VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA STROJNÍHO INŽENÝRSTVÍ
FACULTY OF MECHANICAL ENGINEERING

ÚSTAV AUTOMATIZACE A INFORMATIKY
INSTITUTE OF AUTOMATION AND COMPUTER SCIENCE

DOMOVNÍ ZABEZPEČOVACÍ SYSTÉM

HOME SECURITY SYSTEM

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — Marek Martínek
AUTHOR

VEDOUCÍ PRÁCE — Ing. Daniel Zuth, Ph.D.
SUPERVISOR

BRNO 2018

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA STROJNÍHO INŽENÝRSTVÍ

Zadání bakalářské práce

Ústav:	Ústav automatizace a informatiky
Student:	**Marek Martínek**
Studijní program:	Strojírenství
Studijní obor:	Základy strojního inženýrství
Vedoucí práce:	**Ing. Daniel Zuth, Ph.D.**
Akademický rok:	2017/18

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 o vysokých školách a se Studijním a zkušebním řádem VUT v Brně určuje následující téma bakalářské práce:

Domovní zabezpečovací systém

Stručná charakteristika problematiky úkolu:

Bakalářská práce bude zahrnovat rešerši problematiky mikrokontrolérů a snímačů použitelných v domácím zabezpečovacím sytému. Po rešeršní části bude vybráno jednoduché řešení, které bude otestováno pro možné použití v oblasti zabezpečení majetku.

Cíle bakalářské práce:

Shrňte požadavky na domácí zabezpečovací systém.
Popište stávající řešení systémů dostupných na trhu.
Popište mikrokontroléry a snímače použitelné pro danou problematiku.
Sestavte a popište model (vývojový kit) jednoduchého zabezpečovacího systému.

Seznam doporučené literatury:

VODA, Z., tým HW Kitchen. Arduino - Průvodce světem Arduina. Nakladatelství Martin Stříž, Bučovice, 2015. 240 s. ISBN: 978-80-87106-90-7

MANN, Burkhard. C pro mikrokontroléry: ANSI-C, kompilátory C, spojovací programy - linkery, práce s ATMEL AVR a MSC-51, příklady programování v jazyce C, nástroje pro programování, tipy a triky .. Praha: BEN - technická literatura, 2003. µC & praxe. ISBN 8073000776.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2017/18.

V Brně, dne 27. 10. 2017

doc. Ing. Radomil Matoušek, Ph.D.
ředitel ústavu

doc. Ing. Jaroslav Katolický, Ph.D.
děkan fakulty

ABSTRAKT

Úvodní kapitoly této práce se věnují druhům ochrany objektů, popisují prvky zabezpečovacích systémů a druhy čidel, které se v systémech vyskytují. Další kapitoly se věnují detektorům jiných nebezpečí než je trestná činnost a řeší problematiku přenosu signálu. V závěru práce je prakticky řešen zabezpečovací systém pro dům či byt založený na open-sourcovém řešení ve vývojovém prostředí ARMmbed.

ABSTRACT

The introductory chapters of this work are dedicated to types of object protection, describe the elements of the security systems and the types of sensors that are present in the security systems. The next chapters deal with detectors of other hazards rather than crime and deal with the problem of signal transmission. At the end of the thesis, security system for house or apartment is solved, based on open-source solution in development environment ARMmbed.

KLÍČOVÁ SLOVA

Zabezpečovací systém, Ochrana majetku, ARMmbed, Mbed, NUCLEO-F401RE, Bezpečnostní senzory, GSM

KEYWORDS

Security system, Property protection, ARMmbed, Mbed, NUCLEO-F401RE, Security sensors, GSM

BIBLIOGRAFICKÁ CITACE

MARTÍNEK, M. *Domovní zabezpečovací systém.* Brno: Vysoké učení technické v Brně, Fakulta strojního inženýrství, 2018. 55 s. Vedoucí bakalářské práce Ing. Daniel Zuth, Ph.D..

PODĚKOVÁNÍ

Mé poděkování bych chtěl vyjádřit vedoucímu bakalářské práce Ing. Danielovi Zuthovi Ph.D. za odborné vedení, připomínky a rady. Rovněž bych chtěl poděkovat svým rodičům za podporu během studia.

ČESTNÉ PROHLÁŠENÍ

Prohlašuji, že tato práce je mým původním dílem, zpracoval jsem ji samostatně pod vedením Ing. Daniel Zuth Ph.D. a s použitím literatury uvedené v seznamu literatury.

V Brně dne 22. 5. 2018 ……

Marek Martínek

OBSAH

1 ÚVOD

Bezpečnost a ochrana majetku je priorita každé vyspělé společnosti. Riziko vloupání je reálnou každodenní hrozbou. Pro jakékoliv zabezpečení platí zásada, že je tak silné, jak silný je jeho nejslabší článek.

Počet vloupání a krádeží přibývá právě v období dovolených. Jen za rok 2016 řešila policie asi 7000 takovýchto případů. Za poslední roky se snížil počet vloupání dveřmi, ale zloději začali více využívat vstupy přes balkóny nebo terasy. Za rok 2016 přesahovaly škody způsobené loupežemi až 1,25 miliardy korun. [1]

Při využití integrovaného bezpečnostního systému můžeme docílit toho, že pachatele odradíme od zamýšleného činu nebo mu alespoň znesnadníme proniknutí do budovy.

Ochrana majetku a zdraví bude vždy nutná, může se jednat o preventivní ochranu, ale také o ochranu před nebezpečím. Každá investice do ochrany však musí být také předem dobře zvážena.

Při pojistné události bude pojišťovna zkoumat zabezpečení objektu a v případě, že zabezpečení nebude dostatečné, mohla by plnění krátit. Pokud zloděj nemusel překonat žádnou překážku, pojišťovna plnění odmítne. Při pojistných smlouvách nad 1 milion korun už pojišťovna žádá důkladnější zabezpečení objektu, které má pro pachatele i preventivní účinky. U bytů v přízemí s pojistkou nad 1 milion korun a u bytů v patře s pojistkou nad 2 miliony korun musí mít byt mechanické zajištění v kombinaci s elektronickým zabezpečovacím systémem. [2]

Policie České republiky na svých internetových stránkách také nabádá k používání zabezpečovacích systémů.

Cílem bakalářské práce je shrnout požadavky na domácí zabezpečovací systém a popsat stávající řešení systémů, které jsou na trhu dostupné. Popsat mikrokontroléry a snímače použitelné pro danou problematiku a sestavit jednoduchý model – vývojový kit jednoduchého zabezpečovacího systému.

Struktura bakalářské práce je členěna na teoretickou část a praktickou část. V teoretické části jsou pomocí odborné literatury popsány druhy ochrany objektů, prvky poplachových a zabezpečovacích systémů, rozdělení snímačů PZTS podle typu ochrany objektu a metody přenosu signálu.

V praktické části je popsán vývoj zabezpečovacího systému založeného na open-sourcovém řešení ve vývojovém prostředí Mbed na vývojové desce Nucleo F401RE.

Systém je navržen pro více sektorů, které pracují samostatně. První sektor zajišťuje venkovní okna a dveře domu, druhý sektor zajišťuje vnitřní prostory. Uvnitř domu byly použity kombinace různých senzorů pro zajištění lepších výsledků. Systém lze ovládat pomocí tlačítek uvnitř domu nebo dálkově pomocí SMS. GSM modul slouží jako forma upozornění v případě, že dojde k narušení objektu.

Celý systém je popsán v jednotlivých na sebe navazujících kapitolách a v závěru bude předvedena jeho funkčnost.

2 ROZDĚLENÍ DRUHŮ OCHRANY OBJEKTU

Pro navržení komplexního a účinného ochranného systému je potřeba provést několik kroků, které povedou ke zhodnocení situace a k navržení vhodného systému. Tyto kroky se skládají ze sběru informací a analýze známých a předpokládaných rizik, následuje bezpečnostní průzkum, nutné je také vzít v potaz působení místních vlivů a charakter daného majetku. Po vyhodnocení nasbíraných informací je na řadě zvolit vhodný typ fyzické ochrany a specifikovat všechna organizační a režimová opatření ochrany. Následuje výběr bezpečnostních technologií a jejich napojení na poplachové zabezpečovací a tísňové systémy. K zajištění komplexní ochrany je nutná kombinace fyzické i technické ochrany za pomoci prvků elektrických a mechanických zabezpečovacích systémů.

2.1 Fyzická ostraha

Fyzická ostraha je nejstarší a dodnes nejpoužívanější typ ochrany objektů. Nabízí různorodé typy ochrany jako ochrana vůči neoprávněnému vstupu, vandalismu, ochrana před únikem informací, krádeží či jinou majetkovou újmou. Dále může chránit před ohněm či jinými nežádoucími vlivy přírody. Podle důležitosti a významu může zabezpečení zajišťovat bezpečnostní dohled, strážní služba, ochranný doprovod, nebo příslušníci ozbrojených sil či zaměstnanci bezpečnostních služeb. [3]

2.2 Technická ochrana

2.2.1 Mechanické zábranné systémy

Mezi tradiční mechanickou ochranu patří bezpečnostní dveře, zámky, rolety, mříže a bezpečnostní skla. Dále zde řadíme automatická vrata, vjezdové závory, turnikety, bariéry proti vozidlům a oplocení. Mezi mechanické prvky ochrany patří také některé části samotných budov, jako obvodové zdi, stropy či podlahy.

Mechanické zábranné systémy nemůžou účinně sloužit jako jediná ochrana objektu, jelikož slouží zejména ke zpomalení pachatele při vniku do budovy. To umožní fyzické ostraze zorganizovat a provést patřičný zákrok. Volba materiálů a postupů použitých k výrobě mechanických zábranných systémů má zásadní vliv na odolnost vůči průniku. [3]

Dveře

Dveře patří statisticky k nejčastějšímu vniknutí pachatele do objektu. Jakožto dveře si musíme představit všechny jejich součásti jako dveřní křídlo, dveřní zárubně, uchycení dveří, ochranné kování i vlastní zámek.

Nejvhodnějším řešením je pořízení bezpečnostních dveří a bezpečnostní zárubně. Bezpečnostní zárubně jsou vyrobeny ze silných ocelových pásů nebo

ocelových profilovaných rámů zasazených pomocí kotevních čepů a háků hluboko do zdi, čímž chrání před vyražením zárubně ze zdi. Bezpečnostní dveře jsou souhrnem speciálních bezpečnostních, stavebních a technických prvků jako ocelový skelet dveří, vícero jistících bodů nebo zesílené ochrany zámku. [4]

Bezpečnostní folie na sklo

Mezi mechanické zábrany patří i bezpečnostní folie aplikovaná na prosklené plochy. Dle posudků Kriminalistického ústavu PČR lze bezpečnostní folii považovat za plnohodnotnou náhradu mříže nebo uzamykatelných rolet. Původně byly tyto folie vyvíjeny pro potřeby kosmických letů. Folie jsou silné 50 až 400 μm, čiré a naprosto průhledné s propustností světla kolem 90 %. Z bezpečnostního hlediska zpomaluje postup pachatele podobně jako mříže, zamezuje prohození těžkých předmětů skrz okno a zpomaluje šíření požáru. [4]

2.2.2 Poplachové zabezpečovací a tísňové systémy (PZTS)

PZTS se skládá z kombinace ústředny a čidel. Ústředna má za úkol zpracovat informace přenesené z čidel buďto bezdrátově nebo drátem. V případě narušení (spuštění čidla) může ústředna spustit alarm, kontaktovat monitorovací službu nebo například poslat SMS pomocí GSM modulu a informovat tak o tom, že došlo k narušení.

