



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV INTELIGENTNÍCH SYSTÉMŮ

DEPARTMENT OF INTELLIGENT SYSTEMS

**MULTISENZOROVÉ ZABEZPEČENÍ DOMÁCNOSTI S
POMOCÍ RASPBERRY PI ZERO**

MULTISENSOR FOR HOME SECURITY WITH THE HELP OF RASPBERRY PI ZERO

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE

AUTHOR

JONÁŠ SVOBODA

VEDOUCÍ PRÁCE

SUPERVISOR

doc. Ing. VLADIMÍR JANOUŠEK, Ph.D.

BRNO 2022

Zadání bakalářské práce



Student: **Svoboda Jonáš**
Program: Informační technologie
Název: **Multisenzorové zabezpečení domácnosti s pomocí Raspberry Pi Zero**
Multisensor for Home Security with the Help of Raspberry Pi Zero
Kategorie: Vestavěné systémy

Zadání:

1. Prostudujte problematiku IoT, domácí automatizace a zabezpečení. Seznamte se s existujícími otevřenými řešeními s využitím Raspberry Pi Zero.
2. Definujte požadavky na dostatečně univerzálně použitelné multisenzorové zařízení pro domácí automatizaci s důrazem na dohled a zabezpečení. Uvažujte senzor pohybu, senzor otevření dveří, kameru, detektor kouře/oxidu uhelnatého a doplňující senzory jako teploměr, senzor vlhkosti vzduchu apod. Volitelně uvažujte i možnost připojení aktuátorů, např. relé. Vhodným způsobem řešte napájení a pro komunikaci použijte WiFi a MQTT (lze ale uvažovat i jiné prostředky komunikace).
3. Na základě definovaných požadavků navrhnete vlastní hardwarové řešení i softwarové vybavení multisenzoru na bázi Raspberry Pi Zero W.
4. Navržené multisenzorové zařízení prototypově realizujte v potřebném počtu instancí a demonstруйте ve vhodné aplikaci s využitím IoT brány na bázi Raspberry Pi vybavené softwarem Node-RED a Home Assistant. Proveďte testování v reálném provozu a vyhodnořte dosažené výsledky.

Literatura:

- Dle pokynů vedoucího.

Pro udělení zápočtu za první semestr je požadováno:

- První 2 body zadání a část návrhu.

Podrobné závazné pokyny pro vypracování práce viz <https://www.fit.vut.cz/study/theses/>

Vedoucí práce: **Janoušek Vladimír, doc. Ing., Ph.D.**

Vedoucí ústavu: Hanáček Petr, doc. Dr. Ing.

Datum zadání: 1. listopadu 2021

Datum odevzdání: 11. května 2022

Datum schválení: 3. listopadu 2021

Abstrakt

Cílem tohoto projektu bylo vytvoření multisenzorového zařízení pro domácnost, které by pokrylo všechny důležité aspekty, které se této problematice týkají. Řešení by sestávalo z mikropočítače Raspberry Pi Zero, který by byl vybaven větší škálou senzorů. Takto vytvořený systém by měl být přístupný skrze zvolené softwarové řešení využitím platformy NODE-RED nebo Home Assistant. Úkolem tohoto zařízení by byl monitoring dění uvnitř domácnosti a sběr dat jako je průběžná teplota, vlhkost, míra pohybu a hladiny oxidu uhelnatého. V rámci práce došlo i k analýze již existujících řešení, které se věnují stejné problematice a to v rámci jak komerční sféry, tak i open-source. Došlo k analýze minimálního hardwarového vybavení systému tak, aby splňoval základní požadavky pro zabezpečení a umožnil uživateli získání cenných informací o dění v domácnosti. Výsledkem je funkční systém, jehož data jsou přístupná jak skrze mobilní telefon, tak i osobní počítač. Finální produkt by se pak měl vyjímat svojí finanční nenáročností, která dokáže konkurovat dostupným komerčním řešením.

Abstract

Goal of this project was to create a multisensor device focused on home safety and which would cover all important aspects that are linked with it. The solution would consist of micro computer Raspberry Pi Zero, which would be equipped with wide range of sensors. This system should be reachable via chosen software solution and platform on which the system works such as NODE-RED or Home Assistant. Objective of such device is detailed monitoring of the ongoings inside the home and gathering of data such as temperature, humidity, level of activity and levels of carbon monoxide. There was also an analysis of already existing solutions of this topic within the scope of this work and the analysis was focused on either the commercial products and open-source ones. The proper analysis of required hardware which would cover all the essential functions of the system and which would let user to gain all the important data was also present. Result of my work is working system whose data are accessible via remote devices such as mobile phone or personal computer and which would give user proper control over his real estate. The final product should be cheap device, that is able to compete with available commercial solutions pricewise.

Klíčová slova

raspberry pi, senzor, IoT, zero, zabezpečení domácnosti

Keywords

raspberry pi, sensor, IoT, zero, home security

Citace

SVOBODA, Jonáš. *Multisenzorové zabezpečení domácnosti s pomocí Raspberry Pi Zero*. Brno, 2022. Bakalářská práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce doc. Ing. Vladimír Janoušek, Ph.D.

Multisenzorové zabezpečení domácnosti s pomocí Raspberry Pi Zero

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně pod vedením pana doc. Ing. Vladimíra Janouška Ph.D. Uvedl jsem všechny literární prameny, publikace a další zdroje, ze kterých jsem čerpal.

.....

Jonáš Svoboda
10. května 2022

Poděkování

Rád bych poděkoval mému vedoucímu doc. Ing. Vladimíru Janouškovi, Ph.D za pomoc a rady při realizaci projektu. Rád bych nadále poděkoval Filipu Václavíkovi za vypůjčení použitých nástrojů a všem použitým sensorům, které během mé práce skončily v křemíkovém nebi.

Obsah

1	Úvod	3
2	IoT systémy a otázka zabezpečení	4
2.1	Internet věcí	4
2.1.1	Historie	5
2.1.2	Využití dnes	5
2.2	Komunikace a správa	6
2.2.1	Komunikační technologie	7
2.2.2	Správa a řízení	9
2.3	Rizika a zabezpečení domácnosti	9
3	Existující řešení	12
3.1	Způsoby zabezpečení	12
3.2	Způsoby přístupu a interakce	13
3.3	Dostupná řešení	14
3.3.1	Komerční	15
3.3.2	Open-source	17
4	Návrh řešení	18
4.1	Definice požadavků	18
4.2	Návrh funkcí zařízení	19
4.3	Výběr hardware	20
4.4	Návrh zapojení a vzhledu	25
4.5	Zobrazení a sběr dat	27
5	Realizace	31
5.1	Zapojení senzorů	31
5.2	Software	33
5.3	Vytvoření modelu obalu	39
6	Testování a naměřená data	40
6.1	Testování a úpravy	40
6.2	Vzhled panelu a zobrazení dat	41
7	Závěr	43
	Literatura	44
	Přílohy	47

Seznam příloh	48
A Obsah přiloženého paměťového média	49

Kapitola 1

Úvod

Tento dokument slouží jako bakalářská práce k vypracování projektu Multisenzorové zabezpečení domácnosti s pomocí Raspberry Pi Zero. V následujících kapitolách se věnuji teoretické části, která poskytne dostačující pohled do nitra této problematiky, podrobné analýze dostupných řešení, návrhu vlastního řešení a nadále stručnému popisu použitého hardware a schémat zapojení jednotlivých součástí do celku, který bude řízen zvoleným softwarem.

S rostoucím výskytem IoT zařízení v běžném životě se objevil nový trend chytrých domácností, který otevírá dveře více odvětvím, kterých se tato problematika týká. Jedním z nich je odvětví zabezpečení domácností, ke které se ubírá hodně pozornosti díky praktičnosti šikovných funkcí, dostupnosti a ulehčení každodenního života získáním dokonalého přehledu nad buďto zajímavými nebo důležitými informacemi o stavu obydlí. Na tato zařízení je kladen velký důraz co se týče jejich hardwarového vybavení, které by mělo splňovat jisté základní požadavky a funkce tak, aby bylo zařízení dostatečně kompetentní a jeho uživateli poskytovalo aspoň základní údaje, které jsou pro toto odvětví domácích IoT zařízení důležité. Dalším z faktorů je jednoduchost používání a přehlednost systému samotného tak, aby bylo dostupné širší veřejnosti, která se nepohybuje v technologických odvětvích a není s principem IoT plně seznámeno.

V posledních letech jsou tato IoT zařízení ve velké míře využívány jako řídicí prvky, které řídí základní aspekty obytných prostor nebo mají přehled nad informacemi jako je teplota, spotřeba, pohyb osob a podobně. Klasickým příkladem je sledování stavu přístupových bodů jako jsou dveře nebo okna, sledování teplotních hladin a jejich regulace pomocí ovládání termostatických hlavice, přehled dostupných zásob v chytrých lednicích, sledování celkové spotřeby energií, ovládání světel, ovládání domácího asistenta pomocí hlasu a mnoho dalších funkcí, které se nám s příchodem IoT v domácnostech zpřístupnily.

Cílem mé práce je vytvoření soudobého IoT zařízení pro domácnost, které by se ve finále věnovalo zabezpečení prostor a které by uživateli poskytlo dostačující kontrolu nad děním uvnitř nemovitosti bez nutnosti být poblíž. Zařízení by disponovalo nejen základní sestavou senzorů, které jsou charakteristické pro tuto problematiku, ale i doplňujícími senzory, které by uživateli dávaly bonusové informace o stavu domácnosti. Základní myšlenkou mé práce bylo analyzovat již dostupné alternativy a vyhodnotit problémové stránky věci, kterých bych se u svého výtvoru vyvaroval. Nejdůležitějším aspektem mé práce je cena finálního produktu, která by měla být razantně nižší než u konkurence.

Kapitola 2

IoT systémy a otázka zabezpečení

Tato kapitola slouží k popisu současné problematiky IoT zařízení, jejich možné a nynější využití v praxi. Cílem kapitoly je seznámit čtenáře s důležitými informacemi, které byly zapotřebí získat při vypracování teoretické části práce v rámci semestrálního projektu. Následující text je nepodrobným uvedením do dané problematiky a není na úrovni encyklopedického textu, tudíž se jedná o povrchový úvod do tématu.

2.1 Internet věcí

Definicí Internet of Things (dále jen IoT) je komplexní síť buďto počítačů, mechanických či digitálních zařízení, zvířat nebo lidí, kteří jsou vybaveni svými unikátními identifikátory v mnoha podobách, v které tyto objekty mezi sebou zvolenou komunikací komunikují a spolupracují v rámci jednoho nebo více systémů a dochází tak k výměně dat bez potřeby tzv. human-to-human nebo human-to-computer interakce. Těmto "věcem" rozumíme kupříkladu jako monitorovací lékařské zařízení, kterými je vybaven člověk, jako například sledovač činnosti srdce s kardiostimulátorem nebo sledovací zařízení, které se běžně používají v zoologii a jsou součástí výzkumu jednotlivých druhů zvířat, až po nejjednodušší zařízení jako jsou výdejní automaty na sladkosti, se kterými se skoro každý člověk někdy za svůj život dostal do styku. U zmíněných výdejních automatů mluvíme například o vzdálené kontrole stavu automatu, z které pak klient získává informace jako aktuální stav zásob nebo interní záležitosti jako vnitřní teplota nebo mechanický výpadek. IoT ekosystém tudíž sestává ze sítě elektronických zařízení, které jsou v dnešní době povětšinou napojeny na internetové připojení a skrze tuto komunikaci jsou naměřená data přístupná ostatním "věcem" v síti pomocí napojení na jakýsi IoT gateway nebo jiné okrajové zařízení, které takto naměřená data buďto posílají například na cloudové úložiště, kde dochází k analýze nebo jsou analyzovány lokálně, což je případem mé práce.[3]

Jak již výklad napovídá, absence potřeby human-to-human a human-to-computer interakce představuje razantní ulehčení procesu, které nám šetří čas a jiné prostředky, které bychom mohli využít jinde. Tento koncept se zamlouvá obzvláště v průmyslových odvětvích, kde je potřeba abnormální velikosti režie logistiky a výhodnost využití tohoto řešení prudce stoupá.

Toto technologické odvětví se těší ze zvýšené popularity automatizace a elektronizace v dnešní době a přímo koreluje s vývojem a popularitou jiných odvětví informatiky. Co se týče termínu IoT, tak v oboru informatiky je to termín docela nový, ale zato velmi diskutovaný.

2.1.1 Historie

Koncept tzv. sítě chytrých zařízení se poprvé objevil a byl diskutovaný v roce 1982 v rámci vývoje komplexnějších výdejových automatů pro občerstvení firmy Coca-Cola. Toto zařízení by sledovalo míru zásobování a hlídalo vzdáleně i aktuální teplotu vně zařízení, což z něho dělalo úplně první komunikující spotřebič napojený na síť ARPANET.

Skutečné přízni se IoT zařízení dostalo circa kolem roku 1999, kdy vznikla myšlenka, že pokud by byly všechny zařízení nebo lidé schopni být identifikováni nebo označeni skrze jedinečné identifikátory jako třeba QR kód, čárový kód, radiofrekvenční identifikace (RFID) a další, tak by to mělo za následek umožnění spolupráce jednotlivých zařízení mezi sebou a dálkové řízení a získání přehledu o stavu zařízení použitím externího počítače. Tudíž prvotním výkladem termínu IoT bylo vybavení všech zařízení svými vlastními identifikátory, které by tento přístup a práci umožnily.

S postupem doby se i pohled na tuto problematiku měnil, ale zásadní změna přichází po roce 2010, kdy se na scénu více protlačuje bezdrátová komunikace, ale je taky brána v potaz velikost a dostupnost součástek a jejich jiné využití než jen v průmyslové sféře. Na scénu přichází využití IoT zařízení v domácnostech a myšlenka autonomního bydlení, které by se chovalo jako soběstačný stroj s minimalizováním nutnosti manuálních úkonů ze strany člověka, které by byly přesunuty do samotné správy IoT systému vně domácnosti. Tato myšlenka se stala hitem a od té doby vidíme nekončící nárůst oblíbenosti a investic u všech tříd společnosti. Vznik odvětví tzv. chytré domácnosti otevřel taktéž dvířka novým problematikám týkajících se těchto systémů, jako například zabezpečení systému jako takového, přístupnost a dostupnost, stálost, udržitelnost nebo maximální soběstačnost.[26]

2.1.2 Využití dnes

V dnešní době, které bez argumentu dominují technologické obory jako je informatika a obecně elektronický průmysl, bez kterého bychom si standard života 21. století nedokázali určitě představit, se využití IoT zařízení dostal do nejrozmanitějších zákoutí každodenních činností. Využití IoT se těší i z budoucnosti, ve které se očekává použití ruku v ruce s uplatněním tzv. AI, neboli umělé inteligence nebo nástupu "bezpilotních" dovožkových služeb. Následující výčet představuje 5 nejčastějších využití v dnešní době, které tomuto poli dominují a tvoří majoritní část populace používaných IoT zařízení.

