FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Název:	SMART vinný sklípek
Student:	Martin Němec
Vedoucí:	Ing. Martin Daňhel, Ph.D.
Studijní program:	Informatika
Studijní obor:	Bezpečnost a informační technologie
Katedra:	Katedra počítačových systémů
Platnost zadání:	Do konce letního semestru 2020/21

Pokyny pro vypracování

Pro vinný sklep navrhněte a implementujte bezpečnostní SMART systém dle těchto pokynů:

1. Seznamte se s pracemi na téma zabezpečení objektů: M. Váňa, M. Mačak, O. Červenka.

2. Analyzujte možnosti zabezpečení vinného sklípku bezpečnostními bezdrátovými čidly a kamerou. Dále zvažte možnost měření hladiny CO2. Zabezpečení vstupu řešte kódovým zámkem. Berte v úvahu možná budoucí rozšíření.

3. Na základě analýzy navrhněte systém, který zabezpečí vinný sklípek pomocí jednoduchého kamerového systému a bezdrátových čidel. Jako platformu zvolte vhodnou verzi Raspberry Pi.

4. V případě vysoké hladiny CO2 by měl systém spustit zvukový výstražný signál. V případě narušení bezpečnosti spustí systém video-nahrávání a pošle SMS notifikaci majiteli. Předpokládá se, že systém bude ukládat logovaný záznam o stavu čidel přímo do svého souborového systému.

5. Navržený systém implementujte a otestujte jeho funkčnost v reálných podmínkách.

Seznam odborné literatury

Dodá vedoucí práce.

prof. Ing. Pavel Tvrdík, CSc.
vedoucí katedry

doc. RNDr. Ing. Marcel Jiřina, Ph.D.
děkan

V Praze dne 7. ledna 2020

FAKULTA
INFORMAČNÍCH
TECHNOLOGIÍ
ČVUT V PRAZE

Bakalářská práce

SMART vinný sklípek

Martin Němec

Katedra počítačových systémů
Vedoucí práce: Ing. Martin Daňhel, Ph.D.

3. června 2020

Poděkování

Na tomto místě bych rád poděkoval především své rodině za podporu, kterou mi nejen při studiích poskytla. Chtěl bych poděkovat také svému vedoucímu závěrečné práce Martinovi Daňhelovi za cenné rady a připomínky. Dík patří také mým přátelům, kteří byli vždy ochotni mě vyslechnout a konzultovat se mnou problémy ohledně této práce. Hlavní dík patří Ondřeji Voroneckému a Michalovi Převrátilovi. V neposlední řadě bych také rád poděkoval své přítelkyni, a to hlavně za projevenou trpělivost a psychickou podporu.

Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval(a) samostatně a že jsem uvedl(a) veškeré použité informační zdroje v souladu s Metodickým pokynem o etické přípravě vysokoškolských závěrečných prací.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona, ve znění pozdějších předpisů. V souladu s ust. § 46 odst. 6 tohoto zákona tímto uděluji nevýhradní oprávnění (licenci) k užití této mojí práce, a to včetně všech počítačových programů, jež jsou její součástí či přílohou, a veškeré jejich dokumentace (dále souhrnně jen „Dílo"), a to všem osobám, které si přejí Dílo užít. Tyto osoby jsou oprávněny Dílo užít jakýmkoli způsobem, který nesnižuje hodnotu Díla, a za jakýmkoli účelem (včetně užití k výdělečným účelům). Toto oprávnění je časově, teritoriálně i množstevně neomezené. Každá osoba, která využije výše uvedenou licenci, se však zavazuje udělit ke každému dílu, které vznikne (byť jen zčásti) na základě Díla, úpravou Díla, spojením Díla s jiným dílem, zařazením Díla do díla souborného či zpracováním Díla (včetně překladu), licenci alespoň ve výše uvedeném rozsahu a zároveň zpřístupnit zdrojový kód takového díla alespoň srovnatelným způsobem a ve srovnatelném rozsahu, jako je zpřístupněn zdrojový kód Díla.

V Praze dne 3. června 2020 ……

Odkaz na tuto práci

Němec, Martin. *SMART vinný sklípek*. Bakalářská práce. Praha: České vysoké učení technické v Praze, Fakulta informačních technologií, 2020.

Abstrakt

Tato práce má za cíl vytvořit SMART bezpečnostní systém pro vinné sklepy, potažmo jiné objekty. Práce se zaměřuje především na bezdrátový přenos dat mezi řídící jednotkou a jednotlivými čidly. Dále se v práci prozkoumávají způsoby zabezpečení komunikace. Bezpečnostní systém je rozšiřitelný o další senzory a umožňuje napojení na nějakou vyšší řídící jednotku.

Zařízení Raspberry Pi model 3B+ slouží jako řídící jednotka a moduly ESP32 slouží k zajištění bezdrátové komunikace. Jelikož řídící jednotka je Raspberry Pi, která ovládá i vyšší programovací jazyky, tak je použit skript psaný v jazyce Python. Důvodem je snadné použití a velká dostupnost knihoven v tomto jazyce. Dále zde jsou čidla poskytující důležitá data jako například pohybové senzory, kamera a senzor plynů. Následně řídící jednotka vyhodnocuje přijímané data a případně upozorní majitele na určitý stav systému.

V práci jsou i další příklady rozšíření systému o SMART prvky, které nejsou primárně vytyčeny zadáním. Hlavní zaměření práce je přenos dat.

Výsledkem je robustní SMART systém, který dokáže monitorovat prostory za pomocí kamery a informovat majitele v případě nepovoleného vniknutí. Zároveň může monitorovat další potenciálně zajímavé údaje pro majitele systému.

Klíčová slova bezdrátová technologie, bezpečnostní systém, ESP, IoT, Python, Raspberry Pi, SMART

Abstract

This work aims to create a SMART security system for wine cellars, or other objects. The work is mainly focusing on wireless data transfer between the control unit and individual sensors. Furthermore, the for examines the ways of securing communication. The security system is expandable with additional sensors and provides a possibility with connection to a higher control unit.

For this, Raspberry Pi 3B + is used as a control unit and ESP32 modules for wireless communication. Since control unit is Raspberry Pi, which also is capable handling higher programming languages, it is using a script written in Python. The reason is simple usage of this language and there are many public libraries. Furthermore, there will be sensors providing all the data like motion sensors, cameras or gas sensors. After this the control unit evaluates incoming messages and eventually alert the owner about system status.

There are other examples of extending the system by SMART elements that are not primarily defined by the assignment. The work is mainly interested in data transfer.

The result is robust SMART system that can monitor the premises using camera and inform the owner in the event of unauthorized intrusion. It is also able to monitor other potentially interesting data for system owner.

Keywords ESP, IoT, Python, Raspberry Pi, security system, SMART, wireless technology

Obsah

Seznam obrázků

Seznam tabulek

Úvod

Fenomén zvaný internet věcí (IoT - Internet of Things) je pro dnešní společnost již zavedený pojmem, díky kterému si lidé začínají zvykat na nejrůznější chytré neboli SMART technologie a to nejen v oblasti mobilních zařízení. Tím jsou myšleny především prvky v moderních domácnostech např. ovládání světel a digitální měření různých údajů jako je teplota, vlhkost atd. ale také bezpečnostní prvky jako například magnety u dveří, pohybová čidla či kamery. Mnoho lidí tyto technologie používá v domnění, že si lépe zabezpečí své domovy, garáže nebo také vinné sklepy. Systém může poskytovat danou funkci spolehlivě, ale lidé se tolik nezamýšlí nad celou integritou systému, ani nad možnostmi zabezpečení komunikace mezi jednotlivými krabičkami, které si rozmisťují po svých domovech. Poté se tato čidla, řídící jednotka potažmo i celý systém ocitají v nebezpečí pro odposlouchávání nebo získání osobních dat jako například záznamy z kamer.

Během výběru tématu jsme s vedoucím této práce konzultovali mnoho různých objektů jako například garáž nebo vchod do domu, ale rozhodli jsme se pro tematičtější a zajímavější směr. Původem jsem totiž z pohraničí Moravy se Slovenskem a znám případy, kdy se známým či někomu v okolí vloupal někdo do vinného sklepa. Jde o to, že vinaři a jejich rodiny jsou obvykle pracující lidé a veškerý svůj volný čas věnují práci ve vinohradech a staráním se o něj. Mnohdy nemají moc financí a času se zaobírat tím, zda je jejich sklep chráněn a dopadá to tak, že zamčené dveře lupiče nezastaví. Proto jsem se rozhodl vytvořit projekt na téma SMART zabezpečení vinného sklepa, který by majitele nejen dokázal upozornit v případě narušení objektu ale i dokázal později poskytovat užitečné informace o stavu sklepa.

Touto prací chci také prohloubit své znalosti v možnostech zabezpečení bezdrátových spojení a zároveň tím poskytnout podklady pro další práce, které budou používat bezdrátové technologie v podobných projektech.

Chci poskytnout přehled současných možnosti pro zabezpečení komunikace. Popsat výhody či nevýhody popisovaných možností. Vysvětlit jednotlivá

úskalí a možná nebezpečí.

Po úvodu následuje kapitola Cíle práce, která definuje výsledek mé práce a dílčí úkoly. Druhá kapitola popisuje seznámení se s prací a celou problematikou zabezpečení objektů. Třetí kapitolou je rozbor všech částí systému a konkrétní specifikace klíčových modulů systému. Čtvrtá kapitola navrhuje systém, detailně popisuje návrh komunikace v bezdrátové síti a řeší zabezpečení systému. Pátou kapitolou je průběh realizace navrhovaného systému. Šestá kapitola popisuje testování systému v reálných podmínkách, reakce na různé druhy testů a pokusy o prolomení zabezpečení systému.

Tato práce navazuje na vícero prací, na každou spíše jen částečně, a to *Inteligentní bezpečnostní systém garáže* od Miroslava Váni, *Inteligentný bezpečnostný systém - sekcia zabezpečený vstup* od Maroše Mačaka a *Inteligentní zabezpečovací systém garáže: nadřazený systém* od Ondřeje Červenky. Na práci Miroslava Váni moje práce přímo navazuje a je jejím vylepšením o bezdrátové technologie. Prací zbylých dvou kolegů se dotýkám spíš okrajově, protože moje práce bude obsahovat zabezpečený vstup a právě bezdrátové technologie, které jsou užity v práci kolegy Červenky za jiným účelem než je v mojí. Celá práce navazuje na práce, které byly vytvořeny na FIT ČVUT v Praze.

Kapitola 1

Cíl práce

Hlavním cílem je vytvoření bezpečnostního řešení aplikované na vinný sklípek, které jsem pracovně nazval SMART vinný sklípek. Řešení bude schopné informovat majitele v případě bezpečnostního narušení. To čítá celou řadu úkolů, jejichž základním vymezením je prostudování prací zkoumající podobné technologie, navrhnout SMART systém pro vinný sklep, zanalyzovat veškeré prvky a vybrat nejlepší pro tuto situaci, realizovat návrh a otestovat ho v reálných podmínkách.

Prvním úkolem je seznámit se s bakalářskými pracemi od Miroslava Váni, Maroše Mačaka a diplomovou prací Ondřeje Červenky. Na základě toho zde budou popsány postřehy, které budou prospěšné pro tuto práci.

Navazuje analýza možností zabezpečení vinného sklepa. Základem je řídící jednotka, která bude zpracovávat veškeré informace z čidel a vyhodnocovat situaci ve sklepě. Platforma je zadáním stanovena, a to Raspberry Pi, tudíž prozkoumám nejvhodnější verze na této platformě pro můj případ. Dále zde budou popsány komunikační moduly pro bezdrátové spojení s řídící jednotkou. Vyhodnotím nejlepší použitelnou variantu pro projekt. Samotná čidla a kameru mnohdy už analyzovali moji kolegové z předchozích prací, takže budu zkoumat také jiné alternativy a případně odůvodním proč jsem vybral stejný senzor jako kolegové.

Dalším krokem bude návrh celého systému, kde vysvětlím a rozepíšu jak bude celý systém fungovat. Zde se bude řešit největší palčivá problematika, a to bezdrátová komunikace a její zabezpečení. Budou se zde zkoumat jednotlivé dostupné a použité protokoly pro zabezpečení komunikace, jejich výhody a nevýhody.

Výsledkem je studie, která rozebírá oblast bezdrátové komunikace v rámci IoT, a realizovaný návrh SMART systému pro vinný sklep.

Kapitola 2

Seznámení se s prací

Kapitola uvádí čtenáře do celé problematiky zabezpečení vinného sklepa a výběru prostředků, které se pro jeho zabezpečení dají použít. Jsou zde probrány podněty a připomínky od lidí, kteří vlastní vinné sklepy, a zamyšlení se nad jejich reálnou možností implementace do mého systému.

Dále kapitola ve zkrácené formě popisuje tři bakalářské/diplomové práce, které jsou zaměřeny na podobnou problematiku nebo mají podobný cíl. Jsou zde klíčové poznatky a vědomosti, které jsou relevantní pro tuto práci. Zaznamenám zde i svůj "osobní"pohled na rozhodnutí kolegů a také uvádím jakou alternativu jsem nakonec zvolil. Ke konci kapitoly jsou diskutovány další možnosti zabezpečení vinného sklepa.

2.1 Jak zabezpečit vinný sklep

Způsobů jak zabezpečit vinný sklep je mnoho. Hovořil jsem s rodinou a celou řadou známých o návrzích jak zabezpečit jejich sklep. Na základě názorů a poznámek zde uvedu od nejzákladnějších po nejzajímavější nápady, jak by se dal zabezpečit vinný sklep.

Jako detekci vniknutí do sklepa se jeví jako nejvhodnější čidla pohybu. Podle všech dotazovaných preferují tuto možnost pro detekci vniknutí před jinými alternativami jako jsou třeba magnetické spínače u dveří či oken, které lze poměrně jednoduše obejít.

Se všemi jsme se shodli na jedné věci, a to, že vizuální záznam v případě vniknutí je klíčová vlastnost bezpečnostního systému. Vizuální záznam by se mohl skládat čistě z pořizování fotografií během vniknutí nebo v ideálním případě pořízení video záznamu. Umístění a množství kamer hraje taky zásadní roli. Mnoho lidí uvádělo, že by měli rádi kameru nejen u vstupních dveří ale i přímo ve sklepě či u jiných vstupů do budovy sklepa.

Jelikož se vinné sklepy nenachází na samotě u lesa, ale obvykle mezi ostatními sklepy, jako vhodným přídavkem do systému je alarm, který by se při

vniknutí spustil. Hlavním důvodem je právě, že vinaři často tráví volný čas ve svých sklepech a tento signál by mohl úspěšně upozornit sousedy ve sklepě, kteří by mohli přivolat pomoc.

Z řady zajímavějších myšlenek zde uvedu například použití biometrického zabezpečení. Několik z dotazovaných uvedlo, že by ocenili vstup do sklepa na otisk prstu. Jsou zde i možnosti rozpoznávání obličeje a jiné biometrické metody autentizace, ale otisk prstu by mohl být možnou nadstavbou mého systému.

Jak již kolega Maroš Mačak rozebíral ve své práci, tak častou připomínkou byl přístup do sklepa pomocí čipu nebo dokonce pomocí mobilního telefonu. Tato část je již prozkoumána, ale rozhodně je zajímavou možností posílit bezpečnost přístup do sklepa. Pro tuto práci bude využito kódového zámku a zadávání hesla přes něj.

S odemykáním přes mobilní telefony to nekončí. Pozoruhodnou myšlenkou je elektronické ovládání zámků dveří a oken. Majitel by měl možnost kontrolovat na dálku zda, je sklep zamčený a mohl by systém takto ovládat na dálku. Toto se úzce váže na přístup přes nějakou formu čipu, protože elektronické zámky musí umožňovat i fyzický vstup u dveří a nejen pouze přes nějakou aplikaci.

Z hlediska bezpečnosti přímo sklepa už moc smysl nedávalo, když se útočník může dostat do místnosti před sklepem. Nápady spíš byly ve formě nějaké meteorologické stanice ve sklepě, která by kontrolovala kvalitu podmínek pro uchovávání vína. Jediné, co je uvedené přímo v zadání práce, je detekce oxidu uhličitého ve sklepě. Příroda sama takto může zaútočit na majitele přímo zevnitř sklepa, a proto je potřeba chránit majitele i zde.

2.2 Studium prací

V této podkapitole projdu již zmíněné tři zmíněné práce od kolegů z fakulty a popíšu zde základní poznatky, které jsem od nich převzal.

2.2.1 Inteligentní bezpečnostní systém garáže

Tato bakalářská práce byla vytvořena Miroslavem Váňou [1], který navrhoval bezpečnostní systém pro garáže. Jeho systém zkoumal a testoval spolehlivost jednotlivých použitých součástek tak, aby systém poskytoval důvěryhodné informace. Dále systém hlídal, jestli někdo nevnikl do garáže a zda v ní nehoří.