Jednotlivé prvky systému (čidla) dělíme na prostorové, plášťové a předmětové. Prostorovými čidly rozumíme takové, které mají za úkol detekovat osoby pohybující se ve vymezeném prostoru. Příkladem jsou PIR detektory, mikrovlnné detektory, magnetické detektory, infračervené závory nebo detektory tříštění skla. Prvky plášťové ochrany můžou být např. magnetické detektory instalované do stavebních otvorů (okna, dveře) a detektory tříštění skla. Předmětová ochrana řeší ochranu cenného majetku nebo zařízení (obrazy, šperky, starožitnosti) pomocí detektorů otřesu, tlaku, náklonu atp. Vhodná je také kombinace s dalšími technickými prostředky, jako jsou požární čidla, kamerové systémy nebo systémy kontroly vstupu osob. [5]

2.2.3 Perimetrická ochrana

Pro zajištění kompletní ochrany je nutno zavést také perimetrickou ochranu. Tento typ ochrany je nedílnou součástí zejména průmyslových, komerčních a veřejných prostor, uplatnění ale nachází také v ochraně soukromých sídel atp. Perimetrická ochrana má za cíl buďto odradit narušitele (například zvuková nebo světelná siréna) nebo poskytnout čas pro ochranné složky ještě před tím, než dojde k proniknutí do hlídaného objektu.

Mezi nejpoužívanější prvky perimetrické ochrany patří infračervené závory, mikrovlnné bariéry, duální bariéry, což je kombinace dvou předchozích nebo také plotové detekční systémy a zemní detekční kabely. Vzhledem k hlídanému prostoru je třeba vybrat vhodnou kombinaci těchto prvků tak, aby byl co nejvíce omezen počet planých poplachů. [3]

2.3 Režimová opatření

Režimovým opatřením se rozumí soubor pravidel a postupů k zajištění požadovaného stupně bezpečnosti, v závislosti na funkci zabezpečovacích systémů a požadovaných zásadách. Cílem režimových opatření je stanovit pravidla pro vstup, pohyb a odchod osob, a to jak zaměstnanců, tak i návštěv. Dále řeší podmínky pro vnášení a vynášení věci do objektu, manipulaci s klíči a s dalšími identifikačními prostředky. Pro správné fungování ochrany objektu je nutno tyto směrnice prosazovat na každodenní bázi. [3]

3 PRVKY POPLACHOVÝCH ZABEZPEČOVACÍCH A TÍSŇOVÝCH SYSTÉMŮ

3.1 Ústředna PZTS

Jedná se o zařízení, které má za úkol přijímat a vyhodnocovat příchozí signály z čidel PZTS, napájet jednotlivé segmenty PZTS a ovládat zařízení, které mají za úkol signalizovat, zapisovat či jinak oznamovat narušení. Ústředna je vybavena klávesnicí a displejem, které slouží k uvedení jednotlivých částí nebo celého systému PZTS do stavu střežení či stavu klidu. Dále by měla ústředna poskytovat možnost provádět diagnostiku systému PZTS. V praxi se setkáváme s různými řešeními lišícími se elektronikou, programováním, vstupně výstupním rozhraním apod.

3.1.1 Smyčkové ústředny

Pro každou poplachovou smyčku má ústředna vstupní vyhodnocovací obvod. Každá smyčka je zakončena zakončovacím odporem, tak aby vykazovala předepsanou hodnotu odporu pro konkrétní ústřednu nebo pro její daný typ. Změna odporu ve smyčce vyvolaná aktivací některého ze zapojených čidel vede k vyhlášení poplachu. Nejčastějším zapojením poplachových smyček je sériové zapojení rozepínacích kontaktů čidel. Počet čidel ve smyčce je limitován typem ústředny. PZTS systém se smyčkovou ústřednou vyžaduje rozsáhlou kabelovou síť. Ke každému čidlu je třeba přivést dva vodiče pro napájení, dva vodiče pro poplachový kontakt čidla a další volitelnou kabeláž. Tou můžou být dva vodiče sabotážního kontaktu čidla a další dva vodiče dodatečných funkcí čidla, jako například paměť poplachu či připojení různých částí čidel jako ultrazvukový či mikrovlnný vysílač. [6]

3.1.2 Ústředny s přímou adresací čidel

Komunikace mezi ústřednou a čidlem probíhá po datové sběrnici. Ústředna periodicky generuje adresy pro jednotlivá čidla a přijímá příslušné odezvy. Každé čidlo musí být vybaveno komunikačním modulem. Výhodou je jednodušší kabelová síť s libovolnou konfigurací kabelové sítě a libovolným pořadím zapojení čidel. Nejčastějším zapojením je do čtyřvodičového vedení, dva vodiče slouží pro napájení čidla a další dva jako datová sběrnice. Při narušení objektu ústředna ohlásí, které konkrétní čidlo zaznamenalo narušení a o jaký typ narušení se jedná. [6]

Jednou z nevýhod tohoto řešení je celková délka vedení a možnost indukce elektrického napětí. Při navrhování projektu je nutné brát také v potaz odběr jednotlivých částí sítě a počítat s úbytky napětí na napájených vodičích.

3.1.3 Ústředny smíšeného typu

Jedná se o kombinaci obou předchozích typů ústředen. Datová komunikace pracuje na principu ústředna – koncentrátor. Mezi koncentrátorem a ústřednou probíhá

komunikace po analogové nebo datové sběrnici, zatímco čidla jsou připojena ke koncentrátorům pomocí smyček. Koncentrátory tedy slouží jako analogové ústředny shromažďující informace z detektorů připojených do proudových smyček a následná komunikace mezi ústřednou a koncentrátory probíhá pomocí datové sběrnice, na podobném principu jako u ústředen s přímou adresací čísel. [6]

Mezi výhody tohoto zapojení patří napájení z jednoho zdroje, včetně záložního. Tím odpadá potřeba měnit baterie v čidlech, což maximalizuje bezúdržbovost systému. Oproti bezdrátovému přenosu disponuje toto řešení velmi vysokou odolností vůči rušení. Snazší je také diagnostika problémů mezi jednotlivými prvky a ústřednou.

Mezi nevýhody se řadí vyšší náročnost montáže spojená i s vyšší pořizovací cenou. Obecně je toto řešení vhodné pro zabezpečení větších komplexů.

3.1.4 Ústředny s bezdrátovým přenosem

U ústředen s bezdrátovým přenosem je kabelová datová sběrnice nahrazena rádiovým signálem v pásmu 433 MHz a 868 MHz. Ve většině případů je přenos poplachového signálu čidla 8 bitový s 4 bitovou adresou čidla. Přenos je kódovaný a duplexní (čidlo i ústředna fungují jako vysílač i přijímač).

Výhodou řešení je snadná montáž do již existujících prostor s minimem technologických zásahů. Přenosový dosah činí 100 až 200 m v otevřeném prostoru, uvnitř budov méně. Další z předností je také jednoduchá rozšiřitelnost o další čidla a menší náchylnost na fyzické útoky. Mezi nevýhody se řadí náchylnost na rušení signálu, a to jak záměrně, tak i nechtěně interferencí s ostatními zařízeními. Nutná je také údržba ve formě výměny baterií. O upozornění na potřebnou výměnu se stará konkrétní čidlo. [6]

3.1.5 Hybridní ústředny

Poslední možností jsou hybridní ústředny spojující možnosti již uvedených řešení. Podle konkrétní aplikace lze zvolit, kam umístit čidla bezdrátové a kde prostředí naopak umožňuje zavést připojení drátové.

3.2 Rozdělní snímačů PZTS podle typu ochrany objektu

3.2.1 Prvky plášťové ochrany

Magnetické kontakty

Jedná se o velice jednoduchý a účinný typ spínače. Vhodný je zejména pro veškeré vstupní otvory, jako jsou dveře či okna. Prvek je složen ze dvou částí, permanentního magnetu a snímací cívky. První polovina (magnet) je přimontována na křídle okna nebo dveří a druhá polovina (snímací cívka) je pevně přimontována na rám okna nebo dveří, tak aby k sobě v zavřeném stavu doléhaly. V momentě, kdy dojde k oddálení magnetu od cívky, dojde k rozepnutí/sepnutí a spuštění poplachu. [3]

Čidla na ochranu skleněných ploch

Tento typ čidel zaznamenává zvuk charakteristický pro tříštění, řezání nebo lámání skla. Umisťuje se přímo na skleněnou plochu s cílem co nejvíce snížit ztráty při přenosu zvuku. Tento typ čidla nazýváme kontaktní. Vlnění vzniklé při narušení skleněné plochy je vyhodnoceno elektronikou čidla a dochází k rozepnutí kontaktu relé zapojeného do poplachové smyčky. Čidlo je vhodné zejména pro střežení neotevíratelných skleněných ploch, dosah čidla činí přibližně 1,5 až 3 metry. [3]

Drátová čidla a rozpěrné tyče

Vhodné pro hlídání vstupů do inženýrských sítí jako například ventilace. Funguje na principu rozpojení mechanického spínače nebo přetržení ocelového lanka.

3.2.2 Prvky prostorové ochrany

Pasivní infračervená čidla (PIR)

PIR čidla fungují na principu zachycování změn vlnových délek v infračerveném spektru. Hlídaná oblast je rozdělena do několika zón, kde každá zóna měří hodnoty infračerveného záření (IR). Pokud je senzor v klidu, jsou naměřené hodnoty infračerveného záření v každé zóně stejné. V momentě, kdy do sledovaného prostoru vstoupí objekt o jiné teplotě než jaká je teplota okolí, například člověk nebo pes, dojde k pozitivní změně mezi jednotlivými zónami. Po opuštění prostoru dojde k opaku a senzor generuje negativní změnu. Takto zaznamenané pulzy jsou vyhodnoceny jako pohyb. Nevýhodou tohoto typu senzoru je náročnost na jeho umístění. Je totiž nutné, aby v zorném poli nebyl jiný zdroj tepla, jako například radiátor nebo kamna. Dále na senzor nesmí dopadat přímé ani odražené světelné záření. [7]

Mikrovlnná čidla (MW)

Mikrovlnný senzor používá dopplerovský radar k detekci pohybujících se objektů za pomoci mikrovlnného záření. Funguje na principu přijímání odražených mikrovlnných vln. Pokud se vysílané vlnění odráží od nepohyblivých předmětů je výsledná interference vzniklá složením vysílaného a přijímaného vlnění konstantní. Při odrazu od pohybujícího se objektu dochází ke změně odraženého vlnění a změně interferenční frekvence. [8]

Výhodou MW čidla je schopnost detekovat i neživé předměty. Není navíc závislé na teplotě, vlhkosti či hluku v okolí, a ani na světelných podmínkách. Záření není škodlivé pro člověka, nicméně je nebezpečné pro kočky, ptáky a myši.

Ultrazvukové čidla

Ultrazvukové čidla fungují na podobném principu jako čidla mikrovlnná. Jak již název napovídá, hlavním rozdílem je použití ultrazvuku. Pracovní frekvence těchto čidel se nachází mezi 20–45 kHz, pro člověka již v neslyšitelném pásmu zvuku. Čidlo vysílá zvukové vlny a přijímá odražené vlnění. Čidlo zároveň měří dobu mezi vysláním vlny a jejím přijetím, čímž je schopno dopočítat přesnou vzdálenost předmětu před čidlem. Vhodná instalace těchto čidel je ve směru nebo proti směru pohybu případného narušitele. Je nutné brát v potaz také prostory, ve kterých budou tyto čidla použita.

