VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV POČÍTAČOVÉ GRAFIKY A MULTIMÉDIÍ
DEPARTMENT OF COMPUTER GRAPHICS AND MULTIMEDIA

DOMOVNÍ ZABEZPEČOVACÍ SYSTÉM S PLATFORMOU ESP32

HOME SECURITY SYSTEM WITH ESP32 PLATFORM

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE **ADAM PASTIERIK**
AUTHOR

VEDOUCÍ PRÁCE **Ing. TOMÁŠ GOLDMANN, Ph.D.**
SUPERVISOR

BRNO 2025

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

Zadání bakalářské práce

164797

Ústav:	Ústav inteligentních systémů (UITS)
Student:	**Pastierik Adam**
Program:	Informační technologie
Název:	**Domovní zabezpečovací systém s platformou ESP32**
Kategorie:	Vestavěné systémy
Akademický rok:	2024/25

Zadání:

1. Seznamte se s moderními zabezpečovacími systémy pro použití v interiéru.
2. Sumarizujte informace o kamerách použitelných s platformou ESP32. Dále se seznamte se senzory pro detekci živých narušitelů, jako jsou PIR senzory nebo radarové senzory.
3. Navrhněte zabezpečovací systém se senzorickými moduly a centrálním ovládacím počítačem. Řešení založte na mikrokontroleru ESP32
4. Implementujte software pro senzorické moduly a centrální jednotku, která bude sloužit k řízení celého systému.
5. Proveďte experimenty zaměřené na vyhodnocení spolehlivosti vašeho řešení.

Literatura:

- PAVAN, Massimo; CALTABIANO, Armando; ROVERI, Manuel. TinyML for UWB-radar based presence detection. In: *2022 International Joint Conference on Neural Networks (IJCNN)*. IEEE, 2022. p. 1-8.
- XIA, Zhaoyang, et al. Person identification with millimeter-wave radar in realistic smart home scenarios. *IEEE Geoscience and Remote Sensing Letters*, 2021, 19: 1-5.

Při obhajobě semestrální části projektu je požadováno:

- Body 1 a 2.

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

Vedoucí práce:	**Goldmann Tomáš, Ing., Ph.D.**
Vedoucí ústavu:	Kočí Radek, Ing., Ph.D.
Datum zadání:	1.11.2024
Termín pro odevzdání:	14.5.2025
Datum schválení:	31.10.2024

Abstrakt

Táto práca sa zaoberá návrhom a implementáciou domového zabezpečovacieho systému založeného na platforme ESP32. Hlavným cieľom bolo vytvoriť cenovo dostupné, modulárne a spoľahlivé riešenie, ktoré kombinuje detekciu pohybu s kamerovým systémom. Navrhnuté riešenie využíva trojvrstvovú architektúru pozostávajúcu z Raspberry Pi ako centrálnej riadiacej jednotky, senzorických modulov s mikrokontrolérmi ESP32 vybavenými PIR a mmWave senzormi a mobilnej aplikácie zabezpečujúcej používateľské rozhranie pre vzdialenú správu. Na zabezpečenie komunikácie v reálnom čase bol implementovaný WebSocket protokol, ktorý umožňuje efektívny prenos konfiguračných údajov, notifikácií a obrazových dát. Experimentálne overenie ukázalo vysokú spoľahlivosť systému pri detekcii pohybu v rôznych podmienkach, pričom mmWave senzor preukázal výrazne lepšie výsledky ako tradičný PIR detektor, najmä pri detekcii cez prekážky a na väčšie vzdialenosti. Používateľské testovanie potvrdilo intuitívnosť mobilnej aplikácie. Navrhnuté riešenie predstavuje funkčnú alternatívu ku komerčným zabezpečovacím systémom s potenciálom pre integráciu do konceptu inteligentných domácností.

Abstract

This thesis focuses on the design and implementation of a home security system based on the ESP32 platform. The main objective was to create an affordable, modular, and reliable solution that combines motion detection with a camera system. The proposed solution utilizes a three-tier architecture consisting of a Raspberry Pi as the central control unit, sensory modules with ESP32 microcontrollers equipped with PIR and mmWave sensors, and a mobile application providing a user interface for remote management. The WebSocket protocol was implemented to ensure real-time communication, enabling efficient transfer of configuration data, notifications, and image data. Experimental verification demonstrated high system reliability in motion detection under various conditions, with the mmWave sensor showing significantly better results than the traditional PIR detector, especially in detection through obstacles and at greater distances. User testing confirmed the intuitiveness of the mobile application. The proposed solution represents a functional alternative to commercial security systems with potential for integration into the smart home concept.

Kľúčové slová

Elektronické zabezpečovacie systémy, ESP32, Senzory, Kamerové systémy, PIR, mmWave, Detekcia živých narušiteľov

Keywords

Electronic security systems, ESP32, Sensors, Camera systems, PIR, mmWave, Detection of living intruders

Citácia

PASTIERIK, Adam. *Domovní zabezpečovací systém s platformou ESP32*. Brno, 2025. Bakalářská práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Ing. Tomáš Goldmann, Ph.D.

Domovní zabezpečovací systém s platformou ESP32

Prehlásenie

Prehlasujem, že som túto bakalársku prácu vypracoval samostatne pod vedením pána Ing. Tomáša Goldmanna Ph.D. Uviedol som všetky literárne pramene, publikácie a ďalšie zdroje, z ktorých som čerpal.

.....
Adam Pastierik
11. mája 2025

Poďakovanie

Rád by som poďakoval vedúcemu mojej práce Ing. Tomášovi Goldmannovi, Ph.D., za odborné vedenie, cenné rady a trpezlivý prístup počas celého procesu vypracovania tejto práce.

Obsah

Zoznam obrázkov

Kapitola 1

Úvod

V súčasnej dobe, keď bezpečnostné riziká narastajú a technologické možnosti sa neustále rozširujú, zabezpečovacie systémy zohrávajú kľúčovú úlohu nielen pri ochrane priemyselných objektov a organizácií, ale čoraz častejšie aj v domácnostiach. Moderné zabezpečovacie systémy sa vyvinuli z jednoduchých mechanických zariadení na komplexné elektronické riešenia kombinujúce senzorické prvky, kamery a inteligentné riadiace jednotky. Súčasný trend digitalizácie a konektivity navyše vytvára priestor pre integráciu zabezpečovacích systémov do širšieho ekosystému inteligentných domácností.

Tradičné komerčné zabezpečovacie systémy sú často nákladné, ťažko prispôsobiteľné špecifickým požiadavkám užívateľov a náročné na inštaláciu. Ich uzavretá architektúra obmedzuje možnosti rozšírenia o nové funkcie alebo zariadenia tretích strán, čo znižuje ich atraktivitu pre technicky zdatných používateľov hľadajúcich prispôsobiteľné riešenia. Nástup cenovo dostupných mikrokontrolérov, akým je ESP32, spolu s rozvojom bezdrôtových technológií a platformy internet vecí (IoT), otvára nové možnosti pre vývoj personalizovaných zabezpečovacích riešení s prijateľnou cenou a vysokou mierou flexibility.

Táto práca sa zaoberá návrhom a implementáciou moderného domového zabezpečovacieho systému s využitím mikrokontroléra ESP32, ktorý vďaka integrovaným Wi-Fi schopnostiam, nízkej spotrebe energie a pokročilej hardvérovej výbave predstavuje ideálnu platformu pre IoT aplikácie. Navrhovaný systém kombinuje schopnosť detekcie pohybu pomocou rôznych typov senzorov s kontinuálnym monitorovaním a prenosom obrazu, čím poskytuje zabezpečenie priestoru s možnosťou vzdialeného prístupu.

Hlavným cieľom tejto práce je ukázať, ako možno využiť dostupné technologické prostriedky na vytvorenie modulárneho a rozšíriteľného zabezpečovacieho systému, ktorý je nielen cenovo dostupný, ale aj jednoducho integrovateľný do konceptu inteligentných domácností. Práca sa zameriava na analýzu existujúcich technológií, detailný návrh komunikačného protokolu medzi zariadeniami, implementáciu senzorických modulov a centrálnej riadiacej jednotky, ako aj vývoj používateľského rozhrania pre mobilnú aplikáciu, ktorá umožňuje vzdialenú správu systému.

Práca je rozdelená do siedmich kapitol. V nasledujúcej kapitole (2) je poskytnutý teoretický prehľad zabezpečovacích systémov a ich komponentov. Kapitola 3 analyzuje detekčné senzory a kamerové systémy kompatibilné s ESP32, najmä PIR detektory a radarové senzory. Kapitola 4 predstavuje návrh zabezpečovacieho systému vrátane blokovej schémy a komunikačných protokolov. V kapitole 5 je opísaná implementácia jednotlivých častí systému, kapitola 6 prezentuje výsledky testovania a experimentov. Záverečná kapitola 7 sumarizuje dosiahnuté výsledky a naznačuje možnosti budúceho vývoja.

Kapitola 2

Zabezpečovacie systémy

Zabezpečovacie systémy, ktoré dnes považujeme za kľúčový prvok ochrany objektov, majú dlhú históriu, ktorá siaha až do počiatkov ľudskej civilizácie. Prvé pokusy o ochranu majetku súviseli s inštinktom prežitia, pričom pravekí ľudia využívali prirodzené bariéry a jednoduché mechanizmy, ako sú kamenné zábrany alebo upozorňovacie systémy z vetiev. Tieto princípy sa postupne rozvíjali spolu s technologickým pokrokom.

Počas stredoveku a doby pred elektrinou sa ochranné opatrenia sústredili predovšetkým na architektúru, dizajn a zbrane. Vlastníci veľkých pozemkov využívali systém fyzických prekážok a obranných prvkov na ochranu svojich majetkov [11]. Medzi najúčinnejšie prostriedky patrili padacie mosty a priekopy, ktoré bránili nežiaducemu prístupu, spolu so strážnymi vežami, ktoré poskytovali strategický výhľad na okolie a včasnú detekciu potenciálnych hrozieb. Dôležitú úlohu v obrannom systéme zohrávali aj kanóny, ktoré slúžili na odstrašenie a prípadné zastavenie útočníkov z väčšej vzdialenosti, zatiaľ čo špeciálne navrhnuté otvory pre lukostrelcov umožňovali obrancom útočiť na nepriateľa bez vystavenia sa priamemu ohrozeniu. Súčasťou stredovekých bezpečnostných systémov boli tiež ťažké železné brány, ktoré predstavovali poslednú fyzickú bariéru pred vstupom do chráneného objektu a poskytovali značnú ochranu proti násilnému vniknutiu [11].

Poľnohospodárska revolúcia priniesla vznik trvalých sídiel, ktoré vyžadovali nové opatrenia na ochranu uskladnených potravín a hospodárskych zvierat. Postupne sa začali objavovať prvé technológie, ako mechanické zámky či strážne veže, ktoré znamenali prelom v ochrane majetku [11].

S rozvojom priemyselnej revolúcie a nástupom elektriny sa bezpečnostné systémy začali posúvať smerom k mechanizácii a automatizácii. Významným medzníkom bola inovácia mechanických a elektrických poplachových zariadení v 19. storočí, ktoré dokázali upozorniť majiteľov na nebezpečenstvo. Mechanické systémy využívali napnuté drôty alebo pružiny, ktoré pri narušení (napríklad otvorení dverí alebo okna) uvoľnili napätie, čo spustilo zvukový signál, ako je zvonček. Elektrické zariadenia zase využívali obvod s elektromagnetom, ktorý po narušení spustil alarm alebo svetelnú signalizáciu [5].

V 70. rokoch 20. storočia sa začala uplatňovať priemyselná televízia (CCTV, z anglického Closed-Circuit Television), ktorá umožňovala vizuálne monitorovanie prostredia [11]. Postupom času sa pridali senzory na detekciu pohybu, rozbitia skla a ďalšie technológie, ktoré priniesli možnosť sledovania udalostí v reálnom čase. Dnešné systémy zahŕňajú aj pokročilé riešenia, ako je integrácia s internetom, vzdialený prístup cez aplikácie či automatizované funkcie v rámci konceptu inteligentných domácností.

2.1 Rozdelenie zabezpečovacích systémov

Moderné zabezpečovacie systémy predstavujú sústavu, ktorá pozostáva z viacerých samostatných subsystémov. Tie sú vzájomne prepojené a spolupracujú s cieľom zabezpečiť ochranu objektu alebo priestoru. V rámci bezpečnostnej architektúry rozlišujeme tri hlavné druhy ochrany.

Režimová ochrana zahŕňa organizačné a režimové opatrenia, ktoré stanovujú pravidlá a postupy pre pracovníkov a návštevníkov chráneného objektu. Jej cieľom je nielen zvýšiť bezpečnosť, ale aj podporovať ďalšie formy ochrany. Tieto opatrenia určujú pohyb osôb v chránenom objekte a jeho okolí, ako aj tok informácií súvisiacich s ochranou [18].

Fyzická ochrana predstavuje prítomnosť fyzických osôb, ktoré vykonávajú obchôdzky, stráženie alebo prevádzkujú zabezpečovacie systémy. Podľa zákona č. 473/2005 Z. z. o súkromnej bezpečnosti môže byť táto ochrana realizovaná vlastnými prostriedkami (napr. osobný strážca alebo susedské hliadky) alebo prostredníctvom bezpečnostných služieb. Bezpečnostné služby sa delia na štátne a súkromné, pričom ich úlohou je vykonávať priamu kontrolu a riadenie ochrany [18].

Technická ochrana predstavuje jednoduchý a relatívne lacný spôsob ochrany, ktorý zahŕňa pasívne a aktívne prvky. Pasívne prvky, ako sú mechanické zábrany (stavebné konštrukcie, bezpečnostné sklá, uzamykacie systémy), plnia predovšetkým preventívnu funkciu. Aktívne prvky, ako sú poplachové systémy (napr. elektronický zabezpečovací systém – EZS, priemyselná televízia – CCTV, systémy kontroly a riadenia vstupu – SKV), poskytujú aktívnu detekciu a upozornenia na hrozby. Kombinácia technickej a fyzickej ochrany zabezpečuje vysokú mieru spoľahlivosti a odolnosti voči pokusom o narušenie [18].

V tejto kapitole sa bližšie zameriam na technickú ochranu, konkrétne na aktívne prvky tejto ochrany, ktoré sa primárne využívajú v interiéroch. Tieto prvky sú navrhnuté tak, aby poskytovali spoľahlivú detekciu a signalizáciu narušenia chránených priestorov, pričom často tvoria základnú súčasť moderných bezpečnostných systémov.

2.2 Elektronické zabezpečovacie systémy

Elektronický zabezpečovací systém (EZS) je súčasťou moderných bezpečnostných opatrení, ktoré slúžia na ochranu objektov pred narušiteľmi. Tento systém zabezpečuje detekciu a signalizáciu akýchkoľvek nežiaducich aktivít, ako je vniknutie do stráženého priestoru, a poskytuje okamžitú reakciu na bezpečnostné hrozby. V dnešnej dobe sa stáva neoddeliteľnou súčasťou ochrany domácností, firiem alebo verejných budov, čím prispieva k zníženiu rizika škôd spôsobených nelegálnymi vniknutiami.

Elektronický zabezpečovací systém predstavuje poplachový systém, ktorý musí podľa normy ČSN EN 50131-1 [21] obsahovať prostriedky pre detekciu a signalizáciu prítomnosti, vstupu alebo pokusu o vstup narušiteľa do stráženého objektu. V prípade narušenia poskytuje systém akustickú alebo optickú signalizáciu, čím zvyšuje ochranu a rýchlu reakciu na potenciálne bezpečnostné hrozby. Taktiež musia všetky komponenty obsahovať prostriedky pre detekciu sabotáže, ktoré zabezpečujú ochranu vnútorných súčiastok pred neoprávneným prístupom. Prístup k týmto súčiastkam musí vyžadovať použitie vhodného nástroja.

