Jihočeská univerzita v Českých Budějovicích

Přírodovědecká fakulta

Zabezpečení objektů na platformě Arduino

Bakalářská práce

Václav Čaloun

Vedoucí práce: PhDr. Milan Novák, Ph.D.

České Budějovice 2016

Bibliografické údaje

Čaloun V., 2016: Zabezpečení objektů na platformě Arduino.
[BuildingsecuritybasedplatformArduino Bc. Thesis, in Czech.]
–51p., Faculty of Science, The University of South Bohemia, České Budějovice,
Czech Republic.

Anotace

Bakalářská práce se zabývá navržením a sestrojením zabezpečovacího systému pro ochranu majetku za použití open-source hardware. V teoretické části se zaměřuje na analýzu již hotových řešení.

V praktické části je navržen a popsán zabezpečovací systém na platformě Arduino. Systém je otestován a jsou vyhodnoceny chyby.

Klíčová slova: Zabezpečovací systémy, Arduino, senzory.

Annotation

The bachelor thesis deals with creating security system, for building using open-source hardware. Theoretical part of work analyze existing solution.

In practical part is designed and described security system based on Arduino platform. System is tested and errors is evaluated.

Key words: Security systems, Arduino, sensors

Prohlašuji, že svoji bakalářskou práci jsem vypracoval samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě fakultou elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Českých Budějovicích dne Václav Čaloun

Poděkování

Děkuji panu Radimu Sejkovi a Bc. Ondřeji Klugeroviza zapůjčení některých komponent. Na závěr bych chtěl poděkovat svým rodičům za financování zbylých komponent použitých na tuto práci.

Obsah

Úvod

Předmětem této bakalářské práce je návrh elektronického zabezpečovacího systému na platformě Arduino. Zabezpečení svého majetku je odpradávna problematikou, kterou se lidstvo zabývá. Z počátku se jednalo pouze o mechanické zabezpečovací prvky. S rozvojem výpočetní techniky se vyvinuly elektronické zabezpečovací systémy. V současné době se k zabezpečení objektu volí mechanické nebo elektronické zabezpečovací prvky. Nejlepší je samozřejmě kombinace obou těchto typů. Na trhu je velké množství komerčních produktů, které jsou nabízeny zákazníkům již hotové a připravené. Je tedy otázkou, zda existuje levnější řešení, které pokryje funkcionality řešení komerčních. Takovým zástupcem by mohla být technologie ARDUINO.

Tato technologie je založena na mikrokontrolerechATmega od firmy Atmel, umožňuje uživateli připojení množství příslušenství ke vstupně-výstupním pinům. Díky použití OpenHardware existuje velká komunita lidí, která sdílí své nápady a zdrojové kódy. Základní myšlenkou této práce je za pomoci této technologie navrhnout a sestrojit zabezpečovací systém, který by přijímal data z jednotlivých senzorů a na jejich základě adekvátně reagoval na možná rizika.

1 Cíle práce

Cílem práce je analyzovat současné způsoby zabezpečení objektů. V této analýze budou zohledněna rizika, která mohou být jedním z faktorů pro výběr zabezpečovacího zařízení. Na základě průzkumu trhu bude vytvořen návrh zabezpečovacího systému na platformě Arduino. A podle něj bude realizován zabezpečovací systém, který by měl ochránit objekt před předem zvolenými riziky.

Cíle postupu práce lze rozdělit na dílčí cíle:

1. Jako první bude provedena analýza současných řešení, která se používají k zabezpečení objektů proti různým rizikům. Na jejím základě budou vybráni nejvlivnější výrobci na trhu na základě průzkumu trhu.
2. Výsledkem průzkumu bude srovnávací tabulka, která by měla ukázat, jak jednotlivá rizika eliminují a s jakým zařízením.
3. Na základě rozkrytí funkcionalit komerčních systémů bude proveden návrh a konstrukce vlastního zabezpečovacího zařízení na platformě Arduino. Při návrhu tohoto zařízení bude zohledněna předchozí analýza současných trendů v oblasti zabezpečení. Tato analýza by měla odhalit nedostatky a nevýhody stávajících řešení. Na jejím základě bude dle vlastního návrhu sestrojen vlastní zabezpečovací systém založený na platformě Arduino. Tento systém se pokusí odstranit všechny nedostatky a zápory komerčně dodávaných systémů.
4. Následně bude tento systém otestován v praxi a budou zjištěny případné nedostatky a chyby. Pokud budou zjištěny výraznější nedostatky, bude popsáno, jakým způsobem tyto chyby odstranit.

2 Úvod do problematiky

2.1 Elektronický zabezpečovací systém

Posláním zabezpečovacího zařízení je podávat informace majiteli a tím ochránit objekt před předem zvolenými riziky. Hlavní částí EZS je zabezpečovací ústředna, která má za úkol vyhodnocovat stav detektorů a která je uživatelem nejčastěji ovládána pomocí klávesnice. Prostory, u kterých je nežádoucí vniknutí pachatele, jsou střeženy pomocí detektorů. Detektorem je myšleno zařízení, jež předá zabezpečovací ústředně signál v případě, že vyhodnotí stav považovaný za narušení. Systém na něj může upozornit akustickou nebo optickou signalizací. V případě, že se v objektu nachází fyzická ostraha, lze zprávu o narušení předat pomocí telefonních linek nebo bezdrátovým přenosem. Pod pojmem fyzická ostraha si lze představit jak samotného zákazníka, tak i bezpečnostní agenturu. Pro bezpečnostní agenturu se vžil název „PCO – Pult centrální ochrany“. [1, 2]

Mezi prvky elektronického zabezpečovacího systému řadíme: [2]

- čidlo EZS;
- ústřednu EZS;
- přenosové zařízení (prostředky);
- signalizační zařízení;
- doplňková zařízení;
- ovládací zařízení;
- napájecí zdroj.

2.2 Názvosloví

Zařízení elektrické zabezpečovací signalizace: soubor čidel, ústředen, tísňových hlásičů, prostředků poplachové signalizace, přenosných zařízení, zapisovacích a ovládacích zařízení, pomocí kterých je opticky nebo akusticky signalizováno narušení střeženého objektu nebo prostoru na určitém místě;

Komponenty systému: jednotlivá zařízení, jež tvoří EZS, pokud jsou uspořádaná;

Čidlo EZS: zařízení reagující na jevy související s narušením střeženého objektu nebo prostoru nebo s nežádoucí manipulací se střeženým předmětem vytvořením předem určeného výstupního signálu;

Ústředna EZS: zařízení určené k příjmu a vyhodnocení výstupních elektrických signálů čidel nebo tísňových hlásičů a vytvoření signálů o narušení;

Signalizační zařízení EZS: zařízení, které opticky, akusticky nebo společně opticky i akusticky signalizuje výstupní informace ústředny;

Základní napájecí zdroj: zdroj napájecí EZS nebo jeho komponenty při normálních provozních podmínkách;

Náhradní napájecí zdroj: napájecí zdroj energie, jenž je schopen napájet EZS v případě výpadku základního napájecího zdroje po předem určenou dobu. [3]

3 Analýza dosavadních řešení

Pro podrobnou analýzu současných řešení je nutné zjistit míru rizik, která se mohou vyskytnout. Tato rizika budou zohledněna při výběru zabezpečovacího systému. Bude zjištěno, jakým způsobem jednotliví výrobci zabezpečují objekt vůči těmto rizikům.

3.1 Rizika

Zde jsou nastíněna rizika, která je potřeba zohlednit při zabezpečení objektů. Rizika rozdělujeme do dvou skupin. První skupinu tvoří rizika z pohledu živlů, druhou skupinu tvoří rizika z pohledu vloupání do objektu cizí osobou.

3.1.1 Rizika z pohledu živlů

Vznik požáru

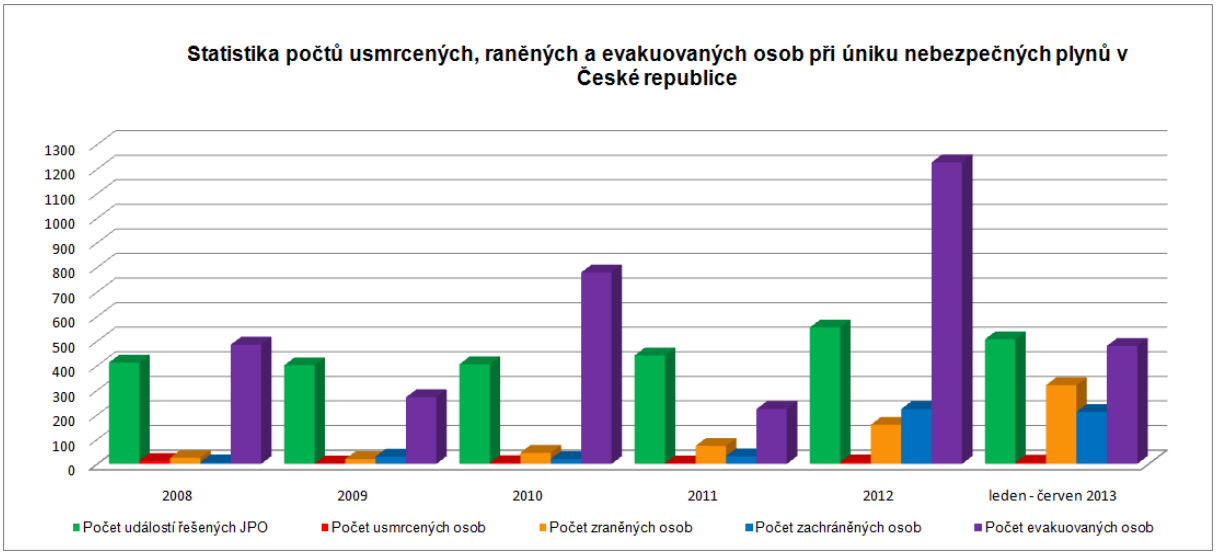
Vznik požáru má mnoho příčin. Za nejrizikovější se považují nemovitosti, ve kterých je manipulováno s otevřeným ohněm. Dále může vzniknout zkratem na elektroinstalaci nebo může být způsoben žhářem. Oheň je pro vlastníka nejnebezpečnější, pokud spí, jelikož po otravě kouřem upadá do bezvědomí a ztrácí možnost úniku. Včasné upozornění na vznikající požár je proto velice důležité. V tabulce č. 1 je vidět počet a následky požárů za léta 2008-2013.

Rok	Počet požárů	Usmrceno osob	Zraněno osob	% požárů budov pro bydlení	% usmrcených osob u požárů budov pro bydlení	% zraněných osob u požárů budov pro bydlení
2008	20946	142	1109	17,3	37,3	47,3
2009	20177	117	980	18,2	44,4	48,6
2010	17937	131	1060	21,9	40,5	52,8
2011	21125	129	1152	16,1	38,8	45,0
2012	20492	125	1286	16,8	43,2	48,1
2013	17105	111	1189	19	45,9	45,9
Celkem	117782	755	6776	15,4	34,7	39,8

Tabulka č. 1: počet a následky požárů za léta 2008-2013[9]

Únik plynu

V mnoha domácnostech je zaveden plyn. V České republice je většinou použit poměrně bezpečný zemní plyn, ale v řadě rekreačních objektů je používán nebezpečnější propan-butan. Největší riziko nastává při vytápění objektu plynem, kdy při nedokonalém spalování vzniká plyn CO. Na otravu CO ročně v ČR umírá asi 150 osob. Na grafu č. 1 je vidět počet úniků plynu a jejich následky v jednotlivých letech.