Předměty absorbující zvuk (koberce, pěnové materiály) mají nežádoucí vliv na citlivost senzoru. Dále je nutné se vyvarovat prostorům s proměnlivými vlastnostmi vzduchu. Průvan vlhkost či teplota můžou vytvářet neviditelné a pro ultrazvuk neprostupné bariéry. [9]

Kombinovaná (duální) čidla

K odbourání nedostatků jednotlivých čidel, se v dnešní době používají duální čidla. Funkce těchto čidel je založena na pravděpodobnosti, že nedojde k falešnému poplachu dvou či více senzorů pracujících na různých fyzikálních principech.

V praxi se nejčastěji setkáváme s kombinací PIR + MW, dále méně častou kombinací PIR + US nebo PIR + detektor tříštění skla. Výstupní informace jsou zpracovány a poplach je vyhlášen pouze v případě, že poplachový signál obou čidel bude spuštěn současně či v daném časovém intervalu. Při instalaci je však nutné přihlížet na obě složky čidla samostatně.

3.2.3 Prvky perimetrické ochrany

IR závory a bariéry

IR závory pracují na principu přenosu infračerveného záření mezi vysílačem a přijímačem. Mezi těmito komponenty probíhá jeden nebo více IR paprsků. V případě, že dojde ke ztrátě nebo změně příchozího signálu (přerušení paprsku), spustí se alarm. Dosah čidel je v rozmezí 50–150 m. [10]

Nevýhodou tohoto systému je obtížná montáž a vysoké nároky na terén. Ten musí být ideálně úplně rovný bez žádných terénních překážek (stromy, keře). Správná činnost může být také ovlivněna zhoršením klimatických podmínek jako je padající sníh či mlha. Nutná je také pravidelná údržba.

Mikrovlnné bariéry

V prostoru mezi vysílačem a přijímačem vzniká elektromagnetické pole. Při vniknutí objektu do magnetického pole dochází k narušení vlnění, čímž dojde k vyvolání poplachu. Dosah těchto čidel se nachází v rozmezí 200 až 300 metrů.

Oproti infračerveným závorám nabízí mnohem vyšší odolnost vůči povětrnostním vlivům. Občas dochází k reakci na pohyb mimo střežené pásmo, tudíž je vhodné, aby v blízkosti bariéry nebyly žádné stromy ani keře. [11]

Štěrbinové kabely

Jedná se o dvojici koaxiálních kabelů položených pod povrchem. Jeden kabel vytváří a vyzařuje elektromagnetické pole, zatímco druhý kabel změny pole vyhodnocuje. Při změně v elektromagnetickém poli dojde k vyhlášení poplachu.

Výhodou je, že se nemusí jednat o rovné úseky, může kopírovat nerovnosti terénu i obvodové hranice objektu. Řešení je náchylné na silné zdroje elektromagnetického záření a zvěř. [12]

Zemní tlakové hadice

Základem jsou dvě přibližně jeden metr od sebe položené hadice napuštěné nemrznoucí kapalinou. Změna tlaku uvnitř hadic, která je vyhodnocována v diferenciálním tlakovém čidle, odešle poplachový signál.

Podobně jako u štěrbinových kabelů může tento systém libovolně kopírovat obvod hlídaného prostoru, další výhodou je možnost uložení i pod vozovku. [12]

3.2.4 Prvky předmětové ochrany

S předmětovou ochranou se setkáváme zejména ve veřejných prostorech (veřejnosti přístupné počítače a jiná výpočetní technika) nebo v muzeích, kde chráníme vystavované exponáty různého druhu. Nicméně využití můžeme najít i v soukromém sektoru, příkladem mohou být čidla sledující průnik do trezoru.

Chráněný majetek se může výrazně lišit hmotností (od několika gramů až po kilogramy) i velikostí a při kontaktu s předmětem může dojít k nenávratnému poškození. Proto existuje veliká škála senzorů a čidel, jako například čidla otřesová, polohová, kapacitní, závěsová nebo váhová. [13]

3.2.5 Ochrana proti ostatním vlivům

Vnější narušitel není jediným nebezpečím, se kterým musíme počítat při návrhu komplexního řešení ochrany našeho majetku. Jedním z největších nebezpečí, které může ohrozit majetek i samotný život je vznik požáru. Ten může vzniknout prakticky kdekoli a včasný zákrok je klíčový k tomu, aby došlo k zabránění či alespoň omezení vzniku škody. Způsobů vzniku požáru je spousta, od vady elektrospotřebiče či jiné elektroinstalace až po hořící svíčku, plynový vařič nebo nedopalek od cigarety. Tudíž je vhodné zvážit instalaci tohoto typu ochranného zařízení do všech prostor domu.

Dalším nebezpečím, které může ohrozit především lidský život je únik plynu. Tady již lze omezit prostory potřebné ke sledování pouze na několik míst, jako je kuchyň či prostor s plynovým kotlem.

Požární hlásiče

Zpravidla se jedná o jednoduché autonomní zařízení, kdy v jedné krabičce jsou obsaženy veškeré komponenty potřebné pro detekci kouře a vyvolání poplachu. Hlásiče požáru jsou autonomní, tudíž dokáží fungovat nezávisle na ostatních zdrojích energie, nejčastěji jim stačí obyčejné baterie.

Vhodným místem k instalaci požárního hlásiče je centrální část domu vedoucí k východu z domu nebo podobné prostory, kde se střetává více východů z jednotlivých místností. Optimálním řešením ale zůstává instalace požárního hlásiče do každé obytné místnosti. Nevhodné místa pro instalaci jsou pak prostory blízko ventilátorů, svítidel či jiných zdrojů tepla a prostory prašné či velmi vlhké (např. koupelna). [6]

Pokročilejší funkce hlásiče požáru nabízí možnost propojení vícero hlásičů tak, aby při detekci požárů došlo k aktivaci poplachu na všech zařízeních. Dále se naskytuje

možnost propojení požárních čidel s PZTS nebo automatickým telefonním volačem, aby došlo k uvědomění majitele nebo konkrétních bezpečnostních složek.

Detektory hořlavých plynů

Nejčastějším plynem, který vzniká při spalování v krbu nebo kotli je oxid uhelnatý (CO). Jedná se o toxický plyn pro člověka nepostřehnutelný čichem, chutí ani zrakem. Vzniká nedokonalým spalování paliv na bázi uhlíku, v domácnosti zejména zemního plynu. Nebezpečí vzniká zejména při špatném odtahu kouřových zplodin, kdy zplodiny zůstanou uvnitř místnosti a postupně vytlačí dýchatelný vzduch.

Existuje mnoho různých způsobů měření přítomnosti plynů, jako například katalytické čidla, polovodičové čidla, infračervená čidla, elektrochemické čidla, ionizační čidla nebo čidla využívající teplotní vodivosti plynů. Nejčastějším čidlem používaným v detektorech dostupných v České republice jsou čidla katalytické, které funguje na principu katalytického spalování hořlavého plynu. Tím dochází ke změně odporu na žhavém odporovém tělísku, což vyvolá poplach. [14]

Tak jako u požárních hlásičů můžou detektory hořlavých plynů fungovat samostatně nebo být propojeny s PZTS.

4 METODY PŘENOSU SIGNÁLU

4.1 Bezdrátový přenos

Užívání bezdrátových zařízení krátkého dosahu je v České republice upraveno všeobecným oprávněným č. VO-R/10/11.2016-13.

V dnešní době ještě stále často používaným pásmem je frekvence 433 MHz u zařízení do výkonu 10 mW. Toto pásmo je vhodné pro zařízení komunikující na krátké až střední vzdálenosti, tedy do 300 m. Nevýhodou tohoto pásma je jeho zahlcení a vysoká pravděpodobnost rušení. Pásmo je totiž volně k dispozici například pro radioamatérství, vysílačky a dětské chůvičky. [15]

Pásmo 868 až 870 MHz je rezervováno výhradně pro poplachová zařízení o maximálním výkonu 25 mW. Dosah těchto zařízení je až 500 m, tudíž se jedná o zařízení se středně velkým dosahem. [16]

Setkat se můžeme také se zařízeními komunikujících na frekvenci 2,4 GHz. Tato frekvence je nicméně velmi zatížená bezdrátovým internetem, Bluetooth, nebo dalšími zařízeními jako jsou například bezdrátové kamery. Navíc tato zařízení spotřebují mnohem více energie k zajištění stejných výsledku, čímž značně zkracují životnost baterie.

4.1.1 GSM

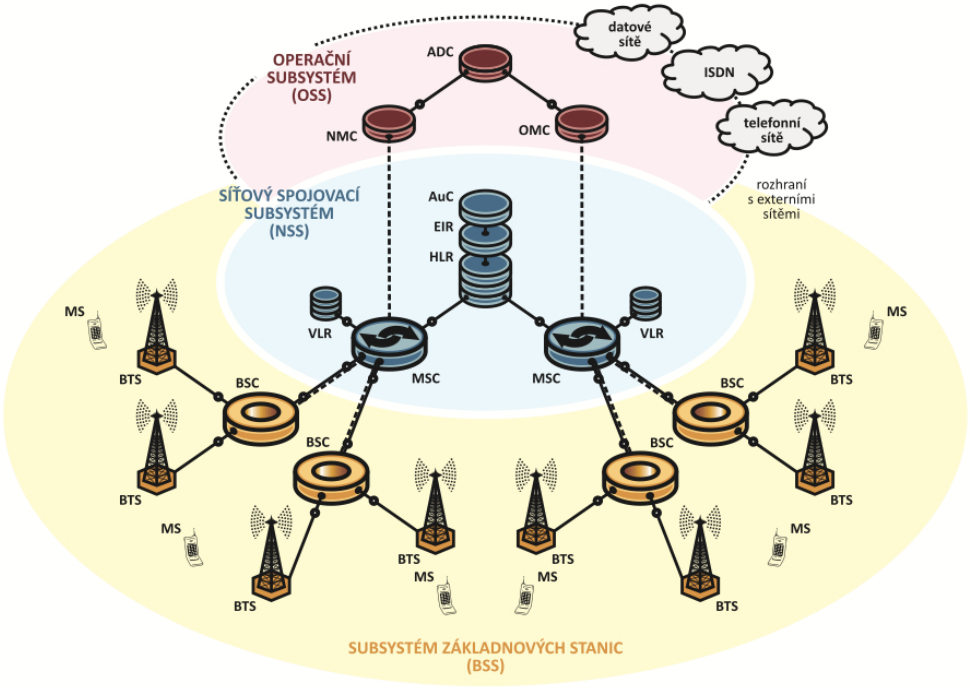
GSM - Globální systém pro Mobilní komunikaci, původně z francouzského Groupe Spécial Mobile. Původně vznikl jako evropský standard pro mezinárodní komunikaci na celulární bázi v kmitočtovém pásmu 900 , s cílem vytvořit mezinárodní roaming, přičemž se s postupem času rozšířil do celého světa. S rozvojem a rozšířením služby postupně vznikly další dva standardy GSM 1800 a 1900, pracující v pásmech 1800 MHz a 1900 MHz. Tyto nové standardy nevznikly jako náhrada, nýbrž jako rozšíření tak aby bylo možno obsloužit co nejvíce uživatelů. [17]

Architektura sítě GSM se skládá z několika základních částí – operační subsystém OSS, síťový spojovací subsystém NSS, subsystém základových stanic BSS a na úplném konci (začátku) mobilní stanice MS. Mobilní stanice je dále rozdělena na dvě části, na mobilní zařízení a SIM kartu. SIM karta slouží jako identifikátor účastníka v síti GSM. Vložením SIM karty do mobilního zařízení dojde k registraci účastníka do sítě GSM. Mezinárodní identifikátor mobilního účastníka IMSI, je uložen uvnitř SIM karty a slouží k identifikaci účastníka v síti GSM. Mezi další funkce IMSI patří lokalizace účastníka v domácím registru (HLR) dané oblasti, nalezení a zahájení hovoru mezi účastníky nebo vyúčtování za využívané služby. [18,19]

Komunikace mezi mobilní stanicí a základní vysílací stanicí probíhá za pomocí rádiových vln. Základní vysílací stanice slouží ke zpracování příchozích a odchozích přenosů ve vrstvě rádiových vln na data, které dále předává řídicí základové jednotce (BSC). Ta se stará o přidělování a uvolňování rádiových kanálů pro komunikaci

s mobilními stanice. Data z BSC jsou přeneseny do mobilních spínacích ústředen (MSC), kde je řešeno spojování hovorů mezi jednotlivými uživateli. [18,19]

Nad fyzickou vrstvou ústředen a vysílacích stanic je operační subsystém. Ten zabezpečuje provoz subsystému BSS a NSS. Dále zajišťuje administrativu (poplatky za užívání, vyúčtování a podobně). Dalším blokem je centrum řízení sítě, které zajišťuje řízení toku informací v síti a nakonec provozní a servisní blok, řešící údržbu a provoz sítě. [17]



Obrázek 1 Architektura systému GSM [17]

Mezi základní služby poskytované sítí GSM patří: Telefonní hovory, nouzové hovory, krátké SMS zprávy (160 znaků), fax, skupinové hovory a nakonec asynchronní a synchronní přenos dat.

