VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV POČÍTAČOVÝCH SYSTÉMŮ
DEPARTMENT OF COMPUTER SYSTEMS

SYSTÉM PRO ZABEZPEČENÍ A STŘEŽENÍ OBJEKTŮ A PROSTOR ZALOŽENÝ NA PLATFORMĚ ARDUINO

SYSTEM FOR GUARDING AND SECURING OF OBJECTS AND AREAS BASED ON ARDUINO PLATFORM

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **JAKUB JURÍČEK**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. JOSEF STRNADEL, Ph.D.**
SUPERVISOR

BRNO 2017

Vysoké učení technické v Brně - Fakulta informačních technologií

Ústav počítačových systémů Akademický rok 2016/2017

Zadání bakalářské práce

Řešitel: **Juríček Jakub**
Obor: Informační technologie
Téma: **Systém pro zabezpečení a střežení objektů a prostor založený na platformě Arduino**
System for Guarding and Securing of Objects and Areas Based on Arduino Platform
Kategorie: Vestavěné systémy

Pokyny:

1. Seznamte se s technologiemi používanými při zabezpečení a střežení vnějších a vnitřních prostor (např. kamery, čidla, světelné závory).
2. Vytvořte specifikaci a s využitím vhodně vybraných technologií z bodu 1 navrhněte blokové schéma systému pro zabezpečení a střežení zvoleného objektu a/nebo prostoru.
3. Systém specifikovaný v bodu 2 navrhněte s ohledem na následující požadavky: snadnost instalace, možnost uživatelského ovládání a změny strukury/vlastností systému, změny komponent systému, archivace a zasílání uživatelem upřesněných dat.
4. Funkčnost celého systému či jeho vybraných podčástí stanovených po dohodě s vedoucím prakticky ověřte.

Literatura:

- *EZK - elektronika Zdeněk Krčmář* [online]. c2016. Dostupné z http://www.ezk.cz/.
- *FLAJZAR... výroba a prodej elektroniky* [online]. c2016. Dostupné z http://www.flajzar.cz/.
- *GME Česko* [online]. c2016. Dostupné z http://www.gme.cz/.
- *Zabezpečení domů, obbchodů, kanceláří - JABLOTRON - elektronické zabezpečovací systémy*. Dostupné z http://www.jablotron.cz/ezs.php.

Pro udělení zápočtu za první semestr je požadováno:

- Splnění bodů 1 a 2 zadání.

Podrobné závazné pokyny pro vypracování bakalářské práce naleznete na adrese http://www.fit.vutbr.cz/info/szz/

Technická zpráva bakalářské práce musí obsahovat formulaci cíle, charakteristiku současného stavu, teoretická a odborná východiska řešených problémů a specifikaci etap (20 až 30% celkového rozsahu technické zprávy).

Student odevzdá v jednom výtisku technickou zprávu a v elektronické podobě zdrojový text technické zprávy, úplnou programovou dokumentaci a zdrojové texty programů. Informace v elektronické podobě budou uloženy na standardním nepřepisovatelném paměťovém médiu (CD-R, DVD-R, apod.), které bude vloženo do písemné zprávy tak, aby nemohlo dojít k jeho ztrátě při běžné manipulaci.

Vedoucí: **Strnadel Josef, Ing., Ph.D.**, UPSY FIT VUT
Datum zadání: 1. listopadu 2016
Datum odevzdání: 17. května 2017

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
Fakulta informačních technologií
Ústav počítačových systémů a sítí
612 66 Brno, Božetěchova 2

L.S.

prof. Ing. Lukáš Sekanina, Ph.D.
vedoucí ústavu

Abstrakt

Táto bakalárska práca sa zaoberá analýzou, návrhom a realizáciou systému využiteľného pre zabezpečenie objektov s cieľom odhaliť a ohlásiť potenciálnu hrozbu. Dôraz je kladený na možnosti ovládania a konfigurácie systému a jeho jednoduchú prispôsobiteľnosť rôznym objektom. Súčasťou práce je i analýza fiktívneho objektu, na ktorom je ukázané vhodné rozmiestnenie senzorov. Návrh je realizovaný na platforme Arduino a s využitím rôznych druhov senzorov a ovládacích prvkov je dosiahnutý funkčný zabezpečovací systém prvej úrovne, ktorý dokáže monitorovať narušenie plášťa, pohyb, oheň či teplotu a okamžite túto skutočnosť hlásiť akusticky i opticky. Pre nastavenie vlastností systému je dostupné konfiguračné rozhranie. Riešenie je testované komplexne i na konkrétne zvolenom objekte s pevne daným počtom senzorov.

Abstract

This bachelor's thesis deals with the analysis, design and implementation of a system, that can be used to secure objects, in order to detect and report a potential threat. Emphasis is placed on the ability to control and configure the system and on its easy adaptability to various objects. Part of the thesis is focused on analysis of a fictitious object, on which the appropriate location of the sensors is shown. The design is carried out on the Arduino platform and with the use of various types of sensors and controls, a first-level functional alarm system is capable to monitor case, movement, fire or temperature disturbance and immediately report this fact both acoustically and visually. Configuration interface is used to set system properties. The solution is tested in a complex way on a particular object with a fixed number of sensors.

Kľúčové slová

elektronický bezpečnostný systém, ochrana objektu, zabezpečenie, vstavané systémy, Arduino, ústredňa, senzory, ethernet, webová stránka, servisný režim

Keywords

electronic security system, object protection, security, embedded systems, Arduino, central, sensors, ethernet, web page, service mode

Citácia

JURÍČEK, Jakub. *Systém pro zabezpečení a střežení objektů a prostor založený na platformě Arduino*. Brno, 2017. Bakalářská práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Ing. Josef Strnadel, Ph.D.

Systém pro zabezpečení a střežení objektů a prostor založený na platformě Arduino

Prehlásenie

Prehlasujem, že som túto prácu vypracoval samostatne pod vedením pána Ing. Josefa Strnadela, Ph.D. Uviedol som všetky literárne pramene a publikácie, z ktorých som čerpal.

.....
Jakub Juríček
15. mája 2017

Poďakovanie

Chcel by som poďakovať svojmu vedúcemu Ing. Josefovi Strnadelovi, Ph.D. za jeho odbornú pomoc a rady, ktoré mi boli poskytnuté pri vypracovávaní bakalárskej práce.

Obsah

Kapitola 1

Úvod

Žijeme v modernej dobe plnej komunikačných technológií, ktorých využitie nepozná hraníc. V mnohých smeroch nám uľahčujú každodennú prácu, pomáhajú riešiť ľahké i zložité problémy, sú neodmysliteľnou súčasťou firemných infraštruktúr, školstva, medicíny, armády, poskytujú nové formy zábavy či napomáhajú pri objasňovaní kriminálnych činov. Pri ich správnom využití máme dostupné nástroje, ktoré okrem pomoci poskytujú ochranu nám i nášmu majetku a tak prispievajú k bezpečnejšiemu a spokojnejšiemu životu.

Táto práca sa zameriava na elektronické systémy a ich komponenty, ktoré poskytujú ochranu pred možným odcudzením majetku alebo jeho znehodnotením, spôsobeným vonkajšími vplyvmi. Popisuje návrh a realizáciu zabezpečovacieho systému, ktorý je schopný samostatne sledovať stav monitorovaných objektov alebo priestorov a identifikovať a ohlásiť prípadnú hrozbu. Vďaka kombinácii rôznych druhov senzorov a signalizačných techník, poskytuje nielen pokročilú a spoľahlivú ochranu pred vniknutím neoprávnených osôb, ale i včasnú reakciu na nepriaznivú zmenu prostredia. Dôležitou vlastnosťou je možnosť konfigurácie a prispôsobenia rôznym objektom podobných rozmerov, čím sa nestáva len jednoúčelovým produktom. Užívateľ môže systém ovládať pomocou zabudovanej klávesnice pričom zmeny sú zobrazované na LCD displeji. Má umožnený vzdialený prístup k informáciám o aktuálnom stave pomocou webovej stránky a o hrozbách je informovaný svetelne, zvukovo či emailom.

V kapitole 2 sú popisované princípy fungovania bezpečnostných systémov a technológie prevažne využiteľné na zabezpečenie priestorov menších rozmerov ako sú pivnice, garáže, byty, domy, záhrady, menšie sklady, reštaurácie, obchody či iné vnútorné alebo vonkajšie priestory. Podrobne sú rozobrané i riziká vzniku falošných poplachov a možnosti ako sa im vyhnúť. Kapitola 3 začína predstavením platformy Arduino, ktorá je hlavnou riadiacou jednotkou navrhovaného systému. Ďalej sa venuje analýze stráženého objektu, ktorá je nutným základom pre správne fungujúci bezpečnostný systém. Tiež popisuje minimálne nároky na jeho funkčnosť, ktoré by mal pre daný objekt splňovať. Zvyšok práce, počínajúc kapitolou 4 podrobne popisuje proces hardvérovej i softvérovej realizácie. Dochádza k aplikovaniu teoretických princípov objasnených v predošlých kapitolách na konkrétny systém. Postupne sú prezentované jednotlivé komponenty, spôsob ich programovej obsluhy, súvislosti s ostatnými komponentami a zmysel ich využitia z pohľadu užívateľa. V neposlednom rade sú zhodnotené výsledky testovania, pričom sú spomenuté i zistené nedostatky, ktorých riešenie môže byť súčasťou ďalšieho vývoja práce.

Kapitola 2

Bezpečnostné systémy a ich prvky

Kapitola sa venuje problematike elektronických zabezpečovacích a monitorovacích systémov. Definuje základné pojmy a bližšie sa venuje popisu technológií a postupov, ktoré sú využívané v bezpečnostných komerčných produktoch a rozboru ochranných a monitorovacích prvkov. Zameriava sa na výhody a nevýhody jednotlivých riešení, skúmanie nových možností a celkovú analýzu problému ochrany majetku. Veľkú časť informácií poskytla kniha [12].

2.1 Elektronický zabezpečovací systém a jeho súčasti

Elektronický zabezpečovací systém (EZS) tiež označovaný ako *poplachový zabezpečovací a tiesňový systém (PZTS)* je skupina elektronických komponentov, ktoré sú schopné zaznamenať a akusticky alebo opticky signalizovať narušenie na určitom mieste [13].

Základné komponenty, ktoré spoločne vytvárajú požadovanú funkčnosť každého EZS, sú:

Ústredňa – základný prvok, ktorý riadi činnosť celého systému. Komunikuje s ostatnými časťami, prijíma informácie, analyzuje ich a vyvodzuje ďalšie akcie. Udáva pokyn k spusteniu signalizácie, môže tiež informovať pult centralizovanej ochrany (PCO) pomocou GSM modulu alebo zaslať sms či email poverenej osobe. Funkcie závisia na konkrétnom prevedení. Podľa úrovne vybavenia môžeme ústredne rozdeliť do 4 kategórií [4]:

- **Kategória 4:** Poplach je zaznamenávaný z tiesňových hlásičov alebo jednotlivých senzorov. Prerušením ktoréhokoľvek vodiča alebo skratom nedochádza k signalizácii poplašného stavu.
- **Kategória 3:** Táto kategória vyžaduje, aby boli poplachové a zaisťovacie slučky elektricky kontrolované po celú dobu činnosti systému.
- **Kategória 2:** Poplachové a zaisťovacie slučky sú naviac kontrolované vrátane izolačného odporu voči zemi. Kontrola musí prebiehať i na slučkách medzi jednotlivými paralelne zapojenými senzormi.
- **Kategória 1:** Vyžadované sú dve samostatne pracujúce ústredne, kde jedna je minimálne 3. kategórie a druhá minimálne 2. kategórie. Každá ešte musí mať samostatný náhradný zdroj napätia pre prípad výpadku a vedenie pre poplachové a zaisťovacie slučky musí byť uložené oddelene. Nie je dovolené použitie jed-

ného združeného kábla. Zariadenie nižšej kategórie musí byť pripojené na ďalší signalizačný panel. Splnené musia byť i všetky náležitosti ostatných kategórií.

Ústredne by mali byť schopné pracovať aspoň v troch základných prevádzkových režimoch [10]:

- **Režim stráženia:** Ústredňa vyhodnocuje informácie od jednotlivých senzorov a pokiaľ situáciu vyhodnotí ako stav narušenia, vyhlási poplach.
- **Pohotovostný režim:** Ústredňa nekontroluje stav objektu, ale naďalej aktívne monitoruje prvky, ktoré ochraňujú EZS pred sabotážou. V niektorých prípadoch je možné do pohotovostného režimu zahrnúť i nejakú časť objektu určenú k nepretržitému stráženiu.
- **Servisný režim:** Slúži na konfiguráciu vlastností celého systému. Nakoľko je určený pre inštaláciu či výmenu jednotlivých komponentov, systém nemonitoruje ani zaisťovaciu slučku. Dostupný býva spravidla po zadaní špeciálneho servisného kódu.

Mikroprocesor zabezpečuje prechod medzi režimami a správnu činnosť všetkých vstupných a výstupných zariadení. Správny chod systému aj akákoľvek chyba by mala byť nejakým spôsobom indikovaná – väčšinou formou stavovej LED diódy, umiestnenej na kryte.

Ovládacie zaradenia – zariadenia, ktoré umožňujú samostatne alebo s pomocou obsluhy ovládať časti EZS, prípadne ich programovať. Spravidla sa na ovládanie používajú zabudované maticové alebo externé klávesnice pripojené prostredníctvom USB či PS/2 portu. Medzi ovládače sa radia tiež čítačky kariet (čipov) a snímače odtlačkov prstov, ktoré kontrolujú oprávnenia užívateľa pri manipulácii so systémom. Ďalšou možnosťou je ovládanie cez internet prostredníctvom integrovaného webového rozhrania umožňujúceho systém riadiť odkiaľkoľvek. Úroveň ovládateľnosti systému závisí na konkrétnom programovom prevedení, no medzi základné funkcie neodmysliteľne patrí možnosť aktivácie a deaktivácie ochrany. Bežná je i kompletná konfigurácia systému, zmena prístupových údajov, zobrazenie informácií o aktuálnom stave a iné.

Signalizačné zariadenia – prvky systému, ktoré opticky, akusticky či kombinovane signalizujú informáciu o poplachu. Hlavnou úlohou je informovať okolie a prípadne odstrašiť narušiteľa. Využívajú sa jednoznačné, vysoké a hlasné tóny, pri ktorých je nízka pravdepodobnosť splynutia s okolitými zvukmi a pri optickej signalizácii jasné blikajúce svetlo (väčšinou červené alebo oranžové). Vhodné sú rôzne druhy sirén, majáky či reflektory.

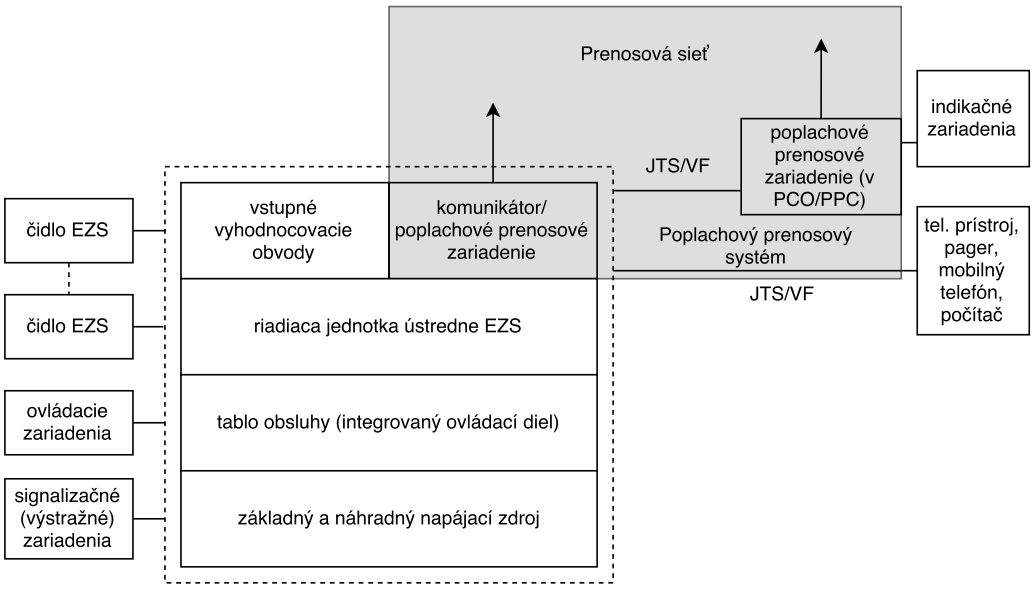
Prenosové prostriedky – nazývajú sa tiež *komunikátory* a umožňujú prenášať výstupné informácie ústredne na vopred určené miesta. Prenos môže prebiehať pomocou GSM modulu, s využitím siete LAN, klasickej telefónnej siete alebo môže komunikátor využívať rádiovú sieť s vyhradeným prenosovým pásmom [25]. Prijímateľom býva buď poverený užívateľ alebo ním môže byť pult centralizovanej ochrany/poplachové prijímacie centrum (PCO/PPC). Prenosové prostriedky môžu tvoriť samostatný modul alebo byť súčasťou ústredne.

Detektory – zariadenia, ktoré sú schopné monitorovať alebo zaznamenávať fyzikálne zmeny prostredia. Informácie predávajú ústredni na vyhodnotenie. Tvoria základnú časť systému a bližšie sú popísané od kapitoly 2.3.

V niektorých prípadoch je okamžité vyvolanie poplachu nežiadúce. Riešením je rozdelenie chráneného priestoru na takzvané slučky alebo tiež zóny. V závislosti na aktivovanom režime sa stavy senzorov patriacich do danej zóny vyhodnocujú rozlične. V užívateľských manuáloch EZS sa spomínajú rôzne typy slučiek, ktoré sú často modifikáciou základných, medzi ktoré patrí [10]:

- **Okamžitá slučka:** V pohotovostnom režime sa na jej narušenie nereaguje. Naopak v režime stráženia musí byť poplach vyhlásený ihneď po zaznamenaní narušenia. Do takejto slučky sú pripájané detektory nachádzajúce sa v priestoroch, v ktorých sa nepredpokladá žiadny pohyb.
- **Oneskorená slučka:** Narušenie sa indikuje len v režime stráženia, no k vyhláseniu poplachu dochádza až po uplynutí predom daného časového intervalu. Často sa daná zóna vyskytuje v miestnosti s ovládacím zariadením EZS, kedy je nutné poskytnúť dostatok času, aby mohol byť režim stráženia vypnutý správnym zadaním prístupového kódu.
- **Trvalá slučka:** Pripájajú sa do nej zariadenia, ktoré musia vyvolať poplach v režime stráženia i v pohotovostnom režime. Väčšinou sú to prvky brániace sabotáži samotného systému či jeho komponentov alebo tiesňové hlásiče.

Na obrázku 2.1 je možné vidieť schému EZS so všetkými základnými súčasťami.