Senzory

IoT senzory sestávají z sensorů, které se při používání napojují na celou řadu řídicích obvodových desek. V dnešní době jsou nejčastějšími používanými typy desek desky značky Arduino nebo Raspberry Pi, kterou v mé práci osobně používám. Tyto mikro počítače jsou programovatelné a slouží ke sběru a analýze dat naměřených skrze zmíněné senzory. IoT senzory nabízejí ucelenou kontrolu nad naměřenými daty skrze automatizaci přehledným pohledem do jádra věci. Použití těchto sensorů je velice rozmanité.[22]

Analýza dat

V komerční sféře se IoT těší přibývajícím využitím firem v oblasti analýzy důležitých dat, které napomáhají k nalezení možných vzorů a trendů ve sféře, kde bylo nasazeno. Existující aplikace, které používají IoT pak nemají problém se zpracováním jak strukturovaných, tak nestrukturovaných dat, ze kterých lze vyčíst důležité poznatky. Vyhodnocení těchto

analýz poté nabízí přívětivé informace, které mohou vést kupříkladu ke zlepšení pracovního prostředí, zlepšení zákaznické zkušenosti nebo vytvoření jiných hodnot ve komerční sféře. Ve firmách se pak používají prediktivní nebo deskriptivní analýza. Rozmanitost dat není problém, neboť senzory se používají v nejrůznějších odvětvích běžného života. [22]

Sledovací a monitorovací systémy

Firmy používají IoT zařízení ke kontrole a přehledem nad spravovaným majetkem. Takto používaná zařízení používají k monitoringu majetku buďto GPS lokátory nebo jiné radiofrekvenční řešení a dávají majiteli aktuální informace o stavu a umístění objektu, což je při velké režii velice vítané a praktické. Jiná chytrá zařízení pak umožňují například vzdálený přístup.[22]

Výrobní linky

Firmy můžou nadále využívat tzv. řešení IoT propojených továren za pomoci různých softwarů jako je například Azure IoT pro správu IoT přístrojů z industriální sféry. Takovýto cloudový software lze pak doplňovat o jiné zdroje s velkou škálou napojených zařízení všech druhů. Toto použití pak firmě odemyká klíčové informace o stavu všech provozovaných zařízení jako je například jejich teplota, efektivnost nebo doba provozu. Data mohou být získávána ze strojů na odlišných místech.[22]

Chytré zásobování

Lidé na manažerských postech zásobovacích či jiných transportních firem najdou užitek v použití IoT pro vytváření přesných predikcí použitím směrovacích algoritmů. Chytrá zařízení přiřazená transportovanému zboží pak můžou nabízet instantní odezvu při nežádaných situacích skrze GPS lokátor nebo radiofrekvenční identifikátor(RFID). Tyto informace dohromady vytvářejí komplexní systém, který uživateli pomáhá při vytváření důležitých rozhodnutí ovlivňujících spravovanou síť. IoT aplikace jsou pak nápomocny při zmírnění rizik v managementu spravovaného řetězce. Manažeři těchto zásobovacích řetězců pak využívají chytrá zařízení použitím různých softwarových řešení k vyzobrazení naměřených dat, která můžou být následně použita například k snížení finálních nákladů a navýšení získaných výdělků.[22]

2.2 Komunikace a správa

S nezastavitelným vývojem technologií všech odvětví se vyvíjí i způsoby možné komunikace mezi lidmi, stroji ve strojním průmysle, domácími spotřebiči ale i IoT zařízeními. Bezdrátové technologie otevřely světu nové možnosti, co se týče mobilních zařízení, praktičnosti, portability a ušetření prostředků pro realizaci komunikace jako takové. V rámci komunikace u IoT zařízení tak vznikly některé dominantní technologie, které tomuto trhu kralují a představují nynější nejlepší řešení pro bezchybnou a spolehlivou komunikaci mezi jednotlivými přístroji. U těchto technologií ale představuje velký faktor jejich spotřeba energie, která limituje možnosti napájení jednotlivých zařízení a adekvátně se podle toho přizpůsobily. Po stránce správy a řízení těchto přístrojů a jejich platforem tak trh dostupných alternativ také nezahálí. Četnosti použití kralují aplikace jako Home Assistant nebo Node-RED, který je oblíbeným nástrojem domácích kutilů, při jejich tvorbě vlastních zařízení. U aplikací tohoto rázu se hodně hraje na přehlednost jejich uživatelského rozhraní, jednoduchost použití a

vytváření nových funkcí, jejich celkovou dostupnost širší veřejnosti a nenáročnost na používaný hardware. Následující výčet představuje množinu technologií, které se v tomto odvětví nejčastěji používají a tvoří tak důležitý aspekt IoT zařízení používaných po celém světě.

2.2.1 Komunikační technologie

WiFi

Wifi již představuje standard veřejných a soukromých prostor 21. století. Je jí vybavena skoro každá domácnost a představuje hlavní řešení, co se týče napojení na internet všech možných elektronických zařízení, které toho jsou schopny. Ve světě IoT představuje Wifi ideální řešení pro vytváření systému mezi sebou komunikujících zařízení, které jsou napojeny do jedné sítě a fungují lokálně skrze sdílenou IP adresu a stanovený port. Wifi je ideálním řešením pro zařízení, která mají spolehlivý a stálý zdroj napájení, neboť použití této technologie u zařízení, které jsou napájeny bateriově se nedoporučuje kvůli velké spotřebě energie. [29]

Bluetooth

Technologii Bluetooth zná převážná část populace díky rozšířenému výskytu v mobilních telefonech, kde se osvědčil jako skvělý způsob přenosu souborů a streamování multimédií díky své rychlosti a kvalitě přenosu.

Bluetooth je způsob, kterým v telekomunikačním průmyslu jsou schopny mobilní telefony, počítače a jiné přístroje komunikovat mezi sebou využitím připojení na krátkou vzdálenost.

Bluetoothem jsou vybavena všechna zařízení, která ve svých perifériích obsahují speciální Bluetooth vysílač, který je zařízením používán pro vysílání signálů na specifické frekvenci 2,45Ghz, která byla schválně vybrána, neboť nebyla do té doby používána. Každý vysílač je vybaven 48 bitovou adresou standardu IEEE 802. Technologie zvládá jak point-to-point, tak i multipoint připojení.

Bluetooth vysílač se v dnešní době bere již jako velice levná součástka, což je důvodem, proč je touto technologií vybavena velká řada zařízení a to již od těch nejmenších jako jsou například špuntová sluchátka, která jsou v dnešní době populární svou praktičností a malou ztrátou kvality pouštěného obsahu, díky propustnosti až 2Mb za sekundu a vzdáleností dosahu až 10 metrů. Bluetooth představuje ideální řešení pro přenos souborů a streamování různého obsahu a multimédií v přenosných zařízeních.[23]

Ve světě IoT existuje speciální verze Bluetooth tzv. Bluetooth LE, což je zkratka pro Low Energy, které byla taky uvedena pod jménem Bluetooth Smart. Tato technologie byla představena kolem roku 2004 společně s Bluetooth 4.0 jako alternativa pro Bluetooth Classic. Tato alternativa se zaměřuje na zařízení, která se snaží o dosažení co nejmenší spotřeby energie a je využívána většinou IoT zařízení, které jsou Bluetooth vysílačem vybaveny. Díky její malé spotřebě se mohou přístroje pyšnit výdrží baterie od 1 až po 40 měsíců, což je samozřejmě ovlivněno i celkovou specifikací periférií. Při přenosu až 1Mb za sekundu dosahuje spotřeba od 0,01 do 0.5 Wattu. Kupříkladu zařízení iBeacon, které funguje jako Bluetooth lokátor mobilních zařízení v místnosti, využívá Bluetooth LE a výdrž baterie se pohybuje kolem 2 let života na jedno nabití. LE je atraktivním řešením pro výrobce konzumní elektroniky díky dlouhé životnosti baterie, nízkých nákladů na výrobu a jednoduchého vestavění do přístrojů.[18]

MQTT

Technologie MQTT, neboli Message Queuing Telemetry Transport, je jednoduchý komunikační protokol pro vytváření sítě klientů, mezi kterými dochází k nenáročné distribuci dat na menších pásmových šířkách a který vytváří tzv. publish/subscribe schéma, které je používáno pro komunikaci mezi přístroji, tzv. "machine-to-machine" komunikace. MQTT bylo vytvořeno jako nenáročný komunikační řešení do vestavěných systémů, kde je potřeba pracovat s dynamickou šířkou dostupného pásma a limitovanou kapacitou procesoru a zároveň by vytvořil spolehlivé komunikační spojení. Tato varianta komunikace se volí u zařízení, která nejsou softwarově náročná a která se potýkají s občasnými omezeními v šířkovém pásmu, což dělá z MQTT ideální volbu pro vytváření bezdrátových sítí. Tato technologie se díky tomu těší z využití v širokém spektru odvětví.

Styl báze komunikace, na které MQTT pracuje, nahrazuje tradiční model client/server pomocí modelu subscriber (odběratel) a publisher ("vydavatel") a to se zužitkováním maxima z dostupného šířkového pásma. V takovém modelu se o distribuci zprávy od klienta, v našem případě publishera, stará tzv. broker, subscribera a publishera poté rozlišujeme podle toho, jestli klient zprávu odesílá nebo přijímá a zároveň má klient k dispozici funkce obou stran. Úkonu odesílání zprávy pak referujeme jako publish a v opačném případě to je subscribe. Více zařízení může být subscribery u jednoho brokera a získávat tak totožné zprávy a informace.

Komunikace probíhá za pomoci použití hned několika typů zpráv a k jejich posílání dochází skrze port 1883 pro nezašifrovanou komunikaci a port 8883 pro zašifrovanou komunikaci za použití tzv. Secure Sockets Layer (SSL)/Transport Layer Security (TLS). Během tzv. podání ruky mezi klienty dochází pak k ověření certifikátu serveru a následného navázání spojení nebo jeho odmítnutí. Zprávy pak rozlišujeme na typ CONNECT, CONNACK, PUBLISH, PUBACK, PUBREC, PUBREL, PUBCOMP, SUBSCRIBE, SUBACK, UNSUBSCRIBE, UNSUBACK a PINGREQ. MQTT je považován za "light-weight" protokol díky jednoduché struktuře zpráv, které sestávají z hlavičky o velikosti 2 bytů a možného odesílaného obsahu až 256MB.[6]

Zigbee

Zigbee je komunikační technologie, která byla vyvinuta pro vytvoření nenákladných IoT sítí. Vhodná pro sítě s menším objemem přenášených dat, tato alternativa umožňuje efektivní užití v kombinaci s jinými implementacemi. Díky podpoře malých objemů dat, nemusí být v síti přítomná centrála pro správu provozu a transportu informací. Tuto architekturu nazýváme mesh network. Zigbee funguje na bázi kontroly ovládnutí a přehledu nad senzory použitím standardu IEEE 802.15.4 se schopností fungovat na frekvencích 2,4Ghz, 900Mhz a 868Mhz. Jako mesh network chápeme připojení, které hostuje decentralizované uspořádání komunikace všech zařízení v síti. Každé toto zařízení pak představuje node, který je napojen na všechna ostatní zařízení ve stejné síti a umožňuje tak komunikaci mezi nimi. Objekty v této síti rozlišujeme na tři typy a to jsou coordinator, který má za úkol uložení všech informací o síti, router, který směřuje data mezi zařízeními a koncová zařízení, která mohou být energeticky úsporná a komunikují s routerem a koordinátorem, ale nedokážou sama komunikaci směřovat.[17]

2.2.2 Správa a řízení

Home Assistant

Home Assistant byl vytvořen jeho tvůrcem v roce 2013 jako bezplatné a open-source softwarové řešení pro domácí automatizaci a navržen jako centrální systém pro chytrá zařízení v chytrých domácnostech, se zaměřením na kontrolu a přehledem nad nimi a ochranu soukromí uživatele. Přístup do uživatelského rozhraní je možný skrze jak webové aplikace, které jsou dostupné pro mobilní zařízení Android a iOS, což umožňuje flexibilní vzdálený přístup k nainstalovaným periferiím a dokonalý přehled o dění uvnitř prostor. Takový systém pak sestává z centrálního zařízení, ne kterém je nainstalovaný Home Assistant firmware a má za úkol propojovat lokální buďto IoT zařízení, software, aplikace nebo služby do jednoho uceleného systému. Díky jeho skvělé optimalizaci a nenáročnosti je Home Assistant skvělým řídicím řešením pro vytváření nízkonákladových systémů, které mohou sestávat již z nejmenších jednodeskových počítačů jako jsou kupříkladu mikro počítače Raspberry Pi 3 a výše.

Uživatelské rozhraní je velice přívětivé svým vzhledem a možností vlastních úprav dle libosti uživatele s vidinou dosáhnutí největší spokojenost a pohodlí uživatele při jeho používání. Dashboard obsahuje vestavěný editor, který tyto úpravy umožňuje již uvnitř aplikace. Zabezpečení uživatelského přístupu je zajištěno skrze dvoufázové ověřování uživatele a ochrana dat je zajištěna jejich uložením a správou čistě samotným uživatelem než jiným subjektem nebo cloudovou službou. Tuto architekturu nazýváme on-premises software.[25]

Node-RED

Node-RED je tzv. "flow-based" nástroj pro vizuální programování vyvinut společností IBM, který byl navržen jako nástroj pro propojení programů, API, hardwaru a IoT přístrojů. Disponuje jednoduchým uživatelským rozhraním, které pomocí architektury "drag and drop" umožňuje jednoduché naprogramování chování zařízení a dovoluje zapojit i složitější funkce, které se vytváří přímo v UI. Runtime aplikace funguje na bázi Node.js a uživatelem psané funkce jsou psány v jazyce javascript.

Stejně jako Home Assistant disponuje dashboardem, který je z pohledu uživatele kompletně upravitelný a dovoluje tak vytvoření esteticky přívětivých rozhraní.

Tato alternativa správy a řízení IoT zařízení je obzvláště vhodná pro méně zdatné jedince v poli programování. Tento nástroj je plně kompatibilní s dalšími platformami jako je Home Assistant, což ve výsledku znamená efektivní cross-platform využití v praxi a otevírá bránu vícero funkcím na místě použití. Stejně jako Home Assistant je i Node-RED open-source projekt.[27]

Architektura výsledné mapy řízení přístrojů sestává z takzvaných nodů, které jsou mezi sebou propojeny a řídí se skrze něj tok událostí a úkonů. Existuje velká škála různých rozšíření, která jsou specifická pro individuální použití s rozmanitým spektrem součástí a periferií.

2.3 Rizika a zabezpečení domácnosti

V rámci této práce bylo nutné si udělat i detailní pohled na problematiku rizik a možného nebezpečí, která na nás všechna číhají v našich domácnostech a které je nutné při mé práci zohlednit a udělat z nich závěr, se kterým lze pracovat při celkové realizaci a návrhu mého bezpečnostního zařízení. Rizika domácností se s postupem času průběžně mění, což koreluje

s novým a modernějším vybavením obytných prostor 21.století. Z celkového výčtu deseti nejčastějších hrozeb, které ohrožují naše životy i v pohodlí našeho domova se mimo případy jako je zadušení, otrava, utonutí, pádů, nedbalého zacházení s ostrými předměty a nehlídané sporáky, objevují celkově tři velmi časté případy, na které svoji práci směřuji. Těmito třemi případy jsou požáry, které vznikají buďto závadou v elektrických spotřebičích, či jiných vadných elementech v domácnosti, úniky plynu, které jsou ve většině případů spojovány s chybným spalováním ohřevu vody v domácnostech, jako jsou plynové karmy nebo únikem z hlavního uzávěru plynu a nelegální vnik do nemovitostí třetí osobou skrze všechny možné průchody. Tyto tři rizika jsem si dal do hledáčku a podíval se jim detailněji na kloub skrze nemalé množství hlášení institucí, které se těmito problémy zabývají a monitorují jejich počty a místa vzniku. Nejlepším zdrojem informací v této problematice jsou záznamy a články pojišťoven, u kterých majitelé nemovitostí své obydlí pojišťují, hlášení hasičských sborů, které v daných lokalitách fungují a hlášení policejních sborů, kterým se dostávají hlášení o vloupáních. Na internetu jsou tak kvalitní statistiky, které jasně potvrzují mé odhady pro situace, kterým by se mé zařízení mělo věnovat.

Požáry

Požáry dle oficiálních statistik Generálního ředitelství Hasičského záchranného sboru České republiky obsazují druhé místo v žebříčku výjezdů a podle statistik z hasičské ročenky z roku 2020 došlo až k 17 tisícům ohlášeným požárům, ke kterým byla přivolána hasičská pomoc.[14] Existuje spousta zabezpečovací techniky, která proti tomuto ničivému živlu bojuje jako například automatické rozprašovače v prostorách budov nebo v domácnostech oblíbené požární hlásiče, které fungují na principu rozpoznání kouřových plynů z ovzduší uvnitř nemovitosti.

Únik plynu

Podle oficiálních statistik Hasičského sboru města Prahy došlo za uplynulý rok 2020 dohromady k 114 případům, kdy byly povoláni hasiči k úniku plynu v domácnostech a jiných zařízeních, což představuje zhruba 20% z celkových výjezdů k úniku nebezpečných látek.[13] Kupříkladu oxid uhelnatý, kterému je přezdíváno "tichý zabiják" díky jeho neutrální vůni, je klasickým strašákem koupelnových a jiných prostor v domácnosti, kde se nachází plynová karma nebo kupříkladu klasický plynový sporák. K nahromadění oxidu uhelnatého dochází při nedokonalém spalování plynu a jeho vdechnutí při větším množství představuje smrtelné nebezpečí. K ohlášení nebezpečných hladin oxidu uhelnatého slouží speciální detektory, které jsou v dnešní době volně přístupné veřejnosti k zakoupení a jsou vybaveny primitivními senzory jako například MQ7, který mimo to používám přímo ve své práci.

Vloupání

Oproti dvěma zmíněným rizikům se počty vloupání do rodinných nemovitostí každým rokem zvyšují. Z průzkumu z roku 2020 došlo dohromady k 1800 případů krádeží v bytových prostorech a dohromady až 2200 násilného vniknutí do rodinných baráků.[16] Stále se navyšující počty korelují s nezastavující vynalézavostí zlodějů a stagnujícím počtem zabezpečovacích zařízení uvnitř obytných prostor. Z menší analýzy v mém okolí bezpečnostním systémem bylo zajištěno pouze 1 obydlí z 8 dotázaných a většina si spojovala takovéto zařízení uvnitř prostor s finanční náročností, která by ovšem v případě zařízení vlastní výroby

nemusela vůbec být. K ochraně majetku se používají klasické senzory snímající otevření dveří a oken nebo kamerové systémy v okolí a uvnitř nemovitosti.

Kapitola 3

Existující řešení

Jak bylo již zmíněno, součástí mé práce byl i detailní pohled do nabídky již existujících řešení, která by se zabývala problematikou stejného rázu jako je můj projekt, tudíž zabezpečení domácnosti. Existující nabídka koreluje s navyšující se poptávkou, což zapříčiňuje, že je na dostupném trhu velké množství zařízení do domácností, které se soustředí na aspekty zabezpečení.