4.1.2 LORA

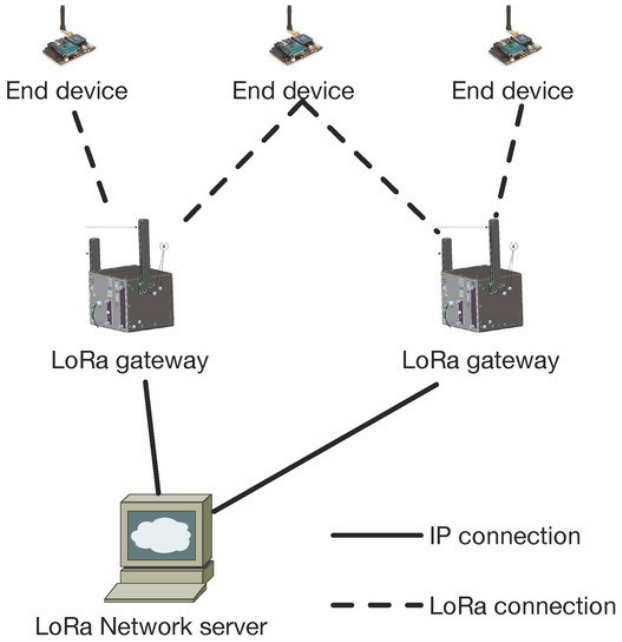
Technologie LoRa je bezdrátový komunikační systém s nízkou spotřebou, nízkým přenosem dat a dlouhým dosahem. Technologie cílí zejména na využití v oblasti Internetu věcí, ale také pro vzdálenou signalizaci a řízení zařízení, které budou používány na velké rozloze. Obecně takové sítě označujeme jako LP-WAN (Low Power – Wide Area Network). [20]

Pod pojmem LoRa se běžné označují dvě odlišné vrstvy a to fyzická vrstva využívající rádiovou modulační technologii Chirp a MAC protokol LoRaWAN.

Fyzická vrstva LoRa umožňuje komunikaci na velkou vzdálenost s minimálním odběrem energie a malým datovým tokem. Pracovní pásma jsou 433 MHz, 868 MHz

pro Evropu a 915 MHz pro Americký kontinent. Vzhledem k tomu, že modulační technologie je proprietárním vlastnictvím společnosti Semtech, jsou dostupné informace velmi omezené. [20]

Zbytek komunikačního protokolu LoRaWAN je na rozdíl od LoRa otevřený. Každé koncové zařízení má vlastní jedinečný identifikátor, což umožňuje velkému počtu koncových zařízení komunikovat s bránou za pomocí modulace LoRa. Protokol LoRaWAN je navržený zejména pro senzorické sítě, kde je výměna dat mezi serverem a senzory minimální a ve velkých intervalech (v řádu jednotek přenosů za hodinu až dny). [21]



Obrázek 2 Architektura sítě LoRa [21]

Síť LoRa využívá hvězdicové topologie a skládá se ze třech základních částí:

- Koncové zařízení – senzory s nízkou spotřebou komunikující za pomoci LoRa
- Brána – zařízení, které přenáší pakety z koncových zařízení na síťový server za pomocí technologií s větší propustností dat, například Ethernet nebo 3G. Vícero bran může přijímat a dál odesílat pakety ze stejného koncového zařízení.
- Síťový server – stará se o deduplikaci a dekódování paketů z koncových zařízení a generuje a posílá zpět odpověď koncovým zařízením [21]

4.1.3 Bluetooth LE

Bluetooth Low Energy, je technologie pro přenos dat na krátkou vzdálenost vyvíjená skupinou Bluetooth Special Interest Group. Stěžejní vlastností oproti klasické technologii Bluetooth je velmi nízká spotřeba energie. Technologie používá stejné frekvenční pásmo 2.4 GHz. Maximální přenosová rychlost činí až 2 Mb/s s maximálním

výkonem 100 mW. Vhodné využití technologie je pro zařízení, které komunikují pouze ojediněle nebo v krátkých sekvencích. Technologie je schopná komunikovat s většinou smart telefonů. Další využití se nachází ve zdravotnických a sportovních zařízeních, chytrých domácnostech a v bezpečnostních systémech. [22]

4.1.4 NB-IoT

Jedná se o bezdrátovou úzkopásmovou LPWA (low power wide area) technologii vyvinutou speciálně pro Internet věcí. Na rozdíl od ostatních IoT technologií pracuje NB-IoT v licencovaném frekvenčním pásmu. Z toho plyne její největší výhoda a to možnost nasazení v pásmech GSM a LTE. K nasazení NB-IoT byly vytvořeny 3 možnosti: Nahrazení původního nosiče GSM, nosičem NB-IoT (výhodné zejména v oblastech kde je k dispozici pokrytí GSM i LTE), dále flexibilním přidělením jednoho 180KHz bloku uvnitř pásma LTE nebo nasazením v nevyužitém ochranném pásmě na hranicích bloků LTE. [23]

Tento systém je založen na technologii LTE a tak i podporuje většinu funkcí LTE, přičemž byl zásadně zjednodušen a optimalizován tak aby došlo k co největšímu zjednodušení jednotlivých zařízení. Výsledkem jsou zařízení s velmi nízkou spotřebou energie, vysokou výdrží baterie a velmi nízkou pořizovací cenou. NB-IoT poskytuje vylepšené pokrytí uvnitř budov, maximální dosah až 15km a možnost připojit až 50 tisíc zařízení k jedné celulární buňce. [23]

4.1.5 Sigfox

Sigfox je bezdrátová komunikační technologie dlouhého dosahu až do vzdálenosti 50 km ve volném prostoru. Cílí na přenos malého množství dat v dlouhých či nepravidelných intervalech. Využití nachází zejména u zařízení kategorie IoT.

Tato technologie využívá tzv. UNB (ultra narrow band) pro přenos s modulací BPSK (binary phase shift keying) s přenosovou rychlostí 100bps. Využitím UNB dochází k efektivnímu využití přenosového pásma, minimálnímu rušení a ztrátám a nízké spotřebě. Navíc tato technologie poskytuje lepší citlivost při příjmu dat a tím snižuje výslednou cenu vynaloženou k výrobě dostatečné antény. Tak jako u NB-IoT má nosná vlna rozměr 200kHz s rozdílem toho, že ve veřejném pásmu o frekvenci 868MHz. [24,25]

Sigfox používá obdobnou technologii jako LoRa pro kontrolu spotřeby. Zařízení si samo vybírá kdy bude naslouchat. To je většinou v případě krátce po odeslání zprávy pro přijetí potvrzení nebo vykonání určité reakce. Spotřeba při přenosu je přibližně 30mA a v „off“ režimu v řádu jednotek nanoampér. Platí také, že čím menší je odeslaná zpráva tím menší i výsledná spotřeba. [24]

Sigfox může denně poslat maximálně 140 zpráv o velikosti 12 bajtů a 4 zprávy zpětně potvrzovací zprávy o velikosti 8 bajtů, což odpovídá přibližně 1 zprávě každých 10 minut. Technologie Sigfox je údajně schopná obsluhovat až milión zařízení v okruhu 30-50 km v otevřené krajině a 3-10 km ve městě. [25]

4.2 Drátový přenos

Systémy založené na drátovém přenosu dat mají velmi vysokou spolehlivost, jelikož nekomunikují pomocí rádiových vln, u kterých se můžeme setkávat s rušením. Pokud nedojde k porušení kabeláže je jen velmi nízká pravděpodobnost selhání v průběhu přenosu dat. Odolnost vůči napadení hackerem je také velice vysoká, jelikož je nutné, aby se dotyčný útočník fyzicky připojil ke kabelové síti. Oproti bezdrátovým řešením je údržba sítě minimální, není totiž třeba hlídat stav baterií jednotlivých senzorů. Drátové sítě dále nabízí možnost přenášet mnohem více dat, toto je zejména vhodné pokud jsou v systému zabudovány například IP kamery. Nejčastěji se s drátovým řešením setkáme ve firemním sektoru, kde je potřeba pokrýt velké prostory, nebo například u novostaveb.

Mezi nevýhody tohoto řešení patří právě složitá instalace, která může být u již stojících budov velmi náročná, jelikož je nutné kabeláž položit buďto pod podlahu nebo zabudovat do zdi. S tím jsou spojené i pravděpodobné vyšší náklady.

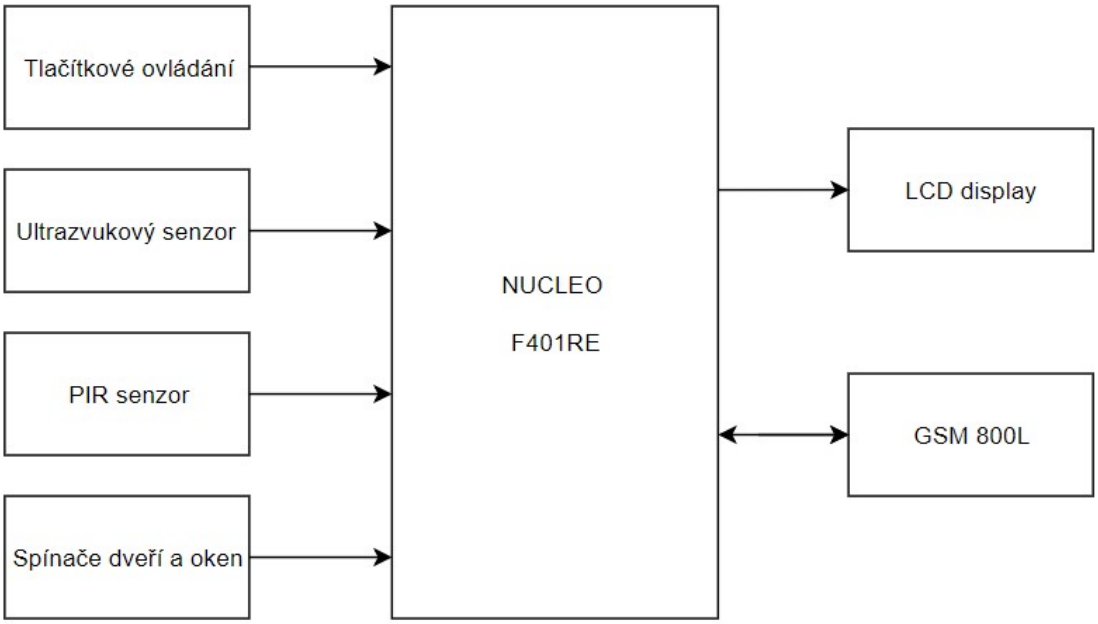
4.2.1 Ethernet

Mezi nejčastější řešení drátových systémů patří zapojení za pomoci Ethernetu. Ethernetový kabel nabízí jednak vysoký tok dat 100–1000 Mb/s na dlouhé vzdálenosti až 100 metrů a také funkci PoE – Power over Ethernet, čímž rozumíme napájení zařízení ze stejného kabelu. Kabely Cat5e umožňují napájení až 57V s odběrem do 100W. [26]

Připojení pomocí protokolu TCP/IP umožňuje bezpečný přenos dat, šifrování nebo například kontrolovat stav jednotlivých senzorů.