Obr. 2.1: Bloková schéma všeobecného EZS [12].

2.1.1 Prepojenie prvkov systému

Niektoré časti EZS sú síce schopné pracovať samostatne, no bez vzájomnej výmeny informácií a ich správnej interpretácie by celý systém nefungoval správne. Preto je nutné jednotlivé prvky prepojiť. Spôsoby prepojenia ovplyvňujú bezpečnosť, cenu, rozmery a náročnosť inštalácie systému, preto je výber nutné dobre zvážiť. Medzi bežne dostupné varianty patrí [8]:

Drôtové prevedenie – všetky súčasti systému sú vzájomne alebo minimálne s ústredňou prepojené káblami. Tie sú vedené buď v elektroinštalácií daného objektu, vo ventilačných šachtách či v lište na stenách. Cenové nároky na jednotlivé komponenty sú výrazne nižšie, než je tomu pri ostatných variantách, no po zahrnutí ceny materiálu (káble, lišty, svorky, oprava omietky) a času stráveného inštaláciou, tomu môže byť inak. Systém je vhodné zavádzať počas rekonštrukcie alebo popri výstavbe objektu, kedy je možné rozvody ukryť do múrov. Medzi hlavné výhody patrí priame napájanie a možnosť kombinovať komponenty rôznych výrobcov.

Kabeláž viditeľne vedená po obvode objektu prináša radu bezpečnostných rizík. Pre narušiteľa zvyčajne nie je problém vyhľadať správny vodič a ten prerušiť. Systém by mal byť preto schopný kontrolovať, či je spojenie s jednotlivými prvkami aktívne.

Podľa spôsobu pripojenia jednotlivých detektorov k ústredni delíme ústredne drôtového prevedenia na [12]:

- **Slučkové:** Pre každú poplachovú slučku existuje vyhodnocovací obvod. Slučka musí vykazovať predpísaný odpor pre danú ústredňu. Zmena odporu znamená buď aktiváciu niektorého čidla alebo sabotáž, v oboch prípadoch dochádza k spusteniu poplachu.
- **S priamym adresovaním senzorov:** Spravidla má vedenie 4 vodiče, dva napájacie a dva dátové. Ústredňa v jeden okamih komunikuje práve s jedným z detektorov a to periodickým generovaním jeho adresy. Senzory tak môžu byť pripojené sériovo v ľubovoľnom poradí.
- **Zmiešaného typu:** Ústredňa komunikuje s takzvanými *koncentrátormi*, na ktoré sú senzory pripojené slučkami. Komunikácia s ústredňou prebieha pomocou dátovej či analógovej zbernice.

Bezdrôtové prevedenie – vzájomná komunikácia prebieha rádiovým signálom, najčastejšie na frekvencii 433 MHz s výkonmi okolo 10 mW. Každý prvok systému je teda vysielač s dosahom zvyčajne okolo 100-200 m vo voľnom prostredí. Je potrebné zaistiť vlastné napájanie, často lítiovou batériou alebo 9 V doštičkovým článkom. Výhodou bezdrôtového prevedenia je rýchla a jednoduchá inštalácia, možnosť jednoduchého rozšírenia o ďalšie komponenty či dynamické prispôsobovanie prostrediu (rýchle premiestnenie senzorov). Treba však rátať s vyššou cenou jednotlivých komponentov a nutnosťou pravidelne vymieňať batérie.

Podľa smeru komunikácie medzi bezdrôtovou ústredňou a jednotlivými prvkami rozlišujeme dva druhy systémov:

- **Systémy s jednosmernou komunikáciou:** Detektor obsahuje vysielač a v ústredni je prijímač. Kontrola stavu detektorov buď nie je zaistená alebo dochádza k pravidelnému vysielaniu kontrolných telegramov. S nárokmi na trvanlivosť batérií však dochádza k odosielaniu raz za niekoľko hodín. Ústredňa je tak informovaná o nefunkčnosti prvku so značným oneskorením.
- **Systémy s obojsmernou komunikáciou:** Prvky najnovších systémov sú vybavené vysielačom i prijímačom – pracujú *duplexne*. Po zapnutí si ústredňa overí stav všetkých senzorov a môže vykonať automatické preladenie pri rušení. Pri vzniku poplachu je možné jednoducho overiť, či nejde len o falošný poplach.

Hybridný systém – kombinuje obe spomenuté prevedenia. Využíva sa pre zabezpečenie viacerých oddelených objektov, kde je v rámci objektu využité drôtové prevedenie, no prenos informácií medzi objektami je zabezpečený bezdrôtovo. Hodí sa pre zakomponovanie diaľkových ovládačov, ktorými je možné aktivovať/deaktivovať systém alebo vzdialene ovládať napríklad otváranie/zatváranie garážových dverí.

2.1.2 Stupeň zabezpečenia

Pri návrhu bezpečnostného systému je potrebné si uvedomiť, aký objekt má byť chránený. Zabezpečenie banky sa pravdepodobne bude líšiť od zabezpečenia rekreačnej chaty. Nutné je preto vypracovať bezpečnostný posudok, ktorým je možné určiť nutný *stupeň zabezpečenia*. Ten je definovaný v norme ČSN EN 50131-1 a stanovuje mieru vybavenosti a nároky na funkcie jednotlivých komponentov či celého systému. Do úvahy sa berie prístupová úroveň, detekcia, monitorovanie, prepojenie, napájanie, zabezpečenie proti sabotáži či potreba záznamu udalostí [12].

Stupeň 1 vyjadruje potrebu jednoduchého zabezpečenia a stupeň 4 naopak najlepšieho možného. Väčšina objektov spadá práve pod stupeň 1–2 (domy, byty, obchody, sklady), 3. sa spája s bankami, kasínami alebo skladmi s utajovanými dokumentami a 4. stupeň prislúcha prevažne vládnym a iným špeciálnym objektom [13]. V tabuľke 2.1 je možné vidieť, akého narušiteľa daný stupeň predpokladá, a teda proti komu musí byť objekt zabezpečený.

Stupeň	**Miera rizika**	**Predpokladaný typ narušiteľa**
1	nízke	narušiteľ má malú znalosť EZS a obmedzený sortiment ľahko dostupných nástrojov
2	nízke až stredné	narušiteľ má určité znalosti o EZS a obmedzený sortiment základných prenositeľných nástrojov
3	stredné až vysoké	narušiteľ je oboznámený s EZS a vlastní úplný sortiment základných prenosných prístrojov a elektronických zariadení
4	vysoké	narušiteľ má možnosť vypracovať podrobný plán vniknutia a disponuje kompletným vybavením vrátane prostriedkov pre náhradu rozhodujúcich prvkov EZS

Tabuľka 2.1: Stupne zabezpečenia [12].

2.1.3 Hlásenie poplachu

Bezpečnostný systém musí dokázať patrične reagovať na vzniknuté podnety. V prípade, že ústredňa vyhodnotí výstup niektorého zo svojich detektorov ako stav narušenia (po prípadnej kontrole falošného poplachu), zaháji proces ohlasovania. V závislosti na prevedení systému sú informácie o poplachu smerované [9]:

- na lokálne signalizačné zariadenie (sirénu, maják), ktorého cieľom je upozorniť okolie na prítomnosť narušiteľa a tým ho odradiť od ďalšieho zotrvania v objekte,
- na pult centralizovanej ochrany (PCO) pomocou poplachového prenosového zariadenia,

- predom určeným osobám (majiteľ, správca, zodpovedný pracovník bezpečnostnej služby) pomocou automatického telefónneho hlásiča,
- cez GSM Pager (umožňuje zasielanie správ z EZS príjemcovi cez sieť GSM) alebo GSM bránu (umožňuje pripojiť k sieti GSM i zariadenia vyžadujúce pevnú telefónnu linku),
- kombináciou predošlých bodov.

Pult centralizovanej ochrany (PCO) – označuje vzdialené stredisko s nepretržitou obsluhou, ktoré prijíma poplašné hlásenia od pripojených EZS. Prijaté informácie môžu obsahovať len správu, že došlo k narušeniu alebo môžu poskytovať komplexnejšie údaje o tom, v ktorej miestnosti a aký typ narušenia vznikol, prípadne naďalej informovať o dianí v objekte. Následne sú vyhodnotené operátormi daného strediska, ktorí na základe závažnosti povolajú príslušné zásahové jednotky (bezpečnostná služba, policajný zbor, hasičský a záchranný zbor).

Okrem PCO sa používa i označenie poplachové prijímacie centrum (PPC), rozdiel je v prevádzkovateľoch (PCO – polícia, PPC – súkromná osoba). V praxi sa používa označenie PCO nezávisle na prevádzkovateľovi.

GSM komunikátor – ide o elektronické zariadenie, ktoré je riadené mikroprocesorom EZS a využíva sa na prenos poplachových správ prostredníctvom GSM siete. Poskytuje nasledujúce funkcie [9]:

- odosielanie SMS textových správ na jeden či niekoľko mobilných zariadení,
- zavolanie na predom určené číslo a prehranie zvukovej správy,
- kontaktovanie PCO,
- možnosť ovládania či programovania EZS SMS správami prostredníctvom SMS brány či aplikačného protokolu pre bezdrôtové zariadenia – WAP (z anglického *Wireless Application Protocol*),
- ovládanie systému či spotrebičov z klávesnice telefónu,
- možnosť pripojenia telefónneho prístroja vyžadujúceho pevnú linku,
- pripojenie na internet,
- nastavovanie systému prostredníctvom webovej stránky.

Medzi hlavné výhody patrí odolnosť voči sabotáži. Klasické pripojenie na telefónnu linku alebo internet môže byť fyzicky prerušené alebo odstavené výpadkom elektrickej energie (záložný zdroj spravidla napája len EZS a nie i zariadenia poskytujúce internetové pripojenie), no GSM modul je závislý len na systéme EZS a prenosové pásmo je možné rušiť veľmi obtiažne.

Akustická signalizácia – patrí medzi najčastejšie inštalované doplnkové zariadenia. Tvorí ju akustický menič s generátorom kolísavého tónu a výkonným zosilňovačom. Podľa prevedenia môže byť vonkajšia i vnútorná. Umiestňuje sa väčšinou na priečelie chráneného objektu do výšky, ktorá je nedostupná bez použitia rebríka alebo iného pomocného náradia. Podľa ČSN EN 50131-1 je doba aktivácie v rozmedzí 90 sekúnd až 15 minút. Moderné sirény majú optoelektronickú ochranu pred zaplnením vnútra penou.

Optická signalizácia – vo väčšine prípadov ide o záblesk ový maják oranžovej alebo červenej farby, ktorý môže byť umiestnený samostatne alebo je súčasťou krytu sirény. Zdrojom svetla je buď 12 V žiarovka budená elektronickým prerušovačom, alebo výbojka používajúca vlastnú elektroniku. Doba aktivácie by mala byť teoreticky nekonečná, dôvodom je pokračovanie indikácie narušenia objektu i po doznení sirény.

2.2 Elektrická požiarna signalizácia

Elektrická požiarna signalizácia (EPS) je systém tvorený ústredňou a zariadeniami, ktoré dokážu zaznamenať a vyhodnotiť vznik požiaru. Systém by následne mal byť schopný signalizovať vzniknutý problém akusticky i opticky a informovať miesto so stálou službou, ktorá môže na signalizáciu zareagovať. Hlavnými úlohami EPS je okrem vyhlásenia poplachu a privolania jednotiek (napr. hasičský záchranný zbor) tiež správne určenie miesta vzniku požiaru a jeho zabezpečenie do príchodu posíl. Pokiaľ nie je požiarom zasiahnutý samotný systém, je možné automatické riadenie odvetrania, evakuačného systému, bezpečnostných dverí, presun výťahov do východzej polohy, v niektorých prípadoch i komunikácia so zásahovými jednotkami či pokus o elimináciu aktiváciou hasiacich zariadení. Význam EPS často prevyšuje ostatné systémy ako z hľadiska ochrany majetku, tak i života a zdravia osôb.

Hlavné komponenty systému, ktoré informujú ústredňu o vzniknutom požiari sa nazývajú požiarne hlásiče. Podľa spôsobu aktivácie rozlišujeme [12]:

Manuálne (tlačítkové) požiarne hlásiče – ako už názov napovedá, ich aktivácia je vykonaná manuálnym stlačením tlačidla. Musia byť červenej farby, umiestnené na viditeľnom a dostupnom mieste. Často je k aktivácii hlásiča potrebné rozbiť sklíčko, čím sa jednak zamedzuje náhodnej aktivácii a tiež je tak možné zistiť, ktorý hlásič poplach spustil (pokiaľ táto funkcia nie je zabezpečená elektronicky). Inštalujú sa hlavne pri východoch z objektu a na únikových trasách a do miest so zvýšeným pohybom ľudí (chodby, jedálne, haly) alebo stálou obsluhou (vrátnice, hliadkovacie veže).

Automatické požiarne hlásiče – sú zariadenia, ktoré monitorujú okolie a reagujú na fyzikálne alebo chemické zmeny (nárast alebo i pokles teploty, dym, otvorený oheň) a následne ich posielajú požiarnej ústredni. Spravidla sa inštalujú na strop alebo do určitej vzdialenosti podeň a pomocou vodičov sú prepojené s ústredňou.

V dnešnej dobe sa inštalujú manuálne hlásiče v kombinácii s automatickými. Výberu automatických hlásičov treba venovať zvýšenú pozornosť, aby sa predišlo falošným poplachom a zároveň bola zaručená maximálna úroveň ochrany. Hlásiče musia byť totiž vyberané v závislosti na chránenom objekte, jeho architektúre, prúdení vzduchu, materiáli a tiež na využití objektu a látkach, ktoré sa v ňom budú vyskytovať. Jednotlivé typy hlásičov sa odlišujú princípom monitorovania okolia a často je potreba ich kombinovať. V ponuke sú najčastejšie [12]:

Teplotný hlásič – monitoruje teplotu okolia a rôznymi spôsobmi určuje, či jej zmena znamená požiar. *Statický* teplotný hlásič informuje ústredňu EPS v prípade, že teplota prekročí určitú hodnotu. Nevýhodou môže byť pomalý nárast teploty alebo vysoká prahová hodnota a tak neskorá reakcia na požiar. Lepšie výsledky dosahuje *diferenciálny* hlásič, ktorý monitoruje rýchlosť zmeny teploty. Obsahuje dva termistory, jeden na povrchu a jeden vo vnútri zariadenia. Vonkajší zaznamená teplotu skôr ako vnútorný a vznikne tak rozdiel v elektrickom prúde, ktorý nimi prechádza. Pri prekročení

určitej medze v nerovnováhe je vyhlásený poplach. Najlepšou možnosťou je zmiešanie oboch prístupov a použitie takzvaného *kombinovaného* teplotného hlásiča, ktorý vyhlási poplach aj pri prekročení teploty, aj pri jej rýchlej zmene.

Optický hlásič dymu – obsahuje komoru, do ktorej zvonku nepreniká žiadne svetlo. V nej sú proti sebe umiestnené dve diódy – infra LED dióda a fotodióda. Pri požiari vzniká dym, ktorý môže vniknúť do komory a zoslabí vyžarovanie infra LED diódy, ktoré zaznamenáva fotodióda. Častejšie sa používa prevedenie, kde diódy nie sú umiestnene priamo proti sebe. Po vniknutí dymu sa infra lúč odráža od jeho čiastočiek a dopadá na fotodiódu, čo má za následok zvýšenie prechádzajúceho elektrického prúdu. Tieto zmeny sú vyhodnocované a predávané ústredni EPS.

Ionizačný hlásič dymu – obsahuje dve komory, vonkajšiu a vnútornú referenčnú. V komore sa nachádza fólia s malým množstvom rádioaktívneho americia 241, cez ktorú prechádza elektrický prúd. Pokiaľ do komory vnikne dym, prúd sa zmení a vznikne tak rozdiel v napätí medzi vnútornou a vonkajšou komorou, čo môže mať za následok vznik poplachu. Princíp je teda podobný diferenciálnym teplotným hlásičom. Dokážu reagovať i na okom neviditeľné splodiny a reagujú veľmi rýchlo. Kvôli problémom s likvidáciou sa ich použitie v dnešnej dobe obmedzuje.

Multisenzorový hlásič s plynovou detekciou – patrí medzi najmodernejšie bodové hlásiče. Kombinuje výhody optických, teplotných aj chemických senzorov a udáva tak novú úroveň technológie detekcie požiaru. Chemický senzor dokáže zachytiť množstvo druhov plynov vznikajúcich pri horení a upozorniť tak naň skôr než akýkoľvek iný senzor. Disponujú tiež obrovskou odolnosťou proti falošným poplachom.

Optický hlásič plameňa – vie identifikovať infračervené alebo ultrafialové žiarenie emitované plameňom. Inštaluje sa na strop alebo stenu do bezprostrednej blízkosti miesta, v ktorom by sa potenciálne mohol oheň vyskytnúť a mal naň priamy výhľad. Používajú sa ako doplnkový prvok k teplotným alebo dymovým hlásičom.

Aspiračný hlásič – disponuje vstavaným ventilátorom alebo kompresorom a nasávacími potrubiami s otvormi. Potrubia je možné vyviesť na miesta, kde sa predpokladá zvýšené riziko vzniku ohňa alebo hromadenie dymu. Keďže nedochádza k čakaniu na voľný príchod dymu k hlásiču, dokáže reagovať veľmi rýchlo už na najranejšie štádium požiaru. Samotná kontrola vzduchu prebieha väčšinou opticky. Zisťuje sa množstvo rozptýleného svetla v komore. Čím viac tuhých častíc sa v nej pohybuje, tým je rozptýlenie väčšie a tým sa pravdepodobnosť požiaru zvyšuje. Ako zdroj svetla sa používa LED dióda, xenónová výbojka alebo polovodičový laser.

Tlakový hlásič – využíva k činnosti snímaciu trubicu a vyhodnocovaciu elektroniku. V pravidelných intervaloch dochádza pomocou kompresoru k vytvoreniu predom definovaného pretlaku v trubici. Monitoruje sa zmena tlaku, ktorú spôsobuje nárast okolitej teploty. Tento typ sa montuje na miesta, kde nie je možné použitie klasických bodových hlásičov alebo na miesta so zvýšeným množstvom prachu, hmyzu, vlhka či iných výparov, ktoré by mohli spôsobovať plané poplachy.

2.3 Klasifikácia ochranných prvkov EZS

Senzor, inak označovaný ako *snímač* alebo *detektor*, je prvok, ktorý je v priamom styku s meraným/sledovaným prostredím. To je charakteristické svojimi vlastnosťami ako sú dĺžka, teplota, tlak, intenzita svetla či zvuku. Senzor sníma tieto fyzikálne, biologické alebo chemické hodnoty a prevádza ich na elektrické veličiny [16].