Jak už to tak bývá, tak byt jsou některá zařízení v rámci komerční sféry, nesplňují tím automaticky podmínky a dostatečné nároky na uspokojující zabezpečení prostor, jako jsou například protipožární senzory, obdobné senzory hlídající faktory ohrožující majetek a způsobující škodu na majetku, nelegální pohyb v nemovitosti, míra pohybu v nemovitosti nebo například dodatečné informace o stavu prostor, které lze získávat skrze dodatečné senzory, jejichž přidání a fungování by mělo na finální cenu produkce minimální dopady.

V této kapitole zmiňuji i průzkum vybavenosti dostupných zařízení a jejich celkovou sestavu periferií a způsoby a technologie, kterými jsou aspekty zabezpečení pokryty nebo aspoň se je pokrýt snaží. Z celkového hlediska širě nabídky je v dnešní době internetu a online obchodů vskutku z čeho vybírat a na scéně se objevuje hned několik výrobců, jejichž výrobky veřejnému trhu dominují a představují nejnabízenější a nejprodávanější řešení.

3.1 Způsoby zabezpečení

S nezastavitelným vývojem technologií ve všech oblastech se i číslo potencionálních hrozeb postupně zvyšuje a spektrum dostupných druhů zabezpečení na to přirozeně reaguje. S tímto pojmem si většinová část populace přirovnává stereotypní řešení jako zastaralé, neestetické kamerové systémy nadměrných velikostí a složité správy, které jsou k vidění na nezměrném počtu budov snad v každém z českých měst.

Vizuální pokrytí perimetru představuje jeden z nejdůležitějších aspektů pocitu bezpečí. Nejčastějším řešením této problematiky jsou komplexní kamerové systémy, jejichž instalace a správa představuje nezanedbatelnou finanční a logistickou zátěž. Pro správu takovýchto systémů jsou v některých případech používány řešení, která vyžadují neustálou interakci třetí strany a majitel tak nemá umožněn přístup z první ruky a musí tak spoléhat na zaměstnance bezpečnostní agentury nebo jiné třetí strany, která je správou takového kamerového systému zavázána. Hlavními specifikacemi kamerových systémů, na které se trh zaměřuje je jejich kvalita obrazu, odolnost, přístup a spotřeba. Standardem kvality obrazu v dnešní době je HD obraz, což odpovídá rozlišení 1920 na 1080 pixelů. V rámci úspory úložiště pořízených videozáznamů a redukce objemu vysílaných dat se snímková frekvence nadále

snižuje tak, aby byla kvalita vizuálního přístupu zachována i při menším omezení funkčnosti, což představuje dvojsečné řešení. Specifické pro kamerové systémy je užití speciálních čoček a objektivů s nestandardním zorným polem, jenž je v těchto případech větší než u klasických kamer. Odolnost kamerových systémů se pak liší podle míst nasazení a rozdělujeme je na venkovní a vnitřní systémy. Místa užití kamerových systémů se pak podepisuje na jejich vnějším zpracování. Přístup k porízeným záznamům pak existuje dvěma způsoby a to buďto z řídicí místnosti, která je specifická pro kamerové systémy v komerčních nemovitostech jako obchody a obchodní centra nebo skrze bezdrátové technologie jako Wifi, které se používají například při instalaci Wifi kamer v domácnostech. Standartní napájení kamer je pak přímo ze sítě nebo adaptéry s klasickým napětím od 5V do 12V. V případě IP kamer, které jsou charakteristické pro použití k zabezpečení prostor, se používá přímé napájení skrze UTP kabel, kterým jsou kamery napojeny. Tomuto řešení napájení říkáme Power over Ethernet (PoE).

K ochraně majetku a prevenci rozšíření již vzniklých požárů se pak používají tradiční detektory kouře nebo požární snímače. Nejčastějším způsobem detekce požáru jsou citlivá kouřová čidla, jenž pracují na bázi průběžné analýzy kvality ovzduší a odchyty nežádoucích kouřových splodin, které jsou při hoření uvolňovány. Napájení těchto zařízení bývá vyřešeno bateriovým osazením, které je více specifické pro požární systémy v menších domácnostech, nebo přímého napájení ze sítě v rámci komplexních požárních systémů, které se nachází například v industriálních zónách a jsou napevno zabudované do energetické sítě. K detekci kouře uvnitř těchto zařízení dochází dvěma používanými způsoby. První způsob detekce je specifický pro tzv. ionizační detektory, ve kterých je užito bezpečné množství radioaktivního materiálu, který je samozřejmě dostatečně odstíněn. Dochází pak k elektrickému nabití částic mezi dvěma kovovými plíšky a průběžné kontrole miniaturního elektrického proudu, který mezi nimi takto vzniká. Větší množství částic v ovzduší pak zapříčiňuje zmenšení tohoto proudu, což spustí poplašné zařízení. Druhá technologie, která je více používaná, využívá tzv. fotoelektrický jev. Dochází k paralelní detekci odráženého světla uvnitř detektoru, které je odráženo od částic v testovaném ovzduší. Pokud v ovzduší žádné částice nejsou, pak není žádné odrážené světlo detekováno a znamená to nepřítomnost kouřových splodin.[28]

Jak již bylo zmíněno, míra nezákonných vniknutí do nemovitostí stoupá a i pro takovéto případy v dnešním světě existuje řešení, které toto ohlídá. Magnetické čidla otevření dveří, oken a jiných potencionálních vchodových prostor jsou dnes již standardem ochrany přístupových cest. Tyto senzory fungují na principu magnetu a spínače, které jsou umístěny ve dvou samostatných částech senzoru. Při zavření dveří tyto součástky vytvářejí uzavřený obvod a při jejich otevření se vzdálením obvod otevírá. Otevření dveří je pak signalizováno centrálnímu kontrolnímu panelu, na který je senzor napojený. Byť jde o technologii primitivní, tak představuje efektivní a finančně nenáročný způsob ohlídky aktivity ve vstupních prostorech.

3.2 Způsoby přístupu a interakce

Způsoby přístupu a ovládání nasazených bezpečnostních systémů sice nejsou stejné, ale sdílí mnoho podobných nebo stejných vlastností. Od dob, kdy bylo stereotypem mít ke každému systému vlastní vyhrazenou místnost se zaměstnancem bezpečnostní agentury uběhlo hodně času a technologie se přesouvají do soukromé sféry samotných klientů. Moderní domácí zabezpečovací systémy jsou z velké míry vybaveny vlastním zobrazovacím médiem jako jsou LCD/LED obrazovky zabudované přímo do centrální řídicí jednotky. Interakce

s takovým panelem pak probíhá skrze dotykové nebo tlačítkové ovládání a uživateli se na displeji zobrazuje rozvržený panel s potřebnými informacemi a rozhraním, které dovoluje úpravu a samotné ovládání systému. Záporné vlastností takového řešení je v uvozovkách vzdálený přístup, u kterého je ale uživatel nucen být přítomen u samotného centrálního panelu, což omezuje dosah přístupu. Dalším řešením jsou softwarové doplňky, které jsou k soudobým systémům někdy dodávány. Skrze aplikace na mobilní telefony Android a iOS získává uživatel přístup k dohledu nad svou nemovitostí skrze mobilní telefon, který je napojen na internetové připojení nebo komunikuje přímo uvnitř nemovitosti na omezenou vzdálenost skrze Bluetooth připojení. Díky nespočtu frameworků, které slouží k vytváření uživatelského rozhraní, jsou tyto aplikace vzhledově moderní a jednoduché na ovládání, což vylepšuje celkovou uživatelskou zkušenost. Přístup skrze externí aplikace je pak chráněn přihlášením uživatele do systému, ve kterém je jeho účet spjat se specifickou zabezpečovací jednotkou.

3.3 Dostupná řešení

Dalším krokem mé práce byla podrobnější analýza nabízených zabezpečovacích řešení, které se zaměřují na stejné aspekty jako můj projekt. Co se týče nabízených variant v komerční sféře, tak je opravdu z čeho vybírat a lze krásně pozorovat, jak se nabídka v reakci na rostoucí poptávku po osobních bezpečnostních systémech rozšiřuje a na trhu vznikají další a další značky, které se tomuto trendu věnují a jimi nabízené zařízení. Nabídka neotálí v žádném z největších českých eshopů a poskytují tak dokonalé místo pro detailnější průzkum nabízených periférií a prostor pro jejich postupné srovnání ve všech aspektech.

V komerční sféře hraje důležitý aspekt finanční nákladnost takovýchto systémů a následná náročnost pro správu a ovládání. Vzniká velmi široké cenové spektrum, do kterého tyto systémy spadají a z podrobnějšího průzkumu ne vždy cena odpovídá skutečné vybavenosti a nabídce zabezpečovacích řešení, jimiž daná periferie disponuje. Široká veřejnost se dostane k nezákladnějším bezpečnostním systémům již od hranice 3.000,-Kč a částka se může vyšplhat až do astronomických čísel jako 25.000,-Kč, které dáme za komplexnější varianty s vícero samostatnými submoduly jak si povíme v následující podkapitole.

Co se týče vnějšího zpracování se komerční systémy těší ze vzhledného designu, který odpovídá dostupným prostředkům výrobce a ve výsledku tak činní ze zabezpečení vkusné estetické vylepšení interiéru nemovitostí.

V otázce obdobných open-source variant mého projektu, mají na scéně celkem slušné zastoupení, které jasně vychází z kutilské nátury komunity, která se pohybuje v technologickém a IT odvětví. Tyto řešení ale mají s komerčními společnou jednu vlastnost a to, že jejich pokrytí zabezpečení ve většině případů není dostatečné a nesplňují všechny nároky, které bych si osobně stanovil jako minimální a reprezentují tak pomyslnou laťku realizace mého projektu. Narozdíl od komerčních variant jsou tyto varianty omluvitelné na úkor jejich open-source a nízkonákladových vlastnostem, které umožňuje neporovnatelně větší dostupnost širší veřejnosti, která je schopna si takovýto vlastní systém sama vyrobit. Co se po finanční stránce open-source řešení týče, tak se dostáváme pomalu k pouhé desetině původní ceny komerčních variant.

Braním v potaz existenci jak komerčních, tak open-source řešení, nám vzniká důležitá srovnávací hranice, jejímž hlavním faktorem se stává finanční stránka věci a nabídka služeb, které tyto systémy nabízejí. Po detailní analýze existujících komerčních variant jsem dospěl k závěru, že cenová laťka je v drtivé většině případů nastavena až moc vysoko a mnohdy neodpovídá reálné vybavenosti a dostupným funkcím těchto prodáváných systémů, které ve

většinou případů velice zaostávají a jsou neporovnatelné se skutečnými funkcemi, které by mohly potenciálně nabízet a byly by jednoduše dostupné a implementovatelné.

Po všimnutí si tak velkého cenového kontrastu, který vzniká při porovnávání dostupných variant, jak ze sféry komerční, tak open-source, jsem si dal za úkol návrh a realizaci řešení, které by bylo schopné konkurovat po obou stránkách věci. Vysoké finanční náročnosti i přispívá fakt, že široká veřejnost si tyto systémy ze stereotypu spojuje s velkou částkou, která se jim nechce investovat a přesto lze vytvořit vlastní efektivní řešení za pouhý zlomek ceny. Toto jasně naznačuje nesrovnatelnou výhodu nekomerčních řešení a vzniká nám tak faktor, který je pro velkou část zájemců o takový systém v jejich domácnosti velmi důležitý a ve věci rozhodnutí, kterou variantu zvolit nebo jestli vůbec, klíčový.

Analýzou existující nabídky jsem dospěl k závěru, že bude dobré se ubírat tímto směrem a v tomto duchu na projektu pracovat. Klíčová slova pro můj projekt tak jsou open-source a finanční nenáročnost.

3.3.1 Komerční

Nabídku komerčních řešení jsem analyzoval skrze vyhledávání na ověřených a autorizovaných e-shopech, které jsou dominantní na českém trhu s elektronikou. Nabídka byla skutečně rozmanitá co se týče značek výrobců, ale spojovala je jedna věc a to velmi podobná hardwarová výbava a cenová relace nabízených modelů. Následující modely byly vybrány tak, abych pokryl všechny cenové relace, ve kterých se tyto systémy objevují.

TUYA chytrý bezpečnostní alarm



Obrázek 3.1: Firmou Tuya nabízený bezpečnostní systém. Převzato z [19]

Zařízení vyráběné společností Tuya je na trhu dostupná za cenu začínající na 6.800,- Kč. Prodávaný systém disponuje klasickým PIR senzorem pro detekci pohybu a dveřními a okeními senzory, které hlídají otevření těchto průchodů. Alarm je napájený skrze DC 5V ze sítě a s komunikační technologií podporující standard IEEE 802.11. Klasické PIR senzory

jsou pak napájeny DC 6V a 4 AAA bateriemi a mají detekční úhel až 110°. Dveřní senzor je napájen DC 3V a lithiovou baterií CR2032. Zakoupený systém obsahuje set 2 dveřních senzorů, 1 PIR senzor pohybu, 1 dálkový tlačítkový ovladač a 1 centrální panel, který je osazen displejem a tlačítkovým ovládáním. Možný přístup skrze mobilní aplikaci.[19]

BEDO Ajax set



Obrázek 3.2: Set Můj dům můj hrad od firmy Ajax. Převzato z [4]

Tento set bezpečnostního systému firmy Ajax lze pořídit za nemalou částku 26.000,-Kč. Sestava disponuje zvukovým alarmem, PIR senzory pohybu, dveřními a okeními senzory a detektorem kouře. Periferie jsou napojeny na ethernetové připojení a napájení je vyřešeno skrze AAA baterie v čidlech a připojením přímo do sítě u centrálního panelu. Tento set ve finále obsahuje 1 centrální panel, 4 PIR senzory pohybu, 1 sirénu, 1 detektor kouře, 1 senzor otevření dveří a 1 senzor pro odposlech tříštění skla. Ovládání a přehled je možný skrze dostupnou mobilní aplikaci pro Android a iOS zařízení.[4]

Bentech WF40C



Obrázek 3.3: Set WF40C od firmy Bentech. Převzato z [15]

Zabezpečovací systém WF40C od firmy Bentech je na trhu dostupný za přívětivější cenu 2.490,-Kč. Centrální panel opět napájen přímo ze sítě a čidla skrze AAA baterie. Panel je osazen klasickým displejem a tlačítkovým ovládáním. Cena pak odpovídá míře vybavení, které za ni zákazník dostane, neboť balení pak obsahuje pouze 1 hlavní panel, 1 PIR senzor pohybu, 1 senzor otevření dveří, 1 sirénu, 1 dálkový ovladač a 2 radiofrekvenční identifikátory.[15]

3.3.2 Open-source

Na webu je až neskutečné množství open-source řešení zabezpečení domácnosti, které jsou volně dostupné a člověk je schopný si ho využitím volně dostupných součástek a zdrojů vyrobit sám tak, aby splňovalo svůj hlavní záměr. Věc, které jsem si ale analýzou tohoto prostoru nabídek povšiml je, že drtivá většina projektů je na velice amatérské úrovni a většinou se zabývají pouze jednou atomickou funkcí, která by mohla ve věci zabezpečení hrát roli. Tyto projekty jsou ve většině případů zaměřené na funkce jako je detekce pohybu, poplašné zařízení, měření teploty, detekce kouře a další, ale vždy jen a pouze na jednu funkci namísto řešení, které by nabízelo vícero funkcí, které by byly nějak propojeny a komunikovaly mezi sebou a ze kterých by se dala generovat nějaká užitečná data pro uživatele. Tímto nám vzniká jakási praktická nepoužitelnost v reálném životě, kde by nám nabízely tyto otevřené řešení plnohodnotné zabezpečení. Tato analýza mi umožnila vytvořit si seznam nároků a funkcí, kterými by moje řešení disponovalo tak, aby mohlo konkurovat komplexnějším systémům, které jsou nabízeny až za desítky tisíc korun.

Kapitola 4

Návrh řešení

V této kapitole se zabývám návrhem celkového řešení zařízení, které se odvíjí od mých poznatků o užití specifických technologií, které se zabývají zabezpečením vnitřních prostor nemovitostí. U návrhu finálního produktu jsem začal se specifikací požadavků, které chci od zařízení splňovat, jeho použití v praxi jako jeho umístění a software, který bude použit pro správu a přístup k měřeným datům.

4.1 Definice požadavků

Požadavky na mnou zhotovené řešení se odvíjí od poznatků ze sféry existujících řešení. Po detailním rozboru jsem si jasně stanovil rozsah pokrytí problematiky a klíčové aspekty, kterým se věnovat.

Návrh mého řešení by měl být vybaven senzory, které by hlídaly pohyb osob, což je nejčastější funkce zabezpečovacích systémů, vznik požárů v prostorech za účelem ochrany zdraví a majetku, vizuální přístup do prostor, který je uspokojující funkcí, kterou uživatel ocení, přehled na hladinou nežádoucích plynů v ovzduší a další bonusové funkce jako měření teploty, které se uživateli mohou hodit a nejsou finančně náročné na zakomponování do systému.