Norma ČSN EN 50131-1 tiež rozdeľuje EZS na štyri stupne zabezpečenia podľa miery rizika, čím umožňuje prispôsobenie ochrany konkrétnym potrebám [21]:

- **Stupeň zabezpečenia 1 (nízke riziko)** — Tento stupeň je vhodný pre objekty s nízkym rizikom, ako sú byty, rodinné domy alebo garáže, kde hrozba neoprávneného vstupu nie je vysoká.
- **Stupeň zabezpečenia 2 (nízke až stredné riziko)** — Používa sa na ochranu komerčných objektov alebo priestorov s mierne vyšším rizikom narušenia.
- **Stupeň zabezpečenia 3 (stredné až vysoké riziko)** — Je určený pre miesta, kde je vyššie riziko, ako sú banky, zlatníctva alebo historické pamiatky.
- **Stupeň zabezpečenia 4 (vysoké riziko)** — Tento stupeň zabezpečenia je navrhnutý pre objekty s najvyšším stupňom rizika, napríklad štátne inštitúcie alebo jadrové zariadenia.

Hlavnou súčasťou EZS je ústredňa, ktorá funguje ako riadiaca jednotka celého systému. Ústredňa spracováva signály zo všetkých pripojených zariadení, ktoré môžu byť pripojené buď káblovo, alebo bezdrôtovo. Kľúčovými komponentami sú tiež detektory, ktoré slúžia na identifikáciu narušenia, signalizačné a napájacie zariadenia.

Ústredňa

Ústredňa EZS je zariadenie určené na prijímanie a vyhodnocovanie elektrických signálov z detektorov alebo čidiel. Zaisťuje ich napájanie a zároveň ovláda signalizačné, prenosové a zapisovacie zariadenia [7]. Ďalej umožňuje ovládanie systému prostredníctvom vlastných ovládacích klávesníc alebo kódových zámkov, čím sa prepína medzi jednotlivými režimami.

Hlavnou funkciou elektronického zabezpečovacieho systému je signalizovanie pokusu nepovolanej osoby o vniknutie do chráneného objektu. Nepovolanou osobou je tá, ktorá nemá prístup k vypnutiu systému, teda nepozná potrebný kód, umiestnenie skrytého tlačidla, ovládač, alebo použije niektorý zo spôsobov na obídenie ochrany. Ústredne EZS typicky disponujú niekoľkými prevádzkovými režimami [18].

V režime stráženia ústredňa neustále monitoruje stav jednotlivých detektorov. Ak dôjde k zmene ich stavu, čo naznačuje narušenie chráneného objektu, systém vyvolá poplach. Pohotovostný režim neaktivuje stráženie celého objektu, ale chráni len komponenty systému EZS pred sabotážou. Poplach je vyvolaný len v prípade pokusu o sabotáž prvkov systému alebo ústredne samotnej [18].

Servisný režim slúži na nastavenie a údržbu systému. Tento režim umožňuje aj testovanie funkcií systému a montáž či demontáž komponentov. V servisnom režime ústredňa nezabezpečuje stráženie, čo je potrebné brať do úvahy pri manipulácii so systémom. Tento režim môže byť rozdelený na časť prístupnú užívateľovi, po zadaní hlavného kódu, a časť prístupnú pre servisné firmy alebo výrobcov, ktorí môžu vykonať zmeny v konfigurácii alebo aktualizáciu softvérového vybavenia [18].

Detektory

Detektor je zariadenie, ktoré slúži na vysielanie poplachového signálu ako reakciu na zaznamenanie neoprávneného vniknutia, zmeny prostredia alebo potenciálnych hrozieb v stráženom objekte. Senzor je komponent detektora, ktorý zaznamenáva zmenu stavu a slúži ako primárny zdroj informácií pre jeho aktiváciu. [18].

Detektory môžeme rozdeliť podľa rôznych kritérií:

- **Deštrukčné detektory** – vykonávajú jednorazovú funkciu a po aktivácii poplachu sa samovoľne zničia.
- **Napájané a nenapájané detektory** – zatiaľ čo napájané detektory vyžadujú externé napájanie na svoju činnosť, nenapájané detektory túto potrebu nemajú.
- **Priestorové detektory** – reagujú na narušenie alebo zmeny v stráženom priestore.
- **Smerové detektory** – detegujú narušenie v určenom smere, čím sledujú pohyb cez definovanú oblasť.

Všeobecné požiadavky na činnosť detektorov

Bezpečnostné detektory musia spĺňať viacero technických požiadaviek, aby zabezpečili spoľahlivú prevádzku v rámci zabezpečovacích systémov. Základnou funkciou každého detektora je schopnosť prijímať fyzikálne podnety zo stráženého priestoru alebo objektu a v prípade, že tieto podnety dosiahnu stanovené hodnoty, generovať zodpovedajúci elektrický signál na výstupe [8].

Z technického hľadiska musia detektory vykazovať odolnosť voči neoprávneným zásahom, ktoré by mohli narušiť ich funkčnosť. Súčasne je nevyhnutná kompatibilita s ostatnými komponentmi systému, čo zahŕňa schopnosť prijímať a spracovávať informácie z iných zariadení v zabezpečovacom systéme [18, 21]. V rámci zabezpečenia integrity celého systému musia detektory poskytovať signalizáciu o svojom prevádzkovom stave, vrátane hlásenia porúch, pokusov o sabotáž alebo manipuláciu [8].

Spoľahlivá prevádzka detektorov vyžaduje stabilitu pri kolísaní napájacieho napätia. Konkrétne musí detektor správne fungovať aj pri zmenách nominálneho napájacieho napätia v rozsahu ±25%. Zároveň nesmie byť citlivý na zvlnenie napájacieho napätia v pracovnom rozsahu s úrovňou 1 Vpp a musí disponovať ochranou proti prepólovaniu napájacieho napätia [18]. Táto požiadavka je podstatná najmä v priemyselných prostrediach, kde môže dochádzať k častým výkyvom elektrického napätia, ktoré by mohli ovplyvniť funkčnosť bežných elektronických zariadení.

Dôležitým parametrom je tiež nízka chybovosť, ktorá by pri maximálnej citlivosti nemala prekročiť jednu chybu za 1000 hodín prevádzky. Minimálna citlivosť detektora musí dosahovať aspoň 20% z celkovej možnej citlivosti [18].

Z hľadiska prevádzky je významná aj rýchlosť aktivácie. Po pripojení k napájaciemu napätiu musí detektor dosiahnuť plnú funkčnosť do 180 sekúnd, pričom pri kapacitných detektoroch je tento čas predĺžený na 5 minút [18, 21].

Špeciálnym typom sú priestorové detektory, ktoré musia byť odolné voči falošným poplachom. Tieto môžu byť spôsobené prítomnosťou malých zvierat, prúdením vzduchu, priamym osvetlením reflektormi automobilov alebo inými zdrojmi svetla [8].

Detektory plášťovej ochrany

Plášťová ochrana zabezpečuje kontrolu stavebných otvorov a povrchu plášťa budovy, aby sa zabránilo neoprávnenému vniknutiu.

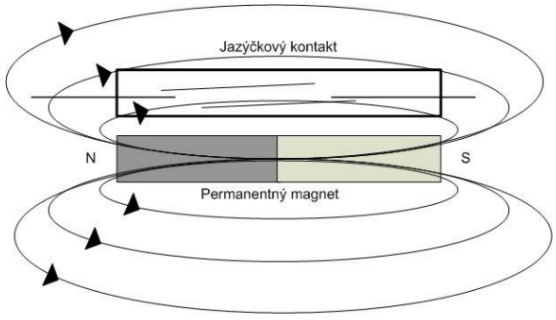
Mechanické kontakty

Mechanické kontakty sa používajú na zabezpečenie stavebných otvorov, ako sú dvere, okná alebo kryty vetracích šácht. Využívajú špeciálne spínače a mikrospínače, ktoré sú prispô-

sobené na zabudovanie do týchto prvkov. Sú ideálnym riešením na detekciu uzamknutia okien alebo dverí, čo nie je možné dosiahnuť pomocou magnetických kontaktov alebo iných typov senzorov. Keď je okno zatvorené alebo zámok uzamknutý, spínač zostáva zopnutý. Ak dôjde k narušeniu, spínač sa rozopne, čím ústredňa signalizuje poplach. Hoci sú mechanické kontakty pomerne jednoduché na obídenie, ich účinnosť sa zvyšuje kombináciou s ďalšími prvkami elektronického zabezpečovacieho systému [18].

Magnetické kontakty

Magnetické kontakty, podobne ako mechanické, slúžia na zabezpečenie stavebných otvorov. Skladajú sa z permanentného magnetu a jazýčkového kontaktu, ktorý je umiestnený v sklenenej rúrke s ochrannou atmosférou [3]. Magnet sa inštaluje na pohyblivú časť, napríklad na dvere alebo okenný rám, zatiaľ čo jazýčkový kontakt je upevnený na pevnú časť, ako je zárubňa. Keď je magnet v blízkosti kontaktu, vplyvom jeho magnetického poľa zostáva zopnutý. Ak sa magnet vzdiali, napríklad pri otvorení dverí alebo okna, pole zoslabne, čo spôsobí rozopnutie. [18]. Princíp fungovania magnetického kontaktu je znázornený na obrázku 2.1.



Obr. 2.1: Princíp fungovania magnetického kontaktu [18].

Vibračné detektory

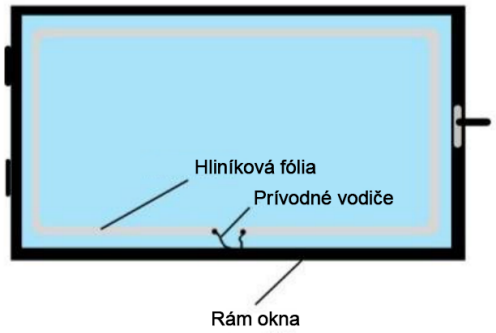
Tieto detektory dokážu rozpoznať nízkofrekvenčné vibrácie alebo energiu, ktoré vznikajú pri pokusoch o násilné preniknutie cez fyzické bariéry, na ktorých sú inštalované. Aj keď sa dajú použiť na ochranu bariér z rôznych pevných materiálov, je potrebná opatrnosť pri ich nasadení na menej pevné steny, ako sú sadrokartónové alebo tenké kovové pláty. Tieto materiály môžu byť ľahko rozvibrované vonkajšími vplyvmi, čo môže spôsobiť falošné poplachy [1, 17].

Detektory rozbitia skla

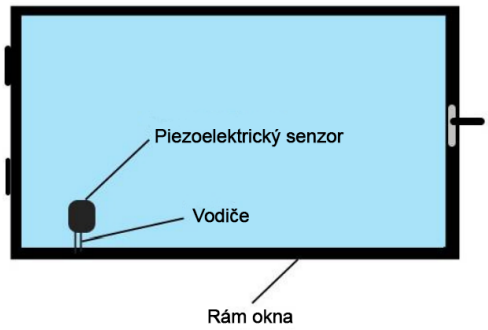
Detektor rozbitia skla je zariadenie, ktoré deteguje vibrácie alebo nárazy na povrchu skla, na ktoré je pripojené. Ak dôjde k rozbitiu skla, zariadenie spustí poplach. Detektory rozbitia skla sa delia na:

- **Kontaktné snímače** – Tieto detektory fungujú na princípe uzavretého elektrického obvodu, ktorý sa preruší rozbitím skla. Obvod je tvorený vodivou fóliou nalepenou na povrchu skla [18]. Nevýhodou je nízka odolnosť voči vyrezaniu skla alebo manipulácii, napríklad prepojením vodičov. Spôsob umiestnenia tohto snímača je znázornený na obrázku 2.2.

- **Piezoelektrické snímače** – Tieto snímače vyhodnocujú vibrácie, ktoré vznikajú pri rozbití alebo rezaní skla. Využívajú piezoelektrický kryštál, ktorý pri vibráciách generuje elektrický signál [18]. Riadiaca jednotka tento signál porovnáva s prednastavenými vzorkami a v prípade zhody vyhlási poplach. Dosah týchto snímačov je 1,5 až 5 metrov, pričom sa inštalujú priamo na sklenené plochy ako je aj možné vidieť na obrázku 2.3.
- **Akustické detektory** – Tieto detektory detegujú zvuk rozbitia skla pomocou mikrofónu. V zariadení sa následne filtruje a analyzuje akustické spektrum pomocou pásmových filtrov, ktoré prepúšťajú iba frekvencie typické pre rozbitie skla. Pokročilejšie modely využívajú viacnásobné pásmové filtre alebo analyzujú zvukové spektrum v diskrétnych bodoch [7]. Alarm sa spustí iba vtedy, keď sú všetky špecifické frekvencie prítomné v určitom časovom intervale.
- **Aktívne detektory** – Tieto detektory obsahujú prijímaciu aj vysielaciu časť a fungujú na princípe detekcie zmien v elektromagnetickom žiarení. Toto žiarenie je vysielané do monitorovaného priestoru a odrazené od okien alebo stien. Ak dôjde k rozbitiu skla, spôsobí to zmenu odrazeného žiarenia oproti normálnemu stavu. Zariadenie zmenu porovná s uloženými hodnotami v pamäti a dokáže tak rozpoznať narušenie [7].



Obr. 2.2: Spôsob umiestnenia kontaktného snímača [18].



Obr. 2.3: Spôsob umiestnenia piezoelektrického snímača [18].

Detektory priestorovej ochrany

Priestorová ochrana slúži ako doplnok k plášťovej ochrane, pričom jej úlohou je zabezpečiť vnútorné priestory objektov detekciou pohybu alebo prítomnosti narušiteľa. Tieto systémy sa inštalujú na strategické miesta, ako sú schodištia, haly alebo spojovacie chodby, aby efektívne monitorovali všetky dôležité prístupové body a zvýšili celkovú bezpečnosť objektu.

Detektory priestorovej ochrany sa podľa typu delia do niekoľkých kategórií, pričom každá z nich využíva odlišné fyzikálne princípy a deteguje rôzne druhy elektromagnetických vĺn [18]. Pasívne infračervené detektory (PIR) fungujú na báze detekcie infračerveného žiarenia, reagujúc tým na tepelné zmeny v chránenom priestore. Na druhej strane, aktívne ultrazvukové detektory (US) aktívne vysielajú ultrazvukové vlny a následne analyzujú ich odraz, pričom zmeny v tomto odraze signalizujú prítomnosť pohybu. Podobne pracujú aj aktívne mikrovlnné detektory (MW), ktoré namiesto ultrazvuku využívajú mikrovlnné žiarenie na detekciu pohybu prostredníctvom zmien v odraze týchto vĺn. V praxi sú často

využívané aj kombinované detektory (PIR-US, PIR-MW), ktoré integrujú dve rôzne technológie, napríklad infračervené s ultrazvukovými alebo infračervené s mikrovlnnými, čím dosahujú vyššiu presnosť detekcie a zníženie počtu falošných poplachov [18].

Pasívne infračervené detektory

Pasívne infračervené detektory (PIR) sú zariadenia, ktoré detegujú zmeny infračerveného vyžarovania. Tieto detektory používajú pyroelektrický senzor na rozpoznanie pohybu objektov s teplotou odlišnou od okolitého prostredia [20, 3]. PIR detektory sú podrobnejšie popísané v sekcii 3.1.