Prevod môže byť analógový alebo binárny. Analógový sa v bezpečnostných systémoch využíva menej, môže slúžiť na zobrazenie aktuálnej teploty, tlaku alebo vlhkosti. Oveľa častejšie nás zaujíma prekročenie stanovenej kritickej hodnoty, k čomu stačí binárny prevod – situácia nastala alebo nenastala. Príkladom sú pohybové senzory, protipožiarne senzory, magnetické kontakty, otrasové senzory, tiesňové hlásiče a iné.

Senzory, je možné rozdeliť do niekoľkých skupín z hľadiska priestorov, pre ktorých ochranu sú primárne určené. Do rozdelenia je možné zahrnúť aj protipožiarne detektory popísané v kapitole 2.2, ktoré nemusia byť nutne len súčasťou EPS, ale môžu tvoriť doplnkový modul i pre bežné zabezpečovacie systémy. Rozdelenie je nasledujúce [12]:

- **Prvky plášťovej ochrany:** magnetické kontakty, detektory na ochranu zasklených plôch, mechanické kontakty, vibračné senzory, poplachové fólie (tapety, polepy, sklá), drôtové senzory.
- **Prvky priestorovej ochrany:** pasívne a aktívne infračervené senzory, ultrazvukové a mikrovlnné senzory, kombinované duálne senzory, protipožiarne detektory.
- **Prvky tiesňovej ochrany:** verejné, skryté a osobné tiesňové hlásiče.
- **Prvky predmetovej ochrany:** otrasové a kapacitné senzory, detektory na ochranu zavesených predmetov.
- **Prvky vonkajšej obvodovej ochrany:** mikrofonické káble, infračervené a mikrovlnné bariéry, štrbinové káble, podzemné tlakové hadice.
- **Špeciálne senzory:** tlakové senzory, nášľapné koberce.

2.3.1 Plášťová ochrana

Plášťová ochrana je jednou z najlepších foriem stráženia objektu. Orientuje sa na zabezpečenie dverí, okien, brán a iných možných vchodov do stráženého objektu, ktoré sú najľahšie preniknuteľnými miestami budovy a je cez ne realizovaná väčšina vniknutí. Senzory sú zväčša jednoducho prepojiteľné s EZS a ich výstupy sú často binárne.

Magnetický kontakt – tvorí základný komponent pri zabezpečovaní objektu. Je malý, jednoducho inštalovateľný a cenovo pomerne dostupný. Bežne sa skladá z *jazýčkového spínača* a *permanentného magnetu*. Magnet sa inštaluje na pohyblivé časti (dvere, okná, rolety) a jazýčkový kontakt na stabilnú časť (rám), oba z vnútornej strany objektu. V uzatvorenom stave je kontakt spínača zopnutý pôsobením magnetického poľa. Pri akomkoľvek pokuse o otvorenie dochádza k prerušeniu kontaktu a rozpojeniu elektrického obvodu, čo má za následok vyhodnotenie stavu narušenia. Magnetické kontakty sa buď prichytávajú priamo na pohyblivý predmet (povrchové) alebo sa zapúšťajú do vnútra (zapustené), čím sa stávajú odolnejšie voči odhaleniu a poškodeniu. Dôležité je dodržanie maximálnej vzdialenosti oboch častí v pokojovej polohe [26].

Pre objekty s vysokým stupňom zabezpečenia existujú špeciálne druhy magnetických kontaktov, ktoré obsahujú sériovo-paralelnú kombináciu viacerých jazýčkov (3 – 7), z ktorých niektoré sú spínacie iné rozpínacie. Nie je tak možné jednoducho priložiť externý magnet k jazýčkovému relé a simulovať tak jeho zopnutie [12]. Obísť toto zabezpečenie je však možné viacerými spôsobmi, napríklad rozbitím skla na okne alebo vyrazením otvoru v dverách mimo kontakt.

Detektor trieštenia skla – ide o zariadenie, ktoré je schopné zaznamenať charakteristický zvuk rozbíjania skla. Odposluch je zabezpečený mikrofónom zabudovaným v zariadení – *akustické detektory*. Elektronika využíva pásmovú prepusť, ktorá prepustí len časť spektra typickú pre trieštenie skla. Lepšie detektory majú viacero prepustí pre lepšiu elimináciu falošných poplachov. Zariadenia sa môžu líšiť v tom, či dokážu sledovať rozbitie skla potiahnutého bezpečnostnou fóliou alebo v minimálnej veľkosti sklenej plochy, ktorej rozbitie je možné zaznamenať. Niektoré typy analyzujú zvukové vlny, ktoré sa v dobe rozbitia šíria sklom. Tie musia byť pevne spojené s plochou skla – *kontaktné detektory*.

Samostatné použitie týchto detektorov poskytuje len minimálne zabezpečenie a narušiteľ je schopný ich často jednoducho obísť. Preto je vhodná kombinácia s magnetickými kontaktami, s ktorými tvoria značne sofistikovanejšiu ochranu.

Poplachové fólie, tapety, polepy, sklá – v dnešnej dobe menej používaný spôsob, no ešte nedávno sa polepy používali na ochranu okien a sklenených vitrín v obchodoch. Či už sa jedná o fóliu, polep alebo sklo, všetky tieto nosiče obsahujú tenký vodivý drôt, ktorého prerušením je vyvolaný poplach.

2.3.2 Priestorová ochrana

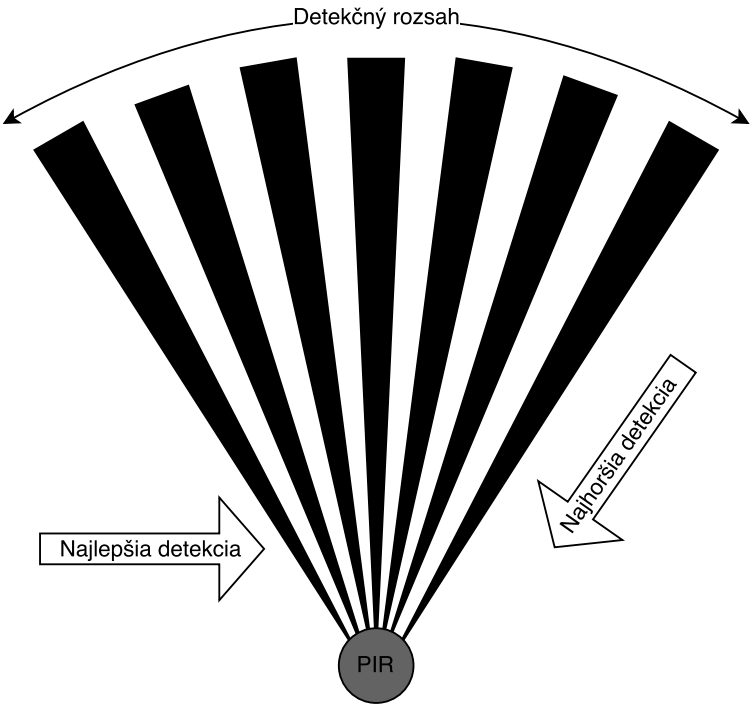
V dnešnej dobe je jej zaistenie súčasťou takmer každého zabezpečovacieho systému a tvorí výborný doplnok k plášťovej ochrane. Hlavným komponentom je *pohybový senzor*, ktorý dokáže zaznamenať pohyb v zornom poli. Podľa spôsobu snímania prostredia ich delíme na:

- **Pasívne pohybové detektory:** sledujú okolité prostredie a indikujú fyzikálne zmeny. Spadajú sem najpoužívanejšie infračervené senzory (PIR – z anlgického *Passive Infra Red*).
- **Aktívne pohybové detektory:** vytvárajú svoje vlastné prostredie, ktorého zmeny následne skúmajú.

Ochrana proti zatemneniu – *antimasking* je funkcia, ktorou sú vybavené pokročilé pohybové detektory a indikuje prekrytie snímacej plochy senzoru farbou alebo predmetom. Aplikujú sa vo verejných priestoroch, kde hrozí riziko prípravy objektu k neskoršej sabotáži.

Infračervený senzor – pracuje na princípe zachytávania zmien vyžarovania v infračervenom pásme kmitočtového spektra elektromagnetického vlnenia [12]. Zdrojom môže byť každé teleso v rozmedzí -273 °C až 560 °C, ktoré vyžaruje vlnenie v infrapásme, odpovedajúce jeho teplote. Pomocou optiky pohybového čidla je obraz priestoru rozdelený na aktívne a neaktívne zóny. Ak dôjde k pohybu objektu, ktorého teplota je odlišná od teploty pozadia, senzor zaznamenáva zmeny pri prechode z jednej zóny do

druhej, čo vedie k vyvolaniu poplachu. Pohyb smerujúci k senzoru je ťažšie zaznamenateľný ako pohyb vodorovný so snímacou šošovkou, znázornené na obrázku 2.2. Tvar zorného poľa a dosah závisia na vyhodnocovacej elektronike a optike.



Obr. 2.2: Zóny tvorené pohybovým senzorom a schopnosť detekcie pohybu.

Parametre detektorov sa môžu rôzniť a pre rôzne typy priestorov je potreba použiť iné typy senzorov. Pri inštalácií je nutné dbať na pokyny výrobcu. Správny chod a vznik falošných poplachov môže ovplyvniť výška umiestnenia čidla, prítomnosť krbu, vzduchotechniky, ústredného kúrenia alebo okná orientované k slnku či reflektory okoloidúcich automobilov.

Ultrazvukový senzor – patrí do kategórie aktívnych pohybových detektorov. Vysiela do priestoru mechanické vlnenie, ktorého kmitočet je nad pásmom počuteľným ľuďmi. Následne prijímačom zachytáva vlny, ktoré sa odrazili od telies v prostredí. Vzájomný vzťah medzi prijatým a vyslaným vlnením je v ustálenom prostredí (bez pohybu) pri opakovanom meraní nemenný. No pri pohybe v priestore sa mení fáza prijatého vlnenia a zmena je vyhodnotená ako stav narušenia. V podstate ide o aplikáciu *Dopplerovho javu*. Pri inštalácii je treba brať ohľad na to, že ľudia síce ultrazvuk nezaznamenajú, ale psi, netopiere či komáre áno.

Mikrovlnný senzor – funguje na podobnom princípe ako ultrazvukový senzor s tým rozdielom, že pracuje v kmitočtovom pásme elektromagnetického vlnenia (2.5 GHz, 10 GHz alebo 25 GHz). Keďže toto žiarenie môže prechádzať cez tenšie steny, sklo, plasty či iné materiály, narušenie môže vyvolať i pohyb mimo strážený objekt. Tiež dlhodobé vystavenie osôb mikrovlnnému žiareniu môže spôsobiť zdravotné problémy.

2.3.3 Predmetová ochrana

Ochrana predmetov sa od ochrany celých objektov líši prevažne len v spôsobe inštalácie ochranných senzorov. Vyžadované je väčšinou zabezpečenie predmetu v inak aktuálne nezabezpečenom objekte s rušnou premávkou ľudí. Monitoruje sa napríklad narušenie bezpečnostnej zóny v blízkom okolí, omedzuje sa pohyb s predmetom alebo aj len obyčajný dotyk.

Predmetové ochranné prvky je možné vidieť v múzeách, galériách či na podobných miestach, kde je počas výstavy ochrana priestoru ako celku značne (úplne) obmedzená, no predmety je potreba i tak udržať v bezpečí. Využitie nachádzajú tiež ako ochrana trezorov či vitrín.

Otrasový detektor – dokáže spracovávať vlnenie v telese (*seizmický*), ktoré vzniká pri jeho presune, pokuse o zničenie či inej manipulácii. Využíva sa hlavne na zabezpečenie kľúčových stien, trezorových skríň či komorových trezorov. Najnovšie detektory zaznamenaný signál digitálne spracovávajú a analýzou amplitúdy a frekvencie signálu dokážu reagovať na všetky dnes známe typy mechanických i termických trezorových napadnutí [12]:

1. použitie hrubého mechanického náradia,
2. vŕtanie vrátane použitia vrtáku s diamantovou korunkou,
3. použitie hydraulického tlakového náradia,
4. rezanie kyslíkovo-vodíkovým plameňom,
5. použitie plastických (a iných) trhavín.

Najjednoduchšie detektory pracujú na princípe spájania a rozpájania obvodu, ktoré spôsobuje kovová guľôčka umiestnená v strede žľabu miskovitého tvaru. Každým otrasom o určitej sile dôjde k pohybu guľôčky od stredu, čo spôsobí prerušenie obvodu.

Závesný detektor – umožňuje zavesenie predmetu na jeho hák a na základe sily, ktorou naň predmet pôsobí, dochádza k vyhodnoteniu zaťaženia. V závislosti na nastavenej citlivosti dokážu moderné detektory reagovať i na tie najmenšie zmeny (dotyk). Primárne určený na ochranu umeleckých a historických diel.

2.3.4 Perimetrická ochrana

Perimetrická ochrana sa zaoberá ochranou vonkajších, obvodových častí chránených objektov. Jedná sa o špeciálny druh zabezpečenia, ktorý vychádza z dôkladného prieskumu zabezpečovaného objektu. Podnetov k vytvoreniu falošného poplachu je vo vonkajšom prostredí mnoho a nie je možné všetky eliminovať. Veľmi dobre sa preto dopĺňajú s priemyselným kamerovým systémom (CCTV). Pri výbere ochranných prvkov je potrebné dbať hlavne na [12]:

- vlnenie trávnatého porastu,
- pohyb listov a konárov stromov či kríkov,
- vibrácie oplotenia vo vetre,
- prúdenie vzduchu a vietor,

- dážď, sneh,
- pohyby rôznych druhov zvere a hmyzu,
- dopravný ruch v blízkosti sledovanej oblasti.

Rozdiely medzi vnútornými a vonkajšími senzormi musia byť hlavne v ich odolnosti. Kryty musia vydržať rôzne klimatické podmienky a často extrémne prudké zmeny teplôt či vlhkosti. Elektronika by mala byť vodotesne uzatvorená, modernejšie zariadenia sú opatrené vnútorným vyhrievaním, ktoré kompenzuje nízke teploty a bráni zahmlievaniu a hrdzaveniu. Tiež je kladený dôraz na vyšší dosah, často i 10 krát väčší ako je tomu u vnútorných senzorov.

Dnešný trh ponúka široký sortiment vonkajších senzorov. Každý má svoje výhody i nevýhody a často treba voliť vhodnú kombináciu, ktorá by zaistila nielen dostatočné zabezpečenie, ale i vyššiu odolnosť voči planým poplachom. Medzi často používané patria:

Infračervené bariéry a závory – patria medzi najbežnejšie inštalovaný ochranný prvok. Sú tvorené jedným alebo viacerými prijímačmi a vysielačmi infračerveného žiarenia, ktoré sú nasmerované proti sebe. Pri prerušení jedného alebo viacerých lúčov v určitom poradí je indikovaný poplachový stav. Nevýhodou je citlivosť na dážď a sneh, zložitá inštalácia, nutnosť úplne rovného terénu medzi vysielačom a prijímačom a potreba plánovania rozmiestnenia tak, aby sa lúče čiastočne prekrývali a eliminovali tak mŕtve koridory (miesta, v ktorých by narušenie nebolo odhalené).

Mikrovlnné bariéry – sú taktiež zložené z vysielača a prijímača, no medzi nimi dochádza k vytvoreniu elektromagnetického poľa. Jeho prerušenie je vyhodnotené ako poplach. Výhodou je značný dosah v rozsahu 200 až 300 metrov a odolnosť voči silnému vetru. V blízkosti by sa nemali vyskytovať pohybujúce sa predmety, trávy, kvety, konáre stromov či kríky. Pri inštalácií pozdĺž plotu je potrebné vysielač umiestniť tak, aby bol minimálne raz tak vzdialený ako je výška plotu.

Podzemné tlakové hadice – tvoria diferenciálny tlakový detektor. Pokladajú sa paralelne pod zem so vzdialenosťou cca 1 meter po obvode celého chráneného priestoru. Sú napustené nemrznúcou kvapalinou, ktorá tvorí substanciu pre prenos tlakových zmien od miest vzniku tlaku po vyhodnocovaciu elektroniku diferenciálneho tlakového senzoru. Porovnáva sa tlak medzi dvoma susednými hadicami a pri prekročení stanoveného rozdielu je vyhlásený poplach. Pomerne náročnú inštaláciu a údržbu kompenzuje veľká odolnosť voči falošným poplachom spôsobených dejmi mimo koridor s umiestnenými hadicami (vietor, dážď, sneh, okolité dopravné prostriedky, pohyb malej zvery, hmyz).

2.3.5 Tiesňový hlásič

Spadá do kategórie tiesňovej ochrany. Slúži k ochrane zamestnancov a verejnosti, ktorí sa môžu dostať do priameho ohrozenia života. Väčšinou sú to obyčajné magnetické kontakty či spínače zabudované v rôznych obaloch, v závislosti na nutnosti ich nepozorovaného stlačenia (pod pultom u prepážky v banke). Spravidla by však mali byť umiestnené na viditeľnom mieste (vchody, chodby, haly), aby boli dostupné ihneď a komukoľvek. Aktivujú sa manuálnym stlačením alebo automaticky s výskytom nejakej inej udalosti a ihneď dochádza k poplašnému hláseniu do miesta so stálou obsluhou (policajný, hasičský zbor), odkiaľ môže byť poskytnutá pomoc.

Kapitola 3

Analýza a návrh systému

Predošlá kapitola poskytla teoretický základ potrebný pre pochopenie všeobecného princípu fungovania bezpečnostných systémov a prvkov, ktoré sa pri ich realizácii využívajú. Táto kapitola sa bližšie venuje možnostiam realizácie a opisuje proces analýzy zabezpečovaného objektu, spracovanie požiadaviek a návrh samotného EZS.

3.1 Platforma arduino

Bezpečnostné systémy spadajú do kategórie vstavaných systémov, čo znamená, že sú spravidla riadené mikrokontrolérom. Väčšina firiem, ktoré sú na trhu už niekoľko rokov, využíva svoje vlastné riadiace jednotky, doslova vyrobené na mieru. Takáto výroba sa však môže menším spoločnostiam či súkromným osobám predražiť a tak je tu možnosť siahnuť po voľne šíriteľných platformách.

Jednou z nich je i platforma Arduino, ktorá je na trhu už od roku 2005. Pôvodne bola vyvíjaná pre študentov a keďže mala veľký úspech, tvorcovia z talianskeho *Interaction Design Institute* sa rozhodli poskytnúť všetky schémy a návody (Open Source). Hlavnou časťou každého Arduina je procesor, takmer vo všetkých prípadoch od firmy Atmel, ktorý je obklopený ďalšími elektronickými komponentami a vstupno-výstupnými pinmi. Vývoj pokračuje a vznikajú stále výkonnejšie dosky. Líšia sa tiež veľkosťou a obsiahnutými komponentami. Známe sú napríklad [23]:

Arduino Mini – ide o najmenšie Arduino na trhu. Neobsahuje USB port a programovať sa musí pomocou externého USB 2 Serial prevodníku. Obsahuje procesor *ATmega328* s taktom 16 MHz.

