

Diplomová práce



České vysoké učení technické v Praze

Fakulta elektrotechnická

Katedra mikroelektroniky

**Model systému pro řízení a zpracování dat  
jednoduchého elektronického zabezpečení  
rodinného domu**

*Bc. Jan Kočí*

Studijní program: Elektronika a komunikace

Vedoucí práce: prof. Ing. Miroslav Husák, CSc.

Květen 2022



## I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: Kočí Jméno: Jan Osobní číslo: 466179  
Fakulta/ústav: Fakulta elektrotechnická  
Zadávající katedra/ústav: Katedra mikroelektroniky  
Studijní program: Elektronika a komunikace  
Specializace: Elektronika

## II. ÚDAJE K DIPLOMOVÉ PRÁCI

Název diplomové práce:

Model systému pro řízení a zpracování dat jednoduchého elektronického zabezpečení rodinného domu

Název diplomové práce anglicky:

Model of a System for Control and Data Processing of a Simple Electronic Security of a Family House

Pokyny pro vypracování:

1. Proveďte rešerši současného stavu řešení elektronických zabezpečení (EZS) rodinných domů, zaměřte se zejména na způsoby řízení EZS, zpracování a ukládání dat, řízení činnosti senzorů a aktuátorů, využití v IoT aplikacích.
2. Navrhněte model systému pro řízení a zpracování dat jednoduchého elektronického zabezpečení rodinného domu řízeného vhodným typem mikroprocesoru. Pozornost věnujte řízení činnosti vybraných zabezpečovacích senzorů, senzorů teploty, kouře, úniku plynu, popř. senzory kvality vzduchu uvnitř chráněného prostoru a též řízení výstupů (akustický a optický). Zpracujte způsob předávání získaných dat vhodným komunikačním standardem a jejich ukládání. Navrhněte možnost řešení pro IoT aplikaci.
3. Zjistěte parametry navrženého systému a porovnejte s parametry komerčních systémů.
4. Proveďte ekonomickou úvahu pro výrobu navrženého systému.

Seznam doporučené literatury:

- [1] STM32 Nucleo Boards [online]. STMicroelectronics, c2022 [cit. 2022-02-01].
- [2] Development Boards [online]. ESPRESSIF SYSTEMS (SHANGHAI) CO., c2022 [cit. 2022-02-01].
- [3] Arduino IDE [online]. Arduino, c2022 [cit. 2022-02-01]. Dostupné z: <https://www.arduino.cc/en/software>
- [4] IoT Device Development. Arm MBED [online]. c2022, <https://www.mbed.com/en/>

Jméno a pracoviště vedoucí(ho) diplomové práce:

prof. Ing. Miroslav Husák, CSc. katedra mikroelektroniky FEL

Jméno a pracoviště druhé(ho) vedoucí(ho) nebo konzultanta(ky) diplomové práce:

Datum zadání diplomové práce: 03.02.2022 Termín odevzdání diplomové práce: 20.05.2022

Platnost zadání diplomové práce: 30.09.2023

prof. Ing. Miroslav Husák, CSc.  
podpis vedoucí(ho) práce

prof. Ing. Pavel Hazdra, CSc.  
podpis vedoucí(ho) ústavu/katedry

prof. Mgr. Petr Páta, Ph.D.  
podpis děkana(ky)

## III. PŘEVZETÍ ZADÁNÍ

Diplomant bere na vědomí, že je povinen vypracovat diplomovou práci samostatně, bez cizí pomoci, s výjimkou poskytnutých konzultací. Seznam použité literatury, jiných pramenů a jmen konzultantů je třeba uvést v diplomové práci.

\_\_\_\_\_  
Datum převzetí zadání

\_\_\_\_\_  
Podpis studenta



## **Prohlášení**

Prohlašuji, že jsem předloženou práci vypracoval samostatně a že jsem uvedl veškeré použité informační zdroje v souladu s Metodickým pokynem o dodržování etických principů při přípravě vysokoškolských závěrečných prací.

V Praze dne .....

.....

## **Poděkování**

V první řadě bych chtěl poděkovat vedoucímu této práce prof. Ing. Miroslavu Husákovi, CSc. za ochotu, čas a obecně za veškerou spolupráci v rámci tvorby této práce. Dále bych chtěl poděkovat rodině a přítelkyni za podporu v průběhu celého studia.

## Abstrakt

Tato práce se zabývá návrhem modelu pro řízení a zpracování dat jednoduchého elektronického zabezpečení (EZS) rodinného domu. Jednotlivé části systému jsem nejdříve realizoval na nepájivých polích a po vytvoření a odzkoušení kódu také na univerzálních jednovrstvých deskách plošných spojů. Tyto desky jsou základem všech vytvořených modulů. Navržený EZS jsem následně instaloval do modelu rodinného domu, kde jsem systém dále testoval. Vytvořený EZS se skládá ze čtyř typů modulů a dohromady ze sedmi kusů modulů. Hlavní funkcí prvních dvou typů modulů je měření dat a jejich předávání ústředně. Další typ modulu představuje centrální řídicí jednotka neboli ústředna. Poslední typ modulu disponuje dotykovým displejem a slouží k autorizaci uživatele a jako přístupový bod systému. Ústředna komunikuje s moduly bezdrátově a samotná komunikace je založena na TCP/IP protokolu. Ústředna dále přes domácí Wi-Fi síť ukládá vybraná data na cloud. K datům uloženým na cloudu je možné přistupovat prostřednictvím webového nebo mobilního rozhraní. Součástí ústředny je GSM modul, který ústředně umožňuje informovat uživatele o vybraných stavech formou SMS. Všechny moduly jsou napájeny z elektrické sítě a zároveň disponují záložním napájením. Při výpadku energie z elektrické sítě se napájení automaticky přepne na záložní baterii. Důraz je kladen na spolehlivost systému a minimalizování falešných poplachů i při použití neprofesionálních senzorů. Dále došlo k ověření funkčnosti vytvořeného systému a změření jeho parametrů. Nejen na jejich základě jsem systém porovnal s komerčními systémy. Na závěr jsem provedl ekonomickou úvahu pro výrobu navrženého systému. Práce může sloužit jako zdroj inspirace při návrhu a výrobě domácího elektronického zabezpečení bytu nebo rodinného domu.

**Klíčová slova:** elektronické zabezpečení domácnosti; esp32; TCP/IP protokol; Blynk cloud

## **Abstract**

The aim of this work is to design a model for data management and processing of simple electronic security system of a family house. I first implemented the individual parts of the system on non-solderable fields and, after creating and testing the code, also on universal single-layer printed circuit boards. These boards are the basis of all the modules I have created. Afterwards, I installed the designed burglar alarm in a family house model, where I further tested the system. The created burglar alarm consists of four types of modules and a total of seven modules. The main function of the first two types of modules is data measurement and transmission to the control panel. Another type of modules is a control panel. The last type of modules has a touch screen and serve to authorize the user and as an access point to the system. The control panel communicates with the modules wirelessly and the communication itself is based on the TCP/IP protocol. The control panel also stores selected data on the cloud via the home Wi-Fi network. Data stored on the cloud can be accessed via a web or mobile interface. The control panel includes a GSM module that allows users to be informed about selected statuses via SMS. All modules are powered from the mains and also have a backup power supply. In the event of a power failure, the power supply automatically switches to the backup battery. Emphasis is placed on system reliability and minimizing false alarms even when using non-professional sensors. The functionality of the created system was verified and its parameters were measured. Not only on the basis of measured parameters, I compared the system with commercial systems. Finally, I made an economic consideration for the production of the proposed system. The work can serve as a source of inspiration in the design and manufacture of home electronic security of an apartment or family house.

**Keywords:** electronic home security; esp32; TCP/IP protocol; Blynk cloud



# Obsah

1	Úvod.....	1
2	Stanovení cílů práce .....	2
3	Teoretická část.....	3
3.1	Zabezpečovací systémy .....	3
3.2	Senzory EZS .....	3
3.2.1	Plášťová ochrana .....	3
3.2.2	Prostorová ochrana .....	4
3.3	Ústředny.....	6
3.3.1	Smyčkové ústředny .....	6
3.3.2	Ústředny s přímou adresací senzorů.....	7
3.3.3	Ústředny smíšeného typu .....	7
3.3.4	Bezdrátové ústředny .....	8
3.4	Mikrokontroléry esp32 .....	9
3.4.1	Možnosti nastavení Wi-Fi sítě.....	9
3.4.2	Režimy spánku .....	10
4	Návrh modelu systému pro elektronické zabezpečení rodinného domu.....	12
4.1	Navržený model.....	12
4.2	Realizovaný model .....	13
4.3	Použitý mikrokontrolér.....	15
4.4	Komunikace v rámci systému.....	17
4.5	Ústředna jako server .....	17
4.6	Komunikace mezi ústřednou a klienty .....	18
4.7	Blynk cloud.....	20
5	Vytvořené moduly a jejich role v systému.....	22
5.1	Napájení.....	22
5.2	Modul typu 1 .....	25
5.2.1	Zapojení.....	26
5.2.2	Program .....	29
5.3	Modul typu 2 .....	34
5.3.1	Zapojení.....	34
5.3.2	Program .....	35
5.4	Modul s displejem .....	37

5.4.1	Zapojení.....	37
5.4.2	Program .....	38
5.5	Ústředna.....	42
5.5.1	Schéma .....	42
5.5.2	Stavy systému.....	43
5.5.3	Program .....	44
6	Parametry navrženého systému.....	50
6.1	Ověření funkčnosti zálohy napájení .....	50
6.2	Ověření procesu znovu připojení na Wi-Fi .....	50
6.3	Výdrž ústředny na záložním napájení .....	51
6.4	Nabití baterie záložního napájení .....	52
6.5	Ověření fungování systému .....	52
6.6	Porovnání s komerčními systémy.....	53
7	Ekonomická úvaha .....	55
8	Závěr.....	57
9	Seznam literatury.....	59

## Obrázky

Obr. 3.1 SA-201-A Kontakt magnetický mini povrchový s vodičem (převzato z [56]).....	4
Obr. 3.2 GBS-210 Detektor rozbití skla (převzato z [55]).....	4
Obr. 3.3 Sběrníkový PIR detektor pohybu (převzato z [58]) .....	5
Obr. 3.4 Bezdrátový duální PIR a MW detektor pohybu (převzato z [57]).....	5
Obr. 3.5 Sběrníkový PIR detektor pohybu s kamerou (převzato z [59]).....	5
Obr. 3.6 Schéma smyčkové ústředny .....	6
Obr. 3.7 Schéma ústředny s přímou adresací .....	7
Obr. 3.8 Schéma ústředny smíšeného typu .....	7
Obr. 3.9 Schéma bezdrátové ústředny.....	8
Obr. 3.10 Základní Wi-Fi módy (převzato z [7]).....	9
Obr. 3.11 Vnitřní blokové rozdělení mikrokontroléru esp32 (převzato z [17]).....	10
Obr. 3.12 Light režim spánku (upraveno z [17]).....	11
Obr. 4.1 Schéma objektu určeného k zabezpečení.....	12
Obr. 4.2 Schéma objektu s navrženým zabezpečením .....	13
Obr. 4.3 Schéma realizovaného chráněného objektu .....	14
Obr. 4.4 Realizovaný chráněný objekt spolu s moduly.....	15
Obr. 4.5 Mikrokontrolér ESP-WROOM-32 (převzato z [12]).....	16
Obr. 4.6 Topologie komunikační sítě (upraveno z [7]).....	16
Obr. 4.7 Ukázka komunikace mezi ústřednou a klientem.....	18
Obr. 4.8 Ukázka grafu z webového rozhraní aplikace Blynk .....	20
Obr. 4.9 Mobilní aplikace Blynk IoT .....	21
Obr. 5.1 Schéma napájení klientů .....	22
Obr. 5.2 Schéma napájení ústředny.....	23
Obr. 5.3 Nabíječka Li-Ion článku TP4056 s ochranou (převzato z [24]).....	24
Obr. 5.4 Step-up měnič s MT3608 (převzato z [23]) .....	24
Obr. 5.5 Automatický přepínač baterie (převzato z [25]) .....	24
Obr. 5.6 Bloky napájení .....	25
Obr. 5.7 Realizovaný modul typu 1 .....	25
Obr. 5.8 Schéma zapojení klientů 1-4 .....	26
Obr. 5.9 Modul se senzorem MQ-135 (převzato z [29]).....	27
Obr. 5.10 Senzor teploty a vlhkosti vzduchu SHT30 (převzato z [30]).....	27
Obr. 5.11 Převodník logických úrovní 5V/3V(převzato z [28]) .....	28
Obr. 5.12 Schéma převodníku logických úrovní 5 V a 3,3 V .....	28
Obr. 5.13 Piezobzučák .....	28
Obr. 5.14 Detektor pohybu, PIR NC-SR501 (převzato z [26]).....	29
Obr. 5.15 Displej OLED 0,96“.....	29
Obr. 5.16 Zobrazení veličin na displeji .....	29
Obr. 5.17 Odpočet na displeji při inicializaci PIR detektoru .....	29
Obr. 5.18 Zobrazení varování na displeji .....	29
Obr. 5.19 Vývojový diagram programu modulu typu 1 .....	30
Obr. 5.20 Schéma zapojení klienta 5.....	33
Obr. 5.21 Realizovaný modul typu 2 .....	33

Obr. 5.22	Senzor vodní hladiny (převzato z [40]).....	34
Obr. 5.23	Dotykový senzor .....	34
Obr. 5.24	Vývojový diagram programu modulu typu 2.....	35
Obr. 5.25	Schéma zapojení klienta 6.....	37
Obr. 5.26	Pohled shora na klienta 6 .....	37
Obr. 5.27	Vývojový diagram programu modulu s displejem.....	38
Obr. 5.28	Kalibrace displeje.....	39
Obr. 5.29	Úspěšné připojení na server .....	40
Obr. 5.30	Neúspěšné připojení na server .....	40
Obr. 5.31	Seznam možností .....	40
Obr. 5.32	Změna hesla .....	40
Obr. 5.33	Vypnutí MQ alarmu .....	40
Obr. 5.34	MQ alarm je vypnutý .....	40
Obr. 5.35	Zapnutí zabezpečení umožněno .....	41
Obr. 5.36	Zapnutí zabezpečení neumožněno .....	41
Obr. 5.37	Schéma zapojení ústředny.....	42
Obr. 5.38	Realizovaný modul – ústředna .....	43
Obr. 5.39	Stavy systému a přechody mezi nimi.....	44
Obr. 5.40	Vývojový diagram programu ústředny .....	47
Obr. 6.1	Testování funkčnosti zálohy napájení.....	50
Obr. 6.2	Testování funkčnosti znovu připojení k Wi-Fi .....	51
Obr. 6.3	Doba výdrže ústředny na záložním napájení .....	51
Obr. 6.4	Nabití baterie záložního napájení.....	52
Obr. 6.5	Průběh teploty v ložnici za 22 dní.....	52
Obr. 6.6	Průběh relativní vlhkosti v ložnici za 22 dní.....	53

# 1 Úvod

Chytrá domácnost a elektronické zabezpečení domácnosti je díky technologickému pokroku čím dál dostupnější. Jedna z možností jak realizovat elektronický zabezpečovací systém (dále jen EZS) je vlastními silami. V takovém případě může být pořizovací cena EZS menší, než při využití profesionálních produktů. Tato skutečnost ovšem není zaručena. Navíc má tento způsob mnoho nevýhod a především rizik spojených s nedostatečnou znalostí dané problematiky. Motivace pro tvorbu této práce je právě vytvoření systému vlastními silami, který zahrnuje prvky EZS a také znaky chytré domácnosti. Použití neprofesionálních senzorů je cenově příznivé, ale vyžaduje různé kontroly pro předcházení výskytu falešných poplachů. Důraz je kladen na minimalizování falešných poplachů a hlavně na spolehlivost systému. Vytvořeným systémem by se dalo inspirovat a jeho základ dále rozšiřovat.

V teoretické části je nastíněna komplexnost návrhu zabezpečovacích systémů. Předmětem této části je primárně seznámení s EZS, jelikož právě návrh modelu EZS je hlavní náplní této práce. Součástí je také popis plášťové a prostorové ochrany, přičemž jako příklad jsou ukázány profesionální senzory firmy Jablotron. Následuje charakteristika centrální řídicí jednotky neboli ústředny. Ústředna představuje klíčovou komponentu každého EZS. Podle způsobu komunikace s prvky systému se ústředny dělí do několika typů, které mají svoje výhody a nevýhody. Závěr teoretické části se věnuje mikrokontroléru esp32 a to konkrétně způsobu použití Wi-Fi a režimům spánku. Důvodem je použití mikrokontroléru esp32 jako řídicí jednotky každého vytvořeného modulu.

Praktická část začíná definováním samotného objektu rodinného domu, do kterého je EZS navrhován. Následuje návrh modelu systému EZS, popis navrženého řešení a jeho realizace. Jednotlivé části systému jsem nejdříve realizoval na nepájivých polích a po vytvoření a odzkoušení kódu také na univerzálních jednovrstvých deskách plošných spojů, které jsou základem všech vytvořených modulů. Vytvořený EZS se skládá ze čtyř typů modulů a dohromady ze sedmi kusů modulů. V dalších částech probírané kapitoly je popis fungování celého systému, což primárně zahrnuje komunikaci mezi moduly. Ústředna komunikuje s ostatními prvky systému a zároveň přes domácí Wi-Fi síť ukládá data na Blynk cloud. Pomocí této aplikaci je vytvořeno webové a mobilní rozhraní pro zobrazení ukládaných dat. Komunikace s prvky systému je bezdrátová a je založena na TCP/IP protokolu.

Druhá kapitola praktické části zahrnuje detailní popis jednotlivých modulů. Všechny moduly jsou napájeny z elektrické sítě a zároveň disponují záložním napájením. Při výpadku energie z elektrické sítě se napájení automaticky přepne na záložní baterii. První část této kapitoly je věnována právě návrhu záložního napájení. Následuje podrobný popis jednotlivých modulů z hlediska zapojení a řídicího programu.

Navržený EZS jsem instaloval do vytvořeného modelu rodinného domu, kde jsem systém testoval. Ověřil jsem funkčnost vytvořeného systému a změřil některé jeho parametry. Nejen na jejich základě jsem systém porovnal s komerčními systémy. Na závěr jsem provedl ekonomickou úvahu pro výrobu navrženého systému.

## 2 Stanovení cílů práce

Cílem práce je navrhnout model pro řízení a zpracování dat jednoduchého EZS rodinného domu. Vytvořený systém by měl být složen z neprofesionálních prvků, což zajistí nižší cenu výsledného systému. Na druhou stranu je potřeba klást důraz na spolehlivost systému a minimalizování falešných poplachů. V rámci EZS se bude řešit pouze plášťová a prostorová ochrana. Kromě těchto prvků bude systém obsahovat komponenty pro měření teploty, relativní vlhkosti a kvality ovzduší. Kvalitu ovzduší měří tzv. senzory prostředí a lze pomocí nich detekovat nebezpečné plyny nebo kouř. Pro takové případy bude systém obsahovat signalizaci (např. akustickou), která se v případě naměření nebezpečné kvality ovzduší aktivuje. Součástí vybraných modulů by také mohl být displej pro zobrazení lokálně naměřených veličin.

Mezi další cíle patří bezdrátová komunikace s ústřednou a ukládání vybraných dat na cloud. Dále je vhodné zajistit přístup k těmto datům prostřednictvím mobilního nebo webového rozhraní, případně by skrz tyto rozhraní měl uživatel možnost ovládat systém vzdáleně. Informování uživatele bude zajištěno také formou SMS. Cílem je také vytvořit modul, který bude sloužit pro autorizaci a jako přístupový bod pro řízení systému. Ovládání tohoto modulu by mělo být ideálně s využitím dotykového displeje. Napájení prvků systému bude z elektrické sítě a zároveň zálohované baterií. Doba, kterou systém vydrží na záložním napájení, by měla být podobná jako je u komerčních systémů. Vytvořený systém je nezbytné otestovat a to alespoň v řádu dvou týdnů. Mezi další cíle tedy patří postavit model rodinného domu, do kterého se systém nainstaluje a dále otestuje. Systém by měl být sám schopen reagovat na události jako je výpadek energie z elektrické sítě či výpadek domácí Wi-Fi.

# 3 Teoretická část

## 3.1 Zabezpečovací systémy

Zabezpečovací systém obecně je komplexní systém, který zahrnuje:

- Mechanické zabezpečovací systémy (MZS): Účelem MZS je ztížit vniknutí do chráněného objektu. Nicméně každý MZS je překonatelný, tedy proniknutí skrz něj je pouze otázkou času. Cílem MZS je tento čas co nejvíce prodloužit.
- Elektronické zabezpečovací systémy (EZS): Součástí EZS je několik druhů ochrany: perimetrická (okolí domu), plášťová (místa proniknutí do chráněného objektu), prostorová (vnitřek objektu) a předmětová (ochrana konkrétních předmětů).
- Elektronické zabezpečovací systémy (EPS): Souhrn organizačních, stavebních a technických opatření vedoucích k zabránění vzniku požáru a k zamezení šíření požáru, pokud již vznikne.
- Přístupové systémy (ACS): Souhrn opatření k zajištění řízení (popř. evidence) přístupu do chráněného objektu na základě předem přidělených přístupových práv.
- Systémy průmyslové televize (CCTV)
- Legislativu, ...

## 3.2 Senzory EZS

Klíčovou část této práce tvoří vytvoření modelu EZS. V následujících kapitolách si ukážeme, jaké lze při návrhu modelu EZS použít senzory. Na ukázkou budou přidány obrázky reálných profesionálních senzorů firmy Jablotron (viz katalog produktů v [46]).

### 3.2.1 Plášťová ochrana

Plášťová ochrana představuje tzv. 2. linii ochrany EZS (1.linií tvoří perimetrická ochrana). Základní funkce této ochrany je zabezpečení míst pláště chráněného objektu proti vniknutí. Do určité míry plášťová ochrana funguje i preventivně, jelikož pokud jsou její části vidět, pak mohou mít odstrašující efekt. Cílem tedy je vyhlásit poplach co nejdříve po proniknutí do chráněného objektu a tím minimalizovat možné škody. Mezi základní zástupce senzorů plášťové ochrany patří magnetické kontakty (viz obr. 3.1) a senzory pro ochranu skleněných ploch (viz obr. 3.2). [52]

#### Magnetické kontakty

Magnetický kontakt se skládá z jazýčkového kontaktu (část s vodiči) a permanentního magnetu (viz obr. 3.1). Jazýčkový kontakt je tvořen zatavenou skleněnou trubičkou zpravidla naplněnou ochrannou atmosférou obsahující dva feromagnetické kontakty. Permanentní magnet bývá tvořen z feritu. Obě části jsou zapouzdřeny v krytu z nemagnetického materiálu, záleží na tom, zda je kontakt montován povrchově či skrytě (typicky do oken či dveří). Funkce magnetického kontaktu je jednoduchá. V případě, kdy se část s magnetem oddálí od

druhé části, feromagnetické kontakty se rozpojí. Tím dojde k přerušení smyčky, ve které je kontakt zapojen, což detekuje ústředna. [46] [52]

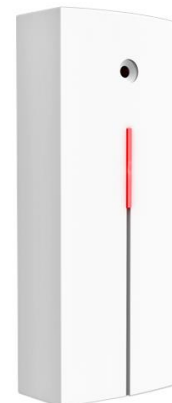
### **Senzory pro ochranu skleněných ploch**

Senzory pro ochranu skleněných ploch jsou založeny na několika různých principech. Dříve se používal senzor monitorující vlnění skla, který rozpoznal vlnění šířící se sklem při jeho rozbití. Tento způsob je však ekonomicky nákladný, proto se v dnešní době nepoužívá. Další typ senzorů pro ochranu skleněných ploch je založen na akustickém principu. Senzor disponuje mikrofonom a z naměřeného akustického signálu se snaží detekovat, zda nedošlo k tříštění skla. Správným nastavením senzoru a zvolením vhodného algoritmu pro zpracování akustického signálu je možné zcela minimalizovat riziko vzniku falešného poplachu. Algoritmus lze dokonce nastavit tak, aby detektor reagoval pouze na zvuk tříštění určitého typu skla (např. tabulového), čímž se opět zmenší riziko vyhlášení falešného poplachu, které by mohlo vzniknout např. při rozbití láhve. [52] [54]

Na obr. 3.2 vidíme příklad senzoru pro ochranu skleněných ploch. Ke střežení prosklených ploch detektor využívá tzv. duální metodu, při které jsou vyhodnocované nepatrné změny tlaku v místnosti (náráz do skleněné výplně) a následně zvuky řinčení skla. Pro svoji činnost tedy senzor využívá již zmíněný akustický princip, ale nově i princip založený na změně tlaku. [55]



**Obr. 3.1 SA-201-A Kontakt magnetický mini povrchový s vodičem (převzato z [56])**



**Obr. 3.2 GBS-210 Detektor rozbití skla (převzato z [55])**

### **3.2.2 Prostorová ochrana**

Prostorová ochrana může svoji funkci vykonávat samostatně, ale její kooperace s plášťovou ochranou vytváří velice kvalitní formu zabezpečení domácnosti (alespoň proti zloději). Základní funkcí prostorové ochrany je detekce pohybu a přítomnosti objektů v chráněném prostoru. Detektory tohoto typu ochrany lze podle funkce rozdělit na detektory obsazení (detekují přítomnost objektů) a detektory pohybu (detekují pohyb). Detektory pohybu můžeme dále rozdělit na pasivní a aktivní, které se liší principem fungování. Pasivní detektory pohybu pouze registrují fyzikální změny ve svém okolí. Příkladem je PIR (Passive Infra Red) detektor, který je založen na principu zachycení změn vyzařování v infračerveném pásmu kmitočtového spektra, neboli na pyroelektrickém jevu. Aktivní detektory pohybu se od pasivních liší v tom, že si v okolí vytváří své pracovní prostředí vyzařováním, tedy



aktivním působením na okolí. Pohyb je detekován jako změna vytvořeného fyzikální prostředí. Aktivní detektory mohou být buď ultrazvukové (angl. ultrasonic, zkráceně US), nebo mikrovlnné (angl. microwave, zkráceně MW). Poslední druh detektorů pohybu se nazývá duální, jelikož kombinuje výše zmíněné principy. [52] [54]

Detektorů pohybu je obecně velké množství, pouze firma Jablotron disponuje desítkami různých produktů. Jako příklad jsem vybral tři typy (viz obr. 3.3, obr. 3.4 a obr. 3.5). První z nich je sběrníkový typu, tedy připojuje se na sběrníkovou ústřednu (viz kap. 3.3.2). Tento detektor umožňuje nastavit eliminaci poplachu způsobeného pohybem drobných zvířat (do cca 25 kg a max. výšky 40 cm na vzdálenost 7 m od detektoru) po podlaze. Druhý z nich je bezdrátový, duální (PIR a MW) a disponuje šedou čočkou, která zvyšuje odolnost vůči bílému světlu. Tato čočka pomáhá redukovat falešné poplachy způsobené např. osvětlením reflektory vozu skrze okna, zapadajícím sluncem, bleskem či reflexními povrchy. Poslední příklad PIR detektoru pohybu (viz obr. 3.5) je opět sběrníkový, ale tentokrát má navíc kameru, která umožňuje přenášet snímky do ústředny, odkud mohou být posílány na externí úložiště a PCO<sup>1</sup>. Kamera je dále vybavena bleskem pro záznamy ve tmě a detektor umí pořídit snímek na vyžádání. [57] [58] [59]



**Obr. 3.3 Sběrníkový PIR detektor pohybu**  
(převzato z [58])



**Obr. 3.4 Bezdrátový duální PIR a MW detektor pohybu**  
(převzato z [57])



**Obr. 3.5 Sběrníkový PIR detektor pohybu s kamerou**  
(převzato z [59])

---

<sup>1</sup> Pult centralizované ochrany (zkráceně PCO) představuje monitorovací místo, ve kterém se neustále střeží na něj připojené objekty zabezpečené pomocí EZS nebo EPS. V případě zjištění problému (např. narušení chráněného objektu) dojde na tomto místě k vyhodnocení situace a případně k zavolání složek integrovaného záchranného systému. [52]

### 3.3 Ústředny

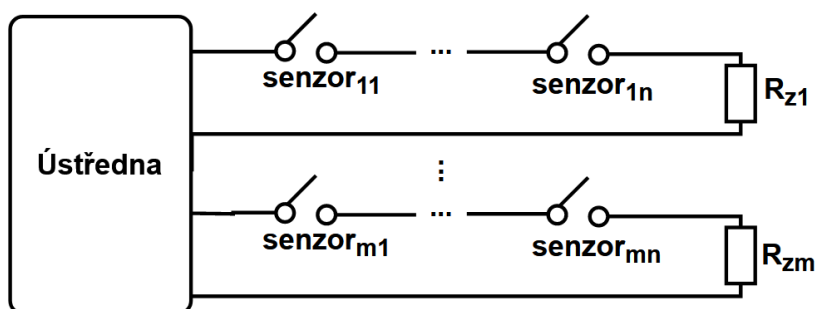
Ústředna představuje klíčovou součást každého EZS, jelikož zastupuje velké množství důležitých funkcí. Mezi tyto funkce primárně patří: [52]

- Přijímat a vyhodnocovat signály od senzorů tvořící EZS.
- Řídit činnost výstupů systému a také zmíněných senzorů (např. spuštění sirény, přenos dat na PCO, ukládání dat na cloud, apod.).
- Komunikovat se zařízeními řídící stav EZS. Systém se musí nějak způsobem přepínat alespoň do dvou základních stavů: klid a střežení. K tomu lze využít ovládací klávesnici, displej, nebo jiné periferie.
- Kontrola činnosti jednotlivých prvků EZS a jejich případná diagnostika.
- Ukládání událostí do připojených či vzdálených úložišť.
- Napájení prvků, ze kterých se systém skládá.