Graf č. 1: počet úniků plynu a jejich následky v jednotlivých letech[9]

Zatopení vodou

Zatopení vodou se týká především objektů v zátopových oblastech vodních toků. Voda u velkých toků většinou stoupá pomalu a vlastník nemovitosti má dostatek času na ochranné opatření. Daleko nebezpečnější jsou bleskové povodně malých vodních toků způsobené přívalovými dešti. Včasné varování je většinou klíčové. Při povodních v roce 2013 byla celková škoda na majetku odhadována na 20 miliard. Zapomínat by se nemělo ani na riziko zatopení z důvodu poruchy domácích spotřebičů, jako je myčka nebo pračka. V objektech, které jsou vytápěny ústředním topením, je také riziko jeho poškození a následné zatopení vodou, která je použita na vytápění.

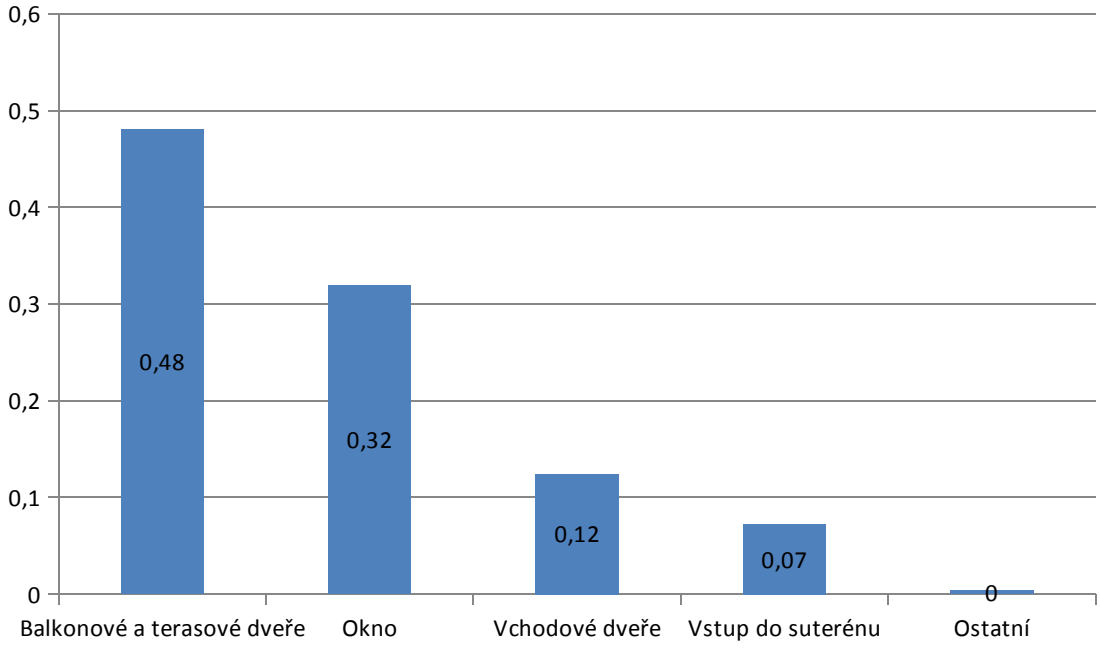
3.1.2 Rizika z pohledu napadení cizí osobou

Pachatel pro násilný vstup většinou volí dveře či okno. Rizikové jsou nemovitosti ležící mimo hustě osídlené oblasti. Cílem zlodějů se stávají především rekreační objekty mimo letní sezónu. V tabulce č. 2 je vidět počet vyloupených objektů v jednotlivých krajích za rok 2012.

Středočeský kraj	1265
Jihočeský kraj	364
Jihomoravský kraj	354
Ústecký kraj	349
Plzeňský kraj	340
Liberecký kraj	339
Kraj Vysočina	278
Moravskoslezský kraj	233
Praha	229
Královéhradecký kraj	217
Olomoucký kraj	196
Pardubický kraj	175
Zlínský kraj	174
Karlovarský kraj	121
Celkem	**4 634**

Tabulka č. 2: Počet vykradených rekreačních objektů v roce 2012[10]

Na grafu č. 2 je vidět německá Kölner studie 2011, která ukazuje, že násilné vniknutí do objektu je nejpravděpodobnější přes přední balkonové či terasové dveře. Toto místo pro násilný vstup volí 48.04% pachatelů. Dále 31.93% pachatelů volí pro násilný vstup okno. Vchodové dveře použilo 12.43% a vstup do suterénu 7.24%.



Graf č. 2: Kölner studie 2011[6]

4 Průzkumné šetření

4.1 Metodika průzkumu

Během analýzy stávajících řešení bude prováděno průzkumné šetření v domácnostech. Profese autora práce umožňuje navštívit v průměru 7 domácností denně. Toto šetření bude probíhat metodou rozhovorů v domácnostech. V navštívených domácnostech budou položeny následující otázky:

1. Disponujete zabezpečovacím systémem?
2. Pokud ano, jakým typem?
3. Jaké má tento systém obsažené funkcionality?
4. V jakém roce byl instalován?
5. Kolik falešných poplachů systém generoval v minulém roce?
6. Kolik finančních prostředků bylo vynaloženo za celý systém?
7. Jak často zapomenete zakódovat?
8. Doplňující otázka (v případě, že bude chybět nějaká zásadní funkcionalita):
9. Proč jste si tuto funkcionalitu nedokoupil?

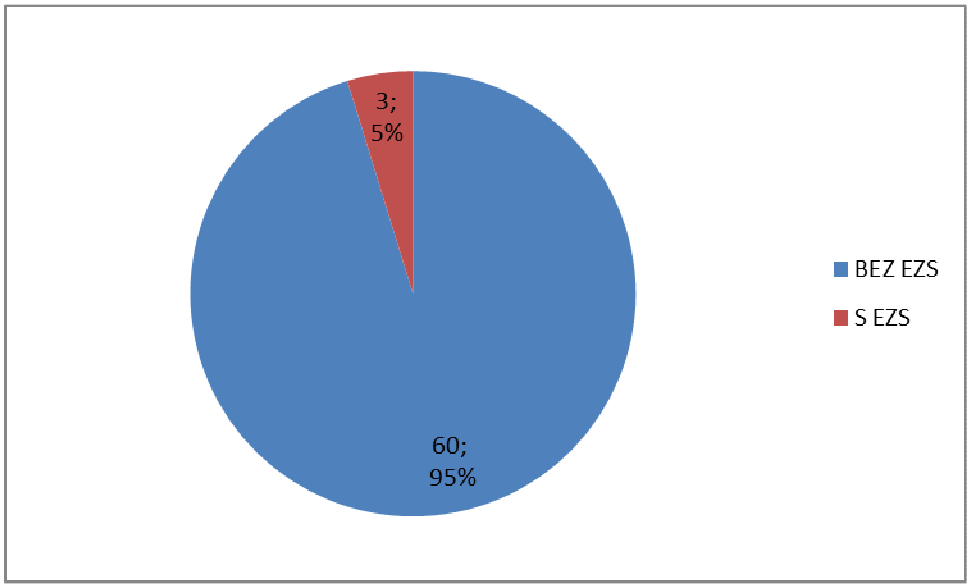
Mezi základní funkcionality autor považuje zabezpečení vstupu přes dveře, okna, detektor pohybu a detektor kouře.

4.2 Výsledky šetření

Na trhu se zabezpečovacími zařízeními funguje mnoho zavedených firem. Pro zvolení největších hráčů byly použity výsledky z provedeného šetření. Toto šetření probíhalo ve 153 domácnostech v následujících obcích: České Budějovice, Dubné, Rudolfov, Dubičné, Lipí, Vrábče, Bavorovice, Hrdějovice, Staré Hodějovice, Plav a Roudné. Navštíveno bylo celkem153 domácností, z toho bylo 63 bytů, 72 domů a 18 firem. Během tohoto šetření se postupovalo na základě metodiky z kapitoly 5.1.

4.2.1 Zabezpečení bytů

Šetřením bylo zjištěno, že pouze ve 3 bytech z 63 bylo instalováno EZS (graf č. 3). Nejprve byl zjištěn výrobce zařízení. 2x byl nainstalován Jablotron a 1x Paradox. Dále byly zjišťovány funkcionality systému. Ve všech 3 bytech byly instalovány pohybové detektory PIR, detekce vniknutí dveřmi. Detekce vniknutí oknem nebyla instalována ani v jednom bytu. Ve všech případech byl instalován detektor kouře, avšak v jednom případě byl pouze autonomní, bez napojení na ústřednu. Instalace systému proběhla průměrně v roce 2011, a to již během výstavby bytu. V průměru systém generuje 3 falešné poplachy ročně. Majitel zapomene zakódovat průměrně 2x do měsíce. Průměrná cena zabezpečovacího systému nebyla určena, neboť ve všech případech lidé kupovali byt již s namontovaným EZS. Zabezpečovací systém se nacházel výhradně v nově vystavených bytech. Ve starších panelových bytech nebyl žádný systém instalován.



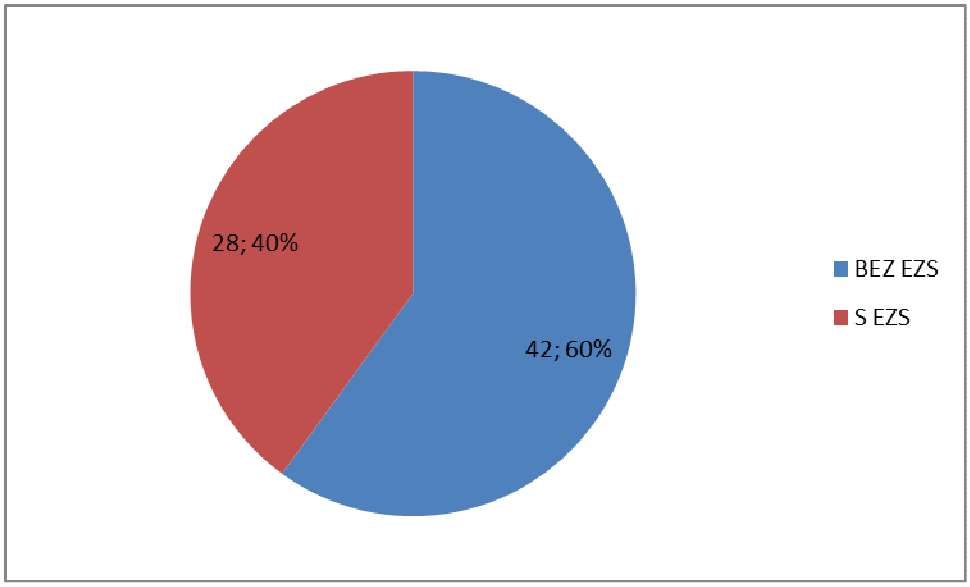
Graf č. 3: Použití EZS v bytech

Zdroj: Vlastní zpracování

4.2.2 Zabezpečení domů

V domech byl EZS přítomen v 28 ze 72 případů (graf č. 4). Zjištěním výrobce jsme došli k výsledku: 9x Jablotron, 11x Paradox, 4x Honeywell a 4x menší výrobci. Ještě

v 8 domech byl instalován autonomní detektor kouře, u něhož nebyl zjišťován výrobce, neboť nebyl napojen na celkový elektronický zabezpečovací systém. Dále byly zjišťovány funkcionality systému. Ve všech domech byly instalovány pohybové detektory PIR a detekce vniknutí dveřmi. Detekce vniknutí oknem byla instalována v 60,71%. Tato funkcionalita nebyla dokoupena z důvodu podcenění tohoto rizika. Ve všech případech byl instalován detektor kouře, přičemž na ústřednu byl napojen v 78,57 %. V průměru systém generuje 2 falešné poplachy ročně. Průměrná cena zabezpečovacího systému byla 38 953Kč, počítáno na základě 16 odpovědí. Zabezpečovací systém v bytech se nacházel většinou v nově postavených domech.