Ultrazvukové detektory

Ultrazvukový detektor pohybu spravidla obsahuje vysielač, prijímač a riadiacu jednotku. Počas činnosti vysielač generuje ultrazvukové vlnenie, ktoré vytvára detekčnú zónu. Vlny sa odrážajú od povrchov, ako sú steny, stropy či podlahy, a sú zachytávané prijímačom. Procesor analyzuje tieto odrazy; ak frekvencia zostane nezmenená, poplach sa neaktivuje. Pohyb v detekčnej zóne však spôsobuje Dopplerov frekvenčný posun, ktorý spúšťa poplach [1]. Tieto detektory majú malé rozmery a používajú sa pri rôznych frekvenciách začínajúcich od 20 kHz, ktoré nie sú počuteľné pre ľudí, ale môžu ovplyvniť zvieratá so zvýšenou citlivosťou na ultrazvuk [18].

Detektory sa inštalujú tak, aby pohyb smeroval k prijímaču alebo od neho, pričom dosah je približne 10 metrov. Ich citlivosť môže byť znížená materiálmi, ktoré absorbujú zvuk, ako sú koberce alebo penové materiály, a tiež objektmi, ktoré blokujú vlny [18].

Mikrovlnné detektory

Mikrovlnné detektory detegujú pohyb na základe elektromagnetických vĺn, podobne ako ultrazvukové detektory, no s využitím vyšších frekvencií v pásme 2.5 až 24 GHz [3, 17]. Tieto detektory sú aktívne zariadenia, ktoré vysielajú mikrovlny do stráženého priestoru a následne vyhodnocujú zmeny, ktoré nastanú pri pohybe objektov. Mikrovlnné detektory majú typicky dosah 15 až 30 metrov. Na rozdiel od PIR a ultrazvukových detektorov sú mikrovlnné detektory citlivé aj na rušenie z priestorov mimo stráženej zóny, čo zvyšuje riziko falošných poplachov [1].

Ovládacie zariadenia

Aby elektronický zabezpečovací systém mohol správne fungovať, je nevyhnutné ho aktivovať (uviesť do stavu stráženia) alebo deaktivovať. Na tento účel slúžia ovládacie zariadenia, ktoré umožňujú používateľom spravovať stav systému. Tieto zariadenia môžu byť rôzneho typu v závislosti od technológie a požiadaviek na bezpečnosť [18]:

- **Blokovací zámok** – Kombinuje mechanickú ochranu dverí s funkciami elektronického zabezpečovacieho systému. Inštaluje sa ako dodatočný zámok na vstupné dvere a ponúka užívateľovi jednoduchý spôsob ovládania EZS bez potreby zapamätať si číselný kód. Uzamknutie zámku je možné iba v prípade, že je systém v normálnom (nealarmujúcom) stave. Ak napríklad zostane otvorené okno, elektromagnetická západka zabráni uzamknutiu zámku a tým aj aktivácii systému do režimu stráženia. Tento mechanizmus poskytuje istotu, že systém sa nemôže aktivovať, pokiaľ nie sú splnené všetky bezpečnostné podmienky.

- **Kódové klávesnice** – Používajú sa ako spínacie zámky a môžu plniť funkciu ovládacieho prvku ústrední elektronických zabezpečovacích systémov. Pri ich použití je dôležité pamätať si správny prístupový kód, ktorý by sa mal pravidelne meniť. Dlhodobé používanie jedného kódu môže viesť k bezpečnostným rizikám, ako napríklad uhádnutie kódu na základe opotrebovania tlačidiel.
- **Ovládanie kartou** – Systém ponúka výhodu v podobe multifunkčnosti identifikačnej karty, ktorá môže byť využitá aj na iné účely. Na druhej strane, jeho nevýhodou je prenosnosť karty a potenciálne riziko jej skopírovania. Pre vyššiu úroveň ochrany je odporúčané kombinovať kartu s ďalšími bezpečnostnými prvkami.
- **Diaľkový ovládač** – Slúži na ovládanie elektronického zabezpečovacieho systému, umožňuje jeho aktiváciu alebo deaktiváciu. Okrem toho môže mať aj ďalšie funkcie, ako napríklad spustenie tiesňového hlásenia. Aby sa predišlo riziku zachytenia signálu a následnému vyrobeniu kópie ovládača, mal by byť chránený vhodným kódom.

Indikačné zariadenia

Indikačné prvky poskytujú informácie o stave ústredne a celkovom fungovaní systému. Tieto informácie môžu byť zobrazené buď opticky, akusticky, alebo kombinovaním oboch foriem. Ovládacie prvky zohrávajú úlohu pri diagnostike systému, ktorá je vykonávaná pomocou špecializovaných diagnostických programov [18].

Podľa normy ČSN EN 50131-1 [21] musí akustické signalizačné zariadenie v prípade narušenia fungovať minimálne 90 sekúnd a jeho maximálna doba prevádzky nesmie presiahnuť 15 minút.

2.3 Priemyselná televízia

Priemyselná televízia, známa pod skratkou CCTV (z anglického Closed-Circuit Television), sa v priebehu posledných desaťročí stala kľúčovým nástrojom v oblasti bezpečnosti a jej technologický pokrok umožňuje plniť rôznorodé úlohy. Okrem prevencie kriminality dnes dokážu tieto systémy efektívne podporovať forenzné vyšetrovanie a okamžitú reakciu na narušenie bezpečnosti. Zatiaľ čo pôvodne boli kamery vnímané najmä ako odstrašujúci prostriedok, ich účinnosť v tejto oblasti sa znižuje, a to najmä v dôsledku ich rozšírenosti a zníženého vnímania rizika zo strany potenciálnych páchateľov [13].

Samostatné kamery však často nestačia na zabezpečenie efektívnej ochrany – ich účinnosť sa zvyšuje, keď sú prepojené s ďalšími bezpečnostnými opatreniami, ako sú dobré osvetlenie, oplotenie či prítomnosť bezpečnostného personálu. V kombinácii s aktívnym monitorovaním a rýchlou reakciou, ako sú zásahy polície alebo iné proaktívne bezpečnostné stratégie, môžu CCTV systémy významne prispieť k zníženiu kriminality a narušení bezpečnosti v strážených oblastiach [13].

V súčasnosti sú CCTV kamery vybavené rôznymi pokročilými funkciami, ako je detekcia pohybu, rozpoznávanie tvárí, kompenzácia protisvetla a inteligentná video analýza, ktorá zlepšuje efektivitu monitorovania tým, že dokáže automaticky analyzovať veľké množstvo informácií [12]. V kombinácii s ďalšími bezpečnostnými systémami, ako sú elektronické požiarne a zabezpečovacie systémy (EPS a EZS), vytvára CCTV komplexný ochranný mechanizmus, ktorý poskytuje vysokú úroveň bezpečnosti a efektívnej detekcie hrozieb.

Termálne kamery v kontexte CCTV

Termálne kamery, ktoré fungujú na princípe snímania tepelného žiarenia, predstavujú špeciálnu kategóriu CCTV systémov. Ich história siaha až do objavenia infračerveného žiarenia v roku 1800 Sir Williamom Herschelom. Ich prvé praktické využitie bolo zaznamenané v roku 1929, keď fyzik Kálmán Tihanyi vyvinul termografickú kameru pre protivzdušnú obranu [2].

Dnešné termálne kamery nachádzajú uplatnenie v širokom spektre aplikácií, pričom medzi najvýznamnejšie patrí perimetrická ochrana, kde detegujú tepelné zdroje aj v úplnej tme alebo cez dym, čím poskytujú efektívne monitorovanie vstupov a pohybov v kritických oblastiach. Táto vlastnosť ich predurčuje na použitie v miestach s vysokými bezpečnostnými požiadavkami. Ďalšou dôležitou oblasťou ich aplikácie je monitorovanie zariadení, pri ktorom dokážu identifikovať potenciálne poruchy na základe detekcie zvýšenej teploty, čím prispievajú k minimalizácii rizika požiarov, neplánovaných odstávok a v konečnom dôsledku aj k zvyšovaniu celkovej produktivity prevádzky [2].

Na rozdiel od bežných infračervených kamier, ktoré pracujú na princípe odrazu svetla, termálne kamery dokážu rozlíšiť aj minimálne rozdiely v teplote, čo umožňuje presnejšiu identifikáciu rizík.

2.4 Systém kontroly vstupu

Systémy kontroly vstupu môžeme všeobecne definovať ako elektronické systémy, ktorých úlohou je riadiť vstup alebo výstup z chráneného objektu alebo miestnosti. Ich cieľom je umožniť vstup oprávneným osobám a zabrániť vstupu neoprávnených osôb do chránených priestorov. Na tento účel kombinujú prvky elektronického alarmového systému s mechanickými zabezpečovacími prostriedkami. V závislosti od požadovanej úrovne bezpečnosti môžu byť tieto systémy doplnené aj o dohľad ľudskou obsluhou v monitorovacom centre [10].

Konkrétna konštrukcia a návrh systému sa prispôsobuje potrebám vlastníka, špecifikám chráneného objektu a požadovanej úrovni zabezpečenia. Tieto systémy sa vyrábajú v rôznych variantoch v závislosti od ich účelu a stupňa ochrany . Základné systémy obsahujú jednu čítačku s integrovaným rozhodovacím modulom a databázou používateľov, čo predstavuje vhodné riešenie pre jednoduchšie aplikácie, kde nie je potrebná vysoká úroveň ochrany - napríklad pre zabezpečenie jednej alebo dvoch miestností či vstupu do menšej budovy. Pre kontrolu viacerých miestností alebo vstupov je však vhodnejšie implementovať komplexnejšiu architektúru systému. Takáto typická architektúra zahŕňa niekoľko kľúčových komponentov: čítače prístupu, ktoré sú umiestnené na vstupoch do jednotlivých chránených miestností; centrálnu riadiacu jednotku, ktorá je pripojená k čítačom a ďalším rozšíreniam systému; a mechanické bezpečnostné zariadenia ako elektronické zámky, dverové uzávery, rôzne typy senzorov a napájacie zdroje [10].

Riadiace jednotky sú však obmedzené svojou kapacitou – štandardne dokážu spravovať 4 až 8 dverí. Pre väčší počet vstupov je nutné systém rozšíriť o ďalšie jednotky a čítačky, ktoré sa vzájomne prepoja. V prípade rozsiahlych systémov môžu byť riadiace jednotky napojené na počítačovú sieť a ich databázy uložené na serveri [10].

Princíp fungovania systému kontroly vstupu

Princíp fungovania systému kontroly vstupu spočíva v tom, že osoba, ktorá žiada o prístup, musí na mieste vstupu preukázať svoju identitu. Existuje niekoľko spôsobov identifikácie:

znalosť (napr. PIN kód alebo heslo), vlastníctvo tokenu (napr. NFC štítok či RFID karta) alebo použitie biometrických údajov, ako sú odtlačky prstov, dúhovka alebo sietnica oka [3, 10]. Čítačka prístupu načíta identifikačné údaje a odošle ich riadiacej jednotke, ktorá ich porovná so svojou databázou. Ak sa údaje zhodujú, systém povolí vstup, napríklad odblokovaním zámku alebo turniketu, pričom žiadosť o prístup zaznamená. Ak sa však identifikačné údaje nezhodujú, vstup nie je umožnený a systém signalizuje pokus o neoprávnený prístup.

Biometria v systémoch kontroly vstupu

Biometria predstavuje moderný spôsob autentifikácie osôb v rámci systémov kontroly vstupu, ktorý využíva jedinečné fyzické alebo behaviorálne vlastnosti jednotlivca. Medzi najčastejšie používané biometrické charakteristiky patrí napríklad odtlačok prsta, tvárové rysy alebo štruktúra ciev na dlani. Tieto charakteristiky sú unikátne pre každého jednotlivca, čím poskytujú vysokú úroveň bezpečnosti a ochrany pred neoprávneným prístupom [3].

Proces biometrickej autentifikácie zahŕňa dve fázy. Najskôr sa biometrický údaj nasníma a uloží ako šablóna do databázy alebo na bezpečnostnú kartu. Pri autentifikácii sa daný údaj znovu nasníma a porovná s uloženou šablónou [3]. Ak je zhoda dostatočne presná, systém povolí prístup. Tento spôsob autentifikácie znižuje riziko podvodu, pretože biometrické údaje nie je možné zdieľať ani jednoducho sfalšovať, ako je to v prípade hesiel alebo fyzických kľúčov.

Postavenie systému kontroly vstupu v oblasti alarmových systémov

Systémy kontroly vstupu zohrávajú kľúčovú úlohu v celkovom zabezpečení budov a alarmových systémoch. Na rozdiel od bežných alarmových systémov zahŕňajú aj mechanické prvky, ako sú turnikety, bezpečnostné priechody, elektrické či magnetické zámky a ďalšie zariadenia. Tieto systémy bývajú často prepojené s alarmovými systémami. Pri pokuse neoprávneného užívateľa prekonať prístupový bod systém pokus zaznamená, a ak dôjde k jeho prekonaniu, môže aktivovať poplachový režim v alarmovom systéme. Systém kontroly vstupu tak môže fungovať ako aktívna súčasť celkového alarmového riešenia [10].

Systémy kontroly prístupu k údajom

Kontrola prístupu k údajom predstavuje spôsob obmedzovania prístupu zamestnancov k firemným súborom za účelom ochrany údajov. Táto metóda sa opiera o princíp najnižších oprávnení (POLP), ktorý zabezpečuje, že zamestnanci majú prístup iba k údajom potrebným na výkon ich pracovných povinností, pričom ich prístup je striktne obmedzený podľa definovaných pravidiel [15].

Modely kontroly prístupu k údajom

Existujú tri hlavné modely, ktoré určujú, ako sa prístupové práva v organizácii prideľujú a spravujú, pričom každý z nich poskytuje odlišnú úroveň bezpečnosti a flexibility.

Diskrečná kontrola prístupu (DAC) predstavuje najvoľnejší spôsob správy prístupu, čo ju robí najmenej vhodnou pre firemné prostredie, keďže kontrolu nad oprávneniami používateľov majú majitelia podnikov namiesto bezpečnostných odborníkov, čím sa výrazne zvyšuje riziko neoprávneného prístupu k citlivým údajom [15].

Na druhej strane, povinná kontrola prístupu (MAC) nachádza uplatnenie v organizáciách, ktoré vyžadujú vysokú úroveň ochrany a súkromia, pretože v tomto modeli má

správca úplnú kontrolu nad prideľovaním prístupových práv a bezpečnostných oprávnení, čo zabezpečuje prísnu ochranu citlivých údajov a významne znižuje riziko bezpečnostných incidentov [15].

Medzi najpoužívanejšie modely však patrí kontrola prístupu podľa rolí (RBAC), ktorá je založená na pracovných pozíciách zamestnancov, kde je prístup k údajom obmedzený výlučne na základe konkrétnej pracovnej role, pričom všetky pokusy o prístup k údajom mimo definovaného rozsahu sú systémom automaticky zamietnuté, čo poskytuje rovnováhu medzi bezpečnosťou a použiteľnosťou [15].

Kapitola 3

Detekčné senzory a kamerové systémy pre platformu ESP32

Táto kapitola sa zameriava na najčastejšie používané detekčné senzory kompatibilné s ESP32, ako sú pasívne infračervené detektory a radarové senzory, a predstavuje možnosti, ktoré ESP32 a jeho špecializovaná verzia ESP32-CAM ponúkajú pre tvorbu zabezpečovacích a monitorovacích systémov.

