ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta elektrotechnická

Katedra mikroelektroniky

Elektronický zabezpečovací systém pro rodinný dům

Electronic Security System for a Family House

Bakalářská práce

Studijní program: Elektronika a komunikace

Autor práce: Lukáš Pospíšil

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

Praha 2022

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: **Pospíšil** Jméno: **Lukáš** Osobní číslo: **483648**

Fakulta/ústav: **Fakulta elektrotechnická**

Zadávající katedra/ústav: **Katedra mikroelektroniky**

Studijní program: **Elektronika a komunikace**

II. ÚDAJE K BAKALÁŘSKÉ PRÁCI

Název bakalářské práce:

Elektronický zabezpečovací systém pro rodinný dům

Název bakalářské práce anglicky:

Electronic Security System for a Family House

Pokyny pro vypracování:

1. Proveďte rešerši současného stavu řešení elektronické ochrany rodinného domu. Pozornost zaměřte na aktuálně používané senzory včetně biometrických systémů, aktuální zásady při instalaci, podmínky pro zajištění standardní úrovně zabezpečení, požadavky zákazníků a nabídky firem.
2. Navrhněte a realizujte jednoduchý hardware model elektronického zabezpečovacího systému s prvky chytré domácnosti pro rodinný dům. Při návrhu využijte senzory pohybu, senzory monitorující otevření dveří a oken. Do návrhu zabudujte přístupový systém, kamerový systém a prvky chytré domácnosti jako např. ovládání světel nebo teploty. Navrhněte vhodné akční výstupy systému s možností připojení přes internet. Informace vyhodnocujte pomocí mobilní aplikace nebo PC.
3. Zjistěte parametry realizovaného systému, porovnejte s profesionálním řešením, proveďte ekonomický rozbor.

Seznam doporučené literatury:

[1] Merz, H.; Hansemann T.; Hubner, C. Automatizované systémy budov. 1. vydání, Grada Publishing, a.s. 2007
[2] Kůtka, Michal. Návrh elektronického zabezpečovacího systému (EZS) s prvky inteligentní domácnosti. FEKT VUT v Brně, 2016, http://hdl.handle.net/11012/60418

Jméno a pracoviště vedoucí(ho) bakalářské práce:

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

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

Datum zadání bakalářské práce: **16.09.2021** Termín odevzdání bakalářské práce: _____

Platnost zadání bakalářské práce: **19.02.2023**

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

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

. _____ Podpis studenta

Datum převzetí zadání

Čestné 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 …… ……..

Lukáš Pospíšil

Poděkování

Rád bych poděkoval svému vedoucímu bakalářské práce prof. Ing. Miroslavu Husákovi, CSc. za odborné vedení a poskytnutí cenných rad a připomínek při zpracování bakalářské práce.

Abstrakt

Práce shrnuje současný stav technologií elektronických zabezpečovacích systémů pro rodinné domy, včetně požárního zabezpečení a prvků chytré domácnosti. Po teoretické části následuje návrh a realizace modelu zabezpečovacího systému s prvky chytré domácnosti. Model je postaven na vývojové desce ESP32 s podporou Wifi rozhraní, které je použito pro vzdálené ovládání celého systému. Dále je popsán výběr všech senzorů použitých pro realizaci modelu, spolu s dalšími možnostmi rozvoje a vylepšení modelu. Práce je zakončena měřením parametrů navrženého modelu a srovnáním ekonomického hlediska navrženého systému s profesionálním systémem dostupným na trhu.

Klíčová slova

Elektronický zabezpečovací systém, zabezpečovací systém, požární ochrana, poplachový zabezpečovací systém, kamerový systém, senzory zabezpečovacího systému, detektory pohybu, detektory požáru, požární detektory, detektory plynů, přístupové systémy, biometrické přístupové systémy, chytrá domácnost, chytrý dům, návrh elektronického zabezpečovacího systému, ESP32

Abstract

This bachelor thesis summarizes the current state of technologies used in electronic security systems for family house including fire protection and smart home systems. The theoretical part of thesis is followed by the design and implementation of a smart home electronic security system model. The model is build using an ESP32 microcontroller with Wifi interface which is used for remote access. This is followed by description of the sensors used in the model and suggestions for upgrades of the whole system. Thesis is completed by measuring the parameters of the model and economic comparison of the designed model with professional electronic security system.

Key words

Electronic security system, security system, fire protection, cctv, security system sensors, motion detectors, smoke detectors, fire alarms, gas detectors, access control systems, biometric access control systems, smart home, smart house, implementation of a smart security system, ESP32

Obsah

Úvod

Chránit majetek měly lidé již od pradávna, ať to byly sofistikované zámky nebo jen ohraničení majetku plotem. V tomto století došlo k velkému rozmachu technologií a to zasáhlo i zabezpečovací systémy. V dnešní době se již mechanické zabezpečení objektů, jako je oplocení nebo bezpečnostní dveře a zámky bere jako samozřejmost. Elektronické zabezpečovací systémy se začaly do objektů instalovat nejen z důvodu lepšího a kvalitnějšího zabezpečení proti vniknutí nepovolaných osob, ale také například pro usnadnění administrativních činností pro firmy nebo pro zjednodušení každodenního života s pomocí prvků inteligentní domácnosti, které jsou popsány v teoretické části práce spolu s rozborem používaných technologií v zabezpečovacích systémech. Praktická část se zabývá návrhem funkčního modelu zabezpečovacího systému se všemi základními druhy senzorů pro zabezpečení a prvky inteligentní domácnosti. Je popsán jak výběr, tak i problémy a poznatky při navrhování hardware a software, včetně možného zdokonalení a rozšíření celého systému.

I. Současný stav zabezpečovacích systémů

Elektronické zabezpečovací systémy (EZS) mají hlavně sloužit k prevenci vniku nepovolaných osob, ale také mají chránit lidské zdraví, které může být ohroženo únikem nebezpečných plynů nebo požárem. V kancelářských prostorech jsou pak součástí zabezpečovacího a protipožárního sytému také různé přístupové systémy registrující příchody a odchody osob pro usnadnění administrace a dozoru nad celým objektem.

EZS se skládá z ústředny, což je řídicí jednotka ovládající celý zabezpečovací systém, která reaguje na signály přicházející ze senzorů, jež jsou spojené s ústřednou buď pomocí drátů nebo pomocí bezdrátové technologie. Dnešní moderní ústředny jsou vybaveny komunikačními zařízeními, které ústředně umožňují přenášet informace přes internet nebo GSM sítě na mobilní telefon. Přes mobilní aplikaci lze pak k ústředně přistupovat vzdáleně a kontrolovat stav střeženého objektu. To je první krok pro vytvoření tzv. inteligentní domácnosti, kde je možné přes mobilní aplikaci vzdáleně ovládat například topení, klimatizaci, žaluzie, světla nebo kontrolovat stav objektu pomocí kamerového systému.

Kamerový systém se stal velmi populární a instalovanou částí zabezpečovacího systému, jelikož doplňuje celý systém o možnost vizuálně kontrolovat celý střežený objekt. Stále větším trendem je instalace samostatného kamerového systému, pokud chce mít dotyčný přehled nad svým majetkem a nechce vydávat větší finance na propracovanější zabezpečovací systém s přídavnými senzory.

V dnešní době máme při výběru zabezpečovacího systému možnost volit z desítek výrobců. V České republice se často používá zabezpečovací systém od firmy Jablotron, jež je ryze českou firmou, zabývající se zabezpečovacími systémy od roku 1990. Další oblíbenou firmou zabezpečovacích zařízení je kanadská firma Paradox nebo americká firma Honeywell nabízející zabezpečovací systémy pro objekty s požadavkem na vyšší úroveň zabezpečení, než se používá například u rodinných domů a menších firem. Na trhu se nachází mnoho dalších firem nabízející zabezpečovací systémy, avšak povětšinou se jedná o jednodušší systémy obsahující pouze základní senzory, které jsou popsané v následujících kapitolách.

1 Ústředna

Je řídicí jednotka ovládající celý zabezpečovací systém. K moderním ústřednám lze senzory připojovat buď drátově nebo bezdrátově. Dnešní moderní ústředny bývají vybaveny komunikačními zařízeními, které ústředně umožňují přenášet informace přes internet nebo GSM sítě na mobilní telefon. S ústřednou lze také komunikovat pomocí chytrého mobilního telefonu s internetovým připojením. V mobilní aplikaci je možné sledovat stav střeženého objektu, kontrolovat kamerový systém nebo využívat možnosti inteligentní domácnosti, jako je například zapínání světel, topení, či klimatizace na dálku.

Senzory mohou být s ústřednou propojeny buď drátově nebo bezdrátově. Pro drátové sběrnicové spojení se používá kroucená dvojlinka pro zabránění indukci rušení a přeslechů. Jeden pár dvojlinky je použit pro napájení senzoru a druhý pár dvojlinky slouží k přenosu dat. Firma Jablotron používá pro napájení dvoulinku s větším průřezem než pro datovou komunikaci kvůli potřebě přenosu většího proudu než je tomu u datového přenosu. Bezdrátové spojení je realizováno na principu vysílač-přijímač nejčastěji s poloduplexním režimem, tj. vždy může komunikovat pouze jedna strana současně.

Firma Jablotron momentálně na trhu nabízí čtyři základní typy ústředen. Ústředny typu JA-101 (Obr. 1) a JA-103 jsou koncipovány do menších objektů, typicky rodinných domů a menších firem.

Obr. 1:Ústředna JA-101K [26]

Ústředny typů JA-106 a JA-107 jsou nejnovější ústředny a jsou reakcí na poptávku zákazníků o možnost připojení většího množství detektorů. Ústředny jsou určeny do velkých objektů, například do škol, či kancelářských budov, které vyžadují zabezpečení více sekcí a přístupu velkého množství uživatelů. Ústředna JA-106K podporuje připojení až 120 sběrnicových nebo bezdrátových zón s přístupem až 300 uživatelů. Typ JA-107 poté rozšiřuje počet uživatelů až na 600 a počet sběrnicových periferií na 230.

1.1 Bezdrátové technologie

Pro komunikaci ústředny se senzory a ke vzdálenému přístupu k ústředně se používají bezdrátové technologie. Nejpoužívanější technologie jsou popsané níže.

1.1.1 Wifi

Je technologie pro bezdrátový přenos ethernetových rámců. Tuto technologii popisuje norma IEEE 802.11 [1], která existuje v několika verzích, také nazývaných standardy nebo generace. Liší se frekvenčním pásmem a maximální rychlostí přenosu. V oblasti zabezpečovacích systémů je nejčastěji používané frekvenční pásmo 2,4 GHz. Nejnovější ústředny mohou mít navíc podporu 5 GHz pásma. V zabezpečovacích systémech se používá pro komunikaci ústředny s mobilním telefonem nebo pro odesílání dat na server.

1.1.2 Bluetooth

Je velmi používanou bezdrátovou technologií v zabezpečovacích systémech. Bluetooth je definován standardem IEEE 802.15.1 [2], jenž existuje v několika verzích, které se liší pouze maximální přenosovou rychlostí. Frekvenční pásmo této technologie je ve všech verzích 2,4 GHz. Technologie Bluetooth se vyskytuje v zabezpečovacích systémech pro komunikaci bezdrátových senzorů s ústřednou a některé zabezpečovací systémy používají technologii Bluetooth pro nastavení parametrů ústředny pomocí mobilní aplikace.

1.1.3 433 MHz

Je pásmo používané pro bezdrátový přenos. Používá se výhradně pro komunikaci prvků inteligentní domácnosti. Pro komunikaci senzorů s ústřednou se již používá velmi zřídka, kvůli náchylnosti k zarušení od zařízení jiného výrobce využívající stejné frekvenční pásmo pro komunikaci.

1.1.4 Zigbee a ostatní technologie

Zigbee je bezdrátová komunikační technologie řídící se standardem IEEE 802.15.4. [3]. Jedná se o nízkovýkonovou technologii, nejčastěji pracující na frekvenčním pásmu 868 MHz. V tomto frekvenčním pásmu na zařízení nepůsobí rušení od zařízeních používající technologie Bluetooth nebo Wifi, kterých bývá v domácnosti a blízkém okolí mnoho. Zigbee se používá v ústřednách pro chytré domácnosti. Umožňuje sdružovat komponenty chytré domácnosti jako například termostaty, chytrá světla, elektrické zásuvky či audio systémy, které lze poté ovládat pomocí jedné mobilní aplikace.

Existuje mnoho dalších bezdrátových technologií, které se vyskytují v oblasti zabezpečovacích systémů a chytrých domácností. Většina z nich pracuje na velmi podobném principu jako technologie Zigbee, například Z wave.

Firma Jablotron si vyvinula svou vlastní bezdrátovou šifrovanou technologii nazývanou Protokol Jablotron. Je použita pro komunikaci bezdrátových senzorů s ústřednou. Tato technologie využívá frekvenční pásmo 868,1 MHz.

1.1.5 Zhodnocení drátového a bezdrátového propojení

Nevýhoda drátového propojení senzorů s ústřednou je nutnost drážkování zdí pro vložení kabelů, které je u již zabydlených objektů náročné nebo vložení kabelů do kabelové lišty, které ovšem po estetické stránce ve výsledku nevypadá dobře. Tudíž realizace drátových rozvodů pro senzory je vhodnější pro novostavby. Do již zařízeného domu je vhodné použít bezdrátové spojení, u kterého není nutné řešit kabeláž. Nevýhodou bezdrátového spojení je nutnost pravidelných výměn baterií v senzorech a lehce vyšší cena oproti drátovým senzorům. K drátovým senzorů je ale také nutné připočíst cenu rozvodné kabeláže a její instalaci, tudíž cena drátových a bezdrátových senzorů je téměř totožná.

2 Senzory

Každý zabezpečovací systém musí mít správně rozmístěné senzory, jinak mohou vznikat slepá místa či falešné poplachy a tím se stává zabezpečovací systém nespolehlivý. Další kritérium pro dobře fungující zabezpečovací systém je správný výběr technologie senzorů. Pokud máme například volně pohybující se mazlíčky nebo velmi prašnou místnost, musíme tomu přizpůsobit umístění senzoru a správnou technologii detekce.

2.1 Perimetrická ochrana

Jako první detekuje narušitele perimetrická ochrana, která se nachází hned za mechanickou zábranou, typicky plotem. Nejrozšířenějším typem perimetrické ochrany je infračervená závora detekující přerušení infračerveného paprsku, vyzařovaného po celé délce plotu. Alternativou je mikrovlnná závora, která je více nákladná na pořízení, ale disponuje menší náchylností na falešné poplachy. Další možností je instalace otřesových senzorů nebo mikrofonního obvodového kabelu podél celého perimetru, detekující jakoukoliv manipulaci či stříhání plotu.