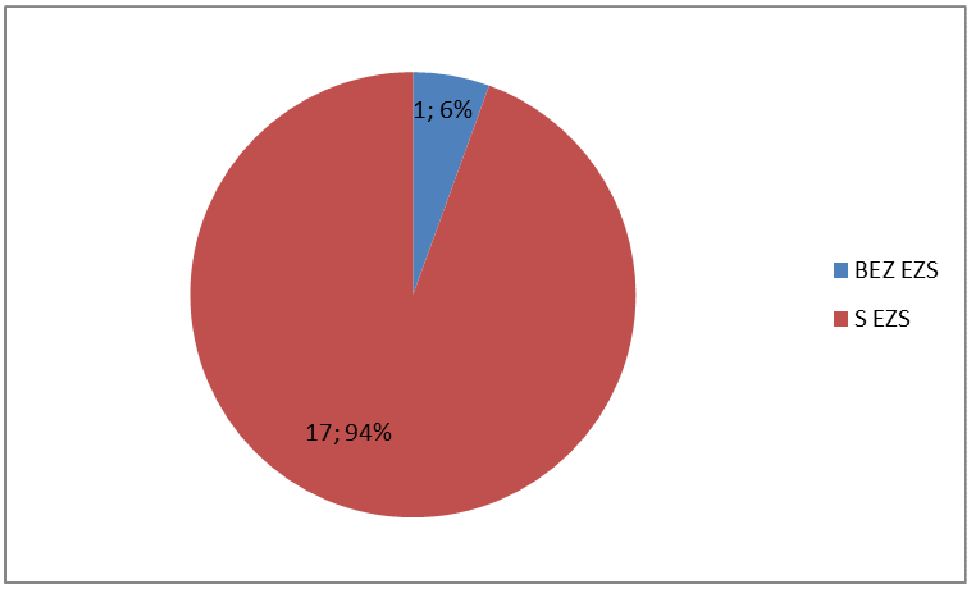
Graf č. 4: Použití EZS v domech

Zdroj: Vlastní zpracování

4.2.3 Zabezpečení firem

Z 18 firem byl v 17 případech instalován EZS (graf č. 5). Ve zbývající firmě byl instalován pouze autonomní detektor kouře. Zde byla situace následující: 7x Jablotron, 7x Paradox, 2x Honeywell a 2x různí malí výrobci. Byly zjištěny funkcionality. Ve všech případech byly instalovány detektory pohybu. Ve všech případech byl instalován detektor vstupních dveří. Detektor rozbití oken byl instalován v 58,82 % případů. Detektor kouře byl rovněž instalován ve všech zkoumaných firmách. Jeho napojení na ústřednu bylo v 88,24 %. V průměru systém generuje 5 falešných poplachů

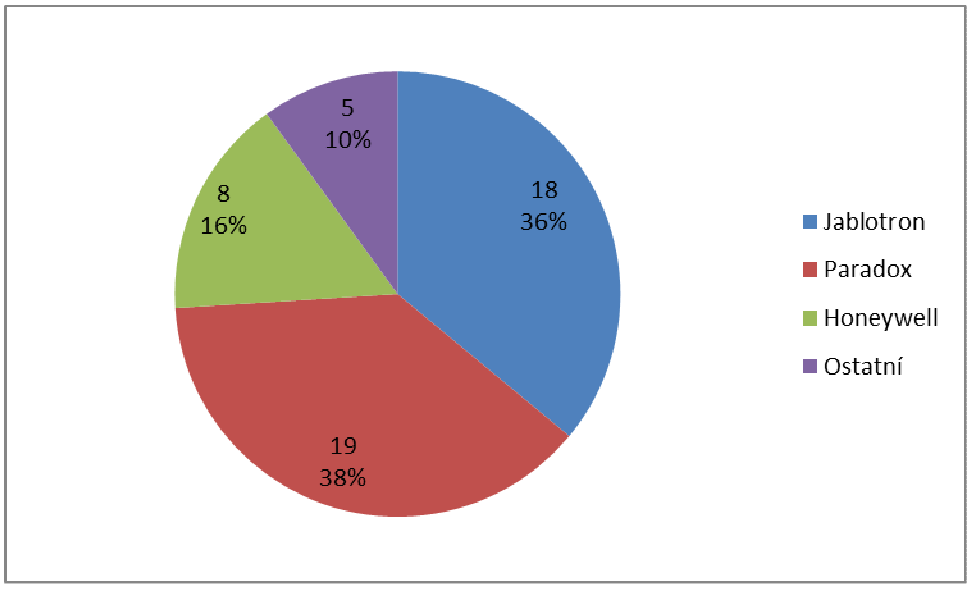
do roka. Tato otázka byla zodpovězena pouze v 8 případech. V ostatních firmách se autor nedostal do kontaktu s kompetentními osobami.



Graf č. 5: Použití EZS ve firmách

Zdroj: Vlastní zpracování

Výsledkem této analýzy je zjištění, že nejvíce lidí používá výrobky firmy Paradox, a to v 19 případech. Firmu Jablotron si pro zabezpečení objektu lidé zvolili v 18 případech. Dále 8x bylo instalováno zařízení firmy Honeywell a 5x zařízení různých menších výrobců (graf č. 6).



Graf č. 6: Jaké značky se nejvíce používají

Zdroj: Vlastní zpracování

5 Komerční zabezpečovací systémy

Jablotron - česká firma sídlící v Jablonci nad Nisou. Specializuje se na výrobu zabezpečovacích zařízení a mobilních telefonů pro seniory. V České republice nabízí systémy např. JA-80, JA-100.

Paradox - kanadská společnost specializující se na výrobu zabezpečovacích zařízení. V České republice nabízí systémy SPECTRA nebo MEGELLAN.

HoneywellSecurity - americká společnost. V České republice je nabízen systém HoneywellGalaxy.

Tyto společnosti mají vypracováno mnoho hotových komplexních systémů na ochranu majetku. Zákazník má na výběr několik konfigurací. Nejlevnější jsou zcela autonomní a disponují pouze akustickou výstrahou.

Většina zákazníků zvolí sofistikovanější systém skládající se z několika prvků. Tento systém je napojen na PCO (pult centrální ochrany), kde v případě narušení objektu okamžitě vyjíždí na místo hlídka bezpečnostní agentury. V základní konfiguraci mají tyto systémy primárně ochránit objekt pouze vůči napadení cizí osobou a nezabývají se ochranou před jinými riziky.

5.1 Možnosti systému Jablotron JA-100

Od firmy Jablotron bude popsán systém JA-100, který byl zvolen pro svou univerzálnost a množství nabízeného příslušenství.

Tento systém se skládá z ústředny a jednotlivých senzorů. Ústředna má vestavěný GSM/GPRS/LAN komunikátor, který umožňuje hlasovou, SMS nebo GPRS komunikaci s koncovými uživateli nebo středisky PCO. Je vybaven 1GB paměťovou kartou pro uchování dat událostí, nabídku hlasových zpráv, ukládání snímků atd.

Systém přenosu dat z čidel k ústředně je veden pomocí drátových rozvodů, kdy je každé čidlo spojeno odpovídajícím kabelem s ústřednou, nebo pomocí bezdrátového přenosu, kdy se informace posílají pomocí rádiového signálu. Komunikace s ústřednou probíhá ve frekvenčním pásmu 868 nebo 433MHz. Jejich výkon je přibližně 10mW. Pro spolehlivý přenos dat ze senzorů do ústředny je z hlediska spolehlivosti vhodnější

použít přenos pomocí drátových rozvodů, které nelze tak snadno zarušit či přenášená data odchytit. Na druhou stranu je nutno říct, že díky přenosu pomocí rádiových vln je celková instalace systému mnohem méně náročná a nezasahuje tolik do interiéru domu.

Typová instalace pro vzorový byt (obrázek č. 1) je připravena v bezdrátové verzi, která je šetrná k interiéru bytu a výrazně zkracuje čas, tím snižuje i cenu montáže v porovnání s drátovým systémem. Ústředna s GSM komunikátorem umožňuje komunikaci s bezpečnostním centrem, mobilními telefony uživatelů a s webovou samoobsluhou. Součástí ústředny je rádiový modul, který zajišťuje komunikaci s bezdrátovými komponenty systému. Přístupový modul s RFID čtečkou je opatřen dvěma ovládacími segmenty pro snadné zajištění a odjištění systému, včetně hlídání bytu během spánku a samostatného hlídání komory:

- 2 pohybové detektory slouží k detekci pohybu v předsíni a obývacím pokoji;
- 3 magnetické detektory hlídají vstupní a balkónové dveře a dveře komory;
- Požární detektor je nainstalován v předsíni;
- Interní siréna pro signalizaci poplachů je umístěna v obývacím pokoji;
- Součástí dodávky jsou dva ovládací čipy;
- Cena vzorové instalace je 18 431 Kč bez DPH, 21 196 Kč včetně 15 % DPH.[11]

Obrázek č. 1: Typová instalace pro vzorový byt[11]

5.1.1 Analýza řešení rizik systémem Jablotron

Napadení cizí osobou

Primární úkol tohoto zabezpečovacího systému je zabezpečit objekt proti napadení cizí osobou. Podle Kölner studie 2011 (graf č.2) je zjištěno, že pachatel volí ke vstupu do objektu nejčastěji balkonové či terasové dveře. Systém Jablotron JA-100 nabízí např. detektor JA-151M, který je určen k detekci otevření okna nebo dveří. Tento detektor pracuje na magnetickém principu. V případě rozbití okna systém JA-100 nabízí detektor JA-120PB, který kombinuje PIR detektor pohybu a akustický detektor tříštění skla. Tento detektor reaguje na typický zvuk tříštění skla. Komunikaci s ústřednou zajišťuje kmitočet 868,1 MHz. Komunikace probíhá protokolem JABLOTRON.

Vznik požáru

K systému JABLOTRON JA-100 lze za příplatek 1223Kč koupit kombinovaný optický detektor kouře a zvýšené teploty detekuje požár v obytných nebo komerčních budovách. Umožňuje detekci: kouře a zvýšené teploty, kouře, nebo zvýšené teploty, jen kouře,

nebo jen zvýšené teploty. Má funkci paměti poplachu, při níž LED kontrolka zůstává svítit i po skončení poplachového stavu. Detektor je napájený alkalickými bateriemi.

Únik plynu

K systému JABLOTRON JA-100 lze za příplatek 1223Kč koupit JA-180Gbezdrátový detektor úniku plynu. Tento detektor slouží k indikaci úniku hořlavých plynů (zemní plyn, svítiplyn, propan, butan) a hořlavých výparů. Napájí se přímo ze sítě, signalizuje únik plynu opticky, akusticky a vysílá též informaci rádiovým protokolem. K detekci jedovatých zplodin se používá katalytické spalování.

5.2 Možnosti systému Paradox MAGELLAN

Systémy od firmy Paradox jsou modulární a zákazník si je sestavuje sám. Systém se skládá z ústředny, detektorů a signalizace. Dále jsou k dispozici expandéry, které rozšiřují možnosti systému. Tento systém se skládá z ústředny a jednotlivých senzorů. Ústředna má vestavěný GSM/GPRS/LAN komunikátor, který umožňuje hlasovou, SMS nebo GPRS komunikaci s koncovými uživateli nebo středisky PCO.

Systém přenosu dat z čidel k ústředně je veden pomocí drátových rozvodů, kdy je každé čidlo spojeno odpovídajícím kabelem s ústřednou nebo pomocí bezdrátového přenosu, kdy se informace posílají pomocí rádiového signálu. Komunikace s ústřednou probíhá ve frekvenčním pásmu 868 nebo 433MHz. Jejich výkon je přibližně 10mW. Pro spolehlivý přenos dat ze senzorů do ústředny je z hlediska spolehlivosti vhodnější použít přenos pomocí drátových rozvodů. Tyto rozvody nelze tak snadno zarušit či přenášená data odchytit. Na druhou stranu je nutno říct, že díky přenosu pomocí rádiových vln je celková instalace systému mnohem méně náročná a nezasahuje tolik do interiéru domu.

