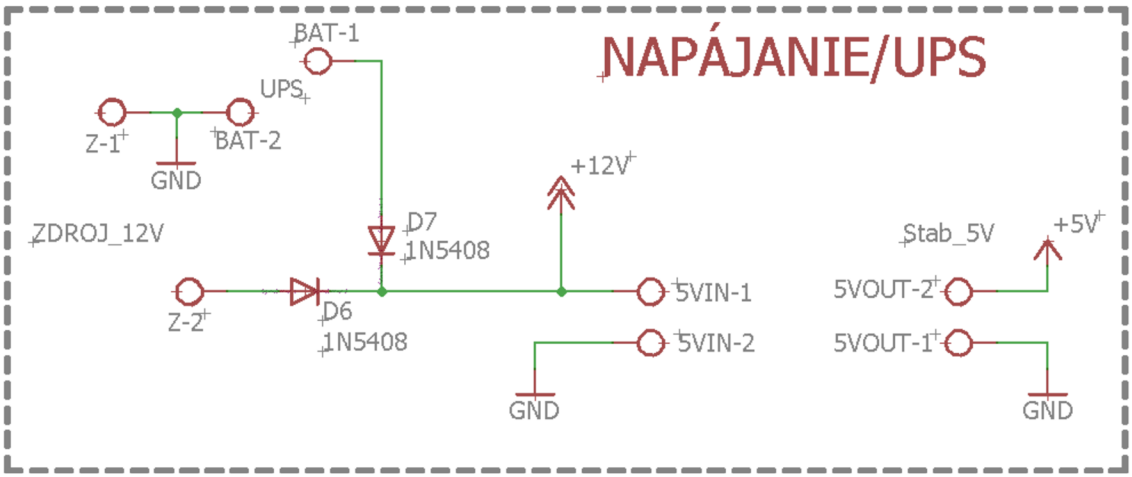
3.2.4 Návrh elektrickej schémy a DPS

Od roku 1943 tvorí doska plošných spojov základ drvivej väčšiny elektrických zariadení. Či sa jedná o malý projekt alebo priemyselný výrobok, málo kedy vyhovuje len kontaktné prepojenie komponentov. Tento fakt si všimol aj Rakúsky vynálezca DPS Ing. Paul Eisler, ktorý ju vyrobil ako časť rádioprijímača počas práce v Anglicku. Existujú aj alternatívne spôsoby prepájania súčiastok a komponentov (breadboard), no tie neposkytujú tak ideálne vlastnosti ako DPS. Navyše dosky plošných spojov majú jednú výraznú výhodu a to možnosť zavedenia automatizácie, nakoľko majú presne stanovené rozmery a parametre.[43] Elektrická schéma a DPS pre túto prácu boli navrhnuté pomocou programu EAGLE 7.6.0 Professional pre Windows (32 bit). Zip súbor celého návrhu je nahratý na priloženom USB -> (Zadná doska práce).

Napájanie a UPS

Napájanie ústredni je realizované pomocou dvoch paralelne zapojených diód 1N5408 (viď. D7, D6 obr.3.26), ktoré zabezpečujú plynulé prepínanie medzi sieťovým napájacím zdrojom a batériou pre UPS. Diódy 1N5408 sú univerzálne, kremíkové, usmerňovacie dimenzované na 1000 V a 3 A. Sledovaným parametrom pri výbere bola veľkosť prúdu.

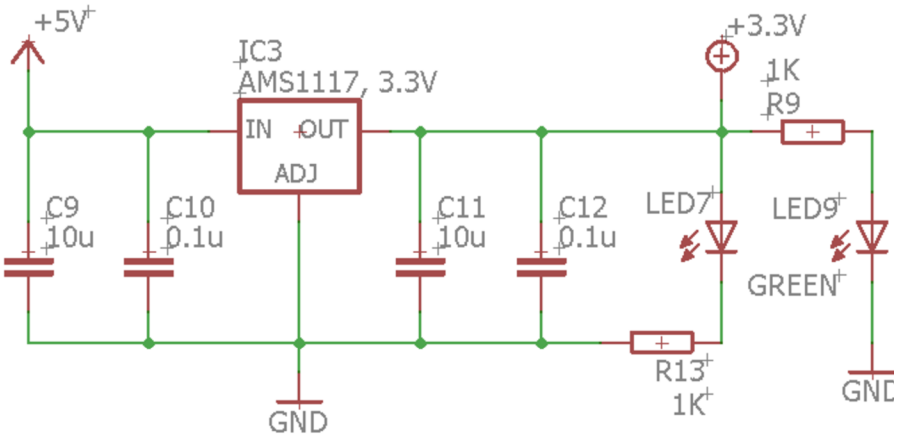
Základný princíp prepínania UPS je založený na diferencií napätí jednotlivých zdrojov ako aj samotnom fyzikálnom princípe polovodičovej diódy a to, že prepúšťa iba v jednom smere. Pokiaľ napojíme na svorky BAT-1 a BAT-2 batériu 11,1 V, vznikne na dióde úbytok napätia 0,6 V a na katóde diódy D7 dostaneme 10,5 V. (Minimálne práci schopné napájacie napätie ústredni je 7 V, ukážka v kapitole meraní viď.obr.3.43). Pokiaľ však pripojíme na svorky Z-1 a Z-2 napájacie napätie zo zdroja 12 V, vznikne na dióde D6 úbytok napätia 0,6 V a ako na katóde D6 tak aj na D7 sa objaví výstupné napätie 11,4 V. Z jednoduchého princípu priepustného smeru diódy vychádza, že ak je na katóde D7 11,4 V a na anóde D7 11,1 V, prepne sa dióda do nepriepustného stavu a tým odstaví prívod od UPS. Keď odpojíme zdroj, všetko sa spätne vráti a dióda D7 znovu začne prepúšťať prúd od UPS. Na výstup usmerňovacích diód je napojený stabilizátor z 12 V -> 5 V a 3 A, ktorý ďalej pokračuje ako napájanie komponentov DPS.



Obr. 3.26: Napájanie a UPS

Stabilizátory

V obvode sú realizované 2 stabilizátory z 5 V na 3,3 V pomocou IC3 AMS1117. Dva sú z dôvodu udržania stabilného napájania. V konečnom dôsledku by postačoval aj jeden ale keďže sa jednalo o 1.prototyp tak sa volili väčšie prúdové rezervy. Na jednom stabilizátore je napájané RTC spoločne so snímačom odtlačkov prstov a na druhom RFID spoločne s modul pre SD-kartu. Na výstupe zobrazeného stabilizátora (obr.3.27) je navyše pripojená LED9 ako indikácia fungovania systému.

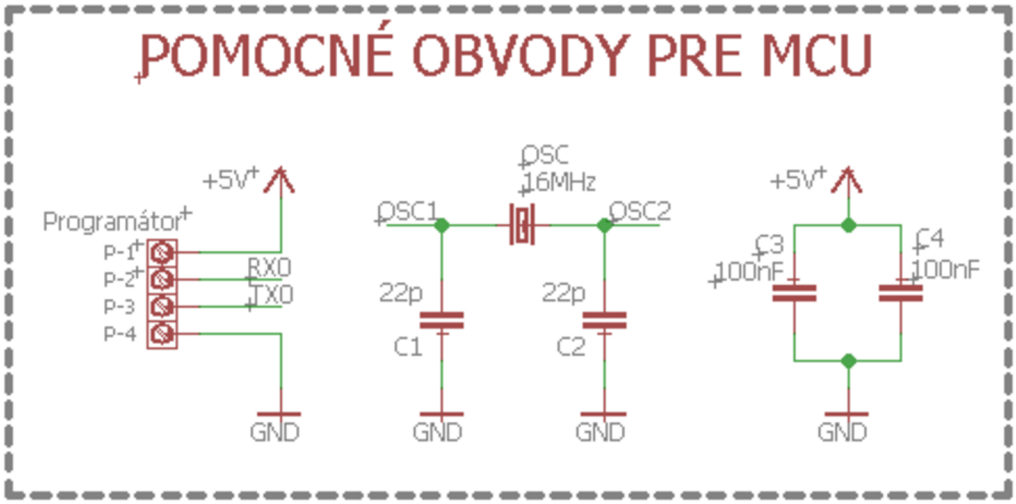


Obr. 3.27: Stabilizátory 3,3 V

Okolité fukcionálne obvody pre MCU

Mikrokontrolér ATmega644-20PU je taktovaný externým kryštálovým oscilátorom OSC 16 MHz (viď. obr.3.28). Ďalej sú pre filtrovanie rušení z napájania zavedené do

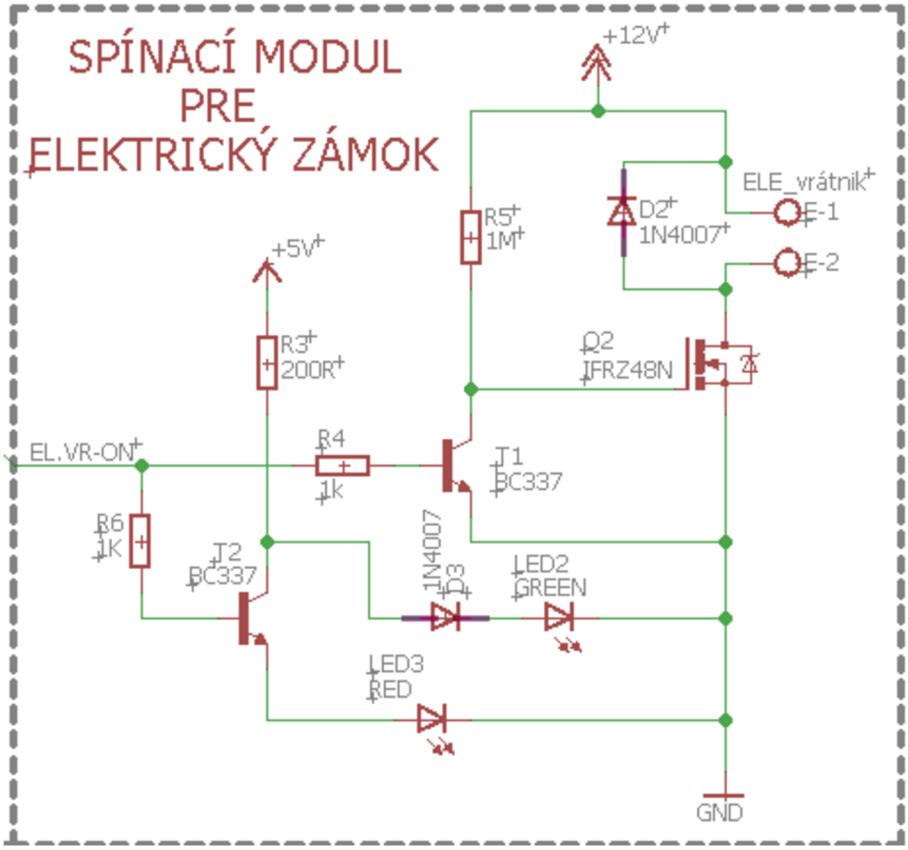
obvodu 2 paralelné 100 nF keramické kondenzátory. A ako posledný je vyvedený 4-pinový konektor phoenix na 1.sériovú komunikačnú linku MCU UART1 pre možnosť externého programovania pomocou programátora.