Hodně do detailu rozebírá tematiku spolehlivosti, jaké chyby a v jakém typu zapojení (sériové/paralelní) mohou nastat. Moje práce z těchto poznatků bude čistě čerpat, nikoli dále rozebírat. Přínosnými poznatky jsou například redundance čidel pro zajištění důvěryhodnosti naměřených hodnot.

Práce je velice přínosná při rozhodování, která čidla použít. Přehledně porovnává nejen různé typy senzorů, které jsou zpracovány do tabulky, ale pro každý typ senzoru poskytuje vícero variant. Díky takovým znalostem je výběr senzorů pro mou práci mnohem jednodušším úkolem a budu se jimi řídit.

Čidlo	**Výhody**	**Nevýhody**
Pohybu	Zajistí do velké míry hlavní aspekt bezpečnosti. Tedy narušení objektu osobou.	Náchylnost na chybu a správné umístění.
Zvuku	Jednoduché a levné. Může navýšit spolehlivost systému.	Snadno ovlivnitelné nežádoucím hlukem.
Světla	Podpůrné čidlo pro snížení chybovosti systému.	V objektu s oknem bude ve dne nízká účinnost.
Vzdálenosti	Schopnost zaměřit se na konkrétní věc, nebo část monitorovaného objektu.	Jedno čidlo nemusí pokrýt celý sledovaný objekt.
Kouře a plynu	Lze včas zareagovat na krizovou situaci.	Nemusí stačit pouze 1 čidlo pro celý objekt.
Optická závora	Možnost jednoduše sledovat pozici vybraného objektu.	Větší rozměry a cena kvalitnějších čidel.
Spínač (magnetický)	Velmi levné a jednoduché. Snadné hlídání oken a dveří.	Pracná instalace. Nepříliš univerzální.

Obrázek 2.1: Tabulka rozebírající jednotlivé typy senzorů. Pro každý typ můžeme vidět jejich jednotlivé výhody a nevýhody. Tabulka převzata z [1]

Mým názorem je, že platforma Arduino je poměrně nevhodně zvolenou platformou pro tvorbu bezpečnostního systému. Primárním účelem platformy je poskytnout desku, která dokáže pracovat s celou řadou senzorů a ovládat například motory. Tím pádem je to vhodnější varianta pro realizaci meteostanic, kde sbírají jen data ze senzorů, nebo třeba robotů. RPI zase na druhou stranu nabízí desku s vlastním operačním systémem podobným Linuxu, takže se mnohem více hodí pro zpracovávání dat, realizaci různých systému a jiné. Arduino je taky omezeno pouze na svůj programovací jazyk, ale na RPI můžete použít téměř jakýkoliv kód, když k němu stáhnete příslušný kompilátor.

2.2.2 Inteligentný bezpečnostný systém – sekcia zabezpečený vstup

Bakalářská práce [2] od kolegy ze Slovenska Maroše Mačaka, která jak název napovídá, spočívá v uložení dat na kartě, kde jsou veškerá data zašifrována. Moje řešení bude poskytovat jednodušší způsob autentizace, a to pomocí kódového zámku. Tento způsob je sice velmi jednoduchý, ale při dostatečném ošetření vstupu, například na maximální počet pokusů, se stává dostatečně bezpečným.

Jedná se o rozšíření či nadstavbu již zmíněné práce od Miroslava Váni, takže daný systém rozšiřuje o zabezpečený vstup do objektu. K tomu používá technologii RFID[1], čtečky karet a platformu Java Card, která se stará o bezpečné ověření karty. V mé práci se řešit bezpečný vstup řešit nebude pomocí těchto technologií, ale bude vyřešen kódovým zámkem.

Použité technologie jsou účelně použity pro maximalizaci bezpečného přístupu.

2.2.3 Inteligentní zabezpečovací systém garáže: Nadřazený systém

Diplomová práce [3], o kterou se budu opírat, byla sepsána Ondřejem Červenkou. Tato práce je lehce mimo mé zaměření, které mám v práci vymezeno, ale lze zde najít určité zajímavé prvky jako například bezdrátová komunikace. Hlavně kvůli bezdrátové komunikaci jsem se ji rozhodl do této kapitoly zařadit a probereme si užitečné znalosti v ní obsažené.

Práce navrhuje a později i implementuje nadřazený systém pro garáž. Podstatná část je celková analýza procesu bezdrátové komunikace, který protokol je využit, posílání upozornění či ukládání dat. Tyto znalosti pro můj systém jsou klíčové, tudíž dokážu srovnat mé názory na návrh systému s někým jiným.

Oproti ostatním pracím se tady zabýváme celým konceptem reálného řešení, a to pomocí bezdrátového připojení. Porovnávání komunikačních protokolů či způsoby notifikací majitele jsou velmi dobře zpracovány. Na základě těchto poznatků můžu uvést jiné alternativy řešení či se shodnout na vhodném výběru komponent s kolegy.

[1]Radio Frequency Identification - technologie využívající rádiových vln pro identifikaci. Příklad čárové kódy nebo přístupové karty.

Kapitola 3

Analýza a výběr komponent

V této kapitole jsou rozebrána rozhodnutí, která jsem provedl při výběru jednotlivých součástek. Objektivně se zaměřím na jednotlivé klady a zápory probíraných možností na platformě Raspberry (dále jen RPI) desek či malých modulů s integrovanou Wi-Fi, které se na trhu vyskytují.

3.1 Analýza řídící jednotky

Jedním z klíčových požadavků kladených na řídící jednotku uvažovaného projektu je možnost využití bezdrátových technologií k přenosu dat. Další aspekty jsou například výkon samotné jednotky, počty vstupů/výstupů na desce a případně recenze od jiných zdrojů.

3.1.1 Raspberry Pi 1 a 2

Původní modelová řada, Raspberry Pi 1, čítá mnoho modelů, které byly označovány A, B, A+ a tak dále. Některé modely této řady jsou stále dostupné na trhu a na některé úkony jsou stále dostačující, ale z pohledu této práce nejsou významné, proto jsou tu zmíněny jen jako vývojový milník.

Hlavním důvodem je, že tato řada neposkytuje žádnou možnost bezdrátového přenosu sama o sobě (WiFi či Bluetooth). Dalšími důvody jsou, že řada je zastaralá a poměr ceny ku výkonu dané jednotky by byl nevýhodný. Nehledě na to, že výkon u starších modelů mohl později omezovat celý systém, protože v návrhu této práce je uvažováno s dostatečným výkonem pro možná rozšíření.

Následující řada, Raspberry Pi 2, co se týče modelů je lehce skromnější. Výkonnostně zde proběhlo podstatné vylepšení, ale bohužel stále nedisponuje integrovanou možností použití WiFi nebo Bluetooth.

3.1.2 Raspberry Pi 3

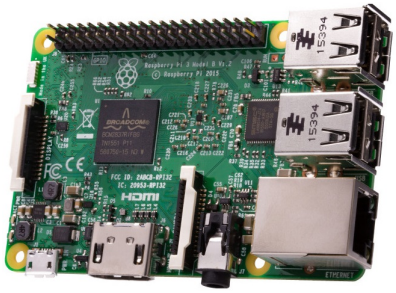
V této řadě bylo opět provedeno výkonnostní zlepšení ale hlavně zde byly přidány integrované WiFi a Bluetooth moduly. Z tohoto důvodu již tato verze splňuje výše uvedené základní požadavky a dokonce výrobce nabízí hned několik modelů.

3.1.2.1 Raspberry Pi 3 B

Tento model byl vydán v únoru roku 2016 a jedná se o první model z řady mikropočítačů Raspberry Pi 3. Oproti jeho předchůdcům nabízí výkonnostní vylepšení jak u procesoru tak i u grafického jádra. Taktéž se zde prvně objevuje nová architektura ARMv8, která poskytuje lepší podporu GNU/Linux systémů. Určitě je důležité zmínit přítomnost WiFi 802.11 b/g/n a Bluetooth 4.1 LE. Jeho cena se momentálně pohybuje přibližně od 800,- Kč. Další důležité specifikace mikropočítače jsou:

Procesor	Cortex-A53 (1,2 GHz 64-bit quad-core)
Grafické jádro	Broadcom VideoCore IV u 3D grafiky 300 MHz, video 400 MHz
Paměť	1 GB(sdílená s GPU)
USB porty	4 (verze 2.0)
Interní paměť	Micro SDHC a USB boot mode
Nízkoúrovňové periferie	40 GPIO pinů a HAT ID sběrnice
Rozměry	85,60 mm x 56,5 mm x 17 mm
Hmotnost	45 g
Cena	800,- Kč(přibližná cena)

Tabulka 3.1: Specifikace shrnující klíčové informace o RPI3B



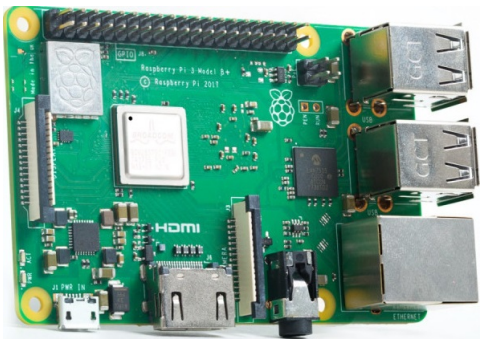
Obrázek 3.1: Raspberry Pi 3 model B [4]

3.1.2.2 Raspberry Pi 3 B+

Mikropočítač Raspberry Pi 3 model B+ oproti staršímu modelu B je v mnohých ohledech vylepšením.

Hlavními změnami jsou v oblasti bezdrátového připojení, a to výkonnější WiFi 802.11ac, novější verze Bluetooth 4.2 a až 3x rychlejší ethernetové připojení. Zároveň s novým ethernetovým připojením se naskytla možnost přes něj napájet celý mikropočítač pomocí technologie PoE skrze externí HAT[2] modul. V neposlední řadě se přepracovalo kompletně napájení na desce a proběhlo i zrychlení procesoru na 1,4 GHz. Specifikace tohoto modelu jsou totožné s modelem B, protože jde pouze o přepracování a vylepšení. Jeho prodejní cena začíná lehce nad 900 Kč.

Přes všechna vylepšení si tento model dokázal udržet stejný výkon i váhu jako jeho předchůdce.



Obrázek 3.2: Raspberry Pi 3 model B+ [5]

3.1.2.3 Raspberry Pi 3 A+

Téhož roku jako model B+ se vydala adaptace Raspberry Pi, a to model A+.

Jedná se o zmenšenou verzi modelu B+, ale se zachovaným výkonem. Pro práci na menších projektech či jako levnější variantu je vhodnou alternativou pro model B+. Téže obsahuje WiFi a Bluetooth moduly pro zprostředkování bezdrátové komunikace.

Nicméně jeho velikost má svá úskalí a je zde zmenšená velikost operační paměti, což by z hlediska budoucího rozšíření mohl být problém.

Cenově se tato deska prodává přibližně za 800 Kč. Další specifikace jsou:

[2]Hardware Attached on Top - jde o přídavné desky či celkově hardware, který rozšiřuje funkcionalitu daného RPI. v konkrétním případě lze nalézt takový modul například tady(link)

Procesor	Cortex-A53 (1,4 GHz 64-bit quad-core)
Grafické jádro	Broadcom VideoCore IV u 3D grafiky 300 MHz, video 400 MHz
Paměť	512 MB(sdílená s GPU)
USB porty	1 (verze 2.0)
Interní paměť	Micro SDHC a USB boot mode
Nízkoúrovňové periferie	40 GPIO pinů a HAT ID sběrnice
Rozměry	65 mm x 56 mm
Hmotnost	29 g
Cena	800,- Kč(přibližná cena)

Tabulka 3.2: Specifikace shrnující klíčové informace o RPI3A+

Obrázek 3.3: Raspberry Pi 3 model A+[6]

3.1.3 Raspberry Pi 4 B

Raspberry Pi se svou novou řadou 4 přišla zatím s jediným modelem, ale za to opravdu s pořádnou novinkou a inovací na trhu. První model B přišel v létě roku 2019 a výrobci se pyšní, že jejich produkt již dokáže být plnohodnotnou náhradou PC.

Oproti minulé řadě se změnila drtivá většina klíčových vlastností. Bylo zvykem, že maximální velikost operační paměti byla pouze 1 GB, ale nově tento model vydávají ve třech variantách, které se liší ve velikosti operační paměti(1/2/4 GB). U procesoru se zmenšila technologie na 28 nm a taky se zrychlil. Grafická výbava se také pozměnila, takže nyní místo VideoCore verze IV je verze VI, která je schopná přehrávat 4k video a podporuje režim 2 obrazovek.

Napájení bylo také vylepšeno, takže se používá napájecí konektor USB-C. Bezdrátovou komunikaci vylepšilo Raspberry Pi pouze na straně Bluetooth

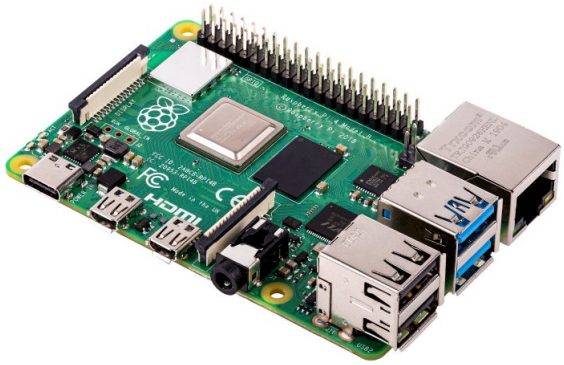
na verzi 5.0. Inovace proběhly i u vstupně výstupních konektorů, takže se zde vyskytují nově USB 3.0 konektory a 2 microHDMI konektory pro přenos obrazu.

Cena tohoto modelu se různí podle typu, ale verze se 4 GB operační paměti se pohybuje okolo 1 500 Kč.

Specifikace tohoto modelu:

Procesor	Cortex-A72 (1.5 GHz 64-bit quad-core)
Grafické jádro	Broadcom VideoCore VI 500 MHz
Paměť	1/2/4 GB(sdílená s GPU)
USB porty	4 (2 verze 2.0 a 2 verze 4.0)
Interní paměť	Micro SDHC a USB boot mode
Nízkoúrovňové periferie	40 GPIO pinů a HAT ID sběrnice
Rozměry	88 mm x 58 mm x 19,5 mm
Hmotnost	46 g
Cena	1 500,- Kč(přibližná cena)

Tabulka 3.3: Specifikace shrnující klíčové informace o RPI4B [7]



Obrázek 3.4: Raspberry Pi 4 model B 4 GB RAM [8]

3.1.4 Výběr vhodné řídící jednotky

Řídící jednotky, které jsem v této kapitolce pokryl, splňují veškeré základní předpoklady pro použití do projektu. Nicméně při porovnávání jsou zde rozdíly cenové i výkonnostní. V následující tabulce je uvedeno základní shrnutí parametrů, které jsem uvedl výše.

	RPI3B	RPI3B+	RPI3A+	RPI4B
Procesor	1,2 GHz	1,4 GHz	1,4 GHz	1.5 GHz
Grafické jádro	400 MHz	400 MHz	400 MHz	500 MHz
Paměť	1 GB	1 GB	512 MB	4 GB
USB porty	4	4	1	4
Rozměry (mm)	85,60 x 56,5 x 17	85,60 x 56,5 x 17	65 x 56	88 x 58 x 19,5
Hmotnost	45 g	45 g	29 g	46 g
Cena	800,- Kč	900,- Kč	800,- Kč	1 500,- Kč

Tabulka 3.4: Tabulka shrnující posbírané informace. Zelená a oranžová barva označují nejlepší model v jednotlivých kategoriích. Červená barva naopak ten nejhorší model v dané kategorii.

Nejstarší ze zmiňovaných, Raspberry Pi 3 B, nepodporuje dnešní používané ethernetové standardy. Navíc jeho cena se pohybuje výše než je cena modelu 3A+, který je i výkonnější. Tudíž model 3B není z vybíraných modelů nejvhodnější.

Jeho nástupce a vylepšená verze, Raspberry Pi 3 B+, je o poznání lepší co se týče dodržování dnešních standardů a také výkonu. Poskytuje širokou škálu konektorů pro připojení zařízení přes USB či obrazu přes HDMI výstup.

Nejmenší model Raspberry Pi 3 A+ je, dalo by se říct, ideálním kandidátem pro projekt. Bohužel s menší velikostí přichází zmenšení operační paměti na polovinu, oproti modelu 3B+, takže při dlouhodobějším běhu by mohl stagnovat výkon. Také celková robustnost systému by byla omezenější, takže možné přidávání funkcionalit systému by bylo obtížnější.

Poslední kandidát, Raspberry Pi 4 B, je ze všech nejvýkonnější a nejmodernější. Do budoucna je rozhodně jednoznačnou volbou. Největším problémem je zde momentální cena na trhu. Další nevýhodou produktu je, že vyšel relativně nově a stále některé věci nejsou úplně odladěny co se týče SW stránky. V bližší budoucnosti jak se odladí kompatibilita pro tento model, tak bude standardem udávající trend v mikropočítačích.