Arduino Nano – je v podstate Mini s vlastným USB portom a prevodníkom. Rozmery sú o niečo väčšie, no odpadá nutnosť použitia externých prípravkov.

Arduino Micro – obsahuje čip *ATmega32u4* s vlastným prevodníkom, vďaka ktorému sa môže pre počítač tváriť ako myš, klávesnica alebo iné periférne zariadenie a posielať príkazy. S ostatnými doskami je možné túto vlastnosť dosiahnuť tiež, no bolo by potreba preprogramovať prevodník.

Arduino LilyPad – je špeciálna verzia určená pre nosenie na textile.

Arduino Fio – je prispôsobené k pripojeniu rôznych bezdrôtových modulov a obsahuje procesor *ATmega328P* (8 MHz).

Arduino Uno – predstavuje najčastejšie používaný typ dosky. Je vybavený USB portom, poskytuje množstvo vstupno-výstupných pinov a procesor *ATmega328*.

Arduino Leonardo – má rovnaké vlastnosti ako Uno s tým rozdielom, že obsahuje už spomínaný čip *ATmega32u4*.

Arduino Yún – vzhľadom pripomína Uno, no ide o dosku na oveľa vyššej úrovni. Obsahuje čip *ATmega32u4* a tiež *AtherosAR9331*, ktorý je schopný riadiť beh odľahčeného linuxu Linino. Vo výbave je softvérový most, ktorý zaisťuje komunikáciu medzi oboma čipmi, ethernetový port a USB pre potreby linuxu.

Arduino Mega2560 – je rozšírená verzia Arduina Uno. Poskytuje väčšie množstvo pinov a hlavne väčší výkon vďaka procesoru *ATmega2560*. Viac v kapitole 3.1.1.

Arduino Due – sa vlastnosťami podobá Arduinu Mega2560, až na to, že obsahuje ďaleko výkonnejšiu výpočetnú jednotku, ktorou je *Atmel SAM3X8E* s frekvenciou 84 MHz a 32 bitovým jadrom.

Arduino Esplora – je hybridná doska, ktorá obsahuje joystick, tlačidlá, posuvný potenciometer, bzučiak, teplomer, trojosový akcelerometer a piny pre pripojenie LCD displeja. Je určené pre tvorbu vlastného herného ovládača (vo výbave *ATmega32u4*).

Arduino Robot – obsahuje napríklad i kompas a je určený pre tvorbu vlastného chytrého robota.

Arduino Intel Galileo – je prvá doska, ktorá pracuje na 32 bitovom čipe *Intel Quark SoC X1000* s frekvenciou 400 MHz. Obsahuje microDS slot, ethernet port, dve USB či mini-PCI Express slot.

Na oficiálnych stránkach [2] je možné nájsť oveľa viac rôznych druhov, ktoré vznikli modifikáciou spomenutých alebo ich kombináciou či rozšírením. Vybrané dosky sú zobrazené na obrázku 3.1.

Programovací jazyk je v podstate C/C++ obohatené o Arduino knižnice, s obmedzením niektorých štandartných funkcií hlavne z dôvodu nízkej kapacity pamäte RAM. Východzou kostrou programu sa tak nestáva funkcia `main` ako je tomu zvykom, ale dvojica funkcií `setup` a `loop`. `Setup` sa vykonáva vždy na začiatku programu a to len raz, čiže je vhodným miestom pre inicializáciu komponentov, premenných a kalibráciu hardvérových súčastí. Po jej skončení dochádza k volaniu `loop` funkcie, ktorá sa opakuje v nekonečnej slučke až do reštartu zariadenia. Práve tu sa nachádza jadro každého programu vytvoreného pre ktorúkoľvek dosku Arduino. Základné funkcie pre prácu s doskou ako nastavovanie smeru toku dát na pinoch, funkcie `setup` a `loop`, získanie uplynulého času, či definície konštánt pre jednotlivé registre sú súčasťou štandardnej voľne dostupnej knižnice `Arduino`.

Niektoré knižnice sú súčasťou inštalátoru vývojového prostredia a automaticky spadajú do kategórie open-source. Z nich boli využité: `Arduino, SPI, OneWire, Wire, Time, Keypad, EEPROM, SD, LiquidCrystal`, pričom ich použitie bude popísané v ďalších kapitolách. Originálne vývojové prostredie určené pre všetky typy dosiek Arduino, ktoré poskytuje jednoduché užívateľské rozhranie a možnosť nahrania programu jedným kliknutím je *Arduino IDE*, dostupné z oficiálnych stránok [2]. V ponuke je však i možnosť písať program online pomocou *Arduino Web Editoru*, či siahnuť po pokročilejšom vývojovom prostredí, napr. *Atmel Studio*.

Obr. 3.1: Arduino dosky (prevzaté a upravené z [1]).

Vývoj EZS prebiehal práve v *Atmel Studiu 7*, ktoré je určené pre vývoj aplikácií založených na procesoroch rodiny *Atmel*. Prostredie je určené pre Windows a používa *Visual Studio Shell*, vďaka čomu je možné ľahko manipulovať s rozsiahlymi projektami s mnohými zdrojovými súbormi. Pre plnú podporu Arduino dosiek je potreba pridať rozšírenie *Visual Micro*, ktoré však vyžaduje cestu k Arduino softvéru inštalovanému s Arduino IDE (od 25. 02. 2017 by mala byť závislosť nevyžadovaná, viď [22]).

3.1.1 Arduino Mega2560

Spomedzi všetkých dostupných dosiek bolo na realizáciu bezpečnostného systému vybrané Arduino Mega2560. Poskytuje dostatočné množstvo pinov a potrebný výkon. Keďže sa jedná o pomerne rozsiahly projekt, poskytuje tiež dostatok pamäťového priestoru pre program, premenné i konfiguračné dáta a tak nie je potrebné výrazne obmedzovať možnosti systému. Základné vlastnosti sú zhrnuté v tabuľke 3.1. Obmedzujúcim kritériom pri výbere riadiacej jednotky ako aj ostatných súčastí systému bola hlavne cena. Zvolené boli najoptimálnejšie prvky v pomere cena–výkon.

Mikrokontrolér	ATmega2560
Operačné napätie	5 V
Vstupné napätie (odporúčané)	7-12 V
Vstupné napätie (limity)	6-20 V
Digitálne piny	54 (z toho 15 poskytuje PWM výstup)
Analógové piny	16
Max. prúd na V/V pine	40 mA
Max. prúd na 3,3 V pine	50 mA
Flash pamäť	256 KB (8 KB for bootloader)
SRAM	8 KB
EEPROM	4 KB
Frekvencia hodín	16 MHz

Tabuľka 3.1: Technické detaily Arduino Mega2560 [3].

3.2 Analýza stráženého objektu

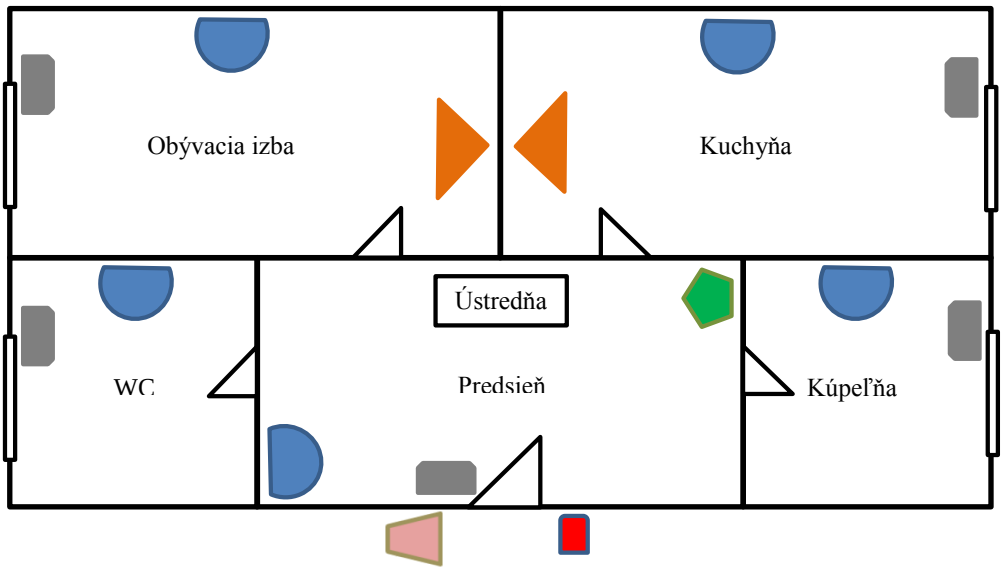
Kvalitný bezpečnostný systém je podmienený analýzou stráženého objektu. Systémy síce môžu byť sériovo vyrábané podľa jednotlivých úrovní potrebného zabezpečenia, no vždy by mali poskytovať možnosti konfigurácie a dodatočných úprav presne podľa zvoleného objektu. Je nedostatočné strážiť bytový dom s ôsmimi miestnosťami len s využitím prvkov perimetrickej ochrany alebo vynechať ochranu miestnosti kvôli nedostatočnému počtu senzorov. Tiež však nie je nutné inštalovať zbytočne predražený systém, ktorý by pomocou závesných detektorov monitoroval každý bezcenný obraz v kancelárii. Je teda nutné dobre zvážiť počet a typ jednotlivých prvkov.

Pre potreby tejto práce bol navrhnutý obytný rodinný dom, ktorý tvorí počiatočný bod v procese návrhu zabezpečovacieho systému. Objekt je z bezpečnostných dôvodov fiktívny a jedná sa len o jednoduchý návrh. Táto práca nerieši, či by tento objekt mohol skutočne existovať alebo či spĺňa akékoľvek podmienky pre život osôb.

Pre objekt je požadované zabezpečenie s prvým, najnižším stupňom zabezpečenia. Pôdorys je znázornený na obrázku 3.2. Tvorí ho päť miestností, kde každá obsahuje minimálne jeden otvor do nestráženej oblasti (vonkajší priestor). Nevyhnutná je preto plášťová ochrana, pre ktorú boli zvolené magnetické kontakty. Tie sú umiestnené na všetky okná a vchodové dvere. Pridaním detektorov trieštenia skla by sme dokázali úplne pokryť prístup cez okná, no v prípade drevených dverí by sme nezabránili možnosti ich vyrúbaniu a prieniku touto cestou. Lepšou možnosťou je preto kombinovať magnetické kontakty s prvkami priestorovej ochrany. Vzhľadom na pobyt osôb a prípadne i zvierat sú zo zdravotných dôvodov najvhodnejšie infračervené senzory pohybu. Naviac sú oproti senzorom trieštenia skla cenovo dostupnejšie. Vhodné je ešte inštalovať optické hlásiče plameňa a to hlavne do kuchyne, kde je najväčšia pravdepodobnosť vzniku požiaru a tiež do obývacej izby, pre zvýšenie pocitu bezpečia počas spánku. Pri objekte týchto rozmerov je nepotrebné zavádzať samostatný EPS a požiarne senzory môžu byť súčasťou EZS. Táto kombinácia detektorov pokrýva celý objekt a je dostačujúca pre zabezpečenie na úrovni prvého stupňa. Okolie objektu neberieme do úvahy a tak je možné vypustiť prvky perimetrickej ochrany.

Zvýšenú pozornosť si vyžadovalo plánovanie pohybových senzorov. Tie je potrebné umiestniť tak, aby sa nenachádzali priamo naproti stráženému vstupu. Pravdepodobnosť zachytenia pohybu sa totiž zvyšuje, pokiaľ osoba prechádza cez aktívne a neaktívne zóny,

ktoré sú vytvárané optikou detektoru. Na obrázku 3.2 je zobrazené konečné umiestnenie všetkých prvkov. Napríklad pohybový senzor v kuchyni lepšie zachytáva pohyb prichádzajúci od okna ako od dverí, čo však neprekáža, pretože dvere sú naopak lepšie chránené senzorom v predsieni.



Piktogram	Zariadenie	Piktogram	Zariadenie
	Pohybový senzor		Akustická signalizácia
	Magnetický kontakt		Optická signalizácia
	Detektor plameňa		Teplomer

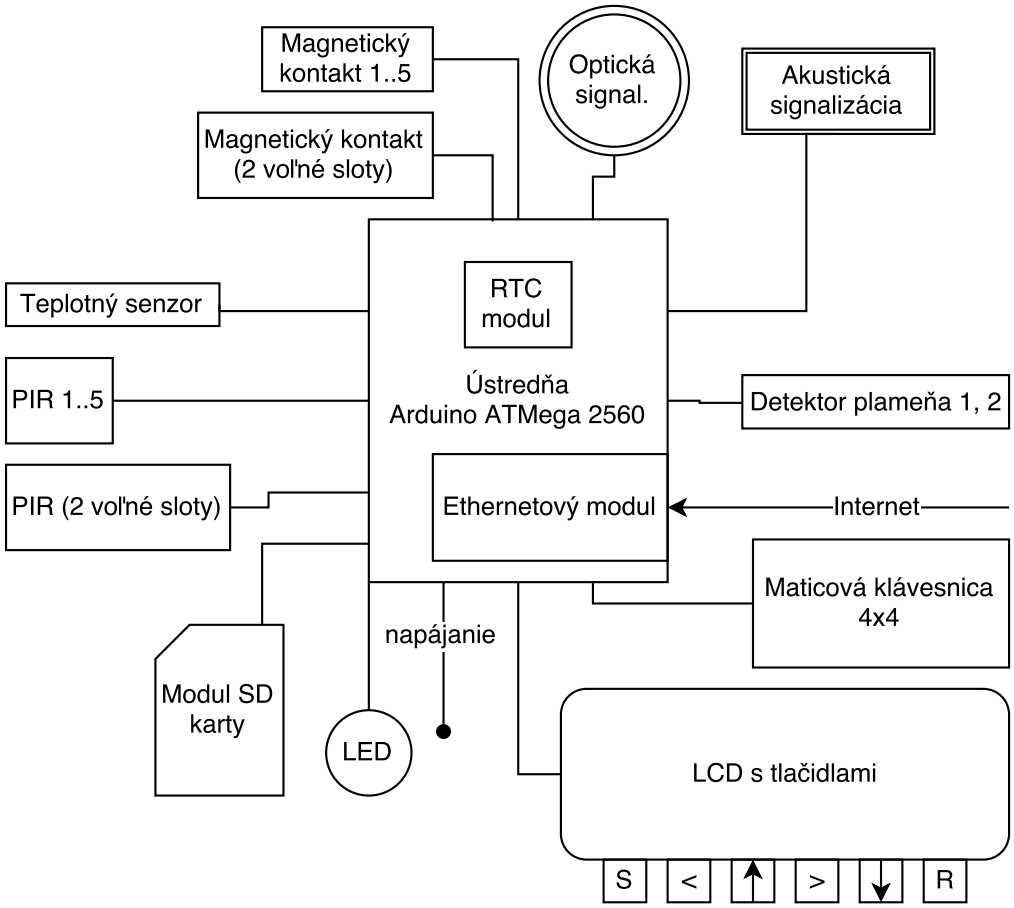
Obr. 3.2: Pôdorys objektu s inštalovanými senzormi.

3.3 Požiadavky na zabezpečovací systém

Systém bol navrhovaný tak, aby sa nestal len jednoúčelovým zariadením stavaným presne pre jeden typ objektu a jedného užívateľa. Programová časť projektu bola vytváraná s ohľadom na prehľadnosť a čo najväčšiu vzájomnú nezávislosť jednotlivých častí. Pre každý typ hardvérového komponentu je vytvorená samostatná knižnica. Je tak ponechaná možnosť budúceho vývoja, kde by mohlo na projekte spolupracovať viac ľudí a každý môže rozvíjať inú časť.

Navrhnutý EZS je zameraný na ochranu objektov s prvým stupňom zabezpečenia. Je možné ho v stanovenom rozmedzí dodatočne upravovať alebo konfigurovať podľa potrieb zabezpečovaného objektu. Zmeny vlastností môžu prebiehať preprogramovaním s upravenými hodnotami alebo pomocou konfiguračného rozhrania popísaného v kapitole 4.6 priamo počas behu.

Podporuje prístup dvoch typov užívateľov. Prvým je majiteľ bezpečnostného systému a druhým je servisný pracovník, zamestnanec firmy, ktorá tento typ EZS dodáva. Každý má stanovené úkony, ktoré môže vykonávať. Pre uskutočnenie akcií, ktoré sú prístupné len jednému typu užívateľa, je potrebné zadať príslušné prístupové heslo.



Obr. 3.3: Bloková schéma navrhnutého EZS.

Dôležitá je existencia jednoduchého užívateľského rozhrania, ktoré musí byť zrozumiteľné i pre technicky menej zdatných používateľov. Ovládanie vyžaduje len znalosť základných pravidiel, popísaných v kapitole 4.3. Interakcia s užívateľom je vedená prostredníctvom LCD displeja, maticovej klávesnice a niekoľkých tlačidiel. O niektorých aktivitách informuje stavová LED dióda. Medzi doplnkové a často chcené vlastnosti patrí i zobrazovanie aktuálneho času a teploty. Teplotné čidlo je možné vyviesť do akejkoľvek miestnosti, či mimo objekt.

Medzi pokročilé vlastnosti patrí možnosť pripojenia k internetu a sledovania stavu objektu prostredníctvom jednoduchej webovej stránky. Systém tiež ukladá záznamy o narušeniach objektu a kľúčových akciách vykonaných na zariadení vo vhodnom formáte na SD kartu, odkiaľ je ich možné prehliadať alebo ďalej spracovávať.

Samozrejmosťou je vyhodnocovanie pripojených senzorov v závislosti na zónach, ktorých priraďovanie je taktiež podporované. Narušenie je signalizované opticky i akusticky.

Celý systém spolu so zvolenými prvkami je znázornený blokovou schémou 3.3. Zobrazený je tak počet použitých senzorov konkrétne pre potreby zabezpečovaného objektu, ako i počet neobsadených slotov, ktoré môžu slúžiť pre realizáciu vo väčších objektoch. Cieľom práce je však realizovať systém s pokrytím čo najväčšieho počtu poskytovaných slotov.

Kapitola 4

Realizácia a implementácia systému

Kapitola postupne popisuje proces vývoja zabezpečovacieho systému špecifikovaného v predchádzajúcej kapitole. Vývoj systému prebiehal s ohľadom na požiadavky uvedené v zadaní bakalárskej práce a dostupný materiál. K projektu však bolo pristupované ako k reálnej firemnej zákazke, ktorá má za cieľ nielen funkčný jednorázový produkt, ale i možnosť jeho jednoduchej rozšíriteľnosti či prispôsobiteľnosti iným podmienkam. Programový kód je preto rozčlenený do niekoľkých vzájomne čo najmenej závislých častí (knižníc) tak, aby bolo možné ich nezávislé použitie v iných (novších) zabezpečovacích systémoch založených na rovnakom princípe. Pozornosť je venovaná i testovaniu (viď. 4.8) a možnosti ďalších verzií systému a limity jeho rozšíriteľnosti sú načrtnuté v kapitole 4.9. Všetky komponenty sú napájané 5 V, okrem ethernetového modulu (viď 4.5), ktorý vyžaduje 3,3 V.