Při návrhu EZS a výběru ústředny je potřeba zohlednit mnoho důležitých kritérií, mezi které patří požadovaný stupeň zabezpečení dle legislativy, parametry chráněné oblasti a samozřejmě pořizovací cena. Ústředny se na základě komunikace s prvky systému dělí do čtyř základních skupin: smyčkové, s přímou adresací senzorů, smíšené a bezdrátové. Předmětem následujících kapitol je vysvětlení rozdílů mezi nimi a porovnání jejich slabých a silných stránek. [52]

#### 3.3.1 Smyčkové ústředny

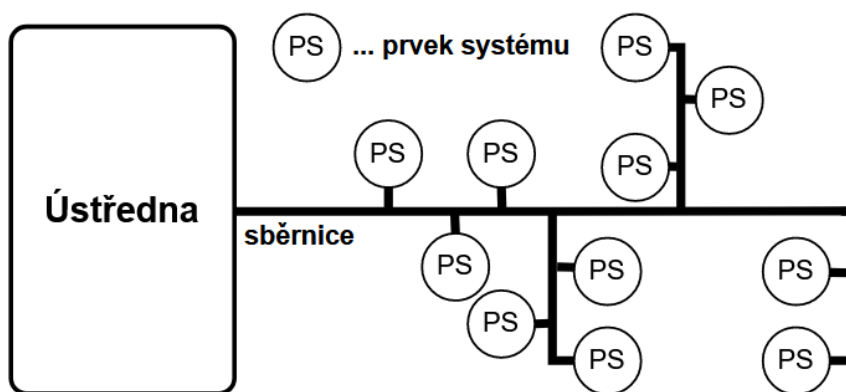
U smyčkové ústředny jsou senzory připojené do max.  $m$  smyček, přičemž v každé smyčce může být připojeno max.  $n$  senzorů (viz obr. 3.6). Každá smyčka musí být zakončena tzv. zakončovacím odporem, jelikož musí vykazovat určitý odpor. Všechny údaje ( $m$ ,  $n$ ,  $R_z$ ) jsou vždy uvedeny u konkrétní ústředny. V klidovém stavu jsou senzory smyčky spojeny. Při rozpojení kteréhokoli z nich se smyčka přeruší, což detekuje ústředna. Obecný princip fungování smyčkové ústředny je tedy založen na změně odporu smyčky. Typicky je každá smyčka tvořena sériovým zapojením rozpínacích kontaktů senzoru, tedy tak jak je znázorněno na obrázku. Mezi nevýhody tohoto typu ústředny patří rozsáhlá kabeláž, instalace této kabeláže a z toho vyplývající cena. Při přerušení smyčky ústředna nemůže poznat, který konkrétní senzor to způsobil. [52]



Obr. 3.6 Schéma smyčkové ústředny

### 3.3.2 Ústředny s přímou adresací senzorů

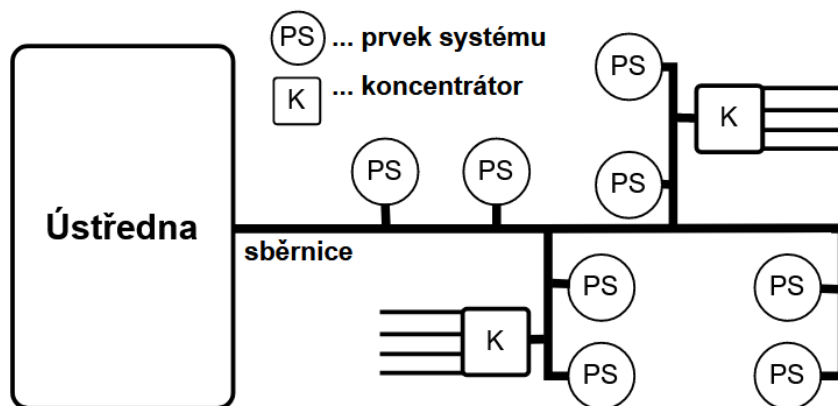
Ústředny s přímou adresací senzorů potřebují pro komunikaci se senzory kabeláž, což je stejné jako u smyčkové ústředny. Kabeláž však u tohoto typu ústředny není tak rozsáhlá. Klíčovou komponentu komunikace zprostředkovává sběrnice (viz obr. 3.7). Blok označený PS neboli prvek systému představuje vstupy i výstupy ústředny (senzory, aktuátoru atd.). Pokud PS komunikaci prostřednictvím sběrnice neumožňuje, musí se k němu přidat komunikační modul, který ale navyšuje cenu systému. Sběrnice limituje samotná sběrnice, konkrétně její max. povolená délka a nebezpečí indukce elektromagnetického rušení. Mezi výhody mmj. patří skutečnost, že ústředna komunikuje s jednotlivými senzory zvlášť, tedy při poplachu lehce identifikuje jeho původce. [52]



Obr. 3.7 Schéma ústředny s přímou adresací

### 3.3.3 Ústředny smíšeného typu

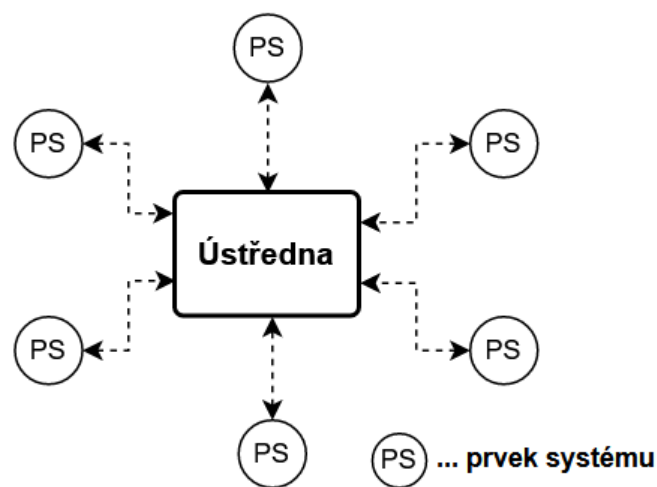
Ústředna smíšeného typu představuje kombinaci předešlých dvou typů ústřed. V podstatě se jedná o sběrnice ústřednu, na kterou lze připojit kromě systémových prvků také koncentrátor (viz obr. 3.8). Koncentrátor umožňuje připojení senzorů ve smyčkách přesně tak, jak to bylo znázorněno v kap. 3.3.1. Pro přehlednost nejsou zobrazeny jednotlivé senzory a zakončovací odpory v jednotlivých smyčkách. [52]



Obr. 3.8 Schéma ústředny smíšeného typu

### 3.3.4 Bezdrátové ústředny

Další typ ústředen tvoří bezdrátové ústředny (viz obr. 3.9). Jako jediné oproti předchozím typům odstraňují problémy spojené s kabeláží. To na druhou stranu implikuje potřebu napájet všechny prvky systému zvlášť. Napájení se typicky řeší bateriemi, což přináší nutnost monitorování jejich stavu. Samotná bezdrátová komunikace je navíc méně bezpečná s ohledem na odposlouchávání a rušení. V některých případech představují bezdrátové ústředny v podstatě jediné možné řešení (např. u památkových budov). Mezi další výhody bezdrátových ústředen patří možnost jednoduše přidávat další prvky systému případně volnost při přemísťování stávajících prvků (u drátové komunikace je přemísťování problém). Drátové i bezdrátové ústředny mají svoje výhody i nevýhody. Existuje ještě poslední typ ústředen označovaný jako hybridní. Tento typ se snaží využít výhod drátových a bezdrátových ústředen a zároveň co nejvíce potlačit jejich nevýhody. [52]



Obr. 3.9 Schéma bezdrátové ústředny

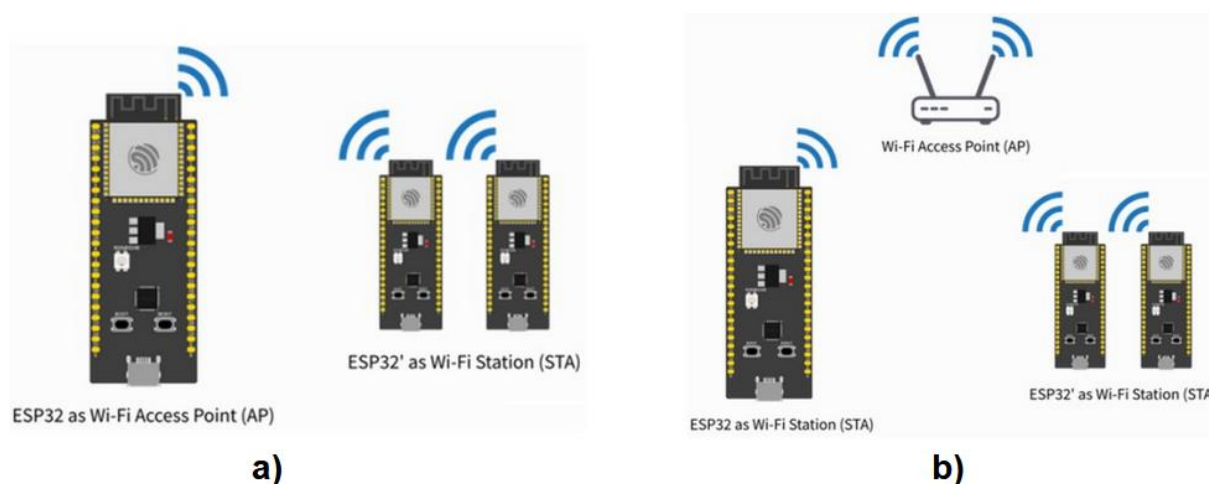
## 3.4 Mikrokontroléry esp32

Obecně esp32 zahrnuje celou řadu levných (angl. low-cost), nízkoenergetických (angl. low-power) systémů na čipu (angl. system on chip, zkráceně SoC) s integrovanou Wi-Fi a tzv. dual-mode Bluetooth<sup>2</sup>. Mikrokontroléry<sup>3</sup> esp32 jsou vytvořené firmou Espressif Systems, přičemž srdcem tohoto MCU je 32-bitový a 3,3V mikroprocesor vyráběný firmou TSMC 40nm technologií. [11]

### 3.4.1 Možnosti nastavení Wi-Fi sítě

Wi-Fi API<sup>4</sup> mikrokontroléru esp32 poskytuje podporu 802.11b/g/n. Součástí Wi-Fi API je mmj. možnost nastavit mikrokontrolér do několika módů, přičemž pro účely této práce jsou klíčové módy:

- Stanice (angl. station mode – zkráceně STA, nebo také Wi-Fi klient): Umožňuje mikrokontroléru připojit se k přístupovému bodu, což může být router anebo jiné zařízení generující Wi-Fi (viz část a) na obr. 3.10).
- Přístupový bod (angl. access point – zkráceně AP): Umožňuje generovat svoji vlastní Wi-Fi s volitelnými parametry. Jiná zařízení se pak mohou na tuto Wi-Fi připojit a jejím prostřednictvím spolu komunikovat (viz část b) na obr. 3.10).
- Hybridní: V hybridním módu mikrokontrolér vykonává oba předchozí módy současně. Může být tedy např. připojen na domácí Wi-Fi a zároveň generovat svoji vlastní Wi-Fi, jejímž prostřednictvím může komunikovat se zařízeními, které se na ni připojí. Právě tohoto módu bude využito v praktické části (viz kap. 4).



Obr. 3.10 Základní Wi-Fi módy (převzato z [7])

<sup>2</sup> Dual-mode Bluetooth označuje zařízení, které podporují verze Bluetooth Classic a zároveň Bluetooth Low Energy (zkráceně BLE).

<sup>3</sup> Mikrokontrolér (angl. Microcontroller Unit, zkráceně MCU) bude dále v textu také označován zkratkou MCU.

<sup>4</sup> API (zkratka Application Programming Interface) označuje rozhraní pro programování aplikací.

### 3.4.2 Režimy spánku

Mikrokontroléry esp32 mohou být nastaveny v tzv. aktivním režimu nebo v některém z režimů spánku (angl. sleep modes). Jednotlivé režimy se mezi sebou liší ve velmi důležitém parametru – spotřebě energie. Mikrokontrolér je designován tak, aby bylo možné odpojit jeho jednotlivé části (viz obr. 3.11) a to v závislosti na vytvářené aplikaci. V normálním režimu (aktivním režimu) jsou napájeny všechny části, což s sebou přináší spotřebu proudu až cca 260 mA. Při vysílání se však tato hodnota může ještě zvýšit. [17]



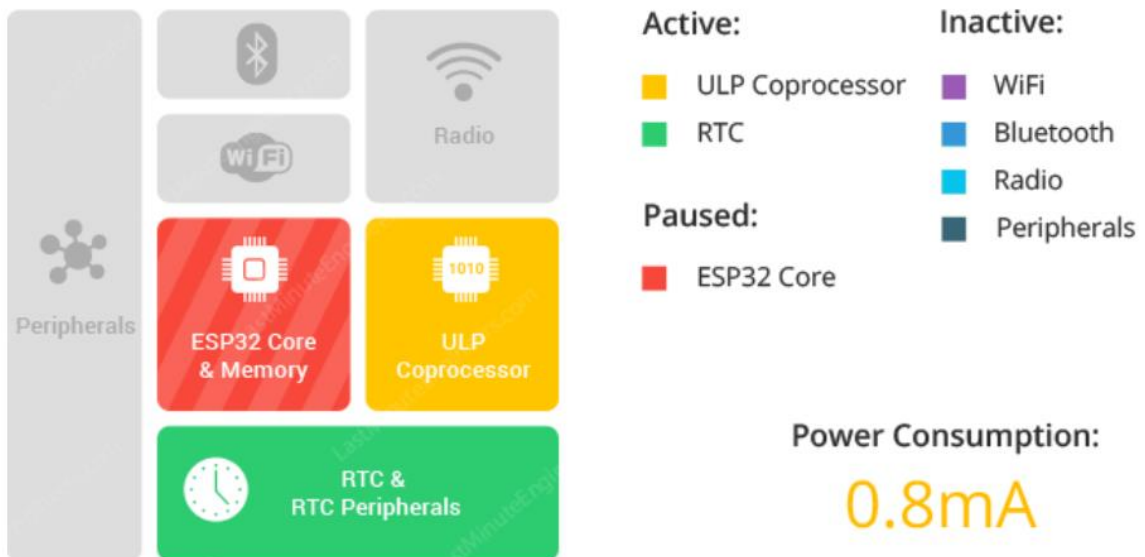
Obr. 3.11 Vnitřní blokové rozdělení mikrokontrolérů esp32 (převzato z [17])

Režimy spánku se liší podle toho, jaké části mikrokontroléru jsou odpojeny. Existují čtyři režimy spánku: mode, light, deep a hibernation. Všechny tyto režimy jsou přehledně popsány v [17] nebo přímo v oficiální dokumentaci (viz [18]). Dále bude rozebrán pouze režim light, jelikož právě ten se používá v praktické části při návrhu elektronického zabezpečovacího systému (viz kap. 4). V práci byl využit light režim, jelikož úspornější režimy neumožňují stejné funkcionality. Kupříkladu nelze u úspornějších režimů spánku zvolit, zda se má MCU při přerušení probouzet na náběžnou nebo spádovou hranu.

#### Light režim spánku

V light režimu spánku jsou odpojeny bloky Wi-Fi, Bluetooth, rádio a také nepoužívané digitální periferie. Používané digitální periferie, většina paměti RAM a CPU<sup>5</sup> jsou tzv. clock-gated. Jedná se o techniku využívanou pro snížení dynamické spotřeby energie. Realizuje se odpojením hodinového signálu od některých částí obvodu, což způsobí nepřepínání flip-flop obvodů, které jsou umístěny uvnitř těchto částí. Využití této techniky redukuje odběr proudu mikrokontroléru na hodnoty kolem 1 mA, což je oproti 250 mA (viz popsany aktivní režim výše) opravdu velká úspora. [17]

<sup>5</sup> CPU (zkratka Central Processing Unit, česky centrální procesorová jednotka, nebo také zkráceně procesor) označuje základní součástku vykonávající strojové instrukce. Přeneseně ji lze označit za srdce mikrokontroléru.

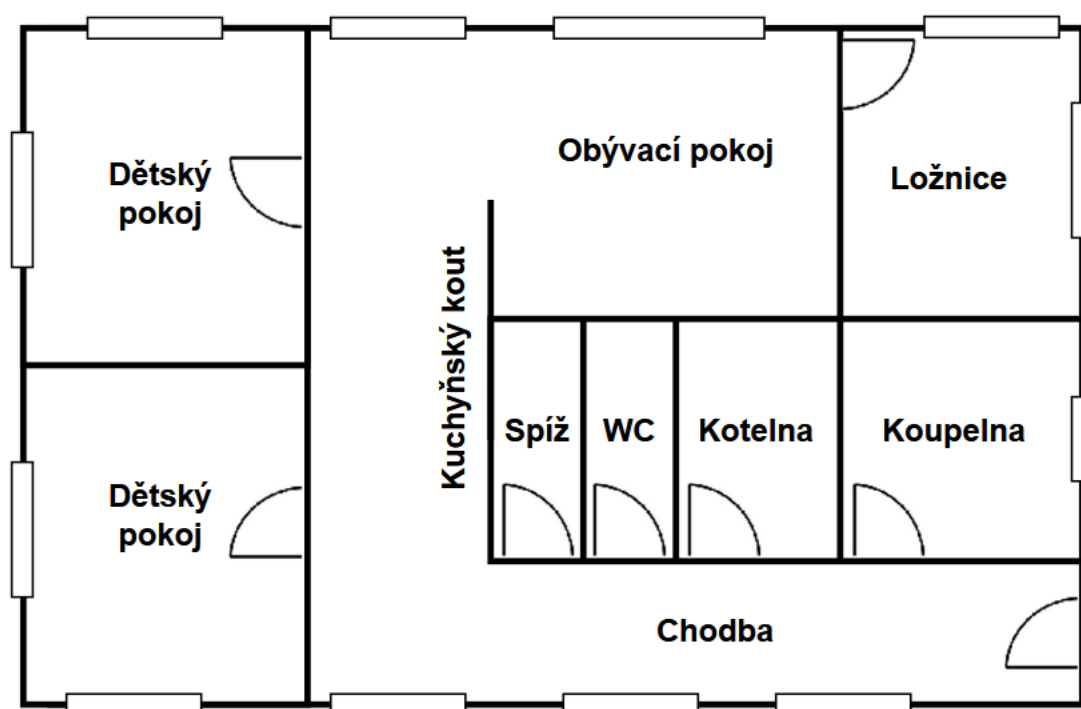


Obr. 3.12 Light režim spánku (upraveno z [17])

# 4 Návrh modelu systému pro elektronické zabezpečení rodinného domu

## 4.1 Navržený model

Hlavním úkolem práce je návrh modelu systému pro řízení a zpracování dat jednoduchého elektronického zabezpečení rodinného domu. Důraz je kladen na cenu a především spolehlivost výsledného systému. Objekt k elektronickému zabezpečení je jednopatrový rodinný dům s dvěma dětskými pokoji, ložnicí, obývacím pokojem s kuchyňským koutem, chodbou, spíží, WC, kotelnou a koupelnou (viz obr. 4.1). Dále se předpokládá, že v kotelně domu se nachází boiler a plynový kotel.

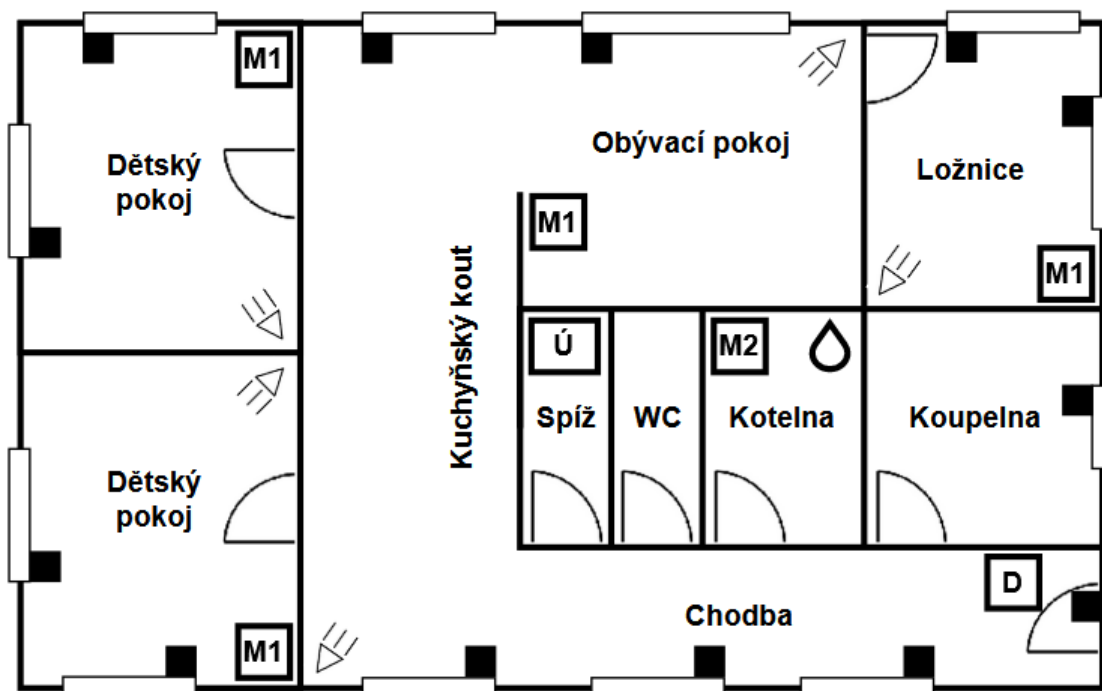


Obr. 4.1 Schéma objektu určeného k zabezpečení

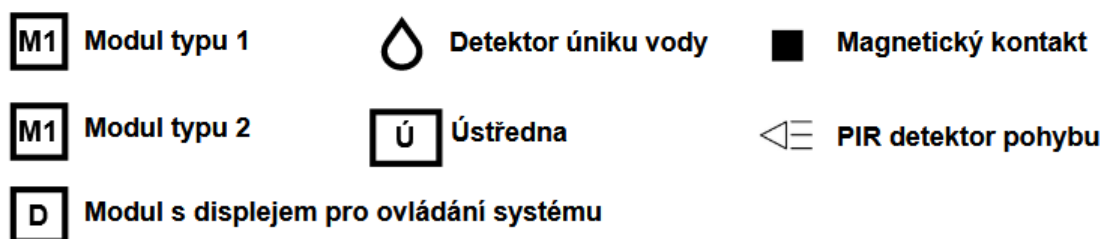
Základem zabezpečení objektu je plášťová a prostorová ochrana. Tyto ochrany realizují pomocí magnetických kontaktů na oknech a dveřích a také za pomoci PIR detektorů pohybu (viz obr. 4.2). Magnetické kontakty jsou spojeny drátově do jedné smyčky vedoucí do ústředny (viz kap. 3.3.1). PIR detektory pohybu jsou naopak připojeny do modulů typu 1 nacházejícího se ve stejné místnosti (viz obr. 4.2). Informace o detekci pohybu je do ústředny přenášena bezdrátově pomocí TCP/IP komunikace (viz dále).

Magnetické kontakty by také mohly být rozděleny do několika menších smyček, které by vedly do modulu typu 1 nacházejícího se ve stejné místnosti (kromě koupelny). V takovém případě by se zjednodušila instalace zabezpečení, jelikož by se nemuselo řešit vedení kabelu skrz zdi. Na druhou stranu by vznikla nová slabina systému, kterou je znemožnění komunikace s ústřednou v případě, kdy narušitel použije rušičku signálu. Z tohoto důvodu je plášťová ochrana realizována drátově pomocí jedné smyčky vedoucí do ústředny.