Zařízení by mělo fungovat jako ucelený systém, který by všechny funkce nabízel na jednom místě a po jeho spuštění a nastavení by nebyla potřeba dalšího zásahu třetí osoby. Zařízení by bylo stacionární a to tak, že pro použití ve specifických prostorech by byla potřeba jej umístit na specifické místo, ve kterém by probíhal sběr dat. Pro splnění ucelenosti je zapotřebí vytvoření speciálního obalu, ve kterém by byly periferie zapojeny a uchyceny. Zařízení by mělo být menší velikosti tak, aby nepůsobilo jako esteticky záporný element v prostorech, ve kterých by byl nasazen.

Přístup k zařízení a jeho naměřeným hodnotám by měl být možný ze vzdálených míst skrze vytvořený dashboard, kde by byla tato data zobrazena. Dashboard by měl být přístupný i mimo lokální síť skrze internetové připojení a měl by být zobrazitelný jak na počítači, tak na mobilních zařízeních disponujících funkcí zobrazování grafického obsahu.

Napájení celého zařízení by bylo realizováno skrze napojení přímo do elektrické sítě skrze komerční adaptér nebo za použití přípojky, která by vedla skrze step-down modul pro generování 5V napětí.

Finální zařízení bude teda disponovat dostatečnou škálou funkcí, jeho ovládání a správa by neměla být pro uživatele náročná, naměřená data by měla být správná a správně se

zobrazovat uživateli, rozměry by měly být zachovány v menším měřítku a celková cena by se měla vejít do určité hranice, která pořád spadá do termínu "finančně nenáročná".

4.2 Návrh funkcí zařízení

Jak jsem v předchozí kapitole zmínil, tak ve většině případů se u komerčních řešení setkáváme s velice chabým arzenálem senzorů a funkcí, které podle výrobců a prodejců stačí k zajištění bezpečnosti domácnosti. Výrobci jsou toho názoru, že zabezpečení domácnosti lze zajistit jen a pouze detektory pohybu, které sestávají z PIR senzoru a senzoru otevírání dveří a oken, což představuje oblíbenou kombinaci periférií, se kterými se můžeme setkat v předních českých e-shopech při vyhledávání řešení pro tuto problematiku.

Aspekty, které jsem chtěl jedním zařízením pokrýt jsou požáry, vloupání, vizualizace prostoru a kontrola vchodových prostor. Způsoby jakými tyto situace pokryji jsem si navrhnul v následujících podkapitolách.

Kontrola pohybu

Kontrola pohybu sehrává klíčovou roli v rámci zabezpečovacích systémů a je použita v největší míře. Návrh mého zařízení by se v tom případě nesměl obejít bez tady tohoto aspektu. Nejčastější formou kontroly pohybu jsou senzory, které snímají oblast v určitém radiusu a vzdálenosti od senzoru. Můj návrh pro pokrytí tady této problematiky je vybavit zařízení jedním senzorem, který by snímal infračervené záření, které vydávají osoby přítomné před zařízením. Senzor by byl v designu zabudován tak, ať je kapacita snímaného prostoru co nejvíce využita a design obalu zařízení pro tady to bude přizpůsoben.

Otevírání dveří

Dalším možným způsobem ošetření kontroly pohybu je již zmíněný jazýčkový magnetický senzor otvírání dveřních a okeních prostor. Tento senzor by se v mém návrhu nacházel v dolní oblasti obalu zařízení a snímal by otevírání dveří, nad kterými by byl umístěn. Druhá část senzoru by se pak nalepila pomocí oboustranné lepicí pásky na horní část dveří tak, aby vytvářela uzavřený obvod s první částí senzoru, která by byla přímo zabudována v zařízení.

Snímání prostor

Další nutnou funkcí je vizuální přístup, který by byl zprostředkován skrze vestavěnou kamerku s dostačující kvalitou obrazu. Tato kamera by snímala dění kolem přístroje v reálném čase a uživatel by byl schopný tento livestream zobrazit přímo v dashboardu. V rámci dodržení finanční nenáročnosti, by měla kamera poskytovat nejlepší poměr cena/výkon.

Detekce požáru

Otázku detekce vzniklého požáru bude řešit protipožární detektor splodin v ovzduší v kombinaci s PIR senzorem, který se hodí i k detekci plamene a kamerou, která by snímala prostory pod zařízením. Senzor kouře by v zařízení byl umístěn tak, aby byl schopný analýzy okolního ovzduší a nebránila mu ve snímání žádná další periférie. Při detekci nežádoucích splodin by byl uživatel upozorněn v rozhraní dashboardu a taky by byl informován o průběžně naměřené hladině oxidu uhelnatého v prostorech.

Měření teploty a vlhkosti vzduchu

Bonusovou funkcí, která je nenáročná na přidání, by byla kontrola vnitřní teploty a vlhkosti, které budou měřeny primitivním teplotním senzorem, jehož umístění bude přizpůsobené pro naměření reálných hodnot, které nebudou zkresleny teplotním rozdílem uvnitř obalu zařízení. Teploty by byly zobrazovány v reálném čase.

Měření hluku

Vytvořil jsem i koncept zabudovaného mikrofonu, který se inspiroval od čidel kontrolující zvýšené hladiny hluku, která by spustila na finálním dashboardu hlášení. Tato funkce by mimikovala zmíněné komerční čidla, které se zaměřují na tříštění skla, což by představovalo nelegální násilné vloupání do prostor. Mikrofon by upozornil na zvýšené hladiny hluku.

4.3 Výběr hardware

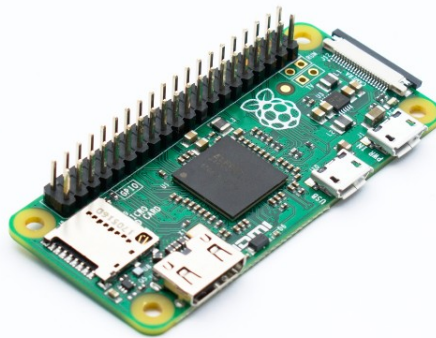
Pro plynulý chod zařízení bylo potřeba vybrat spolehlivé součástky. Preferoval jsem ty, které se nejvíce používají v projektech podobného rázu a se kterými mají uživatelé nejlepší zkušenosti. Každý ze jmenovaných senzorů a součástek plní svoji atomickou funkci, která pak dohromady s ostatními vytvoří komplexní systém vícero funkcí.

Raspberry Pi Zero W

Jedná se o mikropočítač s vestavěným Wifi a Bluetooth modulem. Tento model je zmenšenou verzí klasického Raspberry Pi a kvůli toho disponuje menšími periferiemi jako je 512MB vyrovnávací paměti a taktem použitého procesoru pouze 1GHz. Byť se jedná o zařízení miniaturních specifikací, na použitelnosti v mém projektu to neubírá a tento počítač si hravě poradí se všemi funkcemi, které má plnit. Je vybaven i CSI kamerovým konektorem, který umožňuje připojení kamerového modulu, který by neměl v mé práci chybět. Model W není původně vybaven GPIO hlavičkou připojenou k 40 pinům, kterými je model osazen a je potřeba si tuto součástku obstarat a připojit za použití pájení. Počítač je napájen skrze napětí 5V, které může být dodáno adaptérem nebo jiným řešením. Software počítače je načítán skrze SD kartu, ve které je software nahrán a vložen do SD socketu. Počítač je schopen připojené senzory napájet skrze 5V a 3.3V napětí, které je dostupné skrze umístěné piny.[20] Tato výpočetní jednotka bude v projektu představovat centrální uzel, do kterého budou všechny data senzorů směřovat.

Specifikace počítače:

- 1GHz single-core ARMv6 CPU (BCM2835)
- VideoCore IV GPU, 512MB RAM
- Mini HDMI a USB on-the-go porty
- HAT kompatibilní 40-pin hlavička, CSI kamerový konektor
- 802.11n bezdrátové LAN, Bluetooth 4.0



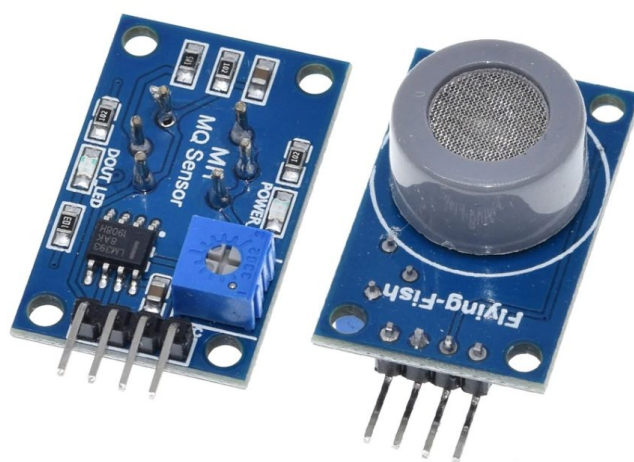
Obrázek 4.1: Mikropočítač Raspberry Pi Zero W. Převzato z [12]

HC-SR505

Tento senzor je nejčastějším výběrem do aplikací, kde je zapotřebí detekce pohybu. Modul pracuje na principu detekce infračerveného záření, které ze sebe vyzařuje lidské tělo. S detekcí pohybu až na vzdálenost 3 metrů, je tento senzor ideální volbou pro zařízení do menších obytných prostor. Infračervené záření je zachyceno kopulí, která sestává z vícero přibližovacích čoček, které ho soustředí na specifické místo čidla. Díky jeho malému energetickému odběru a jeho celkového menšího rozměru, je tento modul vhodný do menších zařízení s omezeným napájením a dokonale se tak hodí do mého projektu. Výstupem senzoru je pak logická 0 nebo 1, což ve finále ulehčuje zpracování signálů. Senzor pracuje s napětím 4,5 až 24V DC. Zorné pole snímání infračerveného záření až 100 stupňů a možná detekce pohybu až 3 metry od senzoru. Rozměry senzoru jsou pak 24x11 mm, což ho dělá praktickým k použití v menších zařízeních. Napěťová logika výstupu je 3,3V DC. Senzor je osazen lineárním regulátorem HT7133-1.[7]



Obrázek 4.2: PIR senzor pohybu HC-SR505. Převzato z [7]



Obrázek 4.4: Senzor oxidu uhelnatého MQ-7. Převzato z [9]

MC-38

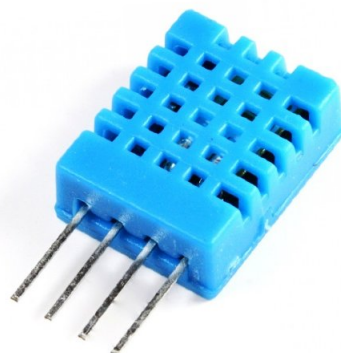
Po senzoru pro detekci infračerveného záření jsou jazyčkové magnetické senzory druhou nej-používanější zabezpečovací součástí. Senzor MC-38 je uzpůsobený na použití u dveřních a okeních prostor, kde vytváří uzavřený obvod, který se při otevření dveří/oken otvírá a dává vědět zařízení, na které je napojen. Díky jeho jednoduchému zapojení, které snese napětí až 100V DC při odběru elektrického proudu maximálně 500mA, nepolárnímu spínači, který dovoluje nespécifické zapojení a jednoduché stavbě, která je odolná vůči opotřebení, je tento model ideální a spolehlivou volbou na použití v místech, kde je potřeba kontrola častého mechanického užívání dveří a oken.[10]



Obrázek 4.5: Jazyčkový senzor dveří MC-38. Převzato z [24]

DHT11

Senzor DHT11 slouží k měření teploty s odchylkou až 2 stupně a vlhkosti vzduchu s odchylkou až 5%. Naměřené hodnoty jsou reprezentovány ve formě digitálního výstupu. Použitím exkluzivní techniky získávání digitálního signálu a technologie měření teploty a vlhkosti vzduchu, je z DHT11 velice spolehlivá součástka s dlouhou životností. K měření teploty je použit termistor a měření vlhkosti pomocí odporové komponenty. Při zapojení do 8-bitového mikrokontroléru, v našem případě Raspberry Pi zařízení, tak vzniká levný, spolehlivý nástroj měření teploty a vlhkosti s rychlou odezvou a důvěryhodnými, naměřenými daty. Díky jeho "jednovodičového", sériového rozhraní je jeho integrace do systému rychlá a jednoduchá. Další výhodou je jeho miniaturní rozměr a malá elektrická spotřeba při napájení 3,3 až 5,5V DC. Sběr dat probíhá v periodě 1 sekundy, během které dochází k odeslání 40bit dat senzorem do napojeného MCU a opětovné čekání na "start-signal" pro další analýzu teploty a vlhkosti.[11]

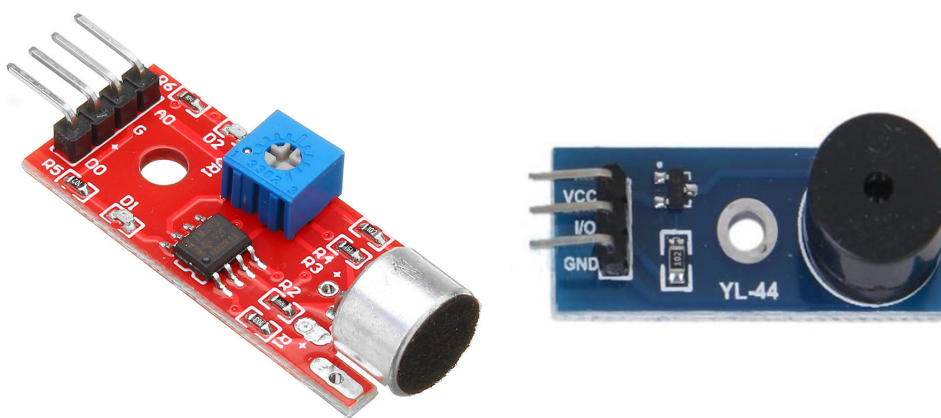


Obrázek 4.6: Teplotní senzor DHT11. Převzato z [11]

KY-037 a YL-44

Mikrofonový modul KY-037 je vhodným řešením do menších zařízení s potřebou odposlechu okolního zvuku. Pyšní se vysokou citlivostí a odchycené zvuk je distribuován skrze analogový výstupní signál. Senzor je napájen skrze 5V DC.[5] Takovýto senzor by mohl být použit se specifickým nastavením pro hlídání překročení hranice hlasitosti jako improvizující detektor tříštění skla, který je obsažen v některých existujících komerčních systémech. Ve spolupráci s nainstalovanou kamerkou by tak uživatel měl dokonalý přehled o dění jak po stránce zvukové, tak i vizuální.

Další součástí, která je vhodná do finálního zařízení je akustický bzučák YL-44, který disponuje frekvencí generovaného zvuku od 100 až 1000Hz. Bzučák by posloužil jako zvukový hlásič možného nebezpečí. Napájení je možné jak 5V, tak 3,3V DC.[1]



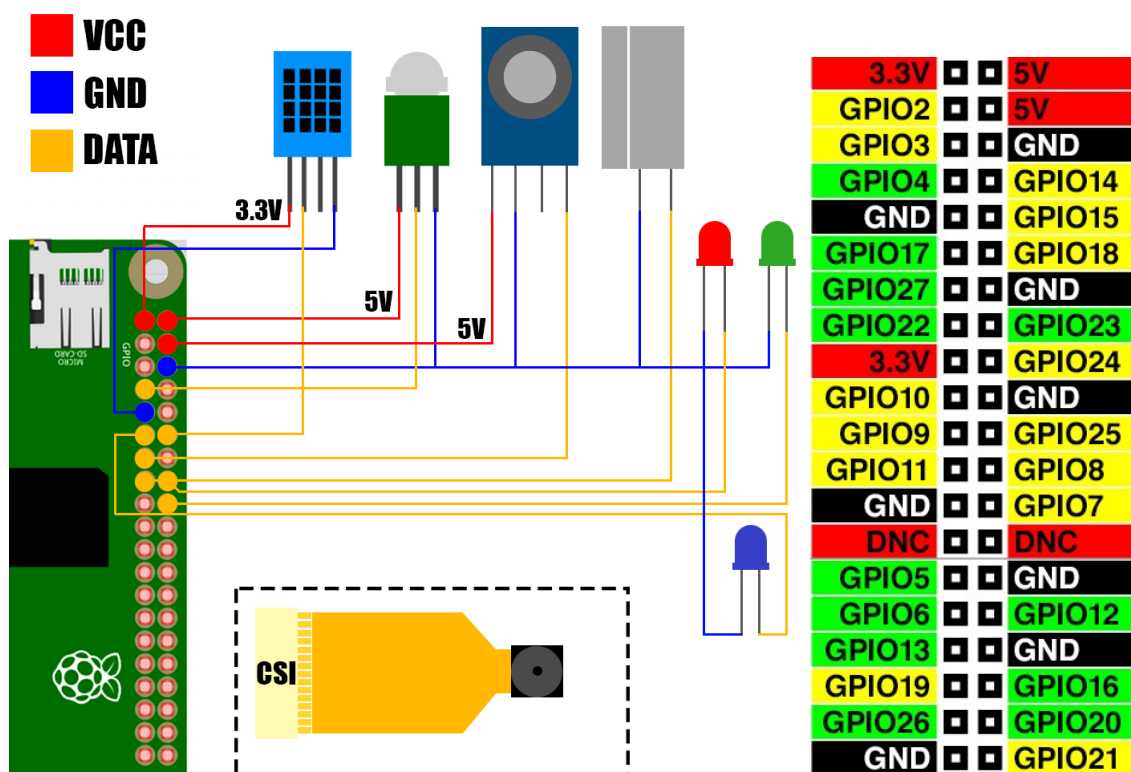
Obrázek 4.7: Mikrofonový modul KY-037 a akustický bzučák YL-44. Převzato z [5] a [1]

4.4 Návrh zapojení a vzhledu

Zapojení

Vybrané součástky by měly ve finálním produktu fungovat jako komplexní systém a existovat a fungovat paralelně bez závislosti na ostatních pokud o to přímo nežadáme. Klíčovým parametrem je v tomto případě celkové vytížení procesoru mikropočítače s ohledem na jeho minimalistické parametry. Byť pracujeme s parametry takového rozměru, tak si Raspberry Pi Zero svým geniálním designem hravě poradí i s tímto úkolem, jak jsem měl šanci si sám odzkoušet.