5 PRAKTICKÁ ČÁST

Cílem praktické části je vytvořit zabezpečovací systém pro dům či byt, založený na open-sourcovém řešení. Pro tento konkrétní příklad bylo vybráno vývojové prostředí Mbed a vývojová deska Nucleo F401RE.



Obrázek 3 Blokový diagram systému

Propojení jednotlivých zařízení a senzorů zabezpečovacího systému s ovládacím panelem bylo vytvořeno za pomocí vodičů. Mezi použité zařízení nezbytné pro funkční zabezpečovací systém patří PIR senzory, ultrazvukové senzory, spínače dveří a oken, display a GSM modul.

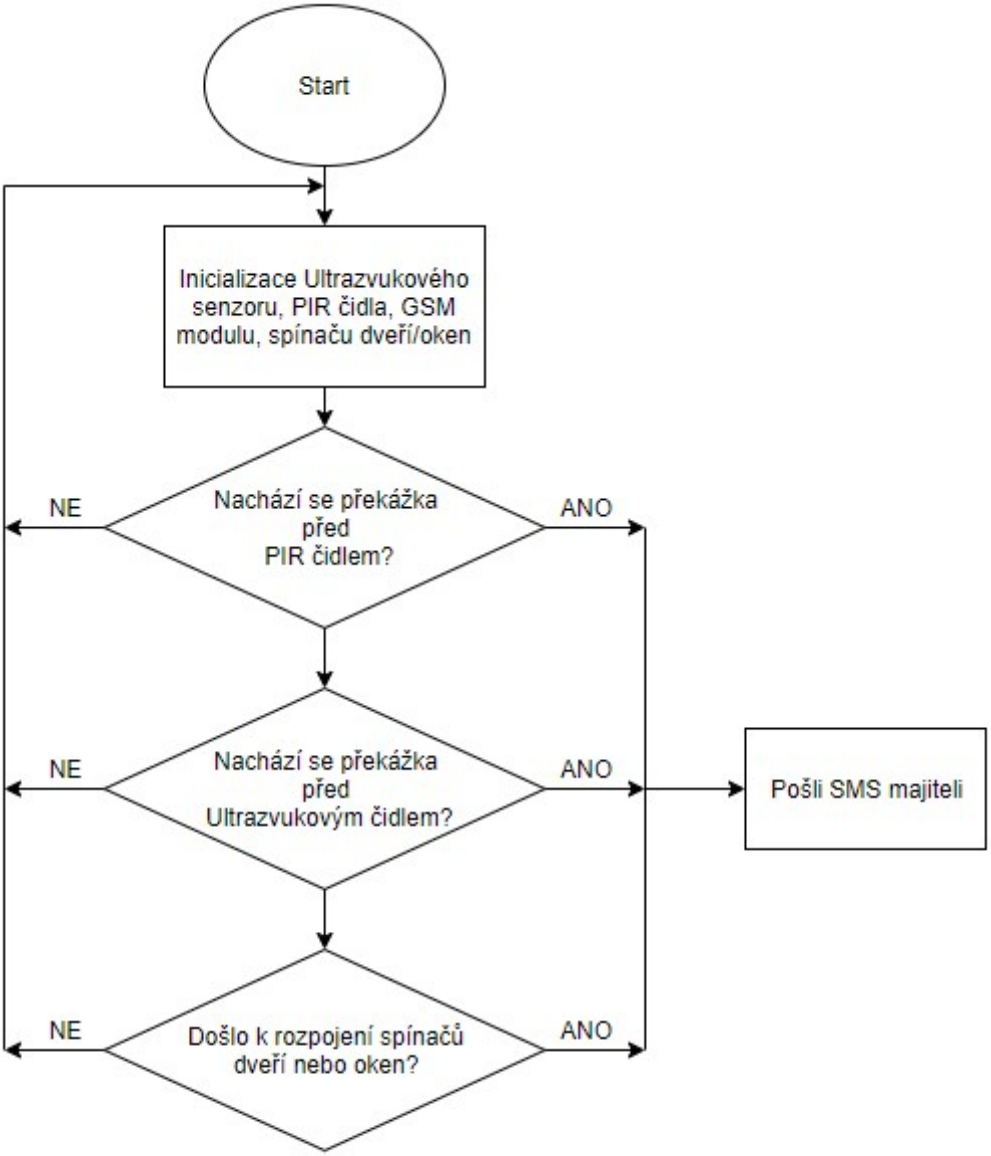
Systém se skládá ze dvou částí: hardware a jeho softwarové řešení. Cílem je, aby spolupracovaly při reakci na různé typy narušení uvnitř nebo v okolí domu.

Systém je navržen tak, aby byla možnost vytvořit více nezávislých sektorů ke sledování. Prvním sektorem je obvod (plášť) domu, zde patří zejména okna a dveře. K simulaci byly využity spínače ON/OFF místo reálně používaných magnetických spínačů. Principiálně se tyto spínače neliší. Pokud jsou spínače sepnuty, systém neeviduje narušení. V momentě rozepnutí (otevření okna nebo dveří) dojde ke změně logického stavu obvodu a situace bude vyhodnocena jako narušení domu.

Druhým sektorem jsou vnitřní prostory domu. Uvnitř domu jsou použity 2 typy senzorů a to PIR senzory a ultrazvukové senzory. Kombinací různých senzorů lze docílit jistějších výsledků.

Takovýmto způsobem lze vytvořit další samostatné sektory, jako například venkovní prostory nebo garáž.

K ovládání systému byly vytvořeny dva způsoby. Uvnitř domu lze zapínat či vypínat jednotlivé části systému pomocí tlačítek. Barevné LED diody indikují, jaké části domu jsou zabezpečeny. Součástí je také LCD display, na kterém se zobrazují informace o právě prováděných operacích. Na LCD displeji se také zobrazují informace, kde došlo k narušení v případě, že senzory zaznamenají pohyb. Druhou možností ovládání je pomocí SMS. Zasláním SMS lze na dálku vypnout či zapnout celý systém. GSM modul slouží také jako další forma upozornění v případě, že dojde k narušení. Odesílané SMS obsahují informaci o tom, jaký senzor byl aktivován.



Obrázek 4 Vývojový diagram navrhovaného systému zabezpečení domu pomocí detekce překážek nebo narušení pláště domu

5.1 Vývojová platforma Mbed

Vývojová platforma ARM Mbed IoT je plně integrované řešení pro správu a vývoj zařízení Internetu věcí. Platforma je založena na dvou základních produktech: software pro jednotlivé podporované zařízení a cloudové vývojové prostředí. Projekt je kolaborativně vyvíjen společností Arm®. [27]

5.1.1 Mbed OS

Arm Mbed OS je open-sourcový operační systém navržený konkrétně pro zařízení v kategorii Internet Věcí.

OS je určený k vývoji produktů založených na mikrokontrolérech Arm Cortex-M. Mbed OS nabízí podporu kompatibilního hardwaru a softwarových knihoven pro komunikační zařízení fungující například skrze Wi-Fi, Bluetooth, RFID, GSM nebo klasický internet. Implementovány jsou také bezpečnostní protokoly SLL/TLS. [27]

5.1.2 Mbed IDE (Integrované vývojové prostředí)

Vývojové prostředí Mbed IDE poskytuje veškeré potřebné nástroje pro vývoj online, jakožto cloudovou službu. IDE obsahuje kompletní a přehledný editor s funkcemi, které najdeme i u klasických editorů a to zvýraznění syntaxe (s možností zvolit několik různých jazyků), dále jsou k dispozici běžné klávesové zkratky, jako jsou zpět/dopředu, vložit/zkopírovat/vyjmout, tabulátory a automatické formátování textu. Pracovat je možné na více souborech i projektech zároveň. Námi vytvořené projekty jsou k dispozici v levé části prohlížeče ve formě stromu. Konkrétní knihovny a programy lze přesouvat formou drag and drop. [28]

K dispozici jsou zde i oficiální nebo uživateli vytvořené knihovny a programy, které lze importovat online přímo skrze IDE nebo nahrát z PC. Skrze stejné rozhraní má uživatel možnost publikovat vlastní programy či vytvářet nové verze programů ostatních uživatelů.

Poslední část tvoří kompilátor. Kompilátor samotný nemá vestavěné limity na velikost kódu. Ten tvoří pouze reálná velikost uložiště na konkrétním zařízení. K dispozici je také souhrn, který nám zobrazí jaké části kódu budou využívat konkrétní části paměti FLASH nebo RAM. [28]

5.2 Použité periferie

5.2.1 Vývojová deska STM NUCLEO-F401RE

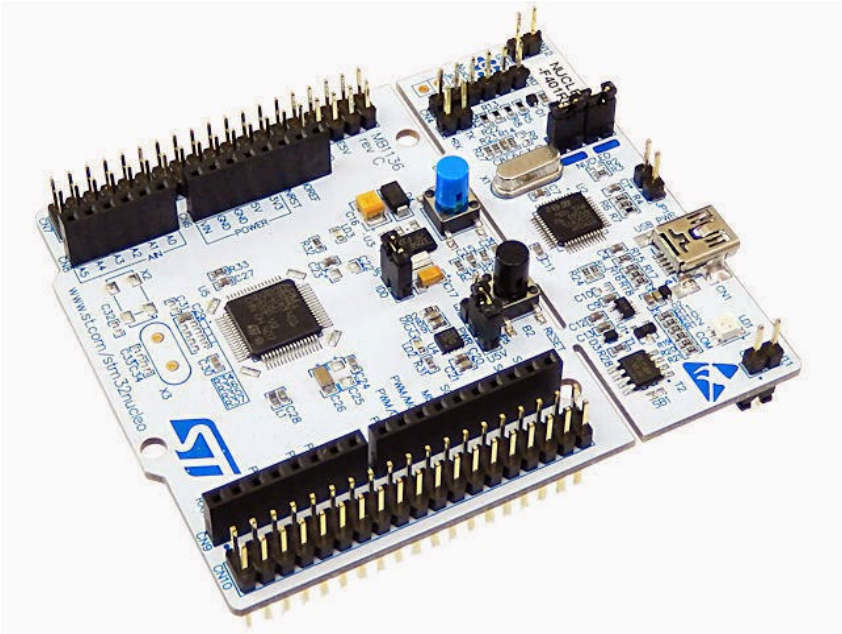
Jedná se o výkonnou vývojovou desku založenou na mikrokontroléru STM32F401RE. Jádrem mikrokontroleru je ARMový procesor Cortex®-M4 s maximální frekvencí až 84MHz. K dispozici je 512kB flash paměti a 96kB SRAM. Na desce je integrován

debugger a programátor ST-LINK/V2-1. Připojení k desce zajišťuje USB konektor. Skrze USB lze desku napájet a to buď 3,3V nebo 5V. Napájení desky je také možno zajistit extérním zdrojem s napětím 7 až 12V. [29]

Deska nabízí 50 vstupně výstupních portů (GPIO). Všechny vstupně výstupní porty jsou 5V tolerantní. Dále 12 komunikačních rozhraní a to konkrétně 3x I2C, 3x SPI, 4x USART. USB lze využít také jako virtuální COM port. Na desce je uživateli k dispozici jedna dioda, jedno tlačítko a jedno tlačítko reset. [30]

Naprogramování desky probíhá jednoduchým přetažením zkompilovaného kódu na paměť desky. V počítači je deska vidět jako obyčejné uložiště na způsob flash disku.