Velmi doporučovanou variantou perimetrické ochrany je venkovní kamerový systém. Na výběr jsou kamery s jednoduchou detekcí pohybu, kamery s možností rozpoznání obličeje nebo termální a bispektrální kamery, kombinující senzor zachycující viditelné spektrum a senzor zachycující infračervené záření. Užitečným doplňkem kamery, pokud tím sama kamera nedisponuje, je obousměrný audio přenos. Cituji [22]: „Pokud je dům zabezpečen perimetricky, zásahové jednotky k němu prakticky vůbec nevyjíždí, PCO ani většinou nemusí nikomu volat a na domě nevznikají žádné škody. Díky kamerám s nočním viděním operátor PCO přesně ví, jak narušitel vypadá a když se najednou odněkud uprostřed noci ozve: „Hej ty v té tmavé bundě s kapucou, opusť prostor, volám policii!“ – funguje to více než spolehlivě.“

2.2 Plášťová ochrana

Další úrovní zachycení narušitele je plášťová ochrana, která se nachází na povrchu objektu a skládá se především z detektorů tříštění skla a magnetických senzorů, detekující otevřené okno nebo dveře. Obrovskou výhodou jsou nulové falešné poplachy. Nevýhoda je, že k detekci dochází až po škodě na majetku, tedy po vypáčení či rozbití okna nebo dveří.

Pro plášťovou ochranu nabízí firma Jablotron bezdrátový magnetický detektor JA-151M vyobrazený na Obr. 2. Na okna, popřípadě dveře s velkou skleněnou výplní je možné použít akustický detektor rozbití skla JA-180B viz Obr. 3.

Obr. 2:Magnetický detektor [29]

Obr. 3:Detektor rozbití skla [29]

2.3 Prostorová ochrana

Naposledy existuje prostorová ochrana využívající především detektory pohybu uvnitř zabezpečeného objektu. Jako detektory pohybu se nejčastěji používají pasivně infračervené detektory v kombinaci s mikrovlnnými detektory nebo vnitřní kamerový systém. Veškerá prostorová ochrana je náchylná na falešné poplachy, pokud se v objektu nachází volně se pohybující zvířata.

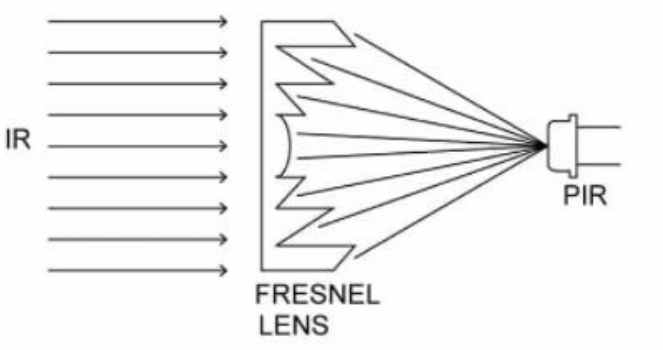
Prostorovou ochranu lze ještě rozdělit na předmětovou ochranu, jež je používaná pro ochranu důležitých a cenných předmětů, umístěných například ve skleněné vitríně s tříštivým detektorem na detekční ploše reagující na změnu hmotnosti.

2.4 Detektory pohybu

2.4.1 Pasivní infračervený senzor (PIR)

PIR senzor využívá toho, že každý objekt včetně lidského těla vyzařuje teplo ve formě elektromagnetického záření. Senzor registruje náhlé změny v intenzitě elektro- magnetického záření, které indikují přítomnost osoby v místnosti.[4] .

Součástí každého PIR senzoru je optika umístěná před senzorem [56]. Optika se skládá z Fresnelových čoček, které soustřeďují infračervené záření do senzoru jak lze vidět na Obr. 4. Počet čoček udává počet segmentů, neboli počet detekčních zón senzoru. Optiku lze navrhnout tak, aby větší částí snímala horní část místnosti, toho se využívá pokud se v místnosti volně pohybují zvířata.



Obr. 4:Optika PIR senzoru [56]

Zásady při instalaci PIR senzoru:

Senzor by se měl instalovat na pevnou zeď do výšky přibližně 2-3 m. Měl by se nacházet ideálně v místech kde se pachatel pohybuje kolmo k senzoru, tudíž by se senzor neměl instalovat přímo nad dveře. Taktéž se senzor nesmí instalovat naproti oknům a do míst, s jakoukoliv náhlou změnou teploty zapříčiněnou topením, klimatizací nebo vytápěnými podlahami. [3] Pokud se instalují PIR senzory do velké místnosti, je třeba zajistit, aby se jejich detekční zóny překrývaly a nevznikly tak slepá místa. K falešným poplachům kvůli překryvu nebude docházet, jelikož se jedná o pasivní senzor, který do okolí nevyzařuje nic, co by ovlivnilo funkci jiných PIR senzorů.

2.4.2 Aktivní ultrazvukový senzor (US)

US senzor pohybu využívá odrazu ultrazvukových vln na principu Dopplerova jevu. Senzor se skládá z vysílače a přijímače. Vysílač vysílá do okolí ultrazvukové vlny o frekvenci cca 40 kHz. Přijímač vyhodnocuje změnu frekvence odraženého paprsku vůči vysílané frekvenci. Po chvilce se v místnosti vytvoří klidový stav, kde má vlna vysílaná a přijímaná stejný kmitočet. Pokud se v místnosti objeví narušitel, dojde ke změně kmitočtu přijímané vlny. [4]

Zásady při instalaci US senzoru:

Senzor by se měl ideálně instalovat nad, nebo naproti dveřím, aby se narušitel pohyboval rovnoběžně k senzoru. Pokud se instaluje více senzorů vedle sebe, je nutné aby se jejich detekční zóny nepřekrývaly. Mohlo by poté dojít k nežádoucí situaci, kdy jeden senzor přijme vysílaný signál z druhého senzoru.

Ultrazvukové senzory by se neměly instalovat v prostorech, kde se vyskytují domácí mazlíčci a teplovzdušné ventilátory (přímotopy) a další topná tělesa s vysokou teplotou. V detekčním prostoru senzoru by se neměly nacházet předměty zhoršující „viditelnost“ jako jsou lampy nebo lustry a je třeba brát v potaz, že absorpční materiály, jako je koberec, snižuje dosah senzoru kvůli pohlcení části vln.

2.4.3 Aktivní mikrovlnný senzor (MW)

MW senzor pracuje na stejném principu jako ultrazvukový senzor pohybu, tj. přijímané odražené vlny mají jinou frekvenci než vlny vysílané. Vlny se vyzařují do okolí pomocí mikropáskového vedení umístěného uvnitř senzoru. Obvyklé vyzařovací frekvence elektromagnetické vlny jsou 2,5 GHz, 10 GHz, nebo 24 GHz. [4]

Zásady při instalaci MW senzoru:

Mikrovlnný senzor se musí instalovat naproti dveřím, aby se narušitel k senzoru přibližoval rovnoběžně. Mikrovlnné záření je pohlcováno vodivým materiálem, proto je nutné dbát na to, aby se v detekční zóně nenacházely velké kovové předměty, jakými jsou například kovové potrubí nebo vodní vedení. V prostoru by se neměly nacházet zapnuté zářivky s vysokonapěťovým buzením a další mikrovlnné senzory se stejnou vysílací frekvencí. Mikrovlnné záření má dobré penetrační vlastnosti, tudíž prochází

zdmi a je nutné při instalaci zkontrolovat, zda MW senzor nedetekuje některý z negativních vlivů popsaných výše v jiné místnosti a popřípadě senzor umístit na jiné místo nebo změnit jeho úhel snímání, tak aby nedocházelo k falešným detekcím.

2.4.4 Duální senzor

Využívá předchozích technologií v kombinacích PIR+MW, PIR+US, PIR+PIR (rozdělení detekovaného prostoru na dvě horizontální části). Každá technologie má se výhody i nevýhody, použitím dvou technologií zároveň lze eliminovat některé nevýhody jednotlivých technologií a snížit počet falešných poplachů. [4]

Firma Jablotron nabízí několik verzí detektorů pohybu, včetně duálních s kombinovanou technologií PIR+MW u modelu JA-162PW nebo PIR detektor s vestavěnou kamerou JA-160.

2.4.5 Detektory pohybu jako prvek inteligentní domácnosti

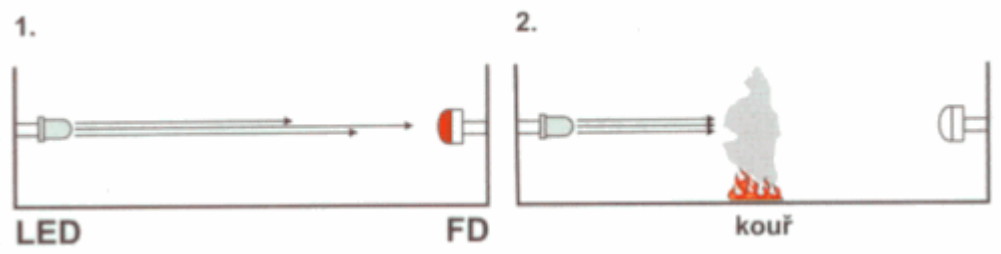
Detektory pohybu nemusí nutně sloužit pouze k zabezpečení, ale lze je použít jako prvek chytré domácnosti. Detektor pohybu lze využít k automatickému rozsvícení, popřípadě i zhasínání světel. Velmi užitečné umístění může být v oblasti schodů, kde nemusíme ve tmě poslepu nahmatávat vypínač, ale světlo se zapne detekcí pohybu automaticky. [6]

2.5 Požární detektory a detektory plynu

Požární detektory jsou zapnuté nonstop, nezávisle na tom, zda je střežený objekt uzamknutý či odemknutý. Při použití zabezpečovacího systému s požární ochranou připojený na pult centrální ochrany, tak při zaznamenání požáru nebo požárního nebezpečí při úniku plynu, má možnost pult centrální ochrany zavolat na místo hasičský záchranný sbor, popřípadě jiné složky IZS.

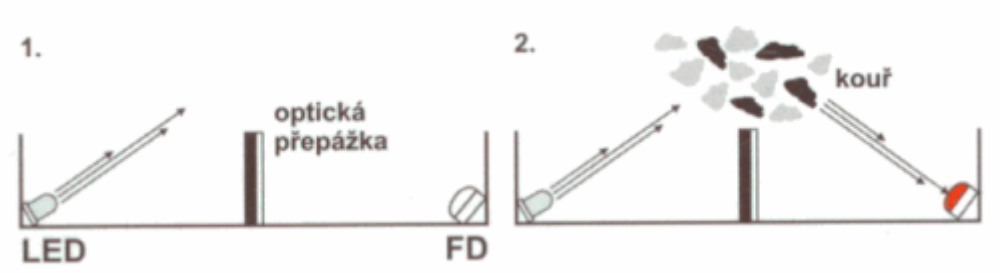
2.5.1 Kouřový požární detektor

Pracuje na fotoelektrickém principu. Na jedné straně se nachází zdroj světla, většinou infračervená dioda (IRED) a naproti je umístěna fotodioda snímající záření z IRED. Existují dva druhy detektorů využívající fotoelektrický princip. První způsob detekce funguje na principu blokování průchodu světla kouřem, kde se nachází IRED a fotodioda naproti sobě. V běžné situaci fotodioda detekuje světlo z IRED viz první část Obr. 5. Pokud se mezi fotodiodu a IRED dostane kouř, přeruší se průtok světla do fotodiody a vyhlásí se poplach viz druhá část Obr. 5. [8]



Obr. 5: Kouřový detektor na principu blokace [8]

Druhý způsob detekce je na principu odklonu paprsků světla pomocí kouře. IRED a fotodioda nejsou nasměrovány přesně proti sobě, ale jsou umístěny pod úhlem. V normální situaci fotodioda nedetekuje žádné světlo vyzařované IRED viz první část Obr. 6. Pokud se mezi IRED a fotodiodu dostane kouř, dojde k lomu světelných paprsků IRED, které detekuje fotodioda viz druhá část Obr. 6. [8]



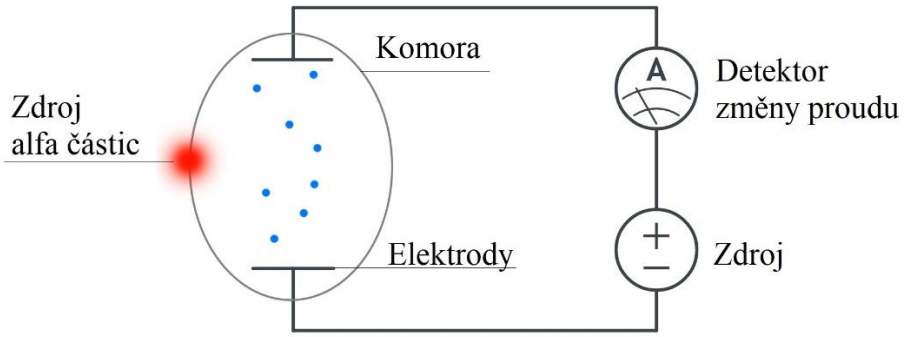
Obr. 6: Kouřový detektor na principu lomu paprsků [8]

Zásady instalace kouřového detektoru:

Tento druh detektoru by se neměl instalovat v prašných prostorách a prostorách s vysokou vlhkostí. Senzor se umisťuje na strop, jelikož horký kouř stoupá směrem vzhůru a hromadí se u stropu. Senzor se nesmí instalovat do míst, kde se běžně vyskytuje hoření nebo nadměrná tvorba kouře, tj. neinstaluje se do kuchyní nebo blízko kamen či bojlerů. Pokud je v domě klimatizace nebo nějaký ventilační systém, senzor se umisťuje alespoň do minimální vzdálenosti od ventilace dané výrobcem senzoru, obecně to bývá minimálně 1 metr od ventilačních systémů, jinak by v případě požáru mohlo dojít k odsávání kouře a detektor by v počátku požáru nezaznamenal nic. Je doporučeno senzor instalovat do každé místnosti v objektu, do které je senzor koncipován, především do ložnice. Pokud objekt obsahuje více pater, instaluje se mimo jiné také nad schodiště.

2.5.2 Ionizační požární detektor

Reaguje na změny vodivosti vzduchu uvnitř ionizační komory v senzoru. Vzduch je ionizován pomocí alfa částic, které generuje radioaktivní prvek v senzoru. Při přítomnosti nebezpečného plynu v senzoru dojde ke změně procházejícího proudu mezi elektrodami viz Obr. 7. Senzor dokáže zachytit i páry vznikající při vaření a vývinu hořlavých plynů. Riziko požáru lze tak detekovat ještě před vznikem hoření. Jeden detektor dokáže detekovat několik druhů nebezpečných plynů nezávisle na vlivu teploty a vlhkosti.



Obr. 7: Princip ionizačního detektoru plynů

Zásady instalace ionizačního detektoru:

Používá se v místech, kde není možné použít klasický kouřový detektor. Lze ho použít v prašných a vlhkých prostorech. Senzor se nesmí instalovat do prostorů, kde se může vyskytovat otevřený oheň nebo horké páry vznikající v kuchyni při vaření, nebo blízko kamen či krbu.

2.5.3 Teplotní požární detektor

Existují dva typy teplotního požárního detektoru:

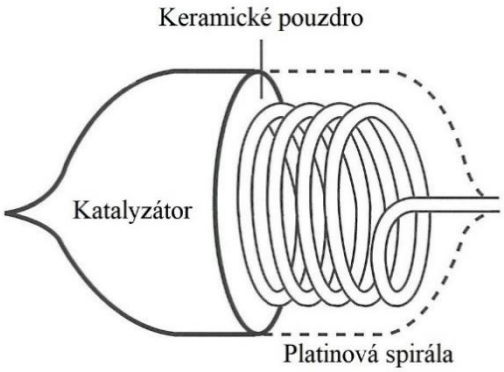
- Termomaximální - detekuje překročení maximální nastavené teploty v místnosti
- Termodiferenciální - sleduje jak rychlý je nárůst teploty (gradient). Pokud je nárůst vyšší než nastavený, senzor sepne alarm.