### Legenda:



Obr. 4.2 Schéma objektu s navrženým zabezpečením

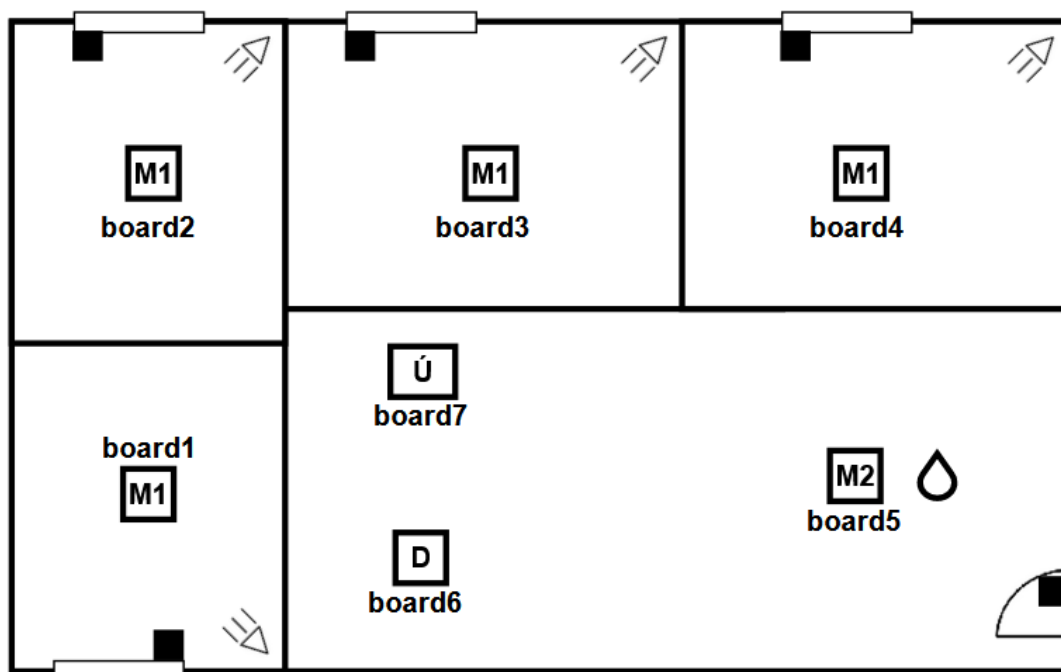
Kromě magnetických kontaktů a PIR detektorů pohybu (viz obr. 4.2) navržený systém obsahuje moduly označované jako typu 1 a 2, modul s displejem pro ovládání systému a ústřednu (viz kap. 3.3). Celkem se jedná o sedm modulů, které svojí komplexností tvoří hlavní část této práce a budou jím věnovány následující kapitoly. Ve zkratce se jedná o moduly, jejichž základní funkcí je měření veličin, komunikace s ústřednou, vyhodnocování výstupu PIR detektoru a informování uživatele za pomoci displeje, LED či bzučáku.

## 4.2 Realizovaný model

Výše zmíněné moduly jsem prakticky realizoval (viz dále). Pro jejich testování a obecně pro testování celého systému bylo nutné postavit model chráněného objektu. Při tvorbě tohoto modelu (viz obr. 4.3) došlo k:

- Vynechání PIR detektoru pohybu umístěného mezi kuchyňským koutem a chodbou.
- Snížení počtu oken z 12 na 4.
- Změně podoby některých místností, případně jejich úplnému vynechání (WC, koupelna).
- Změně umístění modulů, ústředny a PIR detektorů.

Tyto změny nastaly z praktických důvodů, což znamená především lepší manipulaci se systémem při testování. Také by nebylo smysluplné vytvářet v modelu rodinného domu místnosti jako je koupelna a WC, které by na systém neměly žádný vliv. Co se týče redukce počtu oken, tak to prakticky pro zabezpečení znamená pouze menší množství magnetických kontaktů ve smyčce, což na funkci opět nemá vliv.



#### Legenda:

<b>M1</b> Modul typu 1	Detektor úniku vody	Magnetický kontakt
<b>M1</b> Modul typu 2	<b>Ú</b> Ústředna	PIR detektor pohybu
<b>D</b> Modul s displejem pro ovládání systému		

Obr. 4.3 Schéma realizovaného chráněného objektu

Model rodinného domu spolu s vytvořenými moduly vidíme na obr. 4.4, přičemž umístění jednotlivých modulů, PIR detektorů a magnetických kontaktů přesně odpovídá schématu z obr. 4.3. Jednotlivé části systému jsem nejdříve realizoval na nepájivých polích a po vytvoření a odzkoušení kódu také na univerzálních jednovrstvých deskách plošných spojů, které jsou základem všech vytvořených modulů.

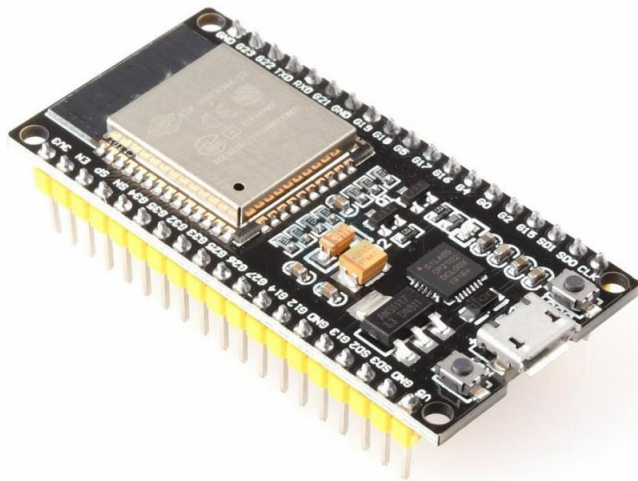


Obr. 4.4 Realizovaný chráněný objekt spolu s moduly

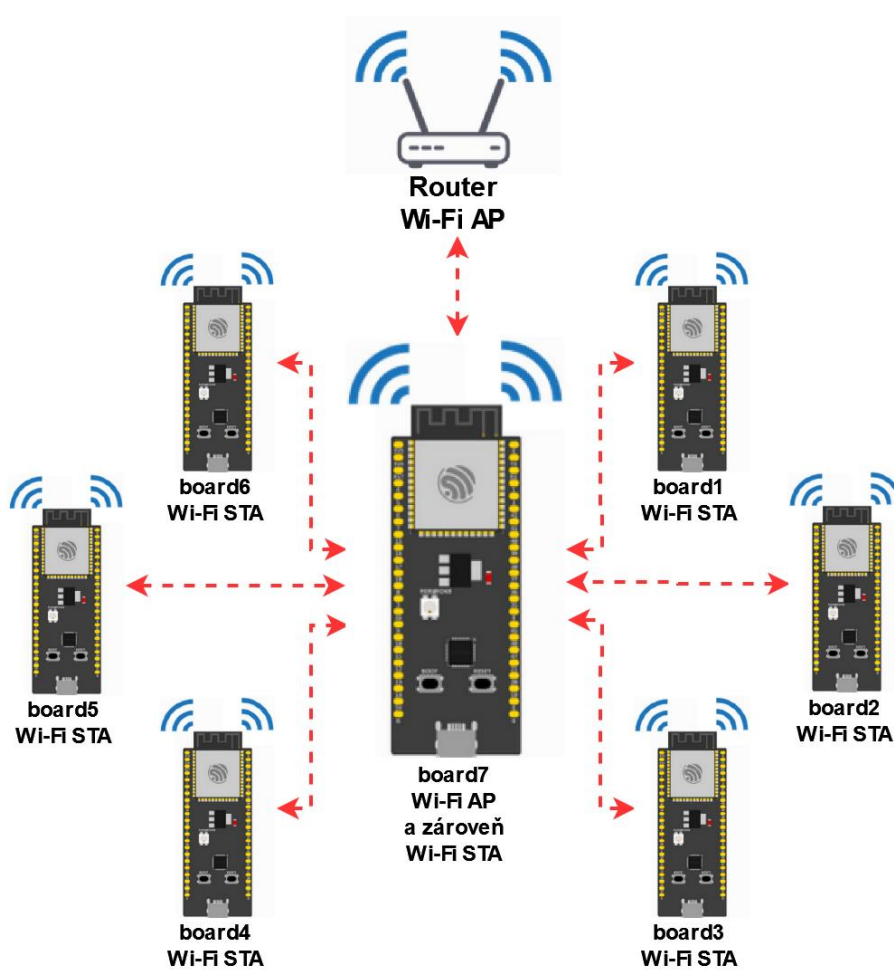
### 4.3 Použitý mikrokontrolér

Řídicí mikrokontrolér všech modulů včetně ústředny je esp32. V práci je konkrétně použit MCU označovaný jako ESP-WROOM-32 (viz obr. 4.5) s SoC ESP32-D0WDQ6 (revision 1), jehož základem je dvoujádrový procesor Tensilica LX6. Použití tohoto mikrokontroléru je díky jeho vlastnostem obecně velmi různorodé, např. to mohou být low-power IoT aplikace nebo aplikace s náročnými úkoly jako např. s kódování hlasu nebo streamování hudby. Navíc MCU disponuje integrovaným USB-UART převodníkem CP2102, který dodává mikrokontroléru jednoduché rozhraní pro nahrávání programu. [12]

Důvodem pro použití právě tohoto mikrokontroléru byla především nízká cena a spotřeba, integrovaná anténa umožňující využít Wi-Fi a Bluetooth, malé rozměry a kompatibilita se softwarem Arduino IDE. Původně bylo zamýšleno využívat BLE pro komunikaci mezi moduly a ústřednou, což by obecně dělalo komunikaci energeticky méně náročnou. Od tohoto záměru jsem ale upustil, jelikož není standardní (tedy jednoduché) používat Wi-Fi a BLE na esp32 zároveň. Navíc podle mé osobní zkušenosti (několik jednoduchých testů) má BLE menší dosah.



Obr. 4.5 Mikrokontrolér ESP-WROOM-32 (převzato z [12])



Obr. 4.6 Topologie komunikační sítě (upraveno z [7])

## 4.4 Komunikace v rámci systému

Z hlediska komunikace s prvky systému se jedná o hybridní ústřednu. S moduly komunikuje bezdrátově s využitím Wi-Fi, ale zároveň je na ni připojena smyčka s magnetickými kontakty. Otevření okna nebo dveří způsobí v pohotovostním režimu přerušeni smyčky, což ústředna detekuje a vyvolá poplach. Jedná se proto o poměrně jednoduchý a zároveň bezpečný způsob komunikace. Bezdrátová komunikace je komplexnější, a proto jí jsou věnovány následující kapitoly.

Komunikace mezi moduly a ústřednou se realizuje prostřednictvím Wi-Fi. Mikrokontrolér esp32 může být nastaven do Wi-Fi módu STA, AP nebo hybridního módu (viz kap. 3.4.1), přičemž v hybridním módu MCU vykonává módy STA a AP zároveň. Právě v tomto módu je nastavena ústředna (viz obr. 4.6), jelikož to jí umožňuje připojit se na domácí Wi-Fi (router) a zároveň generovat svojí vlastní Wi-Fi. Prostřednictvím domácí Wi-Fi ústředna posílá data na cloud a prostřednictvím generované Wi-Fi komunikuje s klienty (moduly) označenými jako board1 až board6. Takto vytvořená síť má hvězdicovou topologii.

## 4.5 Ústředna jako server

Jak již bylo řečeno výše, ústředna v hybridním režimu vykonává mód klienta a zároveň serveru. Komunikace s moduly je postavena na TCP/IP (zkratka angl. transmission control protocol/ internet protocol) komunikaci, ve které ústředna vykonává funkci tzv. asynchronního webového serveru (dále označovaného pouze server). Základem tohoto serveru je knihovna *ESPAsyncWebServer* (viz [8]), přičemž pro její použití na mikrokontroléru esp32 je také nutné nainstalovat knihovnu *AsyncTCP* (viz [9]).

Knihovnu *ESPAsyncWebServer* jsem vybral kvůli asynchronnosti a spolehlivosti komunikace a poměrně jednoduchému způsobu použití. Server stačí nastavit pouze jednou a knihovna se dále stará o celou TCP/IP komunikaci. O konkrétním způsobu nastavení serveru pojednává kap. 5.5.3.

TCP/IP komunikaci prostřednictvím knihovny *ESPAsyncWebServer* jsem označil za spolehlivou, jelikož při komunikaci využívá tzv. handshaking („potřesení rukou“). Jedná se o proces navázání spojení mezi serverem a klientem, který určuje různé parametry komunikace. Pro roli ústředny je velmi důležitá vlastnost, že handshaking, konkrétně v tomto případě označovaný jako three-way handshaking (viz [13]) vyžaduje potvrzení přijetí zprávy od serveru. To znamená, že klient pošle zprávu serveru a ten mu přijetí zprávy potvrdí. Pokud klient neobdrží potvrzení, nebo ho obdrží v chybné podobě, může na to adekvátně reagovat.

V případě této práce klient řeší mnoho situací, které mohou v průběhu komunikace nastat. Jedná se např. o neobdržení potvrzení, v takovém případě klient poslání zprávy zopakuje. Pokud od serveru stále potvrzení nedochází i po několik pokusech, potom se klient od serveru odpojí, uspí se na několik sekund, vzbudí se a znovu naváže spojení, při kterém se snaží zprávu opět poslat. Díky tomu se zabrání situaci, kdy by došlo k detekci pohybu PIR detektorem a klient by tuto informaci nepředal ústředně kvůli momentálním problémům

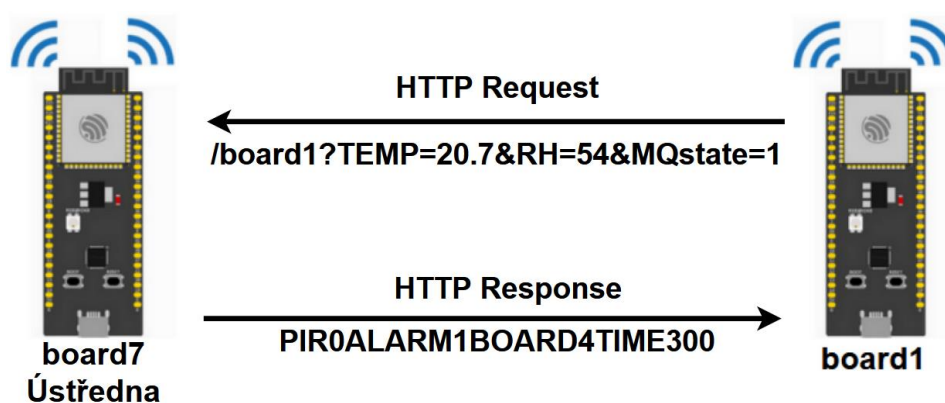
s komunikací. Klient považuje zprávu za doručenou jen v takovém případě, kdy server pošle potvrzení v očekávaném formátu (viz následující kapitola).

Zabezpečení komunikace realizované prostřednictvím knihovny *ESPASyncWebServer* je zajišťováno standardem WPA2. Šifrování tímto standardem rozhodně není neprolomitelné, ale zároveň to není úplně jednoduché. Aktuálně se jedná o nejpoužívanější standard šifrování Wi-Fi na světě (viz [4]). Navíc by se při napadení muselo jednat o lokální útok, tzn. útočník by se musel nacházet přímo u chráněného objektu, což situaci dále komplikuje. [5] [6]

## 4.6 Komunikace mezi ústřednou a klienty

V předešlé kapitole je uvedeno, že klient po poslání zprávy serveru obdrží potvrzení, přičemž klient navíc pozná, jestli má toto potvrzení správnou podobu. Dále bude vysvětleno, co si mezi sebou tyto dva subjekty posílají a jakou mají mít tyto zprávy podobu. Podobu zprávy ve skutečnosti kontroluje i sever. Pokud není správná, pak na tuto zprávu zkrátka nepošle odpověď, což donutí klienta k opětovnému poslání.

Komunikaci mezi ústřednou a klientem si vysvětlíme na konkrétním příkladu (viz obr. 4.7). Komunikaci zahájí klient (obecně ji vždy zahajuje klient), v tomto případě board1, vysláním HTTP požadavku<sup>6</sup> (angl. request) s řetězcem složeným z lomítka „/“, identifikátorem desky (board1 až board6) a otazníkem „?““. Následuje označení parametru, který chce klient předat serveru, rovnítko „=“ a hodnota tohoto parametru. Parametrů lze přenést najednou několik, přičemž se od sebe oddělují znakem „&“. V našem případě posílá board1 parametry *TEMP*, *RH* a *MQstate* a hodnoty těchto parametrů jsou 20.7, 54 a 1. Význam těchto parametrů si vysvětlíme dále.



Obr. 4.7 Ukázka komunikace mezi ústřednou a klientem

Přehled parametrů, které klient posílá v požadavku:

- **TEMP** (temperature) [°C]: Teplota, jedno desetinné místo, posílají klienti 1-4.
- **RH** (relative humidity) [%]: Relativní vlhkost, klienti 1-4.
- **MQstate**: Stav kvality ovzduší (viz kap. 5.2.1), klienti 1-5.
- **PIRalarm**: Detekován pohyb PIR detektorem pohybu, klienti 1-4.

<sup>6</sup> HTTP požadavek bude dále označován pouze zkráceně jako požadavek.

- **MQalarm:** Zjištěna nebezpečná kvalita ovzduší, klienti 1-5.
- **WSleak:** Detekován únik vody senzorem hladiny vody (angl. water sensor), klient 5.
- **TPleak:** Detekován únik vody pinem v kapacitním režimu (angl. touch pin), klient 5.
- **INIT:** Inicializační zpráva, posílá klient 6 po zadání správného PIN kódu, čímž dojde k autorizaci uživatele (viz kap. 5.4.2).
- **STOP\_ALARM:** Příkaz od klienta 6 k zastavení MQ alarmu (viz kap. 5.4.2).
- **MAGN\_CON:** Dotaz od klienta 6, zda je smyčka zajišťující plášťovou ochranu spojena či rozpojena.
- **TURN\_ON:** Příkaz od klienta 6 k uvedení systému do pohotovostního režimu.

Klient od serveru musí dostat HTTP odpověď (angl. response). Podoba této zprávy je trochu jiná, v podstatě se jedná o řetězec, ve kterém jsou zakódovány některé parametry. Podoba odpovědi opět není jednotná, záleží na konkrétní podobě požadavku od klienta. Obecně zpráva obsahuje řadu parametrů, které již nejsou od sebe odděleny znakem „&“. Zároveň není mezi označením parametru a jeho hodnotou vloženo rovnítko, ale hodnota parametru se nachází ihned za jeho označením. V našem případě (viz obr. 4.7) posílá server v odpovědi parametry *PIR*, *ALARM*, *BOARD* a *TIME*, přičemž hodnota těchto parametrů je 0, 1, 4 a 300. Význam těchto parametrů si vysvětlíme dále.

Přehled parametrů, které posílá server v HTTP odpovědi:

- **PIR:** Pokyn k tomu, zda má klient detekovat pohyb pomocí PIR detektoru. V podstatě se pomocí tohoto parametru klient dozví, že se systém nachází v pohotovostním režimu. Zpráva se posílá v každé odpovědi klientům 1 až 4.
- **ALARM:** Informace o tom, jestli je v systému vyhlášen MQ alarm (viz kap. 5.2.2). Zpráva se posílá v každé odpovědi klientům 1 až 4 a také klientu 6 jako součást odpovědi na požadavek *INIT*.
- **BOARD:** Identifikace desky, která MQ alarm vyhlásila. Posílá se v každé odpovědi klientům 1 až 4, kteří následně tuto informaci zobrazují na displeji. Parametr se posílá také klientu 6 jako součást odpovědi na požadavek *INIT*.
- **TIME [s]:** Časový údaj určující, na jak dlouho má klient přejít do režimu spánku (viz kap. 5.2.2). Zpráva se posílá v každé odpovědi klientům 1 až 5.
- **SA\_OK:** Potvrzení přijetí požadavku *STOP\_ALARM* od klienta 6.
- **MAGN\_CON:** Odpověď na stejnojmenný požadavek od klienta 6. Obsahuje informaci o tom, zda je smyčka zajišťující plášťovou ochranu spojena či rozpojena.
- **TURN\_ON\_OK:** Potvrzení přijetí požadavku *TURN\_ON* od klienta 6.

Podrobné vysvětlení komunikace mezi ústřednou a konkrétními klienty je součástí každé podkapitoly v kap. 5.



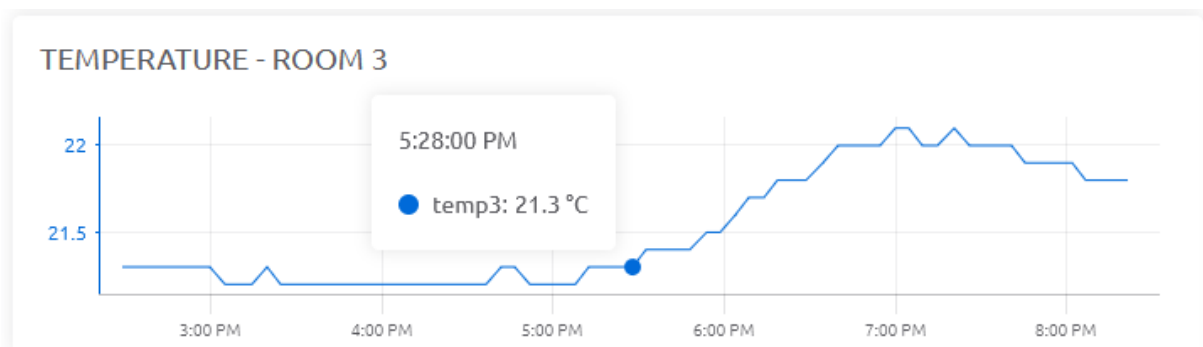
## 4.7 Blynk cloud

Systém sbírá množství dat, o kterých by bylo dobré informovat uživatele a to nejen v rámci domácnosti, ale také vzdáleně. Právě k tomuto účelu slouží mnoho aplikací (např. HiveMQ Cloud, Arduino Cloud IoT, adafruit, Blynk), které se mezi sebou liší v mnoha ohledech. Při výběru takové aplikace je snaha optimalizovat vybrané parametry, mezi které samozřejmě primárně patří cena, která je zpravidla přepočítána na určité množství uložených dat. Důležitou roli dále hraje API a kvalita jeho zpracování, možnost vytvořit si mobilní aplikaci, historie uložených dat (jak dlouho data zůstanou uložena), frekvence nahrávání dat apod.

Já jsem pro účely této práce vybral aplikaci Blynk (viz [14]). Blynk nabízí bezplatnou verzi, která pro účely této práce zcela postačuje. Informace o všech nabízených verzích najdeme v [15]. Dále bude zmíněno několik důvodů, proč jsem vybral právě tuto aplikaci. Blynk umožňuje uživateli vytvořit si webovou a zároveň také mobilní aplikaci. Data (např. proměnná typu float) poslaná na Blynk cloud<sup>7</sup> jsou ukládána po dobu tří měsíců a jejich množství není téměř omezeno. Pouze platí, že se nemá nahrávat více než desetkrát za sekundu, což je pro účely této práce více než dostačující. V rámci bezplatné verze lze vytvořit dva projekty, přičemž na každý z nich může být připojeno až pět zařízení. My využijeme pouze jeden projekt, na kterém navíc bude připojeno jen jedno zařízení (ústředna).

Rozhraní pro tvorbu webové i mobilní aplikace je velmi uživatelsky přívětivé a je podrobně zdokumentováno (viz [16]). Pro účely této práce si vystačíme v podstatě jen s grafy, i když lze využít i jiné způsoby vizualizace dat. Příklad vytvořeného grafu ve webovém rozhraní vidíme na obr. 4.8, jedná se o naměřenou teplotu v pokoji 3 (board3 na obr. 4.3). Aplikace samozřejmě umožňuje zvolit různé typy grafů, různé barvy apod.

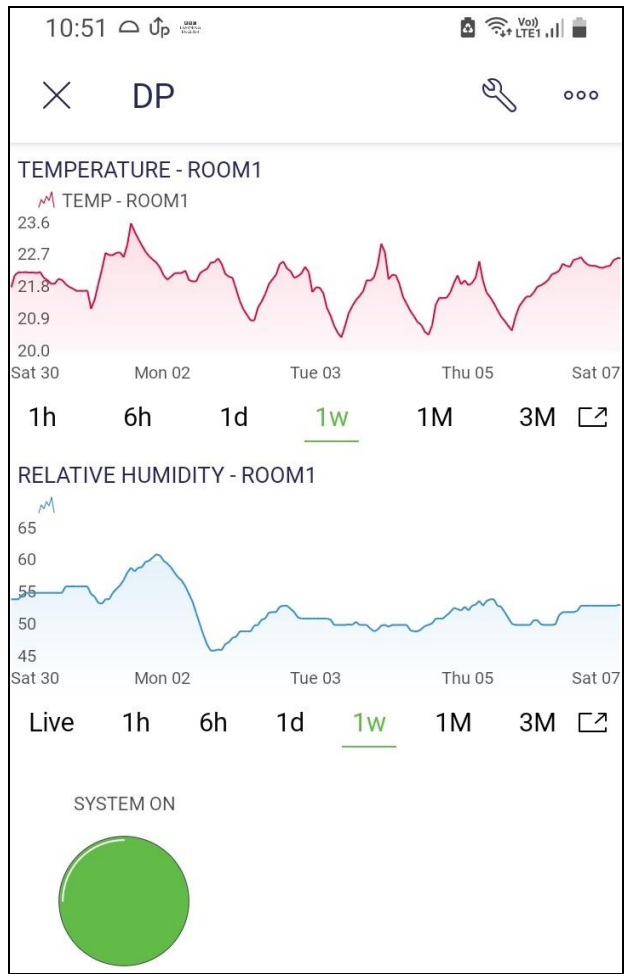
Na obr. 4.9 vidíme podobu mobilní aplikace s názvem Blynk IoT. Na obrazovce jsou vidět grafy vývoje teploty a relativní vlhkosti v průběhu jednoho týdne. Dále je vidět LED informující o aktuálním režimu systému, tedy zda je systém v klidovém nebo pohotovostním režimu (svítí v pohotovostním). Poznamenejme, že grafy aplikace Blynk zobrazuje nesprávně bez popisků os a příslušných jednotek. Pouze v případě vybrání konkrétního bodu se zobrazí jednotka (viz obr. 4.8). Dále se nejedná o českou aplikaci, tedy místo desetinné čárky používá desetinnou tečku. U všech přidaných grafů je vysvětlující komentář, nemělo by proto dojít k nepochopení toho, co daný graf zobrazuje.



Obr. 4.8 Ukázka grafu z webového rozhraní aplikace Blynk

<sup>7</sup> Blynk cloud může být dále v textu označován zkráceně pouze jako cloud.





**Obr. 4.9** Mobilní aplikace Blynk IoT

## 5 Vytvořené moduly a jejich role v systému

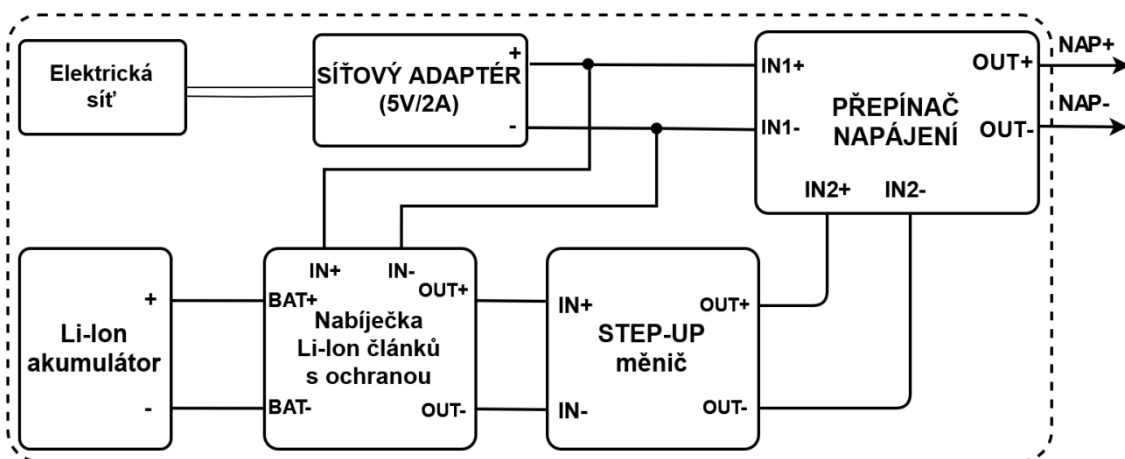
Navržený model (viz obr. 4.3) je tvořen sedmi moduly: modulem typu 1 a 2, modulem s displejem pro ovládání systému a modulem označovaným jako ústředna. Cílem této kapitoly je vysvětlit zapojení a funkci každého z nich.