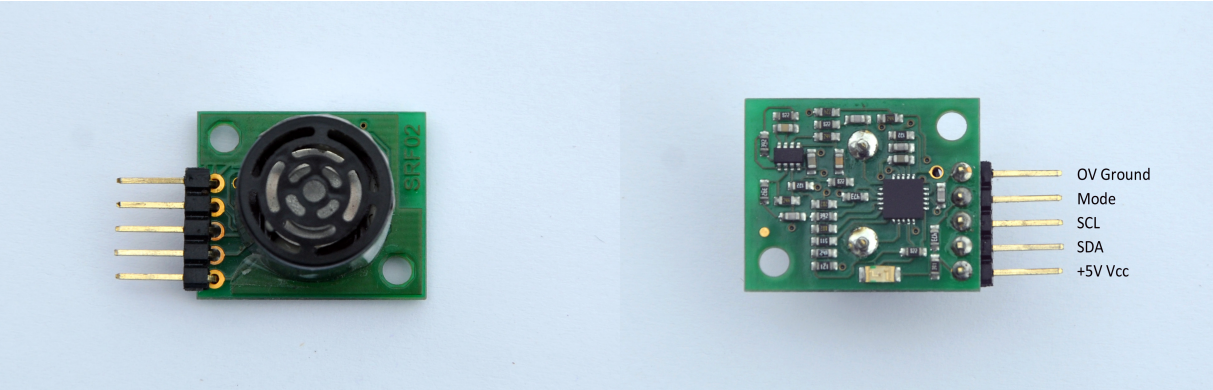
Deska nabízí možnost rozšíření o shieldy Arduino Uno V3 a ST morphio. Slouží například k připojení motorů nebo wi-fi modulu.



Obrázek 5 Vývojová deska Nucleo F401RE [29]

5.2.2 Ultrazvukový dálkoměr SRF02

SRF02 je ultrazvukový dálkoměr s jediným snímačem pro příjem i vysílání impulzů. K dispozici je sériové rozhraní i I^2C sběrnice. K jedné sběrnici je možné připojit až 16 SRF02 a to buď I^2C nebo sériově. SRF02 umožňuje odesílat ultrazvukové impulzy bez příjímacího cyklu nebo provádět cyklus příjmu bez předešlého impulzu. Vzhledem k tomu, že SRF02 používá jediný snímač na příjem i vysílání je minimální měřitelná vzdálenost vyšší než u duálních dálkoměrů. Minimální vzdálenost se různí podle teploty okolí a to za teplých dnů mezi 17–18cm a během studených dnů 15–16cm. SRF02 umožňuje měření vzdálenosti v cm a palcích a dále délku měření v µS. [31]



Obrázek 6 Ultrazuvkový dálkoměr SRF02. Foto autor.

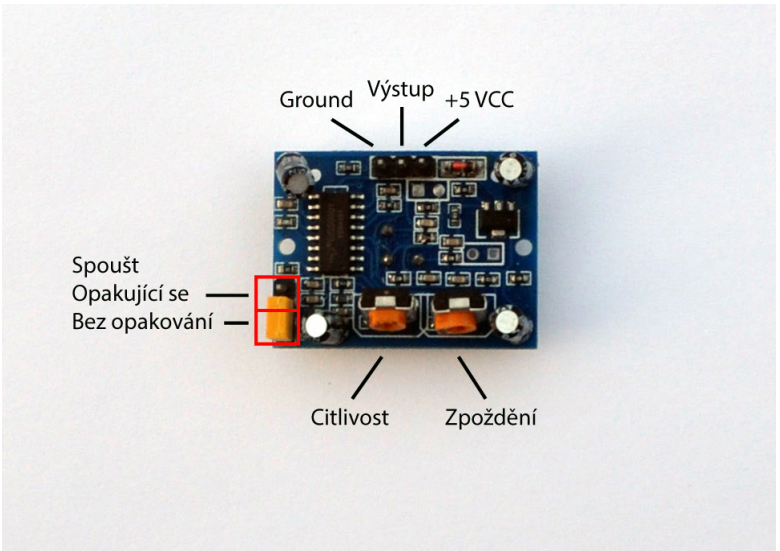
Senzor má na vývodu 5 pinů. Piny SCL a SDA lze připojit k libovolné dvojici SCL/SDA na vývojové desce. K jedné dvojici lze připojit až 16 zařízení SRF02. Pin Mode slouží k přepínání mezi módy I^2C a Serial. Pro sériové připojení součástky, připojíme pin Mode k zemi 0V (Ground). Pro připojení I^2C necháme pin volný nebo ho připojíme ke zdroji +5V. Napájení připojujeme také k +5V (VCC).

Po připojení čidlo blikne 1× dlouze a pak 0–15× v rychlém sledu, čímž oznámí jaká adresa je právě na konkrétním senzoru nastavena.

5.2.3 PIR čidlo SR501

SR501 je infračervené pohybové čidlo, založené na sondě LHI778, má vysokou citlivost i přesnost. Čidlo má velmi nízkou spotřebu (desítky µA) tudíž je vhodné zejména pro výrobky napájené bateriemi.

Čidlo nabízí 2 možnosti zaznamenání události, neopakovací – při zaznamenání pohybu dojde k nárůstu napěti (logická 1) a ihned po uplynutí zpoždění zpět k poklesu napětí na 0 V (logická 0), nebo opakující se kdy je vyšší napětí udržování po celou dobu pohybu před čidlem. [32]

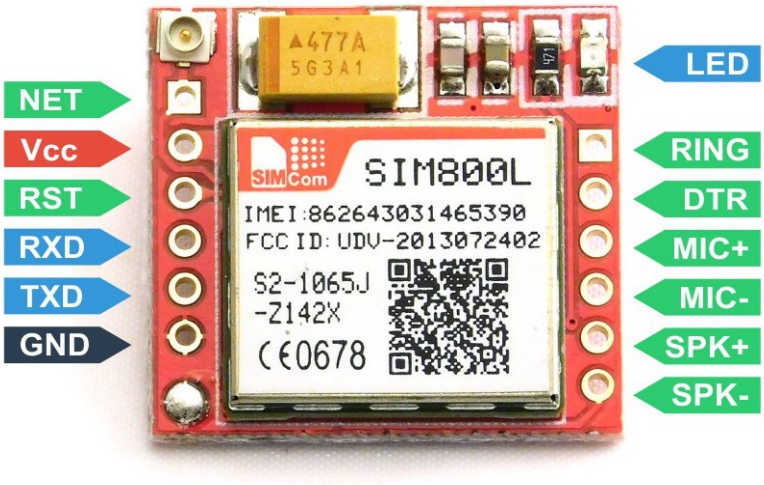


Obrázek 7 PIR čidlo SR501. Foto autor.

Na čidle SR501 najdeme 3 piny. Zem 0V (Ground), napájení +5V (VCC) a pin pro výstup. Pin pro výstup lze zapojit na libovolný pin GPIO. Výstupní hodnota pro logickou 1 je 3,3 V.

5.2.4 GPRS/GSM modul SIM800L

GSM/GPRS deska SIM800L CoreBoard, založená na modulu SIM800L vyráběným společností SIMCom, slouží k přenosu dat skrze GPRS, posílání a přijímání SMS, volání a přijímání hovorů. Modul navíc také podporuje technologii A-GPS za pomocí, které dokáže určit pomocí mobilní sítě svou polohu. Modul je použitelný téměř po celém světě díky podpoře quad-band (850/900/1800/1900MHZ) a taktéž nabízí možnost připojení k internetu s jakoukoli 2G SIM. Komunikace s mikrokontrolerem probíhá pomocí AT příkazů přes sériovou linku. [33]



Obrázek 8 Coreboard SIM 800L [34]

Na modulu SIM800L najdeme celkem 12 pinů. Piny Rx (Recieve – přijímat) a Tx (Transmit – vysílat) připojujeme k desce do kříže k libovolné dvojici Rx/Tx. Pin napájení je nutné připojit k vhodnému zdroji v rozmezí 3,7-4,2 V. Vzhledem k tomu, že napětí dostupné na desce je pouze +3,3 V nebo +5 V, lze k napětí +5 V připojit diodu například 1N4001 a tak snížit výsledné napětí na hodnotu přibližně kolem 4 V. Pin GND připojíme k příslušnému pinu GND na desce. Pin reset není nutné připojovat. Na druhé straně nalezneme 4 piny pro připojení audio vstupu a výstupu, ve dvojicích +5 V a GND.

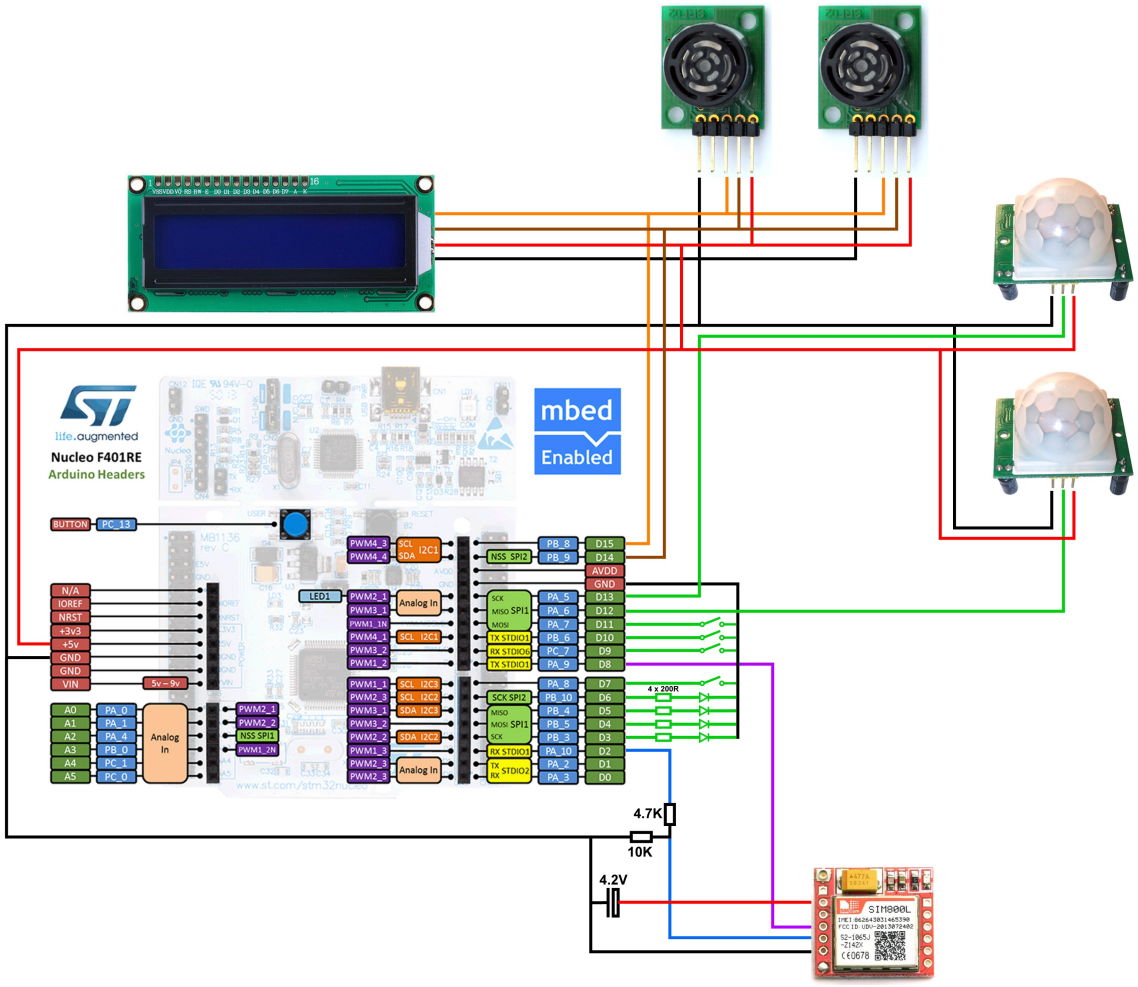
5.2.5 1602 HD44780 LCD display s IIC/I^{2}C adaptérem