3.1 Pasívne infračervené detektory

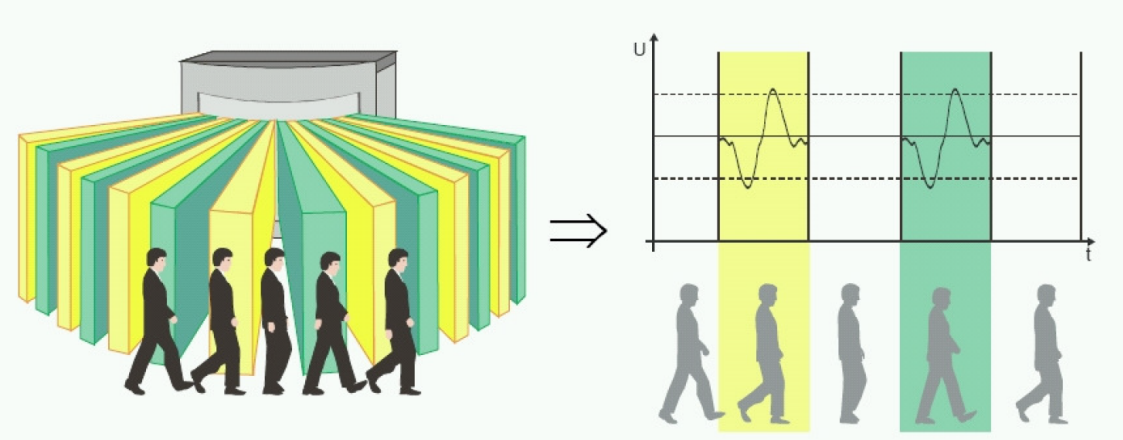
Pasívny infračervený detektor (PIR), slúži na detekciu infračerveného žiarenia. Ako pasívne zariadenie samé nevysiela energiu, ale zachytáva tepelné žiarenie vyžarované objektmi v jeho zornom poli, ako sú ľudia, zvieratá alebo pohybujúce sa predmety [20]. Skratka PIR sa niekedy interpretuje aj ako „pyroelektrický infračervený senzor“ vzhľadom na mechanizmus, ktorým zachytáva zmeny tepelného žiarenia.

Primárnym účelom PIR detektorov je detekcia prítomnosti živých bytostí, pričom sa najčastejšie používajú v bezpečnostných systémoch, alarmoch a na kontrolu prístupu. Keď sa v snímacom rozsahu detektora objaví objekt, ktorý vyžaruje infračervené žiarenie, senzor identifikuje zmenu v tomto žiarení a môže signalizovať prítomnosť osoby alebo zvieraťa [20].

Základné časti PIR detektora

- **Optický systém** – využíva sústavu Fresnelových šošoviek alebo členené parabolické zrkadlo na zaostrenie infračerveného žiarenia na detekčný prvok.
- **Detektor infračerveného žiarenia** – slúži na snímanie zmeny žiarenia v infračervenom spektre.
- **Elektronika na spracovanie snímaného signálu** – analyzuje výstupné signály z detektora a určuje, či došlo k detekcii pohybu.
- **Zaisťovací kontakt (TAMPER)** – zabezpečuje signalizáciu pri pokuse o neoprávnenú manipuláciu s detektorom.
- **Indikačné prvky LED** – slúžia na vizuálnu indikáciu stavu detektora.
- **Doplnkové obvody** – zahŕňajú ďalšie funkčné prvky pre rozšírenie možností detektora.

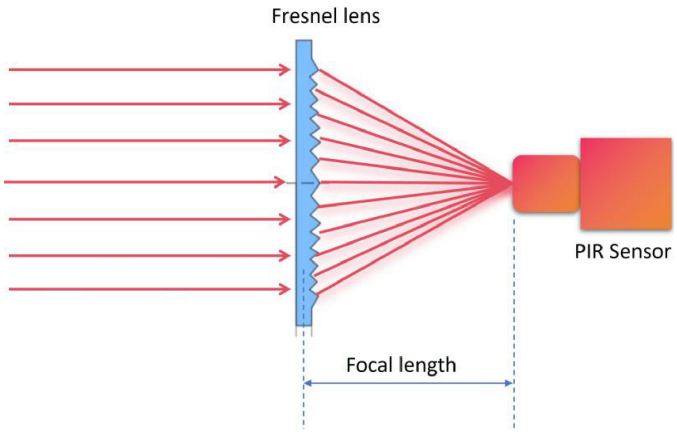
Rozdelenie zorného poľa PIR detektora na jednotlivé zóny umožňuje zachytiť pohyb objektov, ktoré sa medzi týmito zónami presúvajú, do nich vstupujú alebo ich opúšťajú [18]. Na obrázku 3.1 je zobrazený priebeh napätia na senzore pri prechode osoby jednotlivými detekčnými zónami, čo ilustruje spôsob, akým detektor registruje pohyb.



Obr. 3.1: Rozdelenie zorného pola PIR detektora do zón [18].

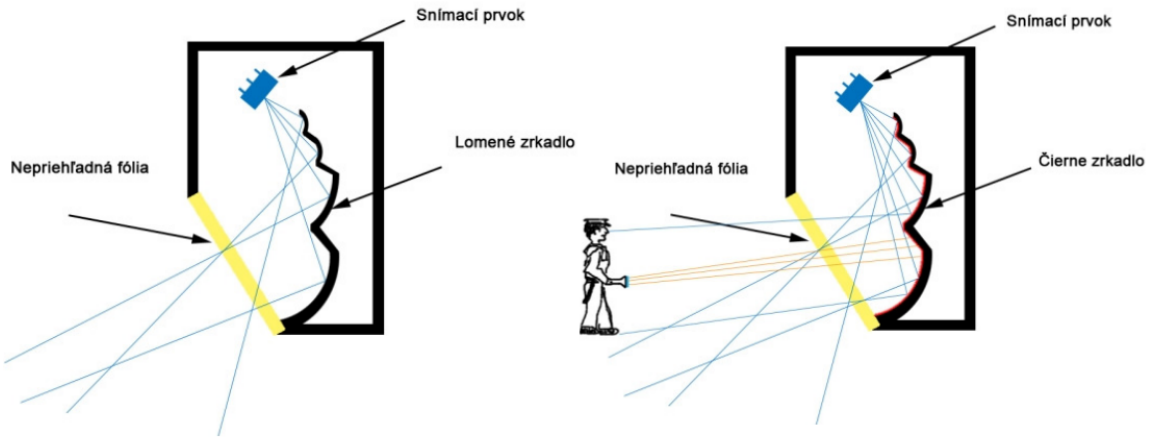
Najvyššiu citlivosť má detektor na pohyb kolmo na svoju optickú os, zatiaľ čo pri pohybe priamo smerom k detektoru alebo od neho je jeho citlivosť výrazne nižšia. Preto je zorné pole detektora často rozdelené nielen horizontálne, ale aj vertikálne, aby sa dosiahla vyššia detekčná schopnosť [18].

Optické systémy v detektoroch zahŕňajú sústavy šošoviek alebo lomených zrkadiel. Šošovky sú umiestnené tak, aby bol pyroelektrický senzor presne v ich ohnisku, čím sa dosiahne optimálna detekcia infračerveného žiarenia, ako je znázornené na obrázku 3.2. Z plastových materiálov sa najčastejšie využívajú Fresnelove šošovky, charakteristické svojím stupňovitým tvarom. Tieto šošovky pozostávajú zo sústavy priehľadných a nepriehľadných prstencov usporiadaných okolo spoločného stredu. Fresnelove šošovky, pôvodne vyvinuté francúzskym fyzikom Augustinom Fresnelom pre použitie v majákoch, sa vyznačujú kratšou ohniskovou vzdialenosťou a vyžadujú menej materiálu než konvenčné šošovky, čo vedie k zníženiu hmotnosti a objemu [19].



Obr. 3.2: Sústredenie infračerveného žiarenia fresnelovou šošovkou na senzor [19].

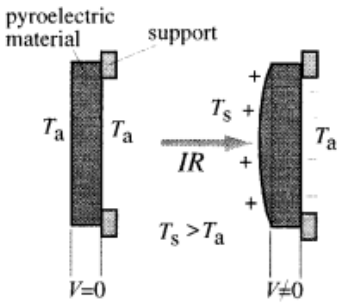
V detektoroch sa okrem Fresnelových šošoviek často používajú aj sústavy lomených zrkadiel. Tento typ optického systému je založený na parabolickom zrkadle, v ktorého ohnisku je umiestnený pyroelektrický senzor [18]. Jedným z typov lomených zrkadiel je tzv. „čierne zrkadlo.“ Toto zrkadlo dokáže účinne odrážať infračervené žiarenie vyžarované ľudským telom, pričom zároveň absorbuje viditeľné svetlo, ako sú reflektory, batérie alebo odrazené slnečné lúče. Obrázok 3.3 znázorňuje príklady klasického lomeného zrkadla a čierneho zrkadla používaných v detektoroch.



Obr. 3.3: Znázornenie detektoru s využitím lomeného a čierneho zrkadla [18].

Pyroelektrický senzor

Pyroelektrický senzor je založený na použití pyroelektrických materiálov, často kryštály alebo špecifické keramické materiály, ktoré generujú elektrický náboj v reakcii na prúdenie tepla cez ich štruktúru. To spôsobuje ich rozťahovanie (termo-expanziu) a generácia náboja je vedľajší efekt tohto javu, čo znázorňuje aj obrázok 3.4. Okrem pyroelektrického efektu sú tieto materiály aj piezoelektrické, čo znamená, že dokážu generovať elektrický náboj aj v reakcii na mechanický stres [20].



Obr. 3.4: Zjednodušený model pyroelektrického efektu ako vedlajší efekt piezoelektriky [20].

Keď materiál absorbuje teplo, spôsobí to jeho rozťahovanie, čo vedie k vývoju piezoelektrického náboja na elektródach umiestnených na opačných stranách materiálu [3]. Tento náboj sa prejaví ako napätie medzi týmito elektródami. Problém však spočíva v tom, že

piezoelektrické vlastnosti materiálu môžu tiež generovať náboj v dôsledku mechanického stresu, ako sú vietor, vibrácie budov alebo silné zvuky, ktoré môžu rušiť detekciu tepelného signálu. Tento signál je často nerozoznateľný od toho, ktorý je generovaný infračervenými tepelnými vlnami [20].

Aby sa oddelili tepelne indukované náboje od tých, ktoré sú spôsobené piezoelektrickým efektom, je pyroelektrický senzor často navrhnutý so symetrickým usporiadaním. To znamená, že vnútri senzora sú dva rovnaké pyroelektrické prvky, ktoré sú navzájom prepojené tak, že generujú opačné signály, keď sú vystavené rovnakým podmienkam. Tento dizajn zabezpečuje, že rušivé vplyvy, ako je piezoelektrický efekt, ovplyvnia oba prvky rovnakým spôsobom, čím sa tieto rušenia na výstupe zrušia [3, 20]. Tepelná radiácia ovplyvní len jeden z pyroelektrických prvkov naraz, pretože každý prvok je umiestnený tak, aby reagoval na zmenu teploty v určitom smere. Keď sa teplo dostane do senzora, vyvolá jeho expanziu a tým aj zmenu v generovaní elektrického náboja. Týmto spôsobom vzniká rozdiel medzi nábojmi v jednotlivých prvkoch [20].

3.2 Radarové senzory

Akronym „RADAR“ (**RA**dio (Aim) **D**etecting **A**nd **R**anging) bol prvýkrát predstavený americkým námorníctvom v roku 1940, poručíkom Samuelom M. Tuckerom a F. R. Furthom. V roku 1943 ho oficiálne prijali spojenecké sily počas druhej svetovej vojny a následne sa stal medzinárodne uznávaným [14].

Radar je elektromagnetický systém určený na detekciu a lokalizáciu objektov. Funguje na princípe vysielania energie do priestoru a detekcie spätného signálu, ktorý sa odráža od objektu, čiže cieľa. Tento odrazený signál, nazývaný ozvena (echo), signalizuje prítomnosť cieľa a umožňuje určiť jeho polohu porovnaním s pôvodným signálom [16].

Radar s kontinuálnou vlnou

Radar s kontinuálnou vlnou (Continuous Wave radar, CW-Radar) funguje na princípe nepretržitého vysielania rádiových vĺn na jednej frekvencii. Tieto vlny sú smerované do pozorovanej oblasti, kde časť z nich narazí na objekt, odrazí sa a následne je zachytená prijímacou anténou. Na základe analýzy prijatých vĺn možno získať informácie o cieli [14].

Dopplerov radar

Dopplerov radar je špecializovaný druh CW radaru, ktorý využíva Dopplerov efekt na meranie rýchlosti objektu. Tento typ radaru vysiela kontinuálnu vlnu s konštantnou frekvenciou a amplitúdou. Odrazený signál (ozvena) má rovnakú frekvenciu, ak je odrážajúci objekt stacionárny. Ak sa však objekt pohybuje radiálne voči radaru, odrazený signál je posunutý o tzv. Dopplerovu frekvenciu, čo umožňuje detekciu rýchlosti objektu [16].

$$f_D = \frac{2v}{\lambda} \tag{3.1}$$

Vzorec 3.1 vyjadruje vzťah medzi Dopplerovou frekvenciou a radiálnou rýchlosťou cieľa, pričom Dopplerova frekvencia f_D v hertzoch predstavuje posun frekvencie vznikajúci pri odraze radarového signálu od pohybujúceho sa objektu. Radiálna rýchlosť cieľa v v metroch za sekundu vyjadruje relatívnu rýchlosť objektu vzhľadom na radar v smere ich vzájomného spojenia. λ predstavuje vlnovú dĺžku vysielača.

V prípade Dopplerovho radaru nie je nutné merať čas návratu signálu, keďže sa nevykonáva určovanie vzdialenosti. Ak by však bolo potrebné vykonať meranie vzdialenosti, musí byť vysielaný signál modulovaný [14]. Táto modulácia umožňuje určiť časovú referenciu medzi vyslaným a prijatým signálom. Takéto modulačné techniky vedú k iným triedam radarov, ako je FMCW radar (frekvenčne modulovaný radar) alebo impulzný radar, ktorý využíva 100% amplitúdovú moduláciu.

Radar s frekvenčne modulovanou kontinuálnou vlnou (FMCW)

FMCW radar (Frequency-Modulated Continuous Wave radar) je špecializovaný radarový systém, ktorý vysiela kontinuálny signál, podobne ako CW radar. Na rozdiel od CW radaru však jeho signál prechádza frekvenčnou alebo fázovou moduláciou. Táto modulácia umožňuje presné časové analýzy prijatých signálov, čím umožňuje určenie vzdialenosti a relatívnej rýchlosti cieľov [14].

Princíp fungovania tohto radaru spočíva v meraní vzdialenosti prostredníctvom porovnávania frekvencie prijímaného signálu s referenčným signálom (obvykle priamo vysielaným signálom), pričom doba trvania modulačnej periódy T je zámerne navrhnutá tak, aby bola podstatne dlhšia než doba šírenia signálu Δt potrebná pre stanovený rozsah merania vzdialenosti [14]. Vzorec pre výpočet vzdialenosti teda môžeme definovať ako:

$$R = \frac{c_0|\Delta t|}{2} = \frac{c_0|\Delta f|}{2\left(\frac{df}{dt}\right)} \tag{3.2}$$

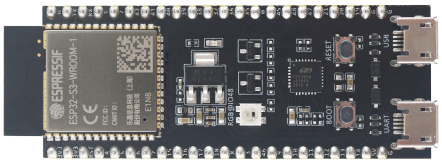
kde rýchlosť svetla c_0 má hodnotu $3 \cdot 10^8$ m/s, pričom meranie vzdialenosti R je založené buď na dobe behu signálu Δt v sekundách, alebo na nameranom rozdiele frekvencií Δf v hertzoch v kombinácii s odchýlkou frekvencie za jednotku času $\frac{df}{dt}$.