### 5.1 Napájení

Než se pustíme do popisu prvního modulu, vysvětlíme si, jak je řešeno napájení modulů. Základním zdroje energie každého modulu je elektrická síť tedy zásuvka. Síťové napětí se transformuje síťovým adaptérem (nabíječkou) na stejnosměrné napětí 5 V. Je vhodné zvolit adaptér s maximální hodnotou výstupního proudu alespoň 2 A, což je důležité zejména pro ústřednu. Ústředna totiž disponuje GSM modulem (viz kap. 5.5), který má zejména při přihlašování do mobilní sítě velké nároky na napájení. Jako vstupní konektor napájení modulů jsem zvolil micro USB.

U elektronického zabezpečení domácnosti nelze spoléhat pouze na přísun energie z elektrické sítě. Zloději by totiž stačilo odpojit chráněný objekt od elektrické sítě a elektronické zabezpečení by bylo deaktivované. Z tohoto důvodu každý modul disponuje záložním zdrojem energie.

Schéma napájení klientů (všech modulů kromě ústředny) vidíme na obr. 5.1 a schéma napájení ústředny na obr. 5.2. Rozdíl mezi nimi je pouze v tom, že napájení ústředny má o dva výstupy více. Pomocí výstupy *D* mikrokontrolér zjišťuje, zda je napájen z elektrické sítě (pokud ano, pak je na *D* napětí 5 V) a pomocí výstupu *AN* si měří napětí na baterii. Napájení modulů se tak kromě elektrické sítě a síťového adaptéru skládá z lithium-iontové (zkráceně Li-Ion) baterie, nabíječky Li-ion článků s ochranou, step-up měnič a přepínače napájení.

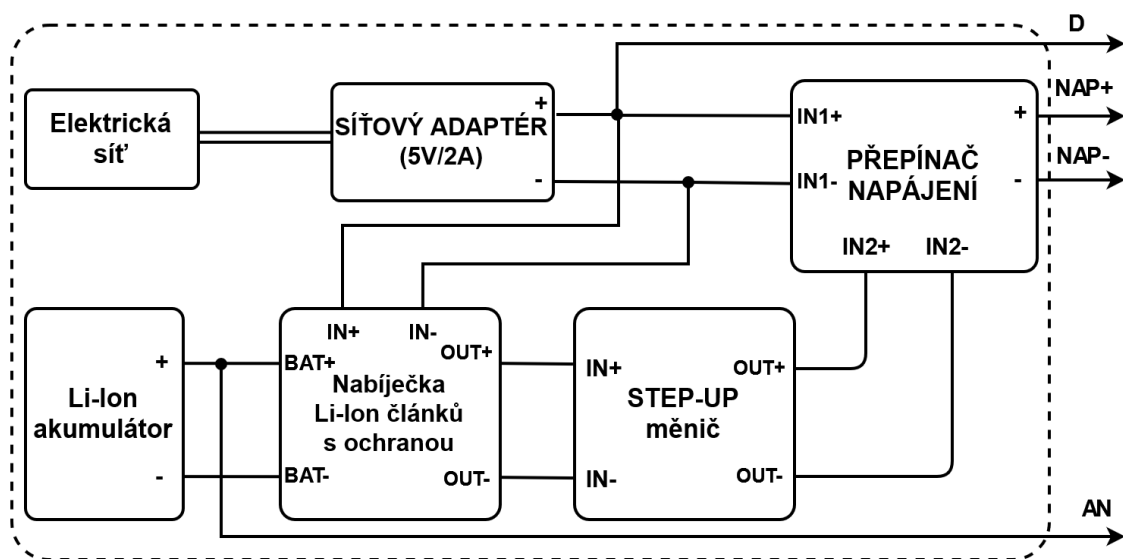


Obr. 5.1 Schéma napájení klientů

Li-Ion typ baterií jsem zvolil, jelikož se jedná o dobré řešení v porovnání cena-výkon. U modulů typu 1 a 2 jsem použil GeB Li-Ion baterii typu 18650 s kapacitou 3000 mAh a jmenovitým napětím 3,7 V (viz [21]) a u modulu s displejem stejnou baterii s kapacitou

2200 mAh (viz [20]). Tento modul má menší spotřebu a proto stačí menší kapacita baterie (viz kap. 5.3.2). U serveru jsem použil GeB Li-Ion baterii typu 26650 s kapacitou 5000 mAh a stejným jmenovitým napětím (viz [22]). Větší kapacita baterie serveru byla zvolena kvůli tomu, že se jedná o hlavní modul zajišťující fungování celého systému. V případě, kdy dojde ústředně energie, přestane fungovat veškeré elektronické zabezpečení.

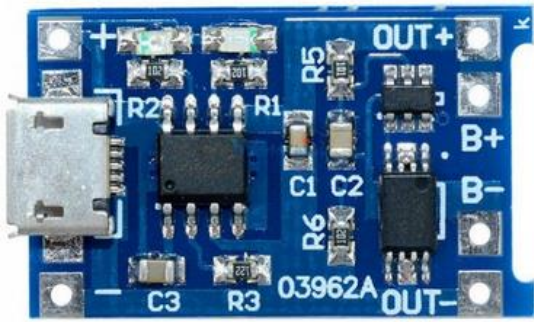
Li-Ion baterie se vyznačují vysokou hustotou uložené energie na jednotku objemu, vysokou životností v porovnání s jinými typy baterií a schopností dodávat vyšší výstupní proudy, což je opět důležité zejména pro ústřednu disponující GSM modulem. Jedná se o válcovitý tvar baterie s délkou cca 65 mm a průměrem cca 18,4 mm (typ 18650) nebo 26 mm (typ 26650). Jedná se proto o poměrně velké baterie, což v této aplikaci nevadí, jelikož krabičky všech modulů mají rozměry 150x110x70 mm, místa pro baterie je tedy dostatek. [19]



Obr. 5.2 Schéma napájení ústředny

Na druhou stranu použité Li-Ion baterie nemají žádné vestavěné ochranné obvody zajišťující udržování napětí a proudu v bezpečných mezích. V navrženém obvodu se nachází nabíječka Li-Ion článků s ochranou (viz obr. 5.3), která právě tyto ochrany zajišťuje. Mezi hlavní funkce této součástky patří:

- bezpečné nabíjení konstantní napětím a proudem,
- ochrana proti vybíjení – chrání baterii proti vybití pod 2,4 V (minimální hodnota pro „zdraví“ baterie),
- ochrana proti přepětí – nabíjí baterii až do 4,2 V, potom baterii odpojí od napájení,
- nadproudová a zkratová ochrana
- rekondice baterie – pokud je napětí na připojené baterii nižší než 2,9 V, potom se tato baterie nabíjí pouze proudem 130 mA, což je pro baterii lepší z hlediska její životnosti.



Obr. 5.3 Nabíječka Li-Ion článku TP4056 s ochranou (převzato z [24])



Obr. 5.4 Step-up měnič s MT3608 (převzato z [23])

Výstupní napětí nabíječky Li-Ion článku je dále nutné transformovat na 5 V, jelikož právě tímto napětím lze externě napájet mikrokontrolér (jedna z možností, viz [33]). Zároveň se jedná o minimální provozní napětí přepínače napájení (viz dále). K transformaci na napětí 5 V je použit step-up měnič s MT3608 (viz obr. 5.4). Vstupní a výstupní napětí měniče je v rozmezí 2 až 24 V, přičemž výstupní napětí se reguluje pomocí trimru. Výstupní proud je 500 mA, což pro tuto práci postačuje. Zároveň je možné po krátkou dobu z měniče odebírat i vyšší proudy (až 1 A), což zajistí dostatek proudu i pro ústřednu a její GSM modul.

Poslední komponentu napájení tvoří automatický přepínač baterie, též označovaný jako UPS modul YX850 (viz obr. 5.5). Na horní svorkovnici vlevo je připojeno napětí ze síťového adaptéru a na spodní svorkovnici vlevo výstup ze step-up měniče. Výstupy přepínače napájení se dále připojí na piny 5 V a GND na mikrokontroléru.

Funkce součástky je v principu jednoduchá. Za normálních okolností je MCU napájen ze síťového zdroje zapojeného na svorky DC+ a DC- (IN1+ a IN1- na obr. 5.1 a na obr. 5.2). V případě výpadku energie z elektrické sítě modul přepne napájení MCU na svorky BAT+ a BAT- (IN2+ a IN2- na obr. 5.1 a na obr. 5.2). Provozní stejnosměrné napětí přepínače je 5 V až 48 V a maximální zátěžový proud je 10 A, což je pro tuto práci dostačující.



Obr. 5.5 Automatický přepínač baterie (převzato z [25])

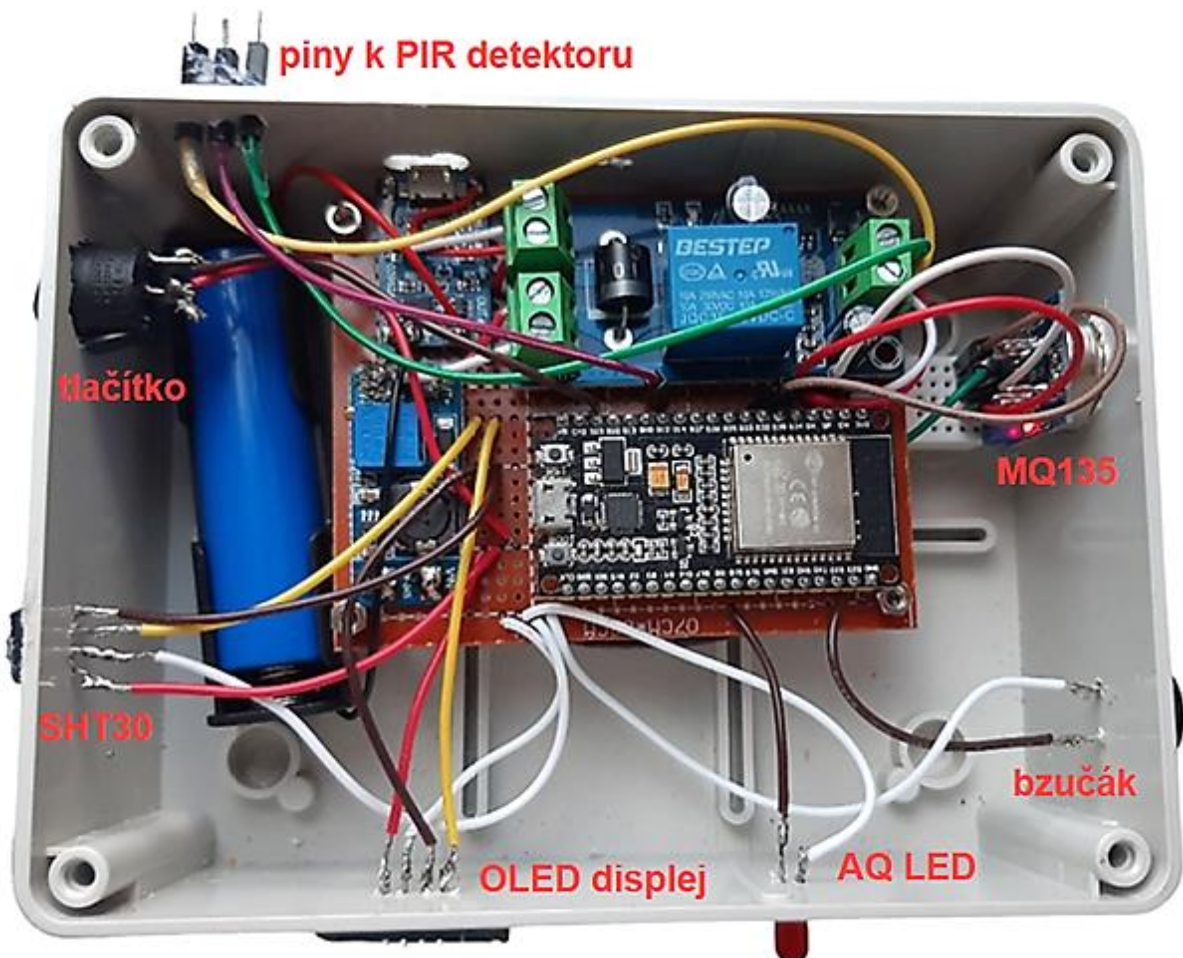
Napájení z obr. 5.1 a obr. 5.2 bude dále ve schématech značeno pouze blokově (viz obr. 5.6). Napájecí část společně s mikrokontrolérem je připájena na univerzální jednovrstvé desce plošných spojů a baterie je umístěna v držáku vedle tohoto modulu (např. viz obr. 5.7).



Obr. 5.6 Bloky napájení

## 5.2 Modul typu 1

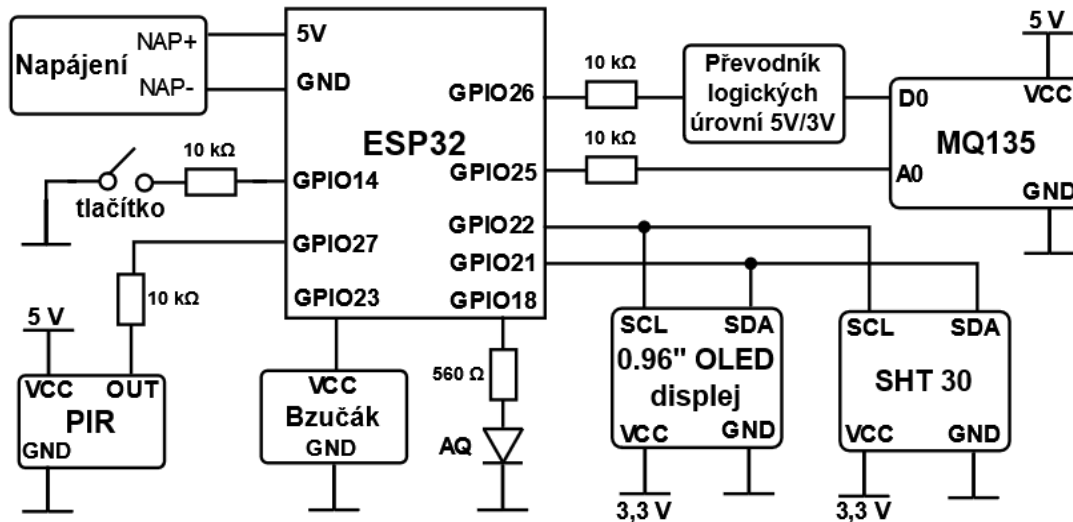
Vytvořený model obsahuje sedm modulů, přičemž čtyři z nich jsou právě moduly označované jako typu 1. Jedná se o moduly umístěné v dětských pokojích, ložnici a obývacím pokoji (viz obr. 4.2), kde se mmj. nacházejí také okna. Ty samozřejmě představují stavební otvor, kudy by zloděj mohl vniknout do chráněného objektu. Okna sice jsou součástí plášťové ochrany realizované pomocí magnetických kontaktů, ale zloděj může vniknout do chráněného prostoru jinak, typicky rozbitím okna, což smyčku nepřeruší a tedy poplach nevyhlásí. Z tohoto důvodu je vhodné použít prostorové ochrany – detektory pohybu.



Obr. 5.7 Realizovaný modul typu 1

## 5.2.1 Zapojení

Schéma zapojení modulu typu 1 vidíme na obr. 5.8 a realizaci jednoho z těchto modulů společně s popisem připojených komponent na obr. 5.7. Jedná se o první vysvětlovaný modul, proto zopakujeme, že základem všech modulů je řídicí mikrokontrolér esp32 a zároveň všechny moduly disponují akumulátorem zálohovaným napájením (viz kap. 5.1).



Obr. 5.8 Schéma zapojení klientů 1-4

### MQ135

Blok MQ135 představuje modul se senzorem MQ-135 (viz obr. 5.9), též označovaný jako detektor kvality ovzduší. Jedná se o senzor pro měření koncentrace skupiny plynů ovlivňujících kvalitu ovzduší jako je např. amoniak, oxidy dusíku, benzen, kouř a oxid uhličitý. Podstatou měření kvality ovzduší je změna odporu tenké vrstvy oxidu cíničitého, který se mění v závislosti na koncentraci nejen výše zmíněných plynů. Při použití tohoto detektoru je nutné myslet na to, že se skutečně neměří pouze koncentrace jednoho plynu (např. se můžeme setkat s chybným označením senzor pro měření oxidu uhličitého), ale skupiny plynů. Z tohoto důvodu se senzor označuje jako senzor kvality ovzduší. Na druhou stranu se jedná o velmi levné řešení, které lze v případě správného užívání použít. Měření je navíc možné zpřesnit kalibrováním. [29]

Modul se senzorem MQ-135 má čtyři piny: zem, napájení (5 V) a digitální a analogový výstup. Analogový výstup slouží pro měření kvality ovzduší. Přesněji se měří odpor vrstvy oxidu cíničitého, který je přepočítáván na koncentraci a ta na kvalitu ovzduší. Digitální výstup slouží ke generování přerušení při změření větší koncentrace kvality ovzduší, než je nastavená prahová hodnota. Ta se nastavuje pomocí interního trimru. Logika je opačná než obvykle, tzn. při generování přerušení se změní napětí na digitálním pinu z 5 V na 0 V. [29]

Vzhledem k principu fungování MQ-135 by nemělo smysl informovat o konkrétní naměřené koncentraci. Z tohoto důvodu se převádí naměřená hodnota do třech stavů: 1 (OK), 2 (BAD), 3 (ERROR). Názvy těchto stavů okamžitě informují o aktuálním stavu kvality ovzduší v místnosti. Hranice stavů byly stanoveny experimentálně. Ideálně by se měl modul dostat



do stavu 2 v případě, kdy je v místnosti „vydýcháno“. Na tuto skutečnost je uživatel upozorněn mmj. také rozsvícením LED s názvem AQ (zkratka air quality). Tento koncept je však nutné brát s rezervou a v podstatě stav 2 představuje pouze přechod mezi stavem 1 (hodnota v normálu) a stavem 3 (vysoká hodnota). Ve stavu 3 se tedy „asi něco děje“, což může představovat vyšší koncentraci CO<sub>2</sub>, ale také např. přítomnost kouře. Jedná se proto o jednoduchý detektor kouře – požární hlásič. Pozn. MQ-135 může nabývat také stavu 0, který značí dosavadní neuplynutí doby zahoření (viz kap. 5.2.2).

Pokud některý modul typu 1 přejde do stavu 3, je aktivován bzučák (viz dále) a zároveň je ústředně poslána HTTP žádost s parametrem MQalarm (viz kap. 4.6). Ústředna o této skutečnosti informuje i ostatní moduly typu 1, které si také aktivují svůj bzučák. Na displejích těchto modulů se navíc objeví informace o tom, který modul typu 1 MQalarm vyhlásil (viz obr. 5.18). Tímto způsobem se informují obyvatelé chráněného objektu o možném nebezpečí. Pozn. deaktivace bzučáků se realizuje prostřednictvím modulu s dotykovým displejem (viz kap. 5.4.2).

Velká nevýhoda modulu se senzorem MQ-135 je jeho spotřeba. Modul spotřebovává proud cca 120 mA a to z velké části na ohřívání vrstvy oxidu cíničitého. Tuto vrstvu ohřívá na teplotu, při které je nejcitlivější na měřené plyny. Výsledná měření tedy jsou také závislá na teplotě prostředí, tato chyba ale není příliš velká a to zejména v teplotách okolo 25 °C. [34]



**Obr. 5.9 Modul se senzorem MQ-135**  
(převzato z [29])



**Obr. 5.10 Senzor teploty a vlhkosti vzduchu SHT30**  
(převzato z [30])

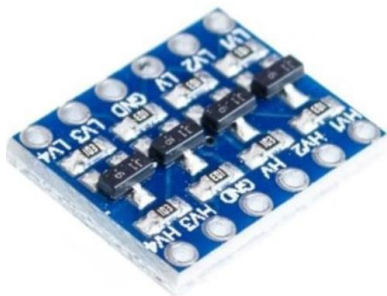
### **Převodník logických úrovní 5 V a 3,3 V**

Součástí modulů typu 1 je také převodník logických úrovní 5 V a 3,3 V (viz obr. 5.10). Jedná se o součástku zprostředkovávající obousměrný převod logických úrovní 5 V a 3,3 V a to až pro čtyři kanály. Tento převodník je součástí také modulu typu 2 a ústředny, vždy se však používá pouze jeden kanál, proto je ve schématu součástky zobrazen pouze jeden kanál (viz obr. 5.12). Ve schématu vidíme, že převodník má dva piny pro napájení: *LV* (zkratka low voltage) pro napájení části s 3,3V logickou úrovní a *HV* (zkratka high voltage) pro napájení části s 5V logickou úrovní. Ve skutečnosti má součástka také dva piny pro zem, ta je však v této práci spojena, proto je ve schématu vyznačena jen jedním pinem. U modulu typu 1 je

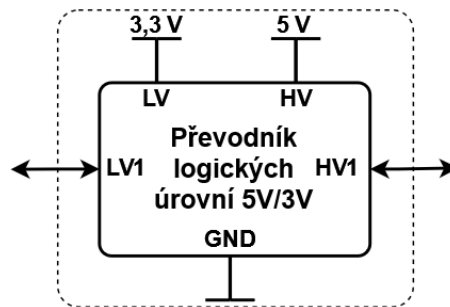
tento převodník použit kvůli tomu, že esp32 má 3,3V logiku, zatímco digitální výstup senzoru kvality ovzduší má 5V logiku. [28]

### Piezobzučák

Bzučák, v našem případě konkrétně piezobzučák (viz obr. 5.15), představuje akustický výstup vytvořeného systému. Jeho funkce v systému je akusticky upozornit na možné nebezpečí v případě, kdy senzor kvality ovzduší naměří nebezpečné hodnoty. To je důvod, proč je umístěn pouze v místnostech, kde se předpokládá zvýšená pravděpodobnost výskytu obyvatel chráněného objektu. Napájecí napětí se může pohybovat v rozmezí 3 V až 24 V a při bzučení součástka spotřebovává proud 10 mA. [27]



Obr. 5.11 Převodník logických úrovní 5V/3V (převzato z [28])



Obr. 5.12 Schéma převodníku logických úrovní 5 V a 3,3 V



Obr. 5.13 Piezobzučák (převzato z [27])

### Senzor teploty a vlhkosti vzduchu SHT30

Pro získávání údajů o teplotě a vlhkosti vzduchu se využívá senzor SHT30 (viz obr. 5.10). Jedná se o sensor, který se od konkurenčních výrobků liší především zkalirováním přímo z výroby a tím související přesností měření. Měřit teplotu a relativní vlhkost sice není potřeba s velkou přesností, ale např. konkurenční senzor DHT11 má při 25 °C přesnost měření teploty  $\pm 2$  °C (viz [32]), což jsem shledal nedostatečné. U senzoru SHT30 je udávaná přesnost měření teploty  $\pm 0,3$  °C a přesnost měření relativní vlhkosti (angl. relative humidity, zkráceně RH)  $\pm 3$  %. [30]

Naměřené hodnoty jsou posílány do mikrokontroléru prostřednictvím standardního protokolu I2C, který se realizuje za pomoci pinů SCL (zkratka angl. serial clock) a SDA (zkratka angl. serial data). Kromě těchto pinů má součástka pin pro zem a napájení, které se zde může pohybovat v rozmezí 2,4 V až 3,6 V. Průměrná spotřeba proudu je s ohledem na jiné části modulu (hlavně MQ-135) zanedbatelná, pohybuje se totiž v řádu desítek mikroampér. Pro představu spotřeba proudu celého modulu při light režimu spánku je cca 170 mA. [30]

### PIR detektor pohybu

Ke všem modulům typu 1 jsou připojeny PIR detektory pohybu, konkrétně PIR NC-SR501 (viz obr. 5.14), které jsou umístěny na zdi ve stejné místnosti. Tyto detektory pohybu mají tři vývody: zem, napájení (5V) a výstup. Jeho základní funkce je, že v případě detekce pohybu přepne na několik vteřin napětí na výstupním pinu z 0 V (logická 0) na 3 V (logická 1). Na začátku programu se čeká 60 s, protože PIR detektor potřebuje tento čas pro ustálení. Odpočet času je zobrazen na displeji (viz obr. 5.17). [38]



## Displej OLED 0,96“

Kromě LED a tlačítka modul typu 1 disponuje poslední komponentou, kterou je 0,96“ OLED displej (viz obr. 5.15). Tento displej je jednobarevný a má velmi malé rozměry (27×27×4,1 mm). Kromě pinu pro zem a napájení (lze napájet napětím 3,3 V až 5 V) má také dva piny (SDA a SCL) pro komunikaci. Ta se stejně jako u senzoru SHT30 realizuje prostřednictvím standardního protokolu I2C. Možnost spojení pinů SDA a SCL senzoru SHT30 a OLED displeje vyplývá z podstaty fungování sběrnice I2C, kdy na začátku komunikace mikrokontrolér specifikuje adresu zařízení, se kterým chce komunikovat. Funkce displeje je informovat o teplotě, relativní vlhkosti a kvalitě ovzduší (viz obr. 5.16). Displej se zapíná tlačítkem, konkrétně byl použit kolébkový přepínač (viz [50]).

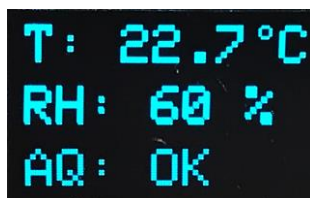


Obr. 5.14 Detektor pohybu, PIR NC-SR501 (převzato z [26])



Obr. 5.15 Displej OLED 0,96“ (převzato z [31])

Kvůli proudovému omezení jsou u vstupních pinů (GPIO14, GPIO25, GPIO26 a GPIO27) přidány 10kΩ odpory. K pinům GPIO14 a GPIO27 jsou navíc připojeny vnitřní pull-down rezistory a u pinu GPIO26 vnitřní pull-up rezistor (inverzní logika). Funkce těchto vnitřních rezistorů je zajištění určité logické hodnoty (např. při rozpojeném tlačítku by na pinu GPIO14 byla nedefinovaná hodnota). Odpor o hodnotě 560 Ω na pinu GPIO18 definuje proud diodou AQ.