Zásady instalace teplotního detektoru:

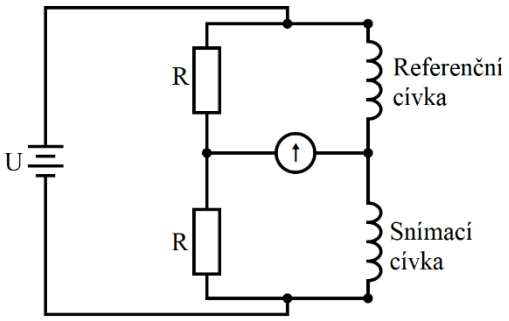
Senzor lze nainstalovat prakticky kamkoliv, ale primárně je požíván v kuchyni a v blízkosti krbu nebo kamen. Je však nutné správně nastavit minimální meze detekce senzoru pro zamezení falešných poplachů například při otevření kamen.

2.5.4 Detektor hořlavých plynů

Funguje na principu katalitického spalování. Uvnitř senzoru se nachází dvě platinové spirály zapojené do Wheatsonova můstku viz Obr 9. [12]. [57] Jedna spirála je napuštěna speciálním katalizátorem, který podporuje oxidaci daného hořlavého plynu a druhá spirála je napuštěna katalizátorem, který naopak potlačuje oxidaci plynu, koncepci senzoru lze vidět na Obr. 8. Pokud se detekovaný hořlavý plyn dostane do blízkosti senzoru, dojde k rozvážení Wheatsonova můstku a následnému sepnutí alarmu.



Obr. 8: Senzor katalitického spalování [57]



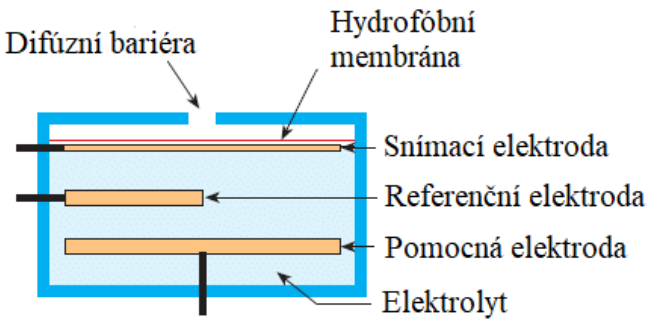
Obr. 9: Schéma zapojení senzoru katalitického spalování

Zásady instalace detektoru hořlavých plynů:

Umisťují se do míst, kde může dojít k úniku hořlavých plynů. V domácnostech se nejčastěji jedná o plynové sporáky nebo plynová kamna. Senzor se umisťuje v závislosti na typu plynu. Senzor pro detekci zemního plynu (LNG, CNG), který je lehčí než vzduch, se umisťuje ke stropu. Senzor pro detekci propan butanu (LPG), který je těžší než vzduch, se umisťuje k podlaze [10], [11].

2.5.5 Detektor oxidu uhelnatého

Funguje jako elektrochemický senzor. Skládá se z několika malých elektrod umístěných v gelovém elektrolytu s difúzní bariérou, která detekuje přítomnost oxidu uhelnatého viz schéma na Obr. 10. [55] Pokud se na difúzní bariéře objeví oxid uhelnatý, dojde k chemické reakci, díky které dojde ke změně potenciálu na elektrodách a přes vyhodnocovací elektroniku dojde ke spuštění alarmu [13]. Oxid uhelnatý vzniká například při nedokonalém hoření v kamnech a ve větším množství je pro člověka nebezpečný.



Obr. 10: Koncepce elektrochemického senzoru CO [55]

Zásady instalace detektoru oxidu uhelnatého:

V případě, že je domácnost vytápěná kamny spalující fosilní paliva, je dobré tento senzor umístit do místnosti, kde se kamna nacházejí. Oxid uhelnatý je o něco málo lehčí než vzduch, senzor se instaluje přibližně půl metru pod úroveň stropu.

2.5.6 Duální požární detektory

Komplexnější senzory obsahují kombinaci těchto technologii, aby bylo možné zabezpečit větší oblast potenciálních rizik s jedním senzorem. Zpravidla se používají kombinace kouřového detektoru a detektoru změny teplot do oblasti kuchyň. Poplach se vyhlásí poté co sepnou oba senzory zároveň, tj. v místnosti se objeví jak kouř, tak náhlá změna teploty. Požární detektory se také instalují do garáží, kde jsou často doplněny hasícím zařízením ve formě sprinklerů.

Od firmy Jablotron je dostupný duální požární detektor, využívající kombinaci optické detekce kouře spolu s termodiferenciálním senzorem JA-150ST, zobrazený na Obr. 11, který je možný zakoupit ještě ve verzi s vestavěnou sirénou [30].

Obr. 11:Detektor kouře JA-150ST [30]

2.6 Magnetické senzory

Magnetické senzory na okna a dveře fungují na principu detekce přítomnosti magnetického pole. Ve většině případů je využíváno magnetického jazýčkového kontaktu (Obr. 12), umístěného v jedné části senzoru spolu s vyhodnocovací elektronikou. Druhá část senzoru je tvořena permanentním magnetem, buď feritovým nebo neodymovým. Při přiblížení permanentního magnetu ke snímacím kontaktům dojde k jejich zmagnetizování a následnému spojení.

Obr. 12:Magnetický jazýčkový kontakt

3 Přístupové systémy

3.1 RFID

Přístupové systémy RFID neboli česky radiofrekvenční identifikace je bezkontaktní technologie pro přenos dat mezi transpondérem a čtečkou [14]. U zabezpečovacích systému se jedná o pasivní transpondéry bez nutnosti napájení. Skládají se z mikročipu a antény, nejčastěji umisťované buď do malého čipu na klíče nebo karty. Čtečka vysílá do prostředí elektromagnetické vlny, které jsou při přiblížení transpondéru pohlceny anténou, na které se indukuje napětí, jež následně napájí čip, na kterém jsou uložena data. Pomocí časovaného tlumení proudu pak transpondér zpět vysílá signál, který přijme čtečka.

Přístupové RFID systémy jsou převážně používány v kancelářských prostorech, pro monitorování příchodů a restrikci přístupu, pokud je objekt rozdělen do zón. Systém se již také začíná objevovat u rodinných domů pro usnadnění přístupu, kde není nutné zadávat číselný kód.

3.2 Biometrické přístupové systémy

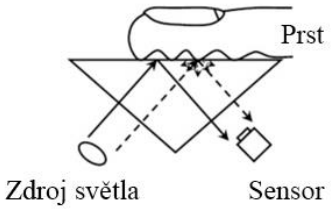
Velkou výhodou biometrických systémů je zvýšená bezpečnost oproti klasickým přístupovým systémům s hardware klíčem, který může být odcizen nebo ztracen. Zároveň se zvýšením bezpečnosti se jedná o ulehčení, jelikož odpadá nutnost nošení klíče či karty. Biometrické systémy využívají unikátnosti lidského těla, především se využívá otisk prstu, sken obličeje nebo oční duhovky. Tyto části těla má každý člověk jedinečné a neměnné, pokud se fyzicky nepoškodí [17]. Prolomení tohoto způsobu přístupu je téměř nulové, pokud je použita dostatečně pokročilá technologie, která by měla odpovídat úrovni zabezpečení, které by měl objekt dosahovat.

3.2.1 Sken otisku prstu

Skenování otisku prstu se stalo velmi hojně využívaným způsobem zabezpečení u mobilních telefonů, tabletů, přenosných počítačů a také v zabezpečovacích systémech [15], [16], [17].

Optická metoda skenování

První a také nejstarší způsob snímání otisků prstů je pomocí optické metody, kde světelný zdroj vyzařuje světelné paprsky, které se lámou na dotykové ploše do senzoru, jak je vyobrazeno na Obr. 13. V případě, že se dotykové plochy nic nedotýká, se všechny světelné paprsky lámou do světelného senzoru. Po přiložení prstu se na vyvýšených místech prstu, tzv. papilárních liniích pohltí světelný paprsek a do světelného senzoru se dostane jen část paprsků, které nepřišly do kontaktu s papilárními liniemi. Pomocí algoritmů se poté porovná právě naskenovaný otisk prstu s referenčním otiskem uloženým v paměti. Tento druh skenování není až tak bezpečný, jelikož se jedná o dvourozměrnou technologii skenování. Senzor lze oklamat výtiskem otisku prstu na obyčejné inkoustové tiskárně.

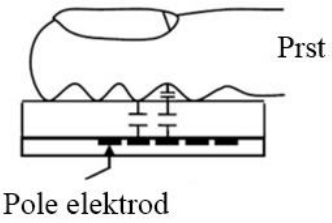


Obr. 13:Optická metoda skenování [18]

Kapacitní metoda skenování

Tato metoda je založena na uchování elektrického náboje ve shluku drobných kondenzátorů, které jsou schopny po přiblížení prstu ke snímači velice přesně zjistit tvar papilárních linií, jak je vidět na Obr. 14 [18]. V místě výstupků dojde v kondenzátoru ke změně náboje, naopak v případě prohlubní zůstane elektrický náboj nezměněn. Tyto data se poté převedou do digitální podoby a porovnají se s předlohou, uloženou v paměti.

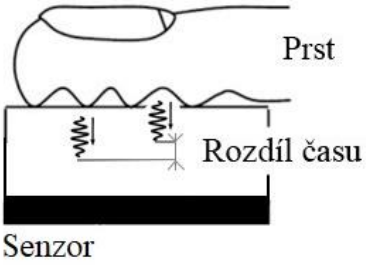
Počet kondenzátorů v senzoru určuje celkové rozlišení a také bezpečnost. Větší rozlišení se rovná větší bezpečnosti. Dalo by se říci, že se jedná o 2,5D metodu skenování, kdy se zaznamenávají jak výstupky, tak prohlubně otisku prstu, ale rozdíl vzdáleností mezi výstupkem a prohlubní je neznámý. I přes to, je tato metoda značně bezpečnější, než optická. Vyrobit prostorový falešný otisk prstu pro oklamání čtečky z pouhé fotografie je již téměř nemožné.



Obr. 14:Kapacitní metoda skenování [18]

Ultrazvuková metoda skenování

Patří mezi nejmodernější dostupné metody. Ultrazvukový vysílač, vysílá vlny o vysoké frekvenci. Vlny odražené od papilární linie prstu dorazí do ultrazvukového přijímače později, protože musí urazit větší vzdálenost, než ostatní vyslané vlny. Z rozdílu časů přijímaných vln lze dopočítat i hloubku papilární linie prstu viz Obr. 15 [18]. Rozlišení výsledného skenu závisí na množství vysílačů a přijímačů, které jsme schopni integrovat na malou plochu senzoru. Větší rozlišení senzoru odpovídá větší úrovni zabezpečení. Po digitálním zpracováním lze vytvořit 3D model otisku prstu, který se porovná s již uloženým referenčním modelem. Hlavní výhodou této technologie oproti optické a kapacitní je, že funguje i s mokrými či vlhkými prsty a tudíž lze ultrazvukové skenování použít i pod vodou.



Obr. 15:Ultrazvuková metoda skenování [18]

3.2.2 Skenování oční duhovky

Oči jsou jednou z nejunikátnějších částí těla, kterou lze jednoduchým způsobem použít pro skenování. S dnešní technologií je možné rozpoznávat až 225 charakteristických bodů duhovky, která se skládá z vazů a tkání, které se tvoří náhodně už ve fázi těhotenství. Teoretická možnost, že by dvě oční duhovky byly identické, je kolem 10^{78}, můžeme tedy říci, že duplicita je nemožná [19]. Skenování duhovky je na rozdíl například od skenování sítnice mnohem jednodušší. Pro sken duhovky není třeba optický snímač s nastavitelnou ohniskovou vzdáleností, jako je tomu v případě skenování sítnice. Skener využívá optický CMOS snímače, který obsahuje maticově uspořádané unipolární transistory citlivé na světlo. Jako zdroj světla je zde umístěna NIR dioda, vyzařující tzv. blízké infračervené spektrum ve vlnové délce 730-2500 nm. Infračervené světlo je pohlcováno některými lidskými tkáněmi a díky tomu lze pomocí CMOS snímače zachytit strukturu tkáně oční duhovky. Skener duhovky funguje i s dioptrickými brýlemi a kontaktními čočkami. Problém se skenem může nastat v případě hodně zatmavených nebo poškrábaných brýlí zapříčiňující nedokonalý sken [20].

3.3 Přístupová klávesnice

Klasická kódová klávesnice je nejrozšířenějším druhem přístupového systému díky její jednoduchosti. Samotné kódové klávesnice jsou často doplněny i jinou technologií pro ověření autorizace, například přístupová klávesnice s RFID čtečkou nebo s nějakou biometrickou přístupovou technologií. Při použití další technologie pro přístup se stává kódová klávesnice sekundární možností přístupu, například v krajní nouzi při zapomenutí nebo ztrátě RFID karty nebo čipu nebo při nuceném zadání kódu pod výhružkami přítomného pachatele. Pro tento krajní případ je v ústředně nastaven speciální kód, který běžně objekt odemkne a zároveň informuje pult centrální ochrany o nestandartním vniku.

4 Kamerový systém CCTV

Kamerový systém se může instalovat jako doplněk zabezpečovacího systému nebo samostatné zabezpečení vnějšího perimetru. Lepší kamerový systém s větším rozlišením a dobrým rozpoznávacím algoritmem dokáže rozpoznat velikost pohybujícího objektu a vyhodnotit, jestli se po zahradě pohybuje osoba nebo jen zvíře [21] [23].

V několika zdrojích [22] [24] je zmíněno, že kamerový systém v budoucnu pravděpodobně nahradí část EZS, jako například senzory dveří, oken a pohybové senzory, jelikož jedna kamera spolu s chytrým rozpoznáváním osob v obrazu dokáže tyto tři druhy senzorů nahradit. Tento trend chytrých kamer již zasáhl levnější třídu zabezpečovacích systémů určených pro samoinstalaci, kde se v systému nachází jedna nebo více kamer a centrální ústředna. Mezi hlavní výhody bezdrátových kamerových systémů je možnost okamžitého přístupu k živému přenosu a také k záznamům. Pokud je EZS s kamerovým systémem připojen na pult centrální ochrany, tak v případě poplachu má operátor bezpečnostní agentury přístup k přenosu z kamery, aby mohl potvrdit vniknutí.

Firma Jablotron momentálně nabízí dvě kamery JI-111C a JI-112C [27], které jsou vyobrazeny na Obr. 16. Kamery jsou plně propojitelné se systémem Jablotron s možností kontroly záznamu přes aplikaci MyJablotron. Kamery podporují rozlišení 1920 x 1080 bodů a 8 snímků za sekundu.