Z těchto čtyřech možností se v současné době jeví jako nejhodnější model 3B+. Ten poskytuje dostatečně velký výkon pro všechny naše potřeby a měl by je zvládat s přehledem. Navíc je tento model již široce používaný, takže má velkou a aktivní komunitu, která má s tímto typem již bohaté zkušenosti. Asi poslední, ale také důležitou, výhodou je cena, která oproti modelu 4B je o několik set korun menší, takže je daleko dostupnější pro kohokoli.

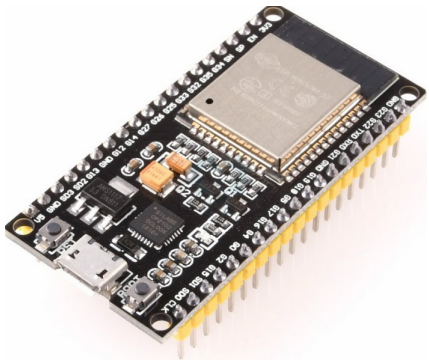
3.2 Analýza komunikačních modulů

Analýza komunikačních modulů je však mnohem složitější problém než analýza jednotlivých verzí RPI. Komunikační moduly mají sloužit čistě pro sběr

informací a při jakékoli neobvyklé naměřené hodnotě posílat data řídící jednotce. Pro takový typ úkolu se jeví jako vhodná vývojová deska ESP[3].

3.2.1 Modul ESP32

Střední cenová varianta mezi ESP8266 a RPI zero. Modul ESP32 je velikosti běžného palce, ale nehledě na jeho velikost poskytuje mnoho možností uplatnění. Výkon zajišťuje dvoujádrový procesor o frekvenci 160 MHz, díky kterému lze používat komplikovanější kód a nebát se problémů s výkonem, Velké množství GPIO pinů mu poskytují možnosti ovládat vícero zařízení najednou. Navíc důležitou vlastností tohoto modulu je, že poskytuje hardwarově zrychlené šifrování (Hardware Accelerated Encryption), což provádí rychlejší výpočet kryptografických funkcí pro AES, SHA2, eliptické křivky nebo RSA do 4096 bitů.

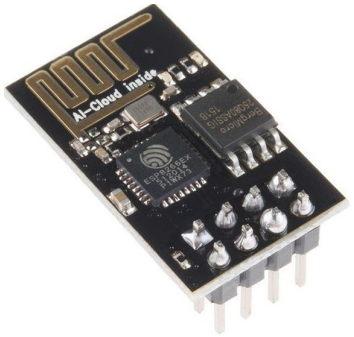


Obrázek 3.5: Modul ESP 32 [9]

3.2.2 Modul ESP8266

Jedná se o nejlevnější a nejmenší variantu z uvažovaných modulů vůbec. ESP8266 je přibližně o trochu větší než nehet na palci a jeho cena se pohybuje okolo 100 Kč. Tyto parametry ho dělají nejvhodnějším kandidátem pro použití, ale má též svá úskalí. Výkon modulu je žalostně nízký v porovnání s ESP32, protože ho pohání procesor o jednom jádru s frekvencí 80 MHz. Jak ESP32 tak i ESP8266 jsou programovatelné pomocí Arduino IDE, což je ideální a nenáročná varianta pro programování těchto modulů.

[3]Výrobce těchto vývojových desek je Espressif Systems. První tři písmena jména výrobce (ESP) tvoří zkratku používanou pro jejich desky.



Obrázek 3.6: Modul ESP 8266 [10]

3.2.3 Raspberry Pi zero

Jedná se o úspornější a mnohem menší variantu RPI. Díky těmto rozdílům je i mnohem levnější, jeho cena se pohybuje od 150 Kč výše. Nicméně základní verze neobsahuje ani integrovaný WiFi modul, ale prodává se i v různých verzích, které ho už obsahují.

Verze jsou označovány písmeny W, H nebo WH. Písmeno W značí, že je na desce je též integrovaný WiFi modul, který poskytuje desce bezdrátovou komunikaci. Písmeno H označuje přídavek GPIO headru na desku, díky které může RPI ovládat ostatní zařízení. Kombinace obou písmenek jen říká, že obsahuje obě zmíněné nadstavby. Bohužel, ale poté se cena zvedá až na 430 Kč přibližně.

Obrázek 3.7: Raspberry Pi zero WH [11]

3.2.4 Výběr vhodného modulu

Po porovnání všech parametrů se jeví ESP32 jako nejvhodnější modul pro účely bakalářské práce. Je dostatečně výkonný, za přijatelnou cenu a navíc poskytuje zrychlený výpočet kryptografických funkcí pro případné použití. Zde bude plnit pouze funkci sbíraní dat ze senzorů, jejich analýzu a případné posílání upozornění řídící jednotce, což by zvládl i modul ESP8266. Vybral jsem ESP32 kvůli dostatečnému výkonu pro možná rozšíření funkcionalit sys-

tému, takže v budoucnu by komunikační modul mohl sbírat data z vícero senzorů a podobně.

3.3 Ostatní komponenty systému

Tato podkapitola popisuje výběr senzorů, které jsou připojeny k jednotlivým komunikačním modulům. Dále jsou zde uvedeny součástky, které jsou připojeny k řídící jednotce. Jedná se o kameru, GSM modul a kódový zámek.

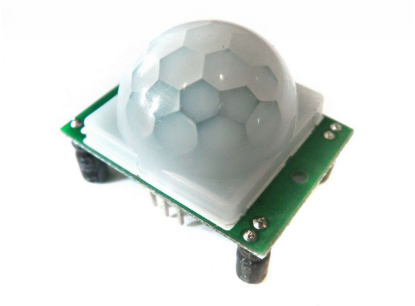
Vhodný senzor je ten, který bude plnit svůj účel, tudíž dokáže detekovat problematickou situaci správně. Toto je základní podmínka pro výběr senzoru, který chci v bakalářské práci použít. Kolegové v pracích, ze kterých jsem čerpal, rozebírali širokou škálu senzorů různých typů a variant. Zde budou vybrány ty efektivnější z nich a budou podrobeny zkoumání, zda jsou pro moji situaci vhodné.

3.3.1 Detektor vniknutí

Problematika vniknutí se dá řešit mnoha způsoby, ať už je to typické pohybové čidlo, magnetický dveřní kontakt či různé jiné varianty. Jedna ideální metoda neexistuje a jak kolega Miroslav Váňa ve své práci zkoumal, tak reálnou spolehlivou hodnotu čidel zajistí větší počet vstupů. Data se poté mohou porovnávat a pokud se všechny či většina čidel shoduje o proniknutí, tak se zahájí nouzový stav. Já se snažím cílit na praktičnost řešení, tudíž se nabízí dvě varianty:

Senzor pohybu HC-SR501

Princip práce senzoru je poměrně přímočarý. Pracuje ve 120 stupňové výseči před sebou na vzdálenost až 7 metrů přibližně a v této oblasti dokáže rozpoznat pohybující se objekty. V případně pohybu vysílá signál, který je dále zpracován v komunikačním modelu a ten dále upozorní řídící jednotku, aby uvědomila majitele. Výhoda tohoto senzoru je, že dokáže pokrýt mnohem větší oblast a dává jednoznačný signál. Nevýhodou je, že má podstatně větší odběr než druhý kandidát, což z dlouhodobého hlediska pro externí napájení může způsobit nutnost častější výměny zdroje. [12]

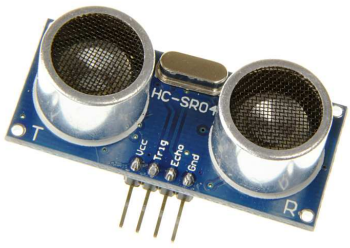


Obrázek 3.8: Senzor pohybu HC-SR501. Ilustrační obrázek.

[13]

Ultrazvukový měřič vzádlenosti HC-04

V tomto případě senzor plní trochu jinou úlohu a je vhodnější taky na jiné situace. Senzor měří vzdálenost v rovné čáře spolehlivě do čtyř metrů, tudíž se hodí na užší koridory či přesnější měření vzdálenosti. Tento typ čidla by se při instalaci musel nakalibrovat na výchozí vzdálenost, aby pak následně mohlo detekovat jakýkoliv druh narušení v přímce. Zamýšlené použití je využití u vstupních dveří a oken, kde by dokázal detekovat jakoukoli změnu přímo u vstupu do sklepa. Značnou výhodou je nižší spotřeba a variabilita použití daného senzoru pro jiné účely. Jeho nevýhody zase naopak jsou dosah (4 metry) a pokrytí užšího spektra. [14]



Obrázek 3.9: Měřič vzádlenosti HC-04. Ilustrační obrázek.

[15]

Vybraný senzor

Jako vhodnější ze dvou výše uvedených variant se jeví jako vhodnější senzor pohybu HC-SR501. Jeho pokrytí je hodně velké, tudíž dokáže pokrýt okna i vstupní dveře najednou například. Nemusím ani řešit žádnou kalibraci, protože senzor pohybu se během úvodní minuty nastaví sám a následně jen vysílá jednoznačný signál zda je detekován pohyb.

3.3.2 Detektor nezdravého ovzduší

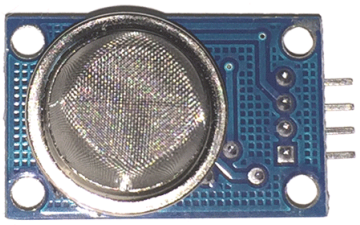
Ve vinném sklepě je období, kdy se systém musí zajímat nejen o bezpečnost majetku ale i bezpečí samotného vinaře. Během doby, kdy kvasí víno ve sklepě, dochází přeměně cukrů na alkohol. Proti oxidu uhličitému se bojuje velmi těžce, protože je bezbarvý či bez zápachu, takže je velice nebezpečný ve vyšší koncentraci.

Pro detekci oxidu uhličitého se na trhu nabízí celá řada senzorů, některé jsou uvedeny v následující tabulce. Nejdůležitější je však vybrat ten správný model, který by odpovídal požadovaným parametrům a byl kompatibilní s vyvíjeným systémem.

Model	Měřené plyny	**Model**	Měřené plyny
MQ-2	Metan, butan, kouř	MQ-3	Alkohol, ethanol
MQ-4	Metan, CNG	MQ-5	Zemní plyn, LPG
MQ-6	LPG, butan	MQ-7	Oxid uhelnatý
MQ-8	Vodíkový plyn	MQ-9	Oxid uhelnatý, hořlavé plyny
MQ131	Ozón	**MQ135**	**Kvalita ovzduší**
MQ136	Plynný sirovodík	MQ137	Amoniak
MQ138	Benzen, Toluen	MQ214	Methan, Zemní plyn
MQ216	Zemní plyn, svítiplyn	MQ303A	Alkohol, ethanol
MQ306A	LPG, butan	MQ307A	Oxid uhelnatý
MQ309A	Oxid uhelnatý, hořlavé plyny		

Tabulka 3.5: Tabulka vysvětlující typy použití jednotlivých modelů řady MQ. U každého modelu je uvedeno, na který typ plynu je čidlo citlivé. Tabulka je převzata z [16]

Z uvedených modelů je nejvhodnější variantou model MQ135, který měří kvalitu ovzduší. Reaguje na vícero plynů než jen na oxid uhličitý, který nás zajímá, ale i na amoniak, oxidy dusíku, benzen či kouř. Nicméně pro účely projektu se tyto ostatní prvky mohou dát stranou, protože se moc ve sklepě vyskytovat nebudou, obzvláště u podlahy sklepa v období kvašení vína. Oxid uhličitý je těžší než vzduch, tudíž se usazuje u podlahy, ale při vyšších koncentracích by mohl ohrozit samotného vinaře. Naštěstí tyto větší koncentrace MQ135 dokáže zachytit, a proto je vhodným adeptem.



Obrázek 3.10: Senzor plynů MQ-135 měřící kvalitu ovzduší [16]

3.3.3 Kamera

Jelikož je bakalářská práce vymezena pouze na platformu RPI, tak příhodným způsobem jak zakomponovat kameru k řídící jednotce je pomocí CSI [4] rozhraní. Díky tomu jsme schopni kameru jednoduše ovládat a nemusíme používat žádnou externí kameru přes USB rozhraní. Dalším faktorem, proč použít kamery používající CSI rozhraní, je poměr cena výkon, protože kamery v podobných cenových relacích zvládají také natáčet i fotit, ale se značně horší kvalitou než poskytují RPI kamery.

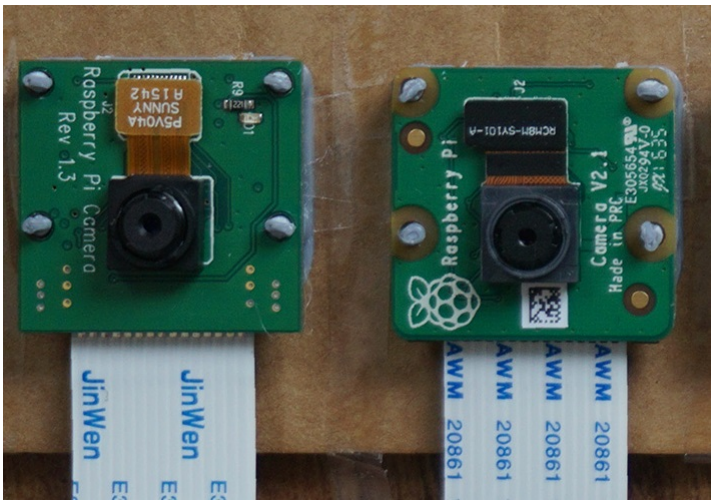
Porovnání RPI kamer

V současné době jsou na trhu dvě možnosti, a to RPI kamera v1.3 nebo v2.1. Starší z obou zmíněných je v1.3 a byla vydána již v roce 2013. Rozlišení této kamery je 5 megapixelů a dokáže dělat fotografie o celkovém rozlišení až 2592 x 1944 pixelů. Video zvládá na 1080p 30 snímků za sekundu nebo 720p 60 snímků za sekundu. Cena této kamery je přibližně 670 Kč.

Novější kamera v2.1 vyšla v roce 2016 a představila se větším rozlišením, které je 8 megapixelů, tudíž celková kvalita pořízených záběrů pomocí této kamery je značně kvalitnější. Fotografie dosahují rozlišení až 3280 x 2464 pixelů, ale video zůstalo ve stejné kvalitě 1080p 30 snímků nebo 720p 60 snímků. Cena této kamery se pohybuje kolem 850 Kč.

Největší rozdíl, který mě zajímá, je v zorném úhlu objektivu kamery. Pro bakalářskou práci je to důležité, protože větší zorný úhel objektivu, konkrétně spíše ten horizontální, mi poskytuje možnost vidět větší část místnosti sklepa jednou kamerou. Horizontální zorný úhel u RPI kamery v1.3 je 53 stupňů a vertikální 41 stupňů. RPI kamera v2.1 má horizontální zorný úhel 62 stupňů a vertikální 49 stupňů. Rozdíl se zdá minimální na první pohled, ale při bližším zamyšlení i necelých deset stupňů udělá značný rozdíl na větší vzdálenosti.

[4] CSI - Camera Serial Interface - je standardizované rozhraní pro propojení kamery s procesory mobilních a smart zařízení. Jedná se standard globální aliance MIPI, která vyvíjí technické specifikace jako je například toto rozhraní. Nejnovějším standardem je CSI-3. Více informací na: `https://www.mipi.org/`



Obrázek 3.11: Vizuální srovnání obou verzí kamer vedle sebe. Vlevo můžete vidět RPI kameru v1.3 a vpravo v2.1 [17].

Z výše uvedených dat vyplývá, že RPI kamera v2.1 je značně kvalitnějším zařízením pro pořizování záznamu. Její vyšší cena, přibližně o 200 Kč, však vypovídá, že už není určena pro menší projekty a pokud se člověk chce spíše naučit pracovat s RPI kamerami, tak je to možná i lepší volba. Nicméně za účelem pořizováním kvalitnějších záběrů a obzvláště kvůli většímu zornému úhlu je pro moji bakalářskou práci lepší RPI kamera v2.1.

Na trhu jsou také RPI kamery s přívlastkem NoIR, což značí, že jsou bez infračerveného filtru. Tyto kamery se používají spíše jako kamery pro noční vidění, když se k nim přidá IR LEDka, která vyzařuje infračervené záření, tak kamera má obstojný obraz i v kompletní tmě. Tyto kamery mohou být zajímavým vylepšením navrhovaného bezpečnostního systému.

3.3.4 GSM modul

Účelem GSM modulu je poskytnutí propojení bezpečnostního systému s mobilní sítí. Zařízení ještě umožňuje vytáčení telefonů, posílání SMS zpráv či jiných dat do internetu pomocí mobilního operátora. Obvykle lze vložit do takového zařízení SIM kartu, díky které GSM modul získá připojení k síti operátora. Všechny funkcionality daného modulu se odráží na tom jaký typ účtování či tarifu je na dané SIM kartě s operátorem domluvený.