Obr. 5.16 Zobrazení veličin na displeji



Obr. 5.17 Odpočet na displeji při inicializaci PIR detektoru

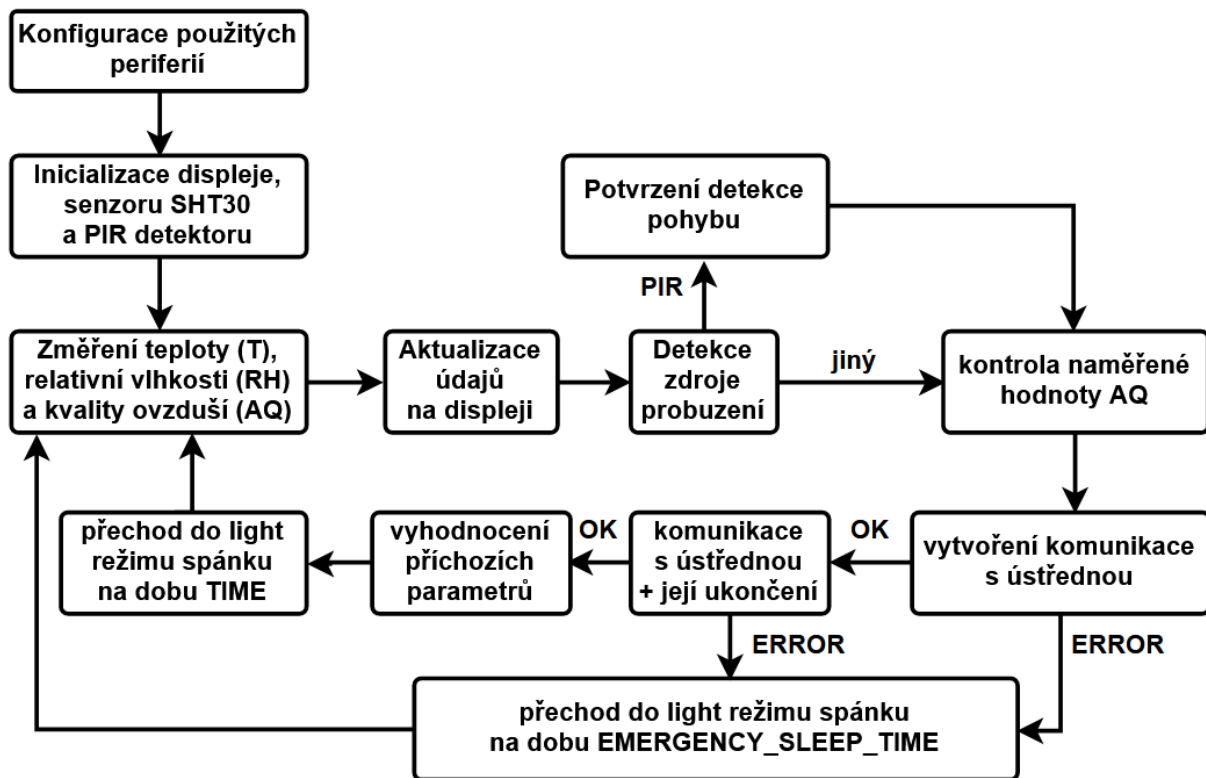


Obr. 5.18 Zobrazení varování na displeji

### 5.2.2 Program

Po předchozí kapitole by již mělo být jasné, jak je modul typu 1 zapojen a jaká je přibližně jeho funkce. V této kapitole se blíže podíváme na program, který v těchto modulech běží. Smyslem není tento program vysvětlit řádek po řádku, ale vyzdvihnout jeho základní fungování. Pro programování jsem používal Arduino IDE, proto jsou programy pro dané

moduly vždy složeny z minimálně jednoho souboru s koncovkou *.ino* a dále souborů s koncovkou *.cpp* a *.h*. Program v modulu typu 1 je složen ze souborů *client.ino*, *mydisplay.cpp*, *mydisplay.h*, *mysleep.cpp*, *mysleep.h*, *mywifi.cpp*, *mywifi.h* a *usefulMacros.h*. Nejdříve dojde k popisu souboru *client*, následují poznámky ke všem zbylým souborům a na závěr také k použitým sensorům.



Obr. 5.19 Vývojový diagram programu modulu typu 1

### Soubor *client*

Soubor *client.ino* představuje klíčovou část fungování celého programu modulu typu 1. Ostatní soubory poskytují rozšiřující funkce, které se v této části využívají. Fungování programu si vysvětlíme pomocí vývojového diagramu (viz obr. 5.19). Program začíná konfigurací použitých periférií (blok vlevo nahoře), což primárně zahrnuje nastavení pinů do příslušných módu, např. se aktivují vnitřní pull-down rezistory na pinech GPIO14 a GPIO27 a vnitřní pull-up rezistor na pinu GPIO26. Následuje inicializace displeje, senzoru SHT30 a PIR detektoru. Po připojení napájení PIR detektoru se čeká 60 s kvůli stabilizaci detektoru (viz [38]). Odpočet této doby je zobrazován na displeji (viz obr. 5.17). Po odpočtu 60 s program přechází do nekonečné smyčky.

Smyčka začíná změřením teploty, relativní vlhkosti a kvality ovzduší. Naměřené hodnoty se aktualizují na displeji. Poté se zjišťuje zdroj probuzení z light režimu spánku a v případě, kdy ho probudil PIR detektor, se detekce pohybu potvrzuje. Tento krok je zde přidán kvůli tomu, že vybraný PIR detektor (obr. 5.14) přeci jen nepředstavuje příliš spolehlivý způsob detekce pohybu. Pro minimalizování falešných poplachů je vyžadováno potvrzení detekce pohybu. Potvrzení se realizuje tak, že po první detekci pohybu musí přijít také druhá detekce

pohybu a to nejpozději za čas definovaný makrem *PIR\_DETECTION\_TIME\_s* (nastaveno na 30). Pokud k potvrzení nedojde, je první detekce pohybu označena za falešnou.

Následuje kontrola naměřené hodnoty AQ, vytváření komunikace s ústřednou, samotná komunikace (viz kap. 4.6) a její ukončení. V průběhu se může ledacos pokazit (viz dále), v takovém případě dojde k přechodu do light režimu spánku a to na dobu definovanou makrem *EMERGENCY\_SLEEP\_TIME\_s* (nastaveno na 15). Zopakujme, že klient posílané informace „nezapomíná“, ale snaží se je poslat znovu v dalším cyklu. Díky tomu se nemůžu stát, že by v případě problémů s komunikací došlo k detekci pohybu PIR detektorem a klient by tuto informaci nepředal ústředně. Pokud vše proběhlo v pořádku, dojde k vyhodnocení příchozích parametrů a nakonec k přechodu do light režimu spánku na dobu definovanou příchozím parametrem *TIME* (viz kap. 4.6). Tím je smyčka uzavřena.

### **Soubor mysleep**

Mikrokontrolér je uspáván do light režimu spánku (viz kap. 3.4.2) a je z něj probouzen dvěma způsoby: časovačem (angl. timer) nebo externím přerušením. Časovač je interní periferie fungující mmj. jako stopky. Od ústředny dostane MCU parametr *TIME* (viz 4.6), který definuje, na jak dlouho má přejít do režimu spánku. Funkcí časovače tedy je uspat MCU na dobu *TIME* a následně ho vzbudit – nastavit do aktivního režimu. Před uplynutím doby *TIME* může být mikrokontrolér vzbuzen externím přerušením. Jeho zdrojem mohou být piny GPIO14 (tlačítko) a GPIO26 (MQ-135) a pokud se systém nachází v pohotovostním režimu pak také pin GPIO27 (PIR).

### **Soubor mywifi**

Před samotným připojením k Wi-Fi ústředny se zjišťuje, zda je tato Wi-Fi vůbec dostupná a pokud ano, potom dojde k připojení. Připojení musí nastat za čas definovaný makrem *WIFI\_MAX\_CONNECTION\_TIME\_ms* (nastaveno na 7000). Následuje vytvoření TCP/IP komunikace a posílání parametrů. Klasicky se v HTTP požadavku posílají parametry *TEMP*, *RH* a *MQstate* (viz kap. 4.6). Pokud se systém nachází v pohotovostním režimu a dojde k detekci pohybu (a jeho potvrzení), pak je součástí také parametr *PIRalarm*. Případně ještě může být součástí požadavku parametr *MQalarm* a to v případě zjištění kritické hodnoty kvality ovzduší.

Ústředna musí na HTTP požadavek poslat HTTP odpověď a to nejpozději za čas definovaný makrem *MAX\_WAIT\_RESPONSE\_TIME\_ms* (nastaveno na 2500). Odpověď serveru by pro modul typu 1 měla být vždy stejná a měla by obsahovat parametry *PIR*, *ALARM*, *TIME* a *BOARD* (viz kap. 4.6). Pokud dojde k neobdržení odpovědi v daném čase, nebo k přijetí odpovědi v nesprávném formátu, HTTP požadavek se odešle znovu. Maximální počet opakování definuje makro *MAX\_SEND\_REQUEST\_ATTEMPTS* (nastaveno na 3).

## Soubor `usefulMacros`

V souboru `usefulMacros` jsou definovány piny připojených komponent a klíčová makra. Kromě již zmíněných maker zde najdeme např. definice důležitých maker pro práci s MQ-135. Jedná se o:

- **`MQ135_INIT_TIME_min`**: Jedná se o tzv. dobu předehřátí. Po uplynutí této doby (od začátku programu) dojde ke kalibraci hodnoty odporu vrstvy oxidu cíničitého a změření referenční hodnoty koncentrace skupiny plynů. Podle manuálu by doba předehřátí měla být 24 hodin (viz [39]).
- **`MQ135_ATTENTION_level`**: Spodní hranice oblasti 2 (BAD) vyjádřena v násobcích referenční hodnoty koncentrace skupiny plynů. Experimentálně jsem tuto hranici stanovil na 5, což představuje poměrně velký rozptyl měřené koncentrace.
- **`MQ135_DANGER_level`**: Horní hranice oblasti 2 (BAD), která je opět vyjádřena v násobcích referenční hodnoty koncentrace skupiny plynů. Experimentálně jsem tuto hranici stanovil na 15. Patnáctinásobek referenční koncentrace skupiny plynů je sice hodně, ale v případě požáru by se měla naměřit koncentrace skupiny plynů i několikrát vyšší. Nastavení vyšší hodnoty tohoto makra zmenšuje výskyt falešných poplachů (MQ alarmů).
- **`MQ135_DANGER_level_value_ppm`**: Hraniční hodnota naměřené koncentrace skupiny plynů pro vyhlášení MQ alarmu v případě, kdy ještě neuplynula doba `MQ135_INIT_TIME_min`. Experimentálně stanoveno na 15000. Pokud by tedy neuplynula doba předehřátí, ale změřená koncentrace skupiny plynů by byla vyšší než je hranice definovaná tímto makrem, potom by i tak došlo k vyhlášení k MQ alarmu.

## Soubor `mydisplay`

Obsahuje funkce pro práci s OLED displejem. Základem je knihovna `Adafruit_SSD1306` (viz [35]). Na displeji se zobrazují naměřené veličiny (viz obr. 5.16), odpočet při inicializaci PIR senzoru (viz obr. 5.17) nebo varování při vyhlášení MQ alarmu (viz obr. 5.18). U varování se na displeji zobrazí označení modulu, který MQ alarm vyvolal. Na obr. 5.18 alarm vyvolal modul 5 (board5) – modul typu 2 umístěný v kotelně (viz obr. 4.2).

## Poznámky k SHT30 a MQ-135

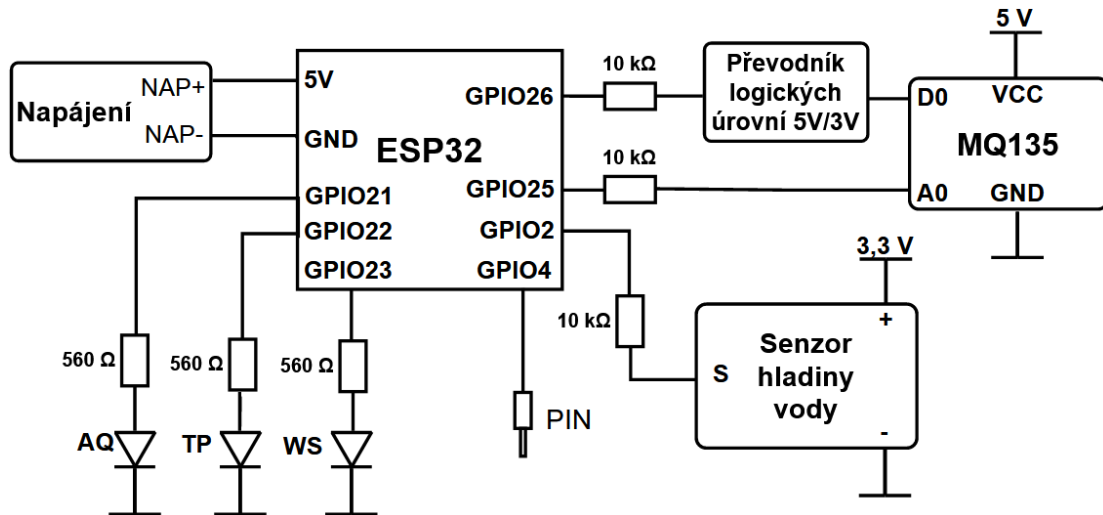
Na závěr této kapitoly je ještě nutné zmínit knihovnu `Adafruit_SHT31` (viz [37]) navrženou pro práci se senzorem SHT31, ale fungující i pro práci se senzorem SHT30. Dále je nutné zmínit knihovnu `MQ135` (viz [36]) navrženou pro práci s Arduino mikrokontroléry. Já jsem tuto knihovnu využil a provedl drobnou změnu, která ji umožňuje použít i pro mikrokontroléry s 3,3V logikou. Upravil jsem funkci `getResistance()` v souboru `MQ135.cpp`. Konkrétně jsem změnil výsledný výpočet a přidal průměrování z deseti vzorků. Upravená funkce vypadá následovně:

```
float MQ135::getResistance() {
    int val = 0;
    for (uint8_t loop = 0; loop < 10; loop++){
```

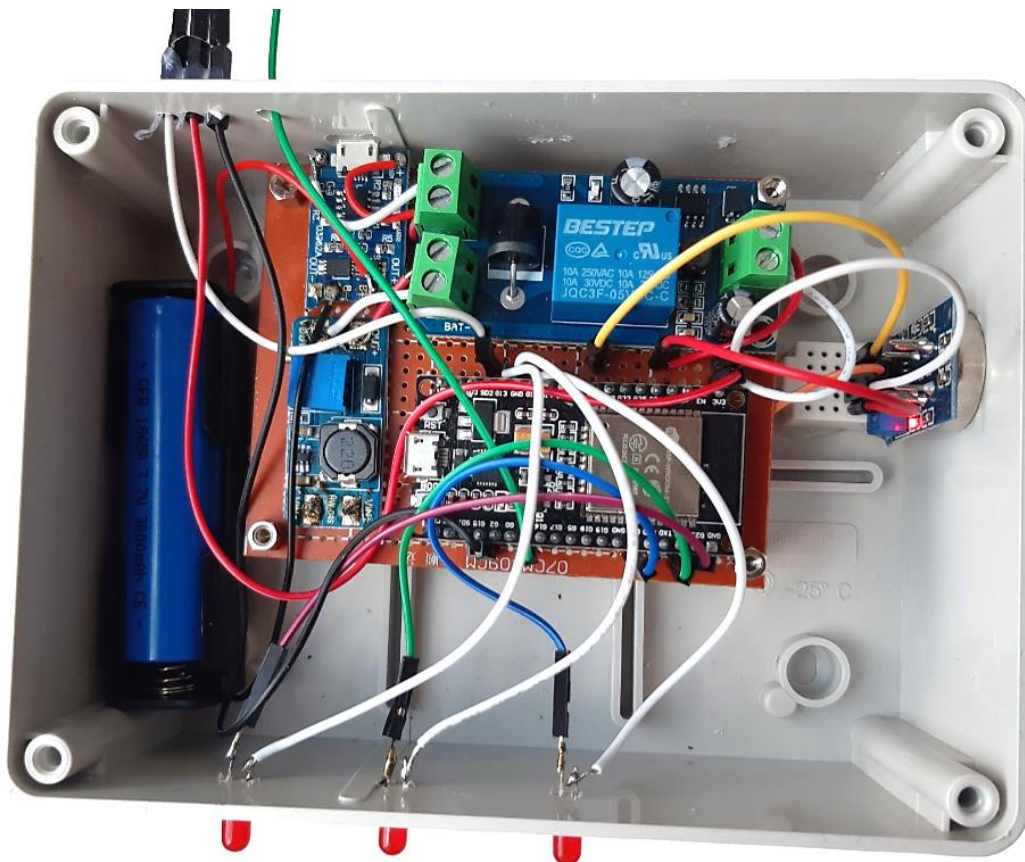
```

val += analogRead(_pin);
delay(25); // wait 25 ms
}
float result = ( ( 4095./(float) (val/10) ) - 1.)*RLOAD;
return result;
}

```



Obr. 5.20 Schéma zapojení klienta 5



Obr. 5.21 Realizovaný modul typu 2



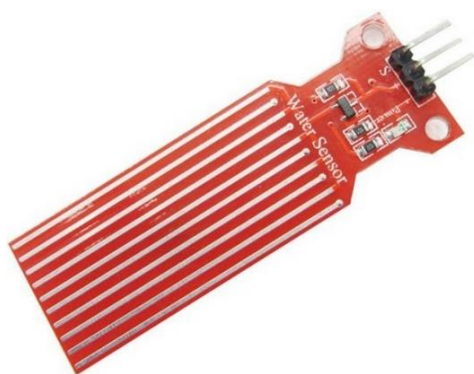
## 5.3 Modul typu 2

### 5.3.1 Zapojení

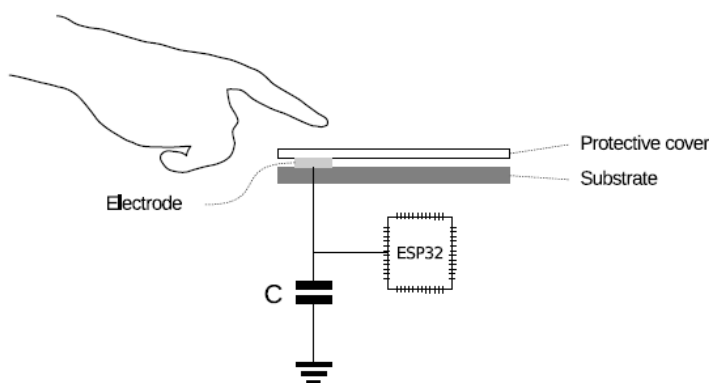
Schéma zapojení modulu typu 2 (též označovaný jako klient 5) je velmi podobné schématu zapojení modulu typu 1 (viz obr. 5.20 a obr. 5.8). Realizaci modulu vidíme na obr. 5.21. Modul typu 2 je umístěn v kotelně a z toho vyplývají i rozdíly mezi těmito moduly. V kotelně nás příliš nezajímá teplota ani relativní vlhkost, proto chybí STH30 a displej. Není-li displej, není potřeba tlačítko. Dále se v této místnosti zpravidla nenachází obyvatelé chráněného objektu, z tohoto důvodu není potřeba bzučák. Jedná se o vnitřní místnost, proto v ní také není umístěn PIR detektor pohybu.

Na druhou stranu se jedná o místnost, ve které se nachází plynový kotel a boiler. Kvůli plynovému kotli na zemní plyn se v modulu ponechává senzor kvality ovzduší MQ-135. Ten by měl upozornit na kouř, zemní plyn či na plyny vzniklé nedokonalým spalováním (typicky oxid uhelnatý). Experimentálně bylo vyzkoušeno, že senzor MQ-135 detekuje kouř i zemní plyn. Chování v reálných podmínkách je však bezpochyby diskutabilní. Základním prvkem zemního plyn je metan a ten je lehčí než vzduch, proto je vhodné modul instalovat ke stropu. Stejně je tomu i s oxidem uhelnatým. Modul typu 2 by tedy bylo vhodné instalovat ke stropu.

Jelikož se v kotelně nachází také boiler, bylo by vhodné detekovat únik vody, který by mohl nastat v případě jeho porušení. Únik vody lze detekovat několika způsoby. Já jsem si vybral dva způsoby, přičemž první by se dal nazvat jako tradiční a druhý jako netradiční. První z nich je založen na použití senzoru hladiny vody fungujícím na kapacitním principu a druhý na použití pinu v módu detekce dotyku. Použitý mikrokontrolér esp32 disponuje dotykovým senzorem, který může podporovat až 10 pinů nastavených najednou do tzv. dotykového kapacitního režimu. [41]



Obr. 5.22 Senzor vodní hladiny  
(převzato z [40])



Obr. 5.23 Dotykový senzor  
(převzato z [41])

Systém dotykového senzoru je postaven na substrátu, na kterém se nachází elektrody a ochranná vrstva (viz obr. 5.23). Detekce dotyku funguje na kapacitním principu, při kterém se periodicky nabíjí a vybíjí kondenzátor u vybraného pinu. Při tomto procesu se zároveň měří napětí na tomto kondenzátoru a z jeho průběhu se dotyk detekuje. Voda z vodovodního kohoutku tento výstup také ovlivní. Z toho vyplývá, že lze využít pin nastavený v módu detekce dotyku také k detekci přítomnosti vody. Navíc se jedná o jednodušší řešení z hlediska

použití, jelikož stačí pouze připojit kabel a přivést ho na připravené místo. Naopak použití komplikuje časová nestálost kabelu, která by mohla po určité době způsobit nefunkčnost vytvořeného řešení. Z tohoto důvodu by bylo vhodné vyzkoušet funkčnost v delším časovém období (např. několika let). Kromě toho by bylo v programu potřeba upravit hodnoty spojené s detekcí vody pro konkrétní použitý kabel. U senzoru vodní hladiny je při instalaci potřeba zajistit, aby se voda nedostala na horní část tohoto senzoru, kde se nachází součástky. [41]

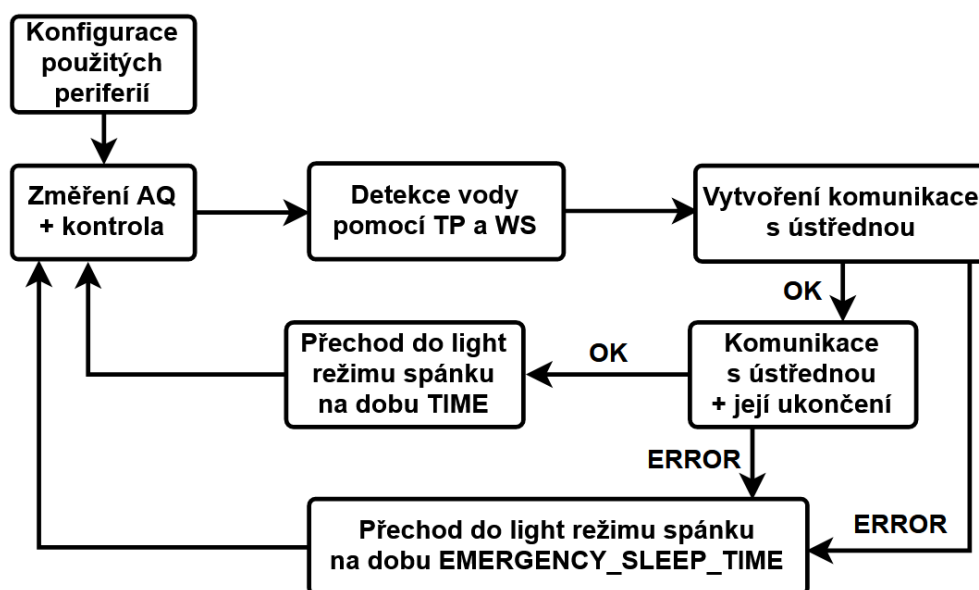
Senzor vodní hladiny má tři piny: zem, napájení (může být 3 V až 5 V) a analogový výstup. Tři vodiče vlevo nahoře na obr. 5.21 vedou k senzoru vodní hladiny a zelený vodič vedle nich je nastaven v detekci dotyku. Kromě LED AQ jsou zde navíc LED nazvané TP (touchpad) a WS (water sensor), které se rozsvítí v případě detekce vody daným způsobem. Všechny rezistory opět plní funkci omezení proudu do nebo z daného pinu. Spotřeba proudu celého modulu při light režimu spánku je cca 160 mA.

### 5.3.2 Program

Funkce modulu typu 2 je velmi podobná jako modulu typu 1, proto je velmi podobný i vytvořený program. Program pro modul typu 2 se skládá ze souborů *client\_kotelna.ino*, *mysleep.cpp*, *mysleep.h*, *mywifi.cpp*, *mywifi.h* a *usefulMacros.h*.

#### Soubor *client\_kotelna*

Vývojový diagram programu vidíme na obr. 5.24. Na začátku musí opět proběhnout konfigurace použitých periférií. Po ní ihned následuje nekonečná smyčka. Nekonečná smyčka se skládá ze změření a kontroly AQ, detekce úniku vody pomocí TP a WS a vytvoření komunikace s ústřednou. Následuje samotná komunikace a její ukončení. V průběhu komunikace se může ledacos pokazit (viz kap. 5.2.1). V takovém případě dojde k přechodu do light režimu spánku a to na dobu definovanou makrem *EMERGENCY\_SLEEP\_TIME\_s* (nastaveno na 15). Pokud vše proběhlo v pořádku, dojde k vyhodnocení příchozích parametrů a nakonec k přechodu do light režimu spánku na dobu definovanou příchozím parametrem *TIME* (viz kap. 4.6). Tím je smyčka uzavřena.



Obr. 5.24 Vývojový diagram programu modulu typu 2

## Soubor mysleep

Mikrokontrolér je opět uspáván do light režimu spánku (viz kap. 3.4.2) a je z něj probouzen dvěma způsoby: časovačem nebo externím přerušením. Časovač uspi mikrokontrolér na dobu definovanou parametrem *TIME*, kterou klient 5 získá v průběhu komunikace s ústřednou. Před uplynutím doby *TIME* může být MCU vzbuzen externím přerušením, jehož zdrojem může být v tomto případě pouze pin GPIO26 (MQ-135). TP ani WS tedy mikrokontrolér z režimu spánku nevzbudí.

## Soubor mywifi

Komunikace s ústřednou probíhá stejně jako u modulu typu 1 (viz kap. 5.2.2). Rozdíl je v parametrech, které si mezi sebou klienta 5 a ústředna posílají. Standardně klient 5 posílá v HTTP požadavku pouze parametr *MQstate*. V případě naměření kritické hodnoty AQ posílá také *MQalarm* a v případě detekce úniku vody pomocí TP nebo WS posílá parametry *TPleak* nebo *WSleak*. Od serveru v HTTP odpovědi modul dostane pouze parametr *TIME*.

## Soubor usefulMacros

V souboru *usefulMacros* jsou opět definovány piny připojených komponent a klíčová makra. Kromě již zmíněných maker zde najdeme makra:

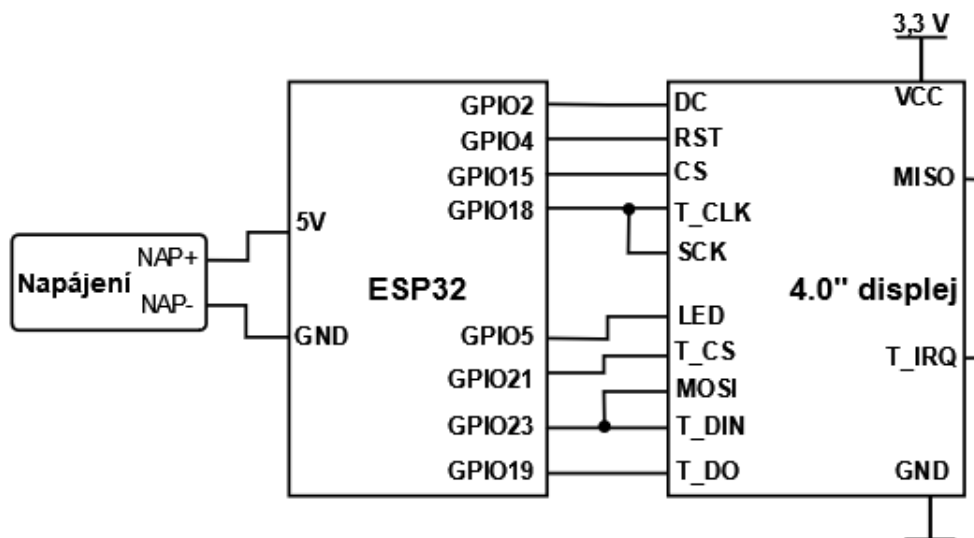
- ***TP\_THRESHOLD***: Při použití TP se vyhodnocuje hodnota dotykového senzoru pomocí funkce *touchRead()*. Pokud se pinu dotkneme, funkce vrátí nižší hodnotu. V případě, kdy funkce *touchRead()* vrátí hodnotu menší než je *TP\_THRESHOLD*, je situace vyhodnocena jako únik vody. Hodnota makra byla stanovena experimentálně na 45. Tato hranice by se měla při použití v reálné aplikaci experimentálně zjistiť a navíc by se měla její hodnota v průběhu času upravovat kvůli časové nestálosti připojeného kabelu.
- ***WS\_THRESHOLD***: Jedná se o hraniční hodnotu WS, kterou lze přepočítat na napětí. Za standardních podmínek je na výstupu WS napětí 0 V a při kontaktu s vodou se napětí zvětšuje. Experimentálně jsem hranici nastavil na 250, což lze přepočítat na napětí cca 0,2 V  $((250/4095)*3,3)$ . Hranice je zvolena dostatečně velká na to, aby nedocházelo k falešným poplachům. Při stanovování této hranice je navíc potřeba zohlednit fakt, že ADC mikrokontrolérů esp32 mívají velkou chybu měření, o čemž jsem se sám experimentálně přesvědčil.