Obr. 16: JI-111C a JI-112C [27]

5 Standartní úrovně zabezpečení

Norma CSN EN 50 131-1 rozděluje úrovně zabezpečení podle rizika vniknutí a tím i definuje, jak pokročilý zabezpečovací systém je třeba použít na zabezpečení daného objektu [33]. Následující tabulka znázorňuje čtyři stupně úrovně zabezpečení dané normou CSN EN 50 131-1:

Tab. 1: Úrovně zabezpečení

Stupeň č.1 – nízké riziko	Rodinné domy, byty, garáže
Stupeň č.2 – nízké až střední riziko	Obchody, sklady, firmy
Stupeň č.3 – střední až vysoké riziko	Banky, klenotnictví, prodejny zbraní, tisky cenin, směnárny
Stupeň č.4 – vysoké riziko	Narušitel s promyšleným plánem na vniknutí a překonání EZS, PZTS. Jaderné elektrárny, sklady zbraní

5.1 Požadavky na EZS

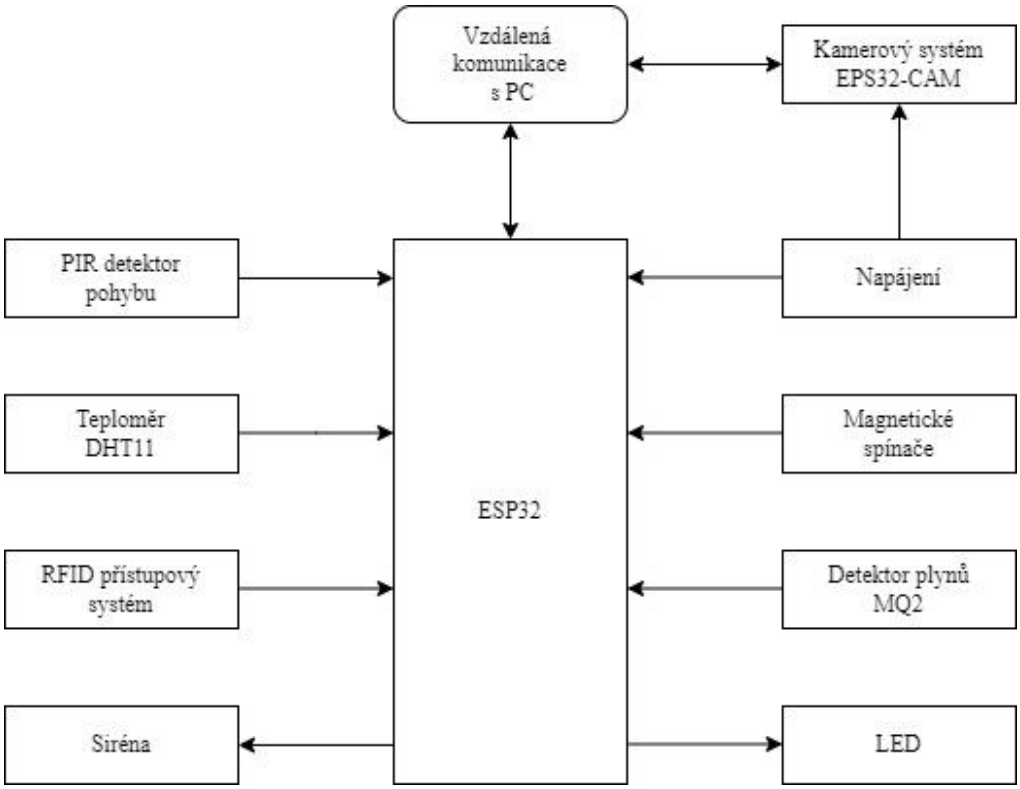
Prvky každého zabezpečovacího systému musí mít certifikaci minimálně pro stupeň zabezpečení, pro který je systém navrhován a musejí být dodržovány podmínky pro správnou montáž a konfiguraci.

Systém Jablotron je určen pro ochranu objektů s požadavkem na stupeň zabezpečení 2. Při stupni zabezpečení 3 a 4 je předpokládáno, že narušitel je obeznámen se zabezpečovacím systémem a podnikne patřičné kroky pro jeho překonání. Pro stupeň zabezpečení 3 je k dispozici na trhu systém Paradox - Digiplex nebo Honeywell -Galaxy Dimension [34].

II. Praktická část

6 Návrh modelu EZS

Cílem je navrhnout jednoduchý model elektronického zabezpečovacího systému včetně senzorů a prvků inteligentní domácnosti s možností monitorování a ovládání přes internet. Základní blokové schéma systému lze vidět na Obr. 17 níže. Jednotlivé prvky systému jsou probrány v dalších kapitolách.

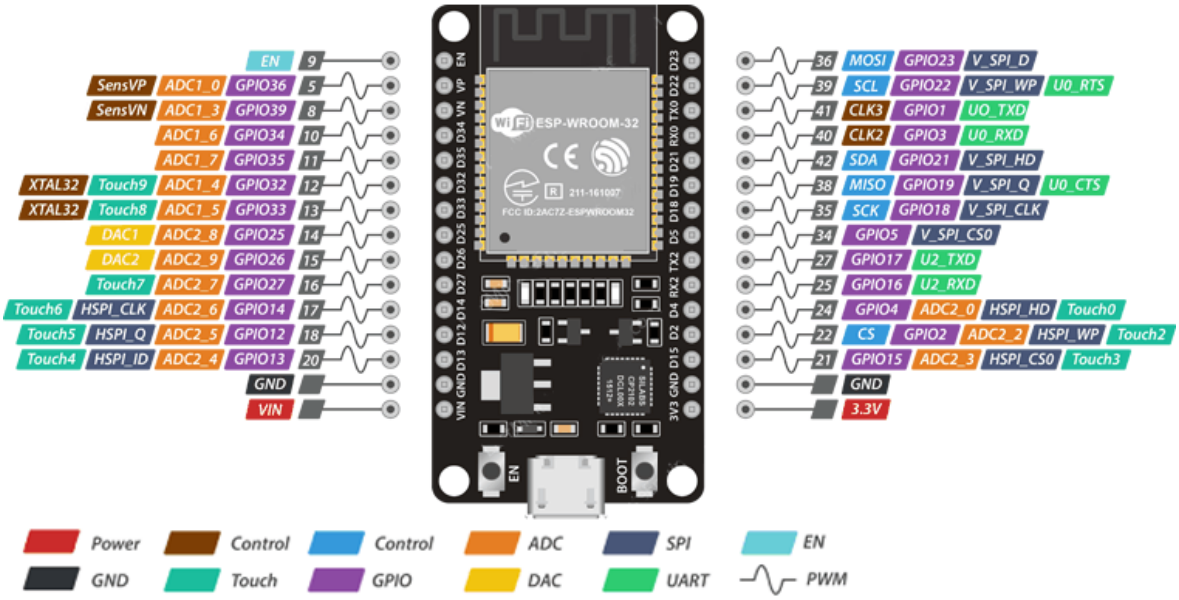


Obr. 17: Blokové schéma systému

6.1 Výběr vývojové desky

První bod je výběr vývojové desky, která slouží jako ústředna. Pro tento projekt jsem vybral vývojovou desku ESP-32 od firmy Espressif. Jedná se o desku s volně programovatelným procesorem s integrovaným WiFi rozhraním a spoustou dalších periférií. Disponuje dvoujádrovým procesorem Tensilica LX6 s počtem 34 plně programovatelných digitálních vstupně-výstupních pinů, anglicky General-purpose input/output označováno zkráceně GPIO. Rozložení pinů na desce je možné vidět na Obr. 18. Deska má 512 kB RAM paměti, kde je pro uživatele volných více než 270 kB. Velikou výhodou této desky jsou 4 MB SPI Flash paměti pro uložení kódu, který je

v tomto projektu poměrně obsáhlý z důvodu použití více knihoven pro senzory a web server. Volně programovatelné rozhraní WiFi na frekvenci 2,4 GHz, je využito pro komunikaci a ovládání přes internet [35], [36].



Obr. 18:ESP-32 [36]

Zvažoval jsem i volbu vývojové desky od firmy Arduino, ale to by z důvodu malé kapacity flash paměti procesorů Atmega používaných na deskách Arduino Uno nebo Mega nebylo možné. Výpočetní výkon 8-bitového procesoru Atmega by pravděpodobně na takto jednoduchou aplikaci stačil, ale díky obsáhlému kódu obsahující knihovny na webový server a mnoho senzorů, dosahuje zkompilovaný kód projektu velikosti kolem 800 kB, což je hodně, když to porovnáme s kapacitou flash paměti procesoru Atmega2560, která činí 256 kB a z toho je 8 kB zabraných bootloaderem. Proto je deska EPS32 ideální volbou pro tento projekt [36], [37].

Deska EPS32 pracuje na napětí 3,3 V, to znamená, že na vstupně-výstupních pinech GPIO se může objevit maximálně 3,3 V.[38] Některé použité senzory jsou ovšem napájeny z 5 V, tudíž jejich datový výstup má také úroveň 5 V a je nutné použít převodník logických úrovní z 5 V na 3,3 V aby nedošlo k poškození desky.

Programování desky probíhá přes USB kabel připojený k počítači s příslušnými ovladači a software (podrobněji rozebráno v kapitole 6.5 Software). Procesor na ESP32 nativně nepodporuje USB komunikační protokol, proto je na desce čip CP2102, který zajišťuje převod z USB na signály sériové linky UART, kterým již procesor ESP32 rozumí.

UART

Je komunikační rozhraní sloužící k asynchronnímu sériovému přenosu dat mezi zařízeními, v mém případě komunikace mezi počítačem a mikrokontrolérem ESP32 [39]. Pro toto rozhraní je nutno použít dvou datových spojení, jedno vysílací TX a druhé přijímací RX přičemž pin TX na jednom zařízení je připojena na pin RX druhého zařízení a pin RX prvního zařízení na TX druhého. Aby nebyla data při přenosu změněna, je potřeba aby odesílací zařízení posílalo data stejným tempem, jakým je přijímací zařízení očekává. UART využívá asynchronního přenosu dat, to znamená, že neobsahuje samostatnou linku s hodinovým signálem, ale před zahájením přenosu je předem nastavena modulační rychlost shodná na odesílacím a přijímacím zařízení.

Modulační rychlost neboli baud rate udává počet změn stavů za vteřinu a u ESP přímo vyjadřuje počet bitů za vteřinu. Při sériovém přenosu dat jdou data v řadě za sebou. Aby zařízení poznalo, kde data začínají a končí, jsou data seskupeny do útvarů nazývaných datové rámce viz Obr. 19.

Obr. 19:Datový rámec

Datový rámec UART protokolu se skládá ze start a stop bitu označující začátek a konec datového rámce. Start bit má vždy délku 1 bit s hodnotu logické 0. Stop bit může mít délku až 2 bity s hodnotu logické 1. Mezi start a stop bitem se nachází samotná data spolu s volitelnou paritou. Maximální délka dat dané protokolem je 5 až 9 bitů, tato délka se ale mezi zařízeními liší, u čipu CP2102 použitého v ESP32 je maximální délka dat 8 bitů při použití 1 start bitu a 2 stop bitů. Za datovými bity se může ještě nacházet 1 paritní bit, který slouží jako kontrola, zda nebyla data po cestě poškozena. Paritní bit obsahuje informaci o počtu logických 1 v datovém slovu. Pokud je lichý počet logických 1, paritní bit má hodnotu logické 1. Je-li počet logických 1 sudý, paritní bit má hodnotu logické 0 [40].

6.1.1 Historie Espressif

První známější produkt firmy Espressif je vývojová deska ESP8266, která měla původně sloužit jako WiFi převodník k Arduinu. To vše bylo v roce 2014 a oproti Arduinu, které má i dnes převážně desky s 8-bitovým procesorem, ESP8266 již mělo procesor 32- bitový s několika násobně vyšším výkonem než má Arduino.

Roku 2016 přišla firma Espressif s novou deskou ESP32, která měla vyřešit všechny neduhy, na které koncoví zákazníci starší desky poukazovali a chyběli jim. Původní jednojádrový procesor byl nahrazen dvoujádrovým procesorem, přidali operační systém s podporou multitaskingu, větší paměť, senzor magnetického pole a teploty, který je integrovaný v křemíkovém čipu a spoustu dalších vymožeností. Deska má taktéž nízkopříkonnový koprocesor (ULP koprocesor), který může být využit pro sběr dat ve chvíli, kdy je hlavní procesor uspaný, aby odebíral minimální proud. Při takovémto úsporném režimu je proudový odběr v řádů desítek mikroampérů [41].

6.2 Výběr senzorů

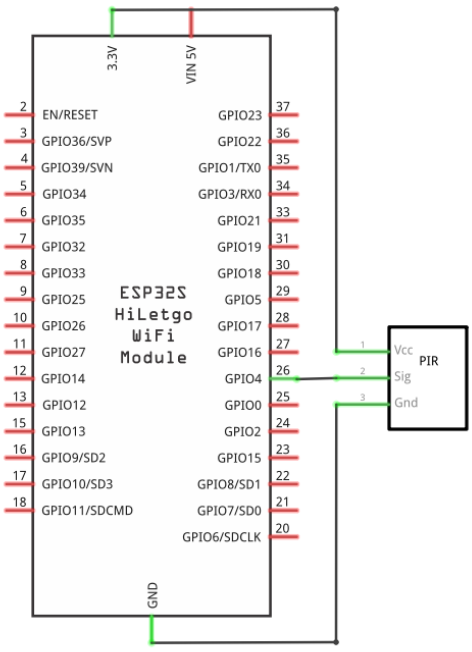
6.2.1 Detekce plynů a kouře

Pro detekci kouře a nebezpečných hořlavých plynů je použit senzor MQ-2 ukázaný na Obr. 20 [47]. Dokáže detekovat hořlavé plyny jako například propan-butan, isobutan, methan, což jsou plyny, které se v domácnostech používají jako topné palivo pro plynové topení nebo plynové sporáky. K dispozici je na výběr velké množství senzorů ze série MQ detekující zdraví nebezpečné plyny. Druh detekovaného plynu se musí volit podle rizika výskytu, pokud se v domácnosti vyskytují kamna spalující fosilní paliva, je vhodné použít senzor MQ-7 nebo MQ-9 detekující přítomnost oxidu uhelnatého, který vzniká nedokonalým spalováním a pro člověka může být velmi nebezpečný.

Obr.20:Detektor plynů MQ-2 [47]

6.2.2 **Detektor pohybu**

Jako detektor pohybu je použit modul PIR HC-SR501 s nastavitelnou citlivostí zobrazený na Obr. 22. Výrobce udává dosah detekce kolem 7 metrů a úhel detekce 120°. Tyto údaje jsou ověřeny jednoduchým měřením v kapitole 6.7.2. Modul je vybaven vyhodnocovacím čipem BISS0001 [42], který pracuje na TTL logice, tj. úroveň logické 1 odpovídá výstupnímu napětí od 2 V do 5 V a úroveň logické 0 odpovídá výstupnímu napětí 0 V až 0,8 V. Jelikož ESP32 pracuje na maximálním napětí 3,3 V a tento senzor je schopen poskytnout na výstupu až 5 V, je nutné u něj použít převodník logické úrovně z 5 V na 3,3 V. Na výstupním pinu se objeví hodnota logické 1, pokud senzor zaznamená pohyb. V klidovém stavu je na výstupním pinu logická 0. Výstupní pin je připojen na GPIO4 dle schématu zapojení na Obr. 21.