Obr. 3.28: Doplnkové obvody MCU

Tranzistorový spínač pre elektrický zámok

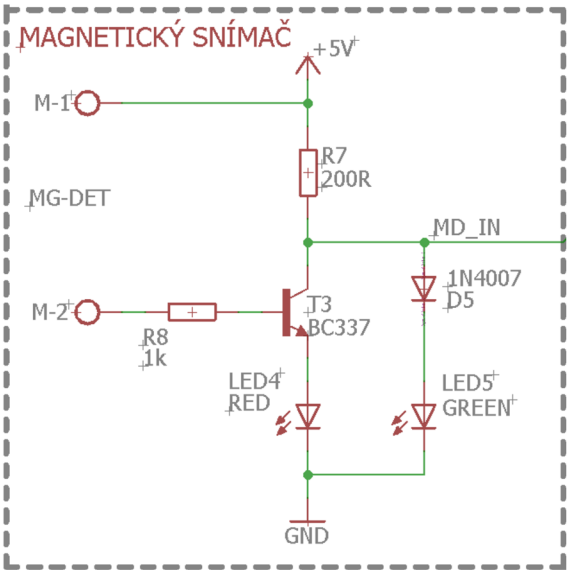
Elektrický vrátnik je realizovaný pomocou solenoidov, ktoré pracujú na napätí 12 V. Maximálne výstupné napätie, ktoré dokáže poskytnúť MCU je však 5 V. Preto je potrebné zaimplementovať do systému spínací prvok, ktorý bude schopný tento nepomer vykompenzovať. Spínací obvod pre elektrický vrátnik (viď. obr. 3.29) je založený na tranzistoroch prevádzkovaných v spínacom režime. Na svorkách elektrického vrátnika je pripojená desaturačná dióda D2, ktorá funguje ako eliminátor zostatkového prúdu, ktorý začne tiecť do obvodu z cievky elektrického zámkou po rozpojení. Na samotné spínanie elektrického zámku je použitý tranzistor MOSFET IRFZ48N s menovitým zaťažením 130 W a maximálnym prúdom Idss 64 A. Na gate tranzistoru Q2 je privedený ďalší spínací tranzistor T1 BC337. Docieli sa tak väčšieho zosilnenia (kombinácia Sziklaiovho a Darlingtonovho páru). MCU tak netrpí prúdovým ani napäťovým nedostatkom a elektrický vrátnik je bez problémov schopný spínať. Posledný tranzistor T2 slúži na prepínanie medzi signalizačnými LED diódami LED2 a LED3, ktoré indikujú aktívny stav elektrického Zámku. Všetky bázy tranzistorov ako bipolárnych tak aj unipolárneho (gate) sú ošetrené vstupným rezistorom pre redukciu vstupného prúdu.



Obr. 3.29: TTL spínač pre elektrický zámok

Tranzistorová logika pre magnetický detektor

Pri obyčajných spínacích prvkoch ako sú napríklad tlačidlá nie je potrebné používať nijaké komplikované zapojenia, doslova postačuje dosadiť sériovo len jeden rezistor. To však neplatí v prípade keď chcete tento stav aj nejak signalizovať. Pre vizuálne potvrdenie uzatvorenia dverí sa preto do obvodu dosadili 2 LED diódy, LED4 a LED5 (viď. obr. 3.30). Každá z nich ale musí svietiť sama a iba za istých podmienok (dvere otvorené alebo zatvorené). Na túto logickú úlohu rozhodovania je využívaný tranzistor T3, ktorý má diódy zapojené do kolektora a emitora. Vo vypnutom stave, kedy je MD rozpojený, bude ustálená hodnota napätia na kolektore 5 V, čo vyvolá to prúdu diódou LED5. V opačnom prípade keď bude MD uzavretý, začne tiecť prúd do tranzistora T3, to vyvolá zopnutie tranzistora a zároveň zvedenie prúdu do zemi skrz LED4. Prúdu, ktorý tiekol predtým do LED5 je postavená ešte jedna prekážka dióda D5 aj s jej úbytkom a teda dióda LED5 zhasne, nakoľko prúd si vyberá cestu menšieho odporu.

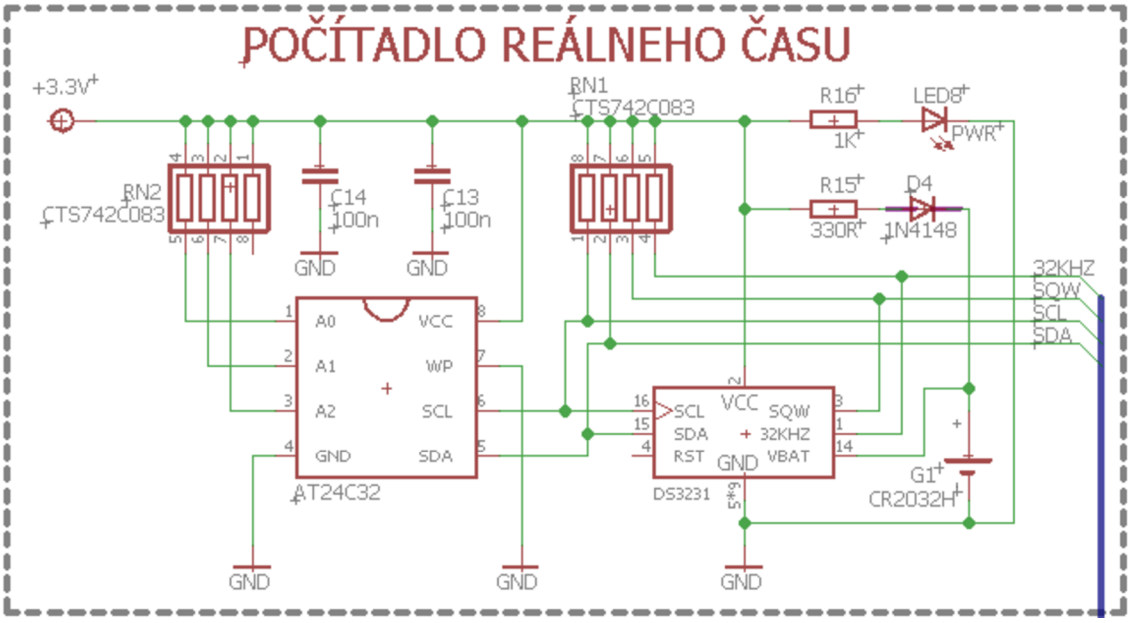


Obr. 3.30: Obvod magnetického detektora

Všetky zvyšné komponenty v navrhovanom systéme fungujú na rovnakom princípe alebo sú zapojené na priamo. Počas výroby práce sa narazilo na menší problém z hľadiska nedostatku výstupných pinov MCU. Tento problém sa podarilo vyriešiť pridaním IC posúvneho (Shift) registra SN74595N, ktorý rozšíril počet výstupných pinov pre spínanie periférií o 6. Shift register je využívaný na spínanie: RGB diódy, snímača odtlačku prstov, servomotora, elektrického zámku, sirény a LED smartbutton readeru. Zvyšné detailné zapojenia sú zobrazené v prílohách (viď. obr. A.1) alebo taktiež na priloženom USB.

Real Time Clock

Schéma RTC (viď. obr. 3.31) je realizovaná pomocou dvoch integrovaných obvodov a to DS3231 (počítadlo reálneho času) a AT24C32 (pamäť EEPROM). Prostredníctvom EEPROM pamäti je možné nastavenie adresy pre komunikovanie po rozhraní I2C. V konkrétnom zapojení je adresa nastavená na 0x57 pomocou permanentných odporov RN2. Taktiež je v obvode zahrnutý header pre gombíkovú 3 V batériu CR2032, ktorej úlohou je držať celkový obvod stále pod napätím pre zamedzenie prerušenia počítania času. Do sérií z batériou je zapojený odpor R15 s diódou D4, ktoré ošetrujú správnu hodnotu nabíjacieho napätia na batérií pri zapnutom systéme. Schéma sa inšpirovala reálnym modulom RTC s použitým obvodom DS3231.



Obr. 3.31: Schéma obvodu RTC

DPS

Od dosky plošných spojov sa požaduje aby spoľahlivo plnila nosnú/opornú funkciu všetkých komponentov na nej osadených a zároveň bola systematicky a úsporne navrhnutá. Rozmiestnenie prvkov na DPS totiž ovplyvňuje výslednú veľkosť, spoľahlivosť a zložitosť inštalácie systému. Najlepšou variantou pre výber DPS je FR-4 (Flame Retardant), ktorá má výborné EMTC vlastnosti a zvýšený samohasiaci prah pre zamedzenie vzniku požiaru pri skrate v obvode. Jej nevýhodou je vyššia cena. Rozmery dosky a topológie vedených ciest sú prispôsobené jej umiestneniu v ráme dverí a rozloženiu komponentov systému. Na výpočet šírok ciest sa využil všeobecný vzťah pre medené vodivé cesty o hrúbke medenej vrstvy $35\mu m$.