4.1 Rozbor zvolených senzorov

Senzory boli vyberané tak, aby boli plne kompatibilné s platformou Arduino a nevyžadovali dodatočné zložité úpravy, ktoré by spomaľovali samotnú realizáciu a zvyšovali cenu výsledného produktu.

K niektorým typom senzorov bola vytvorená samostatná knižnica obsahujúca program na jeho ovládanie. K ich činnosti bola využitá iba štandardná knižnica `Arduino`. Vzhľadom na samostatnosť komponentov bol zvolený objektovo orientovaný prístup.

Magnetický kontakt – je jednoduchá súčiastka, ktorej výber nebolo nutné z hľadiska elektroniky dlho skúmať. Odlišnosti boli maximálne vo farbe či veľkosti, prípadne dosahu magnetického poľa.

Kód potrebný k obsluhe sa nachádza v súboroch `MagSens.h` a `MagSens.cpp`. Magnetický kontakt zastrešuje trieda `MagSens`, ktorej konštruktor vyžaduje zadanie čísla pinu, do ktorého je kontakt zapojený. Ten je nastavený ako vstupný a tiež je využitý interný pull-up rezistor, ktorý je na doske dostupný pre každý digitálny pin. Keďže ide o obyčajný spínač bez akejkoľvek elektroniky, ktorý môže v rozpojenom stave zachytávať okolitý šum, je potrebné v prípade rozpojenia kontrolovať úroveň logickej jednotky a nie nuly. To dosiahneme práve použitím pull-up rezistoru a pripojením druhého vodiča k zemi.

Stav konkrétneho kontaktu je možné zistiť volaním metódy `IsDisconnected`. Objekt tiež uchováva informáciu o zóne, v ktorej sa nachádza a o tom, či má byť kontakt aktivovaný alebo nie. V prípade, že je nastavený ako neaktívny, metóda `IsDisconnected` vracia hodnotu `false` bez ohľadu na skutočný stav.

Bezpečnostný systém podporuje maximálne sedem zapojených magnetických senzorov. Číslo je dané počtom dostupných pinov na Arduine po zohľadnení počtu ostatných senzorov a prvkov. Pre jednoduchšiu manipuláciu so všetkými siedmimi objektami bola vytvorená trieda `Mag_Group`. Tá zoskupuje všetkých sedem objektov do jedného a v hlavnom programe stačí vytvoriť len jeden objekt skupiny magnetických senzorov. Obsahuje metódy podobné tým z triedy `MagSens`, s tým rozdielom, že automaticky dochádza ku kontrole či nastaveniu všetkých siedmych senzorov. Prístup ku konkrétnemu senzoru skupiny je možné získať pomocou metódy `MagSens GetMag(byte mag)`, ktorá vracia objekt magnetického senzoru s poradovým číslom `mag`. Poradie je dané postupnosťou zadaných pinov pri volaní konštruktora skupiny.

PIR senzor – bol zvolený tak, aby bol schopný samostatnej činnosti a využíval operačné napätie 5 V. Vybraný bol modul *HC-SR501* vyobrazený na obrázku 4.1. Špecifikácie sú popísané v tabuľke 4.1. Senzor obsahuje na spodnej časti prepínač, ktorým je možné voliť medzi dvoma režimami:

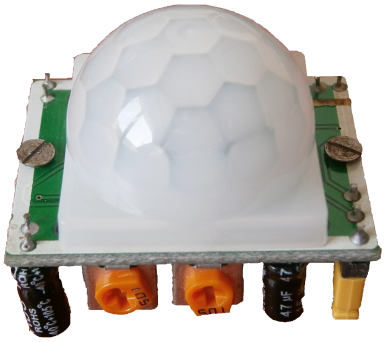
- **Režim bez opakovania:** Pri zaznamenaní pohybu dochádza k zmene výstupu z logickej nuly na logickú jednotku. Po uplynutí doby čakania závislej na vnútornom časovači je na výstupe opäť logická nula.
- **Režim s opakovaním:** Je rovnaký ako režim bez opakovania, s tým rozdielom, že pokiaľ počas logickej jednotky na výstupe senzor opäť zaznamená pohyb, časovač je vynulovaný a výstup zotrváva v logickej jednotke znovu danú dobu čakania.

Dĺžku doby čakania je možné meniť pomocou potenciometru na spodnej strane senzoru. Rovnako je možné meniť citlivosť detektoru pomocou druhého potenciometru. Vo výsledku majú všetky komponenty nastavenú maximálnu citlivosť a doba zotrvania v logickej jednotke je nastavená na minimum, pohybujúce sa v rozpätí 5-12 sekúnd. Zvolený režim je nepodstatný, systém funguje v oboch prípadoch správne.

Snímacia vzdialenosť	3-7 m
Napájacie napätie	5-20 V
Doba čakania	5-300 s
Vstupné napätie (limity)	6-20 V
Režimy aktivácie	2

Tabuľka 4.1: Technické detaily HC-SR501 [15].

Obsluha je implementovaná v súboroch `PIR.h` a `PIR.cpp` veľmi podobným spôsobom ako u magnetického kontaktu. Dostupné sú dve triedy `PIR` a `PIR_Group` (taktiež podporujúca až sedem senzorov). Zisťovanie pohybu je vykonávané metódou `MotionMonitor` s návratovou hodnotu `true`, pokiaľ došlo k pohybu. Pri niektorých druhoch senzorov je potrebný čas na ich kalibráciu. Túto možnosť poskytuje metóda `Calibrate` na základe času nastaveného prostredníctvom `SetCalibrationTime(int ct)`.



Obr. 4.1: Zvolený pohybový senzor.

Teplotný senzor – *DS18B20* je najbežnejší z teplomerov využívaných vo svete Arduina (viď obrázok 4.2a). Zakúpený bol ako praktický modul s troma konektormi pre napájanie, uzemnenie a komunikáciu. Vlastnosti teplomeru sú zhrnuté v tabuľke 4.2.

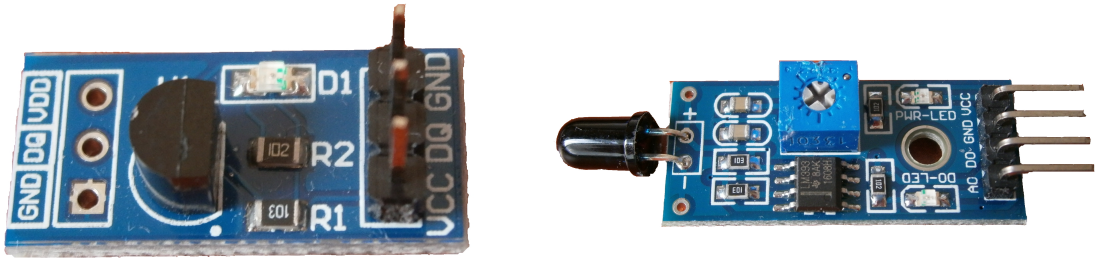
Komunikácia medzi modulom a Arduinom prebieha pomocou zbernice OneWire. Využitá bola voľne dostupná knižnica `OneWire` [20] a knižnica `DallasTemperature` [5] určená priamo pre teplotné senzory od firmy Maxim (skôr Dallas). Bezpečnostný systém využíva 12 bitové rozlíšenie teplomeru (štandardne nastavené), ktoré ponúka presnosť 0.0625 °C. Funkcie poskytované knižnicami sú dostatočné na získanie teploty a jej následné zobrazenie. Nameraná priemerná doba potrebná na prijatie výslednej teploty s rozlíšením 12 bitov je pri izbovej teplote 126 ms.

Napájacie napätie	3,3-5 V
Rozsah merania	-55 °C až +125 °C
Garancia presnosti	±0,5 °C v rozsahu -10 °C až +85 °C
Konfigurovateľné rozlíšenie	9, 10, 11, 12 bitov
Max. čas konverzie teploty (9, 10, 11, 12 bitov)	93,75, 187,5, 375, 750 ms

Tabuľka 4.2: Technické detaily DS18B20 [18].

Infračervený senzor plameňa – tvorí prvok základnej požiarnej ochrany objektu. Zakúpený bol modul znázornený na obrázku 4.2b obsahujúci jednu infračervenú LED diódu a jednoduchý komparátor. Výstup je analógový i binárny (citlivosť prepínača je možné nastaviť pomocou potenciometru). Vzhľadom na úroveň zabezpečenia, jednoduchosť objektu a financie, nie je potrebné voliť pokročilejšie snímače. Použité a zároveň podporované sú dva senzory, ktorých obsluha je implementovaná v knižnici `IRFireSensor`. Obsahuje jednu triedu s názvom `IRFireSensor`, v ktorej konštruktore je možné voliť podporu analógového i digitálneho výstupu senzoru. Metóda `IsFire` hlási vznik požiaru pokiaľ dôjde k prekročeniu prahovej hodnoty (za použitia analógového výstupu), nastavenej pomocou `SetAnalogThreshold(int minValue)` alebo pri zaznamenaní logickej jednotky na digitálnom výstupe senzoru. Pre zamedzenie falošného poplachu pri nechcenom záblesku ostrého svetla do snímacej plochy (blesk foto-

aparátu, odraz slnečných lúčov), je vykonávaná dvojitá kontrola prekročenia medznej hodnoty analógového výstupu.



(a) Teplomer (b) Infračervený detektor plameňa

Obr. 4.2: Zvolené detektory teploty a plameňa.

4.2 RTC

Skratkou RTC (z anglického *Real Time Clock*) sú označované hardvérové hodiny, ktoré dokážu merať reálny, fyzikálny čas. Arduino Mega2560 obsahuje integrovaný obvod RTC, ktorý je však použiteľný iba v prípade, že nie je prekážkou prísť o čas pri každom odpojení od napájania. Pre pohodlie užívateľov bol zakúpený externý modul, ktorý vďaka prídavnej batérii (dobíjateľnej) dokáže fungovať i bez pripojenia k externému zdroju napájania. Konkrétne sa jedná o modul, konštrukciou prispôsobený pre projekty založené na platforme Arduino s označením *DS3231*.

Uchováva informácie o sekundách, minútach, hodinách, dňoch, mesiacoch, rokoch a celkovom dátume. Dátum je na konci mesiaca automaticky prispôsobený pre mesiace s menej ako 31 dňami a tiež je zahrnutá korekcia pre prestupný rok. Na prenos dát je využitá I^2C zbernica. Dostupné sú i dva programovateľné budíky [17].

Pre prácu je využitá volne šíriteľná knižnica `DS3232RTC` dostupná z [6] a `Time`, ktorá je štandardnou Arduino knižnicou dostupnou z [14]. Čas získaný z RTC modulu je použitý na synchronizáciu interných hodín mikrokontroléru volaním `setSyncProvider(RTC.get)`. Následne je možné používať `hour()`, `minute()`, `second()` pre získanie aktualizovaného času z interných hodín. Viac o zobrazení a nastavovaní času v kapitole 4.3.

4.3 Užívateľské rozhranie

Súčasťou systému je i klávesnica, displej s tlačidlami a stavová LED dióda. Poskytujú rozhranie, vďaka ktorému je systém ovládateľný aj pre technicky menej zdatné osoby. Postupne budú popísané jednotlivé komponenty, vzťahy medzi nimi a príslušné programové riešenie.

Stavová LED dióda – zelenej farby, tvorí prvok, ktorý umožňuje informovať užívateľa o stave systému. Svieti pokiaľ je systém zapnutý, keď dôjde k narušeniu začne rýchlo blikať. Pri pokazení výstražných zariadení je tak možné zistiť, že riadiaca jednotka je v poriadku a poplach je zaznamenaný.

Objekt LED diódy a manipulácia s ním sú implementované v súboroch `LED.cpp` a `LED.h`. Okrem možností pre zapnutie a vypnutie, je metódou `Blink(int time)` možné diódu automaticky rozblikať rýchlosťou danou parametrom `time` v milisekundách. Funkcia musí byť volaná v slučke a sama si riadi čas. Jej vykonávanie neblokuje chod programu.

LCD displej – bol zakúpený formou modulu pre platformu Arduino s označením *DFR0009* (viď 4.3). Pod displejom je dostupných 6 tlačidiel, z ktorých sú pre navigáciu využité len tlačidlá `left` (doľava), `right` (doprava) a `select` (potvrdenie). Ostatné sú ponechané pre možnosti ďalšieho vývoja. Zobrazovacia plocha má 2 riadky po 16 znakoch a modré podsvietenie, ktorého intenzitu je možné upravovať pomocou vyvedeného potenciometru.

Obr. 4.3: Zvolený LCD displej s tlačidlami [7].

Knižnica `LCDPlus` rozširuje štandardnú knižnicu `LiquidCrystal` o niekoľko ďalších funkcií. Metóda `ReadLCDButtons` triedy `LCDPlus` zabezpečuje čítanie stlačených kláves čítaním analógového vstupu `A0`, ku ktorému sú pripojené. Hodnoty sa odlišujú podľa toho, či ide o displej verzie 1.0 alebo 1.1, pričom implementovaná je podpora oboch. Pre použitý displej verzie 1.0 sú hodnoty zobrazené v tabuľke 4.3. Opätovné stláčanie tlačidiel je možné s časovým oneskorením 200 ms, ktoré je definované konštantou `KEYPRESS_DELAY` v hlavičkovom súbore hlavného programu (`EZS.h`).

Metóda `PrintOnLine(int row, String item, bool clr)` umožňuje výpis reťazca do užívateľom zvoleného riadku a prípadné vymazanie predošlého obsahu. Preťažovaním metód sú vytvorené rovnomenné funkcie pre výpis čísel typu `float` a `int`.

Menu – je súčasťou knižnice `LCDPlus` implementované triedou `Menu`. Podporuje maximálne 10 položiek a poskytuje metódy pre pohyb medzi nimi, označenie aktuálnej položky za zvolenú či možnosť priradenia hodnoty a iné. Prepínanie medzi položkami prebieha pomocou kláves `right` (nasledujúca) a `left` (predchádzajúca). V zabezpečenom alebo servisnom režime nie je navigácia možná.

Rozsah analógových hodnôt	Klávesa
1-49	Doprava
50-194	Hore
195-379	Dole
380-554	Doľava
555-790	Potvrdenie
iné než vymenované	Nestlačená

Tabuľka 4.3: Analógové hodnoty tlačidiel na LCD displeji.

Obsluha akcií spojených so zvoleným menu je implementovaná v hlavnom projektovom súbore `EZS.ino`. V tabuľke 4.4 je popísaný význam jednotlivých položiek a udalostí, ku ktorým dôjde pri stlačení tlačidla `select` (položka s poradovým číslom 1 je zobrazovaná po zapnutí systému). Zobrazovaný text sa v jednotlivých udalostiach mení tak, aby podľa neho užívateľ vedel čo robí alebo má robiť. Zobrazovanie času je vo formáte *hh:mm:ss* a teplota je vypísaná s presnosťou na dve desatinné miesta. Pri zadávaní prístupových hesiel, sú zadávané znaky zobrazované znakom `'*'`.

Položka č.	Popis položky	Udalosť pri zvolení
1	Zobrazenie teploty a času.	Vyzva k zadaniu nového času.
2	Možnosť aktivácie zabezpečenia	Výzva k zadaniu prístupového hesla.
3	Zmena prístupového hesla.	Výzva k zadaniu starého a dva krát nového hesla.
4	Servisný režim.	Výzva k zadaniu servisného kódu a následné prepnutie režimu.

Tabuľka 4.4: Význam položiek menu.

Maticová klávesnica – tvorí hlavný konfiguračný prvok. Kedykoľvek je užívateľ vyzvaný zadať nejakú hodnotu, môže tak učiniť len prostredníctvom tejto klávesnice. V programe je klávesnica reprezentovaná objektom triedy `Keypad`, definovanej v rovnomennej štandardnej knižnici. Obsluha je voči ostatnému behu neblokujúca. Stisk klávesy je zisťovaný metódou `getKey()`.

Znaky sú ukladané v poradí, v ktorom sú zadávané, počínajúc výzvou až do špecifického momentu daného situáciou:

- **Zmena času:** Užívateľ zadáva postupne 6 číselných údajov, ktoré reprezentujú požadovaný čas vo formáte hh:mm:ss. Zadávané hodnoty sú priebežne zobrazované na LCD. Dvojbodky písať nemusí, sú automaticky doplňované. Prvé dvojčísle môže nadobudnúť len hodnôt 00-23, druhé a tretie 00-59. Pokiaľ dôjde k stlačeniu nevyhovujúcej hodnoty, zadanie sa ignoruje a čaká sa na stlačenie správnej hodnoty. Po zadaní šiestej číslice sa čas automaticky uloží do RTC a zosynchronizuje. Kedykoľvek v priebehu zadávania je možné stlačiť znak `'#'`, pre návrat do menu bez uplatnenia zmien.
- **Zadanie hesla:** Užívateľ po výzve k zadaniu prístupového alebo servisného kódu môže zadávať ľubovoľné znaky dostupné na klávesnici okrem `'#'`. Tá slúži k po-

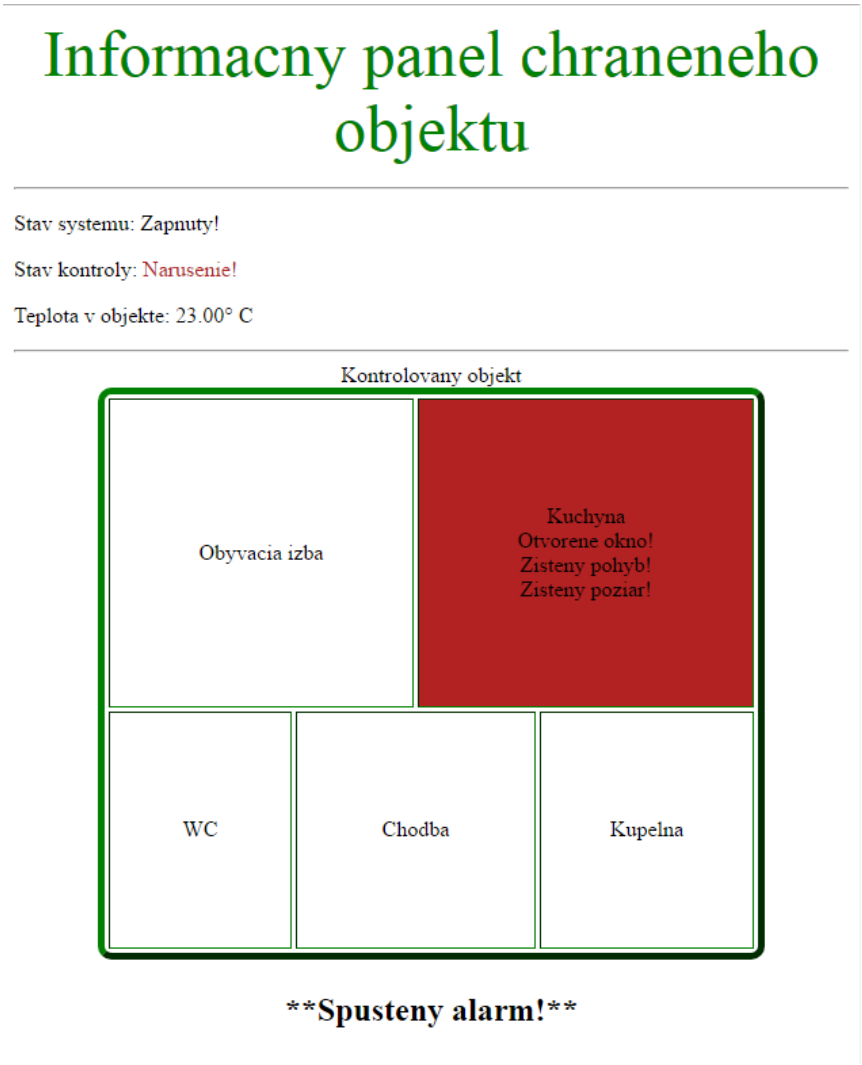
tvrdeniu napísaného hesla. Podporované je heslo dĺžky 1-8 znakov. Z režimu zadávania je užívateľ automaticky presmerovaný do menu po pokuse zadať viac ako 9 znakov. Načítanie a porovnanie je implementované funkciou s predpisom `int ReadCompareCode(String code)`, ktorá vracia hodnotu `true`, pokiaľ sa zadaný kód zhoduje s kódom daným parametrom `code`. Zjednodušený výňatok funkcie a príklad jej použitia je znázornený v nasledujúcom kóde:

```
String inputCode = "";
String correctCode = "1234";

loop(){
   int code = ReadCompareCode(correctCode);
   if(code == false){
      //udalosti pri nespravne zadanom kode
   } else if(code == true) {
      //udalosti pri spravne zadanom kode
   }
}

int ReadCompareCode(String code){
   char c = keypad.getKey();
   if(c){
      if(c == '#' || inputCode.length() == 9){
         if(inputCode == code) {  //spravny kod
            inputCode = "";
            return true;
         } else { //nespravny kod
            inputCode = "";
            return false;
         }
      } else inputCode += c; //ukladanie kodu
   }
   return -1;
}
```

Výberom tretej položky menu je možné prístupové heslo meniť. Po zadaní starého prístupového hesla je užívateľ vyzvaný k zadaniu nového a následne k jeho zopakovaniu pre potvrdenie správnosti.