Pulzný radar

Pulzný radar vysiela krátke a výkonné impulzy a v tichých intervaloch prijíma odrazené signály. Na rozdiel od kontinuálneho vlnového radaru je vysielač vypnutý pred dokončením merania. Tento typ radaru je charakterizovaný moduláciou radarových impulzov s veľmi krátkym trvaním impulzov (typicky trvanie vysielacieho impulzu $\tau \approx 0,1 \ldots 1\,\mu$s). Medzi vysielacími impulzmi sa nachádzajú veľmi dlhé prestávky, ktoré sa označujú ako čas na príjem signálov (typicky $T \approx 1$ ms). Vzdialenosť odrážajúcich sa objektov sa určuje meraním doby letu (pri pevných radaroch) alebo porovnaním charakteristických zmien Dopplerovho spektra s hodnotami vzdialeností uloženými v databáze (pre radary na rýchlo sa pohybujúcich platformách). Impulzné radary sú väčšinou navrhnuté na meranie na veľké vzdialenosti a prenášajú relatívne vysoký impulzový výkon [14].

3.3 ESP32

ESP32 je výkonný a cenovo dostupný mikrokontrolér od spoločnosti Espressif Systems, ktorý sa vyznačuje nízkou spotrebou energie. Je nástupcom ESP8266, pričom ponúka viac možností a vyšší výkon. Najnovšie modely ESP32 sú vybavené dvojjadrovým 32-bitovým mikrokontrolérom s maximálnou taktovacou frekvenciou 240 MHz. Majú integrovanú podporu Wi-Fi a Bluetooth a disponujú veľkým množstvom GPIO pinov. Taktiež podporujú rôzne komunikačné rozhrania ako I2C, SPI a UART [4]. Príklad mikrokontroléra ESP32 je možné vidieť na obrázku 3.5.



Obr. 3.5: Príklad mikrokontroléra ESP32-S3-WROOM-1 [4].

Porovnanie variant ESP32

Rodina ESP32 zahŕňa široké spektrum modelov, ktoré sú navrhnuté tak, aby vyhovovali rôznym aplikáciám a potrebám. Tieto varianty sa líšia v parametroch ako počet jadier, frekvencia, veľkosť pamäte a podporované komunikačné rozhrania, čo umožňuje vývojárom vybrať najvhodnejší model pre konkrétny projekt. V tabuľke 3.1 sú porovnané hlavné parametre najpoužívanejších modelov.

Parameter	**ESP32**	**ESP32-S3**	**ESP32-C3**	**ESP32-C6**
CPU	Dual-Core	Dual-Core	Single-Core	Single-Core
Frekvencia	240 MHz	240 MHz	160 MHz	160 MHz
SRAM	520 KB	512 KB	400 KB	512 KB
Wi-Fi	802.11	802.11	802.11	802.11ax
Bluetooth	4.2 (LE)	5 (LE)	5 (LE)	5 (LE)
USB	-	USB OTG	-	-
GPIO piny	34	45	22	30

Tabuľka 3.1: Porovnanie variant ESP32 [4].

Medzi novšie a špecializované varianty patrí ESP32-C6, ktorý je prvým SoC (System on Chip) od Espressifu podporujúcim Wi-Fi 6 (2,4 GHz) a Bluetooth 5 (LE). Vďaka tomu predstavuje ideálne riešenie pre moderné IoT produkty vyžadujúce spoľahlivé bezdrôtové pripojenie a vysoký výkon. ESP32-S3 je zase vybavený podporou vektorových inštrukcií, ktoré umožňujú akceleráciu výpočtov pre neurónové siete a spracovanie signálov [4].

Vývojové prostredia

Pre programovanie ESP32 existuje niekoľko vývojových prostredí s rôznou komplexnosťou. Arduino IDE sa vyznačuje intuitívnym rozhraním a širokou komunitnou podporou, čo z neho robí ideálnu voľbu pre začiatočníkov. ESP-IDF od spoločnosti Espressif naopak poskytuje profesionálne nástroje a maximálnu kontrolu nad hardvérom s využitím FreeRTOS. PlatformIO kombinuje jednoduchosť s pokročilými funkciami ako rozšírenie Visual Studio Code a podporuje rôzne frameworky. Pre alternatívne programovacie jazyky je dostupný MicroPython alebo NodeMCU založený na jazyku Lua, ktorý je vhodný najmä pre jednoduchšie IoT aplikácie.

ESP32-CAM

ESP32-CAM je špecializovaná verzia mikrokontroléra ESP32, ktorá má navyše integrovanú kameru a slot na pamäťovú kartu. Keďže využíva mikrokontrolér ESP32, zachováva rovnaké vlastnosti ako iné ESP32 dosky [9]. Jedným z hlavných rozdielov medzi ESP32-CAM a inými ESP32 doskami je, že má k dispozícii menej I/O pinov. To je spôsobené tým, že väčšina pinov je využitá pre integrovaný kamerový modul a slot pre microSD kartu. Príklad ESP32-CAM je zobrazený na obrázku 3.6.

Obr. 3.6: Príklad mikrokontroléra ESP32-CAM [6].

Napriek tomu, že staršie špecifikácie uvádzajú, že ESP32-CAM podporuje iba dva typy kamier (OV2640 a OV7670), v skutočnosti je možné použiť aj ďalšie kamery. Okrem týchto dvoch oficiálne podporovaných kamier, ponúka spoločnosť Espressif repozitár kamier[1], ktoré sú kompatibilné s ESP32-CAM. Ich prehľad, vrátane rozlíšenia a veľkosti objektívu, je uvedený v tabuľke 3.3.

Model	Rozlíšenie (MP)	Veľkosť objektívu
OV2640	1600 x 1200 (2)	1/4"
OV3660	2048 x 1536 (3)	1/5"
OV5640	2592 x 1944 (5)	1/4"
OV7670	640 x 480 (0.3)	1/6"
OV7725	640 x 480 (0.3)	1/4"
NT99141	1280 x 720 (1)	1/4"
GC032A	640 x 480 (0.3)	1/10"
GC0308	640 x 480 (0.3)	1/6.5"
GC2145	1600 x 1200 (2)	1/5"
BF3005	640 x 480 (0.3)	1/4"
BF20A6	640 x 480 (0.3)	1/10"
SC101IOT	1280 x 720 (1)	1/4.2"
SC030IOT	640 x 480 (0.3)	1/6.5"
SC031GS	640 x 480 (0.3)	1/6"

Tabuľka 3.3: Prehľad kamier a ich parametrov

[1]Repozitár kamer, komaptibilných s ESP32: `https://github.com/espressif/esp32-camera`

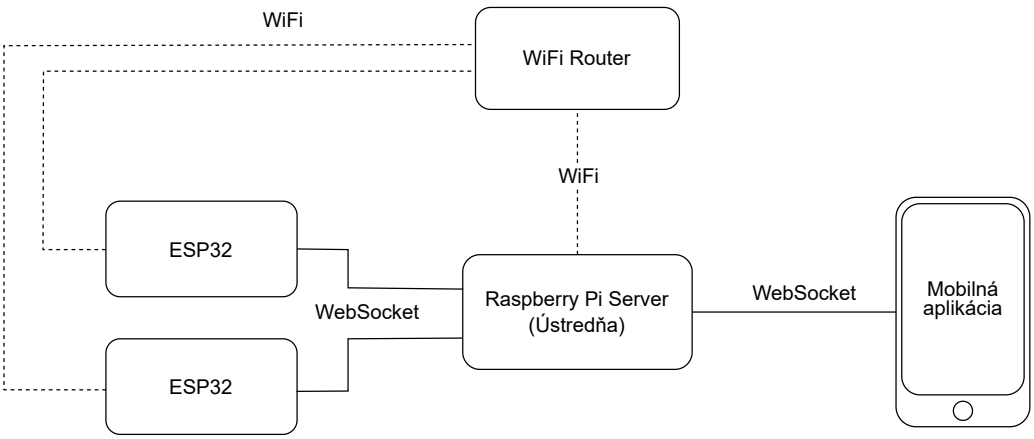
Kapitola 4

Návrh systému

Dôkladný návrh zabezpečovacieho systému je dôležitým krokom pred jeho samotnou implementáciou, pričom je potrebné dobre premyslieť spôsob komunikácie a odosielania dát medzi jednotlivými zariadeniami. Navrhnutý systém musí byť schopný detegovať prítomnosť osôb pomocou senzorických modulov a informáciu o detekcii odoslať na centrálnu jednotku (ústredňu) na ďalšie spracovanie. Centrálna jednotka bude teda v tomto prípade predstavovať server, na ktorý sa jednotlivé ESP32 zariadenia so senzormi pripoja ako klienti. Súčasťou systému je aj mobilná aplikácia, ktorá bude zobrazovať dáta poskytnuté zo senzorov a taktiež bude slúžiť na konfiguráciu a správu senzorov.

4.1 Blokové schéma systému

Obrázok 4.1 znázorňuje blokové schéma navrhnutého zabezpečovacieho systému, ktoré predstavuje jeho celkovú architektúru založenú na mikroprocesoroch ESP32 a centrálnej jednotke Raspberry Pi. Systém pozostáva z dvojice ESP32 modulov, ktoré slúžia na zber údajov zo senzorov a ich následné odosielanie na centrálnu riadiacu jednotku. Tá zabezpečuje spracovanie, ukladanie a ďalšiu distribúciu dát smerom k mobilnej aplikácii, ktorá funguje ako používateľské rozhranie umožňujúce vzdialený prístup k systému, sledovanie živého prenosu z kamier a prijímanie notifikácií o zaznamenaných udalostiach.

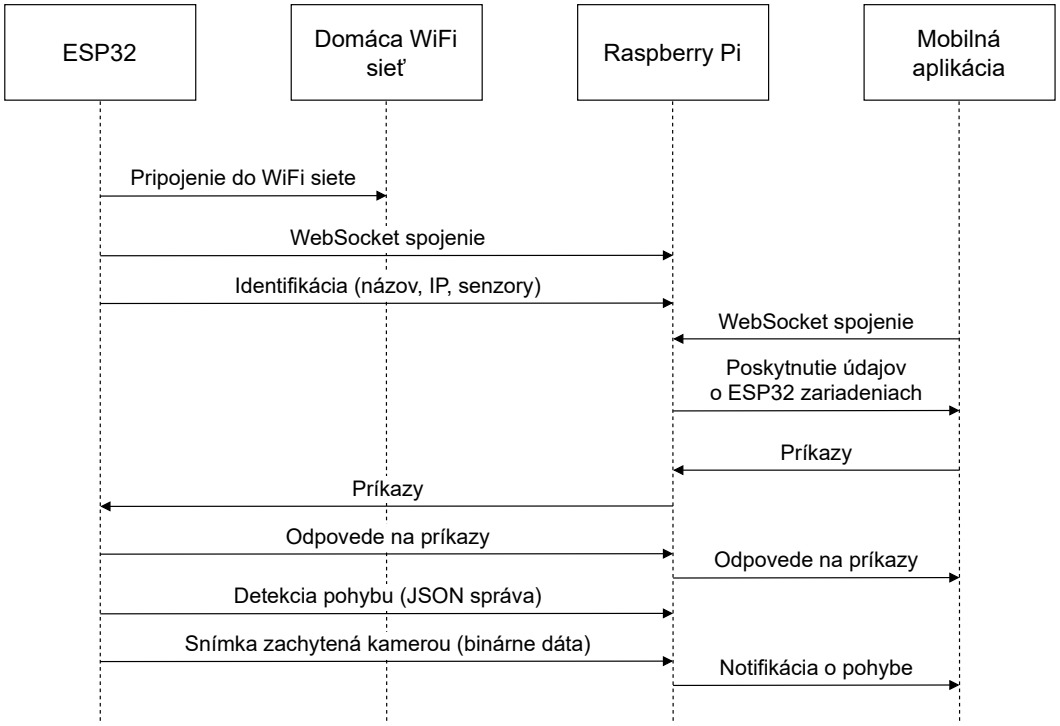


Obr. 4.1: Blokové schéma systému.

4.2 Komunikácia zariadení

Jednotlivé zariadenia v zabezpečovacom systéme budú komunikovať prostredníctvom WebSocket protokolu, čo umožňuje obojsmernú komunikáciu v reálnom čase. Výber tohto protokolu bol motivovaný potrebou minimálnej latencie pri prenose informácií o narušení priestoru a efektívnym prenosom obrazových dát. ESP32 moduly po pripojení do lokálnej Wi-Fi siete nadväzujú spojenie s Raspberry Pi serverom, pričom sa identifikujú svojím jedinečným názvom, IP adresou a zoznamom dostupných senzorov. Následne začnú odosielať dva základné typy dát: JSON správy vo forme štruktúrovaných príkazov a odpovedí a v prípade dostupnosti kamery aj binárne dáta reprezentujúce zachytené snímky.

Mobilná aplikácia bude so serverom komunikovať tiež prostredníctvom WebSocket protokolu, odosielajúc konfiguračné príkazy a požiadavky na živý prenos videa alebo zmenu prevádzkového režimu. Server bude tieto požiadavky smerovať na príslušné ESP32 zariadenia podľa ich identifikátorov. Pri detekcii pohybu by mal senzorický modul odoslať textovú notifikáciu s informáciami o čase a type udalosti, nasledovanú samostatným prenosom zachytenej snímky. Komunikácia medzi zariadeniami je znázornená na sekvenčnom diagrame 4.2.



Obr. 4.2: Sekvenčný diagram komunikácie zariadení.

4.3 Prevádzkové režimy

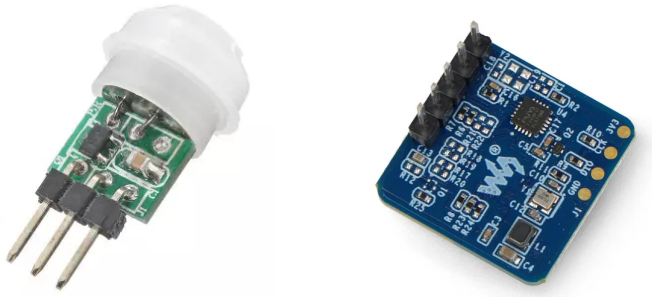
Zabezpečovací systém bude podporovať dva hlavné prevádzkové režimy, ktoré bude možné prepínať podľa aktuálnych potrieb. Servisný režim je určený pre údržbu, testovanie a konfiguráciu systému. V tomto režime je detekcia pohybu deaktivovaná a žiadne automatické upozornenia nie sú generované, čo umožňuje diagnostiku a nastavenie zariadení bez vyvo-

lania falošných poplachov. Naproti tomu režim stráženia aktivuje plnú funkcionalitu zabezpečovacieho systému. V tomto režime je aktívna detekcia pohybu, pri ktorej sú generované automatické upozornenia. Systém bude zachytávať snímky pri detekcii pohybu a odosielať ich do mobilnej aplikácie. Okrem týchto dvoch prevádzkových režimov budú jednotlivé senzorické moduly disponovať aj samostatným konfiguračným režimom, do ktorého vstúpia automaticky pri prvom spustení alebo po vymazaní uložených nastavení.

4.4 Senzorické moduly

Senzorické moduly predstavujú kľúčové jednotky celého zabezpečovacieho systému, pričom ich konštrukcia bude založená na mikrokontroléri ESP32, ktorý je podrobne popísaný v sekcii 3.3. Pre účely tejto práce budem využívať dve zariadenia ESP32. Prvé bude vybavené kamerou OV3660 a PIR senzorom[1] na základnú detekciu prítomnosti. Princíp fungovania tohto senzoru je popísaný v sekcii 3.1. Druhé zariadenie bude obsahovať kameru OV2640 v kombinácii s mmWave senzorom[2], ktorý umožňuje presnejšiu detekciu a zachytenie malých pohybov. Na detekciu využíva technológiu FMCW, ktorá je bližšie popísaná v sekcii 3.2. Obidva tieto senzory sú zobrazené na obrázku 4.3. Ďalšie zariadenia je potom podľa potreby možné jednoducho doplniť.