5.2.1 Analýza řešení rizik systémem Paradox

Napadení cizí osobou

Primární úkol tohoto systému je zabezpečit objekt proti napadení cizí osobou. Podle Kölner studie 2011 (graf č. 2) je zjištěno, že pachatel volí ke vstupu do objektu

nejčastěji balkonové či terasové dveře. Proti vniknutí do objektu cizí osobou dveřmi využívá tento zabezpečovací systém detektor DCT2, který pracuje na magnetickém principu. Pro komunikaci s ústřednou využívá rádiový kmitočet 868MHz. Samotný detektor je napájen 3V baterií. Rozbití okna je detekováno detektorem G550. Detektor pracuje na principu zachycení typického zvuku tříštění skla. Pro zjištění pohybu v objektu je využíván detektor DG65, který detekuje pohyb pomocí infračerveného záření.

Vznik požáru

Pro detekci vzniku požáru slouží detektor WS588P. Pracuje na optickém principu, tudíž nedetekuje plyn, teplotu nebo oheň. Optické kouřové detektory jsou hodně efektivní při detekování doutnajících požárů, jejichž kouř doutná hodiny před vypuknutím požáru. Zdroje těchto požárů mohou být např. cigarety hořící na pohovce nebo v posteli. Detektor má vnitřní sirénu.

Únik plynu

Bylo překvapením, že na oficiálních stránkách Paradox pro Českou republiku není žádný detektor úniku plynu. Nakonec se podařilo najít detektor WC588P-868, který detekuje plyn CO vznikající nedokonalým spalováním.

5.3 Přehledová tabulka jednotlivých systémů

Na přehledové tabulce č. 3 je vidět, že většina výrobců využívá téměř shodnou technologii pro eliminaci různých rizik. Rozdíly jsou v použité bezdrátové technologii, kdy systémy od firmy Jablotron a Paradox používají k přenosu dat pásma 868MHz a 433MHz. Systémy od společnosti Honeywell používají pouze pásmo 868MHz. Další rozdíly lze vidět v tom, že např. pro detekci kouře Jablotron využívá kombinaci dvou technologií v jednom čidle, a to optickou a teplotní. Systém od společnosti Paradox nabízí obě technologie, avšak každou ve speciálním čidle.

Systém	**JA-80**	**JA-100**	**MAGELLAN**	**SPECTRA**	**Galaxy**
Výrobce	Jablotron	Jablotron	Paradox	Paradox	Honeywell
Napájecí napětí	230 V / 50 Hz	230 V / 50 Hz	16V	16V	16.5V
Komunikační frekvence	868 MHz/433MHz	868 MHz/433MHz	868 MHz/433MHz	868 MHz/433MHz	868 MHz
GSM/GPRS	ANO/ANO	ANO/ANO	ANO/ANO	ANO/ANO	ANO/ANO
Násilný vstup dveřmi	Magnetický detektor	Magnetický detektor	Magnetický detektor	Magnetický detektor	Magnetický detektor
Násilný vstup oknem	Magnetický detektor	Magnetický detektor	Magnetický detektor	Magnetický detektor	Magnetický detektor
Rozbití okna	Akustický/otřesový	Akustický/otřesový	Akustický	Akustický	Akustický/otřesový
Detekce pohybu	PIR	PIR	PIR	PIR	PIR
Detekce úniku plynu	ANO	ANO	ANO	ANO	ANO
Detekce kouře	Opticko-teplotní	Opticko-teplotní	Optický/Teplotní	Optický/Teplotní	Opticko-teplotní
Detekce úniku vody	ANO	ANO	ANO	ANO	ANO

Tabulka č. 3: Technologie pro eliminaci různých rizik

Zdroj: Vlastní zpracování

6 Praktická část

V praktické části bude proveden návrh systému, který je založen na platformě Arduino. Tento návrh vychází z analýzy z předchozí kapitoly. Budou zde zohledněny současné trendy v oblasti zabezpečení objektů. Následně bude tento návrh sestrojen a otestován v praxi, výsledky budou zde zveřejněny. Z analýzy lze navrhnout obecné schéma pro platformu Arduino.

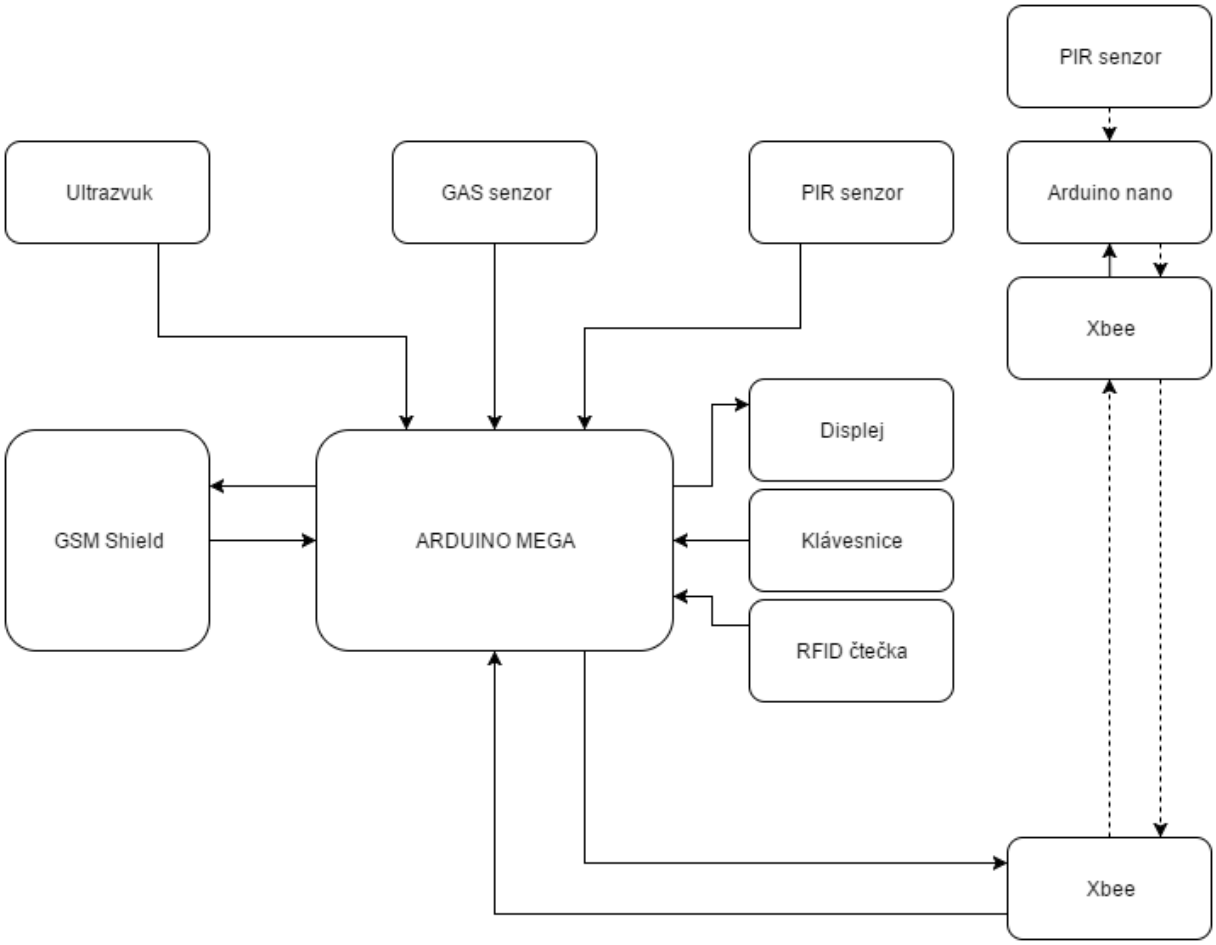


Schéma č. 1: Schéma zapojení systému

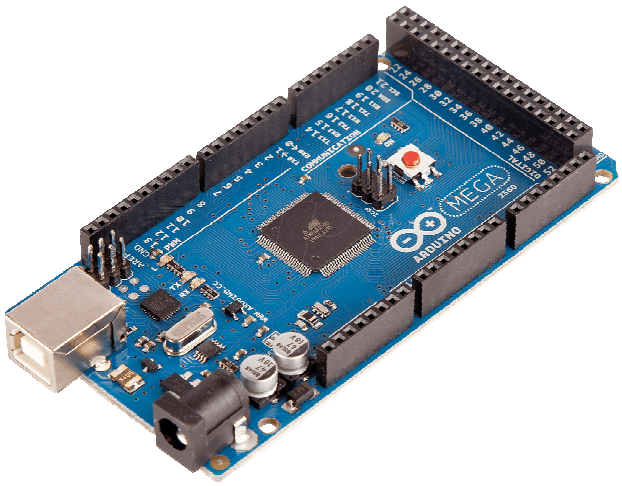
Z blokového schématu č. 1 je patrné, že je nutné provést sekundární analýzu čidel, která lze použít v adekvátní kvalitě …

6.1 Volby senzorů k platformě Arduino

Na základě analýzy bylo zjištěno, jaké senzory se používají u komerčně dostupných systémů k eliminaci různých rizik. Dále zde zvolím, jaký použiji mikrokontroler na přijímání dat z jednotlivých senzorů. V této kapitole se práce bude zabývat existencí open hardware alternativy k jednotlivým prvkům zabezpečovacího systému.

6.1.1 Volba komponentů pro ústřednu

Arduino nabízí několik desek. Pro potřeby zabezpečovacího systému je vhodná deska ArduinoMega2560, a to především pro množství vstupně výstupních pinů. Systém bude zajišťovat ochranu před riziky vloupání, vznik požáru, únik plynu a detekuje zvýšenou vodní hladinu. Senzory budou připojeny jak pomocí kabelu, tak pomocí bezdrátové technologie.

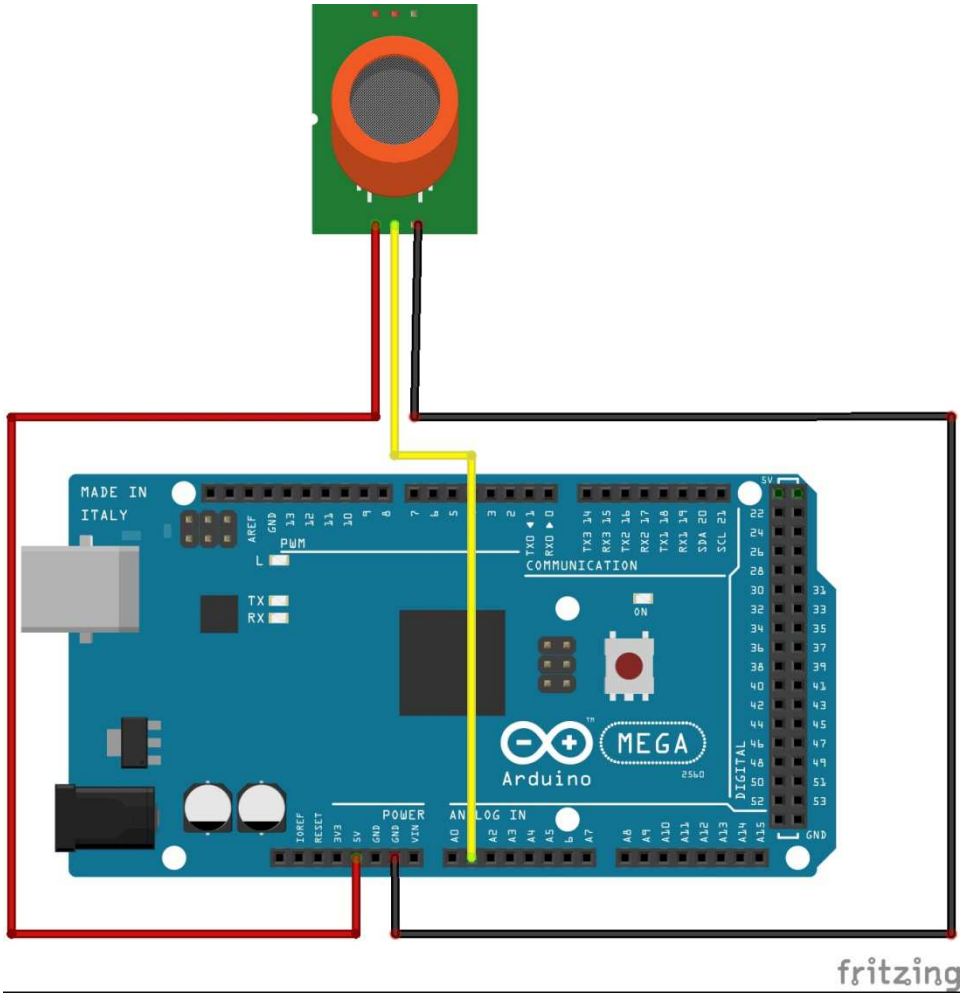


Obrázek č. 2: ArduinoMega2560

Zdroj: [12]

6.1.2 Volba senzoru pro detekci požáru

Na základě analýzy bylo zjištěno, že nejčastěji používanými senzory k eliminaci rizika ohně je kouřový detektor. Kouřové detektory pracují většinou na optickém principu nebo na principu katalytického spalování. Druhá varianta je lepší, jelikož detekuje i únik plynu. K desce Arduino lze pořídit několik senzorů. Jejich cena je velice příznivá.