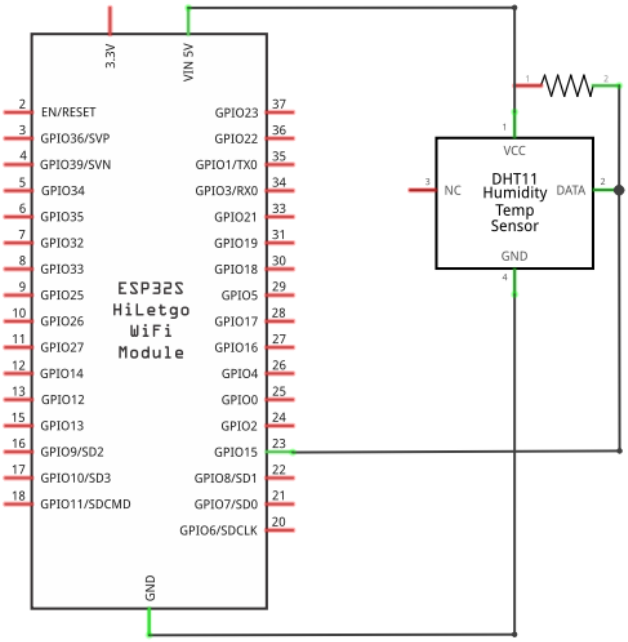


Obr. 21:Schéma zapojení PIR senzoru HC-SR501

Obr. 22:PIR senzor HC-SR501[42]

6.2.3 Senzor teploty a vlhkosti

Měření teploty a vlhkosti provádí senzor DHT11 na Obr. 24 s rozsahem měření teploty 0 až 60 °C a rozsahem měření vlhkosti 20 - 95 %. Senzor je zapojen dle schématu zapojení na Obr. 23, kde je datový pin připojen na GPIO15. Data o teplotě a vlhkosti se posílají do mikrokontroléru pomocí řetězce dlouhého 40 bitů [43]. Řetězec se skládá ze 3 základních částí, kde prvních 16 bitů nese informaci o vlhkosti, dalších 16 bitů informaci o teplotě a posledních 8 bitů slouží jako parita. Na výstupní pin je připojen pull up rezistor o hodnotě přibližně 5,1 kΩ, který slouží k vypnutí komunikační linky a uvolnění jednocestné komunikační linky pro jiné senzory připojené na stejnou linku.



Obr. 23:Schéma zapojení DHT11

Obr. 24:DHT11 [43]

6.2.4 **Detektor otevření oken a dveří**

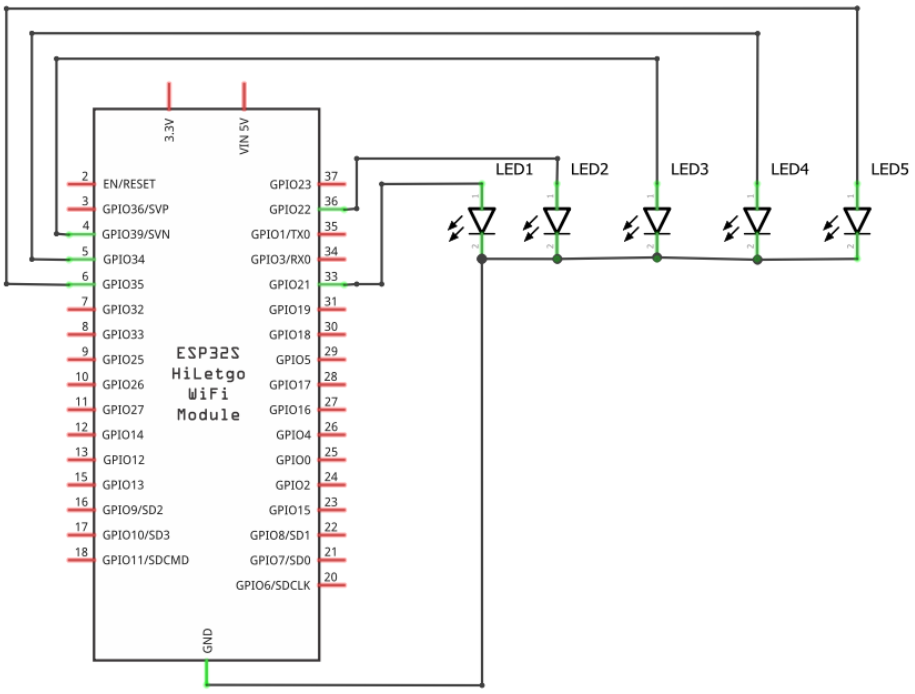
Detekování otevření oken a dveří zajišťuje magnetický jazýčkový kontakt. Pro zabezpečení navrhovaného modelu stačí čtyři magnetické detektory otevření. Jeden umístěn na vstupní dveře a zbylé tři na okna. Při použití většího množství těchto detektorů lze využít multiplexoru. V klidovém stavu, když je okno nebo dveře zavřené, je jazýčkový kontakt sepnutý a na vstupním pinu je logická 1. Po rozepnutí jazýčkového kontaktu se na vstupním pinu objeví logická 0.

Pro navrhovaný model je použit magnetický spínač Meder MK6-8-B, který jsem vybral ze čtyř testovaných magnetických spínačů. Cílem testu bylo zjistit jaký ze snímačů má nejmenší hysterezi z důvodu omezeného pohybu neodymového magnetu připevněného na dveřích a oknech. Při použití prvních magnetických spínačů z Obr. 25 zůstane jazýčkový kontakt spojený až do vzdálenosti 30 mm od magnetu. U posledního magnetického snímače, který je také v modelu použit je tato vzdálenost pouze 5 mm. Pro demonstrační potřeby je snímací vzdálenost 5 mm dostatečná, při reálném použití by bylo vhodné použít magnetické snímače s větší citlivostí, jak z důvodu zamezení falešných poplachů způsobených nepatrným pootevřením, tak snadnější montáží umožňující instalaci v nějaké toleranční vzdálenosti magnetického spínače od magnetu.

Obr. 25:Magnetické kontakty

6.2.5 **Osvětlení modelu**

Chytré osvětlení interiéru modelu a indikační LED jsou zapojeny podle schématu na Obr. 26. Tři bílé LED slouží jako chytré osvětlení, které je možné ovládat vzdáleně přes internet. Zbylé tři barevné indikační LED slouží jako vizuální informace, v jakém stavu se objekt nachází. Červená LED značí narušení objektu, zelená LED označuje uzamčený objekt a žlutá LED zobrazuje odemknutý objekt. Před každou LED byl do série přidán předřadný rezistor 330 Ω pro snížení napětí na samotné LED, kvůli omezení protékajícího proudu LED pro prodloužení životnosti a také snížení intenzity světla.

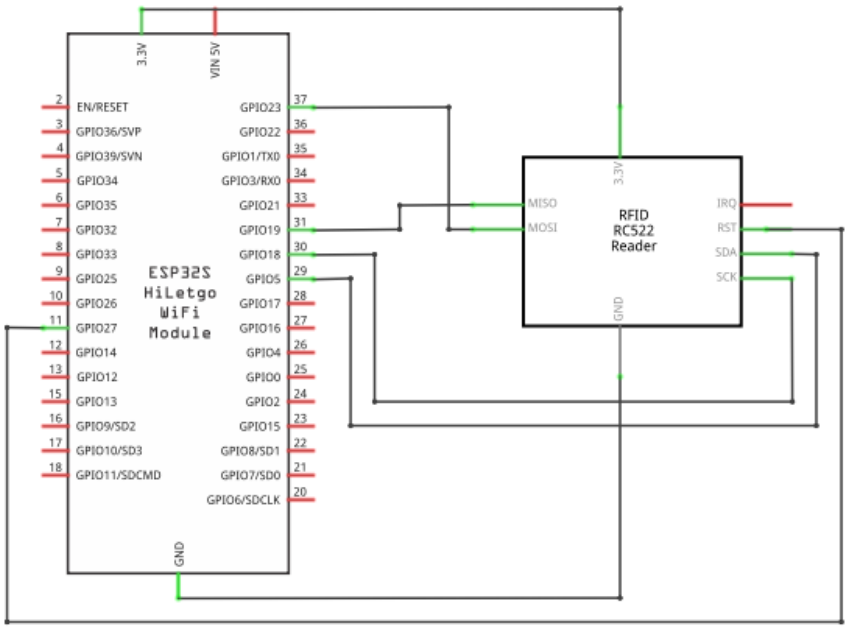


Obr. 26: Schéma zapojení LED

6.2.6 **Přístupový systém**

Pro přístupový systém bude použita RFID čtečka RC522, která umožňuje čtení a zapisování na MIFARE 13.56MHz bezkontaktní čipy [45]. Výrobce udává čtecí vzdálenost až 60 mm, kterou mohu testováním potvrdit. RFID čtečka RC522 umožňuje komunikaci přes sběrnice SPI nebo I^2C.

Schéma zapojení RFID čtečky k desce ESP32 lze vidět na Obr. 27 a samotný modul RC522 na Obr. 28.



Obr.27: Schéma zapojení RFID RC522

Obr.28: RFID RC522 [45]

I^2C

Je sběrnice pracuje podobně jako SPI na principu Master-Slave [47]. Každé Slave zařízení má svojí 7 bitovou adresu pro identifikaci. Komunikace probíhá po dvou linkách SDA a SCL. Po lince SCL se posílá hodinový signál a to vždy směrem Master→Slave. Linka SDA slouží pro navázání komunikace se Slave zařízením a následnému přenosu dat.

SPI

Serial Peripheral Interface [46] je sběrnice, která pracuje na principu Master-Slave. Master řídí celou komunikaci a rozhoduje jaké Slave zařízení bude v danou chvíli komunikovat. Výběr Slave zařízení probíhá přes samostatnou linku označovanou SS neboli Slave Select, do které Master zařízení pošle hodnotu logické 0. Pokud používáme SPI rozhraní pouze pro komunikaci dvou zařízeních mezi sebou, není nutné linku SS používat. Hlavní komunikace probíhá na dvou linkách MISO a MOSI. Linka MOSI slouží pro komunikaci Master→Slave a linka MISO pro komunikaci Slave→Master. Obě komunikační linky mohou být používány najednou, jedná se proto o plně duplexní přenos. Spolu s datovými komunikačními linkami MISO a MOSI je nutné použít hodinový signál SCLK, jelikož SPI je synchronní rozhraní.

6.2.7 Siréna

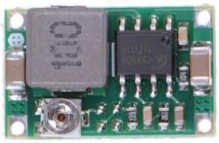
Jeden z akčních členů systému je výstražný zvuk, který bude zajišťovat aktivní elektromagnetický bzučák viz Obr. 29 [48]. Tento typ bzučáku funguje na principu rozkmitání kovové membrány, která produkuje výsledný zvuk, nejčastěji v pásmu frekvencí mezi 2 a 4 kHz. Rozkmit membrány zajišťuje malá cívka uvnitř pouzdra bzučáku, která při průchodu střídavého proudu působí jako elektromagnet a přitahuje již zmíněnou kovovou membránu a tím tvoří slyšitelný zvuk. Elektromagnetické bzučáky se dají pořídit aktivní nebo pasivní. Aktivní má v sobě zabudovaný oscilátor tvořící střídavý proud pro napájení cívky bez možnosti měnit výstupní frekvenci produkovaného zvuku. Frekvence je pevně daná frekvencí oscilátoru. Pasivní bzučák v sobě nemá žádný oscilátor, proto je nutné použít externí. Při použití oscilátoru s nastavitelnou frekvencí je možné dosáhnout téměř libovolné frekvence zvuku bzučáku, která je dána pouze jeho konstrukčními limity. Výhodou aktivního elektromagnetického bzučáku je, že k napájení stačí stejnosměrné napětí.

Obr. 29:Elektromagnetický bzučák [48]

6.3 Napájení

Napájení je řešeno pomocí step down měniče ukázaného na Obr. 31. Maximální výstupní proud tohoto měniče jsou 2A, což je více než dostačující pro napájení vývojové desky včetně všech senzorů. Obě vývojové desky, jak ESP32 tak ESP32-CAM má svůj step down měnič. Měnič provedený s integrovaným obvodem MP1484 má nastavitelné výstupní napětí, které je pro tento návrh nastaveno na 5 V. Dle datasheetu [44] a také z mého testování jsem zjistil, že měnič potřebuje, aby jeho vstupní napětí bylo minimálně o 1,5 V vyšší, než je jeho nastavené výstupní napětí. V případě nastaveného výstupního napětí 5 V musí být vstupní napětí v rozmezí 6,5 V až 23 V. Na napájení měniče bude primárně použit napájecí zdroj 12 V 3 A viz Obr. 30.

Obr.30:Napájecí zdroj 12 V 3 A



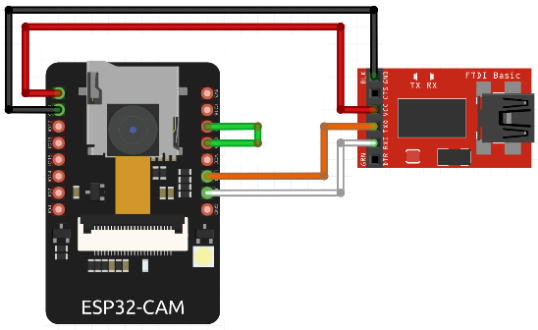
Obr.31: Step down měnič [44]

Téměř všechny komerčně dostupné ústředny zabezpečovacích systémů disponují záložní baterií pro případ výpadku elektrické energie, proto je záložní baterie také zakomponována do navrhovaného modelu EZS. Při odpojení napájecího zdroje se přepne napájení na záložní akumulátor tvořený Li-ion 18650 články, zapojených jako 3SP1 s jmenovitým výstupním napětím 11,1 V. Nabíjení záložního akumulátoru je realizováno přes nabíjecí modul TP4056, který monitoruje napětí článku akumulátoru, aby jeho napětí nepřesáhlo hranici 4,2 V, jež je maximální napětí pro Li-ion články. Maximální nabíjecí proud, který je modul schopen vyvinout je 1 A. Jelikož se jedná o modul primárně vytvořený pro nabíjení přes USB, které má maximální napětí 5 V, je třeba použít step down měnič i pro napájení nabíjecího modulu Li-Ion baterie.

6.4 Kamerový systém

V navrhovaném modelu je k dispozici kamerový systém s možností vzdáleného sledování online přenosu. Pro kamerový systém je použita samostatná vývojová deska ESP32-CAM s vestavěným konektorem pro připojení kamery OV2640, která je schopna poskytnout obraz o rozlišení až 1600x1200 při 15 snímkách za vteřinu. ESP32-CAM využívá stejný mikroprocesor jako obyčejná vývojová deska ESP32, tudíž disponuje WiFi rozhraním, které je použito pro přenos obrazu z kamery. Na zadní straně desky se nachází čtečka pro mikro SD kartu, které lze využít pro uchování video záznamu. Na rozdíl od klasické verze desky ESP32 má méně programovatelných pinů, přesněji 10, protože zbylé jsou využity na propojení kamery a čtečky pro mikro SD kartu s procesorem [49].

Dalším rozdílem a malým ztěžením je absence USB-UART převodníku integrovaného na desce, jako je tomu v případě klasické ESP32 desky použité jako ústředna. Pro naprogramování je nutno použít externí USB-UART převodník připojený na piny U0TX a U0RX podle schématu na Obr. 32 níže [50]. Pro aktivování programovacího módu ESP32-CAM je nutné propojit pin GPIO 0 s pinem GND. Programování jsem prováděl přes USB-UART převodník s čipem CP2102 viz Obr. 33.