Po kratším průzkumu jsem našel dvě varianty, které jsou popsány níže, pro použití v rámci mojí bakalářské práce.

GSM USB modul

Jedním z možných řešení pro připojení do mobilní sítě je právě GSM modul. Nejčastěji člověk narazí na níže ilustrovaný USB modul, který se mnohdy

liší pouze v logu mobilního operátora či výrobce. Použití tohoto zařízení je elegantně vyřešeno pouze zasunutím modulu do USB rozhraní a následně ho můžeme použít pro posílání zpráv, telefonování či přístupu do internetu. Pozitivní vlastností tohoto řešení je, že modul jde použít i jinde, protože USB rozhraní je v dnešní době téměř na všech zařízeních.

Obrázek 3.12: GSM modul značky Huawei [18]

GSM HAT pro Raspberry Pi

Z kategorie HAT modulů jsem jako nejvhodnějšího kandidáta zvolil Waveshare HAT modul. HAT modul se nasadí přímo na RPI a díky tomuto modulu RPI získá celou řadu nových funkcionalit. Tento modul podporuje SMS, MMS a telefonní hovory co se týče mobilního připojení ale také GPS či polohování LBS. Jeho funkce tímto nekončí, je jich celá řada, ale pro potřeby práce tento modul splňuje požadavky na to, aby byl použitelný v mém bezpečnostním systému. Cena tohoto HAT modulu se pohybuje lehce přes 1 000 Kč.

Obrázek 3.13: GSM modul značky Waveshare [19]

Výběr

Vhodnějším a jednodušším řešením je použití varianty USB modulu. HAT modul je naopak mnohem více multifunkční, ale je vhodnější spíše pro lidi, kteří by chtěli více experimentovat s připojením do mobilní sítě, GPS či jinými dovednostmi. Pro účely bakalářské práci bohatě stačí USB modul.

3.3.5 Kódový zámek

Jedinou vstupní periferií celého systému je kódový zámek. Jeho úkolem je poskytovat možnost napsaní vstupní hesla do systému, aby se mohl autorizovat majitel sklepa. Dále ještě poskytuje možnost manuálního resetu, pomocí funkčního tlačítka, aby se řídící jednotka mohla opět dostat do výchozího stavu.

Pro tyto účely RPI má značnou výhodu, protože se k desce může pomocí USB rozhraní připojit jakákoliv periferie. Tudíž jako vstupní periferii můžu použít klasickou klávesnici či pouze numerickou klávesnici.

Další možností jsou zde speciální klávesnice, které mají omezený vstup a propojují se pomocí GPIO pinů. Jednou z takových je například klávesnice značky eses. Jedná se o malou membránovou klávesnici, která má na sobě číslice 0 až 10, hvězdičku, křížek a čtyři programovatelná tlačítka. Její cena je také poměrně nízká, začíná přibližně okolo 30 Kč.

Jednou velkou nevýhodou této klávesnice je, že jediné, co na výstupu posílá, je signál na určitých pinech, které korespondují se souřadnicí zmáčknutého tlačítka. Existují knihovny, které zjednodušují práci s touto klávesnicí, ale celkově se spíše používá při použití u Arduina.

Obrázek 3.14: Membránová klávesnice značky eses [20]

Pro mou bakalářskou práci je vhodnější použít klasickou klávesnici. Poskytuje větší škálu tlačítek, s kterými můžeme pracovat, a je s ní mnohem jednodušší práce, díky USB rozhraní.

Kapitola 4

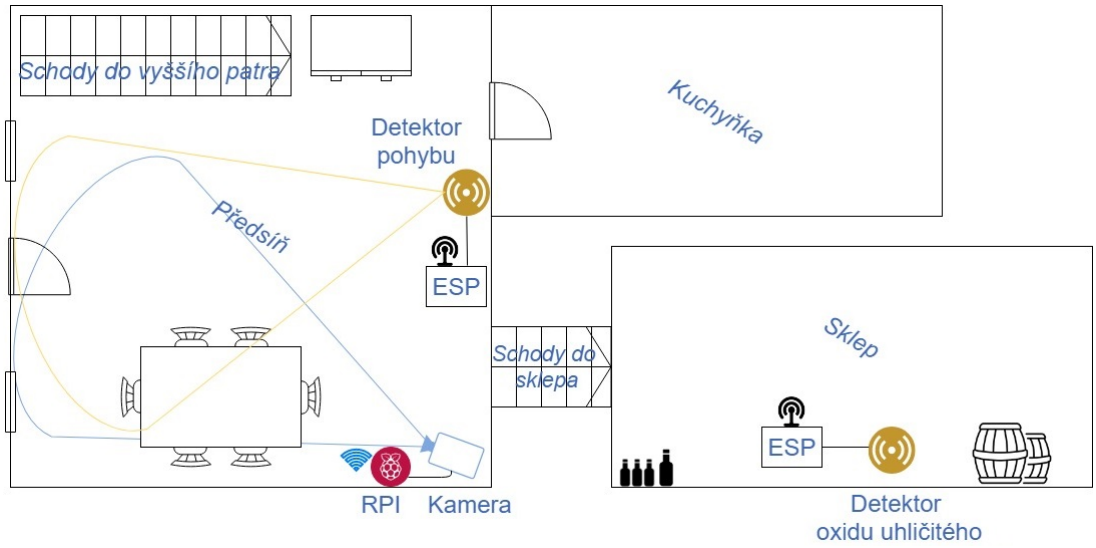
Návrh systému

V této kapitole je popsáno, jak je vymyšlen celý koncept bezpečnostního systému. Vysvětluje principy fungování jednotlivých částí v systému, jaký je jejich účel, jak jsou zapojeny či jak probíhá jejich komunikace se zbytkem systému. Je zde i popsán stavový diagram systému, ve kterém jsou přehledně ukázány jednotlivé stavy a co může systém vyhodnotit. Dále je zde probrána cena celého systému včetně odlišností od práce kolegy Miroslava Váni[1].

4.1 Hlavní koncept

Systém se skládá ze 2 hlavních částí, a to řídící jednotky a komunikačního modulu. Tyto části mezi sebou provozují bezdrátovou komunikaci, pokud je nutné, jinak setrvávají v klidovém režimu.

Z analýzy uvedené v Kapitole 3 jednoznačně vyplynul výběr použitých HW komponent/součástí, které jsou dále popsány v jednotlivých podkapitolách.



Obrázek 4.1: Základní ukázka systému. Ve spodní části obrázku se pod symbolickým logem Raspberry Pi nachází řídící jednotka, ke které jsou připojeny GSM modul a kamera. Dále jsou na dvou místech rozmístěny komunikační moduly ESP, které slouží pro sběr dat ze senzorů, jejich vyhodnocení a případné zaslání varovné zprávy řídící jednotce.

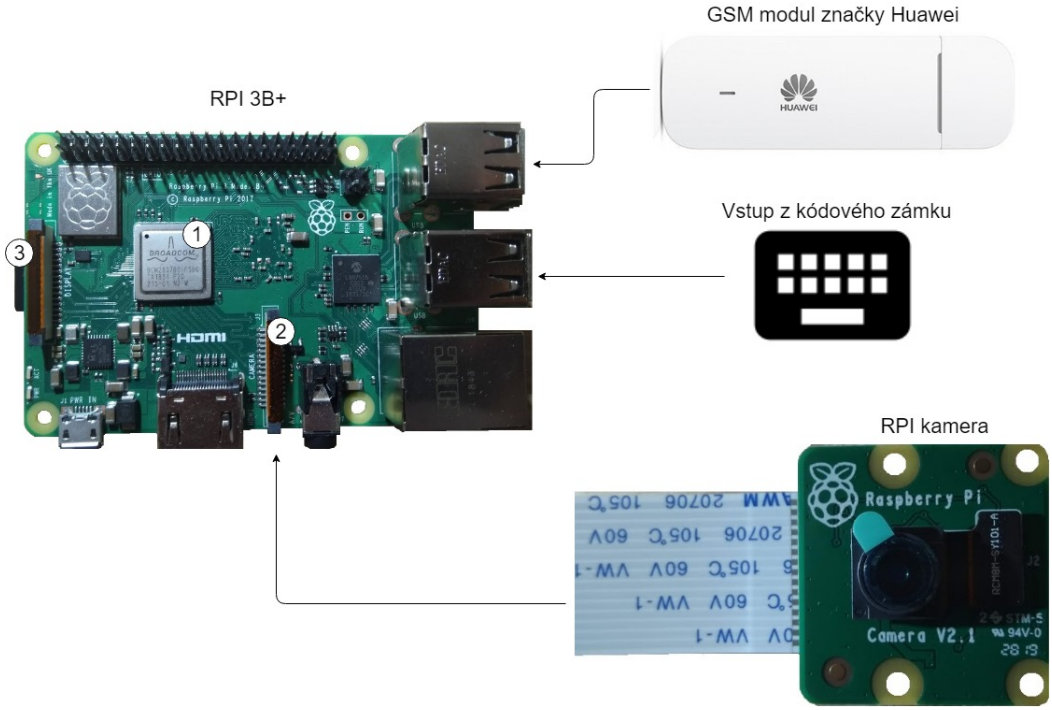
4.1.1 Principy řídící jednotky

Jako řídící jednotku jsem si v podkapitole 3.1 zvolil Raspberry PI 3 model B+. Je to hlavní mozek celého systému, který zpracovává informace z ostatních modulů a podle toho provádí další kroky.

Zvolená řídící jednotka poskytuje možnost autentizace majiteli pomocí kódového zámku, kde po příchodu do sklepa má určitý čas, než ho systém detekuje jako nechtěné vniknutí. Stačí znalost hesla, které naťuká skrze vstup do řídící jednotky, potvrdí a systém se přepne do klidového stavu.

Při vniknutí do sklepa se zapne kamera, která udělá záznam celého vniknutí. Pokud se ve sklepě nahromadí větší koncentrace oxidu uhličitého, řídící jednotka zkontroluje, zda se ve sklepě někdo nachází a následně se rozhodne, jestli poslat upozornění majiteli. Varovný signál z bzučáku je vyslán vždy. Dále také dělá textové záznamy, ve kterých je uveden přesný čas a datum vzniku záznamu, od kterého čidla bylo obdrženo upozornění a případně cesta k uloženému záznamu z kamery.

Pokud se ve sklepě nenachází majitel a nastane vniknutí, systém upozorní majitele o této události pomocí GSM modulu zapojeném v USB rozhraní. GSM modul slouží jako připojení řídící jednotky do mobilní sítě, aby mohla poslat danou zprávu.



Obrázek 4.2: Názorné schéma zapojení klíčových periferií a prvky u řídící jednotky. Číslem 1 je označen integrovaný Wi-Fi modul, zprostředkovávající bezdrátovou komunikaci v systému. Dále na obrázku jsou vidět GSM modul a vstup z kódového zámku, které jsou připojené přes USB. RPI kamera je připojena přes rozhraní integrovaném přímo na desce označené číslem 2. Vlevo je pod číslem 3 umístěna SD karta, která slouží jako úložiště pro celou desku a je zde nahraný operační systém.

Pořizování záznamu a jeho ukládání

Samotný video záznam je poměrně velká položka v řídící jednotce. Běžné bezpečnostní kamery nepořizují záznamy ve vysoké kvalitě, protože vyšší rozlišení znamená podstatně větší náročnost na kapacitu zařízení kam se záznam ukládá.

Hlavním parametrem, který ovlivňuje velikost souboru video záznamu, je rozlišení kamery. Cílem je mít co nejmenší rozlišení pro úsporu paměti, ale na druhou stranu je potřeba pořizovat dostatečně kvalitní záznam, aby bylo možné rozeznat tvář osoby na záznamu např. Kapacita řídící jednotky se odvíjí od použité paměťové karty, ale reálně se systém musí snažit pracovat úsporně.

Z možných konfigurací [21] mé kamery jsou nejmenší rozlišení 1280x720 nebo 640x480. Menší ze zmíněných rozlišení je už poměrně dost nekvalitní a při zaznamenávání celé místnosti nejsou zřejmé detaily. Zásadním problémem je

částečné omezení zorného pole kamery, ale z důvodu úspory místa lze na tento fakt opomenout.

Výsledný záznam vniknutí může být poměrně dlouhý, tudíž výsledná velikost souboru bude v řádech GB. Z toho důvodu je vhodné mít fixně stanovenou maximální délku nahrávání.

Zajímavou myšlenkou je použití principu cyklické fronty pro natáčení. Po dosažení určité délky záznamu, například 10 minut, by se začal soubor od začátku znovu přemazávat, takže by vždy bylo k dispozici alespoň posledních 10 minut záznamu. Nicméně tento přístup je spíše vhodný pro monitorovací kamery, které pracují nepřetržitě a poskytují živý přenos aktuálního dění v pozorované oblasti.

4.1.2 Principy komunikačního modulu

Z analýzy v podkapitole 3.2 jsem si jako modul pro bezdrátovou komunikaci vybral ESP32. Hlavním cílem tohoto modulu je sledování senzorů, které jsou k němu připojeny, poslouchat příkazy od řídící jednotky a upozornit řídící jednotku na rizikový stav v systému.

ESP je čistě autonomní a nepotřebuje příkazy od řídící jednotky pro svůj chod. Jeho primárním cílem je sledovat data na senzorech, což zpracovává a nepotřebuje žádný vnější impulz. Díky tomu může zredukovat používání zdrojů, protože nepotřebuje nutně vždy používat svůj integrovaný Wi-Fi modul.

Pokud však dostane ze senzorů data, které značí rizikový stav, nastává zahájení bezdrátové komunikace s řídící jednotkou. Hlavním účelem této komunikace je nahlásit neobvyklou situaci na senzoru, aby potom řídící jednotka mohla provést jeden ze scénářů.

V případě, že ESP má k sobě připojený senzor kvality ovzduší, má k sobě téže připojený i bzučák, kterým dokáže přímo v místě výskytu upozornit majitele na zvýšený obsah oxidu uhličitého. Modul v pravidelných intervalech bude vydávat signalizaci bzučákem o špatném stavu ovzduší. V ostatních případech, kdy k ESP není připojen senzor kvality ovzduší, je k modulu připojen pouze senzor, který má obsluhovat. Každý modul je ještě vybaven externím napájením z tužkových baterií.

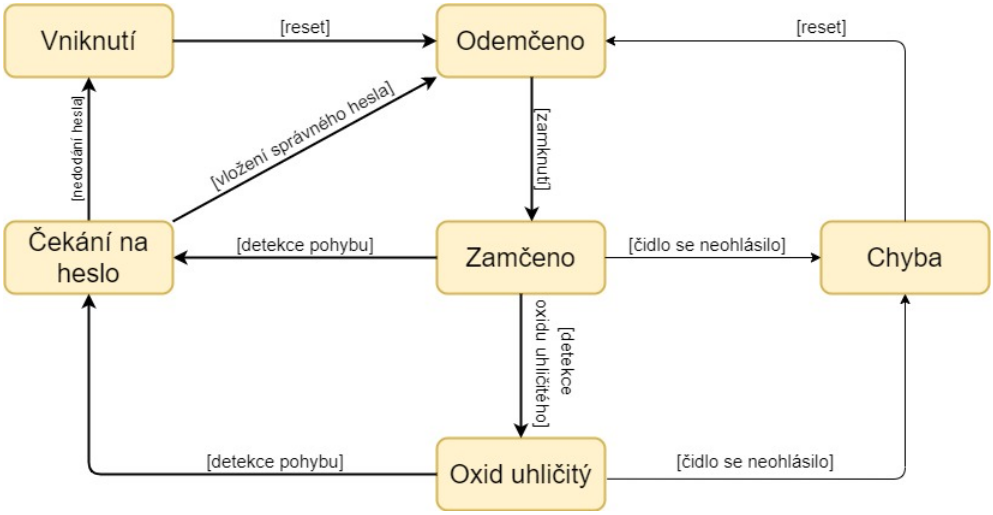
Komunikační modul se také musí umět ohlásit řídící jednotce, že je funkční a je schopen komunikovat. V pravidelných intervalech posílá řídící jednotce zprávu, aby řídící jednotka věděla, že komunikační modul je v dosahu a nic neruší jejich komunikaci.

4.2 Stavová logika systému

Systém je navržen tak, aby jeho chování bylo možné popsat stavovým diagramem. Na základě událostí (akcí) může systém přecházet mezi jednotlivými stavy, které jsou definovány níže. Vzhledem k tomu, že se celý systém skládá ze dvou nezávislých logických částí, vytvořil jsem dva nezávislé stavové diagramy pro každou z nich.

4.2.1 Logika řídící jednotky

Stavy u řídící jednotky jsou ve stručné formě, a to stavy Odemčeno, Zamčeno, Čekání na heslo, Oxid uhličitý, Chyba a Vniknutí. Systém je neustále v provozu nehledě na jeho současný stav. Níže jsou popsány akce, které vykonává řídící jednotka, při přechodu do každého stavu.