## 5.4 Modul s displejem

### 5.4.1 Zapojení

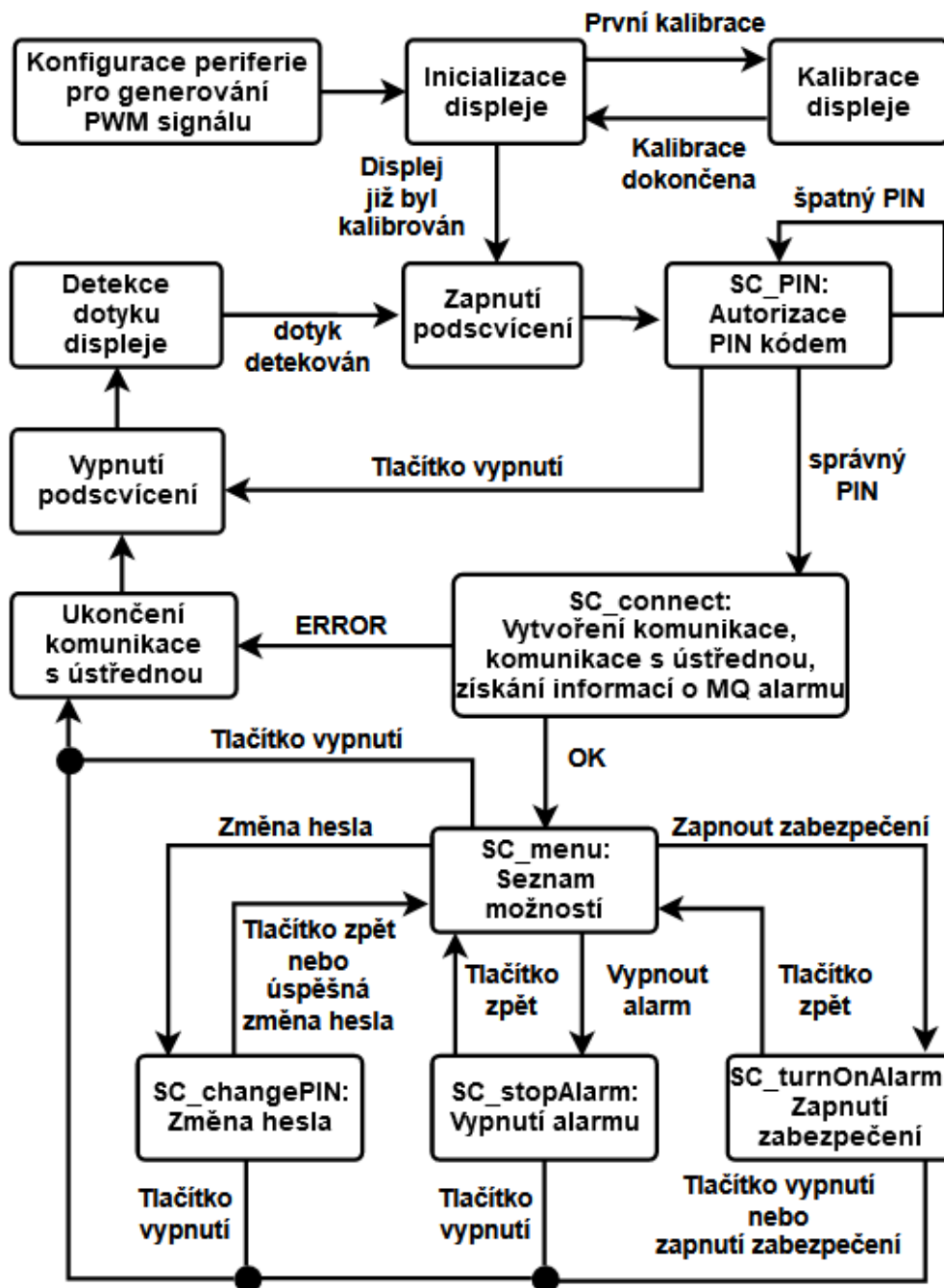
Poslední klient systému je klient 6, který je na obr. 4.2 označen jako modul s displejem pro ovládání systému. Modul disponuje dotykovým 4.0" displejem s rozlišením 480x320 bodů, pracovním napětím 3,3 V až 5 V a SPI komunikačním rozhraním (viz [42]). Již zabudovaný displej na horní části modulu vidíme na obr. 5.26. Modul v systému vykonává dvě důležité funkce, kterými jsou autorizace uživatele a přístupový bod do vytvořeného systému. Klient 6 je složen z napájení, řídicího mikrokontroléru esp32 a dotykového displeje (viz obr. 5.25).



Obr. 5.25 Schéma zapojení klienta 6



Obr. 5.26 Pohled shora na klienta 6



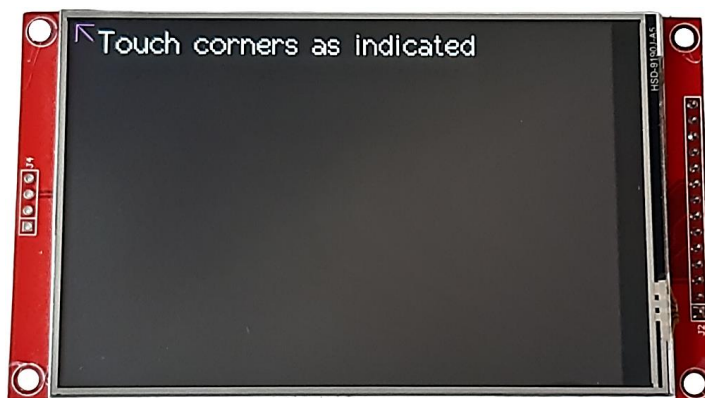
Obr. 5.27 Vývojový diagram programu modulu s displejem

## 5.4.2 Program

Program je složen ze souborů *client\_displej.ino*, *calibration.ino*, *myscreen.cpp*, *myscreen.h*, *mywifi.cpp*, *mywifi.h* a *usefulMacros.h*. Můžeme si všimnout, že program neobsahuje soubor *mysleep.cpp*. Mikrokontrolér není uspáván do light režimu spánku, ale je využito snížení frekvence procesoru z 240 MHz na 80 MHz při zapnutém displeji a na 10 MHz při vypnutém displeji. Spotřeba proudu celého modulu při vypnutém displeji je cca 60 mA a při zapnutém displeji cca 160 mA.

## Soubor client\_displej

Program si opět vysvětlíme na vývojovém diagramu (viz obr. 5.27). Napětí na pinu LED ovlivňuje jas displeje. Přivedením PWM signálu na tento pin a změnou jeho střídy lze měnit jas v průběhu programu. Z časových důvodů jsem funkci změny jasu nepřidal, ale změnu střídy PWM signálu využívám při vypnutí a zapnutí displeje. Při vypínání displeje se střída nastaví na 0 %, což minimalizuje proudový odběr. Při zapínání se naopak nastaví na 100 %. Program začíná konfigurací periferie pro generování PWM signálu (blok vlevo nahoře). Následuje inicializace displeje, a pokud displej nebyl doposud kalibrován, pak se provede také jeho kalibrace. Kalibrace se realizuje pouze jednou a to postupným dotykem na všechny rohy displeje (viz obr. 5.28). Poznamenejme, že uživatel je v průběhu práce s displejem informován o všech důležitých dílčích stavech.



Obr. 5.28 Kalibrace displeje

Po kalibraci program vstupuje do nekonečné smyčky. Zapne se podsvícení displeje a automaticky se přejde do obrazovky označené jako *SC\_PIN* (*SC* je zkratka pro screen), kterou vidíme na obr. 5.26. V tomto stavu se uživatel autorizuje zadáním čtyřmístného PIN kódu na klávesnici. Pokud je PIN správný, je o tom uživatel informován a klient se začne připojovat k ústředně. V opačném případě je o tom také uživatel informován, ale program zůstává ve stavu *SC\_PIN*. Omezení pokusů jsem neimplementoval, jelikož čas na zadání správného kódu je omezený, tedy to vlastně není potřeba (viz kap. 5.5.2). V pravém dolním rohu je tlačítko pro vypnutí displeje, které způsobí vypnutí podsvícení a přechod do stavu detekce dotyku. Po detekci dotyku se podsvícení znovu zapne a program přejde do právě probíraného stavu *SC\_PIN*, čímž dojde k uzavření smyčky.

Po zadání správného hesla se na displeji zobrazí obrazovka *SC\_connect* a proběhne připojování k ústředně, což může být úspěšné (viz obr. 5.29) nebo neúspěšné (viz obr. 5.30). V případě vytvoření komunikace ihned dojde k první výměně parametrů, při které klient 6 dostane od serveru parametry *ALARM* a *BOARD* (viz kap. 4.6). Program dále přejde do stavu *SC\_menu*. Pokud při vytváření komunikace nebo v jejím průběhu nastane chyba, mikrokontrolér vypne podsvícení displeje a vstoupí do stavu detekce dotyku, čímž je opět smyčka uzavřena.

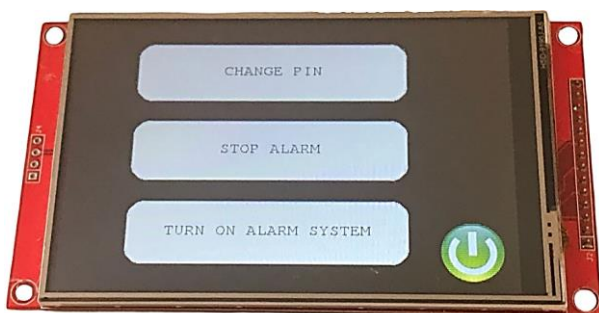


Obr. 5.29 Úspěšné připojení na server



Obr. 5.30 Neúspěšné připojení na server

Ve stavu *SC\_menu* má uživatel možnost vybrat si ze tří možností: změna PIN kódu, zastavení alarmu (MQ alarmu) a zapnutí zabezpečení (viz obr. 5.31). Zároveň existuje možnost vypnutou displej vypínacím tlačítkem, což nově navíc před vypnutím podsvícení způsobí ukončení komunikace s ústřednou. Po vybrání první možnosti se přejde do stavu *SC\_changePIN*, ve které lze změnit PIN (viz obr. 5.32). Proces změny PIN kódu je jednoduchý, napíše se nový PIN, který je z bezpečnostních důvodů potřeba vložit ještě jednou. Pokud se oba napsané PIN kódy shodují, PIN je úspěšně změněn a program automaticky přejde zpět do stavu *SC\_menu*. Kromě vypínacího tlačítka se zde nachází také tlačítko zpět umožňující přechod zpátky do menu nabídky.



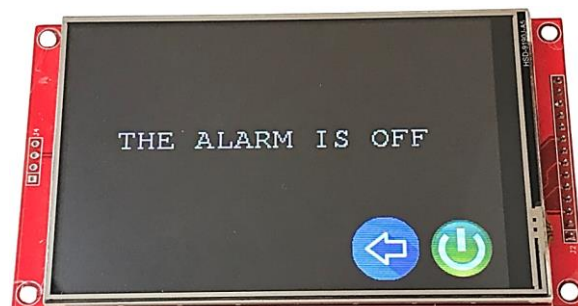
Obr. 5.31 Seznam možností



Obr. 5.32 Změna hesla



Obr. 5.33 Vypnutí MQ alarmu



Obr. 5.34 MQ alarm je vypnutý

Druhou možnost z menu nabídky vidíme na obr. 5.33 a na obr. 5.34. Jedná se o stav *SC\_stopAlarm*, který využívá již od ústředny získané parametry *ALARM* a *BOARD*. MQ alarm je aktivní za podmínky, že je hodnota parametru *ALARM* rovna 1. Na displeji se zobrazí stav z obr. 5.33 pokud je MQ alarm aktivní. Součástí zobrazení je také informace o tom, který modul MQ alarm vyvolal. V tomto případě ho vyvolal modul 5 (board5) – modul typu 2 umístěný v kotelně (viz obr. 4.2). Tuto informativní funkci měly již moduly typu 1,



keré pro tento účel využívaly OLED displej. Zde je však navíc možnost MQ alarm deaktivovat, což se provede zmáčknutím tlačítka „STOP ALARM“, které vyšle serveru HTTP žádost s parametrem *STOP\_ALARM*. Po obdržení HTTP odpovědi s parametrem *SA\_OK* se na displeji objeví hláška „SERVER INFORMED“. Pokud MQ alarm není aktivní je o této skutečnosti uživatel také informován (viz obr. 5.34).

Poslední možností v menu nabídky je zapnutí zabezpečení, tedy stav *SC\_turnOnAlarm*. Zapnutí zabezpečení je umožněno pouze za podmínky, že je smyčka plášt'ové ochrany spojena, tzn. dveře a všechny okna jsou zavřené. Tento případ vidíme na obr. 5.35. Hláška „SERVER INFORMED“ je zobrazena po zmáčknutí tlačítka „TURN ON ALARM SYSTEM“ a následném přijetí správné odpovědi od serveru (viz dále). Po zobrazení této hlášky následuje 4s zpoždění, aby si uživatel mohl informaci přečíst. Poté se displej již probraným způsobem vypne (ukončení komunikace, atd.). Pokud je smyčka plášt'ové ochrany rozpojena, není možné zabezpečení zapnout, přičemž na displeji se zobrazí upozornění (viz obr. 5.36). Ze stavu *SC\_turnOnAlarm* je opět možné přejít do menu tlačítkem zpět a také je možné displej vypnout zeleným tlačítkem.



Obr. 5.35 Zapnutí zabezpečení umožněno



Obr. 5.36 Zapnutí zabezpečení neumožněno

### Soubory calibration, myscreen a usefulMacros

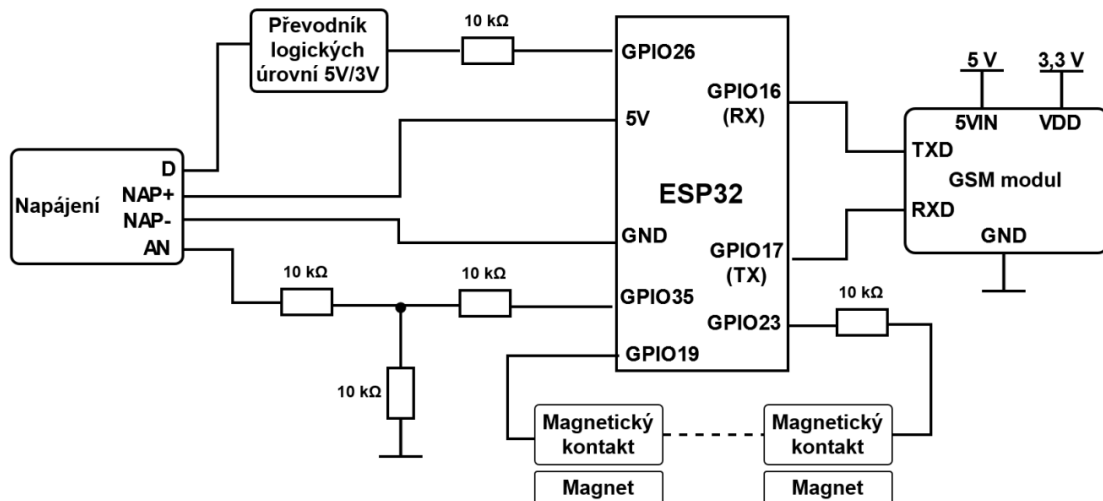
Soubor *calibration.ino* obsahuje pouze funkci na kalibraci displeje, která je převzata z ukázkového programu *Keypad\_480x320.ino* knihovny *TFT\_eSPI* (viz [43]). Obecně je na této knihovně postavena celá práce s použitým TFT displejem. Poznamenejme, že pro použití zmíněné knihovny na vybraný displej je nutné definovat příslušná makra v souboru *User\_Setup.h* (makro *ILI9486\_DRIVER* a makra definovaná za komentářem „For ESP32 Dev board“). V souboru *mymScreen.cpp* jsou implementovány funkce pro jednotlivé stavy programu (*SC\_PIN*, *SC\_connect*, apod.). V souboru *usefulMacros.h* jsou opět definována klíčová makra, přičemž význam všech použitých maker byl již vysvětlen v předchozích kapitolách.

### Soubor mywifi

Komunikace s ústřednou je u klienta 6 trochu odlišná, než tomu bylo u jiných klientů. Klient se na Wi-Fi ústředny připojí po zadání správného PIN kódu a připojen zůstává, dokud není displej vypnut. Komunikace mezi klientem 6 a ústřednou:

- Po zadání správného PIN kódu se posílá serveru žádost s parametrem *INIT* a v odpovědi přichází parametry *ALARM* a *BOARD*.

- Pro vypnutí MQ alarmu posílá klient parametr *STOP\_ALARM* a v odpovědi od serveru dostane parametr *SA\_OK*.
- Při zvolení možnosti zapnutí zabezpečení ve stavu *SC\_menu* se klient dotazuje parametrem *MAGN\_CON* na aktuální stav smyčky plášťové ochrany. Na tuto zprávu server pošle odpověď s parametrem *MAGN\_CON* a příslušným stavem (0 ~ smyčka je rozpojena).
- Poslední parametr, který klient v HTTP žádosti posílá, je *TURN\_ON*. Server na žádost s tímto parametrem posílá odpověď s parametrem *TURN\_ON\_OK*.



Obr. 5.37 Schéma zapojení ústředny

## 5.5 Ústředna

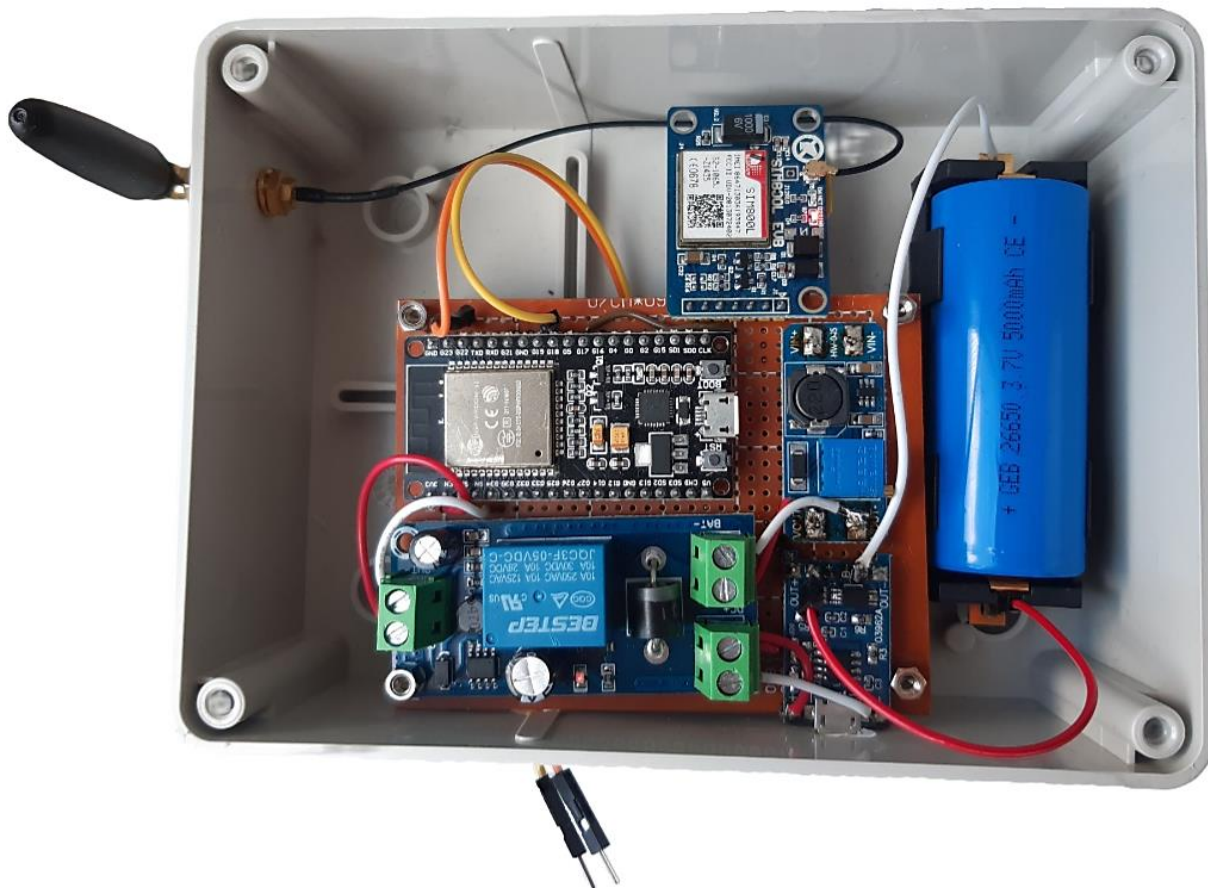
### 5.5.1 Schéma

Schéma zapojení ústředny vidíme na obr. 5.37 a realizovaný modul na obr. 5.38. Ústředna má v porovnání s ostatními vytvořenými moduly trochu jiný blok pro napájení, jelikož kromě pinů *NAP+* a *NAP-* má také piny *D* a *AN* (viz kap. 5.1). Pomocí pinu *D* si mikrokontrolér zjišťuje aktuální zdroj napájení. Pokud je zdrojem napájení elektrická síť, na pinu *D* se naměří napětí 5 V. Toto napětí se dále pomocí převodníku logických úrovní převede na 3V logiku. Pinem *AN* si mikrokontrolér měří napětí na baterii. Maximální napětí na použité Li-Ion baterii je přibližně 4,2 V, zatímco maximální povolené vstupní napětí interního ADC je 3,3 V. Z tohoto důvodu bylo nutné přidat dělič napětí, který zmenší napětí baterie na polovinu, čímž sníží maximální napětí na baterii na hodnotu 2,1 V. V programu je následně samozřejmě potřeba naměřenou hodnotu napětí na pinu GPIO35 zdvojnásobit. U pinů GPIO26 a GPIO35 je opět umístěn 10 kΩ odpor.

### Magnetické kontakty

Další část ústředny představuje bezpečnostní smyčka tvořená magnetickými kontakty (viz [51]), která zajišťuje plášťovou ochranu. Pokud jsou dveře a všechny okna zavřené, smyčka je spojena. Tento stav se otestuje jednoduše tak, že se na pin GPIO19 přivede logická 1 (tedy 3,3 V) a na pinu GPIO23 se zjišťuje logická hodnota. Při reálném použití je potřeba uvažovat úbytky napětí na vedení a tomu vhodně přizpůsobit zakončovací odpor definující

přůchozí proud. Já jsem jako zakončovací odpor použil  $10k\Omega$  odpor. Smyčka s magnetickými kontakty se připojí na vodiče, které vidíme v dolní části na obr. 5.38.



Obr. 5.38 Realizovaný modul – ústředna

### GSM modul

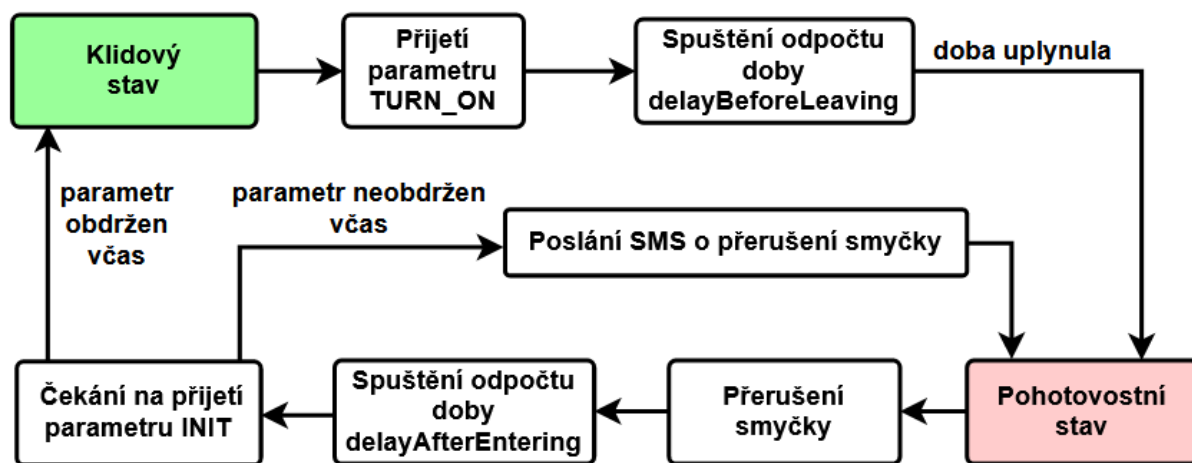
Klíčovou součástí ústředny je GSM modul, který zprostředkovává připojení k mobilní síti. Těchto modulů existuje mnoho variant, které se od sebe mohou značně lišit. Typický problém při použití GSM modulu je zajištění dostatečně stabilního zdroje napájení, jelikož spotřeba proudu bývá poměrně vysoká. Tento problém nastává zejména při připojování do sítě, kdy se může špičková hodnota proudu pohybovat např. i kolem hodnoty 2 A. Řešení bývá připojení dostatečně velkého kapacitoru (např.  $1000\ \mu\text{F}$ ) a napěťového stabilizátoru na napájecí napětí. Obě řešení však mohou být již integrovaná na GSM modulu, pokud vybereme ten správný. Mnou vybraný GSM modul je označen jako GPRS GSM Module SIM800L (viz [44]) a disponuje již zabudovaným  $1000\ \mu\text{F}$  kondenzátorem a 5V napěťovým stabilizátorem. K modulu se připojuje externí anténa a ústředna s modulem komunikuje pomocí sériové komunikace (piny TXD a RXD). Napájecí napětí je 5 V, ale na modulu je integrovaný převodník logických úrovní, který umožňuje realizovat komunikaci s mikrokontrolérem na 3,3V logice. Anténu a GSM modul vidíme v horní části obr. 5.38.

### 5.5.2 Stav systému

Před vysvětlováním samotného programu ústředny by bylo vhodné ujasnit, v jakých stavech se vytvořený systém může nacházet a jaké jsou mezi těmito stavy přechody. Systém se může

nacházet v klidovém anebo pohotovostním stavu. Rozdíl mezi nimi je v aktivovaných ochranách chráněného objektu. Klidový stav je stav, kdy jsou obyvatelé chráněného objektu uvnitř, tedy plášťová a prostorová ochrana není aktivní. Naopak v pohotovostním stavu je chráněný objekt prázdný a systém hlídá bezpečnostní smyčku realizovanou magnetickými kontakty a detekci pohybu pomocí PIR detektorů.