Obr. 32: Programování ESP32-CAM [50]

Obr. 33: USB-UART převodník

Problém, který jsem řešil u této vývojové desky ESP32-CAM je veliká náchylnost na poklesy napětí a obecně měkké napájecí zdroje. Při poklesu napájecího napětí pod 4,8 V již deska nebyla schopna pracovat. Při hledání příčin tohoto problému jsem narazil na informaci, že deska je vybavena hardware ochranou, která vypne procesor pokud se napájecí napětí dostane pod určitou mez nazývanou "brownout voltage" [51]. Děje se to z toho důvodu, aby nedošlo k poškození či ztrátě části obsahu uloženého v paměti. Tento problém jsem vyřešil použitím step down měniče pro napájení ESP32, nastaveného na 5,2 V. Vyšší napájecí napětí nijak neohrozí, či nezmenší životnost vývojové desky, jelikož pokud je napájecí napětí připojeno na 5 V pin, tak nejprve směřuje do 3.3 V regulátoru AMS1117, který má podle datasheetu [52] maximální vstupní napětí 12 V. Jediný parametr, který se změní při použití vyššího napájecí napětí stabilizátoru je maximální výstupní proud, který je schopen poskytnout. Podle měření prováděného na stránce Hobbycomponents.com [53] je při vstupním napětí 5 V maximální výstupní proud 540 mA. Při 5,2 V je výstupní proud 480 mA, což je dostatečné pro napájení vývojové desky EPS32 CAM, která má udávanou maximální spotřebu 260 mA [54]. Step down měniče budou napájeny ze stejného zdroje jako ESP32 ústředna se senzory, včetně možnosti využít záložní baterie při odpojení primárního napájecího zdroje.

6.5 Software

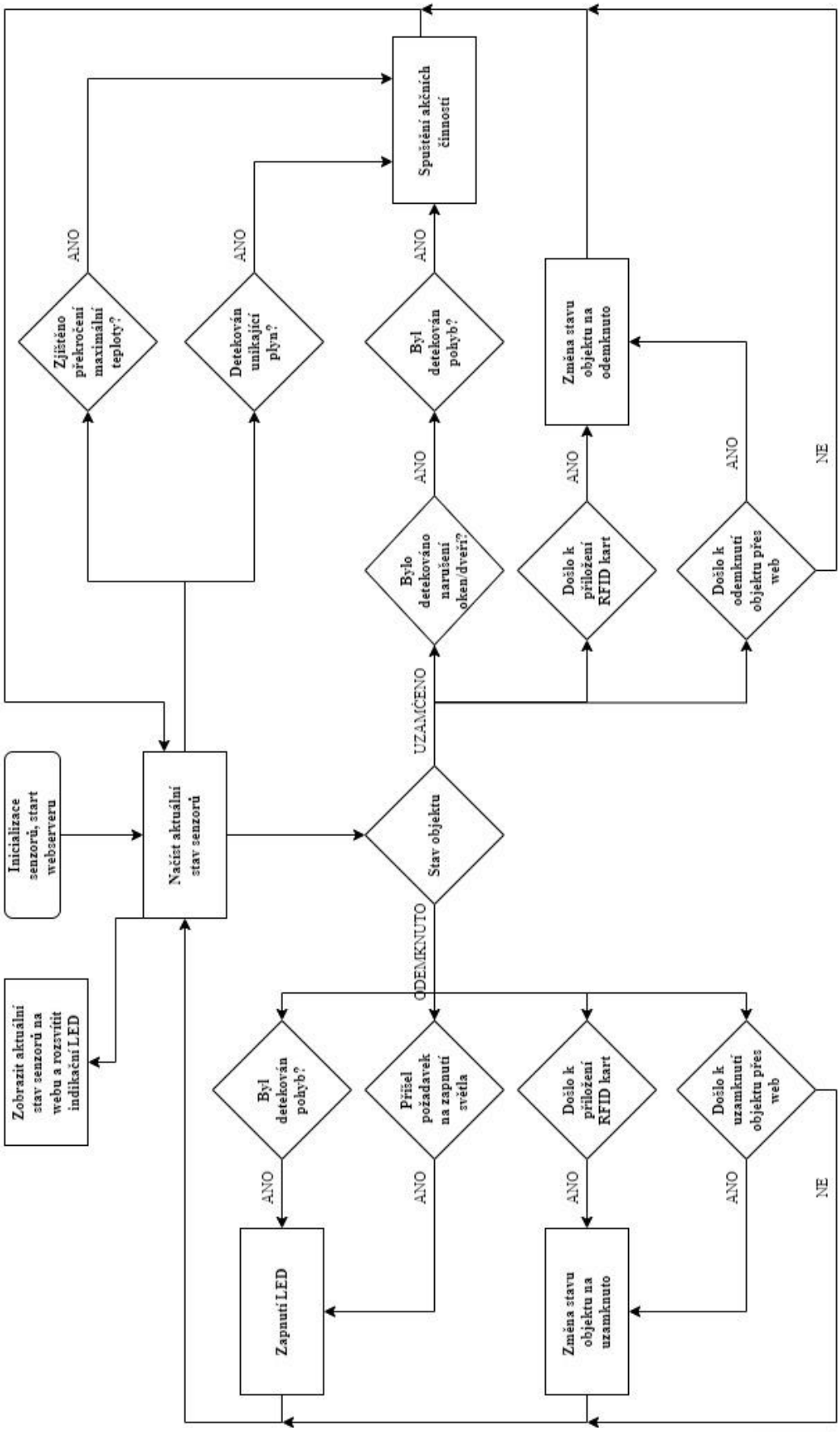
Programování jsem prováděl v prostředí Arduino IDE, které je primárně vytvořené pro kompilaci a nahrání kódu na desky Arduino. Podporu desek ESP32 lze zařídit po přidání odkazu na .json soubor, který obsahuje potřebné informace o deskách ESP32 do kolonky „Správce dalších desek URL“ v záložce „vlastnosti“ v prostředí Arduino IDE a nainstalování knihovny „esp32“ přes správce knihoven.

V prostředí Arduino IDE se používá programovací jazyk C++ doplněný o dodatečné funkce a metody. Kód vytvořený uživatelem v prostředí Arduino IDE se nazývá „sketch“. Ten je poté zprocesován a zkompilován do strojového kódu, který je poslán do mikrokontroléru přes UART rozhraní.

Kód v prostředí Arduino IDE se skládá z hlavních dvou funkcí:

- **void setup()** : je zavolána pouze jednou po startu desky, slouží k inicializaci proměnných, načtení knihoven, definování vstupů a výstupů pinů
- **void loop()** : je volána pořád dokola, umožňuje tak čtení hodnot ze senzorů nebo zapisování příslušných hodnot

Při tvoření kódu pro model zabezpečovacího systému jsem dbal na to, aby systém pracoval jako běžně dostupné zabezpečovací systémy na trhu. Výstupní signály ze senzorů jsou mezi sebou porovnávány a některé jsou na sobě závislé. Detektor plynů je svázaný s teplotním senzorem a oba jsou zapnuté nonstop a nezávisle na stavu zabezpečení. Při detekci plynu nebo nárůstu teploty nad definovanou mez 50 °C dojde ke spuštění akčních činností. Detektor pohybu je nastaven na dva režimy. Pokud je objekt uzamknutý, čeká na přerušení magnetických spínačů na oknech nebo dveřích, aby potvrdil narušení objektu a zahájil akční činnosti systému. Při odemknutém objektu slouží pro chytré rozsvícení světel v místnosti po detekování pohybu. Přístupový systém RFID umožňuje odemknutí a zamknutí objektu přiložením příslušné karty, jejíž ID číslo je uloženo v kódu. Kamerový systém je zde pro vizuální kontrolu objektu a je možné k němu přistupovat jak v zabezpečeném, tak i nezabezpečeném stavu objektu. Primárním akčním členem celého systému je siréna, která při narušení rozezní. Dalším akčním členem, který slouží spíše pro demonstrační účely je rozsvícení červené LED znázorňující narušení objektu. Posledním akčním členem je zobrazení hlášky „NARUŠENÍ!“ na webové stránce zabezpečovacího systému.



Obr. 34:Vývojový diagram

6.5.1 Rozbor kódu

Na začátku jsou definovány knihovny pro následné používání Wifi a SPI rozhraní, MFRC522 RFID modulu a DHT teploměru. Čtení z ostatních senzorů jako PIR detektoru, magnetických spínačů oken a dveří a detektoru plynů je realizováno přes funkci digitalRead(). Následně jsou definovány globální proměnné použité pro zaznamenání aktuálního stavu zapnutí světel, uložení výstupních hodnot ze senzorů, pomocné proměnné použité pro přepočty a proměnné sloužící pro definování čísel pinů senzorů a indikačních LED.

Ve funkci setup() je definována modulační rychlost sériové linky, inicializace SPI rozhraní a knihoven pro použití RFID a DHT. Dále jsou nastaveny módy pinů pomocí funkce pinMode(*pin, mode*), která nadefinuje určitý pin tak, aby se choval buď jako vstup, nebo výstup. Parametr *pin* reprezentuje číslo pinu, které je uloženo v proměnné pro lepší přehlednost. Parametr *mode* volíme *INPUT* pro definování pinu jako vstup pro čtení dat, nebo *OUTPUT* pro nadefinování výstupního pinu, použitého například pro ovládání LED. Po tomto následuje funkce digitalWrite(*pin, mode*) sloužící pro ovládání pinů definovaných jako výstupní. Na požadovaný *pin* můžeme poslat hodnotu logické 1, kde se následně objeví 5 V, nastavením parametru *mode* na *HIGH*. Při nastavení parametru *mode* na *LOW* se na výstupním pinu objeví hodnota logické 0. V mém případě jsou takto nastaveny všechny LED na hodnotu logické 0.

Dále proběhne inicializace Wifi rozhraní, připojení se na definovanou wifi síť a zapnutí web serveru na portu 80. Tím je ukončená funkce setup() a následuje hlavní část programu ve smyčkové funkci loop(). Zde dojde prvně ke zjištění, zda je k web serveru připojen nějaký účastník, pokud ne, probíhá pouze načtení výstupních dat ze senzorů. Poté se zjišťuje, zda není přiložena karta k RFID přístupovému modulu. Správnost karty se kontroluje porovnáním 8 bitového ID tagu, který je během přiložení přečten. Načtený tag se porovná s tagem uloženým v programu. Pokud je splněna podmínka na správnost karty, je změněn stav zabezpečení objektu do druhého stavu, tj. původní odemknutý objekt se nově zamkne a naopak zamknutý objekt se odemkne. Následuje kontrola stavu pohybového PIR senzoru. Při detekci pohybu v zabezpečeném stavu dojde ke kontrole stavu magnetických senzorů na oknech a dveřích, pokud některý z nich hlásí otevření neboli na výstupu je hodnota logické 0, je tento stav zaznamenán do proměnné jako narušení.

Tato proměnná je následně použita pro spuštění sirény, rozsvícení indikační červené LED a pro zobrazení hlášky „NARUŠENÍ!“ na webové stránce.

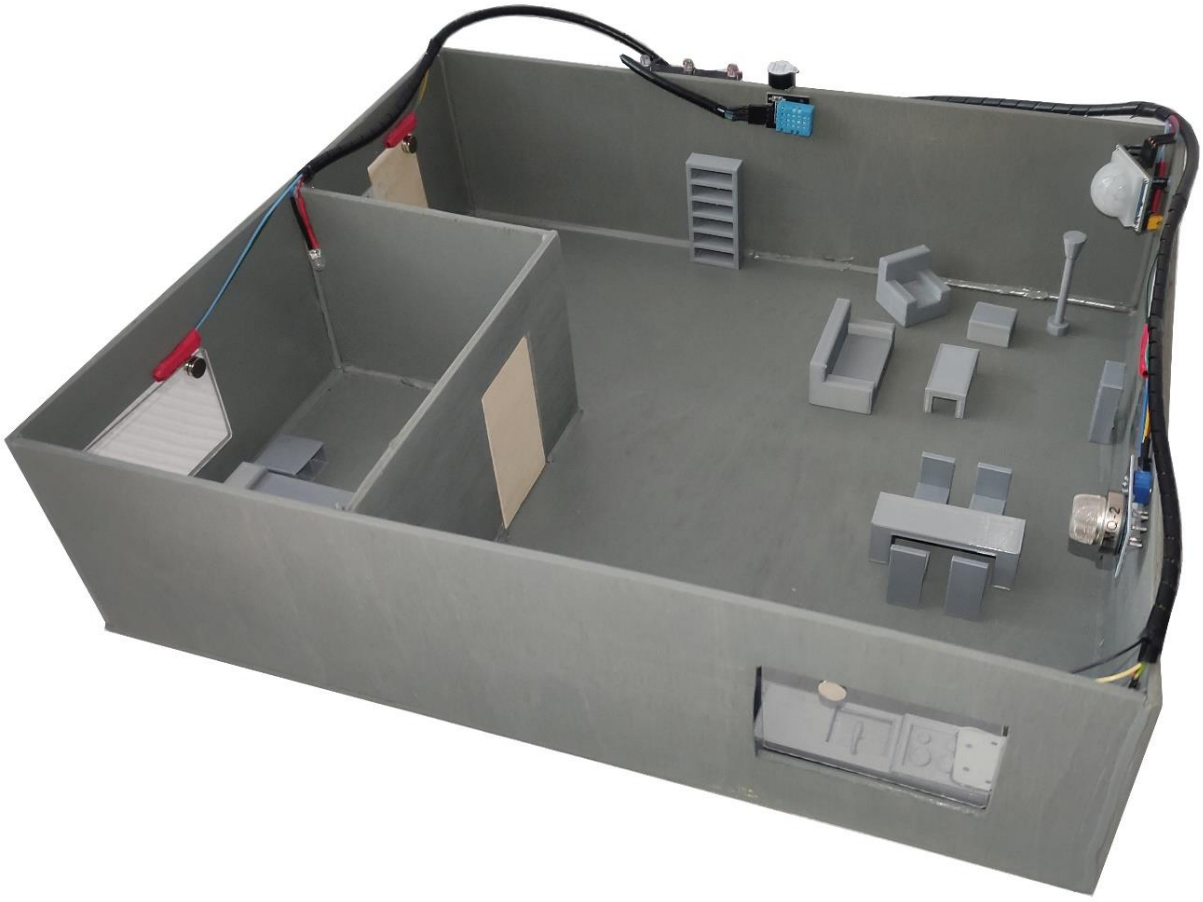
Další velká část kódu obsahuje samotné webové stránky, které jsou psány v HTML. Prostředí Arduino IDE s knihovnou Wifi podporuje naprostou většinu příkazů a klíčových slov HTML jazyka. S jediným problémem jsem se setkal u formátování. Toto prostředí je velmi citlivé na správné umístění uvozovek, které ovšem mají jiná pravidla umisťování, něž je tomu u klasického HTML. Samotnou webovou stránku jsem se snažil navrhnout tak, aby byla co nejvíce přehledná a intuitivní na ovládání včetně barevných tlačítek znázorňující aktuální stav, kde červená reprezentuje zapnuto a červená vypnuto.