Webová stránka – je vytvorená na mieru podľa zabezpečovaného objektu. Umožňuje užívateľovi vzdialene sledovať jeho stav a v prípade narušenia zistiť, ktorý senzor spôsobil poplach. Stránka sa obnovuje každé 4 sekundy. Zobrazuje pôdorys objektu a v prípade narušenia zmení farbu príslušnej miestnosti na červenú, aby bola zmena situácie viditeľná. Tiež vypíše typ narušenia (pohyb, otvorené okno/vchod alebo požiar) v danej časti objektu. Okrem toho zobrazuje informáciu o tom, či je ochrana zapnutá alebo vypnutá a teplotu. Na obrázku 4.4 je znázornený stav stránky pri zaznamenaní poplachu všetkými senzormi v kuchyni. Realizácia pripojenia systému k internetu a proces odosielania stránky je popísaný v kapitole 4.5. HTML kód sa nachádza v súbore `index.html`.

Textové konfiguračné rozhranie – je dostupné len v režime servisného módu a je určené pre pokročilú konfiguráciu systému servisným pracovníkom. Interakcia prebieha



Obr. 4.4: Webová stránka v stave narušenia.

formou príkaz – odpoveď. Bližšie informácie vrátane dostupných príkazov a spôsobu realizácie sú uvedené v kapitole 4.6.

4.4 Princíp riadenia a zabezpečenia

Hlavnou úlohou zabezpečovacieho systému je schopnosť prijímať informácie od jednotlivých senzorov a ovládacích zariadení, vyhodnocovať ich a vhodne interpretovať. Celý proces je riadený ústredňou – Arduinom. Obslužná rutina je implementovaná v hlavných projektových súboroch `EZS.ino` a `EZS.h`. Kapitola sa venuje popisu programovej časti a použitým algoritmom a princípom.

Definícia pinov – je vlastne priradenie slovných pomenovaní k jednotlivým číslam pinov, pre jednoduchšiu orientáciu v kóde. Zároveň je možné ich zoznam použiť pri inštalácii systému, nakoľko poskytujú dokonalý obraz o tom, ktorý pin k čomu slúži. V tabuľke 4.5 sú vypísané slovné označenia a adekvátne priradené čísla vstupu/výstupu na doske.

Definície sú súčasťou hlavičkového súboru `EZS.h`. Tabuľka zároveň môže slúžiť ako pomôcka pri inštalácii systému, ktorá sa tak stane veľmi jednoduchou.

Označenie	**Pin**	**Označenie**	**Pin**	**Označenie**	**Pin**
PIR_0_PIN	22	MAG_0_PIN	23	THERM_0_PIN	36
PIR_1_PIN	24	MAG_1_PIN	25	IR_0_A_PIN	A8
PIR_2_PIN	26	MAG_2_PIN	27	IR_1_A_PIN	A9
PIR_3_PIN	28	MAG_3_PIN	29	STATUS_LED_PIN	15
PIR_4_PIN	30	MAG_4_PIN	31	SD_SS	16
PIR_5_PIN	32	MAG_5_PIN	33	ACOUSTIC_SIG_PIN	40
PIR_6_PIN	34	MAG_6_PIN	35	OPTICAL_SIG_PIN	41
K_ROW_1	48	K_ROW_4	42	K_COl_3	45
K_ROW_2	46	K_COL_1	49	K_COl_4	43
K_ROW_3	44	K_COL_2	47		

Tabuľka 4.5: Definície využitých pinov.

Inicializácia systému – je veľmi dôležitá z hľadiska správneho nastavenia a následného bezproblémového chodu. V prvom rade dochádza k vytvoreniu objektov reprezentujúcich jednotlivé komponenty, čím vznikne náväznosť na adekvátne piny. Okrem objektov sú vytvorené i potrebné globálne premenné. Samotný proces inicializácie je zahájený funkciou `setup` a to v nasledujúcom poradí:

1. inicializácia rýchlosti prenosu dát sériovej komunikácie (SPI) na hodnotu 56000 baud,
2. načítanie konfiguračných hodnôt z pamäte EEPROM,
3. nastavenie servisného rozhrania,
4. inicializácia SD karty,
5. konfigurácia a spustenie ethernetového serveru,
6. zapnutie LCD displeja,
7. získanie údajov o aktuálnom čase z RTC modulu a aktualizácia interných hodín mikrokontroléru,
8. nastavenie oneskorenia pre opätovné stlačenie kláves maticovej klávesnice na hodnotu 50 ms,
9. získanie a uloženie informácií o stave jednotlivých senzorov a vytvorenie archivačného záznamu o spustení,
10. rozsvietenie stavovej LED diódy na znak, že systém je úspešne spustený.

Väčšina použitých komponent požaduje konfiguračné dáta na upresnenie činnosti. Niektoré sú pevne dané a ide o štandardné hodnoty, nemožné meniť inak než preprogramovaním. Iné je však možné meniť za chodu, čím je poskytnutá možnosť úprav vlastností bez nutnosti pokročilých znalostí programovej štruktúry. Aby zmeny pretrvali i po reštarte systému alebo výpadku napájania, je k ich ukladaniu použitá pamäť EEPROM (z anglického *Electrically Erasable Programmable Read-Only Memory*), ktorá uchováva obsah i po odpojení zariadenia. V tabuľke 4.6 je zoznam

využitých počiatočných adries, ich programových definícií a popis a maximálna veľkosť na nich ukladaných dát. Kvôli prehľadnosti sú počiatočné adresy deliteľné číslom osem.

Adresa	Názov konštanty	Veľkosť	Popis
0	EEADR_BYTEIP1	1 B	Prvý byte IP adresy.
8	EEADR_BYTEIP2	1 B	Druhý byte IP adresy.
16	EEADR_BYTEIP3	1 B	Tretí byte IP adresy.
24	EEADR_BYTEIP4	1 B	Štvrtý byte IP adresy.
32	EEADR_PORT	4 B	Port webového serveru.
128	EEADR_MAILSERVER	48 B	Emailový server.
176	EEADR_DEVICENAME	48 B	Názov zariadenia.
224	EEADR_FROMMAIL	48 B	Adresa odosielateľa emailu.
272	EEADR_TOMAIL	48 B	Adresa prijímateľa emailu.
320	EEADR_SUBJECT	48 B	Predmet emailu.
368	EEADR_TEXT	64 B	Text emailu.
432	EEADR_TIMETOLEAVE	4 B	Čas na opustenie budovy.
440	EEADR_IRFIRE0THRESHOLD	2 B	Citlivosť požiarneho sen. 0.
448	EEADR_IRFIRE1THRESHOLD	2 B	Citlivosť požiarneho sen. 1.
456	EEADR_PIRACTIVATION	8 B	Aktivačný reťazec PIR sen.
472	EEADR_PIRZONES	8 B	Zónový reťazec PIR sen.
480	EEADR_MAGACTIVATION	8 B	Aktivačný reťazec mag. sen.
488	EEADR_MAGZONES	8 B	Zónový reťazec mag. sen.
496	EEADR_USERPASS	10 B	Užívateľské prístupové heslo.

Tabuľka 4.6: Zoznam položiek uložených v pamäti EEPROM.

Pre zapisovanie a čítanie pamäte bola využitá štandardná Arduino knižnica `EEPROM`. Tá však nepodporuje prácu s premennými typu `String`. Vytvorené bolo rozšírenie o funkcie `EEPROMReadString` a `EEPROMWriteString`, ktoré sa nachádzajú v súboroch `EepromPlus.cpp` a `EepromPlus.h` a umožňujú zápis a čítanie reťazcov. Zároveň je doplnená i funkcia pre výpis časti pamäte a jej zmazanie. Konfigurácia hodnôt v pamäti je vykonávaná prostredníctvom servisného režimu, popísaného v kapitole 4.6. Bezprostredne po dokončení inicializácie dochádza k volaniu hlavnej programovej slučky – funkcie `loop`.

Pracovné režimy – sú hlavnými parametrami, ktoré ovplyvňujú správanie systému. Reprezentované sú troma premennými typu `boolean` – `PROTECTED_MODE`, `EMERGENCY_MODE` a `SERVICE_MODE`. Tie sú v rámci hlavnej slučky neustále kontrolované, pričom aktívny môže byť v daný okamih práve jeden. Činnosť jednotlivých režimov je možné zhrnúť následovne:

- **Núdzový (pohotovostný) režim:** Jedná sa o režim, ktorý je aktívny okamžite po zapnutí systému a nevyžaduje nutnosť aktivácie zabezpečenia. Kontroluje stav oboch požiarnych senzorov. Tento režim nie je možné užívateľsky vypnúť. Poplach je po zaznamenaní plameňa z bezpečnostných dôvodov vyvolaný okamžite, bez zisťovania príčin vzniku požiaru. Zrušenie je možné vykonať zadaním prístupového kódu, ku ktorému je po dobu poplachu užívateľ vyzvaný. V pokojovom stave režim nijak nebráni práci so systémom. Pri vstupe do servisného

režimu treba dbať na zvýšenú opatrnosť, pretože počas tejto doby je núdzový režim neaktívny.

- **Chránený režim:** Je hlavným zabezpečovacím režimom, ovládateľným prostredníctvom užívateľského rozhrania. Po zapnutí systému je neaktívny. Zvolením druhej položky menu – *Start protection* a zadaním prístupového hesla dochádza k jeho aktivácii. Zároveň je vypnutý núdzový režim, nakoľko je automaticky kontrolovaný stav všetkých senzorových vstupov a výstupov (vrátane požiarnych). Počas stráženia je užívateľovi zobrazená výzva k ukončeniu opätovným zadaním prístupového hesla a tak nie je možné pristupovať k ostatným vlastnostiam. Narušenie spúšťa poplach ihneď alebo s miernym oneskorením, v závislosti na zóne vzniku.
- **Servisný režim:** Je využívaný servisným pracovníkom ku konfigurácii vlastností systému. Aktivuje sa výberom štvrtej položky menu – *Service mode* a zadaním prístupového hesla a servisného kódu (v tomto poradí). Po aktivácii nie je možné využívať klasickú systémovú navigáciu až do jej ukončenia klávesou `'#'` bez nutnosti zadávania hesla či kódu. Viac informácií v kapitole 4.6.

Zóny – rozdeľujú senzory na skupiny. Každá skupina môže byť následne vyhodnocovaná rozdielnym spôsobom. Možnosť jej nastavenia je dostupná pre pohybové PIR senzory a magnetické kontakty. Aktuálne sú podporované dva typy zón:

- **Dôležitá zóna:** Programovo reprezentovaná konštantou `ZONE_IMPORTANT` s hodnotou `0`. Pokiaľ senzor patriaci do tejto zóny zaznamená narušenie, je nutné vyhlásiť poplach okamžite.
- **Odchodová zóna:** Definovaná ako `ZONE_LEAVING` s hodnotou `1` existuje pre potreby senzorov nachádzajúcich sa v priestoroch s ovládacím panelom systému a v ktorých je nutné učiniť pohyb po spustení chráneného režimu pre opustenie priestorov. Narušenie týchto senzorov je po dobu stanovenú premennou `timeToLeave` (štandardne 10 sekúnd) ignorované, čím je obyvateľom poskytnutý čas na odchod. Po uplynutí tohto času je narušenie registrované, avšak nedochádza k vyvolaniu poplachu ihneď; obyvatelia majú pred spustením signalizácie čas na vypnutie ochrany. V oboch prípadoch je na LCD displeji zobrazovaný odpočet zostávajúcich sekúnd.

Vyhodnotenie a signalizácia poplachu – je kľúčovou úlohou bezpečnostného systému. V programe sa vyhodnocovania zhosťuje funkcia s predpisom `CheckSensors`, ktorej zjednodušená implementácia je nasledovná:

```
bool CheckSensors(){
   bool violation = false;  //informacia o naruseni

   //funkcia je volana i v nudzovom rezime, kedy dochadza len ku
       kontrole poziarnych senzorov
   if(PROTECTED_MODE){
      for(int i = 0; i < 7; i++){ //kontrola kazdeho slotu PIR a
          magnetickeho kontaktu

         //pohybove senzory
         if(PIRgroup.GetPir(i)->MotionMonitor()){
            if(PIRgroup.GetPir(i)->GetZone() == ZONE_IMPORTANT){
```

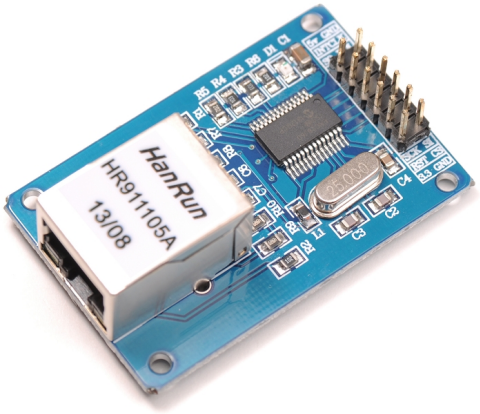
```
                instantAlarm = true; //globalny priznak, ze narusenie
                    vzniklo v dolezitej zone a je potreba spustit poplach
                    okamzite
                }
                violation = true; //narusenie
            }

            //obdobne pre magneticke kontakty
            if(MAGgroup.GetMag(i)->IsDisconnected()){
                if(MAGgroup.GetMag(i)->GetZone() == ZONE_IMPORTANT){
                    instantAlarm = true;
                }
                violation = true;
            }
        }
    }

    //poziarne senzory Fire0 a Fire1 sa kontroluju bez ohladu na rezim
        cinnosti
    if(Fire0.IsFire() || Fire1.IsFire()){
        instantAlarm = true;
        violation = true;
    }

    //navratova hodnota je true pokial vzniklo narusenie aspon na jednom
        zo senzorov
    return violation;
}
```

Pri kontrole pohybových detektorov a magnetických kontaktov sa kontroluje všetkých 7 slotov, čo znamená, že nevyužité sloty by mali byť nastavené ako neaktívne, aby nedochádzalo k vzniku falošných hlásení. Funkcia je volaná v pohotovostnom i chránenom režime z hlavnej programovej slučky.

Pokiaľ má byť vyhlásený poplach (ihneď alebo po uplynutí času potrebného na príchod), je tak učinené akusticky i opticky. V tejto práci sú z finančných i prezentačných dôvodov využité ľahko dostupné komponenty – LED dióda pre optickú a piezoelektrický bzučiak pre akustickú signalizáciu. Obsluha diódy je implementovaná v už spomínanej knižnici `LED` a bzučiak v súboroch `Buzzer.cpp` a `Buzzer.h`. Nakoľko je využitý aktívny modul bzučiaku, stačí na dátový vstup priviesť úroveň logickej nuly a spustí sa rovnomerné vydávanie zvuku. Obdobným spôsobom ako blikanie LED diódy, je implementovaný i striedavý tón, ktorý je podobný zvuku bežných alarmov.

4.5 Sieťové pripojenie

Pre hardvérovú realizáciu sieťového pripojenia je použitý modul 4.5. Ten komunikuje s riadiacou jednotkou pomocou SPI zbernice. Arduino Mega2560 má pre SPI vymedzené nasledujúce piny: `50` (MISO), `51` (MOSI), `52` (SCK), `53` (SS), do ktorých je modul zapojený. Proces vytvorenia serveru a obsluha pripojených klientov je súčasťou voľne dostupnej knižnice `UIPEthernet`, ktorá je založená na štandardnej Arduino knižnici `Ethernet` a dostupná z [21]. Ponúka však len základné funkcie potrebné pre prepojenie a všeobecnú komunikáciu



Obr. 4.5: Použitý ethernetový modul [19].

dvoch sieťových zariadení, preto bolo nutné vytvoriť rozšírenie implementované v knižnici `EthernetPlus`. To okrem iného zahrňuje odosielanie štandardnej http hlavičky a emailu, dopĺňanie a posielanie webovej stránky, konfiguračné rozhranie pre servisný režim, načítanie vlastností z EEPROM či jednoduché parsovanie dotazu GET.

V inicializačnom procese dochádza k vytvoreniu serveru s IP adresou nastavenou v servisnom režime. Číslo portu je štandardne `58000` a v aktuálnej verzii ho nie je možné meniť inak než zmenou konštanty v programe. Pre pripojenie na internet treba nastaviť IP adresu z rozsahu adries prideľovaných smerovačom, ku ktorému je zariadenie pripojené, ktorá zároveň nekoliduje s inými sieťovými zariadeniami. Následne je nutné nakonfigurovať presmerovanie použitého portu (58000) pre danú IP adresu tak, aby boli všetky http požiadavky presmerované na bezpečnostný systém. Proces nastavenia sa líši pre jednotlivé typy smerovačov.