Použité periferie včetně doplňkových jako jsou LED diody budou zapojeny dvěma způsoby. První způsob bude zapojení přímo do GPIO hlavičky samotného počítače bez použití vedlejších cest a druhý způsob bude napojení skrze pájivé pole. Druhý způsob je ve finále nutný, neboť možnosti napájení senzorů jsou omezené a je potřeba rozvrhnout adekvátní redistribuce napájení. Většina senzorů má pracovní napětí od 5V výše a v GPIO se nachází pouze dva takovéto konektory, tudíž bude zapotřebí napětí natáhnou mimo a za použití rezistorů napájet více senzorů najednou. V návrhu zapojení (viz. 4.8) je 5 nejzákladnějších

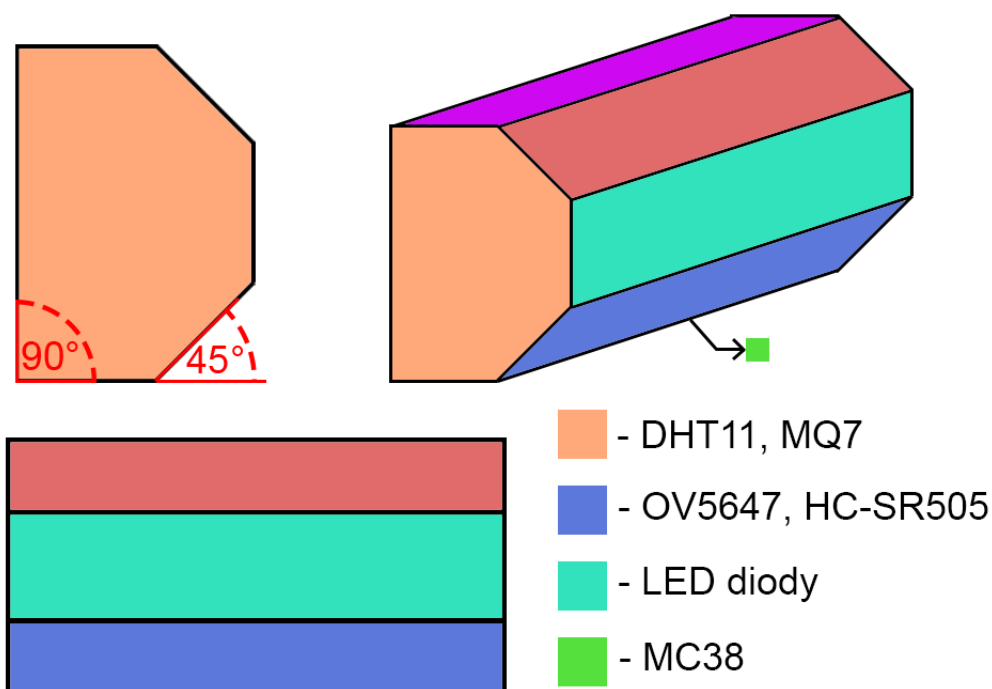


Obrázek 4.8: Návrh periferií do GPIO a mapa GPIO samotného

součástí, které ve finálním výtvaru nesmějí chybět a doprovázeny jsou 3 LED diodami. Způsob zapojení bude následovný. Senzor teploty a vlhkosti vzduchu DHT11(první) je napojen na napětí 3.3V, což je dolní hranice pro jeho pracovní napětí a jeho datový výstup povede do pinu GPIO18. Senzor infračerveného záření HC-SR505(druhý) je napojen přímo do počítače na pin s napětím 5V. Jeho datový výstup bude připojen k pinu GPIO4. Následuje senzor plynu v ovzduší MQ-7(třetí), který je taktéž napojen na napětí 5V a jeho datový výstup zpracováváme na pinu GPIO27. Jazyčkový magnetický senzor otevření dveří HC-38(čtvrtý) je zapotřebí zapojit pouze do uzemění a programovatelného pinu GPIO22. Kamera bude samostatně zapojena do speciálního kamerového slotu CSI konektorem. Systém bude doplněn o diody, které budou znázorňovat aktuální stav a probíhající činnosti zařízení. Diody budou napojeny na programovatelné piny GPIO 17, 23 , 24 a do uzemění.

Vzhled

Aby se zařízení mohlo brát jako celistvý prvek, bude potřeba návrh a realizace samostatného obalu, do kterého veškeré vybrané periferie vložíme a ve kterém bude zařízení schopné fungovat po celý čas provozu. Design obalu by měl být nenápadný a podobat se například klasickému zavírací dveří, který je vždy umístěn nad zárubněmi dveří a svými rozměry neomazuje své okolí.



Obrázek 4.9: Náčrt vzhledu obalu

Prvotní návrh je pouze náčrt toho, co si představuju jako finální výsledek. Tvar a velikost pouzdra je přizpůsobena umístění senzorů tak, aby jimi naměřená data nebyla ovlivněna vedlejšími jevy, jako je kupříkladu hromadění tepla uvnitř obalu a jiné. Profil zařízení bude mít tvar půleného osmihranu, neboť jeho specifické zkosení je ideální pro všechny mnou použité senzory a součástky.

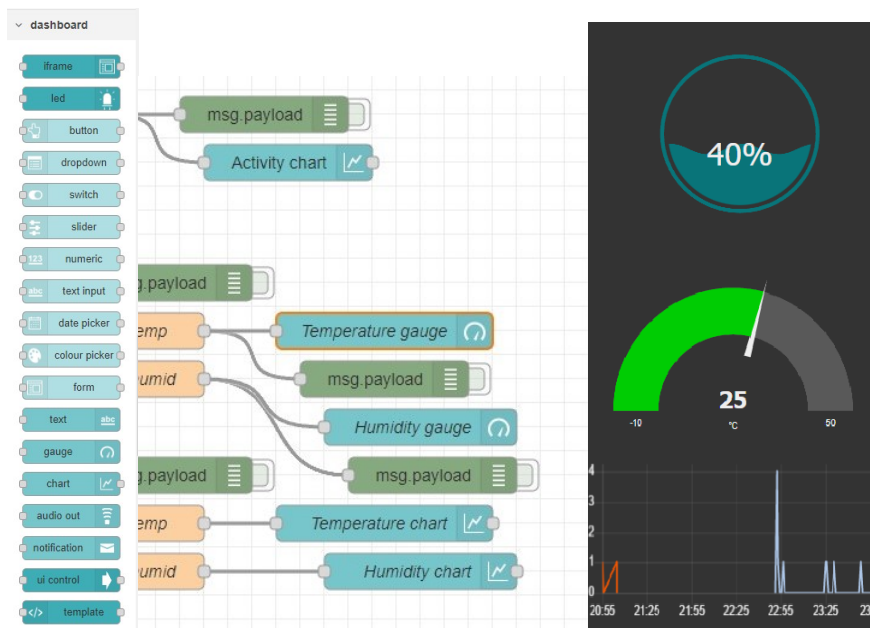
Umístění kamery je ideální na spodní ploše o náklonu 45 stupňů. Takto umístěná kamera je nasměrována přímo na prostor pod přístrojem a není problém ani omezené zorné pole kamery. Senzor detekce otevření dveří bude umístěn na nejspodnější ploše, neboť k jeho fungování je potřeba být vodorovně s hlídanými dveřmi. Senzor pro měření teploty se bude nacházet v dolní části pravé, boční strany obalu. Jeho umístění do spodní části je schválně z důvodu možnosti ovlivnění naměřených dat nahromaděným teplem z mikropočítače a kamery, jež vydávají při provozu nemalé množství tepla. PIR senzor je spolu s kamerou umístěn na dolní zkosené straně pro lepší perimetr pokrytí a náhradu funkce kamery při její možné nedostupnosti. Poslední senzor pro umístění je MQ-7, který bude stejně jako teplotní senzoru umístěn na boční straně obalu, tentokrát na levé, kvůli ušetření místa. Na kolmé čelní straně obalu budou umístěny LED diody, pro zobrazení aktuálního stavu zařízení. V tomto místě bude zajištěna jejich kvalitní viditelnost.

4.5 Zobrazení a sběr dat

Co se týče správy zařízení a přístupu k naměřeným datům, je mým hlavním cílem zachovat celkovou režii co nejméně složitou. Novodobé trendy uživatelských rozhraní se řídí heslem "v jednoduchosti je krása" a podobným stylem bude vytvořen i zobrazovací panel mého projektu. Panel by měl zobrazovat všechna primární data generovaná senzory a vyhnout se

zobrazování matoucích dat a ovládání, které celkovou přehlednost ztíží a tím i zhorší celkovou uživatelskou zkušenost. Po softwarové stránce by mělo docházet k přístupu k datům skrze řešení, které je i nenáročné na provoz s ohledem na periférie užitého mikropočítače.

Skvělým řešením této problematiky pro IoT zařízení menších kapacit je rozšíření pro tvorbu uživatelského rozhraní v programu Node-RED, které je schopno s menší režií vytvořit esteticky přívětivé rozhraní. Takto vytvořený dashboard by měl obsahovat grafické prvky, které znázorňují všechny naměřené data jako je teplota, vlhkost vzduchu, okýnko realtime vysílání kamerového modulu, stav otevření dveří, míra pohybu v rozmezí několika posledních hodin v podobě grafu a naměřené hodnoty CO v ovzduší.



Obrázek 4.10: Příklad nabízených elementů z rozšíření, jejich užití ve flow a finální zobrazení na zobrazovacím panelu

Grafiky v zobrazovacím panelu by byly stacionární elementy, jejichž poloha a vzhled by byl stacionární a neměnný, takto zachováme jakousi konzistenci, která nebude pro uživatele matoucí a ulehčí čtení naměřených dat.

Způsob a perioda měření dat se bude odvíjet od jejich povahy. Například na časové rozmezí měření teploty a vlhkosti okolního vzduchu bereme jiné nároky než na měření aktivity z nasazeného PIR senzoru, neboť průběh teplotních hladin během posledních 24 hodin nám dá zajímavé informace, které mohou vést k dalším úpravám v domácnosti, jako je například kooperace zabezpečovacího systému a ovládání termostatických hlavíc topných těles, jejichž nastavení se od naměřených dat může odvíjet a uživateli nabízí bonusovou funkci ve formě snížení nákladů na energie.

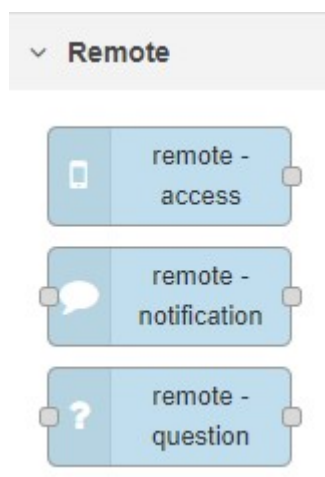
V rámci měření teplot by bylo v tomto případě ideální nastavení 24 hodinového okna spolu se zobrazením reálné nynější teploty v prostorech. Ideální grafické elementy pro tyto funkce jsou v tomto případě klasický linkový graf s osou pro teplotu a postupující čas a budík s odpovídajícím zbarvením podle aktuální teploty. Pro zobrazení vlhkosti a hladiny CO ve vzduchu pak použijeme grafiku zobrazení aktuální hladiny. Viz. 4.10

Časové okýnko pro naměřenou aktivitu v domácnosti je pak ideální nastavit na rozmezí menší, jako například 3-5 hodin, neboť od uživatele se očekává průběžná kontrola podle

libosti a takto naměřená data ve větší míře nepřináší žádné jiné výhody. Uživatel si samozřejmě finální rozmezí bude moci nastavit podle svého vkusu a finální vzhled není nijak permanentní.

Aktivita se od měření dat jako je teplota a vlhkost vzduchu bude lišit způsobem jakým je zapisována do grafu. Návrh pro měření aktivity je v tomto případě vytvoření 3-5 hodinového okénka pro zobrazení aktivity v čase a perioda 10 minut, během kterých se aktivita pomocí vestavěné funkce bude počítat a posléze předávat na vyhodnocení do grafu a nulovat pro další měření v periodě 10 minut. Realtime zobrazení aktivity bude pak znázorňovat virtuální dioda, která své zbarvení mění v reakci na aktuální stav PIR senzoru, čili logická 0 nebo 1.

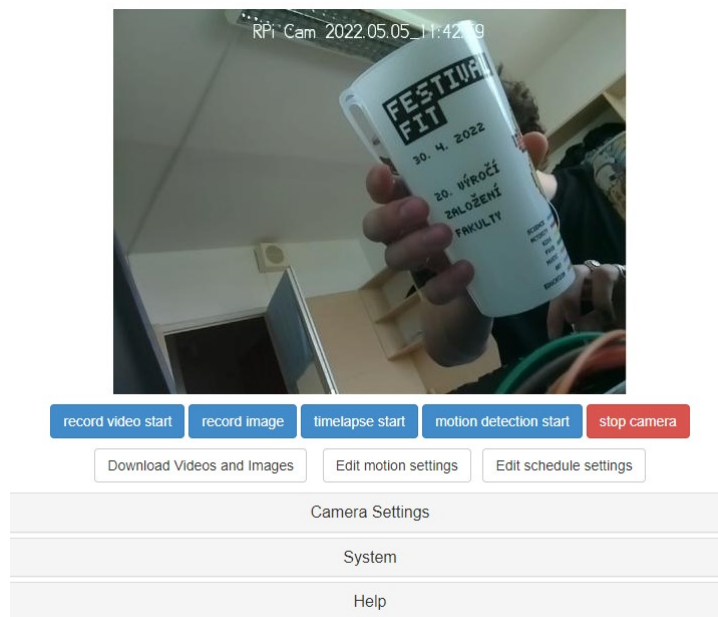
Přístup k panelu pak bude možný dvěma způsoby. Prvním bude webová stránka, která je hostovaná přímo skrze Raspberry Pi Zero a ideálně navštěvována použitím stolního počítače nebo notebooku. Druhým způsobem je vzdálený přístup z jiné sítě. Vzdálený přístup je možný za použití Remote-RED pluginu, který vytváří komunikační tunel se zvolenými servery, které se nacházejí v Americe nebo v Německu. Uživatel si pomocí unikátního vygenerovaného QR kódu autentizuje mobilní telefon se specifickým systémem, který se mu poté zobrazí v nabídce mobilní aplikace, která je volně přístupná zařízením Android a iOS. Rozšíření nabízí možnosti jako push notifikace do mobilní aplikace a navázání samotného vzdáleného spojení. [21]



Obrázek 4.11: Node-RED elementy rozšíření Remote-RED

Vzhledem k dobré kompatibilitě s oblíbeným Home Assistant, bude možno vytvořenou flow z Node-RED propojit s používaným Home Assistant, což umožní vnoření přístupu ke správě a zobrazení přímo z druhé aplikace. K tomuto se používá rozšíření Home Assistant websocket za použití speciální API.