Obrázek 4.3: Stavový diagram řídící jednotky obsahující stavy a přechody mezi nimi. U každého přechodu je v hranatých závorkách zaznačeno jaká událost se musí stát, aby systém přešel z jednoho stavu do druhého. Podrobný popis jednotlivých stavů je v odstavcích pod obrázkem.

Stav Odemčeno

Při prvotním spuštění se systém nachází ve stavu Odemčeno. Během tohoto stavu systém neposílá žádné zprávy přímo majiteli sklepa, ale všechny ostatní čidla stále fungují. Zprávy od čidel jsou ignorovány, ale veškeré zprávy o komunikaci jsou stále zaznamenávány. Jediný přechod je do stavu zamčeno. Do stavu zamčeno se systém dostane, když majitel zadá heslo pro uzamknutí systému. Naopak přechody do stavu odemčeno jsou dva. Ze stavu Čekání na heslo se systém dostane při příchodu majitele do sklepa, zadáním kódu a po-

tvrzením na zámku. Pokud by uživatel chtěl systém odemknout, přestože by se nacházel ve stavu vniknutí, musí ho manuálně resetovat, aby chování systému bylo opět v pořádku.

Stav Zamčeno

Systém se může dostat do stavu zamčeno pouze, když už systém běží a zamkne ho manuálně majitel pomocí kódového zámku. Během tohoto stavu se chování systému mění tak, že při obdržení jakékoli zprávy, danou zprávu si zaznamená a provede nějakou akci. Přechody z tohoto stavu jsou dva. Pokud je detekován pohyb, systém přechází do stavu Čekání na heslo. Když systém detekuje zvýšenou hladinu oxidu uhličitého přechází do stavu Oxid uhličitý.

Stav Oxid uhličitý

V tomto stavu vím, že se objevila větší koncentrace oxidu uhličitého ve sklepě, tudíž systém si danou skutečnost zaznamená a pošle informaci majiteli, takže majitel při své další návštěvě ví, že by měl vyvětrat ve sklepě. Tato zpráva se posílá majiteli pouze jednou. Pro systém je tento stav takovým mezi stupněm stavu Zamčeno, kdy systém stále reaguje na detekci pohybu a pokud nějaký detekuje, přechází do stavu Čekání na heslo.

Stav Chyba

Řídící jednotka může přejít do stavu Chyba, když se komunikační modul v určité době neozve řídící jednotce. Jakmile řídící jednotka zjistí, že je část systému nefunkční, oznámí tuto skutečnost majiteli. Omezení funkčnosti systému může být kritické, takže jediný způsob jak znovu zprovoznit systém je resetování celého systému. Tomu předchází manuální zjištění závady v systému a případnou náhradu komponent systému.

Stav Čekání na heslo

Jakákoliv detekce pohybu ve stavu Zamčeno či Oxid uhličitý znamená, že systém se přesouvá do stavu Čekání na heslo. Systém začíná pořizovat záznam kamerou, jakmile do tohoto stavu přejde. Poté nastává 30 sekundový čekací interval, jestli detekovaná osoba vloží správné heslo do systému. Pokud se tak stane, systém přechází do stavu Odemčeno a smaže pořizovaný videozáznam. Jestliže se nezadá správné heslo třikrát nebo uplyne zmíněných 30 sekund, detekovaný pohyb je vyhodnocen jako hrozba, takže nastává přechod do stavu Vniknutí.

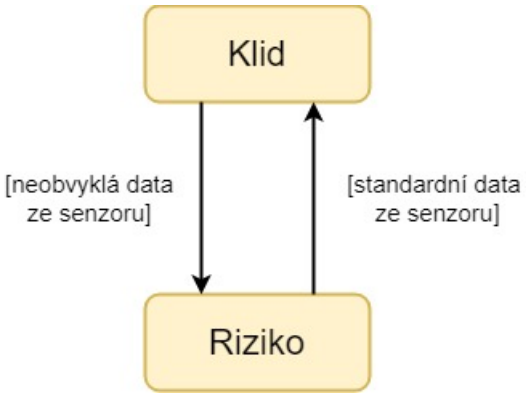
Stav Vniknutí

Když systém přejde do tohoto stavu, znamená to, že opravdu nastalo nedovolené vniknutí do sklepa. Systém informuje majitele o této skutečnosti pomocí zprávy na jeho mobilní zařízení. Již od stavu Čekání na heslo pracuje kamera,

připojená k řídící jednotce, a zaznamenává celou skutečnost. Po vniknutí a návratu majitele do sklepa se systém může už pouze zresetovat pomocí tlačítka do stavu Odemčeno, aby se obnovil chod systému. Okrajovým případem je, že systém přejde do tohoto stavu, když majitel nezadá včas heslo nebo ho zadal vícekrát špatně. I v tomto případě je majitel informován zprávou, protože systém nerozpoznává, zda se o vstup pokoušel majitel či zloděj.

4.2.2 Logika komunikačního modelu

Komunikační modul nezávisle na řídící jednotce pracuje a také se jinak chová. Proto je zde druhý stavový diagram, který vysvětluje chování komunikačního modulu, a to pomocí stavů Klid a Riziko. Systém se chová čistě v závislosti na vstupu od připojeného senzoru.



Obrázek 4.4: Stavový diagram komunikačního modulu obsahující stavy a přechody mezi nimi. U každého přechodu je v hranatých závorkách zaznačeno jaká událost se musí stát, aby systém přešel z jednoho stavu do druhého. Podrobný popis jednotlivých stavů je v odstavcích pod obrázkem.

Stav Klid

Modul v klidovém stavu poslouchá informace přicházející od čidla a podrobně je analyzuje. Momentálně neprovádí žádnou bezdrátovou komunikaci, takže tím šetří i externí napájení. Přechod do stavu riziko může nastat, když senzor modulu začne poskytovat data, která značí nebezpečí pro majitele sklepa, ať už je to vniknutí či oxid uhličitý ve sklepě. Systém nepřechází do rizikového stavu při první naměřené rizikové hodnotě, ale nejprve si počká na dostatečné množství dat nasvědčující této skutečnosti.

Stav Riziko

Po přechodu do rizikového stavu se inicializuje bezdrátová komunikace s řídící jednotkou a pošle ji informaci o tom, že modul zaznamenal větší množství

rizikových hodnot. Pokud navíc se jedná o modul s detekcí kvality ovzduší, je k němu připojen také bzučák. Pomocí něj v pravidelných intervalech provádí jasné a hlasité upozornění majitele nehledě na stav, v kterém se nachází řídící jednotka. Zprávu řídící jednotce posílá také v pravidelných intervalech dokud se data ze senzoru nestabilizují. Jakmile se tak stane a data jsou na normálních hodnotách, modul přesune do stavu klid a nadále jen monitoruje stav senzoru.

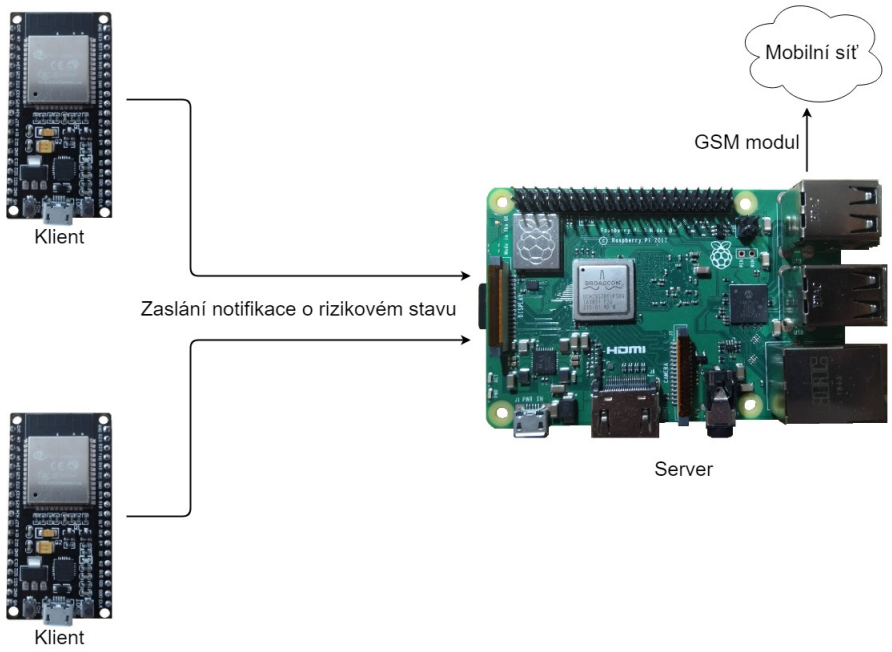
4.3 Síť a posílání zpráv

Celý systém pracuje pomocí bezdrátové komunikace, která je stavebním kamenem pro dnešní systémy. Proto bychom se měli zajímat o bezpečnost této komunikace a jak probíhá. Odpovědi na možnosti jak zabezpečit můj systém rozeberu v této podkapitole. Popíšu jak systém vypadá, síť systému, jaká komunikace v síti probíhá a její strukturu.

4.3.1 Síť

Zařízení, která se v síti vyskytují, jsem již uvedl výše během návrhu. Důležitý je zde princip komunikace a jak bude probíhat. Půjde o základní princip komunikace klient-server, kde řídící jednotka (RPI) bude zastupovat roli serveru a komunikační moduly (ESP) u senzorů roli klienta. V mém projektu jde čistě o jednosměrnou komunikaci, ale mohla by být zde možnost udělat vylepšení tak, že by řídící jednotka mohla upravovat chování či přikázat něco komunikačním modulům. Při tomto návrhu jsem čerpal z předmětu BI-PSI, kde jsme pracovali na podobném scénáři komunikace mezi klientem a serverem. Řídící jednotka je ještě skrze GSM modul připojena k mobilní síti operátora, odkud může poslat notifikaci přímo majiteli sklepa.

Důležité je zmínit, jak je komunikace zprostředkována, a to pomocí řídící jednotky, která pracuje na bázi access pointu. To znamená, že v oblasti sklepa je vytvořena síť, do které se může připojit zařízení ESP a následně zahájit komunikaci. V řídící jednotce je udělán script, který poslouchá a čeká na příchozí komunikaci do tohoto zařízení. Veškerá komunikace probíhá pomocí socketů.



Obrázek 4.5: Diagram sítě ukazující základní návrh komunikace. Vlevo jsou klienti, kteří zpracovávají data ze svých senzorů a vyhodnocují je. V případě vyhodnocení rizikového stavu zahájí komunikaci s řídící jednotkou a zašlou notifikaci o tomto stavu. Řídící jednotka následně vyhodnotí tuto zprávu a zachová se podle toho (viz 4.3). Ještě je zde vyobrazeno připojení do mobilní sítě, které zajišťuje GSM modul.

4.3.2 Komunikační standard a zaznamenávání zpráv

Pro jednoznačný a srozumitelný přenos dat v síti si musím určit jasný formát zpráv, které se budou mezi prvky sítě posílat. Jelikož je forma komunikace pouze jednosměrná, takže komunikační modul posílá data řídící jednotce a ne jinak, řešení tohoto standardu bude vcelku přímočaré.

Mým návrhem je, aby v obsahu zprávy byla MAC adresa komunikačního modulu jako identifikátor, další bude tří znaková sekvence označující zda upozornění je od pohybového čidla nebo od čidla detekující kvalitu ovzduší. Poslední částí zprávy je stav, který chce komunikační modul oznámit. Délka poslední části zprávy se liší.

Část zprávy - MAC adresa

První částí zprávy je samotná MAC adresa komunikačního modulu, který odesílá zprávu. Jedná se o základní identifikátor odesílatele, aby řídící jednotka věděla přímo ze zprávy, o které zařízení se jedná. Tento údaj neslouží jako ověření identity odesílatele, ale slouží pro jednodušší zaznamenávání zpráv.

Část zprávy - Typ čidla

Typ čidla je krátká tří znaková sekvence označující, kterého čidla se zpráva týká. V této práci jsou rozeznávány dva typy čidel, a to pohybové čidlo a čidlo měřící kvalitu ovzduší. V této sekvenci bude uvedena zkratka **PIR** nebo **GAS**. Zkratka **PIR** značí pohybové čidlo a **GAS** značí kvalitu ovzduší. Díky tomuto údaji se ke komunikačnímu modulu může zapojit vícero senzorů. Ve speciálních případech může být v této části zprávy i zkratka **ESP**, která označuje zprávy od komunikačního modulu.

Část zprávy - Oznámení

Poslední část zprávy je zde za účelem rozlišení typů zpráv. Řídící jednotka zaznamenává každou přijatou zprávu, ale každá zpráva může mít jiný význam. Nejdůležitějším typem zprávy je hlášení rizikového stavu (vniknutí nebo vyšší obsah oxidu uhličitého). Tuto skutečnost v oznámení řídící jednotka rozeznává jako textovou sekvenci **"alert"**.

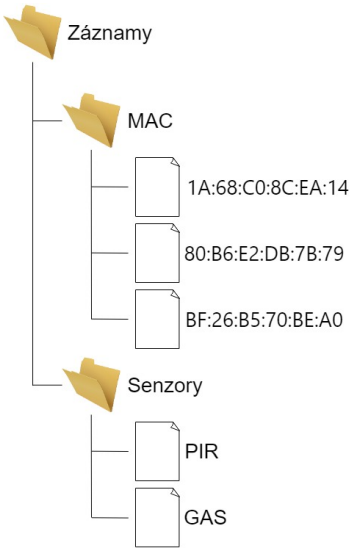
Z bezpečnostních důvodů se komunikační modul také musí umět nahlásit. Proto musí řídící jednotka rozeznávat zprávu přímo od ESP s oznámením **"alive"**. Mimo tato oznámení může řídící jednotka přijímat například pravidelné hlášení, každou hodinu či dvě, o stavu kvality ovzduší. Další možností je, že pohybové čidlo bude hlásit, že přestalo zaznamenávat pohyb ve své pozorované oblasti.

Obrázek 4.6: Znázornění struktury komunikačního standardu. Každá zpráva se skládá z MAC adresy odesílajícího, typu čidla, kterého se zpráva týká, a oznámení řídící jednotce.

Díky takové struktuře zpráv systém umožňuje komunikačním modulům mít na sobě připojeno vícero čidel. Určité čidlo může být také na více než jednom komunikačním modulu. Takto navržený systém se může jednoduše rozšířit o další komunikační moduly nebo typy čidel a dovoluje komunikačním modulům být více multifunkční.

4.3.2.1 Zaznamenávání zpráv

Jako jeden z bodů zadání práce je zaznamenávat zprávy o detekovaných událostech ve sklepě. V této podkapitole výše jsem si rozvrhl základní strukturu zpráv, které se v síti posílají, takže musí být i způsob jak tyto zprávy přehledně organizovat do záznamů.



Obrázek 4.7: Ukázka adresářové struktury pro zaznamenávání zpráv.

Vlevo lze vidět základní ukázku jak se data budou organizovat. Na jednoduchém příkladu uvedu jak proces probíhá.
Mějme **1A:68:C0:8C:EA:14PIRalert** jako ukázku zprávy. Systém si nejprve přečte MAC adresu ve zprávě a následně celou zprávu uloží do příslušného souboru se stejným názvem ve složce MAC. Poté si přečte tři znaky, které označují typ čidla, a stejně jako u MAC adresy provede uložení celé zprávy do souboru **PIR** ve složce senzory. Jelikož jsou záznamy pouze textové, ukládání tudíž probíhá duplicitně za účelem přehlednosti všech záznamů. Takže pokud by si majitel chtěl zjistit jaké hodnoty byly naměřeny u všech senzorů kvality ovzduší, stačí se povídat do souboru **GAS**. Naopak pokud by chtěl zjistit, jak fungují čidla u konkrétního komunikačního modulu, může si tak projít všechny záznamy příchozí z daného modulu ve složce MAC.

Výsledkem je tedy přehledné uspořádání veškeré komunikace probíhající v síti. Potenciálním vylepšením systému by mohlo být ukládání těchto dat na nějakém externím úložišti třeba na internetu, protože momentálně jsou všechny záznamy uloženy lokálně a z hlediska bezpečnosti to není ideální řešení.

4.4 Zabezpečení systému

Podkapitola se zaměřuje na zabezpečení systému jako celku. Vysvětlím veškeré použité praktiky pro zabezpečení systému a proč jsem je použil. Známým pravidlem v bezpečnosti je, že čím více vrstev bezpečnosti a použitých způsobů jak ochránit svoji síť, tím potenciální vniknutí do sítě minimalizováno. To znamená, že se nemůžeme spoléhat čistě na kvalitní šifrování, ale je třeba použít více způsobů ochrany současně.

V předchozí podkapitole jsem popsal, že komunikace v síti bude probíhat na principu klient-server. Z toho vyplývá, že RPI musí ze sebe vytvořit

přístupový bod, aby se následně mohly zařízení do sítě k němu připojit.