Pre $1,5\,mm^2$ prierezu cesty je dovolený prúd $14\,A$. Z toho vyplýva pomer: $9,3\,A/mm^2$. Šírky ciest na navrhovanej DPS sa pohybujú vo veľkostiach (0,3; 0,4; 0,6; 0,8 až 1 mm) a najmenší priemer vrtáku je 0,6 mm. To zaraďuje konkrétnu DPS do IV. konštrukčnej triedy nenáročných aplikácií na výrobu, čo sa odzrkadlí aj na nižšej cene. Najhrubšie cesty sú použité pre výkonové prepoje schopné viesť 3 A pri 12 V (spínanie elektrického zámku/sirény) a najtenšie pre dátové prepoje. Detailné zobrazenie celkovej DPS je v prílohách (viď. obr.B.1 a B.2).

3.2.5 Zostrojenie modelu dverí

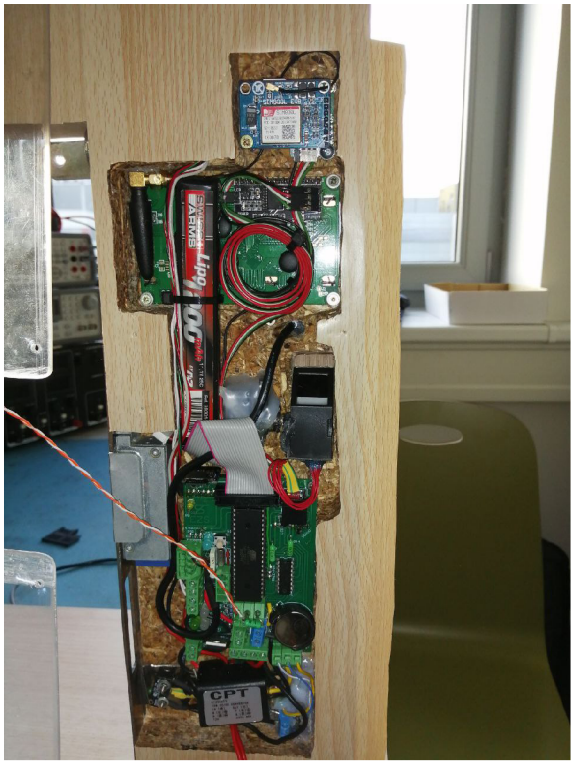
Súčasťou náplni práce nie je len návrh systému po elektronickej stránke ale aj zostrojenie hmotného modelu dverí (viď.obr. 3.32) s ohľadom na vhodné bezpečnostné prevedenie. Drvivú väčšinu materiálu výrobku tvorí drevo. Základná stolárska doska MDF (Medium Density Fibreboard) ponúka dostatočnú pevnosť pri zachovaní dobrej opracovateľnosti. Navyše je veľmi dostupná a často využívaná v praxi napríklad konkrétne aj na výrobu dverí. Tento druh dosky je použitý na celý model od zárubni cez podstavu, dvere a aj bočné oporné steny.

Postupný vývoj a výroba dverovej konštrukcie od modelu po hotový výrobok je popísaná obrázkovou metódou na priloženom USB -> (Zadná doska práce).

Práve bezpečnostné prevedenie je na tomto systéme špeciálnou doménou. Nejedná sa o bežne komerčne dostupné systémy EKV s riadiacou externou ústredňou, ktorá sa musí montovať na vnútornú stenu stráženej miestnosti. I keď by bol systém v tomto prípade decentralizovaný, tak hrozí riziko odpozorovania polohy umiestnenia riadiacej krabice ústredni a následného zdefunkčnenia zo strany útočníka. Druhý spôsob systému EKV v praxi sa zakladá na čiste terminálovej báze, prepojenia terminálu s určitým akčným členom, najčastejšie elektrickým zámkom. Tento spôsob je riešením predošlého prípadu no ak by užívateľ požadoval od systému funkcií viac ako len prístup pomocou jedného terminálu, tak to nie je možné z rozmerových obmedzení, prípadne bude systém ukrátený o plnohodnotné možnosti využitia.

Obr. 3.32: Ilustračné foto hotových dverí

Práve táto práca je akýmsi kompromisom medzi prvý a druhým spôsobom realizácie systému EKV a to osadením celého ústrojenstva do rámu dverí (viď. obr.3.33). Priestoru pre zakomponovanie prídavných funkcií je v stene neobmedzene a zároveň zasadenie do steny nevzbudzuje pozornosť zo strany útočníka dokým o tom nenadobudne povedomie.



Obr. 3.33: Elektronika systému zasadená do zárubne

Ďalšou bezpečnostnou vychytávkou systému je neštandardné prevedenie prístupnosti terminálu. V informatickom sektore počítačovej bezpečnosti sa tento pojem nazýva "Security by obscurity", kedy k utajovaniu dát dochádza používaním neštandardných konštrukcií či postupov. V tomto systéme sa to týka snímaču odtlačkov prstov, ktorý sa sprístupní len po prevedení presne definovaných úkonov. V opačnom prípade bude jeho umiestnenie a prístup utajený v dutine steny. Pre manipuláciu so snímačom sa využíva servo 9g. Jeho úlohou je vysúvať a zasúvať snímač cez vopred na mieru vyrezaný otvor. Význam zasúvania spočíva v znemožnení odsnímania tepelnej stopy odtlačku prsta útočníkom, ktorý by ju následne mohol použiť ako zdroj útoku. Týmito a ďalšími podobnými bezpečnostnými funkciami disponuje navrhovaná realizácia EKV. Zvyšné si len stručne popíšeme:

UPS - Neprerušiteľná dodávka energie v prípade zlyhania sieťového napájania. Použitá Li-pol batéria s kapacitou 1200 mAh postačuje pre chod systému za bežnej

prevádzky na 15 h čo je vzhľadom ku jej veľkosti veľmi dobrá výdrž. Pri častom využívaní vstupu však stúpa odber a tým môže výdrž batérie klesnúť až na sedminu.

GSM - Funkcia tichého alarmu. Každý zabezpečovací systém obsahuje poplašné zariadenie, najčastejšie v prevedení akustickej sirény. Tento systém ale ponúka využitie takzvaného tichého alarmu prostredníctvom GSM mobilnej siete. V prípade zistenia incidentu, systém vytočí alebo zašle SMS o poplašnom hlásení na vopred nastavené telefónne číslo bez vedomia útočníka. Kontaktovať tak môže aj priamo PCO alebo iné bezpečnostné inštitúcie, ktoré môžu ihneď zasiahnuť.

Elektrický zámok - zohráva bezpečnostnú funkciu sám o sebe, nakoľko je jedinou časťou celej konštrukcie, ktorá bráni proti otvoreniu dverí. Z toho dôvodu musí byť spoľahlivý a odolný. Konkrétny EZ použitý v tejto práci má parameter zádrži pliešku stanovený na 5000 N čo znamená, že pri vodorovnom uložení dverovej konštrukcie by mal vydržať uniesť na dverách váhu 500 kg.

Na bezpečnostnom prevedení sa podieľajú dokopy tri faktory. Mechanická a elektrická konštrukcia ale taktiež dôležitým tretím faktorom je aj programová vybavenosť. Práve v tejto časti systému môže dôjsť nedokonalým ošetrením všetkých možných kódových stavov a rizík ku zlyhaniu.

3.2.6 Popis programu a funkcionalita systému

Medzi anatómiou ľudského tela a elektronickým systémom existujú isté podobnosti. Tak ako sa človek skladá z mäsa a kostí aj elektronický systém musí obsahovať svoje potrebnosti. Mikrokontrolér predstavuje mozog systému. Moduly a periférie znázorňujú všetky údy, s ktorými je človek schopný vykonávať prácu. A ako posledné bez čoho by žiadna živá bytosť nemohla existovať je duša. Tú v elektronickej sfére predstavuje program. Jedná sa o softwarové vybavenie, na prvý pohľad neviditeľné no zdanie môže klamať. Bez neho by bol vytvorený prototyp iba holou nepoužiteľnou maketou.

Program pre MCU v tejto práci je napísaný prostredníctvom open source programovacieho prostredia Arduino IDE 1.8.18 v programovacom jazyku Wiring, čo je konštrukčne prerobená verzia programovacieho jazyka C a C++.

Pred začiatkom programovania bolo potrebné si upraviť programovacie prostredie o prídavné knižnice pre komunikáciu s periférami ale aj MCU samotným. Na vypálenie zavádzača (bootloader) sa použila platforma Arduino UNO v nastavení ISP. Nastavenie bootloaderu prispôsobeného na MCU ATmega644-20PU zabezpečil stiahnutý skeč v jazyku C pod názvom MightyCore dohľadateľný na prítomnom linku: $(https://mcudude.github.io/MightyCore/package_MCUdude_MightyCore_index.json)$.

Po úprave programovacieho prostredia sa mohlo prejsť ku prvotným programovým testom systému. Pre nahrávanie kódu sa využilo externého prevodníku (USB to TTL) zapožičaného u vedúceho práce. Funkčnému programovaniu predchádzalo množstvo overovacích testov jednotlivých periférií a komunikačných rozhraní. Výsledný kód hotového funkčného systému EKV zaberá 64% pamäte Flash a 84% pamäte RAM čo značí o dobrom výbere MCU. Dokopy aj s komentármi sa roztiahol na 1922 riadkov pričom všetky hlavné body programu sú v ňom prehľadne popísané aj s rýchlym návestidlom na riadok v obsahu (viď. priložený program na USB). Programom sa teda práca nebude detailnejšie zaoberať nakoľko všetky subjekty kódu sú jednoduché a jasne pochopiteľné z jeho štruktúry. Navyše niektoré časti kódu sú sofistikovanejšie a nebolo by prehľadné dosádzať ich do práce. Pre demonštrovanie princípu a funkcie programu bude slúžiť stručný popis doprevádzaný prehľadnými vývojovými diagramami.

Celkový program sa skladá zo 4 častí:

1. Definícia konštánt – v tejto časti sú definované všetky číselné premenné a konštanty používané počas celého behu programu. Tak isto sú v nej zahrnuté knižnice či bindovanie pinov.
2. Void setup – prvá časť funkčného programu. Prvotné inicializovanie vstupno výstupných pinov MCU. Zároveň sa tu štartujú všetky komunikačné rozhrania a vykonávajú prvé overovacie, vyrovnávacie a štartovacie funkcie.
3. Void loop – hlavná časť programu (najdlhšia zo všetkých štyroch). Tvorí výslednú formu priebehu správania systému EKV.
4. Definícia funkcií – nachádza sa za loopom. Definíciou funkcií sa zredukoval počet riadkov programu a zároveň sprehľadnil celkový syntax. Funkcie sú všetky osobne vytvorené.