Jedná se o LCD display založený na standardu HD44780. Dokáže zobrazit 16×2 znaků. K displeji lze připojit převodník IIC/I^{2}C. Hlavní výhodou tohoto řešení je ušetření 5 I/O portů.

Obrázek 9 LCD display 1602 s I2C převodníkem [35]

Z převodníku vychází pouze 4 piny a to napájení 5V, zem 0V (GND) a piny SCL/SDA, ty připojíme k libovolné dvojici SCL/SDA na vývojové desce, stejně tak jako tomu je u ultrazvukových senzorů.

5.2.6 Návrh připojení komponent

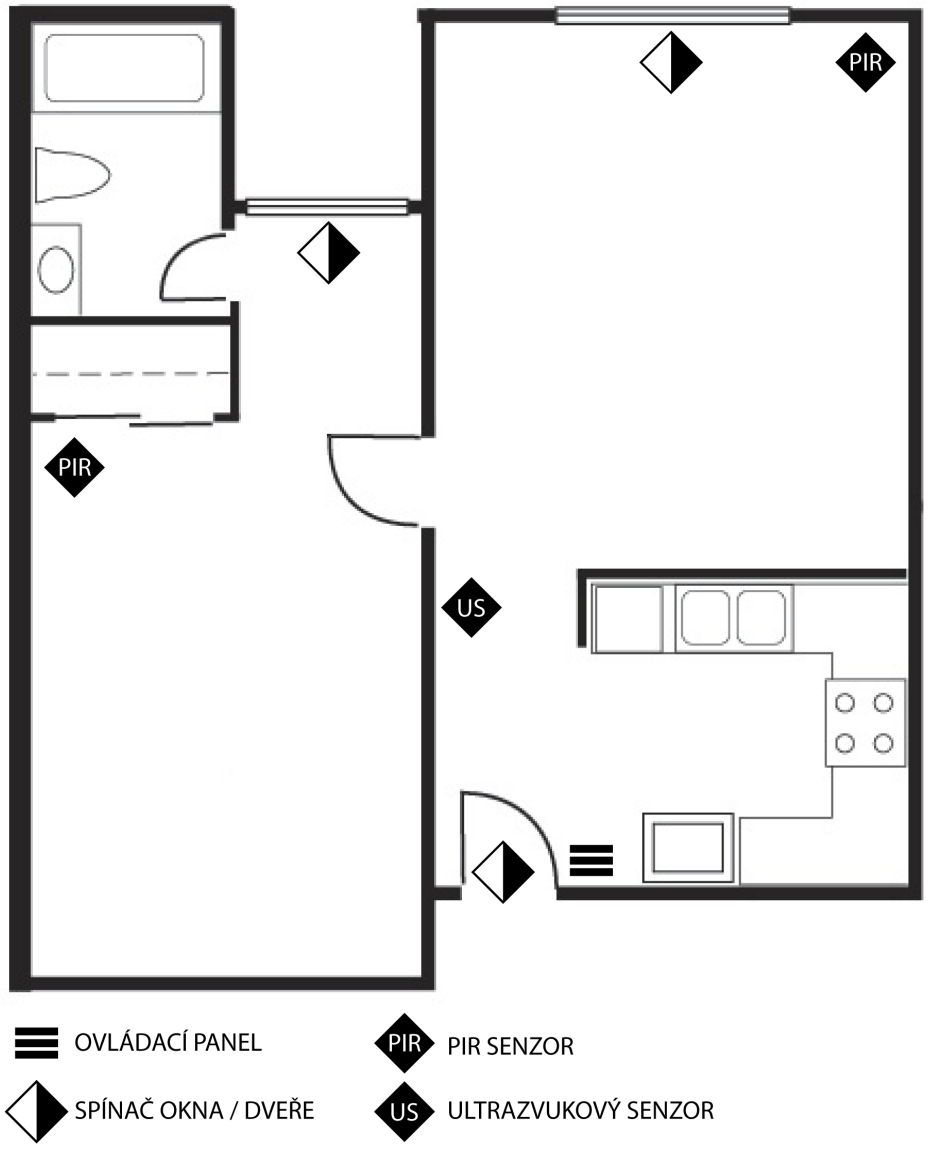


Obrázek 10 Schéma připojení komponent

Jednotlivé komponenty připojíme dle výše uvedeného schématu. Při zapojení komponentů ke sběrnici I^2C (LCD display, ultrazvukové senzory) je nutné dbát na připojení správné dvojice – v našem případě dvojice I2C1, deska nabízí další 2 dvojice, těch bychom využili v případě vyčerpání adres pro konkrétní senzor (ultrazvukových čidel lze připojit maximálně 16 na jednu sběrnici). Na správné zapojení je nutné dohlédnou i při zapojení GSM modulu – v našem případě dvojice STDIO1. Dvojice STDIO2 nelze použít, jelikož je zarezervovaná pro komunikaci s PC. Ostatní komponenty jako jsou diody, spínače a PIR čidla můžeme připojit libovolně, jelikož všechny PINy umí fungovat jako vstup pro digitální signál.

5.3 Modelová situace

Jako modelovou situaci uvedu byt 2+1. Uvnitř bytu bude nainstalován 3x spínač (vstupní dveře a dvě okna), dva PIR senzory a jeden ultrazvukový senzor.

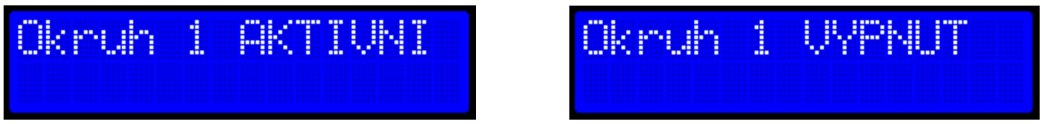


Obrázek 11 Půdorys bytu [36]

První hlídaný okruh budou tvořit výhradně spínače umístěny na oknech a dveřích. Druhý hlídaný okruh pak bude sestaven z ultrazvukového čidla a dvou PIR čidel. Takovéto rozdělení umožňuje, aby byl systém částečně v pohotovosti i v případě, že je majitel doma (například v noci). Kombinaci čidel je vhodné volit s přihlédnutím na dispozice místnosti a také například na to zdali jsou uvnitř bytu psi nebo kočky, tak aby nedocházelo k planým poplachům.

5.4 Ovládání systému

K ovládáni systému byly vytvořeny dvě varianty. První variantou je ovládací panel nacházející se uvnitř bytu, který se skládá z LCD displeje, dvou tlačítek a dvou RG diod. Každé tlačítko slouží k zapnutí nebo vypnutí konkrétního okruhu. Při každé změně se navíc vypíše zpráva na LCD displeji. Diody indikují stav bezpečnostních okruhů: zelená – vypnuto, červená – zapnuto.



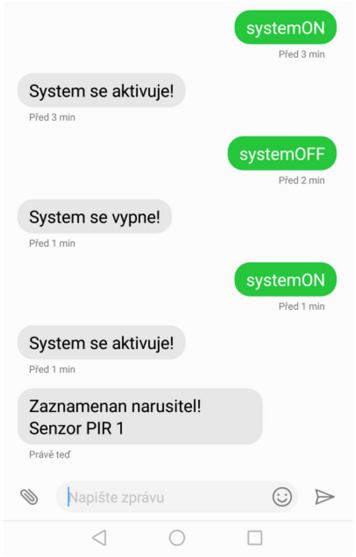
Obrázek 12 Okruh 1 AKTIVNÍ/VYPNUTO

První tlačítko slouží k zapnutí prvního okruhu složeného ze spínačů oken a dveří. Tento okruh je možné zapnout samostatně. Při stisknutí druhého tlačítka se aktivují bezpečnostní okruhy oba, jelikož se nepředpokládá, že by majitel chtěl zabezpečit pouze vnitřní prostory a okna a dveře nechal nestřežené. Systém se aktivuje se zpožděním tak, aby bylo možné opustit byt před spuštěním alarmu. Po opuštění bytu lze systém vypnout zasláním SMS ve tvaru „systemOFF“.

V případě narušení se na LCD displeji vypisují informace o tom, který konkrétní senzor zaznamenal pohyb nebo jaký spínač byl přerušen. Stejná informace je odeslána majiteli formou SMS.

Obrázek 13 Zpráva - Narušitel

Druhá varianta je ovládání za pomocí SMS. V tomto případě je k dispozici pouze možnost celý systém zapnout nebo vypnout. Toho docílíme posláním SMS ve tvaru „systemON“ pro zapnutí nebo „systemOFF“ pro vypnutí. Po zpracování příkazu přijde uživateli SMS o tom, že příkaz byl vykonán, nebo že příkaz nebyl rozpoznán (je třeba dbát na velká a malá písmena). Jako bezpečnostní prvek proti zneužití slouží kontrola telefonního čísla. V případě, že se systém pokusí vypnout neoprávněný uživatel, bude majitel upozorněn SMS zprávou.



Obrázek 14 Komunikace za pomocí SMS

Při zaznamenání pohybu jakýmkoli senzorem dojde k vytvoření SMS zprávy, která obsahuje informaci o tom, který senzor narušení zaznamenal. Samotné vytvoření a odeslání SMS trvá přibližně 5 sekund. Prodleva mezi jednotlivými AT příkazy je nutná pro správný chod GSM modulu. Průměrná doba mezi odesláním a doručením SMS se pohybuje mezi 5-15 sekundami. Pro správný chod je nutné, aby měl GSM modul dostatečný signál.

V případě, že uživatel chce, je možné přidat do zprávy i aktuální čas, ten lze získat pomocí zaslání AT příkazu na modem ve formě AT+CCLK? A odpověď připojit k odesílané zprávě. Nicméně tato informace lze vyčíst ze samotné zprávy, vzhledem k tomu, že prodleva mezi narušením a doručením je velmi nízká.