Obrázek č. 3: Senzor MQ-2

Zdroj: Vlastní zpracování

Na obrázku č. 3 je vidět senzor MQ-2, který se připojuje na analogový vstup. Napájení je 5V. Tento senzor dále detekuje i únik plynu.

```
voidGAS()
{
int GASPIN = digitalRead(GAS_PIN1);
Serial.println(GASPIN);
delay(1);
}
```

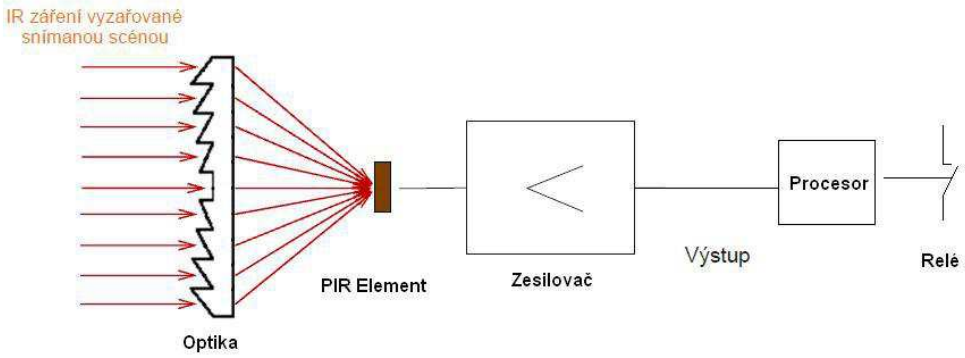
Na zdrojovém kódu je vidět načtení hodnoty z analogového vstupu a její uložení do proměnné „GASPIN“. Funkce určitého pinu se nastavuje ve funkci Setup (). Konkrétní nastavení pinu pro vstup z detektoru kouře: pinMode(GAS_PIN1,INPUT).

6.1.3 Volba senzoru pro detekci pohybu

K pohybu cizí osoby se především používají PIR detektory. PIR (Passiveinfra-red sensor) čidla jsou nejpoužívanějšími detektory v EZS. Fungují na principu zachycení pohybu těles, která mají jinou teplotu než okolí a způsobují změnu vyzařování v infračerveném pásmu (obrázek č. 4). Každé těleso s teplotou mezi -273 °C a 560 °C vyzařuje vlnění v infračerveném spektru odpovídajícímu jeho teplotě (pro lidské tělo ~ 35 °C odpovídá vlnová délka 9,4 mm). Detektorem je zde materiál vykazující pyroelektrický jev. Čidlo detekuje změny záření na něj dopadající. Obraz prostoru v infračerveném pásmu je transformován optikou na plochu senzoru. Zorné pole se dělí na aktivní a neaktivní zóny. Pohybuje-li se těleso s teplotou odlišnou od teploty okolí v zorném poli čidla, jsou zachycovány jeho přechody mezi aktivními a neaktivními zónami. Elektronika vyhodnotí signál vyvolaný těmito změnami a vyhlásí poplach

Snížení tendencí k planým poplachům se dá dosáhnout pomocí tzv. černých zrcadel. Ty omezují odrazivost mimo požadované infračervené spektrum jako odlesky slunce atd. Základy montáže PIR čidel jsou:

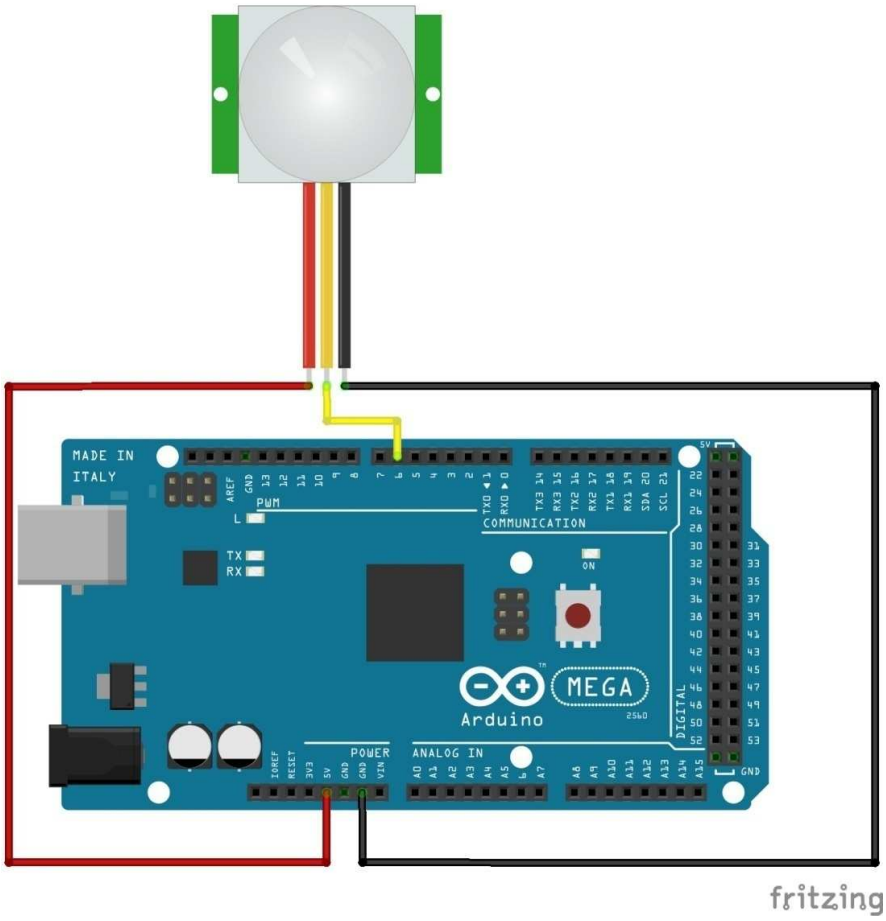
- instalace kolmo (tangenciálně) k pravděpodobnému pohybu pachatele;
- umístění na pevném podkladu bez vibrací;
- je možná instalace více čidel do jednoho prostoru bez nebezpečí vzájemného ovlivnění;
- v prostorách s podlahovým vytápěním se od použití PIR čidel upouští;
- PIR čidla nesmí být nasměrována na okna, vnější dveře a vrata;
- čidla nesmí být vystavena vlivům ventilace (průvan), vyzařování světla, proměnným zdrojům tepla a spínaným rušivým zdrojům IR.



Obrázek č. 4: PIR senzor

Zdroj: [13]

K Arduinu lze pořídit PIR senzory. Jejich cena je velice nízká. Připojují se na digitální či analogový vstup. Jejich kvalita se odvíjí od jejich ceny.



Obrázek č. 5: Schéma zapojení k Arduinu

Zdroj: Vlastní zpracování

Na obrázku je vidět schéma zapojení k Arduinu. Napájení probíhá 5V a signál ze senzoru je přijímán na digitální vstup.

Příklad funkce PIR (), která provádí načtení hodnoty z digitálního vstupu. Na tento vstup je připojen PIR senzor. Tato hodnota se uloží do proměnné „PINPIRP“.

```
voidPIR ()
{
int PINPIRP = digitalRead(PIR_PIN1);
Serial.println(PINPIRP);
delay(1);
}
```

6.1.4 Volba senzoru pro detekci rozbití skla

V případě napadení objektu cizí osobou často dojde k rozbití skla, proto se používají detektory rozbití skla. K Arduinu lze připojit piezoelektrický snímač. Piezoelektrický jev je schopnost krystalu generovat elektrické napětí při jeho deformování. Při rozbití skla dojde tudíž ke generování elektrického napětí, které přivedeme na vstupní pin.

6.1.5 Volba senzoru pro detekci otevření dveří

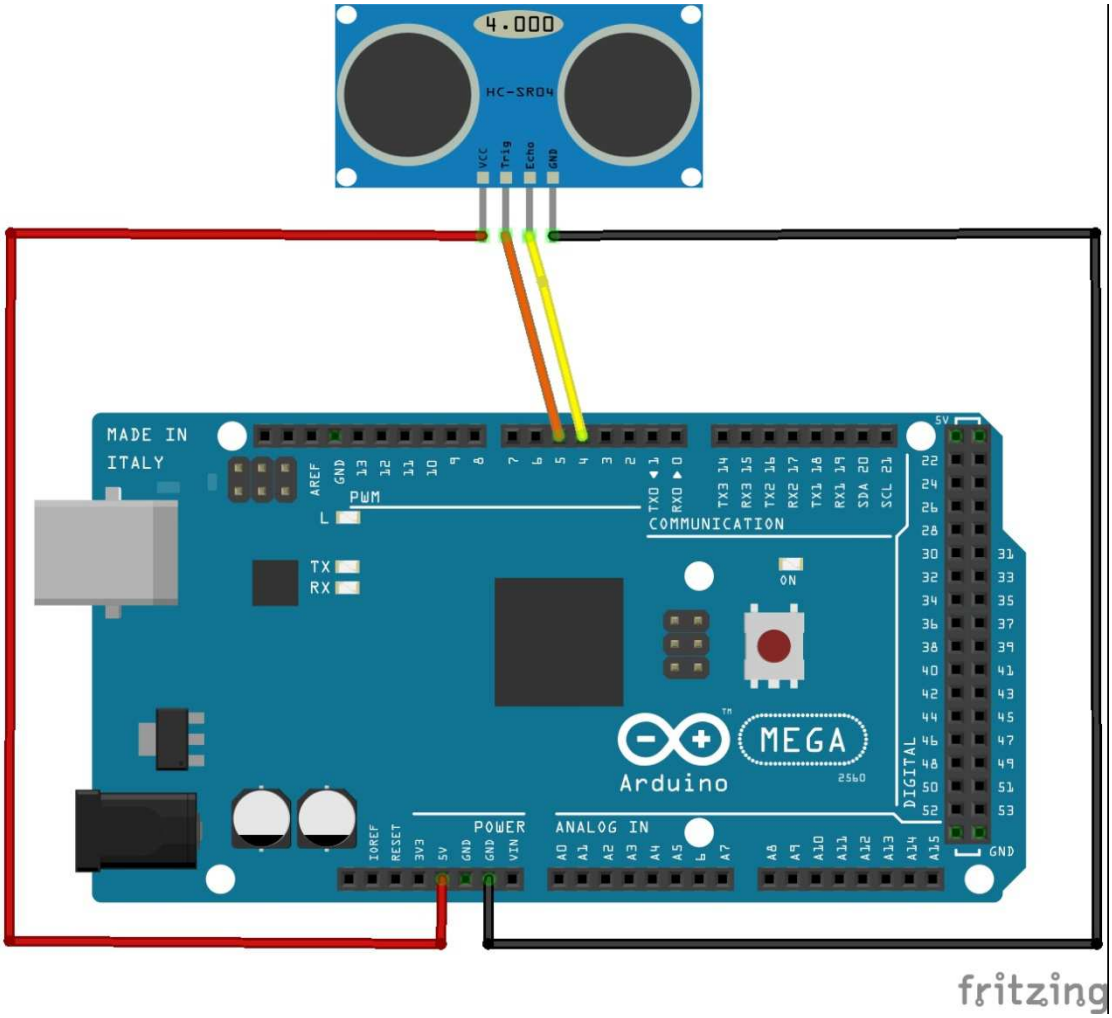
Magnetický dveřní kontakt je velmi spolehlivý, nenapájený prvek plášťové ochrany s minimálním počtem konstrukčních dílů, vysokou odolností a dlouhou životností slouží k detekci otevření dveří. Magnetické kontakty jsou tvořeny dvojicí dílů - jazýčkovým kontaktem a permanentním magnetem. Permanentní magnet je nejčastěji zmagnetovaný váleček z feritu. Jazýčkový kontakt je tvořen zatavenou skleněnou trubičkou naplněnou ochrannou atmosférou, v níž jsou umístěny dva feromagnetické kontakty. Pro detekci otevření dveří se používá magnetický detektor otevření dveří. V klidovém stavu je kontakt jazýčkového relé sepnut magnetickým polem permanentního magnetu. Při aktivaci oddálením magnetu se kontakt rozepne a spustí poplach. Tento senzor se přivede na digitální vstupní pin.