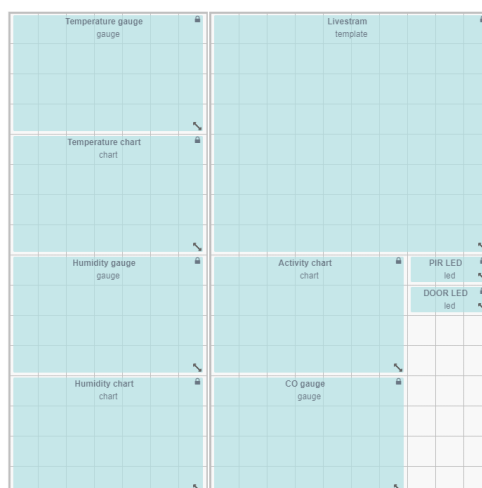
Pro vizualizaci snímaných prostor by byl ideálním řešením kamerový modul v módu livestream, který by snímal reálné dění před kamerou a generoval živé vysílání, které by bylo promítáno do zobrazovacího panelu. Pro použití v Node-RED aplikaci existuje projekt s pojmenováním RPi Cam Web Interface, které funguje na principu vytvoření jednoduché html stránky na hostující IP adrese a portu. Viz. 4.12. Toto rozhraní je pak možno vnořit do samotného Node-RED dashboardu skrze iframe element s nastavitelnými parametry jako je rozlišení obrazu a estetická úprava efektů nad pořízenými snímky. [2]



Obrázek 4.12: Ukázka ovládání kamery skrze vygenerovanou html stránku

Rozložení panelu

Rozložení panelu pak závisí na množství použitých grafických ukazatelů a okének. Vestavěná funkce aplikace Node-RED dovoluje pohodlné úpravy za použití jednoduchého a přehledného ovládání nastavení. Jednotlivé grafické elementy se balíčkovávají do skupin s pojmenováním a jejichž šířka je libovolně nastavitelná spolu s šířkou samotných elementů uvnitř. Sestavení takového návrhu je pak velmi rychlé, jednoduché a ve výsledku esteticky přívětivé, neboť Node-RED používá pro vytváření těchto uživatelských rozhraní Angular framework, který je velmi moderním a efektivním nástrojem pro tvorbu UI.



Obrázek 4.13: Návrh rozložení zobrazovacího panelu uživatele

Kapitola 5

Realizace

V této kapitole se zabývám již finálním sestavením a zapojením zvolených periférií, vytvoření softwarové stránky, jako je zobrazovací panel a spolupráce jednotlivých senzorů mezi sebou a vytvoření modelu krabičky, ve které přístroj bude zasazen a připraven k použití.

5.1 Zapojení senzorů

Prvotním krokem před zapojením všech periférií, bylo jejich otestování při samostatném chodu a ověření správnosti jejich výstupních dat a jestli nejsou závadné nebo jinak mechanicky poškozené. Vadný ze všech pořízených senzorů byl pouze senzor detekce pohybu, který měl problém s odstíněním nechtěných okolních signálů, což způsobovalo falešné pozitivní signály, které zkreslovaly celkovou detekci okolního pohybu. Tento vadný senzor byl model HC-SR501, který údajně tento problém má docela často a já se rozhodl vyměnit tento model za lepší HC-SR505, který se s těmito problémy již nepotýká a další výhodou byly i menší rozměry.

Postup a styl testování jednotlivých senzorů byl u každého velice podobný. Principem bylo řízení a výpis naměřených dat senzoru skrze skripty napsané v jazyce Python za pomoci doplňkových knihoven, které podporují použité senzory a součástky a skrze které bylo čtení dat velice jednoduché. Komunikace a ovládání mikropočítače bylo zajištěno skrze SSH připojení v lokální síti, která byla nakonfigurována v souboru `wpa_supplicant.conf`, který se nachází v SD kartě s nahráním OS. Přes navázané SSH spojení bylo pak možné tyto skripty vytvořit a pustit přímo v rozhraní mikropočítače. Operační systém, který byl do SD karty nahrán je Raspbian, což je oficiální Raspberry Pi OS. Pro minimalizaci režie jsem použil verzi bez grafického rozhraní, se kterou se operuje jen a pouze přes terminál.

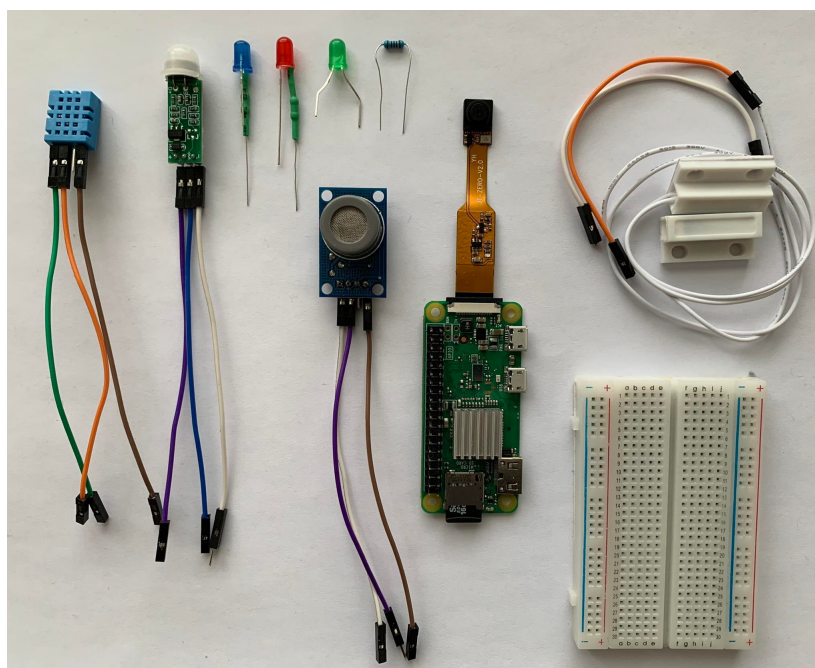
```

import Adafruit_DHT
import time
DHT_SENSOR = Adafruit_DHT.DHT11
DHT_PIN = 17
while True:
    humidity, temperature = Adafruit_DHT.read(DHT_SENSOR, DHT_PIN)
    if humidity is not None and temperature is not None:
        print("Temp= {:.1f}C Humidity={:.1f}%".format(temperature, humidity))
    else:
        print("Sensor failure. Check wiring.")
    time.sleep(2.0)

```

Obrázek 5.1: Příklad skriptu pro ověření funkčnosti teplotního senzoru DHT11

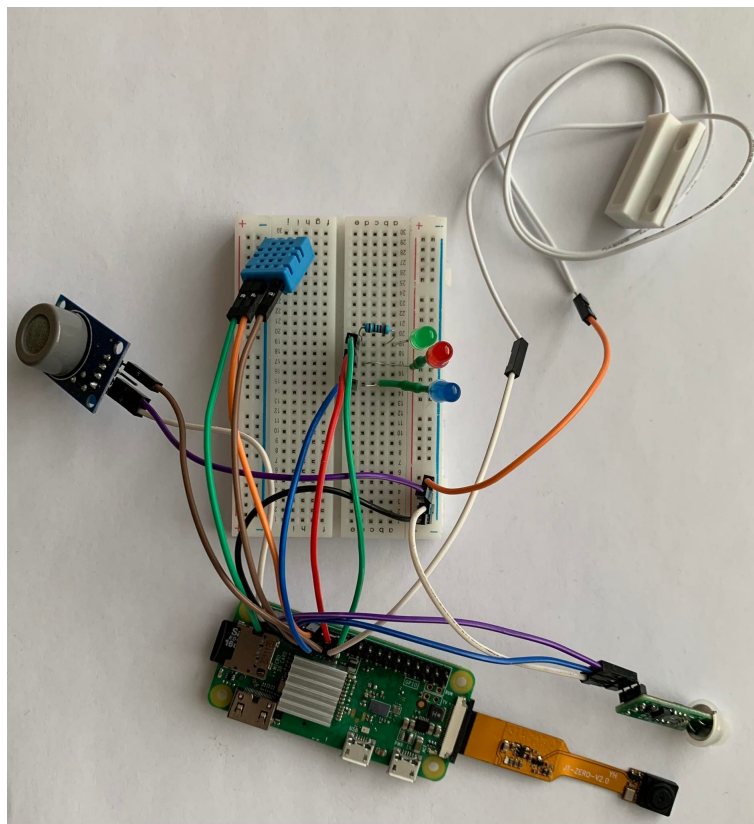
Styl zapojení použitých senzorů je velmi obdobné. Jedná se o napojení na napětí distribuované samotným mikropočítačem, ve kterém se nachází piny s voltáží 3.3 a 5V a napojení výstupu senzorů s tokem dat na programovatelné piny v GPIO hlavičce. Mapování programovatelných pinů je čistě numerické a tak ulehčuje celkovou práci s vytvářením testovacích skriptů pro jednotlivé senzory.



Obrázek 5.2: Použité periferie

Finální zapojení senzorů a LED diod bylo realizováno přesně podle původního návrhu (viz. 4.8) s výjimkou použitých rezistorů, které jsem v návrhu nezmínil a bylo je nakonec potřeba do systému zakomponovat z důvodu zamezení zkratu diod. Použité LED diody jsem za použití pájení vybavil přímo vlastními rezistory, což ve finále ulehčilo režii při zapojování. Co se týče pájení, bylo zapotřebí připájení i samotné GPIO hlavičky, která se k prodávanému modelu W mikropočítače Raspberry Pi Zero nedodává. Sensory jsou

pak paralelně zapojeny buďto přímo do GPIO mikropočítače nebo použitím pomocného zapojení do pájivého pole pro sdílení omezených zdrojů jako například uzemnění.



Obrázek 5.3: Finální zapojení všech senzorů a součástek

5.2 Software

Mikropočítač běží na operačním systému Raspbian OS, jenž je volně dostupná odnož Debian OS, distribuovaná přímo firmou Raspberry Pi. Verze bez grafického rozhraní tak představuje jednoduchý a zároveň efektivní způsob provozu. Při prvotní konfiguraci je nutné nastavit bezdrátové připojení vytvořením nebo přepsáním již zmíněného konfiguračního souboru. Takto vytvořený soubor se pak při prvním spuštění zařízení zaeviduje do systému a počítač je pak schopen opětovného připojení k síti při dalším použití. Jakmile je počítač připojen do lokální sítě, tak je uživatel schopen o napojení a řízení skrze klasické SSH.

K řízení všech napojených periférií zabezpečovacího zařízení byl použit podle zadání software Node-RED. Ten je potřeba nejdříve stáhnout a nakonfigurovat pro vytvoření lokálního hostingu, na kterém jsme schopni vytvářet řídicí elementy zařízení. Následující příkazy jsou esenciální pro nachystání fungujícího Node-RED na našem zařízení:

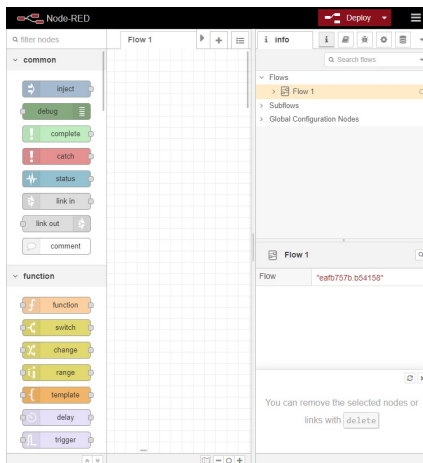
```
sudo apt-get install nodered
node-red-pi --max-old-space-size=256
sudo systemctl enable nodered.service
```

První příkaz slouží k samotnému stáhnutí a instalaci balíčku Node-RED, která je zapotřebí. Dalšími důležitými doplňky pro spuštění Node-RED je přítomnost Node.js a NPM v zařízení. Je nutné zmínit, že na použitý model Raspberry Zero W jsou omezeny dostupné verze potřebného softwaru a v tomto projektu byla použita vývojová verze 10.24.0 Node.js, 5.8.0 NPM a ve finále 1.34 Node-RED, jenž je nejaktuálnější podporovanou verzí na modely Zero W. Toto omezení je výsledkem specifikací počítače, které zamezují použití aktuálnější verze. Naštěstí to nijak neomezuje funkce a potenciál použití na zařízení tohoto typu.

Druhý příkaz slouží ke spuštění samotného Node-RED s doplňkovým omezením využití paměti na 256Mb kvůli omezené celkové paměti 512Mb, kterou je počítač vybaven.

Třetí příkaz pak zajišťuje automatické spuštění služby při opětovném spuštění zařízení, takto nastavené zařízení je pak připraveno hostovat službu v řádu několika minut po spuštění.

Aplikace samotná je pak skrze webový prohlížeč dostupná na IP adrese samotného počítače v naší síti a portu 1880, který aplikace používá. Při návštěvě stránky se pak dostaneme do hlavního rozhraní aplikace.



Obrázek 5.4: Vzhled rozhraní Node-RED

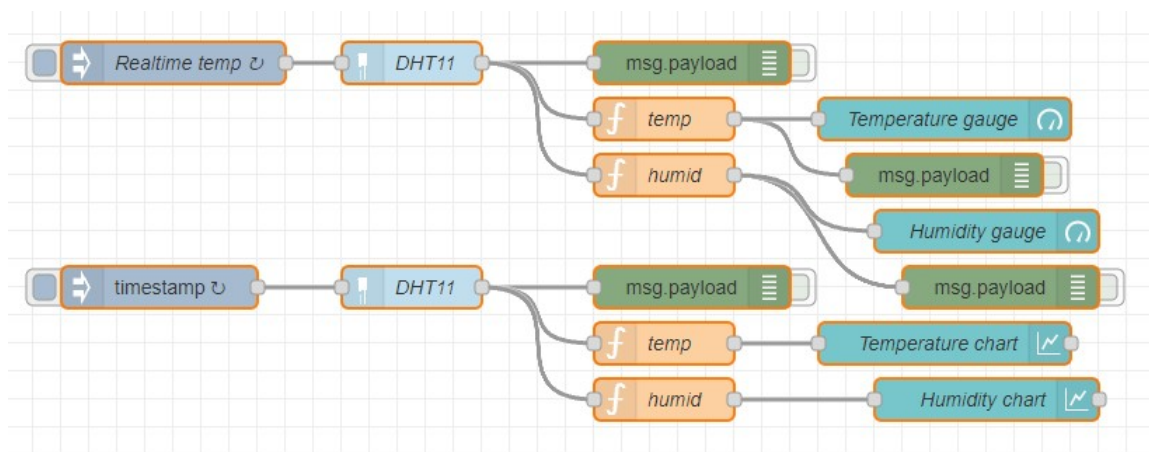
Pro tvorbu flow, která řídí celé zařízení jsou používány tzv. nodes, které představují jednotlivé elementy jako jsou senzory, piny GPIO hlavičky, vlastní funkce nebo zobrazovací elementy panelu a další. Pro realizaci mého systému bylo zapotřebí stáhnutí doplňujících rozšíření, která jsou kompatibilní s použitými součástkami a zapotřebí k finální implementaci.

Stažená rozšíření:

- node-red-contrib-dht-sensor - teplotní senzor DHT1
- node-red-contrib-remote - vzdálený přístup do hlavního panelu
- node-red-contrib-ui-led - virtuální LED dioda do hlavního panelu
- node-red-dashboard - zobrazovací panel
- node-red-node-pi-gpio - mapování GPIO hlavičky Raspberry Pi Zero
- node-red-node-ui-iframe - vnoření webové stránky do hlavního panelu

V tomto uživatelském rozhraní pak bylo potřeba vytvořit flow diagram, který by znázorňoval celkové ovládání a fungování systému spolu se zobrazováním naměřených dat. Pro každý senzor jsem tak vytvořil sled nodů, ve kterých byly vestavěny buďto funkce, časovače nebo jiné elementy.

Pro senzor DHT11 byly vytvořeny dohromady 2 sady nodů, které se skládají z časovače Realtime temp a timestamp, nodu DHT11, který je získán ze staženého doplňku `node-red-contrib-dht-sensor`, vlastní funkce `temp` a `humid`, zobrazovacích elementů Temperature gauge, Humidity gauge, Temperature chart, Humidity chart a debugovacích nodů pro výpis hodnot do vestavěného debuggeru Node-RED. Obě sady se liší pouze nastavením jejich časovačů. Intervaly měření teploty jsem nastavil na každou jednu sekundu a každých 10 minut, přičemž kratší interval byl použit pro zobrazení aktuální teploty a delší interval byl použit pro vytváření grafu průběžné teploty. Nody DHT11, byly nakonfigurované pro čtení dat z pinu číslo 1, neboť byl použit standard číslování pinů GPIO Rev2. Vlastní funkce `temp` a `humid` slouží k vyseparování dat, které jsou posílány z DHT11 nodu, který je posílá ve struktuře `msg`, ve které je obsažena proměnná `msg.payload` s teplotou a `msg.humidity` s vlhkostí. Naměřená data jsou nakonec posílána buďto do grafů posledních 24 hodin nebo do budíků, které zobrazují aktuální hodnoty. Celý proces pak probíhá tak, že časovače posílají startovací signál nodům DHT11, které naměřená data posílají skrze funkce `temp` a `humid` a ty je promítají do zobrazovacích elementů.