Princíp ovládania výstupnej hodnoty Shift registra

Na spínanie výstupných periférií (LED, siréna, EZ...) sa využíva posuvný register SN74595N. Jeho riadenie prostredníctvom MCU funguje na 3 pinoch. LATCH, DATA a CLK. Tieto tri signály je potrebné v presných intervaloch meniť. Na to slúži už vopred preddefinovaná funkcia (shifOut). V kóde sa zapisuje nasledovne (viď.kód 3.34). V tomto programe je riadenie postavené na hexadecimálnej sústave z dôvodu najjednoduchšieho spracovania riadiacej hodnoty. Na začiatku zápisu bitov do registra je potrebné snížiť hodnotu signálu LATCH na nízku úroveň. Následne sa prevedie posuv jednotlivých bitov od LSB po MSB. Po ukončení posúvania možno zapísané bity na jednotlivých klopných obvodoch vyniesť na výstup zodvihnutím úrovne signálu LATCH na HIGH.

```
digitalWrite(latch, LOW);
shiftOut(data, clk, LSBFIRST , 0xE5);     // Základný stav, všetko vypnuté.
digitalWrite(latch, HIGH);
```

Obr. 3.34: Zápis hexadecimálnej hodnoty E5 do shift registra

Pracovanie s integrovanou pamäťou EEPROM

Počas tvorby prototypu sa narazilo na množstvo identifikovateľných problémov. Jedným z nich je aj disfunkcia modulu pre SD kartu. Nakoľko je ukladanie dát v systéme potrebné, musela sa nájsť pre tento úkon iná cesta.

Pozitívnou stránkou zvolenia MCU ATmega644-20PU je taktiež prítomnosť integrovanej pamäte EEPROM, ktorú možno voľne ovládať. Preto je pre funkciu ukladania kariet využívaná práve interná pamäť MCU. Veľkosť internej pamäte zvoleného MCU je 2 kB čo bohate postačuje pre objem dát tohoto typu.

V programe stačí jednoducho zahrnúť preddefinovanú knižnicu v jazyku C, ktorá sa postará o všetky náležitosti pre komunikáciu s pamäťou. V ďalších krokoch sa s pamäťou pracuje už len ako s klasickým jednodimenziálnym poľom a veľkosti 2048 b.

Pre zápis a čítanie z pamäti je ale aj napriek tomu potrebných pár konštrukcií, ktoré sú definované vo funkciách strEPP a EPPstr (viď.kód 3.35).

```
void strEEP(int address, String str) {       // Zápis do EEPROM
  byte len = str.length();
  EEPROM.write(address, len);
  delay(5);

  for (int i  = 0; i < len; i++) {
    EEPROM.update(address + 1 + i, str[i]);
    delay(5);
  }

}

String EEPstr(int address) {                // Čítanie z EEPROM
  int len = EEPROM.read(address);
  char DAT[len + 1];

  for (int i  = 0; i < len; i++) {
    DAT[i] = EEPROM.read(address + 1 + i);
  }
  DAT[len] = '\0';
  return String(DAT);
}
```

Obr. 3.35: Funkcie pre zápis a čítanie z EEPORM

Funkcionalita systému

Nakoľko je navrhovaný systém členitý, bude prehľadnejšie nasledujúci popis rozdeliť do samostatných častí sprevádzaných vývojovým diagramom.

1. Hlavné menu: Po naštartovaní a inicializácií systému sa objaví na displeji užívateľa základná obrazovka (viď.obr.3.36). Na nej stojí názov práce, dátum, čas a deň. Tieto informácie získa MCU z obvodu RTC. Následne sa začne súčasne vykonávať počítanie času a snímanie obsadenia čítačky Ibuttonu. Pokiaľ užívateľ nepriloží Ibutton knoflík do doby 15 s, systém ho sám na to vyzve po dobu 2 s. Následne sa znovu vráti základné zobrazenie názvu, dátumu, času a dňa. Tento cyklus sa opakuje do momentu pokým sa nepriloží nejaký z RFID knoflíkov. Po priložení čierneho RFID knoflíku, systém rozpozná, že sa jedná o "Master" a plynulo prejde do správy systému. V prípade detegovanie akéhokoľvek farebného knoflíku, systém zaháji sekvenciu autentiozovania. Prehľadné zobrazenie behu programu je zobrazené aj vývojovým diagramom (viď.obr. C.1).

Obr. 3.36: Úvodná obrazovka

2. Autentizácia: Po priložení akéhokoľvek farebného RFID knoflíka na čítačku, systém vypíše na displeji jeho farbu ako indikáciu rozpoznania a následne zaháji sekvenciu autentizovania. Tá prebieha v samotnom základe v 4 krokoch. Prvým bolo autentizovanie pomocou Smartbuttonu. V druhom kroku systém vyzve užívateľa o priloženie prstu na snímač odtlačkov prstov (viď. obr.3.37). V treťom kroku systém požaduje priloženie RFID mikroprocesorovej karty o terminál (viď. obr.3.38). A ako posledným štvrtým krokom je zadanie 6 miestneho číselného hesla (viď. obr.3.39). Po správnom prevedení všetkých autentizačných úkonov systém povolí vstup do stráženej miestnosti odblokovaním elektrického zámku sprevádzaného akusticko-vizuálnym efektom. Mohlo by sa zdať, že je to príliš jednoduché no každý autentizačný krok je doplnený o bezpečnostné opatrenia. Tými sú napríklad časové obmedzenie trvania autentizácie na jednom termináli (časomiera sa vždy zobrazuje v pravom hornom

rohu displeja) alebo obmedzený počet pokusov pri chybnom overení DF. Konkrétny čas na autentizovanie je u každého druhu terminálu 30 s a počet chýb stanovený maximálne na 3. Pri každej snahe o porušenie stanovených pravidiel systém upozorní autoritu zaslaním varovnej SMS na mobilné zariadenie. Po zahájení autentizačného protokolu z neho nie je inak možné vystúpiť. Prehľadné zobrazenie behu programu pomocou vývojového diagramu (viď.obr. C.2).

Obr. 3.37: Autentizovanie biometrikou

Obr. 3.38: Autentizovanie predmetom

Obr. 3.39: Autentizovanie znalosťou

3. Správa systému: Alebo inak nastavenia, slúžia na vykonanie autorizačných činností, zaevidovanie nového užívateľa do systému alebo nastavenie spôsobu alarmu. Do nastavení sa možno dostať iba za pomoci čierneho "Master" buttonu. Po priložení o čítačku ho systém automaticky rozpozná a prepne ústredňu do režimu správy (viď.obr.3.40). Tu systém ponúka na výber zo štyroch možností pre nastavenie. Prepis karty umožňuje pridávanie alebo prepisovanie

RFID kariet. Systém disponuje štyrmi pozíciami pre ukladanie kariet, ktoré je možné ľubovoľne meniť a prepisovať. Ďalšou možnosťou ako z názvu vyplýva je pridanie odtlačku prsta. Alarmová metóda je spôsob akým bude systém o vzniku incidentu autoritu/užívateľa informovať. Systém ponúka na výber z dvoch možností a to, tichý alebo hlasný alarm. V prípade tichého alarmu je vznik incidentu signalizovaný vytočením vopred zadaného telefónneho čísla do systému. Naopak pri zvolení hlasného alarmu je vznik incidentu signalizovaný rozozvučaním sirény. Poslednou možnosťou voľby v nastaveniach je ukážka hesla, kedy systém zobrazí na 2 sekundy prístupové heslo v prípade krátkodobej pamäte užívateľa. Z každého bodu v nastaveniach sa možno vrátiť späť stlačením klávesy "#". Týmto spôsobom sa možno vrátiť až na hlavné menu (viď.obr. C.3).

Obr. 3.40: Správa systému

4. Sleep mode: Ďalšou funkciou systému je prechod do spánkového režimu v momente uzamknutia dverí. Keď sú dvere uzamknuté tak by bolo zbytočné prevádzkovať celé systém EKV, nakoľko nikto sa dnu aj tak dostať nemôže. Preto je na detekciu zapadnutia západky do protiplechu dverí určený koncový spínač, ktorého aktiváciou sa systém prepne do spánkového režimu. V činnosti ostane jedine detektor pohybu PIR, ktorý bude naďalej kontrolovať stav v stráženej miestnosti a v prípade detekcie incidentu o tom ústredňu informuje. Tá hlásenie vyhodnotí a zašle SMS prostredníctvom sieti GSM na mobilný telefón autority prípadne na PCO. Samozrejme po vykopnutí dverí je akustická siréna ihneď pripravená k aktivácií aj po prebudení so spánkového režimu.

3.2.7 Meranie a overenie funkčnosti

Posledným štádiom dokončenia prototypu systému EKV po skonštruovaní je jeho patričné otestovanie. Priebežné testy funkcionality systému samozrejme prebiehali počas celého vývoja a výroby, avšak konečné celkové testy sú istotou potvrdenia správnej funkčnosti.

Zameranie testov sa špecializovalo na mechanickú odolnosť konštrukcie. Overovanie prudkými opakujúcimi sa zabuchnutiami dverí. Tak isto splnil požadovanú mechanickú pevnosť aj elektrický zámok, ktorý ani po vyvinutí značnej sily nepovolil.

Čo sa týka testov po elektronickej funkcionálnej stránke, tie boli už overené v predošlej kapitole. Predsa však neboli prevedené všetky, hlavne tie výkonové.

Výkonové meranie spotreby prebiehalo na laboratórnom zdroji DIAMETRAL L240R51D. Pri napájaní ústredni s napätím 12 V, bol prúdový odber po ustálení systému 0,08 A (viď.obr. 3.41). Pri nábehu však môže prúd vzrásť až na trojnásobok. Je to spôsobené pripájaním GSM modulu do mobilnej sieti a nastavovaním shift registra do neutrálneho stavu. Nie vždy sa po zapnutí systému objaví na výstupe shift registra rovnaká hodnota. Práve tá sa na začiatku štartu systému resetuje. Keďže je shift register využívaný na spínanie periférií, môže sa stať na zlomok sekundy, že zapne alarm, elektrický zámok alebo preblikne iná z periférií naň pripojených.