Keďže ESP32 nemá obrazovku ani klávesnicu, nie je možné ho konfigurovať tradične cez fyzické rozhranie. Z tohto dôvodu bol zvolený prístup, pri ktorom každé zariadenie po prvom spustení automaticky prejde do konfiguračného režimu, v ktorom vytvorí vlastný Wi-Fi prístupový bod. Na tento prístupový bod bude potrebné sa pripojiť pomocou mobilného zariadenia s nainštalovanou riadiacou aplikáciou. Zariadeniu sa tak poskytnú kľúčové parametre – názov zariadenia pre jeho identifikáciu v systéme, prihlasovacie údaje do lokálnej Wi-Fi siete (SSID a heslo) a IP adresa a port Raspberry Pi servera, ku ktorému sa má zariadenie pripojiť. Po prijatí týchto údajov sa ESP32 modul pripojí na špecifikovanú Wi-Fi sieť a nadviaže spojenie so serverom, čím sa stane aktívnou súčasťou zabezpečovacieho systému bez potreby ďalšej manuálnej konfigurácie. Postup pripojenia zariadenia do systému je možné vidieť na sekvenčnom diagrame 4.4.

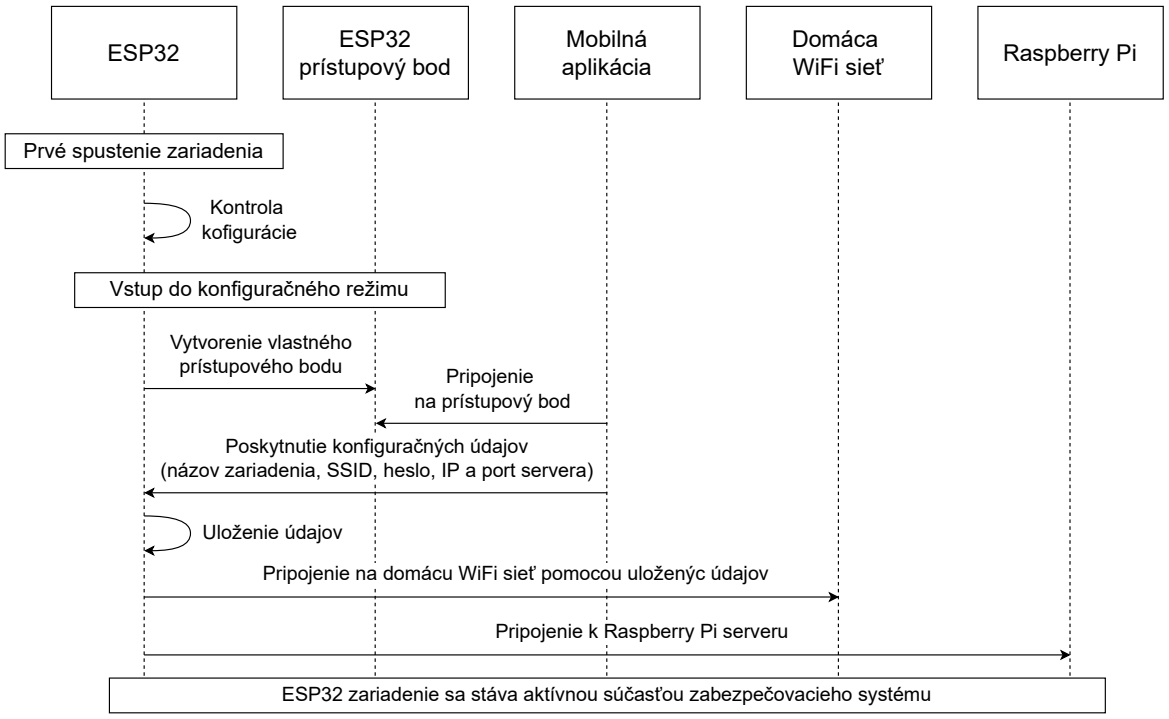


(a) PIR senzor (b) mmWave senzor

Obr. 4.3: Senzory vybrané pre zabezpečovací systém.

[1]Dostupný na: `https://www.gme.sk/v/1508403/sb00312a-1-pir-modul`

[2]Dostupný na: `https://botland.cz/pohybove-senzory/24790-human-micro-motion-detection-mmwave-24ghz-senzor-s3km1110-waveshare-26536-5904422385699.html`



Obr. 4.4: Sekvenčný diagram pripojenia ESP32 zariadenia do systému.

4.5 Centrálna jednotka

Centrálnu jednotku zabezpečovacieho systému bude predstavovať Raspberry Pi server, ktorý zabezpečí komunikáciu medzi senzorickými modulmi a mobilnou aplikáciou. Zvolená jednotka Raspberry Pi 4 Model B[3] bude napájaná prostredníctvom štandardného USB-C adaptéra a pre pripojenie k sieti využije Wi-Fi bezdrôtové pripojenie.

Dôležitým aspektom servera bude jeho schopnosť spracovávať príkazy z mobilnej aplikácie a preposielať ich príslušným ESP32 zariadeniam. Medzi tieto príkazy patria požiadavky na zmenu prevádzkového režimu, spustenie alebo zastavenie živého prenosu videa, zachytenie aktuálnej snímky alebo získanie informácií o zariadení.

[3]Dostupný na: `https://www.raspberrypi.com/products/raspberry-pi-4-model-b/`

Kapitola 5

Implementácia

Implementácia zabezpečovacieho systému pozostáva z troch vzájomne prepojených komponentov. Prvým sú zariadenia ESP32, ktoré slúžia ako hardvérové senzorické moduly zodpovedné za zachytávanie obrazu, detekciu pohybu a prvotné spracovanie údajov. Druhým komponentom je serverová infraštruktúra, prevádzkovaná na Raspberry Pi, ktorá funguje ako centrálny uzol pre správu pripojených zariadení, spracovanie prichádzajúcich dátových tokov a koordináciu celkovej prevádzky systému. Tretím komponentom je mobilná aplikácia, ktorá poskytuje používateľom rozhranie na sledovanie kamerových prenosov, prijímanie upozornení, správu pripojených zariadení a konfiguráciu nastavení systému.

5.1 ESP32 Zariadenia

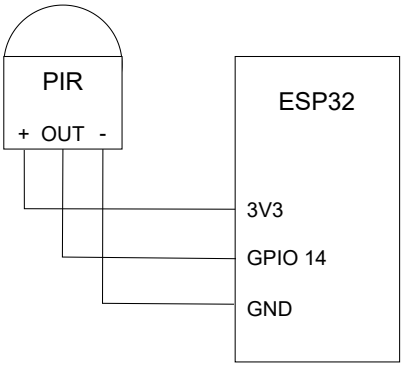
Softvérové riešenie na strane zariadení ESP32 zabezpečuje komunikáciu so serverom pomocou protokolu WebSocket a zároveň umožňuje obojsmernú výmenu informácií – od odosielania živého obrazu z kamery a notifikácií až po prijímanie príkazov zo servera. Riešenie bolo implementované v programovacom jazyku C++ s využitím vývojového prostredia Arduino IDE.

V rámci realizácie boli použité dve samostatné zariadenia ESP32, pričom každé z nich bolo vybavené odlišným typom pohybového senzora. Prvé zariadenie obsahuje PIR detektor, ktorý umožňuje jednoduchú detekciu pohybu. Druhé zariadenie je osadené mmWave senzorom, ktorý, na rozdiel od PIR senzora, pracuje na princípe vysielania a prijímania mikrovlnného signálu. K tomuto senzoru je dostupná technická dokumentácia, z ktorej boli čerpané podrobné informácie o jeho fungovaní a vlastnostiach[1]. Zapojenia oboch typov senzorov k zariadeniu ESP32 sú uvedené v blokových diagramoch 5.1 a 5.2.

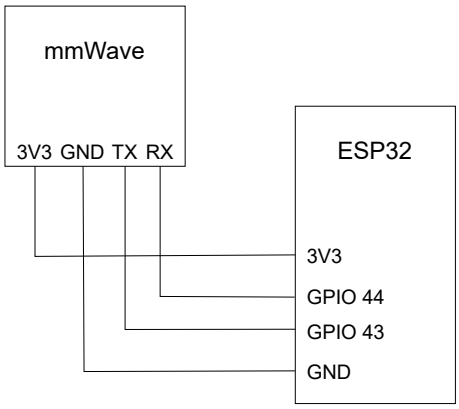
Inicializácia a konfigurácia

Základné konfiguračné hodnoty sú definované v súbore `config.h`. Tento súbor obsahuje definíciu SSID a hesla, ktoré zariadenie použije v prípade, že sa prepne do konfiguračného režimu, kedy vytvorí prístupový bod (Access Point). Okrem toho sú v ňom definované aj ďalšie konštanty, ako piny pre pripojenie senzorov a zoznam senzorov, ktoré zariadenie obsahuje. Tieto informácie sú neskôr použité pri odpovediach na požiadavky zo servera.

[1]Dostupná z: `https://www.waveshare.com/wiki/HMMD_mmWave_Sensor`



Obr. 5.1: Zapojenie PIR senzora na ESP32.



Obr. 5.2: Zapojenie mmWave senzora na ESP32.

Trieda WebSocketHandler

Jadro komunikácie zabezpečuje trieda `WebSocketHandler`, ktorá sa nachádza v hlavičkovom súbore `websocket_handler.h`. Táto trieda je navrhnutá tak, aby abstrahovala všetky činnosti súvisiace s WebSocket komunikáciou, a zároveň ponúka rozhranie pre odosielanie dát, spracovanie príkazov a riadenie živého prenosu z kamery.

Trieda poskytuje metódu `sendNotification`, ktorá slúži na odosielanie štruktúrovanej správy vo formáte JSON na server. Notifikácia obsahuje názov, typ správy, popis, časový údaj a voliteľne príznak, či je súčasťou notifikácie aj obrázok. Táto metóda sa používa pri zachytení pohybu alebo pri potvrdení vykonania príkazu.

Na zabezpečenie prenosu obrazových dát z kamery slúži metóda `handleCameraStream`. K samotnému prenosu obrazu v reálnom čase dochádza len vtedy, ak je aktivovaný režim živého prenosu. V pravidelných intervaloch sa zo senzora získa aktuálny snímok, ktorý je následne odoslaný na server vo forme binárnych dát pomocou funkcie `sendBIN`.

Metóda `sendPong` slúži na odosielanie odpovede na ping signál, ktorý je súčasťou udržiavania spojenia medzi ESP32 a serverom. Táto metóda vytvára JSON správu s typom 'pong', aktuálnym časovým údajom a názvom zariadenia, ktorá potvrdzuje, že zariadenie je aktívne a reaguje na komunikáciu.

Spracovanie príkazov zo servera

Jednou z najdôležitejších funkcií triedy je `handleCommand`, ktorá prijíma JSON správy zo servera, analyzuje ich a vykonáva príkazy. Medzi podporované príkazy patria:

- `getDeviceInfo` – Zariadenie odpovie s informáciami ako názov zariadenia, aktuálna IP adresa a zoznam pripojených senzorov.
- `capturePhoto` – Zariadenie nasníma aktuálny záber z kamery a odošle ho na server.
- `setServiceMode` – Aktivuje alebo deaktivuje servisný režim zariadenia.
- `startStream` / `stopStream` – Zapne alebo vypne režim živého prenosu obrazu.
- `removeDevice` – Vymaže uložené konfiguračné údaje z pamäte a následne sa reštartuje.

Po prvom spustení alebo po odstránení z aplikácie sa zariadenie automaticky prepne do konfiguračného režimu, v ktorom vytvorí vlastný prístupový bod. Používateľ sa k nemu môže pripojiť cez smartfón a pomocou aplikácie zadať prihlasovacie údaje k Wi-Fi sieti, IP adresu a port servera.

Zadané údaje sa následne uložia do trvalej pamäte pomocou knižnice `Preferences`. Po ich uložení sa zariadenie automaticky reštartuje a po opätovnom spustení sa pokúsi pripojiť k zadanej Wi-Fi sieti a nadviazať spojenie so serverom.

Ak je pripojenie úspešné, ESP32 prejde do normálneho (operačného) režimu, v ktorom získava aktuálny čas zo servera cez NTP klienta, udržuje WebSocket pripojenie so serverom, monitoruje pohyb pomocou senzorov a pri detekcii pohybu odosiela upozornenie.

5.2 Centrálna jednotka

Zabezpečovací systém využíva server bežiaci na Raspberry Pi ako centrálny komunikačný uzol. Tento server je implementovaný v jazyku Python v súbore `server.py`. Je navrhnutý ako most (bridge) medzi senzorickými modulmi založenými na ESP32 a mobilnou aplikáciou používateľa. Pre efektívnu komunikáciu v reálnom čase využíva WebSocket protokol. Server je implementovaný ako trieda `WebSocketServer`, ktorá spravuje súčasne dva WebSocket endpointy:

- Na porte 8081, ktorý slúži výhradne pre pripojenie ESP32 zariadení
- Na porte 8080, určený pre pripojenie mobilnej aplikácie

Súčasťou implementácie servera je aj zabezpečenie jeho automatického spustenia pri štarte Raspberry Pi. Server je nakonfigurovaný ako `systemd` služba, ktorá sa automaticky spúšťa pri štarte zariadenia a pripojení k sieti. Vďaka tomu systém funguje automaticky po každom reštarte Raspberry Pi alebo výpadku prúdu, bez potreby ručného zásahu. Pre účely diagnostiky a monitorovania server zaznamenáva všetky operácie a chyby do súboru `server.log`, čo umožňuje spätnú analýzu a riešenie prípadných problémov.

Po pripojení nového ESP32 zariadenia ho server v metóde `handle_esp32_connection` zaregistruje do zoznamu pripojených zariadení a priradí mu jedinečný identifikátor. Následne pošle uvítaciu správu vo formáte JSON. Po nadviazaní spojenia začína medzi zariadením a serverom obojsmerná komunikácia:

- **Správy od ESP32 na server:**
  - **Notifikácie o detekcii pohybu** – JSON správy obsahujúce informácie o udalosti
  - **Obrazové dáta z kamery** – Binárne dáta snímok z kamery po detekcii pohybu
  - **Stavové informácie** – Informácie o stave zariadenia a senzorov
  - **Odpovede na ping** – Potvrdenia aktivity zariadenia (`pong` správy)
- **Príkazy zo servera na ESP32:**
  - **Ping požiadavky** – Kontrola aktivity zariadenia
  - **Prepínanie servisného režimu** – Aktivácia/deaktivácia monitorovania
  - **Požiadavky na snímku** – Vyžiadanie aktuálneho obrazu z kamery
  - **Požiadavky na informácie** – Vyžiadanie konfiguračných údajov zariadenia

Podobným spôsobom funguje aj metóda `handle_app_connection`, ktorá zaobstaráva komunikáciu s mobilnou aplikáciou. Po pripojení aplikácie je klient zaregistrovaný a server mu pošle uvítaciu správu s dostupnými zariadeniami. Následne server spracováva príkazy od aplikácie, aktualizuje vnútorný stav a preposiela požiadavky na pripojené zariadenia.

Spracovanie bezpečnostných upozornení

Pri detekcii pohybu ESP32 zariadenie najskôr zasiela notifikačnú JSON správu s príznakom `hasImage=true` a následne snímku. Server uloží obrazové dáta do súboru v adresári `alerts/images/`. Následne ich zakóduje do formátu base64 a pripojí k pôvodnej notifikácii. Túto kompletnú notifikáciu uloží ako JSON súbor v adresári `alerts/`. Nakoniec odošle notifikáciu s priloženými obrazovými dátami všetkým aktuálne pripojeným mobilným klientom.