Schování SSID

První věc, co použiji, bych nazval spíše ochrannou praktikou než bezpečnostní vrstvou. Jedná se totiž o vypnutí SSID[5] broadcastu. Díky tomuto se přestane RPI vysílat do prostoru svůj název sítě, takže člověk co jde třeba kolem sklepa nevidí, že se ve sklepě vůbec něco takového nachází. Toto opatření je spíše takové preventivní a používá snad ve všech smart systémech, aby se zamezilo náhodnému připojení do sítě.

Problém je, že se do sítě dá stále bez problému přihlásit, pokud znáte její SSID. Jedná se tedy spíš o bezpečnostní prvek, kterým se říká **"Security through obscurity"** - bezpečnost skrze neznalost. Na internetu je spousta nástrojů jak vyhledat skryté sítě v okolí.

Dostatečně dlouhé heslo

Bez přístupového hesla do sítě by celé zabezpečení nemělo moc smysl. Takže použití hesla je nutnost a díky tomu, že v mé síti se vyskytují pouze počítačem ovládaná zařízení, nemusíme brát ohledy na čitelnost či snadno zapamatovatelnost hesla.

number of Characters	Numbers only	Upper or lower case letters	upper or lower case letters mixed	numbers, upper and lower case letters	numbers, upper and lower case letters, symbols
3	Instantly	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	3 secs	10 secs
6	Instantly	Instantly	8 secs	3 mins	13 mins
7	Instantly	Instantly	5 mins	3 hours	17 hours
8	Instantly	13 mins	3 hours	10 days	57 days
9	4 secs	6 hours	4 days	1 year	12 years
10	40 secs	6 days	169 days	106 years	928 years
11	6 mins	169 days	16 years	6k years	71k years
12	1 hour	12 years	600 years	108k years	5m years
13	11 hours	314 years	21k years	25m years	423m years
14	4 days	8k years	778k years	1bn years	5bn years
15	46 days	212k years	28m years	97bn years	2tn years
16	1 year	512m years	1bn years	6tn years	193tn years
17	12 years	143m years	36bn years	374tn years	14qd years
18	126 years	3bn years	1tn years	23qd years	1qt years

Key:

k – Thousand (1,000 or 10^{-3})
m – Million (1,000,000 or 10^{-6})
bn – Billion (1,000,000,000 or 10^{-9})
tn – Trillion (1,000,000,000,000 or 10^{-12})
qd – Quadrillion (1,000,000,000,000,000 or 10^{-15})
qt – Quintillion (1,000,000,000,000,000,000 or 10^{-18})

Obrázek 4.8: Tabulka popisující jak dlouho by útočníkovi trvalo prolomit heslo podle použité sady znaků a délky řetězce [22].

[5]Název sítě, který se vám zobrazuje například na mobilním zařízení, když se chcete připojit k Wi-Fi.

Doma člověk jako heslo použije něco co je snadno zapamatovatelné, ideálně nějaké slovo či slovní spojení. Pokud člověk něco málo ví o bezpečnosti, tak do hesla přidá čísla, ale reálně mnohdy jenom přidají na konec jedničku nebo použijí datum či rok svého narození. O stupeň lepší je ještě použít kombinaci velkých a malých písmen, ale ani to mnohdy nebývá účinné, protože opět uživatel použije velké písmeno na začátku hesla nebo na jeho konci.

Tady tyto typy hesel jsou velmi zranitelné. Těmto typům útoků na hesla se říká slovníkové a jejich princip je, že program zkouší použít hesla za použití velké databáze používaných hesel, které například unikly některým firmám v minulosti. Dále zkouší různé varianty těchto hesel, přidává čísla na konec, mění některé písmena za čísla (například A za 4, protože znaky jsou vzhledově podobné) nebo zkouší velké či malé písmena na různých místech slova.

Tím, že můžeme mít pseudonáhodně vygenerované heslo, odbouráváme toto velké riziko slovníkových útoků, protože použité heslo bude dlouhé a je velmi nízká pravděpodobnost, že se ve vygenerovaném hesle bude vyskytovat nějaké slovo. Navíc jak je v tabulce výše vidět, tak už jen použití speciálních symbolů jako například dolar, křížek nebo vykřičník rapidně zvyšují sadu použitých znaků, takže doba prolomení už i hesla o délce devět znaků trvá přibližně 12 let.

Použití aktuálního šifrování

Když je síť skryta a zaheslována, potřebuji se ujistit, že heslo nelze snadno zjistit. V bezdrátovém přenosu se používá spousta protokolů pro zabezpečení, ale bohužel málokteré jsou bezpečné.

Jeden z nejstarších je protokol WEP (Wired Equivalent Privacy), který je velmi starý a roku 2004 Wi-Fi aliance od něj upustila. Jeho přímým nástupcem je protokol WPA (Wi-Fi Protected Access), který opravil velké díry v bezpečnosti jako například mnohem delší klíče pro šifrování, ale bohužel byly nalezeny bezpečnostní mezery. Takže ani jeden z uvedených protokolů není vhodný pro užití.

S představením WPA2, jakožto lepší verzí WPA, se zavedl jako nový standard pro použití v bezdrátové síti. Hlavní rozdíl oproti jeho předchůdci bylo zavedení používání šifrovacího protokolu AES (Advanced Encryption Protocol). Jeho použití pro domácí či malé sítě sítě je už poměrně bezpečné. Bohužel v dnešní době jsou známé slabiny.

Asi největší a nejjednodušší slabinou je pokud má přístupový bod aktivní WPS (Wi-Fi Protected Setup), kdy se útočí na přístup do konfigurace zařízení. Je však na to jednoduchá obrana, a to že se musí vypnout WPS, tudíž nebude možné konfigurovat přístupový bod na dálku. Já ani nemám v plánu poskytovat tuto možnost, protože veškerá konfigurace bude na přímo zapsaná v RPI. Tento typ útoku se týká obzvláště routerů.

Druhá slabina jsou KRACK útoky neboli útoky znovuzavedením klíče,

kde se útočí na 4-way handshake[6]. Útok spočívá v tom, abychom vynutili cíl znovu zavést svoje klíče. Dociluje se toho právě manipulací zpráv ve 4-way handshake. Tento útok je už poměrně komplexní a útočník musí být znalý bezpečnostních pojmů. Proto tyto útoky se zas tak často neprovádí na menší sítě za účelem získání přístupu, ale u větších sítí s citlivými daty.

Protokol WPA2 má sice slabiny, ale vyžadují už nějakou přípravu a cílený útok. Tudíž ho neprolomí úplný amatér, takže ho použiji ve své bakalářské práci.

Ještě za zmínku stojí, že v roce 2018 vyšel nový standard WPA3, který opět opravuje spousty chyb ve WPA2, takže je reálně nejlepší volbou z uvedených protokolů. Bohužel stále není podporován všude a spousta zařízení nejsou aktualizovány, aby mohly využívat WPA3.

MAC filtering

Asi nejdůležitější bezpečnostní prvek, který systém obsahuje. Jedná se o mechanizmus, kdy řídící jednotka bude mít seznam zařízení, které se k ní mohou připojit. Po připojení k řídící jednotce se klient zkontroluje, zda se jeho MAC adresa shoduje s některou v seznamu. Pokud se připojené zařízení v seznamu nenachází, řídící jednotka odmítne jakoukoli komunikaci s daným zařízením. Je to poměrně silný bezpečnostní prvek, protože MAC adresa je unikátní pro každé zařízení, díky kterému jednoduše mohu detekovat útočníka.

Opět jsou zde slabiny. Existují nástroje, které vám mohou zamaskovat MAC adresu za jinou a takto obejít MAC filtering, ale má to háček v tom, že je potřeba vědět jaké MAC adresy jsou povolené. Ve výchozím stavu komunikační moduly, které jsou povolené v systému, nijak nekomunikují s okolím ani je nejde nijak zachytit. Útočník by musel zachytávat vlny, které jsou zašifrované, aby zjistil vůbec nějaké informace.

Detekce rušení či nefunkčnosti komunikačního modulu

Jedná se o prevenci proti rušení bezdrátové komunikace mezi komunikačním modulem a řídící jednotkou. V celém systému probíhá bezdrátová komunikace, která je snadno rušitelná, tudíž tento typ útoku se musí ošetřit. Na internetu je nespočet útoků pomocí rušení signálu zařízení.

Proto systém musí kontrolovat jestli se navzájem jednotlivé komponenty slyší. Ve výchozím stavu řídící jednotka pouze spoléhá na to, že spojení je důvěryhodné a vždy funkční. Abych riziko rušení signálu eliminoval, komunikační modul vždy v pravidelných intervalech bude posílat zprávu řídící jednotce. Zpráva obsahuje klasicky MAC adresu, jako typ čidla je uvedeno samotné ESP a ve zprávě je uveden řetezec **"alive"**. Na základě těchto zpráv je řídící jednotka schopna rozhodnout, zda je komunikační modul stále dosažitelný a naživu.

[6] 4-way handshake je mechanizmus výměny čtyř zpráv, během kterých si klient s přístupovým bodem domluví šifrovací klíče.

Bonusem tohoto posílání zpráv je nejen zjištění potenciálního rušení ale i možného výpadku napájení komunikačního modulu.

4.5 Náklady a porovnání

Náklady na zakoupení všech součástek pro můj bezpečnostní systém jsou 2793 Kč. Jedná se o cenu součástek, které jsem nakoupil v době, kdy pracuji na své práci. Pokud by člověk nespěchal, cena se dá trochu snížit tím, že se objednají součástky ze zahraničí. Nejdražší součástkou je RPI, které je mozkem celého systému. Poté samostatná kamera, která je schopna kvalitních fotografií a videa, ale levnější variantou může být starší verze RPI kamery. Nakonec jsou tu ještě dvě desky ESP32, které by se nemusely nutně použít, protože by stačily méně výkonné ESP8266, které jsou výrazně levnější a menší.

Pro porovnání jsem uvedl cenu systému kolegy Miroslava Váni, protože pracoval na kompletním systému od základu stejně jako já. Kolega si zvolil platformu Arduino jako řídící jednotku, která ho vyšla na téměř dvojnásobek ceny. Arduino ale skýtá mnoho výhod oproti RPI, takže jeho volby také chápu. Nicméně z svých zkušeností jsem spokojenější s RPI, protože funguje na principu mini počítače. Moduly ESP32 se chovají hodně podobně jako Arduino, ale jsou složitější na použití.

Ostatní menší součástky, jak je možno vidět, jsou poměrně podobné s menšími rozdíly. GSM modul nebyl započítán do nákladů, protože mi byl zapůjčen od školy a taky následně vrácen.

Položka	Cena v Kč	**Položka**	Cena v Kč
Raspberry Pi 3B+	959,-	Arduino Yún	1774,-
Raspberry Pi kamera v2	858,-	Magnetické spínače (2x)	142,-
ESP32S (2x)	596,-	PIR (2x)	118,-
Senzor kvality ovzduší	95,-	Senzor kouře (2x)	198,-
Pohybové čidlo PIR	60,-	Nepájivé pole	50,-
Externí napájení	35,-	Propojovací kabely	160,-
Bzučák	10,-	Ethernet a USB kabel	80,-
Arduino stabilizátor napětí	80,-	Ostatní	40,-
Ostatní	100,-		
Celkem	**2793,-**		**2562,-**

Tabulka 4.1: Porovnání cen bezpečnostních systémů. Vlevo je můj bezdrátový systém a vpravo je systém kolegy Miroslava Váni. Na spodním řádku se nachází celková cena za systém.

Kapitola 5

Implementace a realizace

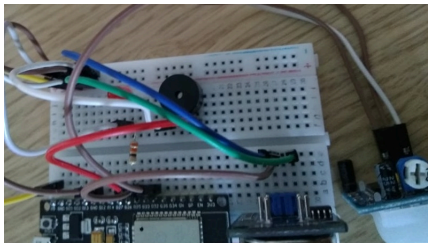
Tato kapitola se zaměřuje na realizaci návrhu systému. Je zde popsáno, jak jsem celý systém zapojil a realizoval funkční prvky systému. Podstatnou částí realizace je nastavení řídící jednotky, kde je popsáno, jak jsem zabezpečil přistupování do sítě. V neposlední řadě představím a rozeberu kód použitý pro realizaci systému. Na konci kapitoly je fotodokumentace nasazení bezpečnostního systému do sklepa.

5.1 Schéma zapojení systému

V podkapitole je ukázáno jak jsou zapojeny dvě hlavní části systému, RPI a ESP, a popisuje jaké další zařízení jsou použity.

5.1.1 Zapojení modulu ESP

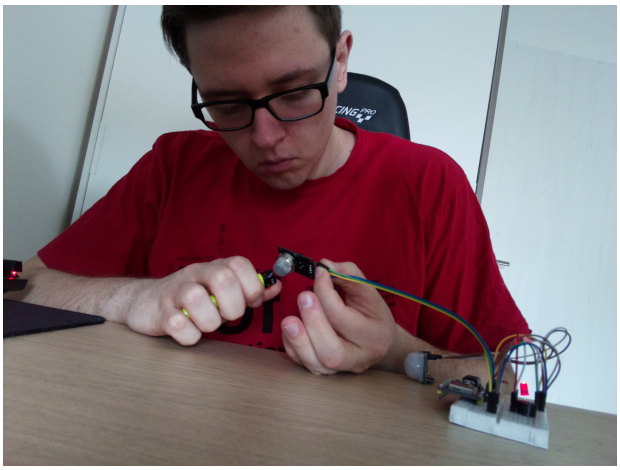
Zapojení ESP modulu je komplexnější než zapojení hlavní řídící jednotky RPI.



Obrázek 5.1: Ukázka pracovního zapojení ESP modulu. Na fotce je možné vidět v pravém dolním rohu pohybové čidlo, vlevo od něj je na nepájivém poli připojený detektor kvality ovzduší a ještě nalevo od něj se nachází samotný ESP modul.

Připojené součástky k ESP modulu pro testování a zkoušení funkčnosti systému jsou:

- ESP32
- MQ-135 (v testovací verzi je použit senzor MQ-2, kvůli nedostupnosti vhodného senzoru)
- HC-SR501
- bzučák Piezo
- červená LED dioda
- nepájivé pole
- propojovací kabely a rezistor



Obrázek 5.2: Sám autor práce při testování senzoru MQ-2 a reakce systému na detekci vyšší koncentrace nebezpečných látek v ovzduší. Na nepájivém poli je možné vidět i svítící LED diodu, která poukazuje na detekci pohybu čidlem v sledované oblasti. Fotografie byla pořízena pomocí RPI kamery.

Hlavním rozdílem oproti návrhu je použití nepájivého pole. V návrhu je určeno, že vše je uloženo přesně v krabičce a kabely jsou přímo propojeny se senzorem. Také zde není externí napájení, které mám k dispozici se všemi součástkami, ale v době kdy jsem realizoval bezpečnostní systém, tak jsem neměl přístup do laboratoře, tudíž napájení je řešeno přes USB rozhraní.

Návrh se zmiňuje také o signalizaci nebezpečí v případě detekce nekvalitního ovzduší. To je vyřešeno pomocí bzučáku Piezo, který při detekci špatného ovzduší začne bzučet v pravidelných intervalech. Menším rozšířením je indikátor detekce pohybu pomocí červené LED diody.

Jelikož mám k dispozici pouze jeden modul ESP, rozhodl jsem se celou realizaci provést tak, že oba typy komunikačních modulů (detektor pohybu a

kvality ovzduší) jsem spojil do jednoho. To je důvod, proč na fotografii výše je najednou zapojeno jak pohybové čidlo tak i detektor kvality ovzduší.

Pohybové čidlo má 3 piny, a to na 5V přívod energie, zem a 3,3V digitální výstup. Země i přívod energie jsou připojeny z ESP do vrchního řádku pro rozvedení napájení do vícero zařízení. Díky tomu, že používám na napájení USB rozhraní, tak ESP má 5V pin, přes který za normálních okolností modul napájíme, ale nyní slouží jako 5V vývod pro napájení. Prostřední digitální výstup vede k GPIO pinům ESP modulu.

Senzory MQ-2 i MQ-135 mají totožná rozhraní pinů. Senzor má 4 piny, a to opět 5V napájení, zem, digitální výstup a ještě k tomu je zde výstup analogový. Zapojení je opět totožné jak u pohybového čidla, takže napájení a zem jsou připojeny do vrchních dvou řádků. Výsledná realizace využívá pouze 3,3V digitálního výstupu a je připojen k GPIO pinu na ESP. Nevyužitým zůstává analogový výstup, který vysílá napětí od 0V do 5V, díky kterému jsme schopni sledovat hladinu kvality ovzduší. Bohužel GPIO piny ESP modulu zvládají napětí maximálně do 3,3V, tudíž by zde bylo potřeba tranzistoru, děliče napětí či jiného převodníku, abychom mohli data spolehlivě číst na ESP.