Email – je odosielaný pri každom spustení poplachu. Informuje tak užívateľa o tom, že niečo nie je v poriadku. Prenos je realizovaný pomocou `SMTP` protokolu, z čoho vyplýva, že email je možné posielať len na poštové servery, ktoré tento protokol podporujú. Predmet, mailový server, prijímateľ či odosielateľ a iné parametre sú nastavované podľa požiadaviek zákazníka v servisnom režime. Názorný príklad formátu správy v tvare, ktorý je odosielaný funkciou `SendEmail` a spĺňuje pravidlá SMTP protokolu je nasledujúci:

```
HELO
MAIL FROM: <email@email.sk>
RCPT TO: <email@email.sk>
DATA
From: Me <email@email.sk>
To: You Example <email@email.sk>
Subject: EZS - narusenie

Toto je text emailu.
.
QUIT
```

Webová stránka – je uložená na SD karte v súbore `index.htm` (viac o SD karte v kapitole 4.7). Jednoduchým, no prehľadným prevedením poskytuje všetky dôležité informácie o objekte. Klientovi je odoslaná stránka a následne skript v jazyku *JavaScript*, ktorý upraví hodnoty jednotlivých položiek podľa údajov získaných so senzorov. Webová stránka je zobrazená akémukoľvek klientovi, ktorý pozná IP adresu a port serveru bežiaceho v systéme. Zabezpečenie sa však dá docieliť napríklad nastavením IP filtrov na smerovači.

4.6 Servisný režim

Je špeciálnym režimom činnosti, určeným pre správu systému. Bežným užívateľom nie je dostupný, nakoľko vstup je podmienený zadaním servisného kódu, ktorý poznajú len servisný pracovníci, školení na pokročilú manipuláciu so systémom. Toto opatrenie zamedzuje zásahom do systému, ktoré by viedli k jeho nefunkčnosti a následnej neznalosti nápravy problému. Servisný kód pevne daný a nemenný, môže byť špecifický pre každé zariadenie alebo rovnaký pre celú skupinu produktov. Z bezpečnostných dôvodov je vyžadovaná dvojitá kontrola prístupových údajov – zadanie prístupového hesla a následne až servisného kódu pre prípad, že by došlo k jeho vyzradeniu. Po aktivácii dochádza k zastaveniu monitorovania objektu.

Režim poskytuje možnosť konfigurácie systému cez počítač prostredníctvom sériového portu Arduina. Komunikácia prebieha formou príkaz – odpoveď a k odosielaniu príkazov sa dá použiť napríklad aplikácia *PuTTy* alebo sériový monitor, ktorý je súčasťou prostredia Atmel Studio 7. Zadaním nejakého príkazu a prípadnej hodnoty sa spustí príslušná udalosť, ktorá buď uloží hodnotu do pamäte EEPROM alebo odošle požadovanú informáciu naspäť užívateľovi.

Príkaz	**Parametre**	**Popis**
Xn	**n** - číslo knižnice	Nasledujúce príkazy budú interpretované zvolenou knižnicou.
Hlavné konfiguračné rozhranie EZS (X1)		
H	**-**	Vypíše všetky podporované príkazy.
Lx	**x** - čas v sekundách	Nastaví odchodový čas na zvolenú hodnotu.
Pax	**a** - 'A' pre aktiváciu, 'Z' pre zóny; **x** - postupnosť 7 čísel, kde poradie reprezentuje 0.-7. pohybový senzor a hodnota nastavenie vlastnosti	De/Aktivuje pohybové senzory (0/1) alebo priradí senzoru zónu (0-n).
Sieťové konfiguračné rozhranie (X2)		
H	**-**	Vypíše všetky podporované príkazy.
F<s>	**s** - emailová adresa odosielateľa	Nastaví odosielateľa emailu.
Ms	**s** - adresa emailového serveru	Nastaví emailový server.
R	**-**	Reštart systému.

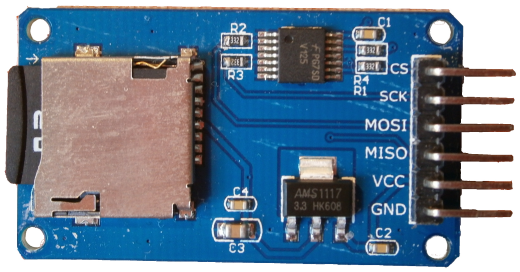
Tabuľka 4.7: Vybrané príkazy konfiguračného rozhrania servisného režimu.

Implementácia rozhrania spravujúceho udalosti je v súboroch `DoEvent.cpp` `DoEvent.h`. Základnou myšlienkou je možnosť zvolenia knižnice (modulu, celku), ktorú je možné následne nastavovať. V každej knižnici, ktorú je možné zapojiť do servisného režimu, musí existovať funkcia typu `void f(int event, String data, int hodnota)`. `Event` udáva číslo udalosti, ktorá sa má vykonať a zvyšné dva parametre dáta, s ktorými je možné manipulovať. Táto funkcia je následne použitá ako parameter funkcie `InitDoEvent`, ktorá s prípadnými inými ukazateľmi inicializuje servisné rozhranie. Užívateľ je pri spustení servisného módu povinný zvoliť, s ktorou knižnicou chce pracovať príkazom `Xn`, kde `n` je číslo knižnice. Pri odoslaní príkazu dochádza k jeho rozdeleniu na jednotlivé významové časti – prvý znak určuje identifikátor príkazu a zvyšok sú dáta. Na základe zvoleného modulu je volaná príslušná obslužná funkcia, ktorej je predaný identifikátor príkazu, reťazec dát a ich číselná hodnota v prípade platnej konverzie. Funkcia na základe prijatých dát vykoná príslušnú rutinu. Zmeny vlastností sa prejavia až po reštarte systému. Názorná ukážka formátu vybraných príkazov a ich popis je v tabuľke 4.7.

Okrem spomenutých je dostupné i nastavovanie magnetických kontaktov obdobne ako pohybových, infračervených hlásičov plameňa, dátumu, zmazanie obsahu EEPROM, obnovenie počiatočných sieťových nastavení či výpis nastavenia všetkých senzorov.

4.7 Archivácia

Každá kľúčová činnosť vykonaná v systéme je zaznamenávaná. Údaje je možné využiť pri následnej analýze narušenia, či môžu poslúžiť servisnému pracovníkovi ako podklad pri riešení problémov. K ukladaniu bola zvolená micro SD karta, ktorá je plne podporovaná na väčšine bežne dostupných zariadení. Užívateľ tak môže priebežne sledovať jej obsah bez potreby špeciálneho softvéru. Na prácu s SD kartou bol zvolený modul určený pre platformu Arduino zobrazený na obrázku 4.6.



Obr. 4.6: Zvolený modul SD karty.

Použiť je možné ktorúkoľvek micro SD kartu formátovanú na *FAT16* alebo *FAT32* [11], doporučuje sa však *FAT16*. Z toho vyplýva, že názov súboru nesmie byť dlhší ako 8 znakov a prípona dlhšia ako 3 znaky. Ku komunikácii je využitá zbernica SPI. Zapojenie je podobné ako pri ethernetovom module (viď 4.5) s tým, že k výberu zariadenia slúži digitálny pin s číslom 16.

Program pre inicializáciu karty, zápis a čítanie je dostupný v štandardnej knižnici `SD`. Za kľúčové udalosti, pri ktorých dochádza k archivácii sú považované:

1. spustenie systému,
2. zapnutie zabezpečenia,
3. okamžité spustenie poplachu,
4. oneskorené spustenie poplachu,
5. ukončenie poplachu zadaním hesla,
6. zahájenie servisného režimu,
7. opustenie servisného režimu,

Vo všetkých prípadoch je ukladaná rovnaká informácia, ktorá obsahuje identifikátor udalosti, dátum a čas jej vzniku a aktuálny stav senzorov. V tabuľke 4.8 je vysvetlený význam jednotlivých položiek vzorového záznamu.

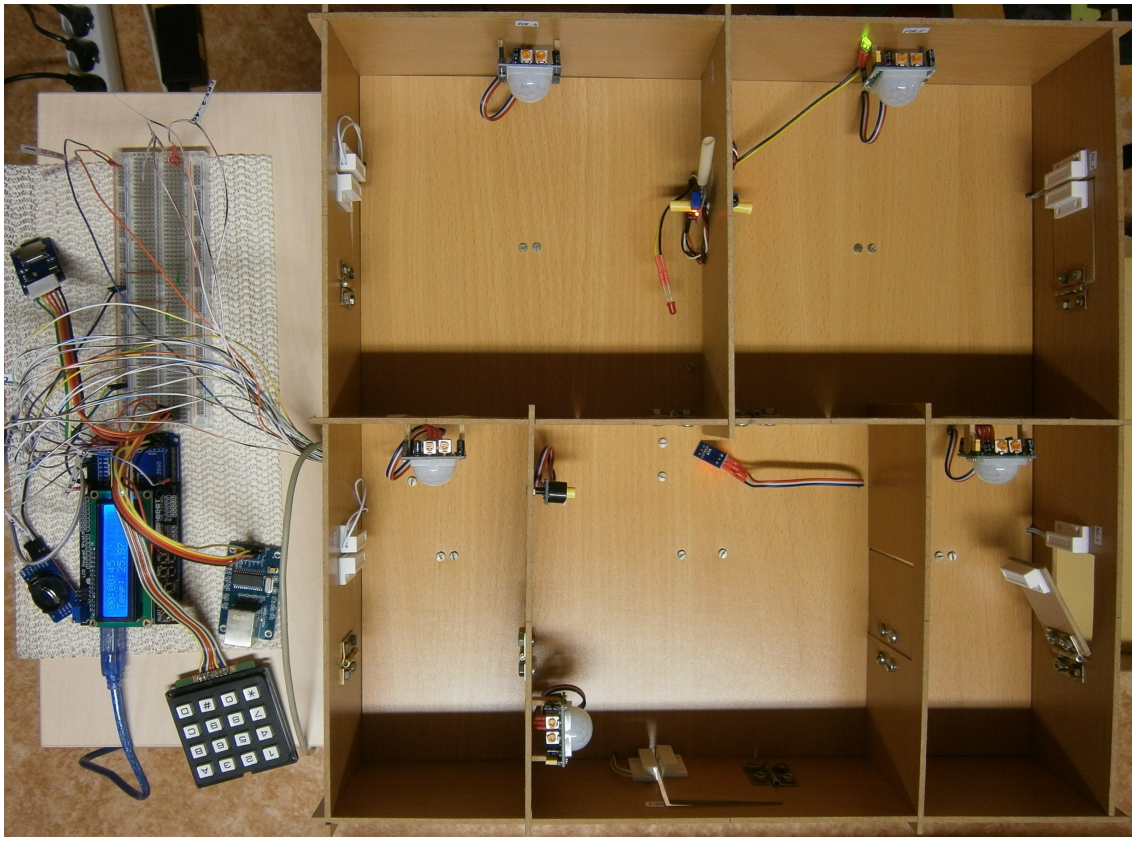
Položky záznamu	**Popis**
SERVICE_STARTED	Názov udalosti, zahájenie servisného režimu.
22/04/2017	Dátum vzniku udalosti vo formáte dd/mm/yy.
01:46:09	Čas vzniku udalosti vo formáte hh:mm:ss.
PIR0011	Stav senzoru PIR s číslom – 0, narušenie nezaznamenané – 0, senzor aktivovaný – 1 a patrí do zóny – 1.
Magnetic0000	Stav magnetického senzoru s číslom – 0, narušenie nezaznamenané – 0, senzor neaktivovaný – 0 a patrí do zóny – 0.
IR0_752_1	Stav infračerveného snímaču číslo – 0, hodnota analógového výstupu – 752, senzor aktivovaný – 1.
Therm0_24.37	Stav teplotného senzoru č. – 0, nameraná teplota – 24,37 °C.

Tabuľka 4.8: Popis položiek záznamu.

CSV (z anglického *Comma-separated values*) je jednoduchý súborový formát vo forme čistého textu, ktorý sa využíva na ukladanie dát tabuliek. Súbor v tomto formáte je tvorený niekoľkými riadkami, kde v každom riadku je ľubovoľný počet prvkov oddelených iným znakom, zvyčajne čiarkou [24]. Formát je využitý pre archiváciu záznamov z dôvodu širokej podpory rôznymi tabuľkovými editormi. Je tak možné v prípade potreby s dátami ďalej pohodlne pracovať. Názov súboru s uloženými záznamami je `history.csv`.

4.8 Testovanie

Pre účely testovania a prezentácie výsledného produktu bol vytvorený 3D model zabezpečovaného objektu, do ktorého boli následne rozmiestnené jednotlivé senzory podľa pravidiel uvedených v kapitole 3.2. Na fotke 4.7 je zachytený kompletne zapojený zabezpečovací systém inštalovaný do modelu objektu. Testovanie prebiehalo od začiatku vývoja, čím bola



Obr. 4.7: Výsledná realizácia navrhnutého EZS.

priebežne overovaná činnosť jednotlivých komponentov ako z pohľadu hardvéru, tak i vytvoreného softvéru. Vďaka výsledkom testovania bolo možné vhodne kalibrovať senzory tak, aby poskytovali čo najlepšie výsledky.

Magnetické kontatky – boli testované priamo na 3D modely objektu, nakoľko sa ich činnosť v tejto mierke neodlišuje od činnosti v reálnych podmienkach. Pôvodne mali kontakty pri rozpojení indikovať úroveň logickej nuly. Testovaním však bolo zistené, že po ich rozpojení sa na vodičoch zachytával okolitý šum, čím nedošlo k odhaleniu narušenia. Vyriešené použitím pull-up rezistoru a kontrolou logickej jednotky v prípade narušenia.

Pohybové senzory – neboli pri testovaní súčasťou modelu. V prvom rade bol testovaný dosah. V tabuľke 4.9 sú výsledky testovania pre maximálne nastavenú citlivosť. Pre náhodný senzor bol uskutočnený pohyb v určitej vzdialenosti. Meraná bola vzdialenosť, ktorú osoba prešla kým bol zaznamenaný jej pohyb (pri vzdialenosti dlhšej ako 3 metre bol test vyhodnotení ako neúspešný). Pohyb mohol byť buď kolmo alebo rovnobežne s plochou snímacej šošovky. Každý typ testu bol vykonaný štyrikrát, pričom bol označený ako úspešný, pokiaľ bol zaznamenaný pohyb. Neboli individuálne testované všetky senzory, no predpokladá sa ich obdobná činnosť.

Hlásiče plameňa – je možné analyzovať na základe ich digitálneho alebo analógového výstupu. Digitálny výstup je nastavený na hodnotu 1 podľa citlivosti nastavovanej

Vzdialenosť PIR	Pohyb	Max. prekonaná vzdialenosť	Úspešnosť
30 cm	Rovnobežne	20 cm	4/4
1 m	Rovnobežne	30 cm	4/4
4 m	Rovnobežne	60 cm	4/4
4 m	Kolmo	2 m	4/4
7 m	Rovnobežne	1,8 m	4/4
7 m	Kolmo	2,8 m (2-krát nad 3 m)	2/4

Tabuľka 4.9: Výsledky testovania pohybového senzoru.

pomocou potenciometru. Toto mechanické ladenie je však nepresné a nebolo možné ľahko nastaviť všetky senzory na rovnakú hodnotu. Zvolený bol preto analógový výstup. V tabuľke 4.10 sú vypísané jednotlivé situácie, ktoré senzor zaznamenáva a príslušná poskytovaná analógová hodnota. Z nameraných hodnôt vyplýva, že prah

Situácia	Vzdialenosť	Hodnota
Noc (miestnosť bez okna)	-	1018-1023
Zamračený deň	-	400-800
Slnečný deň	-	35-400
Plameň sviečky	15 cm	23-28
Plameň sviečky	30 cm	32-40
Horiaci list papiera	50 cm	25-40

Tabuľka 4.10: Výsledky testovania IR senzoru.

reakcie na požiar by sa mal pohybovať v hodnotách od 20-40. Pri zvolení hodnoty väčšej ako 30 je nutné čidlo umiestniť čo najďalej od okien. Infračervené senzory sú veľmi citlivé na slnečné svetlo, preto je vhodné ich zapustiť do obalu, z ktorého by snímač nevytŕčal, no mal by dostatočný výhľad. Strop sa javí ako najlepšie miesto na umiestnenie – malá pravdepodobnosť priameho zásahu slnečnými lúčmi a dostatočný výhľad. Avšak spoľahlivosť a dosah použitých senzorov nie je ideálny a vhodným miestom na umiestnenie by tak bola skrinka alebo odsávanie nad sporákom.

Funkčnosť systému – bola testovaná priebežne. Po doplnení novej vlastnosti bola kontrolovaná nie len daná vlastnosť, ale znovu všetky funkcie systému, ktoré by mohli byť ovplyvnené. Hlavné testovanie pozostávalo zo simulácií narušení v jednotlivých režimoch činnosti.

- **Núdzový režim:** V núdzovom režime bolo simulované narušenie postupne oboch požiarnych senzorov (plameňom zapaľovača z krátkej vzdialenosti). Po narušení sa ihneď spustil poplach a došlo k výzve k jeho ukončeniu zadaním hesla, čo sa podarilo. Tiež bolo testované či je úspešne ignorované narušenie od ostatných senzorov.
- **Chránený režim:** Zopakovalo sa testovanie detektorov plameňa – úspešne a zároveň bolo postupne po jednom vyvolávané narušenie každého senzoru. Po spustení poplachu bol poplach vypnutý, zabezpečenie znovu zapnuté a pokračovalo sa na ďalší senzor. Následne s využitím servisného režimu došlo k vypnutiu náhodných senzorov a opätovná skúška, či dané senzory na narušenie naozaj ne-

reagujú. Otestované boli aj zóny – všetky senzory mali nastavenú okamžitú zónu a poplach sa spustil ihneď (naopak u odchodovej zóny).

- **Servisný režim:** V prvom rade bolo kontrolované, či vyžaduje na vstup naozaj obe heslá a či je možné zadávanie kedykoľvek opustiť. Po vstupe do režimu nie je možné aby ktorýkoľvek senzor spustil poplach.

Vykonané testy nevykazovali chybné správanie avšak neboli testované všetky možné kombinácie. Bezpečnostným problémom je reštart systému pri výpadku napájania, čím dôjde k vypnutiu ochrany objektu (možné riešiť záložným zdrojom). Prerušenie vodičov senzorov nie je žiadnym spoľahlivým spôsobom kontrolované (ústredňa 4. kategórie). Šanca spustenia poplachu je v tomto prípade náhodná a záleží na množstve zachyteného šumu na ponechaných vodičoch. Maximálna zaznamenaná doba behu systému bola 40 hodín, po tejto dobe bolo potrebné systém vypnúť z dôvodu nahrávania novej verzie softvéru.