Pro přechod mezi stavy je klíčový modul s displejem. Před odchodem z objektu je potřeba zabezpečení zapnout na displeji (viz kap. 5.4.2). Ústředna obdrží parametr *TURN\_ON* a začne odpočítávat dobu definovanou makrem *DELAY\_AFTER\_LEAVING* (nastaveno na 30 s). Po uplynutí této doby systém přejde do pohotovostního stavu. Naopak z toho stavu se systém dostane přerušením smyčky, čímž by mělo být otevření vstupních dveří. Poté je potřeba se autorizovat zadáním PIN kódu na displeji, načež ústředna obdrží parametr *INIT* a přejde do klidového stavu. Autorizaci je nutné provést do doby definované makrem *DELAY\_AFTER\_ENTERING* (nastaveno na 30 s), jinak se pošle SMS o narušení plášťové ochrany.



Obr. 5.39 Stav systému a přechody mezi nimi

### 5.5.3 Program

Program ústředny je rozdělen do souborů *server.ino*, *GSMmodule.cpp*, *GSMmodule.h*, *myblynk.cpp*, *myblynk.h* a již tradičně *usefulMacros.h*. Ústředna stejně jako modul s displejem nepřechází do light režimu spánku. Po ústředně bychom chtěli, aby při výpadku napájení z elektrické sítě vydržela na záložní baterii co nejdéle. Použitý mikrokontrolér esp32 však nedisponuje žádným uspávacím režimem, do kterého by mohl MCU přejít a zároveň si zachoval možnost generovat vlastní Wi-Fi – fungovat jako AP. Mikrokontrolér je proto neustále v aktivním režimu, ve kterém generuje vlastní Wi-Fi. Spotřeba proudu za těchto podmínek je vysoká, pohybuje se kolem 240 mA. I když není možné prodloužit dobu výdrže na baterii využitím některého z uspávacích režimů, lze použít i jiný softwarový způsob. Snížení hodinové frekvence procesoru z 240 MHz na 80 MHz sníží spotřebu proudu z 240 mA na cca 200 mA, což je poměrně dobrý výsledek na jeden řádek kódu:

```
setCpuFrequencyMhz(80); // decrease CPU frequency -> everything else works the same
```



## Nastavení serveru

Server se v programu nastaví pomocí funkce zpětného volání (angl. callback functions) a dále není potřeba žádné řízení ani dotazování spojené s činností serveru. Vše zajišťuje samotná knihovna. Veškeré nastavení serveru se realizuje metodou *on()* na objektu serveru:

```
server.on(route, HTTP_GET, [] (AsyncWebServerRequest * request){}
```

První argument metody *on()* je řetězec, který slouží pro server jako identifikátor cesty. V programu jsou použity jednoduché řetězce `"/board1"` až `"/board6"`, přičemž s jejich pomocí dochází k identifikaci klienta. Druhý argument je výčtový typ `HTTP_GET` specifikující, že server přijímá pouze HTTP GET požadavky. Poslední parametr je funkce definovaná pomocí tzv. lambda syntaxe: [10]

```
[captures](params){body}
```

Kupříkladu kód pro nastavení serveru s identifikátorem `"/board1"` vypadá následovně:

```
server.on("/board1", HTTP_GET, [] (AsyncWebServerRequest * request) {  
    esp_task_wdt_reset(); // reset watchdog  
    // send a response if the request has a known parameter  
    if (parseRequest(request, 1)) {  
        sendResponse(request, 0);  
    }  
    uploadToCloud(1); // update parameters  
});
```

Tímto krátkým kódem se nastaví, že v případě obdržení HTTP GET žádosti s identifikátorem „board1“ se resetuje WDT, příchozí zpráva se rozdělí na jednotlivé parametry, na zprávu se pošle odpověď a data se pošlou na cloud. Server na žádost klienta posílá HTTP odpověď, což realizuje metoda *send()* objektu žádosti: [10]

```
request->send(200, "text/plain", responseMsg);
```

První argument je HTTP kód odpovědi, který v bezproblémovém případě nabývá hodnoty 200. Druhý specifikuje typ obsahu odpovědi a třetí je samotná odpověď. Konkrétní odpovědi se liší podle toho, s jakým klientem server komunikuje (viz kap. 4.6). [10]

Na závěr je potřeba server spustit metodou *begin()*:

```
server.begin();
```

## Soubor server

Fungování programu si vysvětlíme na vývojovém diagramu (viz obr. 5.40). Program začíná již tradičně konfigurací použitých periférií (piny, frekvence procesoru, apod.). Následuje načtení stavu systému z EEPROM, který se aktualizuje vždy při přechodu do nového stavu. Bez využití tohoto procesu by po resetování (např. způsobeném výpadkem napájení z elektrické sítě) server nevěděl, v jakém stavu se má systém nacházet. Dále se inicializuje komunikace mezi GSM modulem a mikrokontrolérem a také periferie watchdog timer.

Watchdog timer (zkráceně WDT) je interní periferie MCU, která odpočítává předem definovaný čas, po jehož uplynutí dojde k resetování mikrokontroléru. K tomu nedojde, pokud se WDT stihne restartovat, čímž se znovu začne zmíněný čas odpočítávat. Jedná se o ochranný způsob, jak zajistit fungování mikrokontroléru i po tom, co nastane nějaká neočekávaná událost (zaseknutí programu, apod.). Já jsem WDT použil hlavně kvůli knihovně zprostředkávající TCP/IP komunikaci. Z toho plyne i umístění funkcí pro resetování WDT, které je v obsluze serverů. Pokud MCU obdrží zprávu od některého z klientů, dojde k resetování WDT. Poznamenejme, že k resetování MCU dochází také při přepnutí zdroje napájení, jelikož samotné přepnutí realizované přepínačem napájení (viz kap. 5.1) zkrátka není dostatečně rychlé. [45]

Následuje připojení k domácí Wi-Fi a Blynk cloudu, vytvoření vlastní Wi-Fi pro komunikaci s klienty a nastavení serveru podle postupu popsaného na začátku této kapitoly. Název generované Wi-Fi definuje proměnná *ssid\_AP* a heslo pro přístup k této síti proměnná *password\_AP*. Pro zvýšení bezpečnosti sítě je vhodné zvolit takové SSID, které je unikátní a neobsahuje žádné osobní informace, přičemž maximální počet znaků je 32 [1]. Stejně pro bezpečnost je heslo, které může obsahovat minimálně 8 a maximálně 63 znaků. Heslo bychom měli volit dostatečně silné, přičemž důraz se klade zejména na použití různých znakových sad (a-z, A-Z, 0-9, symboly) a dostatečné délky. Pokud např. zvolíme heslo o 10 znacích s použitím pouze jedné znakové sady a-z potom prolomení takového hesla metodou „hrubé síly“<sup>8</sup> může trvat i několik měsíců [3].

Než dojde k popisu dalších částí vývojového diagramu, je potřeba ještě ujasnit několik skutečností, které se v diagramu nevyskytují. Pokud je domácí Wi-Fi dostupná, dojde k připojení na tuto síť a také k následnému připojení na Blynk cloud. Data jsou na cloud nahrávána vždy, když přijdou od klienta, případně nastane změna parametru, který se na cloud ukládá. Měření napětí na baterii a zjišťování aktuálního zdroje napájení (elektrická síť nebo baterie) tvoří výjimku. Tyto informace se zjišťují a posílají na cloud periodicky jednou za čas definovaný makrem *BATTERY\_MEAS\_TIME* (nastaveno na 120 s).

V případě výpadku domácí Wi-Fi dojde k přenastavení z hybridního do STA módu (viz kap. 1). V tomto módu ústředna funguje úplně stejně, akorát se data neposílají na cloud. Zároveň se při výpadku Wi-Fi aktivuje proces, který jednou za čas definovaný makrem *RECONNECTING\_INT\_s* (nastaveno na 180) kontroluje, zda již není domácí Wi-Fi dostupná.

---

<sup>8</sup> Jedná se o metodu, při které se zkouší zadávat postupně všechny možné kombinace znaků z vybraných znakových sad.



V programu se dále zjišťuje, zda nenastalo několik událostí, na které má systém reagovat posláním SMS různého obsahu. Jedná se o kontrolu, zda nedošlo k:

- Výpadku napájení z elektrické sítě.
- Naměření nebezpečných hodnot kvality ovzduší (klienty 1 až 5).
- Detekci úniku vody.
- Detekování pohybu za podmínky, že se systém nachází v pohotovostním režimu.
- Přerušení smyčky s neautorizováním se do doby *delayAfterEntering* za podmínky, že se systém nachází v pohotovostním režimu (viz kap. 5.5.2).

Poslední neprobraný blok ve vývojovém diagramu je pokyn k resetování WDT. Tento pokyn je aktivní v případě, že došlo ke komunikaci s některým klientem. V takovém případě se periferie WDT resetuje a pokyn se deaktivuje.

### Soubor **GSMmodule**

Soubor *GSMmodule.cpp* obsahuje implementace dvou funkcí. První slouží k inicializaci komunikace mezi mikrokontrolérem a GSM modulem *GSM\_init()* a druhá je na posílání SMS, přičemž argumentem této funkce je daný text: *GSM\_sendSMS(String text)*.

### Soubor **myblynk**

V soubor *myblynk.cpp* se nachází implementace funkcí pro inicializaci a řízení komunikace s Blynk cloudem. Důležité je zmínit, že na začátku souboru se nachází definice maker *BLYNK\_TEMPLATE\_ID*, *BLYNK\_DEVICE\_NAME* a *BLYNK\_AUTH\_TOKEN*, které jsou nezbytné pro navázání komunikace s Blynk cloudem. Definice těchto maker jsou součástí každého vytvořeného projektu v aplikaci Blynk. V této části souboru jsou také definovány údaje o domácí Wi-Fi, přes kterou se realizuje nahrávání dat na Blynk cloudu. Tato Wi-Fi je definována proměnnými *ssid* a *password*.

### Soubor **usefulMacros**

Soubor *usefulMacros.h* opět obsahuje definice klíčových maker, přičemž některé z nich jich byly v minulých částech zmíněny:

- ***DEEPSLEEP\_TIME\_INIT***: Údaj předávaný všem klientům (kromě přístupového bodu) určující dobu, za kterou se má klient probudit z light režimu spánku (viz kap. 3.4.2)
- ***DELAY\_AFTER\_LEAVING***: Čas definující zpoždění, po jehož uplynutí má systém přejít do pohotovostního režimu (viz kap. 5.5.2). Prakticky se jedná o čas, za který je nutné opustit chráněný objekt (a zavřít vstupní dveře).
- ***DELAY\_AFTER\_ENTERING***: Čas definující zpoždění, po jehož uplynutí systém ohlásí formou SMS přerušení plášťové ochrany objektu. Do uplynutí této doby je potřeba se autorizovat vložení čtyřmístného PIN kódu na displej.

- ***RECONNECTING\_INT***: Perioda definující po jaké době má MCU kontrolovat dostupnost domácí Wi-Fi s názvem *ssid*. V případě její dostupnosti se na ní připojí a připojí se také na Blynk cloud, čímž obnoví posílání dat na cloud.
- ***BATTERY\_MEAS\_TIME***: Perioda s jakou se provádí měření napětí na baterii a také zjišťování zdroje napájení. Oba údaje se následně posílají na cloud.

## 6 Parametry navrženého systému

V této kapitole otestujeme navržený systém a změříme některé jeho parametry, které zároveň porovnáme s parametry komerčních systémů. Zároveň je však nutné myslet na to, že navržený systém je pouze model, který se ve své podstatě s komerčními systémy porovnávat nedá.

### 6.1 Ověření funkčnosti zálohy napájení

Součástí každého modulu je záloha napájení (viz kap. 5.1). Zdroj napájení ústředny je monitorován, tedy informace o aktuálním zdroji napájení je nahrávána na cloud. Cílem této kapitoly je ověřit, že záloha napájení ústředny skutečně funguje, tedy při výpadku napájení z elektrické sítě se modul začne napájet z baterie. Pokud je zdrojem napájení baterie a elektrická síť obnoví dodávku elektrické energie, dojde opět k přepnutí zdroje napájení.

Při testování v modulu běžel program popsáný v kap. 5.5.3 avšak s hodnotou makra *BATTERY\_MEAS\_TIME* 10, tedy měření napětí na baterii a zjišťování zdroje napájení se uskutečňuje každých 10 s. Experiment jsem realizoval odpojováním a připojováním napájení ústředny z elektrické sítě. Každý tento úkon jsem provedl pětkrát, přičemž na začátku experimentu byl modul napájen ze sítě (hodnota 0). Dohromady se tedy ústředna resetovala desetkrát. Úkon byl proveden vždy ve chvíli, kdy se obnovila komunikace s cloudem a nahrály se tři po sobě jdoucí hodnoty. Výsledek experimentu vidíme na obr. 6.1. Průměrná doba mezi poslední uloženou hodnotou z předešlého zdroje napájení a první hodnotou nového napájení je cca 27 s. Z obr. 6.1 je patrné, že záloha napájení skutečně funguje.



Obr. 6.1 Testování funkčnosti zálohy napájení

### 6.2 Ověření procesu znovu připojení na Wi-Fi

Ústředna se pomocí domácí Wi-Fi připojuje na cloud, kam nahrává data (viz kap. 5.5.3). Pokud Wi-Fi přestane fungovat správně a ústředna se od ní odpojí, aktivuje se proces kontroly dostupnosti této Wi-Fi. Jakmile je opět dostupná, mikrokontrolér se na ní připojí a obnoví nahrávání dat na cloud. Důležité je při tomto procesu makro *RECONNECTING\_INT* definující frekvenci zjišťování dostupnosti Wi-Fi. Cílem této kapitoly je ověřit, že k automatickému obnovování připojení k domácí Wi-Fi síti a následnému obnovení nahrávání dat na cloud skutečně dochází.

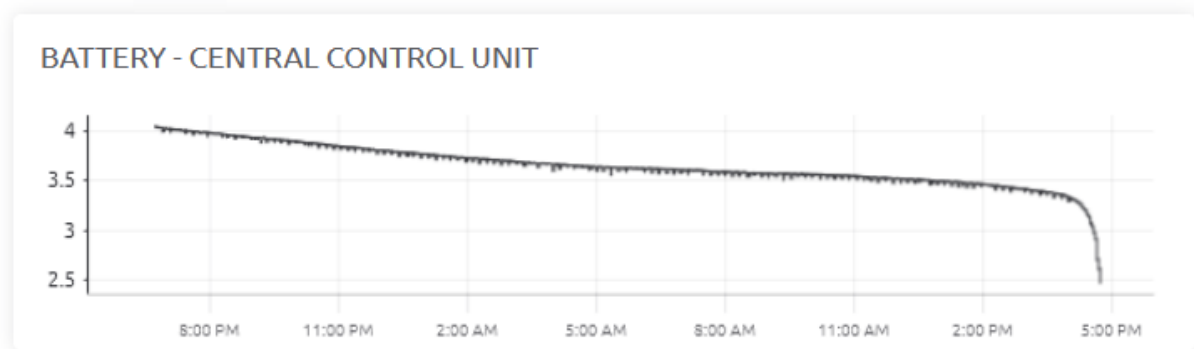
Při testování v ústředně běžel program popsáný v kap. 5.5.3 avšak s hodnotou makra *RECONNECTING\_INT* 10, tedy měření napětí na baterii a zjišťování zdroje napájení se uskutečňuje každých 10 s. Experiment jsem realizoval odpojením a okamžitým znovu připojením napájení Wi-Fi routeru z elektrické sítě. Stejný postup jsem provedl třikrát, přičemž na začátku experimentu byl Wi-Fi router připojen k napájení. Úkon byl proveden vždy ve chvíli, kdy se obnovila komunikace s cloudem a nahrálo se několik po sobě jdoucích hodnot. Funkčnost je ukázána na grafu znázorňujícím aktuální zdroj napájení ústředny, kterým byla po celou dobu experimentu baterie (hodnota 1). Výsledek experimentu vidíme na obr. 6.2. Vždy se uloží několik hodnot a komunikace s cloudem se přeruší. Následuje obnovení funkce Wi-Fi routeru, připojení ústředny a obnovení komunikace s cloudem, načtež se začnou hodnoty znovu ukládat. Přerušování komunikace trvalo 157 s, 106 s a 86 s, tedy průměrně cca 117 s. Z obr. 6.2 vidíme, že znovu připojování ke cloudu a obnovení ukládání dat na cloud funguje.



Obr. 6.2 Testování funkčnosti znovu připojení k Wi-Fi

### 6.3 Výdrž ústředny na záložním napájení

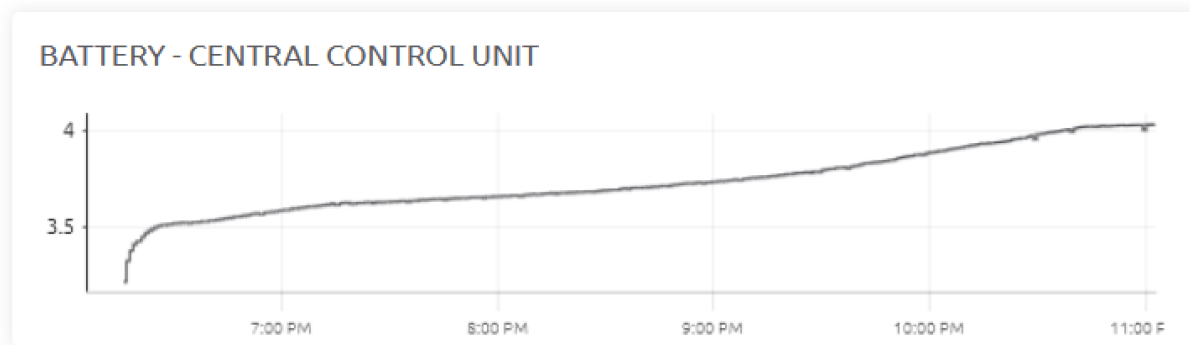
Důležitým parametrem je výdrž ústředny na záložním napájení – Li-Ion baterii. Zkoumal jsem pouze výdrž ústředny a ne celého systému, jelikož ústředna představuje hlavní část systému. Při testování byl v ústředně nahrán program popsáný v kap. 5.5.3. Klienti se připojovali každých 5 min (makro *DELAY\_AFTER\_LEAVING* nastaveno na 300) a měření napětí na baterii a uložení této hodnoty na cloud se realizovalo každých 60 s (makro *RECONNECTING\_INT* nastaveno na 60). Ústředna za těchto podmínek vydržela na záložním napájení od 18:44 do 16:45, tedy cca 22 h (viz obr. 6.3). Na začátku byla baterie plně nabitá a ústředna se nechala úplně vybit.



Obr. 6.3 Doba výdrže ústředny na záložním napájení

## 6.4 Nabití baterie záložního napájení

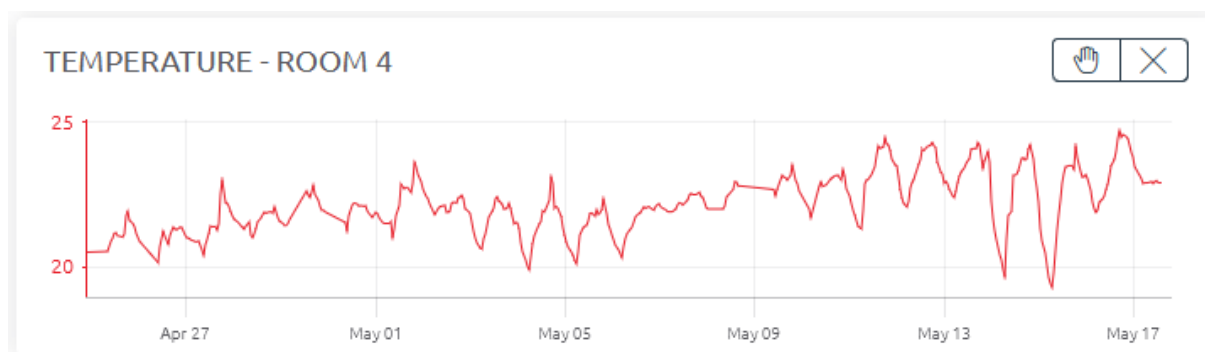
Dalším důležitým parametrem ústředny je doba, za kterou se baterie záložního napájení nabije ze stavu úplného vybití do stavu úplného nabití. Podmínky při experimentu byly stejné jako při testování výdrže ústředny na záložním napájení, tedy klienti se připojují každých 5 min a napětí na baterii se měří a posílá na cloud každých 60 s. Ústředna se z 0 % na 100 % nabije za necelých 5h (18:16 až 23:03) – viz obr. 6.4.



Obr. 6.4 Nabití baterie záložního napájení

## 6.5 Ověření fungování systému

Funkčnost vytvořeného systému byla otestována po dobu 22 dní (od 25. 4. 2022 do 17. 5. 2022). Po celou tuto dobu všechny moduly fungovaly správně, klienti předávali data ústředně a ta je dále ukládala na cloud. Kupříkladu grafy teploty a relativní vlhkosti v místnosti 4 (ložnice) vidíme na obr. 6.5 a na obr. 6.6. V průběhu testování se ani jednou nevyhlásil PIR alarm či MQ alarm (viz kap. 5.2.2) a zároveň za celou dobu nedošlo k detekci úniku vody pomocí TP nebo WS (viz kap. 5.3.1). Všechny tyto skutečnosti nasvědčují, že vytvořený model systému elektronického zabezpečení domácnosti funguje.



Obr. 6.5 Průběh teploty v ložnici za 22 dní





**Obr. 6.6 Průběh relativní vlhkosti v ložnici za 22 dní**

## 6.6 Porovnání s komerčními systémy

Jak již bylo řečeno na začátku této kapitoly, vytvořený systém se dá s komerčními systémy porovnávat obtížně, přesto se o to do určité míry v této kapitole pokusíme. Porovnání provedeme s produktem firmy Jablotron nazvaným JABLOTRON 100+, který je označován jako alarm do bytu/domu (viz [46]). Nejedná se o systém složený z konkrétních komponent, proto budeme porovnávat pouze vlastnosti, které jsou o tomto systému uvedeny.

Vytvořený systém a JABLOTRON 100+ mají společné následující aspekty:

- Možnost mobilního a webového rozhraní pro ovládání systému.
- Přístupový modul k systému.
- Možnost rozšíření systému (např. dodatečně o další modul/komponentu).
- Sledování historie událostí.
- Autorizace pomocí kódu nebo čipu: Mám jen pomocí kódu.
- Upozornění na události pomocí PUSH notifikací, e-mailů nebo SMS: Mám jen SMS, ale zbylé dvě možnosti by šli přidat.
- Možnost nastavování systému na dálku: Ve vytvořeném systému není co nastavovat, tedy tato možnost implementována není, každopádně ji aplikace Blynk také umožňuje (např. by bylo možné zapínat topení na dálku).

Lze říci, že zabezpečení bytu/domu systémem JABLOTRON 100+ je obecně tvořeno z podobných komponent jako vytvořený systém. Rozdíl mezi nimi je samozřejmě v provedení, ceně a spolehlivosti. Jistě bude kouřový detektor použitý v komerčním systému daleko více sofistikovaný než použitý modul se senzorem MQ-135. U systému JABLOTRON 100+ se navíc můžeme setkat s komponentami jako je detektor rozbití skla, vnější siréna nebo kamery, které se ve vytvořeném systému nevyskytují.

Jelikož se systém JABLOTRON 100+ neskládá z konkrétních komponent, je obtížné porovnat naměřenou dobu výdrže ústředny na záložním napájení a také dobu nabití baterie z 0 % na 100 %. Obecně lze říci, že minimálně doba výdrže ústředny na akumulátoru se pohybuje kolem 12 h, tedy 22 h je dobrý výsledek. V katalogu ústředny firmy Jablotron se často uvádí, že akumulátor musí být nabit maximálně do 48 h. U vytvořeného systému se akumulátor nabil

za přibližně 5 h, což by tedy poměrově představovalo dobrý výsledek. Na druhou stranu v ústřednách firmy Jablotron bývají použity akumulátory olověné gelové. Jedná se tedy o jiný druh akumulátoru s velmi odlišnými vlastnostmi, proto porovnání tohoto parametru je diskutabilní.

## 7 Ekonomická úvaha

Cílem této kapitoly je získat přibližný odhad ceny navrženého elektronického zabezpečení domu z obr. 4.2. Na jednotlivé součástky bylo odkazováno již v příslušných kapitolách. Použitá cena součástek je převzata z obchodu, na který bylo u dané součástky odkazováno, případně je odkaz na obchod s danou cenou součástky uveden. Cena je uváděna včetně 21% DPH a zahrnuje pouze zmíněné součástky, neobsahuje proto ceny odporů, LED, tlačítek, SIM karty do GSM modulu, vodičů, univerzální desky plošných spojů, pájky apod. Dále v ceně není zahrnuta práce na vývoj a pájení, což by představovalo významnou část finální ceny. Aby se vytvořený systém mohl prodávat, museli bychom získat licenci, jejíž cena by se do ceny také promítla.

Výpočet ceny jednotlivých modulů vidíme v tab. 1 a tab. 2. Celková cena modulů navrženého systému je 7 998,16 tedy přibližně **8000 Kč**. V této ceně jsou čtyři moduly typu 1, modul typu 2, ústředna (s 13 magnetickými kontakty) a modul s displejem.

**Tab. 1 Odhad ceny modulu typu 1 a modulu typu 2**

Modul typu 1		Modul typu 2	
komponenta	Kč/kus	komponenta	Kč/kus
síťový adaptér (viz [49])	106,48	síťový adaptér (viz [49])	106,48
přepínač napájení	133,10	přepínač napájení	133,10
Li-Ion baterie 3000 mAh	132,00	Li-Ion baterie 3000 mAh	132,00
držák článku 18650 (viz [48])	7,87	držák článku 18650 (viz [48])	7,87
nabíječka Li-Ion článků s ochranou	24,00	nabíječka Li-Ion článků s ochranou	24,00
step-up měnič	24,00	step-up měnič	24,00
modul se senzorem MQ-135	56,87	modul se senzorem MQ-135	56,87
mikrokontrolér esp32	198,00	mikrokontrolér esp 32	198,00
převodník logických úrovní 5V/3V	18,00	převodník logických úrovní 5V/3V	18,00
bzučák	13,31	senzor hladiny vody	12,00
OLED displej	106,48	krabice 150x110x70 mm (viz [53])	86,20
SHT30	108,00		
PIR detektor pohybu	41,14		
krabice 150x110x70 mm (viz [53])	86,20		
<b>Celkem 1 055,45 Kč</b>		<b>Celkem 798,52 Kč</b>	

**Tab. 2 Odhad ceny ústředny a modulu s displejem**

<b>Ústředna</b>		<b>Modul s displejem</b>	
<b>komponenta</b>	<b>Kč/kus</b>	<b>komponenta</b>	<b>Kč/kus</b>
síťový adaptér (viz [49])	106,48	síťový adaptér (viz [49])	106,48
přepínač napájení	133,10	přepínač napájení	133,10
Li-Ion baterie 5000 mAh	208,00	Li-Ion baterie 2200 mAh	98,00
držák článku 26650 (viz [47])	219,00	držák článku 18650 (viz [48])	7,87
nabíječka Li-Ion článků s ochranou	24,00	nabíječka Li-Ion článků s ochranou	24,00
step-up měnič	24,00	step-up měnič	24,00
mikrokontrolér esp32	198,00	mikrokontrolér esp 32	198,00
převodník logických úrovní 5V/3V	18,00	4.0" displej	758,00
krabice 150x110x70 mm (viz [53])	86,20	krabice 150x110x70 mm (viz [53])	86,20
GSM modul	258,00		
13 x magnetický kontakt	20,57		
<b>Celkem 1 542,19 Kč</b>		<b>Celkem 1 435,65 Kč</b>	

## 8 Závěr

V práci jsem navrhl, realizoval a otestoval systém s prvky EZS a také znaky chytré domácnosti. Za účelem minimalizování ceny výsledného systému jsem použil neprofesionální senzory. Na druhou stranu jsem musel zajistit spolehlivost systému a minimalizování falešných poplachů. Kupříkladu minimalizování falešných poplachů PIR detektoru pohybu je programově zajištěno tak, že je nutné detekovat pohyb dvakrát v průběhu 30 s.