5.1.2 Zapojení modulu RPI

Jelikož řídící jednotka má poměrně širší paletu rozhraní oproti komunikačnímu modulu a je celkově univerzálnějším prvkem, zapojování je zde o dost jednodušší. Na druhou stranu vykonává důležitější funkci při pohledu na systém jako celek. Řídící jednotka je zodpovědná za to nejdůležitější, a to monitorování sklepa a notifikaci majitele.

Obrázek 5.3: Ukázka pracovního zapojení RPI. Přes CSI rozhraní je propojená RPI kamera. Kódový zámek je připojen skrze USB rozhraní. V pracovní verzi je pro funkci kódového zámku použita klávesnice.

Součástky použité s RPI pro testování a zkoušení funkčnosti systému jsou:

- RPI3B+
- RPI kamera
- klávesnice

Zde oproti návrhu tolik rozdílů není. Bohužel nemám k dispozici GSM modul, takže jsem notifikování majitele alternativně zprostředkoval pomocí bluetooth, které je integrované přímo na desce. Jedná se čistě o náhradu kvůli nepříznivým podmínkám a ve výsledném systému by měl být GSM modul. Následně by se také musela provést úprava kódu, aby byl systém schopný GSM modul použít.

Ze zapojeného příslušenství je zde pouze klávesnice a abych simuloval klasický kódový zámek, omezil jsem používání pouze na její numerickou část. Kdybych začal používat celou klávesnici, nastala by zde řada potíží s ošetřením vstupů, protože při odemykání či zamykání by člověk mohl použít zkratky pro ukončení procesu (CTRL + Z) a tím rozbít celý systém. Ve výsledném modelu by měla být pouze numerická klávesnice připojená přes USB rozhraní.

Dále už je pouze RPI kamera, která je připojena přes CSI rozhraní. Tento prvek se zcela shoduje s návrhem systému a její zapojení je možné pouze do jediného specifického portu na desce.

5.2 Nastavení RPI

Operační systém, který na RPI běží, je odnoží operačního systému Debian, tudíž je distribucí Linuxu. Díky této znalosti je nastavení velmi jednoduché. Mým cílem je, aby se řídící jednotka chovala jako bezdrátový přístupový bod, díky kterému se budou moct k RPI připojit komunikační moduly.

Pro nastavení jsem využil stránky s návodem [23], kde podrobně popisují krok po kroku jak nastavit RPI, aby sloužilo mému účelu jako bezdrátový přístupový bod. K zajištění funkčnosti jsou potřeba dva programy, a to **hostapd** a **dnsmasq**.

5.2.1 Konfigurace dnsmasq

Nejdříve je potřeba určit na zařízení v */etc/dhcpcd.conf* statickou adresu pro bezdrátové rozhraní na RPI. Aby byla zajištěna komunikace v síti a mohla probíhat komunikace, tak je zapotřebí, aby RPI rozdávalo IP adresy komunikačním modulům a celkově se chovalo jako DHCP server. K tomu právě slouží program **dnsmasq**, který lze změnit v konfiguračním souboru */etc/dnsmasq.conf*.

Ukázka základního nastavení DHCP serveru pro rozhraní *wlan0*:

```
interface=wlan0
  dhcp-range=192.168.0.11,192.168.0.30,255.255.255.0,24h
```

5.2.2 Konfigurace hostapd

Dalším krokem je samotné nastavení přístupového bodu. Využiji k tomu program **hostapd**, který nakonfiguruji v souboru */etc/hostapd/hostapd.conf*. Po nastavení tohoto souboru je téměř hotovo a RPI po restartu programů bude fungovat jako přístupový bod.

Rozhraním pro bezdrátovou komunikaci je *wlan0*. Dále je zde vidět použité SSID pro síť, ale síť je skryta díky řádku *ignore_broadcast_ssid=1*. Díky tomu zajistíme, že se nerozesílá SSID do prostoru, takže není viditelné běžným uživatelům.

Důležitou součástí je zde heslo pro přihlášení do sítě. Jak bylo v kapitole 4.4 návrhu zmíněno, tak do sítě se přihlašují pouze komunikační moduly, takže heslo jsem zde nechal pro ukázku. Je dlouhé, obsahuje malá a velká písmena a speciální znaky. Heslo je generováno pomocí */dev/random*, což je generátor implementovaný přímo v jádře systému, z kterého sbírá potřebnou entropii. Při nastavování bezpečnostního algoritmu je možné si povšimnout co všechno je zde použito.

Ukázka nastavení hostapd:

```
interface=wlan0
driver=nl80211
ssid=RPIsecuritysystem
hw_mode=g
channel=6
auth_algs=2
wpa=2
wpa_passphrase=TvHJiu%Oh}|qz
wpa_key_mgmt=WPA-PSK
wpa_pairwise=TKIP
rsn_pairwise=CCMP
ignore_broadcast_ssid=1
macaddr_acl=1
accept_mac_file=/etc/hostapd/accept
```

Závěrečným krokem pro nastavení **hostapd** je ukázat souboru cestu ke konfiguračnímu souboru, který jsem před chvílí nastavil. V souboru */etc/default/hostapd* musím změnit řádek *DAEMON_CONF=* a nastavit mu cestu k souboru s koncovkou *.conf* výše popisovanému.

5.2.3 Aktivace MAC filteringu

Poslední důležitou částí je nastavení **MAC filteringu**. Toho je docíleno posledními dvěma řádky, kde povolím filtrování provádět a specifikuji soubor, v kterém jsou povolené MAC adresy pro vstup do sítě. Soubor */etc/hostapd/accept* je pouze textový soubor, kde je na každém řádku specifikovaná MAC adresa povoleného zařízení.

Manuál poté už dál popisuje přesměrovávání datového toku tak, aby připojená zařízení v síti měla k dispozici internet. Já tyto kroky dál neprovádím, protože komunikační moduly nemusí mít přístup k internetu. Samotné RPI nemá připojení k internetu samo o sobě, ale dalo by se ho docílit pomocí GSM modulu, který by měl tuto službu dostupnou.

5.2.4 Automatické spouštění

Pro automatické spouštění musím RPI nastavit tak, aby stačilo pouze připojit zařízení do zásuvky a systém poběží. Vyzkoušel jsem dvě možná řešení, ale jen jedno se ukázalo jako použitelné.

První, které mě napadlo, bylo spustit skript jako službu a takto nechat skript spuštěný na pozadí. Tato varianta spustila skript při startu počítače a byl i funkční, ale problém nastal se vstupem z klávesnice. Skript by šel přepsat, aby se dal používat i jako služba tak, že by nepracoval s klasickým vstupem či výstupem, ale musel by zachytávat jednotlivá klepnutí do klávesnice jako systémové události. Proto jsem tuto variantu nezvolil.

Použitá varianta, pro kterou jsem se rozhodl, je trochu oklika. Nicméně je funkční a jednoduše nastavitelná. Přepnul jsem úvodní načítání operačního systému tak, aby jako výchozí rozhraní bylo použito TUI a automaticky se přihlásilo na uživatele *"pi"*. Po přihlášení uživatele se automaticky spouští soubor *.bashrc*. Tudíž stačí do souboru přidat jednu řádku navíc, která spustí můj skript, a docílím požadované funkcionality.

5.3 Ukázka zdrojového kódu řídící jednotky

Implementace řídící jednotky je skript napsaný v jazyce Python. Jedná se o prototypovou implementaci, na které se může dále stavět a dále ji rozšiřovat. Využívám vícevláknového běhu skriptu k zpracovávání více komunikačních modulů najednou, paralelního zpracovávání vstupu a běhu celé stavové logiky systému.

Skript na začátku svého běhu inicializuje všechny potřebné proměnné, spustí vlákna pro stavy a vstup. Poté vyčká na propojení majitele skrze bluetooth a jako další krok inicializuje veškerou komunikaci přes TCP sockety, na kterých poslouchá data od komunikačních modulů.

Na obrázku 4.3 jsem popsal návrh stavové logiky řídící jednotky. Ve zkráceném pseudokódu zde ukážu implementaci stavové logiky ve skriptu.

```
def stavy(): stavova logika celeho systemu
  camera = PiCamera(...) nastaveni kamery
  while True:

    if(system odemcen):

      if(system se zrovna odemkl):
        print("zastavit nataceni")
        camera.stop_recording()
        Path(...).unlink() smazani souboru
      zresetovani vsech vlajek

    elif(system zamcen):

      if(spatne ovzdusi and not poslana notifikace):
        client_sock.send("ovzdusi!")
        notifikace o vzduchu poslana

      if(notifikuj):
        client_sock.send("vniknuti!")
        ukonceni stavoveho cyklu

      elif(dalsi detekce pohybu):
        if(system zamcen and uplynulo 30 sekund od
           prvniho pohybu):
          notifikuj majitele

      elif(prvni detekce pohybu):
        zaznamenani casu vniku
        print("zacalo nataceni")
        camera.start_recording(...)
        vyzadovat pristupove heslo
```

Celá stavová logika se opírá o nastavování vlajek, podle kterých přechází do různých částí kódu. První věc, kterou systém kontroluje, je, zda systém se nachází ve stavu odemknuto či zamčeno.

Pokud se systém nachází ve stavu odemčeno, nastávají dvě možnosti. Buď se systém zrovna odemkl, tudíž systém začal natáčet potenciální vniknutí. V takovém případě systém smaže videozáznam. Další věc, kterou systém provádí ve stavu odemčeno je resetování všech vlajek do výchozího stavu.

Jakmile se systém zamkne, je zde celá řada možností co se může stát.

Jedna z možností je, že pokud řídící jednotka dostane výstražnou zprávu od senzoru kvality ovzduší, tak musí o této skutečnosti notifikovat majitele. Notifikace probíhá pouze jednou.

Řídící jednotka může také obdržet zprávu o detekci pohybu, takže se zaznamená kdy k vniknutí došlo a systém spustí kameru. Taky si nastaví vlajku, že vyžaduje přístupové heslo, takže vlákno, kde běží čtení ze vstupu, započne rozpoznávat zda se jedná o heslo.

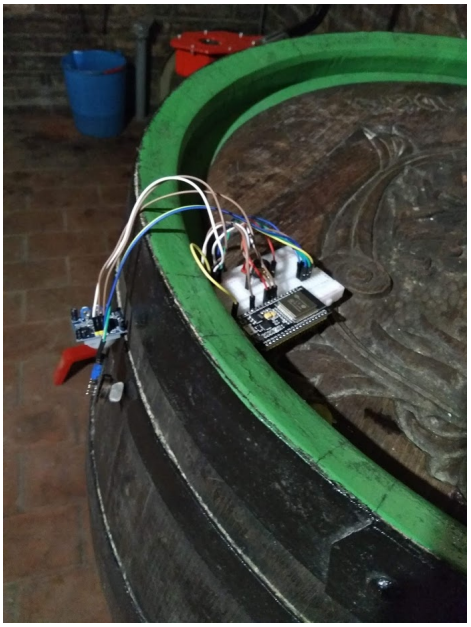
Když systém tedy zachytil pohyb, začne 30 sekundový interval, kdy má majitel šanci napsat heslo. Je zde nastavené pravidlo tří špatných pokusů, takže pokud se třikrát špatně zadá heslo, systém si nastaví vlajku, aby upozornil majitele o nedovoleném vniknutí a stavová logika se celá zastaví na tomto bodě.

Řídící jednotka se následně musí manuálně zresetovat, aby systém správně fungoval.

5.4 Implementace ESP modulu

Při návrhu logiky komunikačního systému na obrázku 4.4 je možno vidět, že logika je hodně jednoduchá. Z tohoto důvodu ani nemá smysl uvádět pseudokód zdrojového kódu. Vše je psané v Arduino IDE, kde s pomocí externí knihovny pro ESP se dokáže snadno přeložit a nahrát do modulu.

Arduino má klasickou konstrukci **setup** a **loop**. Rozhodování kdy ESP pošle data řídící jednotce provádí na základě vlajek, které se mění vždy když nastane přerušení, které je nastavené v setupu. Následně se připojí k řídící jednotce, pošle data a následně změní vlajku, aby se mohlo ESP vrátit do pozorovacího režimu.



Obrázek 5.4: Hledání vhodného umístění pro komunikační modul pro otestování čidel (foto č. 1).

Obrázek 5.5: Hledání vhodného umístění pro komunikační modul pro otestování čidel (foto č. 2).

Kapitola 6

Testování

Kapitola uvádí celý proces testování a ladění systému do konečné podoby. Během realizace se naskytla celá řada komplikací, které jsou zde popsány. Hlavní podstatou mého testování je ověřit, zda komunikace mezi zařízeními proběhla správě a že se útočník nemůže jen tak nabourat do systému. Bylo provedeno také testování jednotlivých čidel a jak se zaznamenávají události v systému. Testování bylo prováděno v mém bytě a poté i ve vinném sklepě.

Jednotlivé součásti systému nebyly testovány na spolehlivost. Realizovaný systém nemá redundantní čidla, aby ověřoval jejich spolehlivost výstupů. Cílem práce je realizovat bezdrátovou komunikaci mezi čidly a zabezpečit vytvořenou síť.

6.1 Prvotní testování součástek

Při sestavování jednotlivých součástí systému jsem narážel na mnoho překážek. Asi největší překážkou bylo čidlo pohybu.

První čidlo na odzkoušení mi zapůjčil můj vedoucí práce, ale z neznámých důvodů nefungovalo. Následně jsem si objednal další nefunkční čidlo, takže jsem objednal třetí, které naštěstí konečně fungovalo. Nepovedlo se mi specifikovat příčinu nefunkčnosti čidel. Pro bližší prozkoumání by mi pomohl přístup od HW laboratoře na fakultě, která byla z důvodu COVID-19 zavřená.

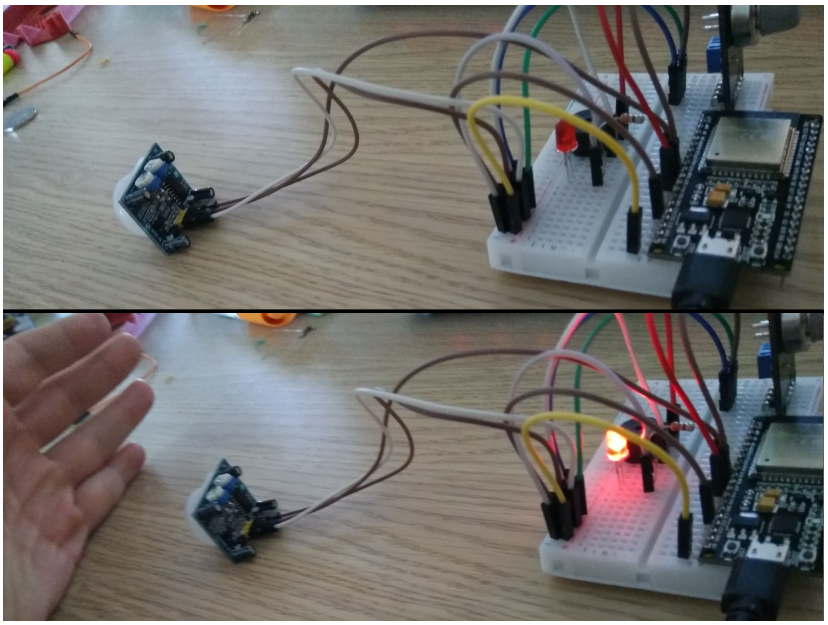
Detektor kvality ovzduší se ke vší smůle nedostal ani do prototypu. Důvodem je, že v době realizace nebyly téměř nikde ke koupi. Povedlo se mi sehnat jedno čidlo MQ-135, ale bylo ve značně opotřebeném stavu. Promáčklý krycí klobouček nesvědčil nic dobrého a během prvního zapojení senzor začal smrdět specifickým zápachem, který ale nebyl jako spálené obvody. Jakoby čidlo, které je pod krycím obloučkem, mělo nevhodné podmínky pro fungování. K této hypotéze mě dovádí to, že na čidle neustále svítila dioda, která indikuje nevhodné ovzduší.

Takže nakonec pro otestování funkčnosti systému využiji čidlo MQ-2, které mám zapůjčené od mého vedoucího bakalářské práce.

Samotné ESP a RPI jsou funkční. Jediná překážka byla seznámení se s ESP modulem, protože jeho chování a vlastnosti jsou trochu odlišné od používání Arduina, v kterém jsem psal program pro tuto desku. S RPI nebyl žádný problém, ani s připojením kamery, která krásně funguje. Propojení mezi jednotlivými zařízeními bylo taky celkem bezproblémové a funkční jak bylo uvedeno v návrhu podkapitole 4.3.

6.2 Vniknutí do objektu

Ochrana proti vniknutí je ošetřena pohybovým čidlem HC-SR501. Během testování čidla jsem došel k velmi pozitivním výsledkům. Čidlo mě dokázalo zachytit i na vzdálenost větší než 5 metrů bez problému jakmile jsem do snímaného prostoru vešel.