Užívateľské testovanie: Vzhľadom na objemnosť, závislosť na napájaní a obmedzenú kvantitu sa užívateľského testovania zúčastnilo 7 osôb rôznych vekových kategórií. Približne v polovici (3) prípadov bol prekážkou anglický jazyk rozhrania. Po preklade však neboli zaznamenané problémy s intuitívnosťou menu a všetky testovacie subjekty dokázali spustiť a ukončiť ochranu či nastaviť hodiny. Webová stránka sa nestretla so žiadnou pripomienkou k jej vlastnostiam a funkčnosť bola testovaná na prehliadačoch *Mozilla Firefox 53* a *Chrome v. 58*. Testy preukázali, že k webovej stránke môže pristupovať ktokoľvek, kto pozná IP adresu.

Servisný režim boli pomocou zoznamu príkazov schopné ovládať len dve osoby s pokročilými znalosťami informačných technológií. Po dôkladnom zaškolení a vedení ostatných osôb, pretrvali dve, ktoré si stále neboli isté tým čo robia. Kópia originálneho dotazníku položeného testovacím subjektom a grafické zobrazenie výsledkov je zobrazené v prílohe A.1. Lepšia kvalita je dostupná na CD v adresári *Prílohy* v súboroch *dotaznik_otazky.pdf* a *dotaznik_odpovede.pdf*.

4.9 Možnosti ďalšieho vývoja

Každý produkt by sa mal neustále vyvíjať a prispôsobovať trhu a okolitým podmienkam. Vždy je čo zlepšovať a dobré meno si výrobok môže zachovať jedine vtedy, pokiaľ komunita vidí, že sa na ňom pracuje. Kapitola popisuje návrhy na zlepšenie systému či jeho jednotlivých častí, ktoré nemohli byť z finančných či iných dôvodov uskutočnené alebo by sa hodili pre systém zameraný na ochranu iných objektov a vyšších úrovní zabezpečenia.

Napájanie – by bolo možné zálohovať z batérie, čím by sa odstránilo riziko vypnutia ochrany v dôsledku výpadku elektrického prúdu v objekte.

Ochranný kryt – by mohol byť zhotovený z pevného kovového materiálu a prístup by bol zabezpečený špeciálnym kľúčom. Tiež by sa dnu do krytu mohli inštalovať senzory citlivé na svetlo pre zaznamenanie svetla pri násilnom vniknutí a spustenie poplachu. Ich monitorovanie by pravdepodobne mohlo byť súčasťou núdzového režimu.

Precíznejšie senzory – sú otázkou ceny. Najväčšie zlepšenie by však na aktuálnom systéme spôsobila výmena detektorov plameňa za ionizačný hlásič dymu alebo multisenzorový s plynovou detekciou. Program je aktuálne pripravený s malými úpravami podporovať i digitálne požiarne senzory.

Webová stránka – by mohla podporovať prístup chránený heslom, čo by však vyžadovalo omnoho rozsiahlejšiu programovú podporu. Zároveň by sa mohol upraviť vzhľad a prípadne doplniť možnosť konfigurácie prostredníctvom webového rozhrania.

Rozšírenie počtu senzorov – v malom rozsahu pre digitálne piny, v o niečo väčšom pre analógové. Doplnenie viacerých pohybových detektorov a magnetických kontaktov alebo i iných, ktoré pracujú podobným spôsobom. Knižnicu pre magnetické senzory by bolo možné využiť napríklad pre mechanické otrasové detektory.

Zavedenie kontrolných slučiek – by vyžadovalo patričné senzory, ktoré touto slučkou disponujú alebo by bolo potrebné vykonať mechanické úpravy na aktuálnych. Systém by tak dokázal zaznamenať prerušenie vedenia jednotlivých komponentov, čím by sa zvýšila celková úroveň zabezpečenia.

Testovací režim – by mohol byť dostupný priamo z menu. Po jeho výbere by bol užívateľ vyzvaný k postupnému vyvolaniu narušenia na jednotlivých senzoroch. Po úspešnom zaznamenaní všetkých narušení a kontroly signalizačných zariadení, by bol test označený za úspešný. Týmto spôsobom by bolo možné pravidelne kontrolovať funkčnosť prvkov a včas tak odhaliť chybu.

Vylepšení je možné nájsť určite ešte nespočetné množstvo. Navrhnutý systém je však pre jednoduché zabezpečenie dostačujúci a je vhodný na demonštráciu funkčnosti zabezpečovacích systémov.

Kapitola 5

Záver

Cieľom tejto bakalárskej práce bolo navrhnúť a vytvoriť vlastný zabezpečovací systém postavený na platforme Arduino, ktorý okrem zabezpečenia a signalizácie poplachu poskytuje možnosti jeho jednoduchého ovládania, konfigurácie a viac-užívateľského prístupu k informáciám.

Na začiatku práce boli popísané všeobecné mechanizmy činnosti bezpečnostných systémov a poskytnutý prehľad dostupných monitorovacích prvkov. Následne bola podrobne popísaná analýza fiktívneho rodinného domu, ktorá tvorí nutný základ pre tvorbu kvalitného bezpečnostného systému. Pri výbere senzorov bol braný ohľad na proporcie samotného objektu i na vlastnosti senzorov. Výsledkom bolo správne pokrytie senzormi s ohľadom na zdravie a bezpečnosť obyvateľov.

Návrh samotného systému prebiehal s ohľadom na jednoduchosť inštalácie, možnosti viac-užívateľského ovládania, dostupnosť informácii a konfiguráciu vlastností systému. Ústredňa je tvorená platformou Arduino Atmega 2560, na ktorú sú napojené všetky súčasti systému. Hlavnými ovládacími prvkami sú LCD displej so zabudovanými tlačidlami pre zobrazovanie a pohyb v užívateľskom menu a maticová klávesnica, slúžiaca primárne na zadávanie prístupových hesiel. Všetky dôležité udalosti sú zaznamenávané a ukladané na SD kartu spolu s informáciami o stave senzorov pre potreby neskoršej analýzy. S využitím RTC modulu s batériou si systém udržiava čas a dátum i po odpojení z napájania. Súčasťou je aj teplomer. Poplach je signalizovaný akusticky i opticky. Užívateľ môže aktuálny stav objektu sledovať prostredníctvom jednoduchej webovej stránky alebo byť o poplachu informovaný emailom.

Napriek tomu, že systém bol prezentovaný na konkrétnom objekte s konkrétnym počtom senzorov, je realizovaný tak, že je možné počet detektorov ľubovoľne meniť v stanovenom rozsahu. Systém je tak použiteľný i pre iné objekty podobných rozmerov s rovnakou úrovňou zabezpečenia. Nastavenie vlastností systému ako povolovanie nových senzorov, priraďovanie zón, nastavenie oneskoreného poplachu či sieťové nastavenia, je možné vykonávať pomocou počítača cez sériové konfiguračné rozhranie odosielaním konkrétnych príkazov. Inštalácia systému so zmenenou štruktúrou je tak otázka pár minút.

Testovanie prebiehalo súčasne s vývojom. Nakoniec bolo vykonané v priestoroch reálnych rozmerov a tiež na zhotovenom 3D modely objektu. Testované boli vlastnosti jednotlivých senzorov a možnosti ovplyvnenia ich činnosti. V obmedzenom počte (7 osôb) bolo vykonané i užívateľské testovanie ovládateľnosti a následné dotazovanie ich spokojnosti, viď prílohu A.1 (v lepšej kvalite na CD). Elementárna funkčnosť je zdokumentovaná formou krátkych videí taktiež priložených na CD.

Za vlastný prínos by bolo možné označiť vytvorenie návrhu systému na základe nadobudnutých znalostí problematiky, ktorý pozostáva z niekoľkých rôznorodých komponentov a prepojenie jednotlivých prvkov v jeden funkčný výsledný produkt, poskytujúci všetky vyššie spomenuté možnosti. Problémy zaznamenané v priebehu vývoja alebo pri testovaní boli buď ihneď vyriešené alebo sa stali predmetom budúcich rozšírení a vylepšení ako napríklad fyzická ochrana ústredne, záložné napájanie, kvalitnejšie senzory, úprava systému pre podporu bezdrôtových senzorov či len jednoduchá zmena vzhľadu webovej stránky alebo pridanie testovacieho režimu.

Literatúra

[1] Alex: *The Arduino Ecosystem*. [Online], [rev. 2014-08-20], [cit. 2017-04-27].
URL http://learnelectronicsblog.com/the-arduino-ecosystem/

[2] Arduino: *Arduino - Home*. 2017, [Online], [cit. 2017-04-27].
URL https://www.arduino.cc/

[3] Arduino: *Arduino MEGA 2560 & Genuino MEGA 2560*. 2017, [Online], [cit. 2017-04-27].
URL https://www.arduino.cc/en/Main/arduinoBoardMega2560

[4] Bureš, M.; Borovec, J.: *Zařízení elektrické zabezpečovací signalizace*. [Online], [rev. 2003-04-23], [cit. 2017-01-11].
URL http://elektrika.cz/data/clanky/nozs030423

[5] Burton, M.; Newsome, T.; Barros, G.; aj.: *DallasTemperature*. [Online], [cit. 2017-04-29].
URL https://github.com/milesburton/Arduino-Temperature-Control-Library

[6] Christensen, J.: *DS3232RTC*. [Online], [cit. 2017-04-30].
URL https://github.com/JChristensen/DS3232RTC

[7] DFRobot: *Arduino LCD KeyPad Shield (SKU: DFR0009)*. [Online], [rev. 2017-03-28], [cit. 2017-05-01].
URL
https://www.dfrobot.com/wiki/index.php/Arduino_LCD_KeyPad_Shield_(SKU:_DFR0009)

[8] Hloušek, Z.: *EZS zabezpečovací systémy*. [Online], [cit. 2017-01-21].
URL http://www.zabezpeceni-domu.cz/

[9] Hofreiter, L.; Veľas, A.; Kaluža, F.: *Systémy prenosu informácií v bezpečnostných aplikáciách*. Žilinská univerzita v Žiline, první vydání, 2008, [Online], [cit. 2017-01-20].
URL http://fsi.uniza.sk/kbm/wp-content/uploads/2013/12/Velas_SPI.pdf

[10] Hofreiter, L.; Veľas, A.; Kaluža, F.: *Elektronické zabezpečovacie systémy*. Žilinská univerzita v Žiline, první vydání, 2010, [Online], [cit. 2017-03-20].
URL http://fsi.uniza.sk/kbm/wp-content/uploads/2013/12/Velas_EZS.pdf

[11] Ježek, A.: *13. díl - Arduino a SD karta*. [Online], [cit. 2017-05-01].
URL https://www.itnetwork.cz/hardware-pc/arduino/arduino-sd-karta

[12] Křeček, S.: *Příručka zabezpečovací techniky*. S.l.: s.n., 2006, ISBN 80-902938-2-4, 313 s.

[13] Komínek, P.: *Návrh a analýza systémů pokročilého zabezpečení a střežení objektů a prostor*. Diplomová práce, VUT FIT v Brně, Brno, 2011.

[14] Margolis, M.: *Time*. [Online], [cit. 2017-05-11].
URL https://www.pjrc.com/teensy/td_libs_Time.html

[15] Marlin P. Jones & Assoc. Inc.: *HC-SR501 PIR MOTION DETECTOR*. [Online], [cit. 2017-04-29].
URL https://www.mpja.com/download/31227sc.pdf

[16] Martinek, R.: *Senzory v průmyslové praxi*. Praha: BEN - technická literatúra, 2004, ISBN 978-80-7300-114-4, 199 s.

[17] Maxim Integrated Products, Inc. : *Extremely Accurate I2C-Integrated RTC/TCXO/Crystal*. 2015, [Online], [cit. 2017-04-29].
URL https://datasheets.maximintegrated.com/en/ds/DS3231.pdf

[18] Maxim Integrated Products, Inc. : *Programmable Resolution 1-Wire Digital Thermometer*. 2015, [Online], [cit. 2017-04-29].
URL https://datasheets.maximintegrated.com/en/ds/DS18B20.pdf

[19] Santy: *Mini Ethernet modul HR911105A pro Arduino*. [Online], [cit. 2017-05-07].
URL http://www.santy.cz/moduly-c22/ethernet-arduino-mega-uno-2560-1280-328-hr911105a-online-sd-enc28j60-mini-i146/

[20] Stoffregen, P.; Studt, J.; Pollard, T.; aj.: *OneWire*. [Online], [cit. 2017-04-29].
URL https://www.pjrc.com/teensy/td_libs_OneWire.html

[21] Truchsess, N.: *UIPEthernet*. [Online], [cit. 2017-05-04].
URL https://github.com/ntruchsess/arduino_uip

[22] Visual Micro: *Setup - Arduino IDE for Visual Studio and Atmel Studio*. [Online], [cit. 2017-05-01].
URL http://www.visualmicro.com/page/User-Guide.aspx?doc=First-steps.html

[23] Voda Z.; Tým HW Kitchen: *Průvodce světem Arduina*. Bučovice: Nakladatelství Martin Stříž, 2015, ISBN 978-80-87106-90-7, 240 s.

[24] Wikipedia: *Comma-separated values*. [Online], [rev. 2015-06-19], [cit. 2017-05-2].
URL https://sk.wikipedia.org/wiki/Comma-separated_values

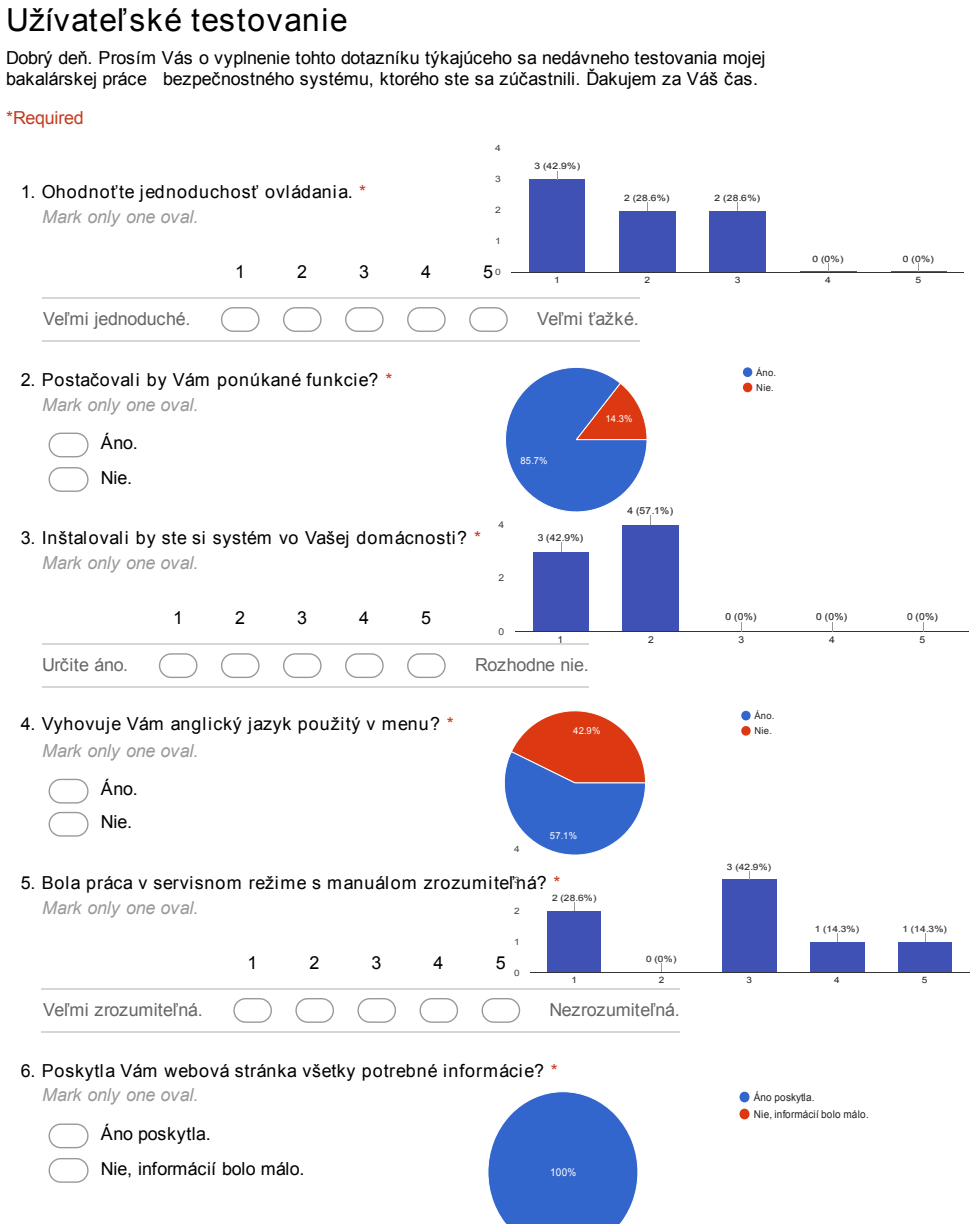
[25] Wikipedia: *Elektronická zabezpečovací signalizace*. [Online], [rev. 2016-08-03], [cit. 2017-01-11].
URL https://cs.wikipedia.org/wiki/Elektronick%C3%A1_zabezpe%C4%8Dovac%C3%AD_signalizace

[26] Zahrádka, J.: *Začínáme s EZS*. VARIANT plus s.r.o., 2005, [Online], [cit. 2017-01-15].
URL https://www.stasanet.cz/out/media/Zaciname%20s%20EZS.pdf

Prílohy

Príloha A

Dotazník užívateľského testovania



Užívateľské testovanie

Dobrý deň. Prosím Vás o vyplnenie tohto dotazníku týkajúceho sa nedávneho testovania mojej bakalárskej práce bezpečnostného systému, ktorého ste sa zúčastnili. Ďakujem za Váš čas.

*Required

1. Ohodnoťte jednoduchosť ovládania. *
Mark only one oval.

1 2 3 4 5

Veľmi jednoduché. Veľmi ťažké.

2. Postačovali by Vám ponúkané funkcie? *
Mark only one oval.

Áno.
Nie.

3. Inštalovali by ste si systém vo Vašej domácnosti? *
Mark only one oval.

1 2 3 4 5

Určite áno. Rozhodne nie.

4. Vyhovuje Vám anglický jazyk použitý v menu? *
Mark only one oval.

Áno.
Nie.

5. Bola práca v servisnom režime s manuálom zrozumiteľná? *
Mark only one oval.

1 2 3 4 5

Veľmi zrozumiteľná. Nezrozumiteľná.

6. Poskytla Vám webová stránka všetky potrebné informácie? *
Mark only one oval.

Áno poskytla.
Nie, informácií bolo málo.

Obr. A.1: Ukážka otázok a odpovedí užívateľského testovania