6.1.6 Volba senzoru pro detekci zvýšené vodní hladiny

K eliminaci rizika povodně od vodních toků. Hladinu vodního toku můžeme měřit ultrazvukovým senzorem. Vysílaný ultrazvuk se nám odrazí od vodního toku a přesně

změříme jeho výšku. Nejvhodnější se jeví použití senzoru HC-SR04, který vyniká svou dostupností a nízkou cenou.

Na obrázku je vidět schéma zapojení ultrazvukového senzoru HC-SR04.



Obrázek č. 6: schéma zapojení ultrazvukového senzoru HC-SR04

Zdroj: Vlastní zpracování

Na zdrojovém kódu je vidět, že se nejdříve vyšle impuls do senzoru. Dále se spočítá vzdálenost, která přišla z ultrazvukového čidla, a ta se uloží do proměnné distance. Tyto informace odešleme na sériový port a můžeme s nimi pracovat.

```
voidloop()
{
digitalWrite(TRIGPIN, LOW);
delayMicroseconds(2);
digitalWrite(TRIGPIN, HIGH);
```

```
delayMicroseconds(10);
digitalWrite(TRIGPIN, LOW);

float distance = pulseIn(ECHOPIN, HIGH);
distance= distance*0.017315f;
Serial.print(distance);
Serial.print("cm\n");
}
```

6.1.7 Volba systému upozornění majitele

Pro informování majitele objektu je možné využít mnoho způsobů. Jednou z variant je zasílání dat na server přes wifi, kde by varování zajišťovala mobilní aplikace. Dále můžeme zvolit informování prostřednictvím sítě GSM, kde by majiteli systém zasílal údaje prostřednictvím SMS.

Na zdrojovém kódu je vidět zaslání SMS prostřednictvím GSM shieldu SIM900. Tato SMS se zasílá sadou příkazů. V této části zdrojového kódu bude zvoleno telefonní číslo, na které se SMS má odesílat, a text této zprávy.

```
Sim900Serial.print("AT+CMGF=1\r");
delay(100);
Sim900Serial.println("AT + CMGS = \"602872752\"");
delay(100);
Sim900Serial.println("POPLACH!");
delay(100);
Sim900Serial.println((char)26);
delay(100);
Sim900Serial.println();
```

Dále se používá hlasitá siréna, která upozorní majitele, pokud je v objektu. Siréna může být zvolena jakákoliv, např. z autoalarmu. K jejímu spuštění je zapotřebí stálého napájení 12V a MOSFET, přes který bude siréna spuštěna. Jako zdroj stálého napětí může být zvolena např. autobaterie, která se vyznačuje velkou kapacitou a může poskytnout dostatek proudu.

6.1.8 Připojení senzorů

Analýzou bylo zjištěno, že senzory jsou k řídící jednotce připojeny drátově, nebo bezdrátově. Připojení pomocí drátových rozvodů je nepohodlné a zastaralé. Jinou

možností je použít druhé Arduino, které by zasílalo data ze senzoru do řídicí jednotky bezdrátově. K Arduinu můžeme zvolit mnoho modulů na různých frekvenčních pásmech. U komerčních systémů se pro přenos dat používá pásmo 868 nebo 433MHz. U Arduina je možnost využít moduly XBee (obrázek č. 7), které pracují ve frekvenčním pásmu 900MHz nebo 2,4GHz.

Obrázek č. 7: Modul XBee

Zdroj: [14]

6.2 Možné problémy

6.2.1 Zajištění stálého napájení

Jedním z problémů při návrhu spolehlivého zabezpečovacího zařízení je zajištění stálého napájení i při přerušení dodávky elektrické energie. Tento problém jde řešit přidáním záložní baterie. Stav této baterie lze hlídat pomocí odporového děliče napětí, který připojíme na analogový vstup a přepočteme si to na aktuální stav baterie. Na případnou slabou baterii systém automaticky informuje majitele.

6.2.2 Hlídání stavů čidel

Dalším problémem je zajištění ochrany před ztrátou signálu z nějakého čidla. Tato ztráta může být náhodná (přehlodání kabelu myší) nebo úmyslná pachatelem. Bezdrátové senzory lze zarušit rušičkou daného pásma. Tato kontrola stavu čidla byla vyřešena v případě kabelového rozvodu připojením čidla na analogový vstup. Jelikož

digitální vstup řeší pouze stav 0 nebo 1, v případě odpojení byl stav stále 0. Z analogového vstupu se při odpojení senzoru stane „anténa“ a stále nám to hlásí libovolné hodnoty. Proto k čidlu přidáme odpor, kterým se „uzemní“, a odpojení poznáme.

6.3 **Finanční srovnání se systémem JABLOTRON JA-100**

	Jablotron JA-100	Systém založen na Arduinu v ČR	Systém založen na Arduinu v Číně
Bezdrátová GSM/GPRS ústředna	12 511.00 Kč	3 768.00 Kč	$47.20
Detektor pohybu	1 777.00 Kč	2 547.00 Kč	$9.80
Detektor otevření	1 190.00 Kč	2 587.00 Kč	$17.49
Detektor požáru	1 439.00 Kč	2 593.00 Kč	$9.90
Detektor rozbití skla	1 331.00 Kč	2 488.00 Kč	$8.90
Výsledná cena v USD			$93.29
Výsledná cena v Kč	18 248.00 Kč	13 983.00 Kč	2 332.25 Kč

Tabulka č. 4: **Finanční srovnání se systémem JABLOTRON JA-100**

Zdroj: Vlastní zpracování

Na finančním srovnání je vidět, že systém založený na Arduino se vyplatí především tehdy, když jednotlivé součásti jsou objednány z Číny např. přesebay.com. Ve srovnání jsou srovnatelné systémy. Bezdrátová GSM ústředna se skládá zArduina MEGA+ GSM shieldu+Xbee modulu pro připojení bezdrátových čidel. Dále každý senzor bude připojen bezdrátově prostřednictvím xbee s použitím ArduinoNano. V České republice není nabídka příslušenství pro Arduino velká a pořizovací ceny jsou poměrně vysoké. I tak výsledný systém dopadl finančně mnohem lépe než komerční systém Jablotron JA-100.

6.4 Návrh vlastního systému založeného na Arduinu

Pro návrh zabezpečovacího systému bylo zvoleno Arduino MEGA 2560. Tato deska je založena na mikroprocesoru Atmega 2560. Poskytuje nám 54 digitálních vstupů/výstupů, přičemž 14 z nich může být použito pro hardwarové generování pwm signálu. Dále obsahuje 16 vstupů s A/D převodníkem pro detekci analogových veličin, 4 hardwarové sériové linky. K dispozici je zde také 16MHz krystal a Atmega 16U2 pracující jako převodník USB-sériová linka.

Tento typ Arduino MEGA 2560 se jeví pro tyto potřeby zabezpečovacího systému jako nejvhodnější zejména z toho důvodu, že má více vstupně/výstupních pinů.

6.4.1 Způsob připojení senzorů

Senzory, které jsou blíže k ústředně, budou připojeny kabelovým rozvodem. Vzdálenější senzory budou připojeny k řídicí jednotce bezdrátovým systémem. K bezdrátovému řešení byly zvoleny moduly XBee. Jsou u nich na výběr 2 frekvenční pásma, a to 900MHz a 2.4GHz. V České Republice je z těchto dvou pásem povoleno pro bezlicenční provoz pouze pásmo 2.4GHz. Pásmo 900MHz je vyhrazeno pro provozování GSM a LTE sítí. Pro potřeby zabezpečovacího zařízení se ale zdá být pásmo 900MHz vhodnější, a to zejména z důvodu většího dosahu a lepší průchodnosti překážek. Při bezdrátovém použití je potřeba ke každému senzoru přidat ještě desku Arduino. Při cenách ArduinaNano (asi 200Kč) toto není výrazný problém.

6.4.2 Použité technologie

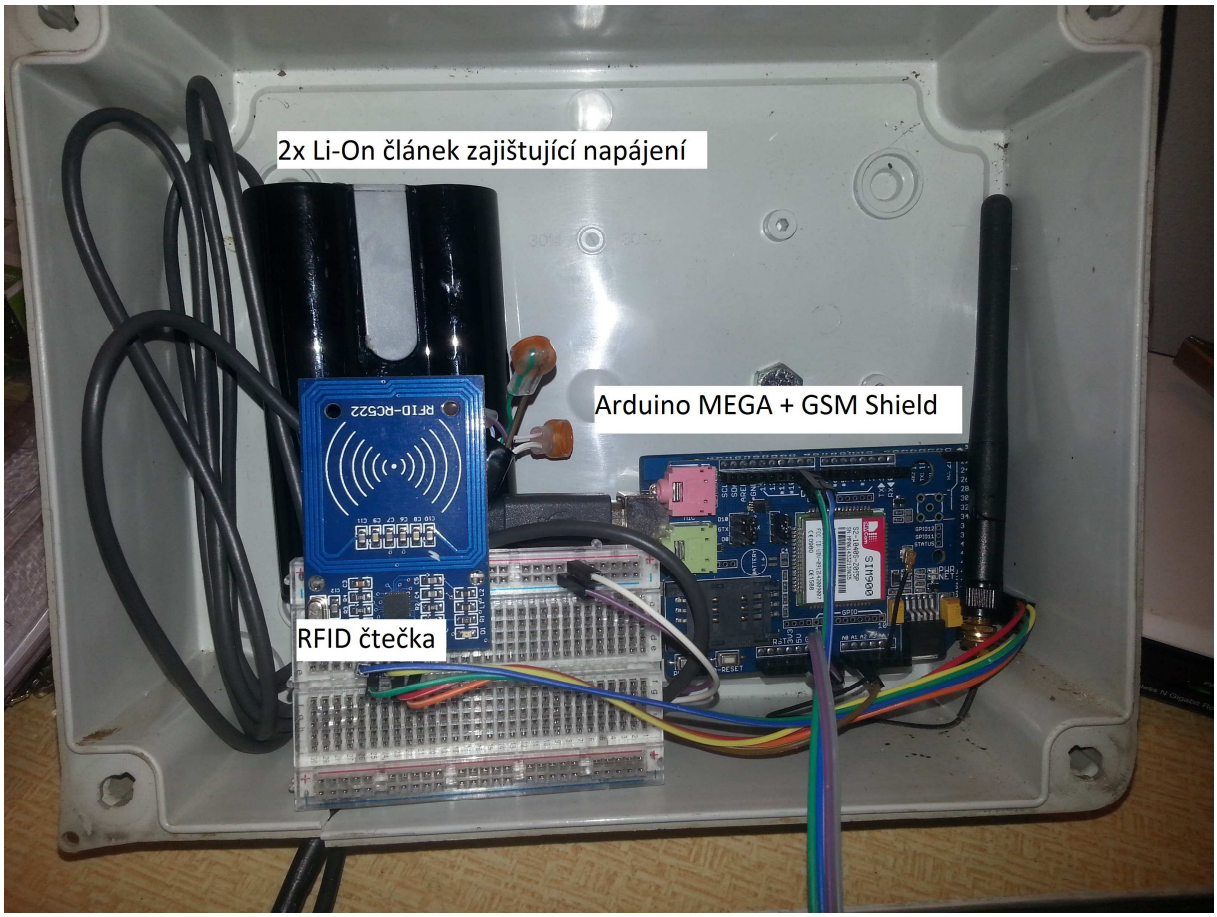
Senzory k eliminaci rizika napadení cizí osobou bude použito několik PIR (passiveinfrared sensor) čidel. Tento typ detektoru byl zvolen z důvodu jeho ceny. PIR detektory nám obsluhuje funkce PIR (), která zjišťuje aktuální stav čidla. To je připojeno na digitální vstup. Tento stav se nám ukládá do proměnné a v případě zjištění pohybu nám zavolá funkci poplach. K eliminaci rizika úniku plynu byl použit detektor plynu, který nám obsluhuje funkce GAS (). Tato funkce čte analogově hodnoty, které nám čidlo posílá. Pokusem bylo zjištěno, jaké hodnoty jsou v normálním stavu a jaké hodnoty senzor posílá v případě úniku plynu. Tento detektor reaguje i na kouř v místnosti.