Nakonec je v kódu sekce se čtením všech ostatních senzorů pomocí funkce digitalRead() popsanou výše. Stav těchto senzorů je kontrolován podmínkami, zda nedošlo k překročení nastavených mezí v případě detektoru plynů a teploty a zda nedošlo k otevření v případě magnetických senzorů oken a dveří. Výstupní hodnoty senzorů spolu s údajem o teplotě jsou následně zobrazeny na webové stránce. Na stránku byly také přidány tlačítka + a - pro nastavení teploty termostatu použitelné pro budoucí rozšíření modelu.

6.6 Realizace modelu

Malý model rodinného domu byl vyroben z překližky, která byla následně nabarvena šedou barvou. Aby šlo jednoduše rozeznat o jakou část místnosti se jedná, byl model doplněn o modely nábytku a vybavení vytisknuté na 3D tiskárně. Senzory jsou umístěny na stěnách modelu pro přehlednost a demonstrační účely, nejedná se o úplně ideální rozmístění, které bylo popsáno v zásadách instalace senzorů v kapitole 2. Senzory.

Pro ESP32 jsem vyrobil jednoduchou patici umístěnou na univerzálním plošném spoji spolu s měniči napětí pro napájení obou ESP32 desek a ochranných nabíjecích obvodů pro záložní Li-Ion baterii. Celá deska plošných spojů je umístěna v ochranném krytu vytištěném na 3D tiskárně. Kompletní model je možné vidět níže na Obr. 35.



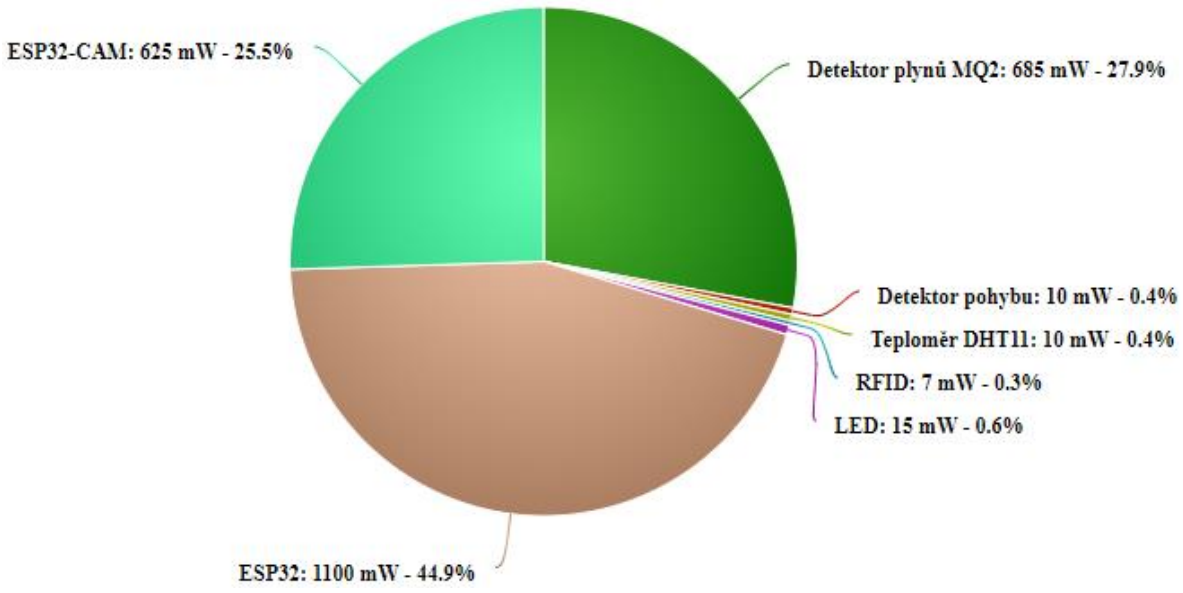
Obr. 35:Model

6.7 Měření parametrů realizovaného modelu

6.7.1 Měření spotřeby

Jeden z důležitých parametrů systému je spotřeba elektrické energie. Tuto informaci můžeme použít pro výpočet potřebné kapacity záložního akumulátoru použitého pro nouzové napájení systému v případě výpadku elektřiny. U profesionálního elektrického zabezpečovacího systému je pro každou úroveň zabezpečení dána minimální doba, po kterou musí být akumulátor schopen napájet celý systém při výpadku elektřiny. U elektronických zabezpečovacích systémů s úrovní zabezpečení 1 a 2, což odpovídá úrovni zabezpečení mnou realizovaného systému, je tato doba 12 hodin.

Měření je prováděno multimetrem Aneg AN8009, který má v režimu měření proudu na rozsah 999 mA chybu měření do 1% z rozsahu. Při měření je model napájen ze zdroje 12 V 3 A. Na následujícím grafu lze vidět spotřebu jednotlivých prvků realizovaného systému v mW.



Graf 1: Spotřeba prvků systému

Jak lze z grafu vidět, největší spotřebu má samotná ústředna ESP32 a kamerový systém ESP32-CAM. Velká spotřeba je kvůli WiFi rozhraní a výkonnému procesoru. Další prvek s vyšší spotřebou je detektor plynu MQ2. Spotřeba je způsobena vyhřívacím elementem uvnitř senzoru, který slouží pro zahřívání oxidu cíničitého, jehož elektrony jsou vázány molekulami kyslíku a brání tak v průchodu elektrického proudu. Při přítomnosti hořlavého plynu se jež elektrony oxidu cíničitého nemají na co vázat a volně protékají do vyhodnocovacího obvodu. Další spotřeby prvků jsou v porovnání s ESP32, ESP32-CAM a MQ2 zanedbatelné, jejich spotřeby jsou v řádu desetin procent.

Aby navrhovaný systém dosáhl požadavků na systém úrovně zabezpečení 1 a 2, musí být záložní akumulátor schopen napájet celý systém po dobu minimálně 12 hodin. Při naměřené spotřebě 2449 mW je třeba záložního akumulátoru s energií 29,39 Wh. Na model je použit akumulátor ze dvou Li-Ion článků o kapacitně 3 Ah a jmenovitém napětí 11,1 V. Při vynásobení těchto dvou hodnot dostaneme celkovou energii akumulátoru 33,3 Wh, což splňuje požadavek pro systém úrovně zabezpečení 1 a 2.

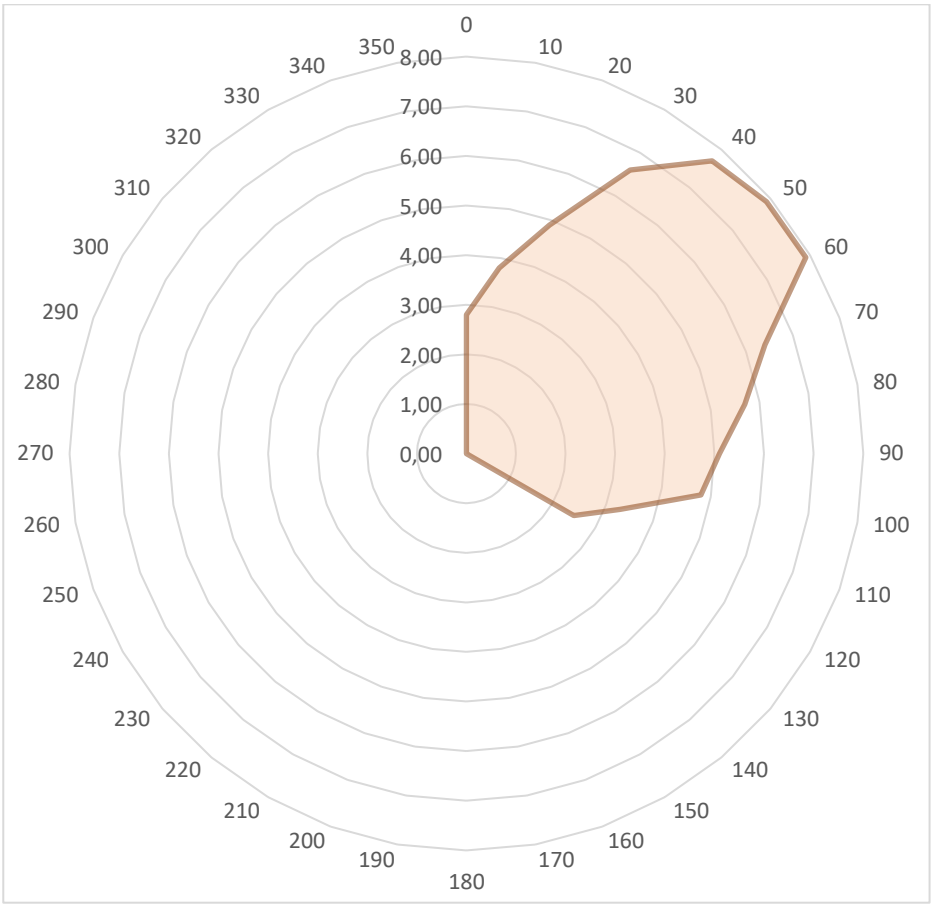
Porovnání spotřeby energií realizovaného systému a profesionálního systému Jablotron lze vidět v následující tabulce. Pro porovnání byly vybrány prvky se stejnou funkcí. Všechna data o spotřebách prvků Jablotron systému byla brána z datasheetů výrobků, ze stránek Jablotron.com. [26] Mnou realizovaný systém má o 50 % menší spotřebu energie.

Tab. 2: Porovnání spotřeb systémů

Prvek realizovaného systému	spotřeba [mW]	Prvek systému Jablotron	spotřeba [mW]
Ústředna ESP32	1100	Ústředna JA-103K s LAN	960
Detektor plynů MQ2	685	Detektor plynů GS-133	1200
PIR detektor pohybu	10	PIR detektor pohybu	120
Teploměr DHT11	10	Teploměr JA-111TH	60
Přístupový systém	22	Přístupový systém JA-112E	120
Kamerový systém ESP32	625	Kamerový systém ESP32	2400
Celkem	2452	Celkem	4860

6.7.2 **Měření pohybového senzoru**

Pro PIR senzor pohybu HC-SR501 jsem změřil detekční charakteristiku. Měření probíhalo venku na volném prostoru za oblačného počasí pro zamezení rušivých vlivů. Charakteristika byla měřena s krokem 10° a senzor byl umístěn 1,5 metru od země. Výrobce udává maximální detekční úhel 120° a detekční vzdálenost až 7 metrů. Při mém měření jsem nemohl dosáhnout konstantních výsledků měření pro úhel 0° a 120°, tedy krajních úhlů senzoru a tyto hodnoty jsou velmi orientační. Udávané vzdálenosti výrobcem, která činí 7 metrů jsem dosáhl pouze v rozmezí 35° až 65°. Celou detekční charakteristiku je možné vidět na následujícím grafu.



Graf 2: Detekční charakteristika PIR senzoru

7 Zhodnocení výsledné realizace a ekonomický rozbor

Při porovnání s běžně dostupnými zabezpečovacími systémy na trhu se základní princip detekování nebezpečí neliší. To byl také cíl této realizace, co nejvíce se přiblížit běžně dostupným zabezpečovacím systémům. Rozdíl mezi mým systémem a komerčně dostupným systémem je hlavně absence jakéhokoliv zabezpečení nebo šifrování vzdálené komunikace přes internet. V momentálním stavu se ke vzdálenému ovládání ústředny dostane kdokoliv, kdo má patřičnou přístupovou adresu. Možným rozvojem tohoto systému by mohlo být přidání DNS serveru, běžící na další vývojové desce ESP32, která by umožnila zvýšení úrovně kybernetického zabezpečení, přidáním nějaké formy šifrování spolu s požadavkem na autorizaci pomocí přístupových údajů. Přidáním DNS serveru by také bylo možné sdružit více zabezpečovacích systémů. Dalším možným vylepšením systému by bylo použití EPS32 knihovny pro asynchronní web server s podporou JavaScriptu, který by umožnil například zobrazení okénka s kamerovým systémem na hlavní ovládací stránce ústředny.

Z ekonomického hlediska bude vždy cenově výhodnější amatérsky navržený systém než ten profesionálně navržený. Samotné prvky systému lze pořídit i za desetinové ceny oproti profesionálnímu systému ovšem u profesionálního systému máme záruku funkčnosti všech dílů a senzorů díky velkému množství testování a zátěžových zkoušek, což u dílů, které jsou původem z Číny, kde neprocházejí výstupní kontrolou kvality žádnou záruku nemáme. Aby se stal amatérsky navržený systém volně dostupný na trhu, je zapotřebí mnoho úsilí a vylepšování systému. Všechny senzory a vývojové desky pro tento systém byly zakoupeny na e-shopu laskarduino.cz, proto budou ceny pro porovnání čerpány odtud.

V následující tabulce lze vidět porovnání cen navrženého systému a profesionálního systému Jablotron 100. Ceny prvků sytému Jablotron jsou brány z e-shopu elcar.cz. Do celkové ceny navrhovaného modelu nejsou započítány náklady na překližkový model spolu s vytištěnými modely nábytku a náklady na kabeláž. Uvedené ceny v tabulce jsou včetně DPH a jsou platné ke dni 1.12.2021.

Tab. 3: Porovnání cen systémů

Můj systém		Jablotron 100	
Prvek systému	Cena	Prvek systému	Cena
Ústředna ESP32 + napájení*	482 Kč	Ústředna JA-103K*	6 249 Kč
PIR senzor HC-SR501	38 Kč	PIR senzor JA-110P	635 Kč
Senzor teploty DHT11	68 Kč	Senzor teploty JB-TS	429 Kč
4x Magnetický jazýčkový spínač	48 Kč	4x Magnetický dveřní kontakt SA-200A	328 Kč
Detektor plynů MQ-2	44 Kč	Detektor kouře JA-110ST	1 122 Kč
Přístupový modul RFID + LED	90 Kč	Přístupový modul RFID JA-113E	1 811 Kč
Aktivní bzučák 5 V	6 Kč	Siréna JA-110A	609 Kč
kamerový systém ESP32-CAM	328 Kč	Kamera JI-111C	5 620 Kč
Celkem	1 104 Kč	Celkem	16 803 Kč
*V ceně jsou zahrnuty veškeré prvky potřebné k napájení bez záložní baterie			

8 Závěr

První část práce se zabývá shrnutím současného stavu technologií používaných v elektronických zabezpečovacích systémech pro rodinné domy. Do práce jsou zahrnuty i některé moderní technologie využívající se především ve větších objektech, typicky kancelářských prostorech. Zmíněny jsou možnosti propojení ústředny zabezpečovacího systému se senzory. Dále jsou popsány základní druhy senzorů, které se v současné době nejvíce používají. Ke každému typu senzoru jsou sepsány základní zásady instalace, které je nutno dodržovat pro správnou funkci systému a ukázka senzoru dostupného na trhu. Krátce jsou také popsány přístupové systémy a to včetně nejmodernějších biometrických systémů využívající jedinečnost lidského těla jako identifikační klíč. Mezi progresivní technologie v oblasti zabezpečení také patří kamerové systémy jejichž klíčové vlastnosti jsou v práci popsány. Na konci první části práce je shrnutí úrovní zabezpečovacích systémů a které volně dostupné systémy tyto požadavky splňují.