Obrázek 5.5: Logika zapojení sady nodů pro řízení a zobrazování dat ze senzoru DHT11

PIR senzor HC-SR505 je řízen sadou nodů, která se skládá z nodů reprezentující vstup pinu v GPIO hlavičce PIR, na který je výstup senzoru napojen, časovače Activity timer, vlastních javascript funkcí `NOT` a `activity counter`, výstupní piny pro ovládání fyzických LED diod LED-motion a LED-nomotion, zobrazovací elementy virtuální LED diody PIR LED a grafu Activity chart a výpis do debuggeru. Reprezentace PIR senzoru je skrze node vstupu z pinu GPIO04, na který je výstup senzoru napojen. Senzor při detekci pohybu spíná a posílá buďto jedničkový nebo nulový signál, který je předáván dále virtuální diodě, která v zobrazovacím panelu mění barvu na základě přijaté hodnoty a dvěma výstupními nodům GPIO, který při získání signálu rozsvěcuje nebo zhasíná červenou a zelenou LED diodu. Funkce `NOT` v tomto případě slouží k negaci přijatého signálu převrácením 1 na 0 a naopak. Toto slouží k ovládání zelené LED diody. Funkci `activity counter` předchází časovač, který je nastaven na periodu 10 minut. Při sepnutí časovače posílá signál funkci, která měřila četnost detekce pohybu PIR senzorem v uplynulém intervalu a funkce předává naměřenou

```

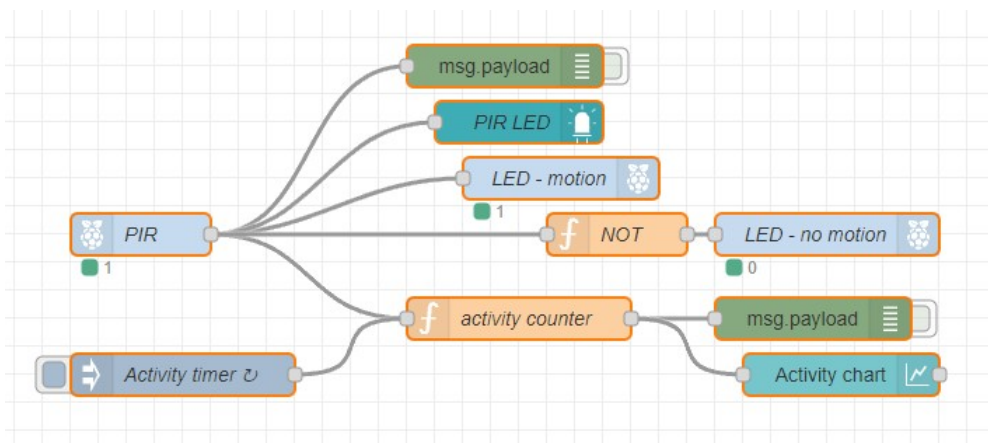
var activity = context.get('activity') || 0;
if(msg.payload === true){
    msg.payload = activity;
    context.set('activity', 0);
    return msg;
}
else if(msg.payload === 1){
    activity += 1;
    context.set('activity', activity);
}

```

Obrázek 5.6: Kód funkce activity counter

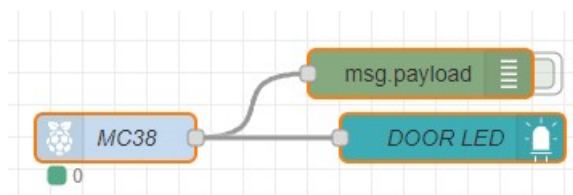
hodnotu zobrazovacímu elementu grafu a nuluje se pro následující měření (viz. 5.6). Funkce rozlišuje přijaté zprávy podle typu získané struktury `msg` pomocí čtení z `msg.payload`.

Ve finále uvidíme na zobrazovacím panelu graf četnosti detekce pohybu za posledních 5 hodin a virtuální LED diodu, která slouží k zobrazení aktuální detekce pohybu v okolí.



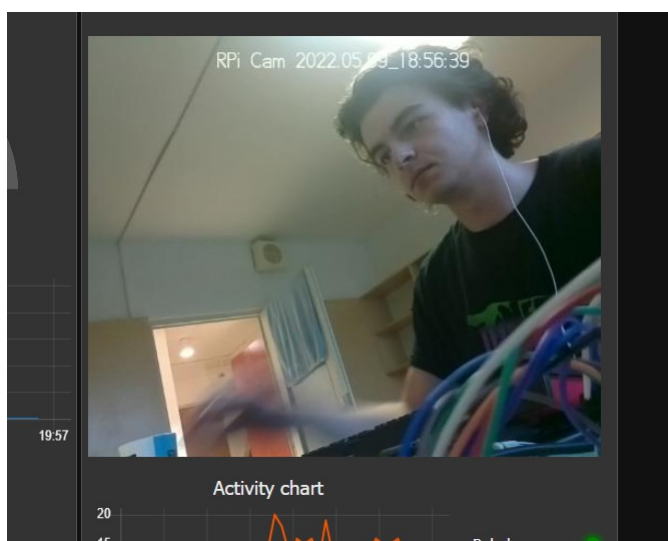
Obrázek 5.7: Logika zapojení sady nodů pro řízení a zobrazování dat ze senzoru HC-SR505

Jazýčkový magnetický senzor otevření dveří MC-38 je ovládán primitivní skupinou nodů, která sestává z nodu reprezentující vstup pinu v GPIO hlavičce MC38, elementu virtuální LED diody DOOR LED a výpisu debuggeru. Při zavřeném stavu dveří je posílán nulový signál, který se mění po otevření na jedničkový. Tento signál je GPIO nodem posílán do nodu virtuální diody, která mění svou barvu podle přijatého signálu. GPIO node je podle návrhu namapován na pin GPIO22.



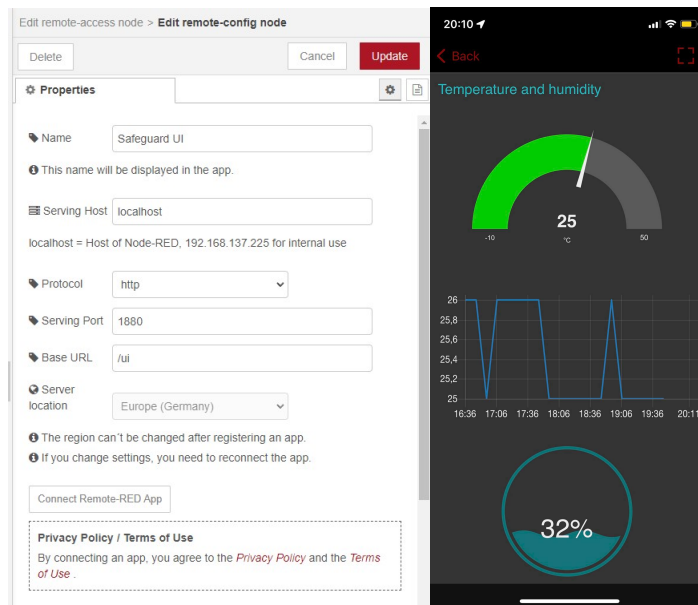
Obrázek 5.8: Logika zapojení sady nodů pro řízení a zobrazování dat ze senzoru MC-38

Kamerový modul OV5647 je nastaven pro živé vysílání za použití dostupného software RPi Cam Web Interface. Tento program je nejdříve zapotřebí stáhnout z Github repozitáře (viz. [2]) a nainstalovat pomocí skriptu `install.sh`. Program se pak spouští skriptem `start.sh`, který se poté automaticky spouští se zapnutím počítače. Program vytvoří na adrese `X.X.X.X/html` lokálně hostovanou stránku (`X.X.X.X` je nutno nahradit IP adresou mikropočítače), kterou nadále zpracovávám v Node-RED rozhraní. Je nutné podotknout, že aby byl kamerový modul schopný operovat, je důležité ho povolit v záložce interface v nastavení počítače, které je dostupné skrze příkaz `sudo rpi-config`. Po povolení kamery v nastavení je nutné počítač restartovat. Takto vytvořená stránka je vsazena do zobrazovacího panelu pomocí nodu `iframe` z rozšíření `node-red-node-ui-iframe`. U takto vsazeného nodu do celkového flow diagramu je zapotřebí nastavení zdroje na adresu `X.X.X.X/html/min`, na které je dostupný námi hostovaný livestream v minimalistické verzi bez panelu nastavení.



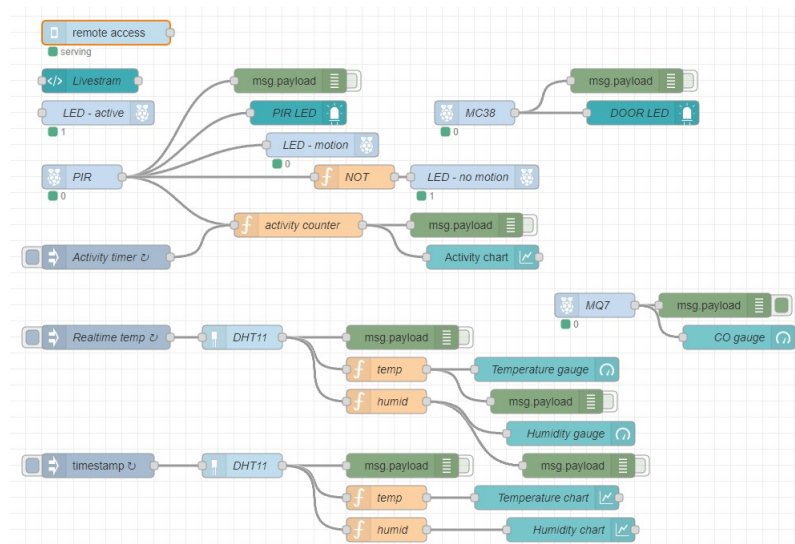
Obrázek 5.9: Vnořený livestream do zobrazovacího panelu

Finální zpřístupnění zobrazovacího panelu pro vzdálené zařízení mimo lokální síť je zprostředkováno použitím již zmíněného rozšíření `node-red-contrib-remote`. Toto rozšíření přidává do nástrojového panelu aplikace Node-RED nodu `remote access`, ve kterém probíhá pomocí naskenování QR kódu párování zobrazovacího panelu s aplikací staženou do telefonu. Aplikace používá pro stream panelu dva servery, které jsou umístěné v USA a Německu a lze si vybrat skrze který server data budou procházet. Nastavení samotného nodu je dostupné v záložce Properties, kde se nachází i tlačítko pro generování QR kódu a následné párování s mobilní aplikací.



Obrázek 5.10: Nastavení nodu s výsledným zobrazením v mobilní aplikaci na zařízení iOS

Takto sestavený flow diagram fungování jednotlivých součástí je schopný vyzobrazovat veškerá data skrze zobrazovací panel, který je generován na adrese X.X.X.X:1880/ui a lze ho navštívit jak z počítače, tak z mobilního zařízení ve stejné síti. Vzdálený přístup pak lze skrze mobilní aplikaci. Základ zobrazovacího panelu je generován za použití rozšíření `node-red-dashboard`, které dodává potřebné grafické elementy panelu. Celá struktura diagramu je uchováována ve formě json souboru, který umožňuje jednoduché sdílení a sestavení identických systémů na jiných zařízeních. Základní výbava Node-RED aplikace umožňuje i MQTT komunikaci, která je vhodná v případě sestavení více obdobných zařízení v jedné domácnosti.

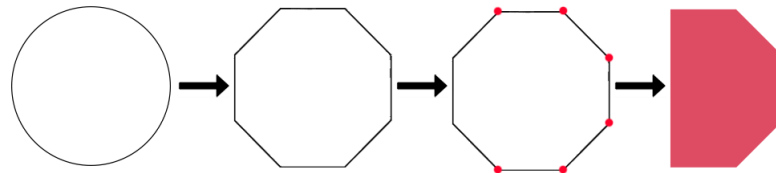


Obrázek 5.11: Komplettní, vytvořený flow diagram v aplikaci Node-RED

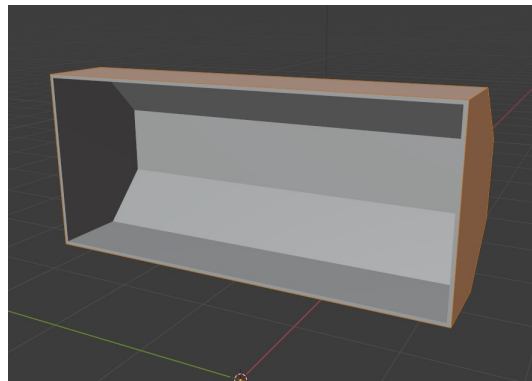
5.3 Vytvoření modelu obalu

K vytvoření modelu obalu, do kterého bude finální systém zasazen, jsem použil aplikaci Blender, která slouží k vytváření 3D modelů za použití specializovaných, virtuálních nástrojů. K dosažení rozměrů a tvarů, které byly vytvořeny již v dvojrozměrném grafickém návrhu, jsem postupoval následovně.

Jelikož z profilu je navrhnutý obal půlený, rovnostranný osmihran, tak k těmto rozměrům šlo dojít vytvořením půdorysu ve tvaru kružnice, jejíž vrcholy byly postupně redukovány na konečný počet 8 vrcholů. V takto vytvořeném půdorysu lze pak vybrat specifické vrcholy, a vytvořit novou plochu. Tato plocha reprezentuje tvar, který obal nabývá z profilu. Nastavením výšky modelu a odstraněním jedné stěny jsem následně z vytvořeného půdorysu vytvořil základní tvar celkového obalu, kterému bylo zbývalo jen nastavit tloušťku jednotlivých stěn a přidat otvory pro senzory zařízení.



Obrázek 5.12: Logika vytvoření půdorysu návrhu obalu



Obrázek 5.13: Vytvořený model v aplikaci Blender

Vytvořený model je uložen ve formátu STL, což je stereolitografický formát, který se používá pro tisk modelů na 3D tiskárnách. Model bylo ještě potřeba předimenzovat pro adekvátní velikost pro použití v praxi. Finální rozměry obalu jsou 49,44x157,67x69,9mm. Obal byl vytisknut za pomoci 3D tiskárny CREALITY Ender V2 a materiál použitý pro zhotovení byl běžně dostupný PLA filament, který je odolný a cenově dostupný. Otvory pro senzory byly ve finále dodatečně přidány mechanickou úpravou vytisknutého modelu.

Kapitola 6

Testování a naměřená data

V této kapitole se věnuji testování finálního, vytvořeného zařízení a vlastnostem a vzhledu dat, které během testování přístroj nasbíral.

6.1 Testování a úpravy

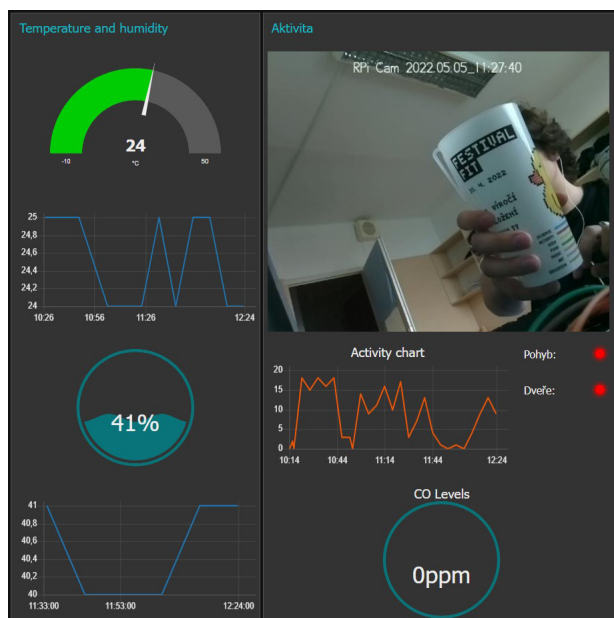
Všemu dalo základ klasické testování na pracovní ploše stolu, kde jsem ověřoval kvalitu zapojení a funkčnost všech zapojených senzorů. Po zapojení zařízení (viz. 5.3) jsem byl schopen okamžitého provozu za použití provizorního umístění. Takto zapojené zařízení jsem nechal v delším časovém pásmu běžet, abych ověřil konzistenci, stálost, validitu naměřených dat a jestli se s postupem času data nezkrusují nebo jestli součástky vydrží po tak dlouhou dobu fungovat bez zkratu či jiného problému. Výsledné testovací, časové segmenty proběhly bez problémů a já dospěl k závěru, že sestavené zařízení je vhodné pro nasazení a použití v terénu a na místech, kde byl původní návrh používaného umístění a snímat námi zvolené prostory po delší časové pásma bez hrozby disfunkce nebo naměření špatných nebo nepoužitelných dat.

Pro finální testovací lokalitu instalace mého zařízení jsem se rozhodl vybrat moji bytovou buňku na kolejičkách, která v moment testování představovala nejdostupnější prostory, kde zařízení testovat. Zařízení bylo umístěno nad dveřní prostory hlavní místnosti, kde jsem trávil se spolubydlícím nejvíce času a bylo to tak ideální místo pro generování a sběr většího objemu dat, které by se zobrazovaly na hlavním panelu. Celkové testování finálního produktu jak na místě nad dveřními prostory, tak na pracovní ploše stolu, probíhalo v delších časových segmentech z důvodu aspoň částečného naplnění kapacity zobrazovacích elementů a sběru esteticky přívětivějších dat.