Obr. 3.41: Odber za neutrálnych podmienok

Pri zapnutom elektrickom zámku (viď.obr.3.42) bola výsledná hodnota prúdu odpovedajúca parametrom definovaným výrobcom a to, že pri jednocievkovom zapojení sa môže zámok prevádzkovať na 12 V pri prúdovom odbere 0,5 A. 10 mA je prúd pre chod samotného systému.

Obr. 3.42: Odber pri zopnutom elektrickom zámku

Doplnkovým skúšobným meraním bolo overenie minimálneho možného napájacieho napätia, pri ktorom je ústredňa a celkovo systém ešte schopný fungovať. Pomalým plynulým uberaním napätia sa prišlo na hodnotu 7 V, kedy sa prvé známky nezrovnalosti začali objavovať na LCD displeji (odchádzali jednotlivé zobrazovacie body). Pri tak malom napätí však ale nebude fungovať princíp UPS a teda je to pre správnu funkčnosť systému nepoužiteľné. Zároveň došlo vplyvom Ohmovho zákona pri znížení napájacieho napätia ku vzrastu prúdu, čo je navyše neefektívne zo strany spotreby.

Obr. 3.43: Minimálne napájacie napätie v kľudovom stave

Po výkonových testoch sa následne zahájila testovacia línia elektronického systému EKV samotného. Otestovali sa všetky možné stavy a funkcie, ktorými systém disponuje pre prípadný debugging systémového programu. Postupnými testami sa prišlo na pár drobných chýb v programe ako je chýbajúci delay alebo možnosť redukcie programu, no nakoľko už nezostal čas pre opätovné rozoberanie a nahrávanie programu do dverí, ponechal sa systém v kondícií posledného programovania.

Záver

Výsledkom tejto semestrálnej práce je hotový návrh a realizácia hmotného prototypu pre systém elektronickej kontroly vstupu. Jeho zostavenie a použité prvky naplnili zadanie stanovené na začiatku semestra. Systém EKV je teda schopný autentifikovať užívateľov pomocou RFID čítačky mikroprocesorových kariet a optického snímača odtlačkov prstov. Umožňuje tiež autentifikovanie a správu systému prostredníctvom maticovej klávesnice. Do ústredni je možné pripojiť množstvo ďalších konfigurovateľných periférií ako sú sirény, magnetické detektory otvorenia dverí, koncové spínače, LCD displej, detektor PIR, elektronický vrátnik a plus prídavné vizuálno-akustické interakčné zariadenia ako sú LED diódy či buzzer. Prídavnými extra funkciami systému EKV sú, podpora komunikácie prostredníctvom GSM mobilnej siete či kompatibilita s onewire čítačkou Smartbutton. Pri realizácií sa dbalo na vhodné bezpečnostné prevedenie. Z toho dôvodu je v systéme obsiahnutých množstvo bezpečnostných prvkov ako elektrických tak mechanických. Názorným príkladom je samotná 3 faktorová autentizácia, použitý elektrický zámok s prídržnou silou 5000 N či výklopné prevedenie snímača odtlačku prsta.

Ústredňa a teda celý systém je postavený na mikrokontroléri z rodiny AVR rady ATmega644-20PU. Konkrétny výber mikrokontroléra vyplýva z jeho vhodných parametrov a prijateľnej ceny. Všetky podrobné parametre a postupy výberu jednotlivých prvkov sú v projekte jasne opísané.
Ani tento návrh systému sa ako každý prvotný prototyp nezaobišiel bez malých chýb a nezrovnalostí, ktoré sa však podarilo v konečnom dôsledku všetky vyriešiť. Najčastejšou príčinou porúch boli elektrostatické výboje pri nedostatočnom dodržaní ESD ochrán a nekvalitná výroba DPS.

Využitie systému má v praxi veľký potenciál pri ochrane prísne strážených priestorov bánk, laboratórií, armádnych skladov a mnoho ďalších. Nemusí sa dokonca jednať len o stráženie a kontrolu vstupu do miestnosti. Tento systém je totiž iba modelom a jeho reálne využitie siaha omnoho ďalej (trezory, riadenie jadrovej elektrárne). V dnešnej dobe je systém EKV veľmi známy a široko rozšírený, čo z danej témy nerobí nijaký prevratný objav. Prínosom práce do tejto problematiky je napríklad lacnejšia varianta realizácie systému ako ponúkajú dnešné autorizované firmy na trhu. Len jeden obyčajný prístupový terminál od nemenovanej spoločnosti sa pohybuje v hodnote približne 2905 Kč. Navyše keď sa zoberie do povedomia fakt, že bežným užívateľom nie je potrebné také množstvo funkcií akým disponujú moderné ústredne, je cena za tieto komponenty príliš vysoká. Ďalšou výhodou je jednoduché prevedenie systému, ktoré zaručí rýchlu a jednoduchú správu, možnú i zo strany užívateľa. Navyše je systém založený na embedded štruktúre, čo znamená, že všetky implementované zapojenia si volí návrhár podľa potreby, vrátane tvaru DPS, čo mu

dodáva na univerzálnosti a flexibilnosti. Možnosťou regulovať rozmery sa otvorila cesta ku praktickému prevádzaniu dizajnu ústredni napríklad aj do rámu dverí, čo je pre útočníka nepredpokladaným útočiskom. Celkový čas strávený tvorbou tejto práce sa odhaduje na cca. 300 hodín bez započítaného času čakania na DPS. Vypočítaná celková suma minutá na realizáciu projektu činí 5930 Kč vrátane konštrukčných materiálov. Výsledná suma projektu by bola ale minimálne o 2500 Kč menšia nakoľko pri návrhu a vývoji sa materiálu vždy viac minie ako nakoniec použije.

Literatúra

1. K.BURDA. *1.základné pôjmy* [IS VUT - elearning]. 2022-09. Dostupné tiež z: https://moodle.vut.cz/pluginfile.php/492818/mod_resource/content/1/BZSY. [cit. 2022-11-17].
2. BURDA, Karel. *Základy elektronických zabezpečovacích systemů*. 1. vyd. Brno: Akademické nakladetelství CERM, 2017. ISBN 978-80-7204-967-7.
3. K.BURDA. *3.Objektové detektory* [IS VUT - elearning]. 2022-09. Dostupné tiež z: https://moodle.vut.cz/pluginfile.php/505109/mod_resource/content/1/BZSY. [cit. 2022-11-17].
4. *Displej z tekutých krystalů* [online]. 2022-11. Dostupné tiež z: https://cs.wikipedia.org/wiki/Displej_z_tekut%C3%BDch_krystal%C5%AF. [cit. 2022-11-17].
5. $LCD_{\text{štruktúra}}$ [online]. Technikálie, 2012-03. Dostupné tiež z: https://www.cnews.cz/technikalie-jak-zobrazuje-lcd-panel/. [cit. 2023-5-24].
6. AXIMA, spol. s.r.o. *Postup návrhu výstražné akustické signalizace* [online]. 2022. Dostupné tiež z: https://www.axima-obchod.cz/admin-data/storage/get/75-vystrazne_akusticke.pdf. [cit. 2022-11-20].
7. *Elektrický vrátnik* [online]. TWD, 2022. Dostupné tiež z: https://eshop.twd.sk/produkt/zamky-vlozky/zamky-na-vchodove-dvere/prislusenstvo/elektrovratnik-geze-iq-estrike-a5000-a-plny-nabeh-bez-aretacie/54-154780. [viď. 2022-11-27].
8. *Typy klávesníc* [online]. Wikipedia, 2022-11. Dostupné tiež z: https://cs.wikipedia.org/wiki/Typy_kl%C3%A1vesnic. [cit. 2023-5-26].
9. *Princíp funkcie maticovej klávesnice* [online]. Circuit Basics, 2022-01. Dostupné tiež z: https://www.circuitbasics.com/how-to-set-up-a-keypad-on-an-arduino/. [cit. 2022-11-27].
10. *USART* [online]. Wikipedia, 2021-03. Dostupné tiež z: https://cs.wikipedia.org/wiki/USART. [cit. 2023-5-26].
11. *IIC* [online]. Sparkfun, 2023-03. Dostupné tiež z: https://learn.sparkfun.com/tutorials/i2c/all. [cit. 2023-5-26].
12. *Systém kontroly vstupu a dochádzky* [online]. Alcom Security, 2006-11. Dostupné tiež z: http://www.alkom.cz/sluzby/technologie/systemy-kontroly-vstupu-a-dochazky-ekv-a-ds/. [cit. 2022-11-17].

13. *ČSN EN 60839-11-1* [online]. TECHNOR, 2014-02. Dostupné tiež z: https://www.technicke-normy-csn.cz/csn-en-60839-11-1-334593-182006.html#. [cit. 2022-11-17].

14. K.BURDA. *4.Elektronická kontrola vstupu* [IS VUT - elearning]. 2022-09. Dostupné tiež z: https://moodle.vut.cz/pluginfile.php/513746/mod_resource/content/1/BZSY%5C%2007d.pdf. [cit. 2022-11-17].

15. BITARA, Peter. *Konstrukce systému kontroly vstupu pomocí Arduina.* 2018. Bakalárska práca. Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky. [cit. 2022-11-20].

16. WOSTL, Marek. *Co je to mikrokontrolér?* [Online]. 2019. Dostupné tiež z: https://blog.zonepi.cz/maker-uno-ve-vyuce-1-5-co-je-to-mikrokontroler/. [cit. 2022-11-20].

17. *Komunikačné rozhranie* [online]. Wikipédia, 2021-01. Dostupné tiež z: https://sk.wikipedia.org/wiki/Komunika%C4%8Dn%C3%A9_rozhranie. [cit. 2022-11-20].

18. MATOUŠEK, David. *Práce s mikrokontroléry ATMEL AVR AT90S.* 1. vyd. Brno: Nakladatelství BEN-technická literatura,Praha 2003, 2003. ISBN 80-7300-088-1.