Vytvořený systém se skládá ze čtyř typů modulů a dohromady ze sedmi kusů modulů. Hlavní funkcí prvních dvou typů modulů je měření dat a jejich předávání ústředně. Modul prvního typu měří teplotu, relativní vlhkost a kvalitu ovzduší. Kvalitu ovzduší měří senzory prostředí a lze pomocí nich detekovat nebezpečné plyny nebo kouř. Moduly prvního typu disponují malým displejem pro zobrazení naměřených veličin a také bzučákem, který se aktivuje v případě naměření nebezpečné kvality ovzduší (kterýmkoli modulem).

Modul typu dva měří kvalitu ovzduší a umožňuje detekci úniku vody. Další typ modulu představuje modul s dotykovým displejem a slouží jako přístupový bod systému. Poslední typ modulu je ústředna. Plášťová ochrana realizovaná magnetickými kontakty je drátová a tvoří jednu bezpečnostní smyčku ústředny. Prostorová ochrana je tvořena PIR detektory pohybu, které jsou připojeny k modulům v dané místnosti. Jednotlivé moduly jsem nejdříve realizoval na nepájivých polích a po vytvoření a odzkoušení kódu také na univerzálních jednovrstvých deskách plošných spojů, které jsou základem všech vytvořených modulů. Jednotlivé moduly by se daly rozšiřovat o další periferie.

Ústředna komunikuje s moduly bezdrátově a samotná komunikace je založena na TCP/IP protokolu. Kromě toho je ústředna připojena k domácí Wi-Fi a jejím prostřednictvím ukládá vybraná data na cloud. Možností při výběru cloudu je mnoho, já jsem zvolil aplikaci Blynk, jelikož ve své zdarma verzi umožňuje ukládat data až po dobu třech měsíců. Blynk dále poměrně jednoduše umožňuje vytvořit webové a mobilní rozhraní. Toho jsem využil a tyto uživatelská rozhraní vytvořil. Aplikace Blynk také poskytuje možnost posílat data z uživatelského rozhraní do vysílacího zařízení – ústředny. Této možnosti není využito, ale dal by se tímto způsobem řídit vytvořený systém vzdáleně. Kupříkladu by se dalo vzdáleně spínat topení nebo mechanismus pro otevírání garážových vrat apod.

Součástí ústředny je GSM modul umožňující ústředně informovat uživatele o vybraných stavech formou SMS. GSM modul obecně poskytuje připojení k mobilním sítím, tedy i k internetu. V tomto ohledu by se dala práce rozšířit např. o posílání PUSH notifikací, emailů apod. Také by bylo možné ukládat data na cloud s využitím mobilních dat, což by odstranilo závislost na domácí Wi-Fi.

Všechny moduly jsou napájeny z elektrické sítě a zároveň disponují záložním napájením. Při výpadku energie z elektrické sítě se napájení automaticky přepne na záložní baterii. Ústředna na záložním napájení vydrží cca 22 h a baterie se opět plně nabije za cca 5 h. Tyto parametry dosahují srovnatelných hodnot s komerčními systémy.

Pro účely testování jsem vytvořil model rodinného domu, do kterého jsem vytvořený systém instaloval. Testování probíhalo 22 dní, přičemž celou dobu systém nastavený v pohotovostním režimu fungoval správně a to bez vnějšího zásahu. Za tuto dobu nebyla ani jednou vyhlášena detekce pohybu, tedy PIR detektory pohybu fungují obstojně. Také se nevyskytl žádný poplach způsobený naměřením nebezpečné kvality ovzduší. Samotný senzor kvality ovzduší by však chtělo otestovat mnohem více a podrobněji. Vytvořený systém pracuje po výpadku energie z elektrické sítě a také při výpadku domácí Wi-Fi. V takovém případě ústředna stále komunikuje s ostatními moduly, přičemž zároveň každých několik minut kontroluje, zda již domácí Wi-Fi není opět dostupná.

Na závěr jsem provedl ekonomickou úvahu pro výrobu navrženého systému. Celková cena modulů navrženého systému je cca 8000 Kč. V této ceně jsou čtyři moduly typu 1, modul typu 2, ústředna (s 13 magnetickými kontakty) a modul s displejem. Na základě výše popsáných skutečností lze tvrdit, že všechny cíle stanovené na začátku této práce byly splněny.

Práce může sloužit jako zdroj inspirace při návrhu a výrobě domácího elektronického zabezpečení bytu nebo rodinného domu. Vytvořený systém lze v mnoha ohledech rozšířit a vylepšit. Výše již bylo zmíněno několik nápadů na vylepšení a dále jich ještě několik uvedu. Například by bylo možné přidat aktivaci detekce pohybu ve vybraných částech domu. Možné by také bylo přidání streamování videa kamerou např. s využitím modulu esp32-cam. Samotná aplikace Blynk tuto možnost v placené verzi poskytuje. Samotná nabídka dotykového displeje má mnoho prostoru pro zlepšení (např. resetování hesla, správa telefonních čísel, na které se posílají oznámení apod.).

## 9 Seznam literatury

- [1] What's in a Wireless Network Name? The Power of the SSID. *Auvik* [online]. USA: Auvik Networks, c2013-2022 [cit. 2022-04-11]. Dostupné z: <https://www.auvik.com/franklyit/blog/ssid-wireless-network-names/>
- [2] Wi-Fi API. *Arduino-ESP32 ESPRESSIF* [online]. c2022 [cit. 2022-04-11]. Dostupné z: <https://espressif-docs.readthedocs-hosted.com/projects/arduino-esp32/en/latest/api/wifi.html>
- [3] Estimating Password-Cracking Times. *BetterBuys* [online]. [cit. 2022-04-11]. Dostupné z: [https://www.betterbuys.com/estimating-password-cracking-times/?fbclid=IwAR2Zaw5q6sAXsmxMH1n70xVwz\\_EmZDoJCf2RGQGav-XU-WPiTihAxLy5mEA](https://www.betterbuys.com/estimating-password-cracking-times/?fbclid=IwAR2Zaw5q6sAXsmxMH1n70xVwz_EmZDoJCf2RGQGav-XU-WPiTihAxLy5mEA)
- [4] WiFi Encryption Over Time. *WiGLE* [online]. c2001-2022 [cit. 2022-04-11]. Dostupné z: <https://wigle.net/stats#>
- [5] STEHLÍK, Richard. *Útok na WiFi síť s využitím ESP32/8266* [online]. Brno, 2021 [cit. 2022-04-11]. Dostupné z: <https://www.fit.vut.cz/study/thesis-file/23435/23435.pdf>  
Diplomová práce. VUT v Brně.
- [6] Wi-Fi Security. *ESPRESSIF: ESP-IDF Programming Guide* [online]. Shanghai: Espressif Systems Co., c2016 - 2022 [cit. 2022-04-11]. Dostupné z: <https://docs.espressif.com/projects/esp-idf/en/latest/esp32/api-guides/wifi-security.html#protected-management-frames-pmf>
- [7] *Wi-Fi API* [online]. Espressif, c2022 [cit. 2022-04-12]. Dostupné z: <https://espressif-docs.readthedocs-hosted.com/projects/arduino-esp32/en/latest/api/wifi.html>
- [8] *ESPAsyncWebServer: Async Web Server for ESP8266 and ESP32* [online]. GitHub, c2022 [cit. 2022-04-20]. Dostupné z: <https://github.com/me-no-dev/ESPAsyncWebServer>
- [9] *AsyncTCP: Async TCP Library for ESP32* [online]. GitHub, c2022 [cit. 2022-04-20]. Dostupné z: <https://github.com/me-no-dev/AsyncTCP>
- [10] ESP32 Arduino: Asynchronous HTTP web server. *TechTutorialsx* [online]. techtutorialsx, c2022 [cit. 2022-04-21]. Dostupné z: <https://techtutorialsx.com/2017/12/01/esp32-arduino-asynchronous-http-webserver/>
- [11] *ESP32* [online]. Shanghai: ESPRESSIF SYSTEMS, 2022 [cit. 2022-04-22]. Dostupné z: <https://www.espressif.com/en/products/socs/esp32>
- [12] IoT ESP-WROOM-32 2.4GHz Dual-Mode WiFi+Bluetooth rev.1, CP2102. *Laskakit* [online]. c2022 [cit. 2022-04-22]. Dostupné z: <https://www.laskakit.cz/iot-esp-32s-2-4ghz-dual-mode-wifi-bluetooth-rev-1--cp2102/>
- [13] ESP32 Web Socket Server. *THE ENGINEERING PROJECTS* [online]. [cit. 2022-04-22]. Dostupné z: <https://www.theengineeringprojects.com/2021/12/esp32-web-socket-server.html>

- [14] *Blynk* [online]. c2022 [cit. 2022-04-24]. Dostupné z: <https://blynk.io/>
- [15] What's included in the plans. *Blynk* [online]. c2022 [cit. 2022-04-25]. Dostupné z: <https://blynk.io/pricing>
- [16] Documentation. *Blynk* [online]. c2022 [cit. 2022-04-25]. Dostupné z: <https://docs.blynk.io/en/>
- [17] Insight Into ESP32 Sleep Modes & Their Power Consumption. *Last Minute Engineers* [online]. c2021 [cit. 2022-04-25]. Dostupné z: <https://lastminuteengineers.com/esp32-sleep-modes-power-consumption/>
- [18] Sleep Modes. *ESPRESSIF* [online]. Shanghai: Espressif Systems, c2016-2022 [cit. 2022-04-26]. Dostupné z: [https://docs.espressif.com/projects/esp-idf/en/latest/esp32/api-reference/system/sleep\\_modes.html](https://docs.espressif.com/projects/esp-idf/en/latest/esp32/api-reference/system/sleep_modes.html)
- [19] Is Lithium-ion the Ideal Battery?. *Battery University* [online]. c2022, 5-Jul-2016 [cit. 2022-04-27]. Dostupné z: <https://batteryuniversity.com/article/is-lithium-ion-the-ideal-battery>
- [20] GeB Li-Ion Baterie 18650 2200mAh 3.7V. *Laskakit* [online]. c2022 [cit. 2022-04-27]. Dostupné z: <https://www.laskakit.cz/geb-li-ion-baterie-18650-2200mah-3-7v/>
- [21] GeB Li-Ion Baterie 18650 3000mAh 3.7V. *Laskakit* [online]. c2022 [cit. 2022-04-27]. Dostupné z: <https://www.laskakit.cz/geb-li-ion-baterie-18650-3000mah-3-7v/>
- [22] GeB Li-Ion Baterie 26650 5000mAh 3.7V. *Laskakit* [online]. c2022 [cit. 2022-04-27]. Dostupné z: <https://www.laskakit.cz/geb-li-ion-baterie-26650-5000mah-3-7v/>
- [23] Step-up boost měnič s MT3608. *Laskakit* [online]. c2022 [cit. 2022-04-27]. Dostupné z: <https://www.laskakit.cz/step-up-boost-menic-s-mt3608/>
- [24] Nabíječka Li-ion článku TP4056 s ochranou microUSB. *Laskakit* [online]. c2022 [cit. 2022-04-27]. Dostupné z: <https://www.laskakit.cz/nabijecka-li-ion-clanku-tp4056-s-ochranou-microusb/>
- [25] Automatický prepínač baterie - UPS modul YX850. *HADEX* [online]. Softima, c2011-2022 [cit. 2022-04-27]. Dostupné z: <https://www.hadex.cz/m523-automaticky-prepinac-baterie---ups-modul-yx850/>
- [26] Detektor pohybu, modul PIR NC-SR501. *HADEX* [online]. Softima, c2011-2022 [cit. 2022-04-27]. Dostupné z: [https://www.hadex.cz/m356a-detektor-pohybu-modul-pir-nc-sr501/?gclid=Cj0KCQjw06OTBhC\\_ARIsAAU1yOXXEgQVgwKwPg-gWHvOHZad7AASAKLQptG1GIHxQ0QnjJ1Vo3IJTNgaAp1REALw\\_wcB](https://www.hadex.cz/m356a-detektor-pohybu-modul-pir-nc-sr501/?gclid=Cj0KCQjw06OTBhC_ARIsAAU1yOXXEgQVgwKwPg-gWHvOHZad7AASAKLQptG1GIHxQ0QnjJ1Vo3IJTNgaAp1REALw_wcB)
- [27] Piezobzučák 14mm, napájení 3-24V/10mA. *HADEX* [online]. Softima, c2011-2022 [cit. 2022-04-27]. Dostupné z: <https://www.hadex.cz/q183-piezobzucak-14mmnapajeni-3-24v10ma/>
- [28] 4 kanály Obousměrný převodník logických úrovní 5V a 3.3V. *Laskakit* [online]. c2022 [cit. 2022-04-27]. Dostupné z: <https://www.laskakit.cz/4-kanaly-obousmerny-prevodnik-logickych-urovni-5v-a-3->



[3v/?gclid=Cj0KCQjw06OTBhC\\_ARIsAAU1yOWNXbjfIOZx5kpuXiXJ4leNpGOGf4IayY9OdNmzA-dx3k0VqybWCIMaAnuvEALw\\_wcB](https://www.hadex.cz/m470d-detektor-kvality-ovzduasi-modul-s-cidlem-mq-135/?gclid=Cj0KCQjw06OTBhC_ARIsAAU1yOWNXbjfIOZx5kpuXiXJ4leNpGOGf4IayY9OdNmzA-dx3k0VqybWCIMaAnuvEALw_wcB)

- [29] Detektor kvality ovzduší, modul s čidlem MQ-135. *HADEX* [online]. Softima, c2011-2022 [cit. 2022-04-28]. Dostupné z: [https://www.hadex.cz/m470d-detektor-kvality-ovzduasi-modul-s-cidlem-mq-135/?gclid=CjwKCAjw9qiTBhBbEiwAp-GE0Wh7pUZu4yUlerxWhKScpgjJU2GaqVKZC\\_p-Zc\\_rJUG6u16-jRGoVBoCygAQAvD\\_BwE](https://www.hadex.cz/m470d-detektor-kvality-ovzduasi-modul-s-cidlem-mq-135/?gclid=CjwKCAjw9qiTBhBbEiwAp-GE0Wh7pUZu4yUlerxWhKScpgjJU2GaqVKZC_p-Zc_rJUG6u16-jRGoVBoCygAQAvD_BwE)
- [30] Senzor teploty a vlhkosti vzduchu SHT30. *Laskakit* [online]. c2022 [cit. 2022-04-28]. Dostupné z: [https://www.laskakit.cz/senzor-teploty-a-vlhkosti-vzduchu-sht30/?gclid=CjwKCAjw9qiTBhBbEiwAp-GE0XC3cvewUf9NeuHe5dMVCMiJoT26sDqX-ej9QR2Nxz5KbcDEv8NjJB0CwhYQAvD\\_BwE](https://www.laskakit.cz/senzor-teploty-a-vlhkosti-vzduchu-sht30/?gclid=CjwKCAjw9qiTBhBbEiwAp-GE0XC3cvewUf9NeuHe5dMVCMiJoT26sDqX-ej9QR2Nxz5KbcDEv8NjJB0CwhYQAvD_BwE)
- [31] Displej OLED 0,96", 128x64 znaků, IIC/I2C, 4piny, modrý. *HADEX* [online]. Softima, c2011-2022 [cit. 2022-04-28]. Dostupné z: [https://www.hadex.cz/m508-displej-oled-096-128x64-znaku-iici2c-4piny-modry/?gclid=CjwKCAjw9qiTBhBbEiwAp-GE0ewAFLdeNHMCCb\\_KzNgYU3nHp2dMDYnDQE0mzYvOJUUsHP6DkjMHxoCX1IQAvD\\_BwE](https://www.hadex.cz/m508-displej-oled-096-128x64-znaku-iici2c-4piny-modry/?gclid=CjwKCAjw9qiTBhBbEiwAp-GE0ewAFLdeNHMCCb_KzNgYU3nHp2dMDYnDQE0mzYvOJUUsHP6DkjMHxoCX1IQAvD_BwE)
- [32] ASAIR senzor teploty a vlhkosti vzduchu DHT11. *Laskakit* [online]. c2022 [cit. 2022-04-28]. Dostupné z: <https://www.laskakit.cz/arduino-senzor-teploty-a-vlhkosti-vzduchu-dht11/>
- [33] ESP32: Power options. *Tech Explorations* [online]. c2022 [cit. 2022-04-28]. Dostupné z: <https://techexplorations.com/guides/esp32/begin/power/>
- [34] LHOŤECKÝ, Vlastimil. *Komunikační brána pro smart home* [online]. Praha, 2020 [cit. 2022-04-28]. Dostupné z: <https://dspace.cvut.cz/handle/10467/92801>. Diplomová práce. ČVUT FEL. Vedoucí práce Vladimír Janíček.
- [35] Adafruit\_SSD1306. *GitHub* [online]. c2022 [cit. 2022-04-29]. Dostupné z: [https://github.com/adafruit/Adafruit\\_SSD1306](https://github.com/adafruit/Adafruit_SSD1306)
- [36] KROCKER, Georg. Arduino library for the MQ135. *GitHub* [online]. c2022, 29 Dec 2014 [cit. 2022-04-29]. Dostupné z: <https://github.com/GeorgK/MQ135>
- [37] Adafruit\_SHT31: Temperature and Humidity Sensor Breakout. *GitHub* [online]. c2022 [cit. 2022-04-29]. Dostupné z: [https://github.com/adafruit/Adafruit\\_SHT31](https://github.com/adafruit/Adafruit_SHT31)
- [38] *HC-SR501 PIR MOTION DETECTOR* [online]. Laskakit, c2022 [cit. 2022-05-01]. Dostupné z: [https://www.laskakit.cz/user/related\\_files/hc-sr501\\_datasheet.pdf](https://www.laskakit.cz/user/related_files/hc-sr501_datasheet.pdf)
- [39] *TECHNICAL DATA: MQ-135 GAS SENSOR* [online]. Laskakit, c2022 [cit. 2022-05-01]. Dostupné z: [https://www.laskakit.cz/user/related\\_files/mq135.pdf](https://www.laskakit.cz/user/related_files/mq135.pdf)
- [40] Senzor hladiny vody. *Laskakit* [online]. c2022 [cit. 2022-05-01]. Dostupné z: [https://www.laskakit.cz/senzor-hladiny-vody/?gclid=Cj0KCQjw37iTBhCWARIsACBt1IxaR2hzpufxAUEuQXnKBNy5MqJwQDiL4IyGF80TXgG2FSqtoA8qGEwaAgRLEALw\\_wcB](https://www.laskakit.cz/senzor-hladiny-vody/?gclid=Cj0KCQjw37iTBhCWARIsACBt1IxaR2hzpufxAUEuQXnKBNy5MqJwQDiL4IyGF80TXgG2FSqtoA8qGEwaAgRLEALw_wcB)

- [41] ESP32: Technical Reference Manual. *Espressif* [online]. c2022, 2021 [cit. 2022-05-01]. Dostupné z: [https://www.espressif.com/sites/default/files/documentation/esp32\\_technical\\_reference\\_manual\\_en.pdf](https://www.espressif.com/sites/default/files/documentation/esp32_technical_reference_manual_en.pdf)
- [42] 4.0" 480x320 TFT displej, ST7796, SPI, dotykový. *Laskakit* [online]. c2022 [cit. 2022-05-03]. Dostupné z: <https://www.laskakit.cz/4-0--480x320-tft-displej--st7796--spi--dotykovy/>
- [43] BODMER. TFT\_eSPI. *GitHub* [online]. c2022 [cit. 2022-05-04]. Dostupné z: [https://github.com/Bodmer/TFT\\_eSPI](https://github.com/Bodmer/TFT_eSPI)
- [44] GPRS GSM Module SIM800L V2.0 5V, microSIM. *Laskakit* [online]. c2022 [cit. 2022-05-05]. Dostupné z: <https://www.laskakit.cz/miniaturni-sim800l-v2-0-5v-gprs-gsm-module--microsim/#ratingTab>
- [45] Watchdogs. *ESPRESSIF* [online]. Shanghai: Espressif Systems, c2016-2022 [cit. 2022-05-06]. Dostupné z: <https://docs.espressif.com/projects/esp-idf/en/latest/esp32/api-reference/system/wdts.html>
- [46] *JABLOTRON* [online]. c2022 [cit. 2022-05-08]. Dostupné z: <https://www.jablotron.com/cz/>
- [47] Keystone 1106 bateriový držák 1x 26650. *CONRAD* [online]. ČR: Conrad Electronic, c2021 [cit. 2022-05-08]. Dostupné z: [https://www.conrad.cz/p/keystone-1106-bateriovyy-drzak-1x-26650-povrchova-montaz-smd-d-x-s-x-v-86-x-29-x-19-mm-1555510?&vat=true&gclid=Cj0KCQjw1N2TBhCOARIsAGVHQc4GeL1o4VvEBax1kNayLIWBUZvc-1TJi7CCjFH\\_HpcWOJ4jm17Q7JcaAmagEALw\\_wcB](https://www.conrad.cz/p/keystone-1106-bateriovyy-drzak-1x-26650-povrchova-montaz-smd-d-x-s-x-v-86-x-29-x-19-mm-1555510?&vat=true&gclid=Cj0KCQjw1N2TBhCOARIsAGVHQc4GeL1o4VvEBax1kNayLIWBUZvc-1TJi7CCjFH_HpcWOJ4jm17Q7JcaAmagEALw_wcB)
- [48] Držák článku 18650 s vývody. *HADEX* [online]. Softima, c2011-2022 [cit. 2022-05-08]. Dostupné z: [https://www.hadex.cz/1038b-drzak-clanku-18650-s-vyvody/?gclid=Cj0KCQjw1N2TBhCOARIsAGVHQc4N0LtPEIHMfY7M9PauMrYI\\_aUOrtIvMpM8AeIUJwRpJSLIJ0fx\\_UgaAmE8EALw\\_wcB](https://www.hadex.cz/1038b-drzak-clanku-18650-s-vyvody/?gclid=Cj0KCQjw1N2TBhCOARIsAGVHQc4N0LtPEIHMfY7M9PauMrYI_aUOrtIvMpM8AeIUJwRpJSLIJ0fx_UgaAmE8EALw_wcB)
- [49] Napáječ, síťový adaptér USB 5V/3A spínaný, koncovka USB micro. *HADEX* [online]. Softima, c2011-2022 [cit. 2022-05-08]. Dostupné z: <https://www.hadex.cz/g702c-napajec-sitovy-adapter-usb-5v3a-spinany-koncovka-usb-micro/>
- [50] Přepínač kolébkový 3A 250VAC kulatý. *Laskakit* [online]. c2022 [cit. 2022-05-08]. Dostupné z: <https://www.laskakit.cz/prepinac-kolebkovy-3a-250vac-kruhovy/>
- [51] Magnetický kontakt MC-38 (v klidu rozpojeno). *HADEX* [online]. Softima, c2011-2022 [cit. 2022-05-08]. Dostupné z: [https://www.hadex.cz/t516-magneticky-kontakt-mc-38-v-klidu-rozpojeno/?gclid=Cj0KCQjw1N2TBhCOARIsAGVHQc7ZdtBpTXxsFNN-tmYX5kX4WOPCZEYqL28-pVCkB7fJ61VZUrkvawaAhecEALw\\_wcB](https://www.hadex.cz/t516-magneticky-kontakt-mc-38-v-klidu-rozpojeno/?gclid=Cj0KCQjw1N2TBhCOARIsAGVHQc7ZdtBpTXxsFNN-tmYX5kX4WOPCZEYqL28-pVCkB7fJ61VZUrkvawaAhecEALw_wcB)
- [52] HLADÍK, Drahoslav. *Elektronické zabezpečovací systémy a elektronická požární signalizace* [online]. SOUE Plzeň, 2011 [cit. 2022-05-10]. Dostupné z: <https://www.souepl.cz/wp-content/uploads/2020/09/elektronick%C3%A9-zabezpe%C4%8Dovac%C3%AD-syst%C3%A9my-a-elektronick%C3%A1-po%C5%BE%C3%A1rn%C3%AD-signalizace.pdf>

- [53] Krabice Scame SCABOX 686.206 150x110x70mm IP56. *K&V ELEKTRO* [online]. c2022 [cit. 2022-05-08]. Dostupné z: [https://www.kvelektro.cz/krabice-scame-scabox-686-206-150x110x70mm-ip56-p1169854?gclid=Cj0KCQjw1N2TBhCOARIsAGVHQc6KFJEiLbzx2z7c1tumOdXHq6E5E34wyL5r\\_Pg-bNh-WEIglJ2vT4aAjlNEALw\\_wcB](https://www.kvelektro.cz/krabice-scame-scabox-686-206-150x110x70mm-ip56-p1169854?gclid=Cj0KCQjw1N2TBhCOARIsAGVHQc6KFJEiLbzx2z7c1tumOdXHq6E5E34wyL5r_Pg-bNh-WEIglJ2vT4aAjlNEALw_wcB)
- [54] KAISLER, Radek. Principy detekce vniku nežádoucích osob do objektu: Akustické detektory. *Profielektrika* [online]. ElektriKa.info, c1998-2022, 14.06.2002 [cit. 2022-05-10]. Dostupné z: <https://elektrika.cz/data/clanky/pdvnoo020611>
- [55] GBS-210 Detektor rozbití skla. *Jablotron* [online]. c2022 [cit. 2022-05-10]. Dostupné z: <https://www.jablotron.com/cz/produkt/detektor-rozbiti-skla-45/>
- [56] SA-203 Magnetický kontakt mini samolepící. *Jablotron* [online]. c2022 [cit. 2022-05-10]. Dostupné z: <https://www.jablotron.com/cz/produkt/magneticky-kontakt-mini-samolepici-81/>
- [57] JA-162PW (G) Bezdrátový duální PIR a MW detektor pohybu. *Jablotron* [online]. c2022 [cit. 2022-05-10]. Dostupné z: <https://www.jablotron.com/cz/produkt/bezdratovy-dualni-pir-a-mw-detektor-pohybu-1716/>
- [58] JA-110P PET Sběrníkový PIR detektor pohybu se základní imunitou proti zvířatům. *Jablotron* [online]. c2022 [cit. 2022-05-10]. Dostupné z: <https://www.jablotron.com/cz/produkt/sbernicovy-pir-detektor-pohybu-se-zakladni-imunitou-proti-zviratum-1242/>
- [59] JA-120PC Sběrníkový PIR detektor pohybu s kamerou. *Jablotron* [online]. c2022 [cit. 2022-05-10]. Dostupné z: <https://www.jablotron.com/cz/produkt/sbernicovy-pir-detektor-pohybu-s-kamerou-297/>