6 ZHODNOCENÍ A DISKUZE

Použitý hardware i software byl navržen tak, aby bylo možné vytvořit vlastní domácí zabezpečovací systém. Zatímco hardware umožňuje samotnou detekci, software byl navržen tak, aby bylo ovládání jednoduché a efektivní. Hlavním cílem projektu je zajistit zabezpečení domova a zároveň udržet vynaložené náklady co nejnižší.

Komunikace mezi bezpečnostním systémem a majitelem je zajištěna pomocí GSM modulu. Toto řešení se osvědčilo jako funkční, odezva mezi zjištěním narušení a upozornění majitele probíhá v řádu sekund. V případě, že je v budově horší telefonní signál, lze k modulu připojit externí anténu. Nevýhodou tohoto GSM modulu je potřeba vlastního zdroje energie o specifické voltáži, která není dostupná na vývojové desce.

Citlivost PIR senzoru je přibližně 6 až 10 metrů. Vhodným umístěním snímače zvýšíme jeho účinnost při detekci. Vhodné umístění může být například takové, kdy narušitel prochází skrze zorné pole snímače na rozdíl od umístění, kdy jde narušitel přímo ve směru k snímači. Nicméně oba typy umístění pro tento snímač lze hodnotit jako funkční.

Ultrazvukový senzor má na rozdíl od PIR senzoru mnohem menší úhel ve kterém je schopen snímat, tudíž je vhodné ho umístit tak, aby vetřelec prošel skrze zorné pole snímače. Tuto nevýhodu lze využít v náš prospěch, například v případě, že máme v domě psa. Umístěním snímače nad úroveň pasu zamezíme tomu, že by zvíře vyvolalo planý poplach. Senzor je účinný do vzdálenosti přibližně 6 metrů.

Zabezpečení domova je zajištěno pouze v případě, že majitel domu zná aktuální dění uvnitř domu. Systém je proto navržen tak, aby upozornil vlastníka domu na případné vniknutí pomocí SMS. Přímo v SMS pak najdeme informace o tom, kudy došlo k vniknutí do domu. V tomto okamžiku může majitel podniknout kroky nezbytné k tomu, aby došlo k co nejmenší újmě na majetku.

Navržený systém je možné zdokonalit implementací bezdrátových technologií jako je Wi-fi nebo Bluetooth, pro zjednodušení pokrytí domu patřičnými senzory. Dalším možným vylepšením je připojení kamerového systému, díky kterému by byl zajištěn větší přehled o tom co se uvnitř domu děje.

Pro zjednodušení používání a to zejména při odchodu a příchodu do domu by bylo vhodné implementovat kombinaci elektronického zámku a klíčenek například s technologií RFID. Tímto způsobem by bylo možné zamykat dveře i celý zabezpečovací systém jedním přiložením klíčenky. Možnost implementace pouze čtečky RFID je také možná.

7 ZÁVĚR

Cílem práce bylo seznámit se s problematikou zabezpečování nemovitostí a navrhnout vlastní zabezpečovací systém. Zvolil jsem open-sourcové řešení od společnosti Mbed a vývojovou desku Nucleo. Zvolené řešení se projevilo jako dobrá alternativa k ostatním rozšířeným řešením, jako je například Arduino. Zabezpečovací systém se skládá z několika různých typů senzorů a GSM modulu. Systém je navržen tak, aby překonání jednoho bezpečnostního prvku nemělo vliv na schopnost detekovat narušení ostatními senzory. Kód popsaného řešení je k dispozici v příloze.

8 SEZNAM POUŽITÉ LITERATURY

[1] *Policie České republiky: Trestný čin krádeže vloupáním* [online]. [cit. 2018-05-17]. Dostupné z: http://www.policie.cz/clanek/trestny-cin-kradeze-vloupanim.aspx?q=Y2hudW09Ng%3d%3d

[2] *Pojištění majetku proti zlodějům* [online]. [cit. 2018-05-17]. Dostupné z: https://www.pojisteni.cz/majetek/proti-zlodejum

[3] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management I*. Zlín: Radim Bačuvčík - VeRBuM, 2015. ISBN ISBN978-80-87500-05-7.

[4] UHLÁŘ, Jan. *Technická ochrana objektů*. 2. vyd. Praha: Policejní akademie České republiky v Praze, 2009. ISBN ISBN978-80-7251-313-0.

[5] KYNCL, Jaromír. *Bezpečnost objektu ve světle moderních technologií*. Praha: Komora podniků komerční bezpečnosti České republiky, 2014. ISBN ISBN978-80-260-7115-0.

[6] HLADÍK, Drahoslav. *Elektronické zabezpečovací systémy a elektronická požární signalizace.* Plzeň: SOUE Plzeň, 2010.

[7] *PIR Motion Sensor: Overview* [online]. Adafruit [cit. 2018-04-17]. Dostupné z: https://learn.adafruit.com/pir-passive-infrared-proximity-motion-sensor?view=all

[8] HEIDE, Patric. *Commercial microwave sensor technology: an emerging business.* Microwave Journal [online]. 1999, 1 May 1999 [cit. 2018-05-03]. Dostupné z: http://www.microwavejournal.com/articles/2641-commercial-microwave-sensor-technology-an-emerging-business

[9] AGARWAL, Tarun. *Ultrasonic Detection – Basics & Application.* ElProCus - Electronic Projects for Engineering Students [online]. [cit. 2018-05-03]. Dostupné z: https://www.elprocus.com/ultrasonic-detection-basics-application/

[10] *Dual Tech (IR & Microwave) Barriers* [online]. [cit. 2018-05-21]. Dostupné z: http://www.teotec.gr/categories_en.asp?catid=36

[11] *Mikrovlnné bariéry* [online]. 2017 [cit. 2018-05-21]. Dostupné z: http://www.forteza.cz/sortiment/mikrovlnne-bariery.html

[12] *Bezpečnostní systémy*. Studijní materiály SŠEaŠ [online]. Ústí nad Labem: SŠEaS [cit. 2018-05-03]. Dostupné z: http://studijni-materialy.sseas.cz/bezpecnostni-systemy/

[13] MRÁZEK, Martin. *Předmětová ochrana v expozicích muzejí a galerií*. Praha: Národní muzeum, 2015.

[14] SVOBODA, Alexandr. *Plynárenská příručka: 150 let plynárenství v Čechách a na Moravě.* 1. Praha: GAS, 1997. ISBN 80-902339-6-1.

[15] *Využívání vymezených rádiových kmitočtů.* Český telekomunikační úřad [online]. [cit. 2018-04-11]. Dostupné z: https://www.ctu.cz/vyuzivani-vymezenych-radiovych-kmitoctu

[16] *Všeobecné oprávnění č. VO-R/10/11.2016-13 k využívání rádiových kmitočtů a k provozování zařízení krátkého dosahu.* Praha: Český telekomunikační úřad, 2016.

[17] *Mobilní sítě GSM - mobilní sítě 2. generace* [online]. [cit. 2018-05-18]. Dostupné z: https://publi.cz/books/236/03.html

[18] NOLDUS, Rogier. *Introduction to GSM Networks*. John Wiley & Sons, 2006. ISBN 9780470028483.

[19] STEELE, Raymond, Chin-Chun LEE a Peter GOULD. *The GSM System*. 2001. ISBN 9780470841679.

[20] MÁCHA, Miroslav. *LoRa Technology* [online]. 2016 [cit. 2018-05-18]. Dostupné z: http://www.osel.cz/8732-lora-technology.html

[21] AUGUSTIN, Aloÿs, Jiazi YI, Thomas CLAUSEN a William Mark TOWNSLEY. *A Study of LoRa: Long Range & Low Power Networks for the Internet of Things*. 2016. 10.3390/s16091466.

[22] *Radio versions, Bluetooth technology Website* [online]. [cit. 2018-05-19]. Dostupné z: https://www.bluetooth.com/bluetooth-technology/radio-versions

[23] RATASUK, Rapeepat, Nitin MANGALVEDHE, Yanji ZHANG a Michel ROBERT. *Overview of Narrowband IoT in LTE Rel-13*. Nokia Bell Labs, 2016.

[24] VOJÁČEK, Antonín. *SIGFOX - princip, struktura, protokol, použití* [online]. 2017 [cit. 2018-05-19]. Dostupné z: https://vyvoj.hw.cz/sigfox-princip-struktura-protokol-pouziti.html

[25] POURSAFAR, Noushin, Md Eshrat E ALAHI a Subhas MUKHOPADHYAY. *Long-range Wireless Technologies for IoT Applications: A Review*. 2017, , 6.

[26] *Co je to PoE (Power over Ethernet)* [online]. 2018 [cit. 2018-05-18]. Dostupné z: https://kb.netgear.com/cs/209/Co-je-to-PoE-Power-over-Ethernet

[27] *Arm Mbed OS developer site* [online]. [cit. 2018-05-03]. Dostupné z: https://os.mbed.com/

[28] *Mbed Compiler* [online]. [cit. 2018-05-03]. Dostupné z: https://os.mbed.com/handbook/mbed-Compiler

[29] *STM32F401RE* [online]. [cit. 2018-04-11]. Dostupné z: http://www.st.com/en/microcontrollers/stm32f401re.html

[30] *NUCLEO-F401RE: Overview* [online]. [cit. 2018-04-11]. Dostupné z: https://os.mbed.com/platforms/ST-Nucleo-F401RE/

[31] *SRF02 Ultrasonic range finder* [online]. [cit. 2018-04-07]. Dostupné z: https://www.robot-electronics.co.uk/htm/srf02tech.htm

[32] *HC-SR501 PIR MOTION DETECTOR: Product Discription* [online]. [cit. 2018-04-07]. Dostupné z: https://www.mpja.com/download/31227sc.pdf

[33] *SIM800L Hardware design.* V1.08. SIMCom, 2015.

[34] *SIM 800L GSM MODUL.* In: Nettigo: SIM800L [online]. [cit. 2018-05-08]. Dostupné z: https://nettigo.eu/products/sim800l-gsm-grps-module

[35] *LCD Display 1602 + I2C adapter* [online]. In: . [cit. 2018-05-08]. Dostupné z: https://ardushop.ro/en/home/214-lcd-display-1602-i2c-adapter.html

[36] *One Bedroom Layout Floor Plan* [online]. In: . 2018 [cit. 2018-05-22]. Dostupné z: http://bccrss.club/one-bedroom-layout-floor-plan/

9 SEZNAM OBRÁZKU

10 SEZNAM ZKRATEK

PZTS	Poplachové zabezpečovací a tísňové systémy
GSM	Globální systém pro mobilní komunikaci
PIR	Pasivní infračervený detektor
MW	Mikrovlnný
IR	Infračervený
OSS	Operační subsystém
NSS	Spojovací subsystém
BSS	Subsystém základových stanic
MS	Mobilní stanice
IMSI	Mezinárodní identifikátor mobilního účastníka
HLR	Domácí lokalizační registr
BSC	Řídící základová jednotka
LP-WAN	Low power - wide area network
MAC	Řízení přístupu k médiu
NB-IoT	Úzkopásmový Internet věcí
LTE	Long term evolution
UNB	Ultra narrow band
TCP/IP	Primární přenosový protokol/protokol přenosové vrstvy
LED	Elektroluminiscenční dioda
LCD	Displej z tekutých krystalů
RFID	Identifikace na rádiové frekvenci
SSL/TLS	Secure sockets layer / transport layer security
IDE	Integrované vývojové prostředí
GPIO	Vstupně výstupní port

11 SEZNAM PŘÍLOH

PŘÍLOHA 1: CD

1. Text práce ve formátu PDF
2. Zdrojový kód zabezpečovacího systému