Tento mechanizmus zabezpečuje, že žiadne upozornenie nebude stratené, aj keby mobilná aplikácia nebola v danom momente pripojená. Pri každom novom pripojení mobilnej aplikácie server načíta všetky uložené upozornenia a odošle ich klientovi.

Sledovanie dostupnosti zariadení

Server v pravidelných intervaloch odosiela každému pripojenému ESP32 zariadeniu správu typu `ping`. Očakáva, že zariadenie odpovie správou `pong`, čím potvrdí svoju dostupnosť. Každá prijatá odpoveď tohto typu aktualizuje interný čas poslednej aktivity daného zariadenia. Ak server v definovanom časovom limite neobdrží žiadnu odpoveď, predpokladá, že zariadenie je neaktívne alebo došlo k prerušeniu spojenia. V takom prípade server odošle správu mobilnej aplikácii informujúcu o odpojení zariadenia a poslednom čase, kedy bolo zariadenie videné.

5.3 Mobilná aplikácia

Mobilná aplikácia je implementovaná pomocou React Native v spojení s Expo frameworkom, čo umožňuje vývoj pre obe platformy (iOS aj Android) pomocou jednej kódovej základne s využitím jazyka TypeScript. Aplikácia poskytuje podporu len pre anglický jazyk.

WebSocketContext

WebSocketContext je kontext vytvorený pomocou `createContext` funkcie z React knižnice, ktorý slúži ako základný stavebný prvok pre správu stavu pripojenia a komunikácie v celej aplikácii. Slúži na správu pripojenia medzi klientom (aplikáciou) a serverom prostredníctvom WebSocket protokolu a umožňuje ich nepretržitú a obojsmernú komunikáciu. Zapuzdruje všetku potrebnú funkcionalitu súvisiacu s WebSocket pripojením a definuje rozhranie `WebSocketContextType`, ktoré sprístupňuje stav pripojenia, metódy na odosielanie príkazov a prijaté dáta všetkým komponentom aplikácie:

- `isConnected` – Boolean hodnota, ktorá určuje, či je aplikácia pripojená k WebSocket serveru.
- `error` – Obsahuje chybovú správu, ak sa vyskytne problém s pripojením alebo prenosom dát. Stav je nulový, ak nie je žiadna chyba.
- `connectedDevices` – Obsahuje zoznam pripojených ESP32 zariadení a ich informácií

- `imageData` – Predstavuje aktuálny živý obraz z kamery, ktorý sa aktualizuje počas aktívneho živého prenosu.
- `lastCapturedImage` – Uchováva posledný prijatý záber aj po prerušení streamovania, čo umožňuje užívateľovi uložiť tento obrázok aj keď už nie je pripojený k zariadeniu.
- `connect(url: string)` – Funkcia, ktorá inicializuje WebSocket spojenie so zadanou URL adresou. Automaticky upraví adresu, ak neobsahuje protokol alebo port, a nastaví potrebné časovače a stavové premenné.
- `disconnect()` – Funkcia, ktorá bezpečne ukončí WebSocket spojenie, vyčistí všetky stavové premenné a zastáví všetky časovače súvisiace so spojením.
- `sendMessage(type: string, data: any)` – Funkcia na odosielanie správ na server. Správa je formátovaná do štandardizovaného JSON formátu s typom a dátami.
- `getCurrentDeviceInfo()` – Vracia informácie o aktuálne vybranom zariadení.

Proces inicializácie spojenia začína volaním metódy `connect`, ktorej sa predáva IP adresa alebo URL servera. Po zavolaní táto metóda najprv vyčistí všetky existujúce časovače a chybové stavy, ktoré by mohli zostať aktívne z predchádzajúcich pokusov o pripojenie. Následne prichádza pokus o samotné pripojenie k serveru.

V rámci inicializácie spojenia sa tiež registrujú popisovače (handlery) pre všetky dôležité WebSocket udalosti. Popisovač `onopen` sa zavolá pri úspešnom nadviazaní spojenia, `onmessage` spracováva prichádzajúce správy a obrazové dáta, `onerror` zachytáva chyby počas komunikácie a `onclose` riadi správanie systému pri ukončení spojenia.

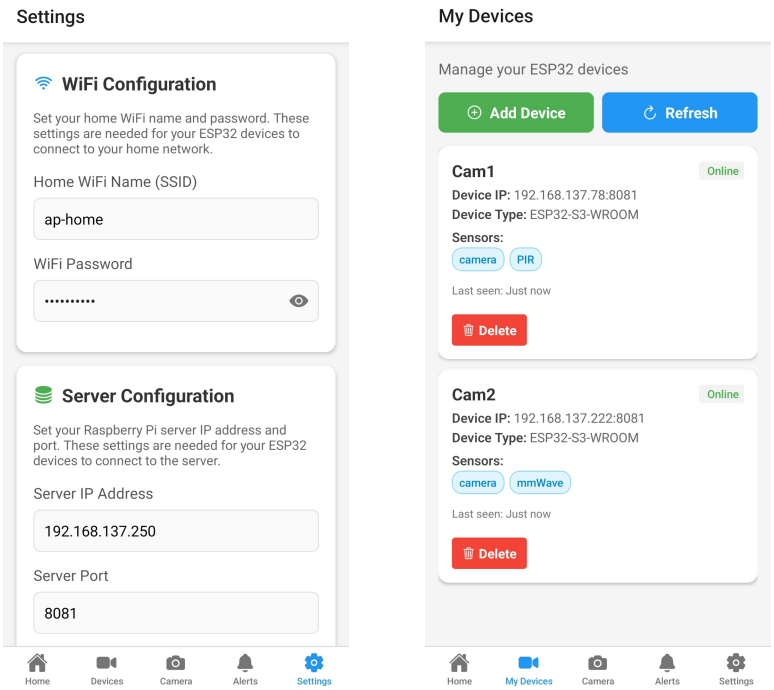
Užívateľské rozhranie

Aplikácia pozostáva z piatich hlavných obrazoviek. Základná konfigurácia systému prebieha na obrazovke **Settings**, kde používateľ zadáva parametre pre pripojenie zariadení do siete, konkrétne Wi-Fi údaje a IP adresu servera. Tieto údaje sa následne využívajú pri procese pridávania zariadení prostredníctvom obrazovky **Devices**, ktorá zabezpečuje inicializáciu a prenos konfiguračných údajov na jednotlivé moduly ESP32. Ukážka týchto obrazoviek je znázornená na obrázku 5.3.

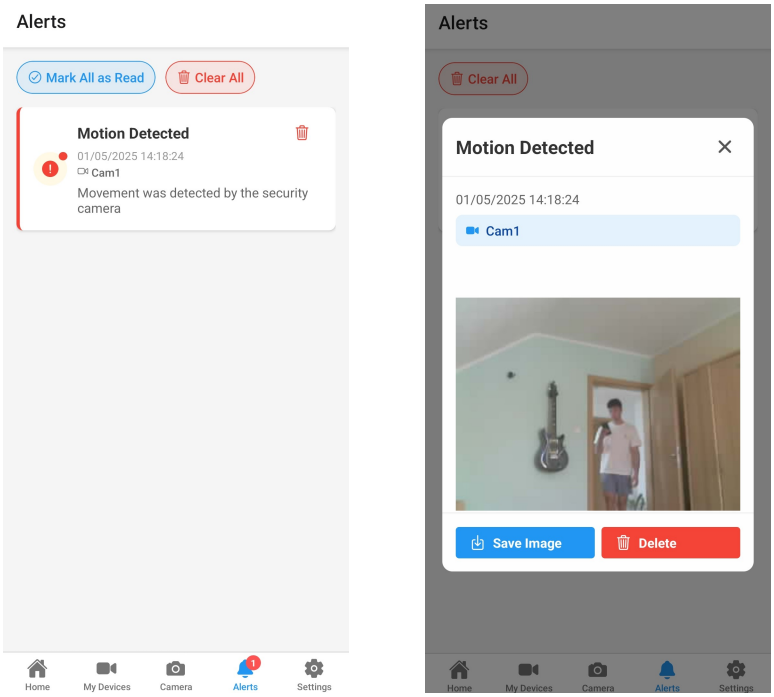
Po úspešnom pridaní zariadení sa používateľ môže pripojiť na obrazovke **Home** na server, od ktorého získa informácie o všetkých dostupných zariadeniach. Tieto informácie zahŕňajú IP adresu zariadenia, jeho typ a zoznam pripojených senzorov.

Následne má používateľ dve hlavné možnosti interakcie so systémom:

- **Sledovanie živého prenosu kamier** – Obrazovka Camera slúži na zobrazovanie obrazových dát prijímaných zo zariadení v reálnom čase. Používateľ má možnosť vybrať konkrétnu kameru a zobraziť jej živý prenos. Okrem samotného náhľadu má možnosť kedykoľvek vytvoriť snímku, ktorá sa následne uloží do galérie zariadenia.
- **Prijímanie upozornení** – Po aktivácii režimu stráženia na obrazovke **Home** začne aplikácia zachytávať upozornenia zo senzorov. Tieto sa ukladajú v pamäti a používateľ k nim má prístup cez obrazovku **Alerts**, kde sa zobrazujú s detailmi ako časová značka a identifikácia zdrojového zariadenia, čo demonštruje obrázok 5.4.



Obr. 5.3: Nastavenie systému a pridávanie zariadení.



Obr. 5.4: Obrazovka Alerts.

Kapitola 6

Testovanie a experimenty

V tejto kapitole sú popísané experimenty zamerané na overenie spoľahlivosti navrhnutého zabezpečovacieho systému vrátane senzorických modulov, servera na Raspberry Pi a mobilnej aplikácie. Testovanie bolo systematicky rozdelené do troch kľúčových oblastí: testovanie konektivity zariadení, spoľahlivosť detekcie pohybu a testovanie užívateľského rozhrania. Cieľom experimentov bolo overiť, či systém stabilne udržiava spojenie, správne odosiela a zobrazuje konfiguračné údaje, spoľahlivo deteguje pohyb vo všetkých prevádzkových režimoch a poskytuje konzistentnú užívateľskú skúsenosť.

6.1 Metodika testovania

Pre zabezpečenie komplexného overenia funkčnosti celého systému bola vytvorená testovacia konfigurácia pozostávajúca z dvoch ESP32 zariadení (konkrétne model ESP32-S3-WROOM-1 s PIR detektorom a ESP32-S3-EYE s mmWave senzorom), Raspberry Pi servera a mobilnej aplikácie s grafickým rozhraním pre nastavenie, správu a monitorovanie zariadení.

Všetky experimenty prebiehali v kontrolovanom domácom prostredí s bežným Wi-Fi pokrytím. Na strane servera boli implementované logy zaznamenávajúce všetky kľúčové udalosti, prichádzajúce aj odchádzajúce správy a diagnostické informácie o stave pripojenia.

Mobilná aplikácia zaznamenávala stavy online/offline pre každé zariadenie, zobrazenie jeho IP adresy, typy senzorov, ako aj notifikácie prijaté v režime stráženia.

6.2 Testovanie konektivity zariadení

Cieľ a postup

Cieľom tejto fázy bolo overiť spoľahlivosť celého komunikačného reťazca zariadení, od úvodnej konfigurácie po bežnú prevádzku. Testoval som nasledujúce kroky:

1. Automatické vytvorenie Wi-Fi prístupového bodu pri štarte ESP32
2. Odoslanie a spracovanie konfiguračných údajov z mobilného zariadenia
3. Opätovné spustenie zariadenia a automatické pripojenie k sieti a serveru
4. Prijatie a zobrazenie identifikačných údajov zariadenia v mobilnej aplikácii
5. Monitorovanie výpadkov a obnovenia spojenia so zariadením

Každý z uvedených testov bol vykonaný desaťkrát na oboch testovaných ESP32 moduloch, pričom testovanie prebiehalo v rôznych časových intervaloch a rôznej vzdialenosti od prístupového bodu.

Výsledky

Po zapnutí zariadenia prebehla inicializácia kamery, senzorov a sériovej komunikácie. Následne zariadenie vstúpilo do konfiguračného režimu, v rámci ktorého aktivovalo Wi-Fi prístupový bod s definovaným SSID a spustilo DHCP službu. Tento proces trval v priemere 4 sekundy, po ktorých bolo zariadenie pripravené na prijatie konfiguračných údajov z mobilnej aplikácie.

Prenos konfiguračných údajov medzi mobilnou aplikáciou a zariadením ESP32 prebiehal prostredníctvom štruktúrovaných JSON správ. Tieto správy obsahovali informácie o požadovanej Wi-Fi sieti, hesle a IP adrese servera a proces od odoslania po prijatie správy trval približne 1 sekundu. Po prijatí údajov ich zariadenie uložilo do internej nevolatilnej pamäte. Tento krok trval približne 0,5 sekundy. Následne ESP32 automaticky iniciovalo softvérový reštart, ktorý trval približne 1 sekundu. Po reštarte zariadenie prešlo do režimu klienta, pričom sa automaticky pripojilo k zadanej Wi-Fi sieti v priemere do 2 sekúnd. Bezprostredne po nadviazaní Wi-Fi spojenia sa zariadenie okamžite pokúsilo nadviazať WebSocket spojenie so serverom, čo trvalo ďalšie 2 sekundy. V 10% prípadov (2 z 20 testov) sa po pripojení mobilného zariadenia k Wi-Fi prístupovému bodu ESP32 nepodarilo úspešne odoslať konfiguračné údaje. Hoci bol prístupový bod aktívny, zariadenie nereagovalo na prichádzajúce požiadavky. Tento problém sa vyriešil až po manuálnom reštarte zariadenia, po ktorom sa konfigurácia vykonala bez problémov.

Po opätovnom zapnutí už nakonfigurovaného zariadenia prebehlo automatické pripojenie k známej Wi-Fi sieti v priemere za 2 sekundy. Následné nadviazanie WebSocket spojenia so serverom trvalo ďalšie 2 sekundy, takže celkovo bol proces opätovného pripojenia dokončený v priemere do 4 sekúnd. Vo všetkých dvadsiatich opakovaniach proces prebehol bezchybne.

Mobilná aplikácia následne v reálnom čase získala informácie zo servera a správne zobrazila dostupné zariadenia spolu s ich stavmi do 3 sekúnd. Tým bola potvrdená funkčnosť komunikačného reťazca – od inicializácie až po úplné začlenenie zariadenia do systému.

Monitorovanie stavu zariadení preukázalo 100% spoľahlivosť pri detekcii výpadkov. Odpojenie zariadenia (simulované odpojením napájania) bolo aplikáciou detegované v čase prekračujúcom nastavený časový limit servera 30 sekúnd. Reálny čas detekcie odpojenia sa pohyboval v rozmedzí 32-38 sekúnd od straty spojenia. Obnovenie spojenia po opätovnom pripojení napájania systém zaznamenal v priemere v priebehu 8 sekúnd, v závislosti od načasovania najbližšieho pravidelného pingu zo servera, ktorý bol odosielaný v intervale každých 15 sekúnd. Zhrnutie výsledkov jednotlivých testov je uvedené v tabuľke 6.1.

Tabuľka 6.1: Výsledky testovania konektivity zariadení.