Druhá část, která tvoří cíl práce se zaobírá návrhem funkčního modelu elektronického zabezpečovacího systému s možností ovládání přes internet. Ústředna systému byla postavena na vývojové desce ESP32 ke které jsou připojeny základní senzory. Na začátku této části práce jsem se zabýval volbou vývojové desky spolu s použitými senzory. U každého senzoru je vyobrazeno a popsáno schéma zapojení daného senzoru s vývojovou deskou včetně parametrů senzoru a důvodu vybrání. Schémata zapojení byla tvořena v open-source programu Fritzing. Do modelu jsem zahrnul také prvky chytré domácnosti, jako je kamerový systém a osvětlení s možností vzdáleného ovládání. Následně je popsáno programování vývojové desky ESP32 a je udělán rozbor celého kódu, který popisuje jakým způsobem systém reaguje na výstupy ze senzorů. Nakonec jsou probrány možnosti rozšíření systému.

Realizaci modelu považuji za úspěšnou. Pokud by se systém rozvíjel o další senzory ovládací prvky, bylo by asi vhodnější použít web server s podporou JavaScriptu, který by umožnil další zdokonalení systému.

9 Seznam literatury

[1] FCCPS. Základní přehled o technologii WiFi. In: Průmyslové počítače a komunikace [online]. [cit. 06.12.2021]. Dostupné z: https://www.fccps.cz/zakladni-prehled-o-technologii-wifi

[2] KOVAŘÍK, David. Bluetooth. In: Mobilizujeme [online] 2011. [cit. 06.12.2021]. Dostupné z: https://mobilizujeme.cz/clanky/bluetooth-modrozub-pod-drobnohledem-vedecke-okenko

[3] IMMAX. V čem tkví krása technologie ZigBee. In IMMAX [online]. [cit.06.12.2021]. Dostupné z: https://www.immax.cz/clanky/detail/v-cem-tkvi-krasa-technologie-zigbee.htm

[4] Alarmsecurity. Typy pohybových senzorů. In: Alarmsecurity [online]. [cit. 06.12.2021]. Dostupné z: https://www.alarmsecurity.cz/www-alarmsecurity-cz/5-TECHNICKA-PODPORA/38-Typy-pohybovych-senzoru

[5] Alarmsecurity. Instalace PIR senzoru. In: Alarmsecurity [online]. [cit. 06.12.2021]. Dostupné z: https://www.alarmsecurity.cz/www-alarmsecurity-cz/5-TECHNICKA-PODPORA/8-Instalace-PIR-senzoru

[6] E-light. Pohybová čidla – kompletní průvodce. In: E-light [online]. [cit. 06.12.2021]. Dostupné z: https://www.e-light.cz/zprava/cidla-pohybu-a-svitidla-s-cidlem-zakladni-rady-a-tipy

[7] Zabezpečovací zařízení. Požární hlásiče a detektory plynů. In: Zabezpečovací zařízení [online]. [cit. 06.12.2021]. Dostupné z: https://www.zabezpecovaci-zarizeni.cz/pozarni-detektory/

[8] NEŠKODNÁ, Jana. Autonomní hlásiče kouře. In: HZSCR [online]. [cit. 06.12.2021]. Dostupné z: http://www.hzscr.cz/soubor/detektory-pozaru-obecna-teorie-jana-neskodna-doc.aspx

[9] KOPÁČEK, Petr. Hlásiče požáru. In: HZSCR [online]. [cit. 06.12.2021]. Dostupné z: https://www.hzscr.cz/clanek/hlasice-pozaru.aspx

[10] HONZÍK, Petr. Jak funguje plynový požární hlásič. In: Zabezpečovací zařízení [online] 2015. [cit. 06.12.2021] Dostupné z: https://www.zabezpecovaci-zarizeni.cz/bezpecnost-majetku/pozarni-bezpecnost-pozarni-hlasice/jak-funguje-plynovy-pozarni-hlasic-%5Bb061%5D

[11] Chromservis. Katalitické spalování. In: Chromservis [online]. [cit. 06.12.2021]. Dostupné z: https://www.chromservis.eu/c/catalytic?lang=CZ

[12] REICHEL, Jaroslav. Wheatstoneův můstek. In: Encyklopedie fyziky [online] 2006. [cit. 06.12.2021]. Dostupné z: http://fyzika.jreichl.com/main.article/view/1631-wheatstoneuv-mustek

[13] Chromservis. Elektrochemický senzor. In: Chromservis [online]. [cit. 06.12.2021]. Dostupné z: https://www.chromservis.eu/c/electrochemical?lang=CZ

[14] Bezpečnostní systémy. RFID princip. In: Studijní materiály SŠEaS [online]. [cit. 06.12.2021]. Dostupné z: http://studijni-materialy.sseas.cz/bezpecnostni-systemy/rfid-princip/

[15] GILLICHOVÁ, Martina. Jak funguje zabezpečení domu pomocí čtečky otisků prstů. In: Bydlení pro každého[online] 2015. [cit. 06.12.2021]. Dostupné z: https://rodinne-domy.bydleniprokazdeho.cz/zabezpecovaci-a-protipozarni-zarizeni/jak-funguje-zabezpeceni-domu-pomoci-ctecky-otisku-prstu-.php

[16] MORAVEC, Petr. Čtečky otisku prstu pod drobnohledem. In: Mobilizujeme [online] 2016. [cit. 06.12.2021]. Dostupné z: https://mobilizujeme.cz/clanky/ctecky-otisku-prstu-pod-drobnohledem-jak-funguji

[17] Datahelp. Čtečky otisků prstů u mobilů a jejich bezpečnost. In: Datahelp [online]. [cit. 06.12.2021]. Dostupné z: https://www.datahelp.cz/clanky/ctecky-otisku-prstu-u-mobilu-a-jejich-bezpecnost

[18] HSU, David. Fingerprint Sensor Technology And Security Requirements. In:Semiconductor Engineering [online] 2016. [cit. 06.12.2021] Dostupné z: https://semiengineering.com/fingerprint-senor-technology-and-security-requirements/

[19] Computerworld. Skenování duhovky. In: Computerworld [online]. [cit. 06.12.2021]. Dostupné z: https://computerworld.cz/securityworld/skenovani-duhovky-miri-do-smartphonu-54218

[20] AUERBACH, Alois. Biometrická analýza oční duhovky [online]. Plzeň 2013 [cit. 06.12.2021]. Diplomová práce. Západočeská univerzita v Plzni, Fakulta aplikovaných věd. Dostupné z: https://dspace5.zcu.cz/bitstream/11025/7587/1/DP_Auerbach.pdf

[21] Zabezpečovací zařízení. Jak vybrat bezpečnostní kamerový systém. In: Zabezpečovací zařízení [online]. [cit. 06.12.2021]. Dostupné z: https://www.zabezpecovaci-zarizeni.cz/jak-vybrat-spravne/kamerovy-system/

[22] Pro Security, Zabezpečení domu, In: Pro Security [online]. [cit. 06.12.2021]. Dostupné z: https://www.pro-security.cz/zabezpecovaci-systemy/kvalitni-zabezpeceni-pomoci-zabezpecovacich-systemu/zabezpeceni-domu/#

[23] MICHALEC, Libor. PIR detektor. In: vyvoj.hw [online] 2013. [cit. 06.12.2021] Dostupné z: https://vyvoj.hw.cz/automatizace/pir-cidlo-skvely-sluha-ale-zly-pan.html

[24] LANGABEER, George. Before You Buy a Home Security Systém. In: YouTube [online] 2021. [cit. 06.12.2021] Dostupné z: https://www.youtube.com/watch?v=ZaDryoOH1ww&t=132s&ab_channel=SilverHammerSurveillance

[25] AZ Elektro. Alarm Jablotron 100+. In: azcasopis [online] 2019. [cit. 06.12.2021] Dostupné z: http://www.azcasopis.cz/informacni-technologie/alarm-jablotron-100-dokaze-zabezpecit-a-ovladat-firmy-bytove-domy-i-skoly

[26] Jablotron. Ústředny Jablotron 100+. In: Jablotron [online]. [cit. 06.12.2021] Dostupné z: https://www.jablotron.com/cz/katalog-produktu/alarmy/jablotron-100/ustredny/

[27] Jablotron. Kamery a příslušenství. In: Jablotron [online]. [cit. 06.12.2021] Dostupné z: https://www.jablotron.com/cz/katalog-produktu/alarmy/jablotron-100/kamery-a-prislusenstvi/

[28] Jablotron. Pohybové detektory. In: Jablotron [online]. [cit. 06.12.2021] Dostupné z: https://www.jablotron.com/cz/katalog-produktu/alarmy/jablotron-100/detektory/pohybove/

[29] Jablotron. Plášťové detektory. In: Jablotron [online]. [cit. 06.12.2021] Dostupné z: https://www.jablotron.com/cz/katalog-produktu/alarmy/jablotron-100/detektory/plastove/

[30] Jablotron. Enviromentální detektory. In: Jablotron [online]. [cit. 06.12.2021] Dostupné z: https://www.jablotron.com/cz/katalog-produktu/alarmy/jablotron-100/detektory/environmentalni/

[31] Alza. iGET Security M4. In: Alza [online] 2018. [cit. 06.12.2021] Dostupné z: https://www.alza.cz/iget-security-m4-d5288766.htm

[32] Alza. EufyCam 2. In: Alza [online] 2020. [cit. 06.12.2021] Dostupné z: https://www.alza.cz//eufy-eufycam-2-kit-2xeufycam-d5776484.htm?kampan=adw4_smart_pla_all_obecna-css_smart-home_c_9062887___EUf011b_413605341827_~94081209529~&gclid=Cj0KCQjwtrSLBhCLARIsACh6RmjLpnJaS2-XZ2Fz8C6qKfQeKMqEgTwd_ks28ieKYaRNBgjx2xTJ2XcaAhMPEALw_wcB

[33] TSS Group. Stupně bezpečnosti. In: TSS Group [online] 2016. [cit. 06.12.2021] Dostupné z: https://www.tssgroup.cz/aktuality/faq/stupne-bezpecnosti-1

[34] Varnet. Poplachový systém stupeň zabezpečení 3. In: Varnet [online]. [cit. 06.12.2021] Dostupné z: https://www.varnet.cz/dokumenty/podpora/EZS/stupen-zabezpeceni-3/

[35] STEHLÍK, Petr. ESP32-S2. In YouTube [online] 2020. [cit. 06.12.2021] Dostupné z: https://www.youtube.com/watch?v=z1izB3lvpt0&ab_channel=InstallFest

[36] ESP32. ESP32 specifications. In: espressif [online]. [cit. 06.12.2021] Dostupné z: https://www.espressif.com/en/products/socs/esp32

[37] Microchip. Atmega2560. In: Microchip [online]. [cit. 06.12.2021] Dostupné z: https://www.microchip.com/en-us/product/ATmega2560

[38] Espressif. 5 V tolerance. In: Esp32 [online] 2017. [cit. 06.12.2021] Dostupné z: https://esp32.com/viewtopic.php?t=877

[39] Circuit Basics. Basics of UART communication. In: Circuit Basics [online]. [cit. 06.12.2021] Dostupné z: https://www.circuitbasics.com/basics-uart-communication/

[40] Silicon labs. Calculating throughput on CP210x devices. In: Community Silabs [online] 2021. [cit. 06.12.2021] Dostupné z: https://community.silabs.com/s/article/calculating-throughput-on-cp210x-devices?language=en_US

[41] STEHLÍK, Petr. ESP32-S2. In YouTube [online] 2020. [cit. 06.12.2021] Dostupné z: https://www.youtube.com/watch?v=z1izB3lvpt0&ab_channel=InstallFest

[42] Laskarduino. HC-SR501 Datasheet. In: Laskarduino [online]. [cit. 06.12.2021] Dostupné z: https://www.laskarduino.cz/user/related_files/hc-sr501_datasheet.pdf

[43] Mouser. DHT11 Datasheet. In: Mouser [online]. [cit. 06.12.2021] Dostupné z: https://www.mouser.com/datasheet/2/758/DHT11-Technical-Data-Sheet-Translated-Version-1143054.pdf

[44] Mouser. MP1484 Datasheet. In: Mouser [online]. [cit. 06.12.2021] Dostupné z: https://www.mouser.com/datasheet/2/277/MP1484-1186021.pdf

[45] ADDIKIT. RFID Quick Start Guide. In: Hadex [online] 2015. [cit. 06.12.2021] Dostupné z: https://www.hadex.cz/navody/m490a.pdf

[46] TIŠNOVSKÝ, Pavel. Externí sériové sběrnice SPI a I²C. In root [online] 2008. [cit. 06.12.2021] Dostupné z: https://www.root.cz/clanky/externi-seriove-sbernice-spi-a-i2c/

[47] Laskarduino. Senzor hořlavých plynů MQ-2. In: Laskarduino [online]. [cit. 06.12.2021] Dostupné z: https://www.laskarduino.cz/arduino-senzor-horlavych-plynu-propanu--metanu--butanu--vodiku-mq-2/

[48] Quisure. What is the working principle of the buzzer. In: Quisure [online] 2020. [cit. 06.12.2021] Dostupné z: https://www.quisure.com/blog/faq/what-is-the-working-principle-of-the-buzzer

[49] Laskarduino. ESP32-CAM. In: Laskarduino [online]. [cit. 06.12.2021] Dostupné z: https://www.laskarduino.cz/ai-thinker-esp32-cam-2-4ghz-wifi-bluetooth-modul/

[50] WICKRAMARATHNA, Nishān. What I Learned About ESP32-CAM and Everything You Need to Know. In: Nishanc [online] 2021. [cit. 06.12.2021] Dostupné z: https://nishanc.medium.com/what-i-learned-about-esp32-cam-and-everything-you-need-to-know-12a9e520a0da

[51] MIKEVANIS. Brownout detector was triggered. In: Stackoverflow [online] 2020. [cit. 06.12.2021] Dostupné z: https://stackoverflow.com/questions/60171641/any-solution-available-for-for-esp32-cam-brownout-detector-was-triggered-error

[52] Advanced Monolithic Systems. AMS1117 Datasheet. In: advanced monolithic [online]. [cit. 06.12.2021] Dostupné z: http://www.advanced-monolithic.com/pdf/ds1117.pdf

[53] Hobby components. AMS1117 regulátor. In: Hobby components [online] 2019. [cit. 06.12.2021] Dostupné z: https://hobbycomponents.com/power/903-ams1117-33v-power-supply-module

[54] Last minute engineers. Insight Into ESP32 Sleep Modes. In: Last minute engineers [online] . [cit. 06.12.2021] Dostupné z: https://lastminuteengineers.com/esp32-sleep-modes-power-consumption/

[55] MAN, Gabriel. Detecting and Identifying Clandestine Drug Laboratories: Sensing Technology Assessment. In: ResearchGate [online] 2018. [cit. 06.12.2021] Dostupné z: https://www.researchgate.net/figure/Schematic-of-a-typical-electrochemical-gas-sensor-17_fig7_255660220

[56] Glolab. Focusing devices for pyroelectric infrared sensors. In: Glolab [online] . [cit. 06.12.2021] Dostupné z: http://www.glolab.com/focusdevices/focus.html

[57] Gas sensors. Catalytic combustion sensors. In: Gastec [online] . [cit. 06.12.2021] Dostupné z: https://www.gastec.co.jp/en/product/detail/id=2205