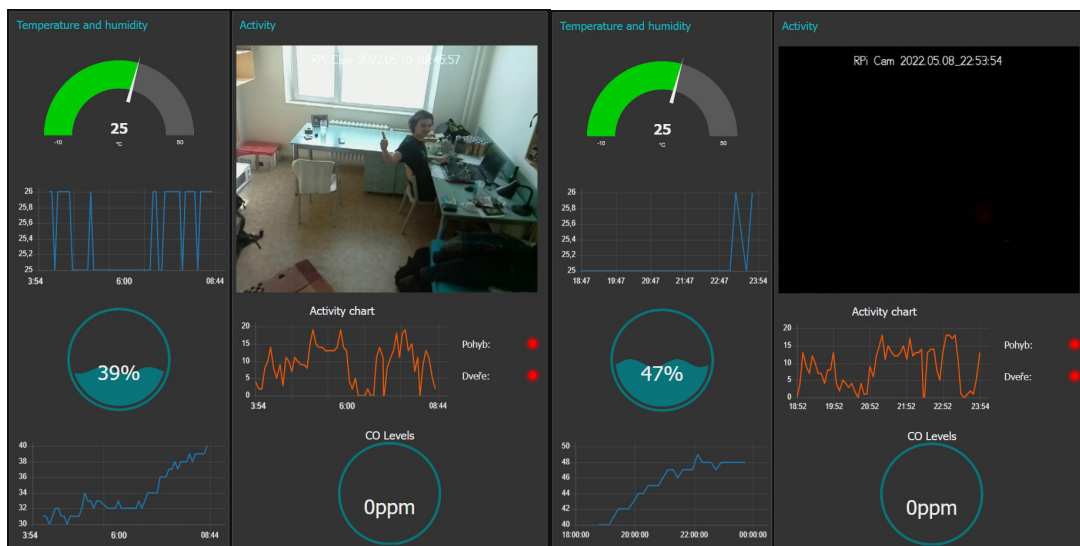
Během těchto segmentů se postupně ubírala moje pozornost na jednotlivé senzory a jejich fungování za delší dobu běhu. Na základě pozorování jsem uskutečnil i drobnější úpravy finálního zařízení jako je celkové rozpoložení senzorů v instalaci. Během prvotního testování docházelo ke zkreslování naměřených dat z důvodu navýšení teploty v okolí zařízení. Důvodem tohoto teplotního výkyvu byl kamerový modul a mikropočítač samotný. Změny, které byly následně uskutečněny vzdálily ostatní senzory od těchto zdrojů tepla a bylo přidáno pasivní, hliníkové chlazení, které bylo umístěno přímo na CPU a paměť RAM, které jsou přímo nad sebou a do obalu zařízení byly v horní části vytvořeny průduchy pro únik tepleho vzduchu ven. Tyto drobné úpravy ve výsledku omezily distribuci nadbytečného tepla a zabránily přehřívání zařízení a vybavených senzorů. Tento problém byl nejméně žádany u teplotního senzoru, který nabýval zkreslených hodnot.

6.2 Vzhled panelu a zobrazení dat

Jak již bylo zmíněno v návrhu a softwarové realizaci, naměřená data byla promítána na zobrazovací panel hostované stránky na lokální síti nebo skrze mobilní aplikaci ze vzdálené sítě. Následující příklady byly schválně vybrány pro zobrazení celkové rozmanitosti nasbíraných dat během testování sestaveného zařízení na různých místech a v jiné časové segmenty.



Obrázek 6.1: Úvodní testování s provizorním umístěním



Obrázek 6.2: Finální umístění testovaného zařízení s nasbíranými daty během dne a noci

Díky nastavení struktury panelu v aplikaci Node-RED, jsem docílil minimalistického uživatelského rozhraní, ve kterém byly nasbírané data přehledně prezentovány bez zbytečných komplikací a čtení v něm bylo intuitivní.

Díky běhu senzorů po delší časové segmenty během různých částí dne bylo možné krásné vyzobrazení pohybu jednotlivých hodnot jako je celková aktivita uvnitř prostor, teplota a vlhkost. Takto získané vývoje jednotlivých hodnot můžou dát za vznik dalších potencionálních úprav v domácnosti jako je dálkové ovládání a nastavení radiátorů s účelem šetření celkových nákladů nebo nastavení již umístěného alarmu, jehož stav se přizpůsobí míře naměřené normální aktivity během dne. Potenciál využití těchto dat je velice široký a dává uživateli velké množství možností jak s nimi ve výsledku naložit.

Kapitola 7

Závěr

Cílem této práce bylo vytvoření komplexního systému, který by pokrýval všechny důležité aspekty zabezpečení domácnosti dnešní doby. Finální produkt měl být vybaven širší škálou senzorů, které by tyto zabezpečovací činnosti plnily a hlídaly. Požadavkem na zařízení byla jeho nenáročnost na sestavení, což by ve finále způsobilo lehkou dostupnost širší veřejnosti. Zdrojové soubory a použitý software by byl volně dostupný a tím pádem by spadl do kategorie open-source.

Součástí této práce byl i detailnější pohled do obecné problematiky IoT sféry jako jsou reálná využití v dnešním světě, způsoby komunikace IoT zařízení a jejich ovládání a správa.

Nejdůležitější záměr této práce bylo vytvoření zařízení, které by ale ve finále spadalo do nízké cenové náročnosti na realizaci. Po nutné detailní analýze dostupných řešení a seznámením se s jejich způsoby zvládání této problematiky spolu s jejich celkovou vybaveností jsem byl schopen vytvořit návrh řešení, který by sestával z použitých hardwarových součástí a jejich zapojení tak, aby finální systém svými funkcemi konkuroval nabízeným komerčním řešením. Vybrané součástky byly zvoleny na základě recenzím jejich uživatelů a četnosti jejich použití v jiných projektech, které jsou dostupné online.

Finální kalkulace ceny celého projektu se pohybuje kolem 750,-Kč až 800,-Kč, což je ve finále pouhý zlomek ceny komerčních řešení, jejichž ceny se pohybují circa od 3.000,-Kč až po sumy jako 26.000,-Kč. Projekt takto splnil můj požadavek na cenovou nenáročnost a zachování všech důležitých funkcí, které jsou standardem zabezpečení domácnosti.

Cíl mé práce byl splněn a výsledkem bylo vytvoření komplexního, byť lehce sestavitelného systému, který by byl schopen samostatného fungování a generování dat, které by uživateli byly dostupné skrze zobrazovací panel. Takto sestavený systém by neodrazoval veřejnost svou cenovou náročností, neboť použité součástky na jeho realizaci jsou velmi cenově dostupné.

Jsem velmi rád, že finální zařízení má v reálném životě velmi praktické využití a podle odezvy z okolí to je elegantní a jednoduché řešení, které přesto zvládá vícero užitečných funkcí najednou.

Literatura

- [1] Akustický bzučák. *Dratek.cz* [online]. Dratek.cz [cit. 2022-5-03]. Dostupné z: <https://dratek.cz/arduino/849-eses-akusticky-bzucak-pro-jednodeskove-pocitace.html>. Path: Domů; Akustický bzučák.
- [2] *RPi-Cam-Web-Interface* [online]. Github [cit. 2022-5-03]. Dostupné z: https://github.com/silvanmelchior/RPi_Cam_Web_Interface.
- [3] ALEXANDER S. GILLIS. What is the internet of things (IoT)? *TechTarget* [online]. TechTarget, 1. března 2022. 2022-3-01 [cit. 2022-5-03]. Dostupné z: <https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT>. Path: Domů; What is the internet of things (IoT)?
- [4] ALZA. Ajax Set Můj dům, můj hrad. *Alza* [online]. Alza [cit. 2022-5-03]. Dostupné z: https://www.alza.cz//bedo-ajax-set-muj-dum-muj-hrad-cerna-d6103529.htm?kampan=adw4_smart_pla_all_obecna-css_smart-home_c_9062809__Bdo_m20v_008_413605341827_-94081209529-#fotovideo. Path: Domů; Ajax Set Můj dům, můj hrad.
- [5] BANGGOOD. Mikrofonní vysílač. *Banggood* [online]. Banggood [cit. 2022-5-03]. Dostupné z: https://www.banggood.com/cs/KY-037-4pin-Voice-Sound-Detection-Sensor-Module-Microphone-Transmitter-Smart-Robot-Car-p-1392070.html?cur_warehouse=CN. Path: Domů; Mikrofonní vysílač.
- [6] CORINNE BERNSTEIN, KATE BRUSH, ALEXANDER S. GILLIS. MQTT (MQ Telemetry Transport). *TechTarget* [online]. TechTarget, 1. ledna 2021. 2021-1-01 [cit. 2022-5-03]. Dostupné z: <https://www.techtarget.com/iotagenda/definition/MQTT-MQ-Telemetry-Transport>. Path: Domů; MQTT (MQ Telemetry Transport).
- [7] DRATEK.CZ. PIR senzor pohybu HC-SR505. *Dratek.cz* [online]. Dratek.cz [cit. 2022-5-03]. Dostupné z: <https://dratek.cz/arduino/7821-pir-senzor-pohybu-hc-sr505.html>. Path: Domů; PIR senzor pohybu HC-SR505.
- [8] DRATEK.CZ. Kamerový Modul Raspberry Pi OV5647. *Dratek.cz* [online]. Dratek.cz [cit. 2022-5-03]. Dostupné z: <https://dratek.cz/arduino/1556-kamerovy-modul-raspberry-pi-ov5647-w-1080p30-2592x1944px.html>. Path: Domů; Kamerový Modul Raspberry Pi OV5647.

- [9] DRATEK.CZ. MQ7 MQ-7 senzor oxidu uhelnatého CO. *Dratek.cz* [online]. Dratek.cz [cit. 2022-5-03]. Dostupné z: <https://dratek.cz/arduino/48468-mq7-mq-7-senzor-oxidu-uhelnateho-co.html>. Path: Domů; MQ7 MQ-7 senzor oxidu uhelnatého CO.
- [10] DRATEK.CZ. Jazýčkový magnetický kontakt. *Dratek.cz* [online]. Dratek.cz [cit. 2022-5-03]. Dostupné z: <https://dratek.cz/arduino/7700-jazyckovy-magneticky-kontakt.html>. Path: Domů; Jazýčkový magnetický kontakt.
- [11] DRATEK.CZ. DHT11 teploměr a vlhkoměr digitální. *Dratek.cz* [online]. Dratek.cz [cit. 2022-5-03]. Dostupné z: <https://dratek.cz/arduino/829-dht11-teplomer-a-vlhkomer-digitalni.html>. Path: Domů; DHT11 teploměr a vlhkoměr digitální.
- [12] ELECTRONIC, G. Vývojový kit Raspberry Pi Zero WH. *GM Electronic* [online]. GM Electronic [cit. 2022-5-03]. Dostupné z: <https://www.gme.cz/raspberry-pi-zero-wh>. Path: Domů; Vývojový kit Raspberry Pi Zero WH.
- [13] HASIČSKÝ SBOR MĚSTA PRAHY. *Ročenka 2020* [online]. Ministerstvo vnitra-generální ředitelství Hasičského záchranného sboru České republiky, 2021 [cit. 2022-5-03]. Dostupné z: <https://www.hzscr.cz/soubor/rocenka-2020-pdf.aspx>.
- [14] HASIČSKÝ ZÁCHRANNÝ SBOR ČESKÉ REPUBLIKY. *Statistika za rok 2020* [online]. Ministerstvo vnitra-generální ředitelství Hasičského záchranného sboru České republiky, 2021 [cit. 2022-5-03]. Dostupné z: <https://www.hzscr.cz/soubor/statistika-za-rok-2020-pdf.aspx>.
- [15] JSHOP. Bezdrátový GSM a WIFI alarm BENTECH WF40C. *JShop* [online]. JShop [cit. 2022-5-03]. Dostupné z: <https://www.jshop.cz/gsm-alarmy/bezdratovy-gsm-a-wifi-alarm-bentech-wf40c>. Path: Domů; Bezdrátový GSM a WIFI alarm BENTECH WF40C.
- [16] KATEŘINA TŮMOVÁ. Počet krádeží vloupáním už zase roste, důležitá je prevence. *TZB-info* [online]. TZB-info, 1. srpna 2021. 2021-8-01 [cit. 2022-5-03]. Dostupné z: <https://www.tzb-info.cz/bezpecnost/22631-pocet-kradezi-vloupanim-uz-zase-roste-dulezita-je-prevence>. Path: Domů; Počet krádeží vloupáním už zase roste, důležitá je prevence.
- [17] LINDA ROSENCRANCE. Zigbee. *TechTarget* [online]. TechTarget, 1. června 2017. 2017-6-01 [cit. 2022-5-03]. Dostupné z: <https://www.techtarget.com/iotagenda/definition/ZigBee>. Path: Domů; Zigbee.
- [18] LISA PHIFER. Bluetooth Low Energy (Bluetooth LE). *TechTarget* [online]. TechTarget, 1. listopadu 2014. 2014-11-01 [cit. 2022-5-03]. Dostupné z: <https://www.techtarget.com/iotagenda/definition/Bluetooth-Low-Energy-Bluetooth-LE>. Path: Domů; Bluetooth Low Energy (Bluetooth LE).
- [19] POHONY, A. TUYA WIFI GSM CHYTRÝ BEZPEČNOSTNÍ ALARM. *AZ pohony* [online]. AZ pohony [cit. 2022-5-03]. Dostupné z: <https://www.azpohony.cz/tuya-wifi-gsm-chytry-bezpecnostni-alarm/p69662?v=>

69663&utm_source=google&utm_medium=gmc. Path: Domů; TUYA WIFI GSM CHYTRÝ BEZPEČNOSTNÍ ALARM.

- [20] PRAKASH, A. Raspberry Pi Zero W Specs, Features and More. *It's FOSS, Raspberry Pi Zero W Specs, Features and More* [online]. It's Foss [cit. 2022-5-03]. Dostupné z: <https://itsfoss.com/raspberry-pi-zero-w/>. Path: Domů; Raspberry Pi Zero W Specs, Features and More.
- [21] REMOTE RED. *Remote-RED* [online]. Remote-RED, 2022. 2022-1-01 [cit. 2022-5-03]. Dostupné z: <https://www.remote-red.com/en/home-en/>.
- [22] SOFTWARETESTING CONTRIBUTORS. 10 Powerful Internet Of Things (IoT) Examples Of 2022. *SOFTWARETESTING* [online], 4. dubna 2022. 2022-4-04 [cit. 2022-5-03]. Dostupné z: <https://www.softwaretestinghelp.com/best-iot-examples/>. Path: Domů; 10 Powerful Internet Of Things (IoT) Examples Of 2022.
- [23] TECHTARGET CONTRIBUTOR. Bluetooth. *TechTarget* [online]. TechTarget, 1. října 2021. 2021-10-01 [cit. 2022-5-03]. Dostupné z: <https://www.techtarget.com/searchmobilecomputing/definition/Bluetooth>. Path: Domů; Bluetooth.
- [24] TIPA. Detector - magnetic contact MC-38. *Tipa.eu* [online]. Tipa [cit. 2022-5-03]. Dostupné z: <https://www.tipa.eu/en/detector-magnetic-contact-mc-38/d-221119/>. Path: Domů; Detector - magnetic contact MC-38.
- [25] WIKIPEDIA CONTRIBUTORS. *Home Assistant* — *Wikipedia, The Free Encyclopedia*. 2022. [Online; accessed 3-May-2022]. Dostupné z: https://en.wikipedia.org/w/index.php?title=Home_Assistant&oldid=1084086931.
- [26] WIKIPEDIA CONTRIBUTORS. *Internet of things* — *Wikipedia, The Free Encyclopedia*. 2022. [Online; accessed 3-May-2022]. Dostupné z: https://en.wikipedia.org/w/index.php?title=Internet_of_things&oldid=1085510691.
- [27] WIKIPEDIA CONTRIBUTORS. *Node-RED* — *Wikipedia, The Free Encyclopedia*. 2022. [Online; accessed 3-May-2022]. Dostupné z: <https://en.wikipedia.org/w/index.php?title=Node-RED&oldid=1075876437>.
- [28] WIKIPEDIA CONTRIBUTORS. *Smoke detector* — *Wikipedia, The Free Encyclopedia*. 2022. [Online; accessed 9-May-2022]. Dostupné z: https://en.wikipedia.org/w/index.php?title=Smoke_detector&oldid=1084500191.
- [29] WIKIPEDIA CONTRIBUTORS. *Wi-Fi* — *Wikipedia, The Free Encyclopedia*. 2022. [Online; accessed 3-May-2022]. Dostupné z: <https://en.wikipedia.org/w/index.php?title=Wi-Fi&oldid=1085017739>.

Přílohy

Seznam příloh

A Obsah přiloženého paměťového média

49

Příloha A

Obsah přiloženého paměťového média

Images Důležité obrázky k zobrazení ve větší kvalitě

Node-RED Adresář s .json souborem, který slouží k vytvoření finálního Node-RED diagramu

RPi_Cam_Web_Interface-master.zip Zip soubor s programem pro vytvoření živého vysílání.

3D Adresář s 3D modelem pouzdra, který je určen k tištění na 3D tiskárně.