19. *AVR* [online]. Wikipédia, 2022-04. Dostupné tiež z: https://sk.wikipedia.org/wiki/AVR. [cit. 2022-11-20].

20. *AVR základné typy* [online]. Wikipédia, 2022-05. Dostupné tiež z: https://cs.wikipedia.org/wiki/AVR. [cit. 2022-11-20].

21. *SvětSoučástek* [online]. Datasheet, 2022. Dostupné tiež z: https://www.svetsoucastek.cz/mikroprocesory-atmel-rada-atmega-c9887/atmel/?f=80. [cit. 2022-11-20].

22. MUHAMMAD ALI MAZIDI Sarmad Naimi, Sepehr Naimi. *The ACR microcontroller and embedded systems using assembly and C.* 2. vyd. Turecko: Nakladatelství BEN-technická literatura,Praha 2003, 2017. ISBN 978-0997925968.

23. *ATmega644-20PU$_A$VRMicrocontroller* [online]. GitHub, 2023. Dostupné tiež z: https://github.com/MCUdude/MightyCore. [cit. 2023-5-30].

24. *Napájací zdroj* [Wikipedie]. 2023. Dostupné tiež z: https://www.google.com/search?q=APV-35-12&source=lnms&tbm=isch&sa=X&ved=2ahUKEwiAnPKF-Jz_AhV77rsIHXFpCYYQ_AUoAnoECAEQBA&biw=1536&bih=763&dpr=1.25#imgrc=bRI7UK0FW_ehsM%5C%5C. [viď. 2022-11-27].

25. ARMS, SWISS. *Li-Po batéria* [online]. 2022. Dostupné tiež z: https://hristo.hr/en/product/swiss-arms-lipo-11-1v-1200mah/. [viď. 2022-11-20].

26. ADRIROBOT. *Modul SD karty* [online]. 2019. Dostupné tiež z: https://win.adrirobot.it/Micro_SD_Card_Module/Micro_SD_Card_Module.htm. [viď. 2022-11-20].

27. *Detektor PIR* [Hadex]. 2023. Dostupné tiež z: https://www.hadex.cz/m356a-detektor-pohybu-modul-pir-nc-sr501/?gclid=EAIaIQobChMIqrHT-omd_wIVh7HVCh1zGQf7EAQYBCABEgLOW_D_BwE. [viď. 2022-11-27].

28. *Odchodové tlačidlo* [Wikipedie]. 2023. Dostupné tiež z: https://www.google.com/search?q=Odchodov%5C%C3%5C%A9+tla%5C%C4%5C%8Didlo&source=lnms&tbm=isch&sa=X&ved=2ahUKEwjFgNK0j53_AhXjlP0HHSEFDGAQ_AUoAXoECAEQAw&biw=1536&bih=763&dpr=1.25#imgrc=AS6PHupcCTVsWM. [viď. 2022-11-27].

29. *Magnetický dverový detektor* [online]. Jabloshop, 2022. Dostupné tiež z: https://www.jabloshop.cz/sa-201a-detektor-magneticky-dverni-kontakt-mini?gclid=EAIaIQobChMI2Nu8-u_3-wIVAtJ3Ch0hTwuuEAYYBSABEgLa3PD_BwE. [viď. 2022-11-27].

30. *Koncový spínač* [online]. Botland, 2022. Dostupné tiež z: https://botland.cz/koncove-spinace/2842-mini-koncovy-spinac-s-primou-pakou-wk320-5-ks-5904422309107.html. [viď. 2022-11-27].

31. *Piezoelektrická siréna* [Techfun]. 2022. Dostupné tiež z: https://techfun.sk/produkt/sirena-12v-ls-103/. [viď. 2022-11-27].

32. *Servomotor 9g* [online]. Google, 2023. Dostupné tiež z: https://www.google.com/search?q=Servo+9g&source=lnms&tbm=isch&sa=X&ved=2ahUKEwjJnbmSnp3_AhV2gf0HHSLPDj4Q_AUoAnoECAEQBA&biw=1536&bih=763&dpr=1.25#imgrc=cdGab4EBpPLPTM. [viď. 2022-11-27].

33. *Elektromagnetické pole* [online]. Wikipédia, 2022-01. Dostupné tiež z: https://sk.wikipedia.org/wiki/Elektromagnetick%5C%C3%5C%A9_pole. [cit. 2022-11-27].

34. *GSM modul* [online]. Alarmtech, 2022. Dostupné tiež z: https://www.alarmtech.sk/produkt/gsm-modul-sim800l-v-2-0/. [cit. 2022-11-27].

35. *LCD displej* [online]. ECLIPSERA, 2022. Dostupné tiež z: https://dratek.cz/docs/produkty/1/1656/1646725751.pdf. [viď. 2022-11-27].

36. *Maticová klávesnica* [online]. Tipa, 2022. Dostupné tiež z: https://www.tipa.eu/cz/maticova-klavesnice-4x4/d-250903/?gclid=EAIaIQobChMIhoOj08z6-wIVUOZ3Ch1SigydEAQYBSABEgKk-fD_BwE. [viď. 2022-11-27].

37. *RFID čítačka* [Drátek.cz]. 2022. Dostupné tiež z: https://dratek.cz/arduino/833-rfid-ctecka-s-vestavenou-antenou.html. [viď. 2022-11-20].

38. *Snímač odtlačku prsta AS608* [Wikipedia]. 2023. Dostupné tiež z: https://www.google.com/search?q=dy50+fingerprint+sensor&source=lnms&tbm=isch&sa=X&ved=2ahUKEwif_vnT-57_AhXLgP0HHRvtAAIQ_AUoAXoECAEQAw&biw=1536&bih=763&dpr=1.25#imgrc=ZXj8fxR9bKng0M. [viď. 2022-11-20].

39. *LED 5mm* [online]. Reichelt electronic, 2022. Dostupné tiež z: https://www.reichelt.com/fr/fr/led-5-mm-color-e-20-mcd-jaune-led-5mm-st-ge-p6825.html. [viď. 2022-11-27].

40. *RGB dióda* [RS]. 2022. Dostupné tiež z: https://cz.rs-online.com/web/p/led-diody/1651765?cm_mmc=CZ-PLA-DS3A-_-google-_-CSS_CZ_CZ_Displeje_a_optoelektronika_Whoop-_-(CZ:Whoop!)+LED+diody+(2)-_-1651765&matchtype=&pla-330832611324&gclid=EAIaIQobChMIicellq_7-wIVJALmCh3oMwKdEAQYBCABEgLLHvD_BwE&gclsrc=aw.ds. [viď. 2022-11-20].

41. *Smart button Dallas* [Amazon]. 2023. Dostupné tiež z: https://www.amazon.com/ASHATA-iButton-Reading-Writing-Indicator/dp/B07WTVRK1Q. [viď. 2022-11-20].

42. *Piezoelektrický menič 5V* [Drátek.cz]. 2022. Dostupné tiež z: https://dratek.cz/arduino/121937-piezoelektricky-menic-5v.html?gclid=EAIaIQobCh%5C%5CMIxcu4jqb7-wIV0omyCh0lvww7EAQYAiABEgIfqfD_BwE. [viď. 2022-11-20].

43. *Doska plošných spojov* [online]. Wikipédia, 2022-04. Dostupné tiež z: https://sk.wikipedia.org/wiki/Doska_plo%C5%A1n%C3%BDch_spojov. [cit. 2022-11-17].

Zoznam symbolov a skratiek

EZS Elektronický Zabezpečovací Systém

PCO Pult Centrálnej Ochrany

VSZ Vzdialené Signalizačné Zariadenie

GSM Global System for Mobile – Globálny systém pre mobilnú komunikáciu

UPS Uninterrupted Power Supply – Neprerušiteľný zdroj energie

PZS Poplachový Zabezpečovací Systém

PZTS Poplašný Zabezpečovací a Tiesňový Systém

EPS Elektronická Požiarna Signalizácia

DVI Dohľadové Video systémy

EKV Elektronická Kontrola Vstupu

CCTV Closed - Circuit TeleVision – Uzavretý televízny okruh

LAN Lokal Area Network – Lokálna miastna sieť

PSTN Public Switched Tepelhone Network – Sieť jednotlivých telefónnych operátorov, pevná linka