Uživatelské rozhraní nám bude zajišťovat RFID čtečka s displejem a klávesnicí. RFID čtečka je k Arduinu připojena k portům SPI SS, SPI MOSI, SPI MISO a SPI SCK. Tato čtečka načte hodnotu NFC karty na frekvenci13,56 MHz. LCD displej je použit o velikosti 16x2 znaků. K připojení slouží i2c sběrnice. Klávesnice je použita číselná o rozměrech3x4.

Upozornění vlastníka nemovitosti nám bude zajišťovat GSM shield SIM900 z důvodu rychlosti, dostupnosti a spolehlivosti sítě GSM. Dále k „vyplašení“ útočníka byla použita 12V autosiréna, sepnutá přes Mosfet (Metal Oxide SemiconductorFieldEffect Transistor). Siréna byla použita z autoalarmu.

6.4.3 Zástavba systému

Pro zástavbu systému bude zvolena krabice s krytím IP55. Do této krabice se ukryje veškerá technologie řídicí jednotky, tj. ArduinoMega, GSM shield, zdroj napájení (viz obrázek č. 8). Zvenku bude na krabici připevněno veškeré uživatelské rozhraní, tj. displej, klávesnice, RFID čtečka - byla též uvnitř, na její funkčnost nemělo plastové víko krabice vliv (obrázek č. 9). Toto krytí bude systému zajišťovat ochranu zejména před poškozením ze strany hlodavců.



Obrázek č. 8: Technologie řídicí jednotky

Zdroj: Vlastní zpracování

Obrázek č. 9: Uživatelské rozhraní

Zdroj: Vlastní zpracování

6.4.4 Používání systému

Aktivace/Deaktivace systému

Při odchodu uživatel pro zakódování přiloží kartu. Systém z ní načte hodnotu UID, kterou porovná s databází uložených UID karet. Tato hodnota je uložena ve čtyřmístném poli. Na displeji se zobrazí nápis „zakodovano“ a nemovitost je chráněná proti všem rizikům, na které se zaměřujeme. Při příchodu a následném odkódování musí uživatel přiložit kartu a zadat 4místný kód. Tím vyřadí z činnosti pouze senzory, které eliminují riziko napadení objektu cizí osobou. Senzory, které nás chrání před ostatními riziky, stále zůstávají aktivní.

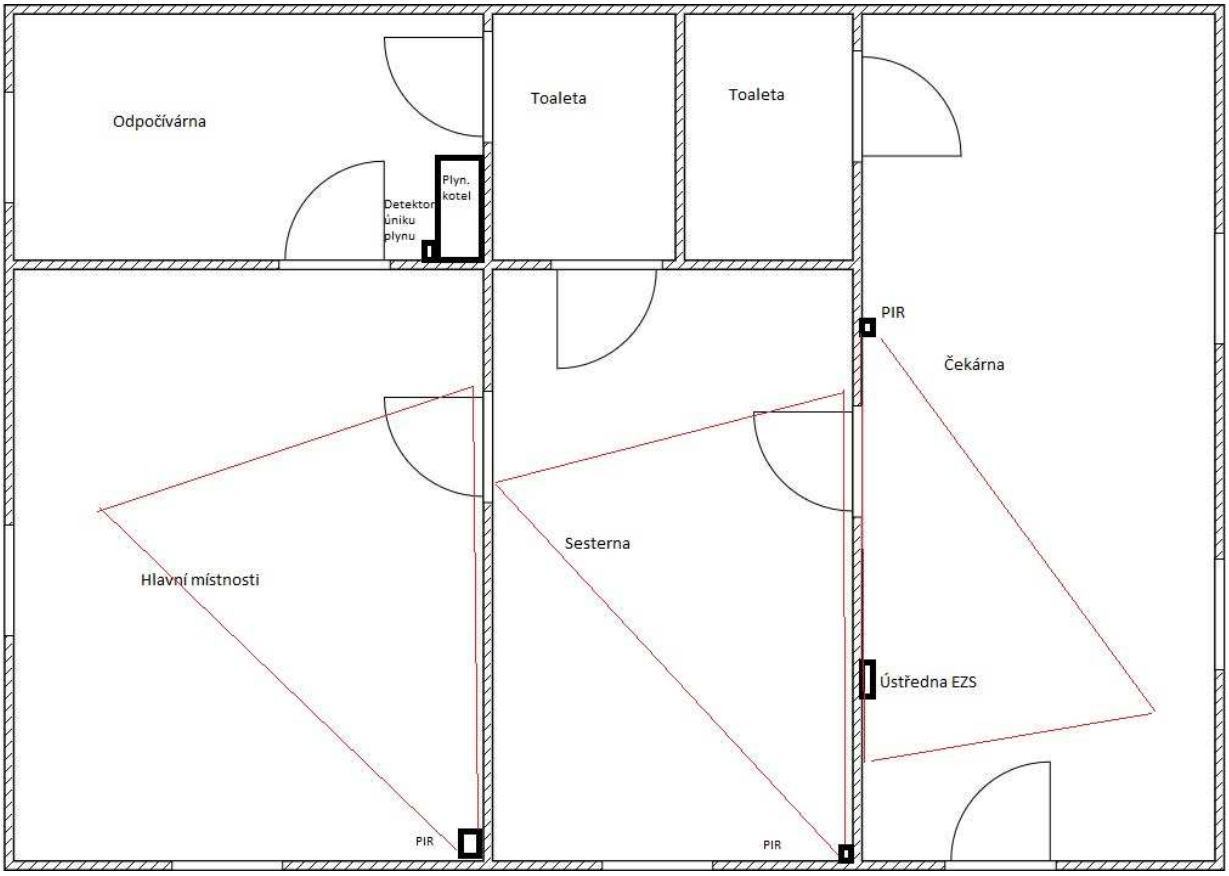
Spuštění poplachu

V případě aktivování poplachu se pomocí GSM shieldu odešle SMS na přednastavené číslo. Toto odeslání probíhá na základě funkce „SendSMS()“. V ní je zadáno telefonní číslo, na které se má SMS zpráva odeslat. Dále sem zadáme text této SMS zprávy, například ve znění „Plyn“ - upozorňuje nás na detekování zvýšené koncentrace plynu. Uživatel může přes GSM také poplach vypnout odesláním SMS ve tvaru „vypni“. V případě vyhlášení poplachu se spouští siréna.

6.5 Vyhodnocení testování a analýza chyb

6.5.1 Testovací provoz v ordinaci praktického lékaře

Systém běžel týden v testovacím provozu v ordinaci praktického lékaře, který mimo to používá i komerční zabezpečovací systém napojený na PCO. Pro potřeby testování bylo zjednodušené používání. K zakódování i odkódování se používala pouze RFID karta a nepoužívalo se zadání kódu prostřednictvím klávesnice.



Obrázek č. 10: Půdorys ordinace praktického lékaře

Zdroj: Vlastní zpracování

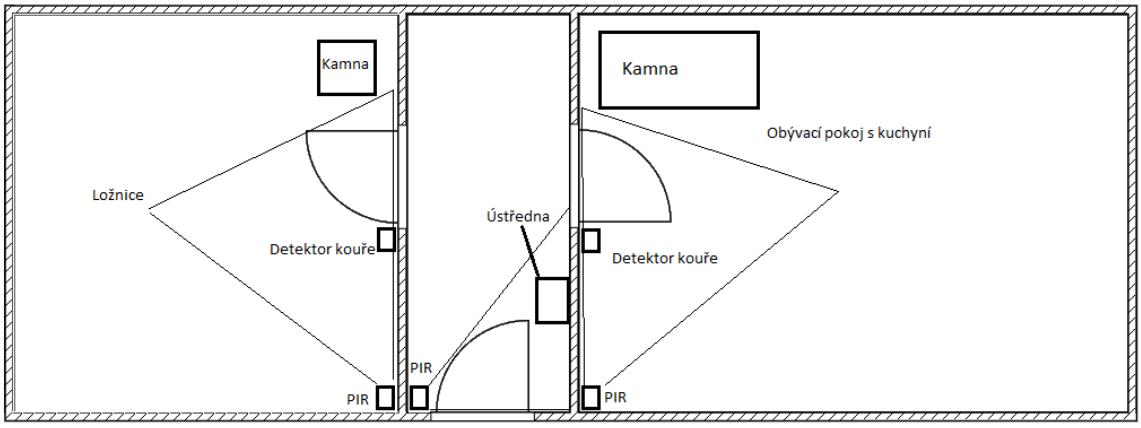
Na obrázku č. 10 je vidět půdorys ordinace praktického lékaře, jež byla už v roce 2010 vykradena. Pachatel zvolil jako místo vniknutí okno v sesterně. Komerční zabezpečovací systém, který je v ordinaci nainstalován, není vybaven detektorem rozbití skla. Proto pachatele detekoval až PIR senzor umístěný v rohu místnosti. Systém potom reagoval zavoláním do PCO prostřednictvím pevné linky telefonu. Pro umístění senzorů vlastního systému založeného na Arduinu byla provedena analýza současného řešení. Následně byly senzory umístěny na stejná místa. Oba tyto systémy běžely současně. Systém založený na Arduinu byl doplněn o senzor úniku plynu, jelikož je celá budova vytápěna pomocí plynového kotle.

Použití levných čínských detektorů se ukázalo jako velice nešťastné řešení. Z celkového počtu 5 kusů po měsíci používání 3 přestaly fungovat. Naopak levný senzor úniku plynu MQ-2 se ukázal jako spolehlivý. Pro použití v zabezpečovacích systémech má

výbornou vlastnost, a to reagovat jak na únik plynu, tak na případný požár. Použitý GSM shield SIM900 se ukázal jako nespolehlivý. Po 14 dnech bezchybného používání ztratil signál a nedokázal ho již nalézt. Tento problém nakonec vyřešil nový pigtail k anténě.