Obrázek 6.1: Ukázka základního principu práce čidla. Nahoře je možno vidět jak čidlo snímá nehybné prostředí před sebou. Když však před něj vložím ruku, čidlo detekuje pohyb. Pro názornost používám LED diodu, která se rozsvítí při detekci pohybu.

Při testování jsem zkoušel různé typy pohybu a jak na ně reaguje čidlo. Zkoušel jsem házet před čidlem menší objekty jako například bačkory či kusy papíru. Z 10 pokusů sepnout čidlo pomocí bačkory se mi nepovedlo ani jednou

a s využitím papíru jsem byl také neúspěšný. Pozorováním je, že na menší objekty čidlo nereaguje.

Testy jsem prováděl i sám na tobě, a to třemi způsoby. Zkoušel jsem vkročit do místnosti hodně pomalu, klasickým krokem a rychle. Bylo provedeno deset měření. Při pomalém vstupu do místnosti jsem se nejdál dostal přibližně 30 centimetrů od dveří než jsem byl čidlem detekován. Při klasické chůzi jsem byl detekován sotva co jsem strčil nohu do místnosti. Vzhledem k výše uvedenému pozorování, kdy jsem vhazoval do místnosti objekty, jsem se rozhodl vyzkoušet hodně rychlé pohyby. Naštěstí moje myšlenka nebyla tak důmyslná a čidlo mě opět detekovalo hned mezi dveřmi.

Moment vniknutí byl vždy notifikován majiteli ve všech možných případech. Zkoušel jsem nezadání hesla a tři špatná zadání hesla. V obou případech majitel vždy obdržel notifikaci a systém dělal videozáznam.

Test	Vhození předmětu	Pomalý příchod	Klasický příchod	Rychlý příchod
1	X	OK (4cm)	OK	OK
2	X	OK (7cm)	OK	OK
3	X	OK (12cm)	OK	OK
4	X	OK (10cm)	OK	OK
5	X	OK (8cm)	OK	OK
6	X	**OK (28cm)**	OK	OK
7	X	OK (15cm)	OK	OK
8	X	OK (6cm)	OK	OK
9	X	OK (17cm)	OK	OK
10	X	OK (16cm)	OK	OK
Úspěšnost		100%	100%	100%

Tabulka 6.1: Tabulka naměřených výsledků při testování pohybového čidla a komunikace v systému. Uvedeny jsou 4 druhy testů. Písmenem "X"jsou označeny testy, kde neproběhla komunikace mezi komunikačním modulem a řídící jednotkou. Naopak písmeny "OK"jsou označeny testy, kde komunikace proběhla. U testu Pomalý příchod jsem navíc měřil vzdálenost, kam jsem se dokázal dostat, než mě čidlo detekovalo. V posledním řádku jsou poté uvedeny úspěšnosti testů.

6.3 Upozornění na nekvalitní ovzduší

Testování kvality ovzduší jsem prováděl jen demonstračně a spíš jsem tím testoval schopnost přijímat různé druhy zpráv a také jejich zpracovávání. Senzor MQ-2 byl funkční ve všech případech. Simulaci jsem prováděl pomocí plynu ze zapalovače a stačilo ho velmi malé množství, aby bzučák začal vydávat výstražný signál. V případě, že majitel není ve sklepě obdržel notifikaci do mobilu ve všech případech.

Test	Detekce
1	Ano
2	Ano
3	Ano
4	Ano
5	Ano
6	Ano
7	Ano
8	Ano
9	Ano
10	Ano

Tabulka 6.2: Výpis průběhu testů čidla MQ-2. V systému proběhla komunikace při každé detekci nebezpečných hodnot.

6.4 Kvalita spojení a jeho spolehlivost

Testování rozsahu sítě odpovídá kvalitě antény, kterou RPI používá. Testoval jsem kvalitu spojení integrované antény a z hlediska rychlosti připojení je velmi kvalitní. Rychlost dosahovala několika jednotek MB za sekundu, takže na menší přenos dat po síti je vhodná. Zkoušel jsem různá umístění v mém bytě a následně se připojit k RPI z různých míst, která byla také různě vzdálená. Po bytě i přes dvě stěny, pokud nejsou z betonu, tak signál stále dosáhl. Asi největším překvapením bylo, když jsem vyšel před dům a stále jsem viděl signál od RPI.

Měření	Vzdálenost	Síla signálu
Moduly vedle sebe	0-1 m	-28 dBm
Ve stejném pokoji	3 m	-51 dBm
Sousední pokoj přes zeď	5 m	-60 dBm
Obývací místnost přes zeď	6 m	-62 dBm
Koupelna přes 2 zdi	6 m	-65 dBm

Tabulka 6.3: Testování kvality připojení v mém bytě. Sloupec Měření uvádí v jakých podmínkách byl test prováděn. V dalších sloupcích je uvedena přibližná vzdálenost mezi měřenými zařízeními a síla signálu uvedená v dBm.

6.5 Pokus o útok

Zkoušel jsem testovat bezpečnost za pomoci dvou subjektů. Já sám jsem byl jedním z figurantů pokoušejících se dostat do sítě a druhým byl můj spolubydlící, za což mu děkuji. Hráli jsme dva typy možných útočníků na RPI,

pokoušející se dostat do systému. Jeden byl zkušenější útočník (já) a druhý byl náhodný kolemjdoucí, který se zkouší připojit k síti.

První vrstva, kterou jsem zkusil je MAC filtering. Už i toto opatření bylo dostatečnou ochranou proti mému spolubydlícímu, kterému jsem nechal síť nezaheslovanou a vysílající svoje SSID do prostoru. Já, útočící od stolního počítače, jsem dokázal podvrhnout svou MAC adresu a připojit se do sítě. Ačkoli je to poměrně snadno prolomitelná vrstva obrany, tak se jeví jako spolehlivá ochrana proti nezkušeným útočníkům.

Další vrstvou je schování SSID broadcastu. Tentokrát je toto jako jediná forma obrany a MAC filtering je vypnutý stejně tak i heslo. S trochou pomoci a vyhledávání na internetu se byl schopen připojit můj spolubydlící do sítě. Proto bych tuto vrstvu bral čistě jako prevenci před kolemjdoucími, kteří díky tomuto opatření o síti ani nebudou vědět.

Když jsem síť zahesloval dostatečně silným vygenerovaným heslem, spolubydlící byl bezradný a já jsem také bohužel neuspěl. Spousta útoků se totiž využívá sniffingu či MITM[7] útoku. Slovníkové útoky neberu v úvahu, protože heslo je dostatečně náhodné, aby na tento typ útoku podlehlo. Problémem předchozích dvou útoků je, že obvykle spoléhají na to, že odposlouchávají či zmanipulují nově připojující se zařízení. Bohužel pro útočníka tato situace nastává pouze při restartu systému či jeho instalaci.

Poslední typ útoku, který beru v úvahu, je DOS. Ačkoli tyto útoky nezískávají žádná data pro útočníka, tak tyto útoky jsou mnohdy velmi užitečné. Právě v mém případě se může jednat o reálnou hrozbu, kdy by útočník mohl shodit celou síť a volně si nakráčet do vinného sklepa.

[7]Man In The Middle - "člověk uprostřed"- je typ útoku, který je založen na odposlouchávání oběti tak, že je aktivním prostředníkem mezi účastníky.

Závěr

Úvodní problematika je mi velmi blízká a o to více jsem byl poháněn zjistit více informací. Díky seznámení se s pracemi od studentů, kteří pracovali na podobných tématech, jsem zjistil, co obnáší něco takového vytvořit a hodně mi to pomohlo.

Zanalyzoval jsem od svého okolí jednotlivé nápady na to, jak zabezpečit objekt vinného sklepa a přineslo to do práce mnoho možností, jak by se dal systém rozvíjet. Provedl jsem analýzu jednotlivých součástek, které by mohly být použity do bezpečnostního systému vinného sklepa, a hlavně se zaměřil na porovnání RPI desek a variant pro komunikační moduly.

Při analýze celého systému jsem si uvědomil celou škálu různých potíží, které USB rozhraní přináší do celého systému. Celá řídící jednotka je díky těmto rozhraním ohromně multifunkční a pro domácí použití výborná volba. Nicméně v oblasti zabezpečení je to problém, protože potenciální útočník má možnost se dostat k řídící jednotce a využít tato rozhraní pro nabourání se do systému. Toto by mohlo být zajímavé prozkoumání možností jak hardwarově ochránit řídící jednotku.

Navrhl jsem bezpečnostní systém, který obsahuje všechny základní prvky pro jeho funkčnost. Čidla sama o sobě nejsou úplně zajímavé objekty pro moje zkoumání, proto jsem se více zaměřil na návrh fungování řídící jednotky, komunikačního modulu a spojení mezi nimi. U RPI to nebylo zas tak složité, díky mým znalostem linuxových systémů. Vytvořil jsem jednoduchý návrh protokolu pro posílání zpráv a veškeré zaznamenávání dat do vnitřního souborového systému RPI.

Při realizaci systému jsem se setkal s celou řadou překážek. Při prvotním seznamováním a návrhu některá čidla vůbec nefungovala, což mi značně stěžovalo práci. Také úvodní seznámení s moduly ESP bylo poměrně složité. Rozložení pinů a celá logika desky není na první pohled jasná jako u Arduina. Bohužel s ESP deskami nemám takové zkušenosti, ale využil jsem konzultace s mým kamarádem Michalem Převrátilem, který má mnohem větší zkušenosti na této platformě.

Naneštěstí kvůli současné situaci, kdy píšu tuto bakalářskou práci, jsou školy uzavřeny a já bohužel nemohl využít prostor HW laboratoře na fakultě. Systém je v návrhu komplexnější, než se celkově povedlo realizovat, ale v domácích podmínkách nemám veškeré nástroje pro jeho realizaci. Výsledný systém je ale funkčním prototypem a jsem s ním spokojen.

Testování ukázalo důvěryhodnost posílaných dat a v takto uzavřené síti, tvořené RPI, spojení probíhá poměrně rychle a kvalitně.

Na tomto výsledku by se dala aplikovat celá řada rozšíření, protože dává podklad pro vývoj bezdrátových bezpečnostních systémů. Výsledek práce na tomto projektu je pro mě velmi kladným a naučil jsem se mnoho nových znalostí v oblasti IoT.

Literatura

[1] Váňa, M.: Inteligentní bezpečností systém garáže. Bakalářská práce, České vysoké učení technické v Praze, Fakulta informačních technologií, 2018.

[2] Mačak, M.: Inteligentný bezpečnostný systém – sekcia zabezpečený vstup. Bakalářská práce, České vysoké učení technické v Praze, Fakulta informačních technologií, 2019.

[3] Červenka, O.: *Inteligentný bezpečnostný systém garáže: nadřazený systém*. Diplomová práce, České vysoké učení technické v Praze, Fakulta informačních technologií, 2018.

[4] rpishop.cz: Raspberry Pi 3 Model B 64-bit 1GB RAM. [online], citováno: 30. 4. 2020. Dostupné z: `https://rpishop.cz/raspberry-pi-3b/283-raspberry-pi-3-model-b-64/bit-5060214370028.html`

[5] rpishop.cz: Raspberry Pi 3 Model B+ 64-bit 1GB RAM. [online], citováno: 30. 4. 2020. Dostupné z: `https://rpishop.cz/raspberry-pi-3b/896-raspberry-pi-3-model-b-plus-64-bit-1gb-ram-713179640259.html`

[6] rpishop.cz: Raspberry Pi 3 Model A+ 64-bit 512MB RAM. [online], citováno: 30. 4. 2020. Dostupné z: `https://rpishop.cz/raspberry-pi-3a/1114-raspberry-pi-3-model-a.html`

[7] Piltch, A.; Halfacree, G.: Raspberry Pi 4 Review: The Gold Standard for Single-Board Computing. [online], Nov 2019, citováno: 30. 4. 2020. Dostupné z: `https://www.tomshardware.com/reviews/raspberry-pi-4-b,6193.html`

[8] rpishop.cz: Raspberry Pi 4 Model B - 4GB RAM. [online], citováno: 30. 4. 2020. Dostupné z: `https://rpishop.cz/raspberry-pi-4b/1598-raspberry-pi-4-model-b-4gb-ram-765756931182.html`

[9] Widy: [IoT ESP-32S 2.4GHz Dual-Mode WiFi Bluetooth, CP2102]. [online], citováno: 30. 4. 2020. Dostupné z: https://www.laskarduino.cz/iot-esp-32s-2-4ghz-dual-mode-wifi-bluetooth-rev-1--cp2102/

[10] spol. s.r.o., C.: Internet věcí je tady! TCP/IP WIFI ESP8266: arduino-shop.cz. [online], citováno: 30. 4. 2020. Dostupné z: https://arduino-shop.cz/arduino/911-internet-veci-je-tady-tcp-ip-wifi-esp8266.html

[11] rpishop.cz: Raspberry Pi Zero WH. [online], citováno: 30. 4. 2020. Dostupné z: https://rpishop.cz/raspberry-pi-zero/685-raspberry-pi-zero-wh-4250236816296.html

[12] *HC-SR501 PIR MOTION DETECTOR*. Citováno: 30. 4. 2020. Dostupné z: https://www.gme.cz/data/attachments/dsh.775-042.1.pdf

[13] arduino shop.cz: HC - SR501 Pohybové čidlo pro jednodeskové počítače. [online], citováno: 30. 4. 2020. Dostupné z: https://arduino-shop.cz/arduino/839-arduino-pohybove-cidlo.html

[14] Elecfreaks: *Ultrasonic Ranging Module HC - SR04*. Citováno: 30. 4. 2020. Dostupné z: https://cdn.sparkfun.com/datasheets/Sensors/Proximity/HCSR04.pdf

[15] arduino shop.cz: eses ultrazvukový měřič vzdálenosti HC-04 pro jednodeskové počítače. [online], citováno: 30. 4. 2020. Dostupné z: https://arduino-shop.cz/arduino/846-arduino-meric-vzdalenosti-ultrazvukovy.html

[16] components101.com: MQ-135 Gas Sensor Pinout, Features, Alternatives, Datasheet and Uses Guide. [online], citováno: 30. 4. 2020. Dostupné z: https://components101.com/sensors/mq135-gas-sensor-for-air-quality

[17] Cholewiak, S. A.: Raspberry Pi Camera Comparison. [online], Jan 2017, citováno: 29. 5. 2020. Dostupné z: http://www.semifluid.com/2017/01/23/raspberry-pi-camera-comparison/

[18] alza.cz: HUAWEI E3372H-320. [online], citováno: 30. 4. 2020. Dostupné z: https://www.alza.cz//huawei-e3372h-320-d5790654.htm?kampan=adw1_sitove-prvky-a-nas_pla_all_sitove-prvky-a-nas-css_3g-lte-modemy_c_9062820__HU901m2&gclid=CjwKCAjwssD0BRBIEiwA-JP5rLiVW8rxtaekDVT_mVB7PPVziyNg9mAm8QykTRljG5OXe-hL8XrDmhoCNgIQAvD_BwE

[19] rpishop.cz: Waveshare GSM/GPRS/GNSS HAT pro Raspberry Pi. [online], citováno: 30. 4. 2020. Dostupné z: https://rpishop.cz/hat/1187-gsmgprsgnss-hat-pro-raspberry-pi.html

[20] arduino shop.cz: eses membránová klávesnice 4x4 pro jednodeskové počítače. [online], citováno: 30. 4. 2020. Dostupné z: https://arduino-shop.cz/arduino/824-eses-membranova-klavesnice-4x4-pro-jednodeskove-pocitace.html

[21] Raspberry Pi Camera Module. [online], citováno: 25. 5. 2020. Dostupné z: https://www.raspberrypi.org/documentation/raspbian/applications/camera.md

[22] Complex Passwords Harder to Crack, but It May Not Matter. [online], citováno: 29. 5. 2020. Dostupné z: https://www.inetsolution.com/blog/june-2012/complex-passwords-harder-to-crack,-but-it-may-not

[23] Lovely, S.: How to use your Raspberry Pi as a wireless access point. [online], Sep 2018, citováno: 8. 5. 2020. Dostupné z: https://thepi.io/how-to-use-your-raspberry-pi-as-a-wireless-access-point/

Příloha **A**

Seznam použitých zkratek

DOS Denial of Service - odepření služby

GPIO General Purpose Input Output

GSM Global System for Mobile Communications

HAT Hardware Attached on Top

IoT Internet of Things

MAC Media Access Control

MB Mega bytes

MITM Man In The Middle

RFID Radio Frequency Identification

RPI Raspberry Pi

SMS Short Message Service

SSID Service Set Identifier

TUI Text User Interface

Příloha B

Obsah přiloženého média

- `readme.txt` ..... stručný popis obsahu CD
- `impl` ..... zdrojové kódy implementace
  - `ESP.ino` ..... implementace komunikačního modulu
  - `RPI.py` ..... implementace řídící jednotky
- `thesis` ..... text práce a její zdroje
  - `thesis.tex` ..... zdrojová forma práce ve formátu LaTeX
  - `thesis.pdf` ..... text práce ve formátu PDF