UTP Unshielded Twisted Pair – Netienená krútená kábľová dvojlinka

NTSC National Television System Committee – Kódovací štandard analog.TV

PAL Phase Alternating Line – Kódovací štandard farebného TV signálu

ACS Acces Control System – Elektronická kontrola vstupu

IR InfraRed – Infračervené

PIR Pasiv InfraRed detektor – Infračervený detektor pohybu

GBS Glass Break Sensor – Detektor rozbitia skla

PZT Plumbum-zirkonato-titan

NFC Near Field Comunication

EMTC Elektrické, Mechanické, Tepelné , Chemické

Zoznam príloh

A Schéma zapojenia DPS **91**

B Doska plošných spojov **92**

B.1 Vrchná strana 92

B.2 Spodná strana 93

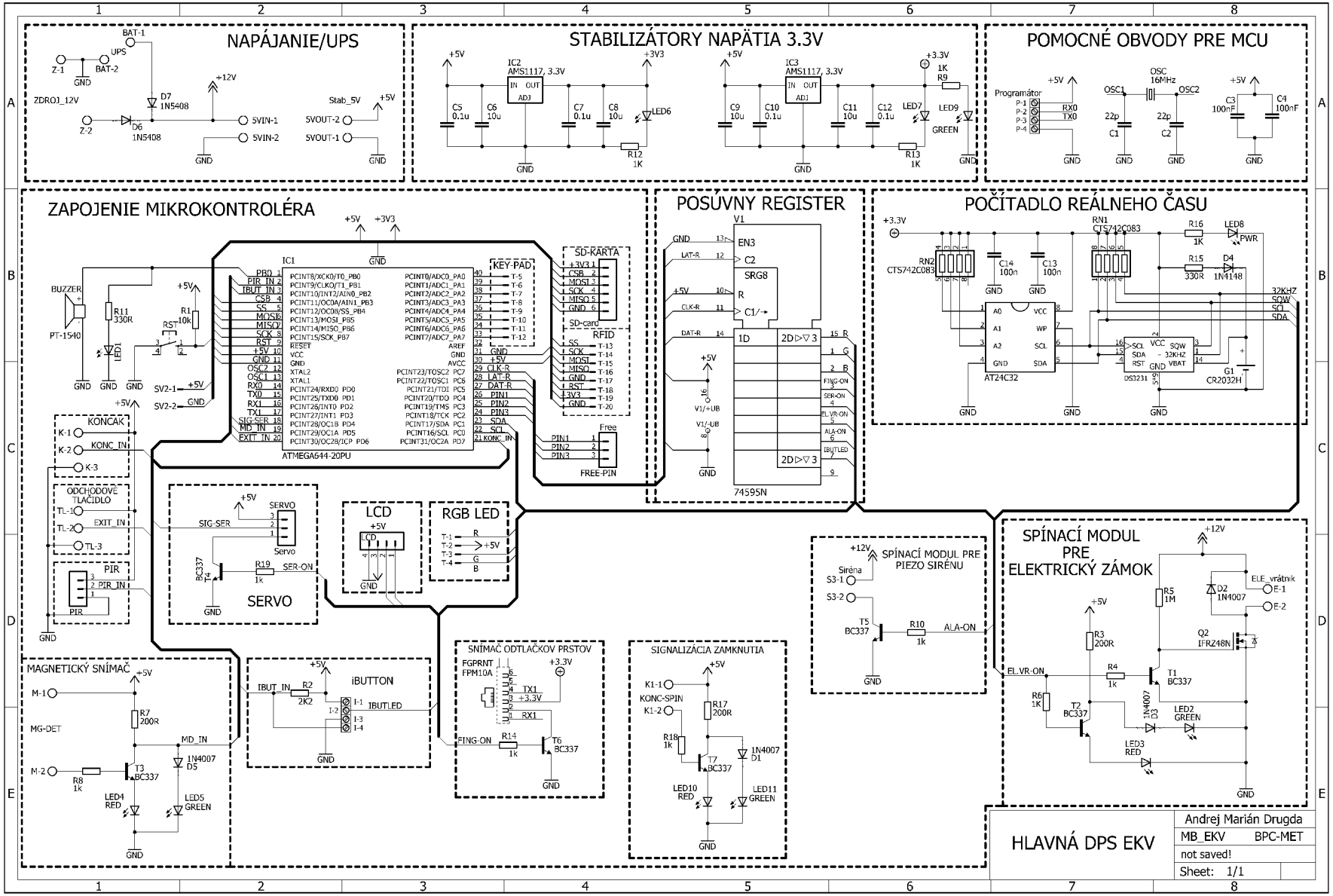
C Vývojový diagram programu systému **94**