Testovaný parameter	**Úspešnosť [%]**	**Priemerný čas**
Vytvorenie prístupového bodu	100	4s
Odoslanie a spracovanie konfigurácie	90	7s
Opätovné spustenie zariadenia po konfigurácii	100	4s
Prijatie a zobrazenie identifikačných údajov	100	3s
Monitorovanie stavu	100	35s/8s

6.3 Testovanie detekcie pohybu

Cieľ a postup

Druhá fáza experimentov bola zameraná na overenie spoľahlivosti detekcie pohybu pri použití dvoch odlišných senzorických technológií v reálnom domácom prostredí. Keďže PIR senzor reaguje na zmeny infračerveného žiarenia a mmWave senzor využíva radarovú technológiu, obe riešenia fungujú nezávisle od svetelných podmienok. Z tohto dôvodu neboli vykonávané testy v rôznych úrovniach osvetlenia, ale boli zamerané na kombinovanie nasledujúcich parametrov: rýchlosť pohybu (od rýchlej chôdze po minimálne pohyby), vzdialenosť subjektu od senzora (1m, 3m, 5m a 8m) a prítomnosť prekážok (od priamej viditeľnosti po umiestnenie za zástenou). Do testovacích miestností boli umiestnené dva typy detektorov s rozdielnou charakteristikou – PIR senzor s detekčným dosahom 5 metrov a detekčným uhlom 120°, a pokročilejší mmWave senzor schopný zachytiť aj jemnejšie pohyby do vzdialenosti 8 metrov, avšak s užším detekčným uhlom 60°. Na zabezpečenie štatistickej relevantnosti výsledkov bol každý testovací scenár po deaktivácii servisného režimu realizovaný presne 20-krát.

- **Scenár 1:** Rýchla chôdza v priamej viditeľnosti na vzdialenosť 1-3 metrov
- **Scenár 2:** Rýchla chôdza v priamej viditeľnosti na vzdialenosť 5 metrov
- **Scenár 3:** Rýchla chôdza v priamej viditeľnosti na vzdialenosť 8 metrov
- **Scenár 4:** Pomalá chôdza v priamej viditeľnosti na vzdialenosť 1-3 metrov
- **Scenár 5:** Pomalá chôdza v priamej viditeľnosti na vzdialenosť 5 metrov
- **Scenár 6:** Pomalá chôdza v priamej viditeľnosti na vzdialenosť 8 metrov
- **Scenár 7:** Minimálny pohyb (napr. pohyb ruky) na vzdialenosť 1-3 metrov
- **Scenár 8:** Rýchla chôdza s čiastočným prekrytím na vzdialenosť 3 metrov
- **Scenár 9:** Pomalá chôdza s čiastočným prekrytím na vzdialenosť 3 metrov
- **Scenár 10:** Rýchla chôdza za zástenou na vzdialenosť 3 metrov

Pri každom scenári som simuloval prejdenie osoby cez sledovaný priestor podľa špecifikovaných parametrov a zaznamenal všetky výsledky detekcie.

Výsledky

Pri testovaní detekčných schopností rôznych typov senzorov sa preukázali výrazné rozdiely v ich efektivite v závislosti od testovaných parametrov. PIR senzor dosahoval optimálne výsledky len v ideálnych podmienkach, kde pri priamej viditeľnosti a krátkej vzdialenosti (1-3m) dokázal detegovať pohyb so 100% úspešnosťou. Jeho efektivita však klesala so zväčšujúcou sa vzdialenosťou - pri 5 metroch úspešnosť detekcie klesla na 70% pri rýchlom pohybe a 65% pri pomalej chôdzi. Senzor zároveň vykazoval neschopnosť detegovať pohyb za prekážkami alebo na vzdialenosť presahujúcu 5 metrov, čo potvrdzuje jeho limitácie v reálnych podmienkach. Výrazne lepšie výsledky preukázala mmWave technológia, ktorá nielen dosiahla 100% úspešnosť detekcie v priamej viditeľnosti nezávisle od rýchlosti pohybu, ale

aj 95% úspešnosť pri minimálnych pohyboch v blízkej vzdialenosti. Najvýznamnejšou výhodou mmWave senzora bola jeho schopnosť detegovať pohyb aj za prekážkami, kde dosiahol 90% úspešnosť aj pri vzdialenosti 3 metre za zástenou. Z hľadiska spoľahlivosti PIR senzor nevygeneroval žiadne falošné poplachy. U mmWave senzora neboli zaznamenané falošné poplachy, ale bol pozorovaný jav, kedy po detekcii pohybu a následnom opustení miestnosti senzor ešte približne 20 sekúnd pokračoval v posielaní upozornení, aj keď sa v priestore už nikto nenachádzal. V každom prípade pozitívnej detekcie systém spoľahlivo odoslal notifikáciu nasledovanú snímkou, ktorá bola okamžite dostupná na zobrazenie v mobilnej aplikácii. Zhrnuté výsledky detekčných testov sú uvedené v tabuľke 6.2.

Tabuľka 6.2: Výsledky testovania detekcie pohybu

Testovací scenár	**PIR senzor Úspešnosť [%]**	**mmWave senzor Úspešnosť [%]**
Rýchla chôdza, priama viditeľnosť, 1-3m	100	100
Rýchla chôdza, priama viditeľnosť, 5m	70	100
Rýchla chôdza, priama viditeľnosť, 8m	0	100
Pomalá chôdza, priama viditeľnosť, 1-3m	95	100
Pomalá chôdza, priama viditeľnosť, 5m	65	100
Pomalá chôdza, priama viditeľnosť, 8m	0	95
Minimálny pohyb, priama viditeľnosť, 1-3m	80	95
Rýchla chôdza, čiastočné prekrytie, 3m	85	100
Pomalá chôdza, čiastočné prekrytie, 3m	75	90
Rýchla chôdza, za zástenou, 3m	0	90

6.4 Testovanie užívateľského rozhrania

Cieľ a postup

Tretia fáza experimentov sa zamerala na užívateľské testovanie mobilnej aplikácie s cieľom overiť jej intuitívnosť, odozvu a spoľahlivosť. Do testovania bolo zapojených 8 účastníkov rôzneho veku (22-65 rokov) a s rôznymi skúsenosťami s technológiami. Účastníci dostali sériu úloh:

1. Nastaviť konfiguračné údaje
2. Pridať nové zariadenie do systému
3. Prezerať živý prenos z kamery
4. Zapnúť režim stráženia a reagovať na prichádzajúce upozornenie

Počas testovania boli zaznamenávané časy dokončenia úloh, úspešnosť a subjektívne hodnotenia užívateľskej spokojnosti.

Výsledky

Výsledky užívateľského testovania potvrdili, že navrhnuté rozhranie aplikácie je prevažne intuitívne a použiteľné pre širokú skupinu užívateľov s rôznou úrovňou technických znalostí.

V základnej konfigurácii systému všetci testovaní účastníci úspešne zvládli nastavenie potrebných parametrov, pričom sa preukázal rozdiel v efektivite medzi technicky zdatnejšími užívateľmi (priemerný čas 1,5 minúty) a menej skúsenými (celkový priemer 2 minúty). Pri pridávaní nového zariadenia bola úspešnosť 87,5% (7 z 8 účastníkov), s jedným prípadom, ktorý vyžadoval asistenciu kvôli problémom s pripojením na prístupový bod zariadenia. Túto úlohu účastníci dokončili v priemere za 2 minúty. Najvyššiu mieru intuitívnosti prejavila funkcia živého prenosu z kamery, ktorú dokázali použiť všetci testovaní účastníci bez dodatočnej pomoci. Reakcia na upozornenia o detekcii pohybu bola tiež stopercentne úspešná - všetci účastníci dokázali zobraziť detaily udalosti vrátane zachytenej snímky. Funkcia uloženia snímky do galérie telefónu bola osobitne pozitívne hodnotená 62,5% (5 z 8) účastníkov, čo naznačuje jej užitočnosť v reálnom používaní systému.

Kapitola 7

Záver

Cieľom tejto práce bolo navrhnúť a implementovať domový zabezpečovací systém s využitím platformy ESP32, ktorý by poskytoval spoľahlivú detekciu narušiteľov, jednoduché ovládanie a cenovo dostupné riešenie pre bežných používateľov. Na základe podrobnej analýzy moderných zabezpečovacích technológií bol vytvorený systém pozostávajúci z centrálnej jednotky, senzorických modulov s ESP32 a mobilnej aplikácie, ktorá zabezpečuje používateľské rozhranie.

V rámci teoretickej prípravy som analyzoval rôzne detekčné technológie, pričom osobitná pozornosť bola venovaná PIR senzorom a radarovým senzorom. Experimentálne overenie potvrdilo, že radarové senzory ponúkajú výhody oproti štandardným PIR senzorom, najmä v schopnosti detegovať pohyb za prekážkami a na väčšie vzdialenosti, čím sa potvrdzuje ich vhodnosť pre pokročilé zabezpečovacie systémy.

Navrhnutá architektúra systému sa osvedčila ako spoľahlivé a flexibilné riešenie, pričom komunikácia medzi zariadeniami prostredníctvom WebSocket protokolu umožnila nielen efektívny prenos konfiguračných údajov a notifikácií, ale aj plynulý prenos obrazových dát z kamier. Implementácia konfiguračného režimu pre ESP32 zariadenia eliminovala potrebu fyzických ovládacích prvkov a umožnila jednoduché pridávanie nových modulov do systému priamo cez mobilnú aplikáciu.

Najvýznamnejším prínosom práce je vytvorenie kompletného, modulárne rozšíriteľného zabezpečovacieho systému, ktorý integruje detekčné technológie s používateľsky prívetivým rozhraním za zlomok ceny komerčných riešení. Používateľské testovanie potvrdilo intuitívnosť ovládania a dobrú spoľahlivosť detekcie v rôznych podmienkach, čo poukazuje na potenciál pre reálne nasadenie v domácnostiach.

V budúcom výskume by bolo vhodné zamerať sa na rozšírenie systému o nové typy senzorov, ako napríklad akustické alebo vibračné, ktoré by doplnili existujúce detekčné mechanizmy a zvýšili celkovú spoľahlivosť. Systém by sa mohol ďalej rozšíriť o podporu geolokácie používateľa, čo by umožnilo dynamicky meniť režim zabezpečenia podľa prítomnosti osôb v domácnosti. Ďalším možným vylepšením je integrácia s existujúcimi platformami inteligentných domácností (HomeKit, Google Home, Amazon Alexa), ktorá by rozšírila možnosti automatizácie a zjednodušila ovládanie systému.

Celkové výsledky práce ukazujú, že aj s limitovaným rozpočtom a dostupnými komponentmi je možné vytvoriť zabezpečovací systém, ktorý poskytuje vysokú úroveň bezpečnosti a používateľského komfortu, a zároveň predstavuje pevný základ pre ďalší výskum a zdokonaľovanie v oblasti technológií pre domové zabezpečenie.

Literatúra

[1] Barnard, R. *Intrusion Detection Systems*. 2. vyd. Butterworth-Heinemann, február 1988. 2506 s. ISBN 978-0750694278.

[2] Brooke, M. An Introduction to Thermal CCTV Systems. *CCTV* online, Jún 2020. Dostupné z: https://www.tecservuk.com/blog/an-introduction-to-thermal-cctv-systems/. [cit. 2025-01-16].

[3] Burda, K. *Základy elektronických zabezpečovacích systémů*. 1. vyd. Akademické nakladatelství CERM, 2018. 124 s. ISBN 978-80-7204-967-7.

[4] Espressif Systems. *ESP32* online. 2024. Dostupné z: https://www.espressif.com/. [cit. 2024-12-08].

[5] Gabriele, R. Who Invented the Home Security System. online, Jún 2023. Dostupné z: https://www.safehome.org/security-systems/history/. [cit. 2024-12-11].

[6] Hadex. *M432C ESP32 CAM 2.4GHz WiFi/Bluetooth modul+kamera OV2640* online. 2024. Dostupné z: https://www.hadex.cz/m432c-esp32-cam-24ghz-wifibluetooth-modulkamera-ov2640/. [cit. 2024-12-08].

[7] Hladík, D. *Elektronické zabezpečovací systémy a elektronická požární signalizace* online. SOUE Plzeň, 2010. 36 s. Dostupné z: https://www.souepl.cz/wp-content/ucitele/hladik/opvk2009/Ukazka-skripta/Skripta_ukazka.pdf. [cit. 2024-12-10].

[8] INTERNATIONAL ELECTROTECHNICAL COMMISSION. *IEC 60839-5-1: Alarm and electronic security systems – Part 5-1: Alarm transmission systems – General requirements*. 2014. [cit. 2025-05-04].

[9] Jackson, L. ESP32-CAM: Machine Vision Tips, Camera Guides and Projects. online, August 2021. Dostupné z: https://www.arducam.com/esp32-machine-vision-learning-guide/. [cit. 2024-12-08].

[10] Lenko, F. a Velas, A. POSSIBILITIES OF USING MODERN ACCESS CONTROL SYSTEMS FOR THE PURPOSES OF RESEARCH AND TEACHING AT UNIVERSITY. *Proceedings of CBU in Social Sciences* online, November 2020, zv. 1, s. 146–151. Dostupné z: https://www.researchgate.net/publication/347167613_POSSIBILITIES_OF_USING_MODERN_ACCESS_CONTROL_SYSTEMS_-FOR_THE_PURPOSES_OF_RESEARCH_AND_TEACHING_AT_UNIVERSITY.

[11] Lloyd Security. The History of Security Systems — From Antiquity to Apps. online, Január 2021. Dostupné z: https://lloydsecurity.com/history-security-systems/. [cit. 2024-12-07].

[12] Mlčoch, V. *Bezpečnostní kamerový systém CCTV*. Brno, 2012. 70 s. Bakalárska práca. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií. Vedúci práce Babnič, P. Dostupné z: https://www.vut.cz/www_base/zav_prace_soubor_verejne.php?file_id=53342.

[13] Piza, E.; Welsh, B.; Farrington, D. a Thomas, A. CCTV surveillance for crime prevention: A 40-year systematic review with meta-analysis. *Criminology Public Policy* online, Marec 2019, zv. 18, s. 135–159. Dostupné z: https://doi.org/10.1111/1745-9133.12419. [cit. 2024-11-16].

[14] Radartutorial. *Radartutorial.eu* online. November 1998. Dostupné z: www.radartutorial.eu. [cit. 2024-12-10].

[15] Satori Cyber. Access Control Systems 101: Everything There is to Know About Access Control Systems. online, 2024. Dostupné z: https://satoricyber.com/access-control/access-control-systems-101-everything-there-is-to-know-about-access-control-systems/.

[16] Skolnik, M. I. *Introduction to Radar Systems*. 3. vyd. McGraw-Hill Education, december 2002. 784 s. ISBN 978-0072881387.

[17] Uhlář, J. *Technická ochrana objektů II. Díl - Elektrické zabezpečovací systémy*. Praha Policejní akademie ČR, 2001. 229 s. ISBN 80-7251-076-2.

[18] Veľas, A. *Elektrické zabezpečovacie systémy*. 1. vyd. Žilina: EDIS – vydavateľstvo ŽU, 2010. ISBN 978-80-554-0224-6.

[19] Vo, S. Q.; Quan, P. V. a Bao, B. D. Global optimization methods for enhancing Fresnel lens design in passive infrared systems. *Opt. Continuum*. Optica Publishing Group, Feb 2025, zv. 4, č. 2, s. 409–420. Dostupné z: https://opg.optica.org/optcon/abstract.cfm?URI=optcon-4-2-409.

[20] Webster, J. G. *The Measurement, Instrumentation and Sensors Handbook*. CRC Press, december 1998. 2506 s. ISBN 978-0849383472.

[21] ČESKÝ NORMALIZAČNÍ INSTITUT. *ČSN EN 50131-1: Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 1: Systémové požadavky*. 2. vyd. 2007. [cit. 2024-11-16].

Príloha A

Obsah pamäťového média

`latex/`	Zdrojové súbory technickej správy
`source/`	Zdrojové súbory všetkých komponentov a súbor README.md s návodom na spustenie
`video.mp4`	Video demonštrujúce dosiahnuté výsledky
`xpasti00_bp.pdf`	Text technickej správy