6.5.2 Testovací provoz v rekreačním objektu

Systém běžel přibližně 3 měsíce v testovacím provozu v rekreačním objektu, půdorys na obrázku č. 6. Za tuto dobu se ukázalo mnohem více problémů než při krátkém testování.



Obrázek č. 11: Půdorys rekreačního objektu

Zdroj: Vlastní zpracování

Prvním zásadním problémem bylo natažení kabelů k jednotlivým senzorům. Použití UTP kabelu se ukázalo jako nevhodné, a to především z důvodu jeho nestínění. Při delším vedení se analogová data zkreslovala především vlivem radiových vln, které kabel zachytával. Byl tedy použit stíněný kabel FTP, u kterého byl zase problém s přenosem elektrické energie na větší dálku. Řešením tohoto problému by bylo použít napájení u každého detektoru, nicméně tím by opět vypadla možnost centrální zálohy celého systému.

Dalším problémem byly čínské senzory. Především IR senzor HC-SR501 se ukázal být velice nespolehlivým. Byl zdrojem velmi častých falešných poplachů (4x za den).

Nakonec po důkladnějším šetření s použitím videokamery bylo zjištěno, že všechny poplachy byly falešné a při spuštění poplachu kamera nic nezaznamenala. Zajímavé je, že tento problém nevznikl u všech čidel. Některá se ukázala jako spolehlivá. Celkem bylo zakoupeno 15 senzorů od 3 výrobců, všechny s označením HC-SR501. Bohužel senzory se během užívání promíchaly, a proto nebylo možné určit, jestli senzory od různých výrobců jsou i různé kvality. Jako spolehlivější se ukázal senzor GH-718C.

Další problém se vyskytl při zajištění stálého napájení. Pro napájení jsem zvolil čínskou powerbanku s dvěma články 18650. Při nepřetržitém provozu ale po 6 týdnech odešel nabíjecí obvod a článek se přestal nabíjet. K hlídání stavu baterie byl použit odporový měnič napětí. Toto řešení se ukázalo jako vhodné, avšak pro bezproblémový chod by bylo vhodnější použití kvalitní powerbanky především s funkcí odpojení článku po jeho plném nabití. Nyní byl systém napájen pouze z článků, které se současně nabíjely z USB nabíječky. Toto řešení velice zkracovalo životnost použitých článků.

Dále se ukázalo, že není vhodné umístit detektor kouře v blízkosti kamen či jiného zdroje otevřeného ohně. Netěsnost kamen způsobila detekci úniku kouře a až do vzdálenosti 2m od kamen. Optimální se ukázalo umístit detektor do vzdálenosti 2,5m. V této vzdálenosti již nedocházelo k planým poplachům a zároveň systém spolehlivě reagoval na vznik požáru (testováno pálením novin v hrnci na plátu kamen).

Posledním zásadním problémem bylo použití SIM karty s předplaceným kreditem. Při velkém množství falešných poplachů se velice rychle vybil kredit. Řešením je použití paušálu.

6.6 Úmyslné testy systému

Testy probíhaly v testovacím provozu v ordinaci. Cíleně bylo testováno na základě zkušeností s EZS.

6.6.1 Test napadení objektu cizí osobou:

V testu cizí osoba šla vstupními dveřmi. Při běžně rychlém pohybu reagoval systém ze 3 pokusů pokaždé spolehlivě. Při znalosti polohy čidla a pomalé chůzi podél zdi systém ze 3 pokusů pouze jednou nereagoval. Při tomto pokusu by se pachatel

nedokázal dostat k ústředně EZS, jelikož je stále hlídaná PIR senzorem. Výrobce udává dosah senzoru 10m. Testy bylo zjištěno, že účinný dosah je přibližně 6m. Od této vzdálenosti byla detekce již spíše otázkou náhody než pravidlem.

6.6.2 Test úniku plynu

Test byl vykonán tak, že senzor byl vzdálen od zdroje plynu nejdříve 15cm, přičemž reagoval do 5 sekund. Dále byl od zdroje plynu 50cm. S touto vzdáleností systém reagoval za 18 sekund. Velice důležité je umístění senzoru. Musíme si uvědomit, jaký plyn nám bude detektor hlásit, a podle toho senzor umístit.:

- Propan butan (LPG): Těžší než vzduch, klesá k podlaze;
- Zemní plyn (LNG, CNG): Lehčí než vzduch, stoupá ke stropu;
- Oxid uhelnatý (CO): Lehčí než vzduch, stoupá ke stropu;
- Etylen: Lehčí než vzduch, stoupá ke stropu.

6.6.3 Test detekce kouře

Test byl vykonán tak, že se místnost zakouřila zapálenými novinami. Kouř stoupal vzhůru. Senzor na něj reagoval za minutu a 32 vteřin Vzduch v místnosti byl však stále dýchatelný. Při přiložení doutnajících novin přímo k senzoru systém reagoval okamžitě do 10 sekund.

Závěr

Cílem práce bylo navrhnout a sestrojit zabezpečovací systém na platformě Arduino. Tento cíl byl rozdělen do několika podcílů, které byly postupně řešeny.

Prvním krokem k úspěšnému dokončení cíle byla analýza dostupných řešení od komerčních výrobců zabezpečovacího zařízení. Tento krok byl dokončen díky průzkumnému šetření v objektech. Byly určeny trendy v oblasti zabezpečení objektů, ze kterých se poté vycházelo při návrhu vlastního systému.

Poté byl na základě této analýzy vytvořen návrh zabezpečovacího systému s možnostmi openhardware. Bylo zjištěno, s jakými problémy se můžeme následně při sestrojení systému potkat.

Následně bylo zařízení sestrojeno a testováno v praxi. Nejdříve byl systém sestrojen pouze do pokusné verze, během níž fungoval velice spolehlivě. Dále byl systém nasazen do pokusného režimu, a to nejprve v ordinaci praktického lékaře na dobu jednoho týdne. Při sestrojení se vyskytlo několik problémů s hlídáním stavů jednotlivých čidel a především s nevalnou kvalitou čínských detektorů. Tyto problémy byly vyřešeny.

Dále bylo zařízení testováno v rekreačním objektu, a to po dobu 3 měsíců. Při testování bylo zjištěno několik chyb, které byly způsobeny levnými a nekvalitními součástkami. Řešením je koupit dražší a kvalitnější. Veškeré problémy, které vznikly při testovacím provozu, byly vyřešeny.

Dalším cílem bylo zjistit, jestli je platforma Arduino vhodná pro zabezpečovací systémy. Na základě veškerých zkušeností bylo zjištěno, že je vhodnější použít již zavedený systém. Tento systém je odladěn a systém založený na Arduinu se mu může maximálně přiblížit.

Budoucnost tohoto projektu autor práce vidí v rozšíření o funkce „inteligentního domu“. Arduino se jeví jako vhodná volba pro ovládání např. klimatizace přes GSM síť. Celý systém by bylo vhodné připojit na internet a posílat upozornění místo GSM sítí prostřednictvím SMTP brány a GSM síť mít pouze jako zálohu. Dále by tento inteligentní dům mohl mít ovládací webové rozhraní, kde by uživatel viděl stav

veškerých svých čidel a zároveň mohl ovládat některé funkce z kteréhokoliv zařízení připojeného do sítě internet.

Seznam použité literatury

[1] *Elektroinstalace: Zabezpečovací systémy EZS* [online]. [cit. 2012-05-22]. Dostupné z WWW: <http://www.elreko.cz/index.php?co=4&pg=sub>.

[2] UHLÁŘ, Jan. *Technická ochrana objektů*. 1. vyd. Praha: Policejní akademie České republiky, 2001, 205 s. ISBN 80-725-1076-2.

[3] KŘEČEK, Stanislav. *Příručka zabezpečovací techniky*. 2. vyd. S.l.: Cricetus, 2003, 351 s. ISBN 80-902-9382-4.

[4] Zabezpeceni-alarmy.cz. *Kouřový senzor Jablotron. DD Technik* [online]. 2014 [cit. 2015-04-16]. Dostupné z WWW: <http://www.zabezpeceni-alarmy.cz/p/4683-JA-150ST-Bezdratovy-kombinovany-detektor-koure-a-teploty/?rid=bot_rid_g>.

[5] Zabezpeceni-alarmy.cz. *JA-180G Bezdrátový detektor úniku plynu. DD Technik* [online]. 2014 [cit. 2015-04-20]. Dostupné z WWW: <http://www.zabezpeceni-alarmy.cz/p/4684-JA-180G-Bezdratovy-detektor-uniku-plynu/?kamid=303&prk=1>.

[6] Schirrmacher-sicherheitstechnik. *Kölner Studie 2011* [online]. 2011 [cit. 2015-04-20]. Dostupné z WWW: <http://www.schirrmacher-sicherheitstechnik.de/koelner_studie.pdf>.

[7] Milan Jindra zabezpečovací systémy. *Bezdrátový detektor DCT10-433/868* [online]. 2014 [cit. 2015-04-20]. Dostupné z WWW: <http://jindra-alarmy.cz/eshop/paradox-a-ostatni-ezs/systemy-spectra-magellan/bezdratove-prvky-mg/dct10-433-868>.

[8] Milan Jindra zabezpečovací systémy. *Bezdrátový detektor WH588P-868* [online]. 2014 [cit. 2015-04-20]. Dostupné z WWW: <http://jindra-alarmy.cz/eshop/paradox-a-ostatni-ezs/systemy-spectra-magellan/bezdratove-prvky-mg/wh588p-868>.

[9] Česká asociace hasičských důstojníků. *Statistika úniků nebezpečných plynů v České republice* [online]. 2011 [cit. 2016-04-19]. Dostupné z WWW: <http://www.cahd.cz/?page_id=1234>.

[10] Město Olomouc. *Krádeže vloupáním do rekreačních objektů* [online]. 2013 [cit. 2016-04-19]. Dostupné z WWW: <http://zpravodajstvi.olomouc.cz/clanky/Chaty-a-

chalupy-jsou-pro-zlodeje-neodolatelne-lakave-Dukladne-si-je-zazimujte-varuje-policie-i-pojistovny-21376>.

[11] Jablotron. *Jablotron JA-100* [online]. 2015 [cit. 2016-04-20]. Dostupné z WWW: <http://www.jablotron.com/cz/alarmy/jablotron-100/>.

[12] Cdn-reichelt.de. *Arduino mega* [online]. 2015 [cit. 2016-04-20]. Dostupné z WWW: <http://cdn-reichelt.de/bilder/web/xxl_ws/A300/ARDUINO_MEGA.png>.

[13] HW.cz. *Blokové schéma PIR čidla* [online]. 2015 [cit. 2016-04-20]. Dostupné z WWW: <http://www.hw.cz/files/styles/full/public/story/9417/blokoveschemapircidla 1.jpg>.

[14] Attie.co.uk. *XBEE1* [online]. 2015 [cit. 2016-04-20]. Dostupné z WWW: <http://doc.libxbee.attie.co.uk/images/xbee1.jpg>.

Seznam tabulek

Seznam grafů

Seznam schémat

Seznam obrázků

Seznam příloh

Příloha A – Slovník zkratek a pojmů

Příloha B – Obsah přiloženého CD

- Text diplomové práce ve formátu pdf
- Zdrojový kód Arduino

Přílohy

Příloha A

Slovník zkratek a pojmů

EZS	elektronický zabezpečovací systém
GSM	globální systém pro mobilní komunikace
NFC	rádiová bezdrátová komunikace na krátkou vzdálenost
UTP	nestíněný datový kabel
FTP	stíněný datový kabel
I2c	sériová sběrnice používaná k připojování nízkorychlostních periferií
LTE	technologie bezdrátového přenosu dat
IR	infračervené záření
LCD	displej z tekutých krystalů
LED	dioda emitující světlo
PC	osobní počítač
PCO	pult centrální ochrany
PIR	detektor vyzařující infračervené záření
SMS	textová zpráva