C.1 Hlavné menu 94

C.2 Spôsob autentizácie 95

C.3 Možnosti nastavení 96

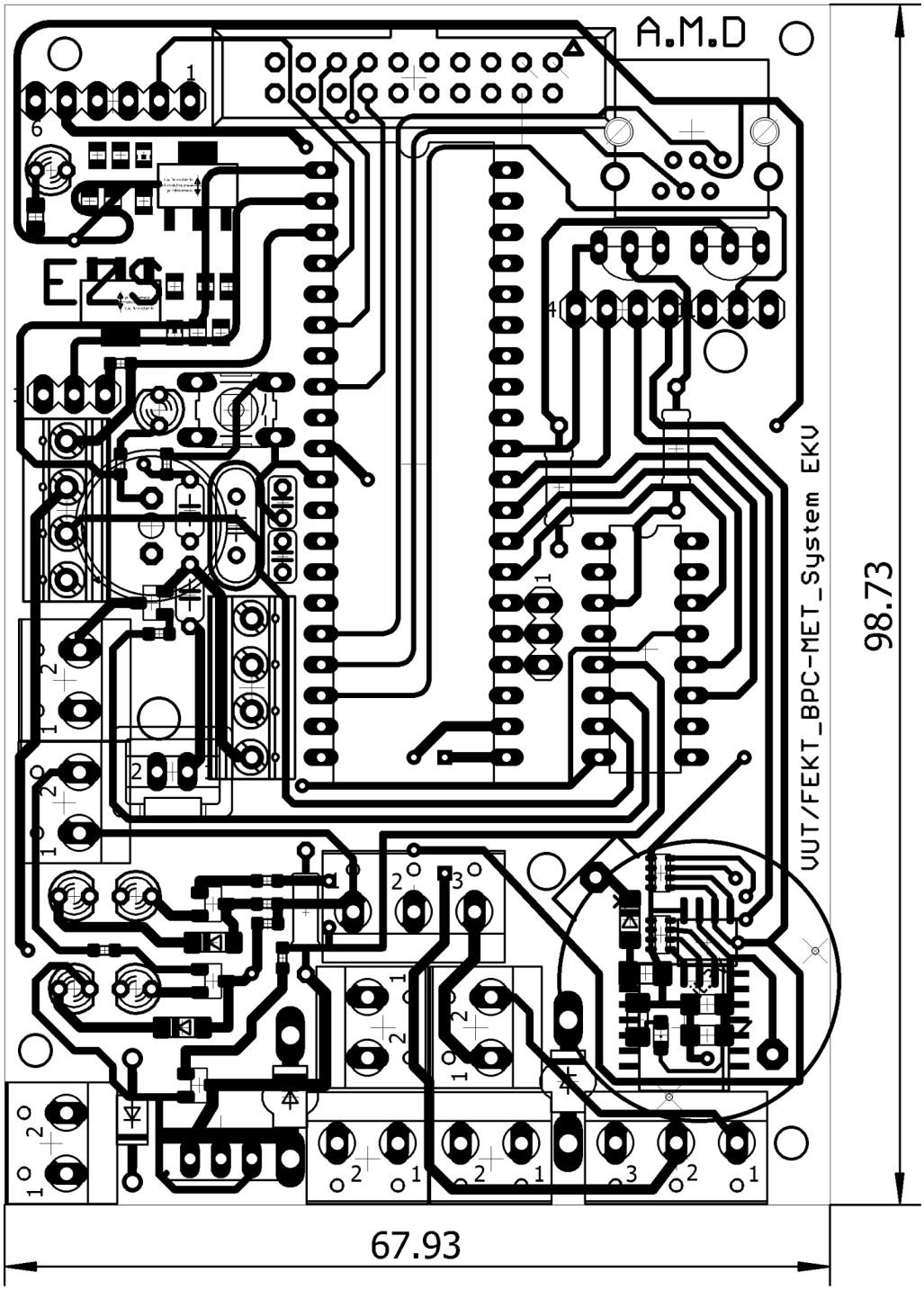
A Schéma zapojenia DPS



Obr. A.1: Elektronická schéma zapojenia systému EKV

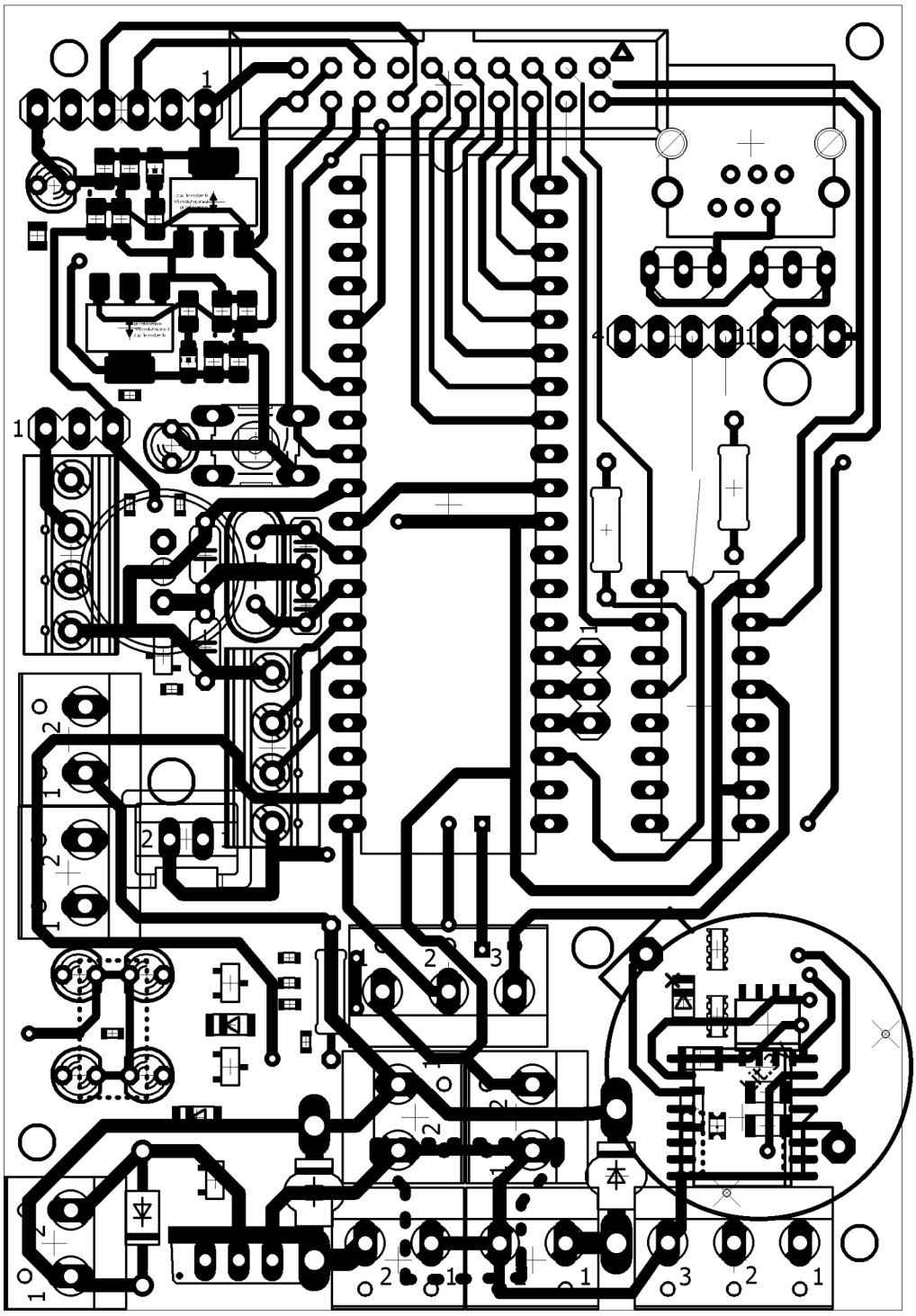
B Doska plošných spojov

B.1 Vrchná strana



Obr. B.1: Pohľad na vrchnú stranu DPS

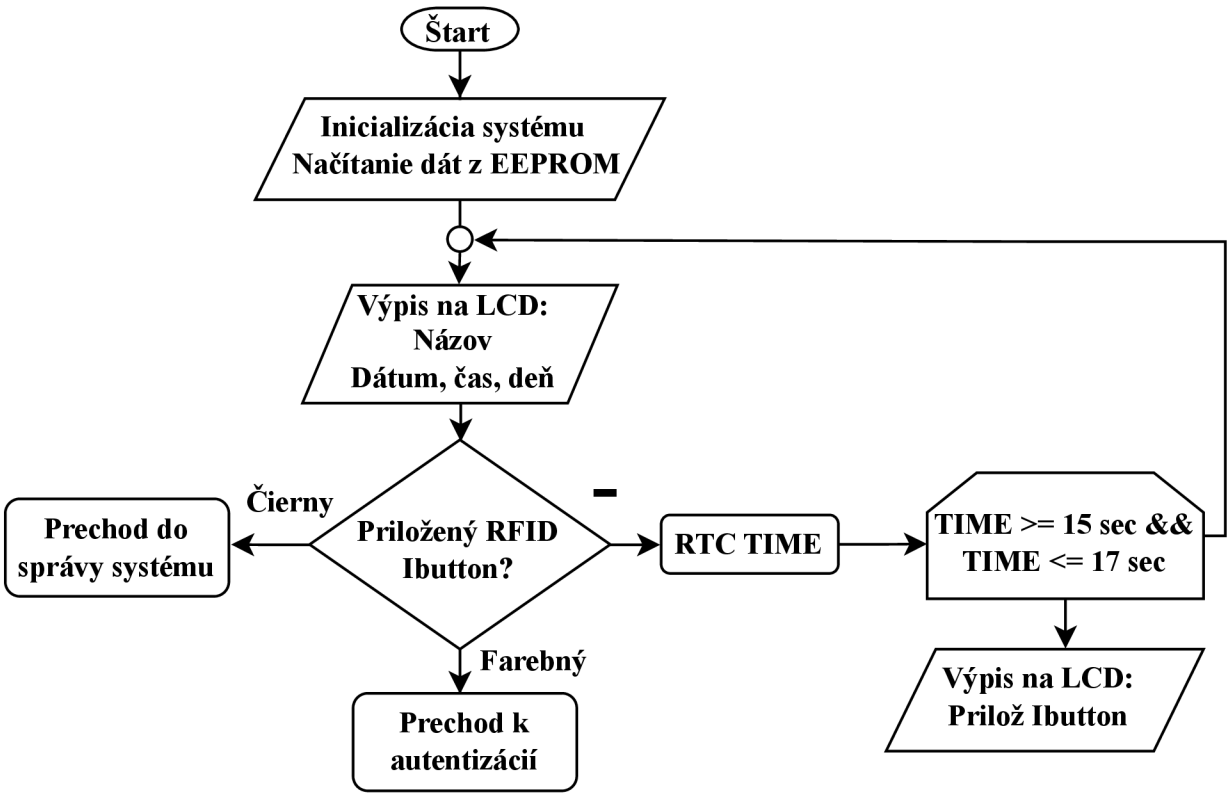
B.2 Spodná strana



Obr. B.2: Pohľad na spodnú stranu DPS

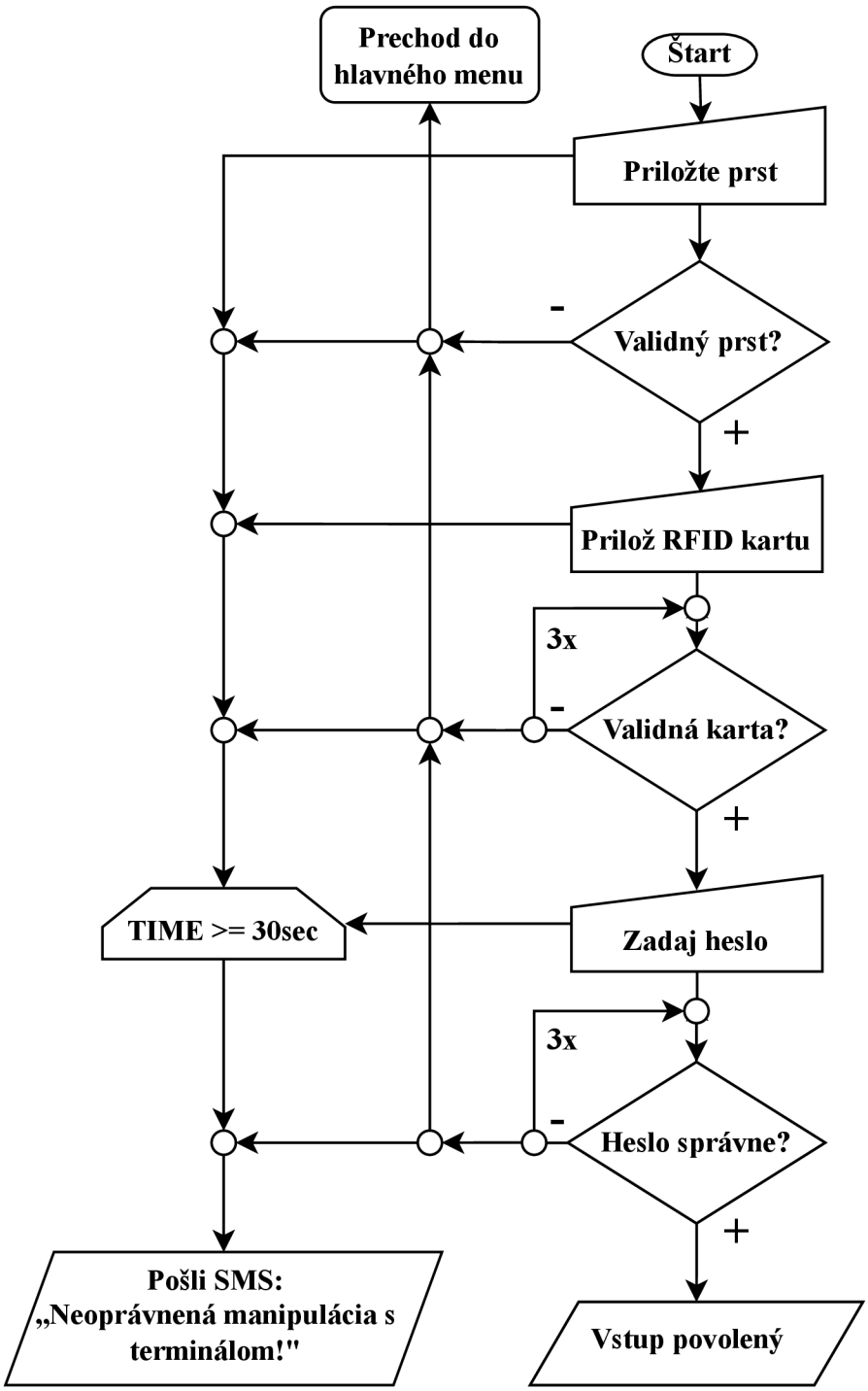
C Vývojový diagram programu systému

C.1 Hlavné menu



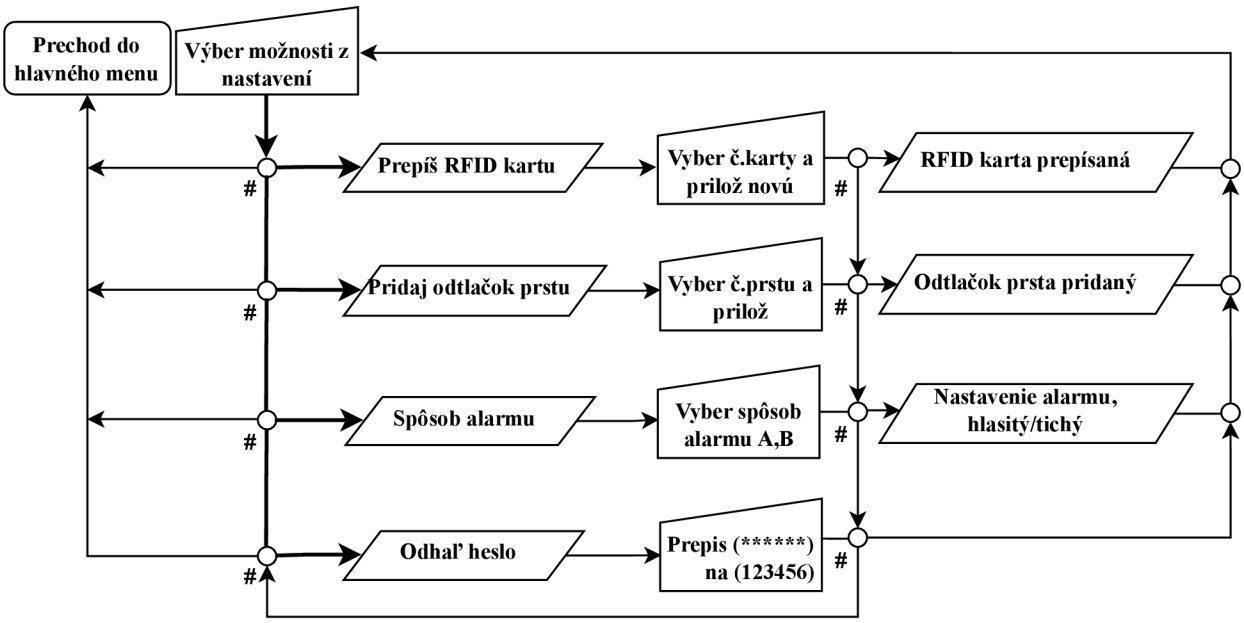
Obr. C.1: Prvotná zobrazenie systému

C.2 Spôsob autentizácie



Obr. C.2: Postup autentizácie

C.3 Možnosti nastavení



Obr. C.3: Nastavenia