Metody duální verifikace osob pro ESKV

Bc. Pavel Zigmund

Diplomová práce
2024

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektroniky a měření

Akademický rok: 2023/2024

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Pavel Zigmund**
Osobní číslo:	**A22403**
Studijní program:	**N1032A020003 Bezpečnostní technologie, systémy a management**
Specializace:	**Bezpečnostní technologie**
Forma studia:	**Prezenční**
Téma práce:	**Metody duální verifikace osob pro ESKV**
Téma práce anglicky:	**Methods of Person's Dual Verifications for EACS**

Zásady pro vypracování

1. Vypracujte literární rešerši současného stavu ESKV a metod smart funkcí využívaných ve VSS.
2. Navrhněte experimentální sestavu zahrnující ESKV a VSS prvky, kterou propojíte s nepoplachovými prvky.
3. Vytvořte aplikaci a databázi pro verifikaci uživatelů.
4. Navrhněte metodu duální verifikace uživatelů.
5. Ověřte funkčnost navrženého systému.

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management IV. Zlín: Radim Bačuvčík – VeRBuM, 2015. ISBN 978-80-87500-57-6.
2. GEVORGYAN, Menua; MAMIKONYAN, Arsen a BEYELER, Michael. OpenCV 4 with Python Blueprints: Build creative computer vision projects with the latest version of OpenCV 4 and Python 3. Second Edition. Packt Publishing, 2020. ISBN 978-178980-181-1.
3. HOWSE, Joseph; MINICHINO, Joe. Learning OpenCV 4 Computer Vision with Python 3: Get to grips with tools, techniques, and algorithms for computer vision and machine learning. Packt Publishing Ltd, 2020.
4. ČSN EN 60839-11-1. Poplachové a elektronické bezpečnostní systémy – Část 11-1: Elektronické systémy kontroly vstupu – Požadavky na systém a komponenty. Praha: Český normalizační institut, 2014.
5. ČSN EN 60839-11-2. Poplachové a elektronické bezpečnostní systémy – Část 11-2: Elektronické systémy kontroly vstupu – Pokyny pro aplikace. Praha: Český normalizační institut, 2016.

Vedoucí diplomové práce: **Ing. Stanislav Kovář, PhD.**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **20. listopadu 2023**
Termín odevzdání diplomové práce: **28. května 2024**

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

Ing. Milan Navrátil, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 1. prosince 2023

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 22.5.2024

Pavel Zigmund, v.r
podpis studenta

ABSTRAKT

Tato práce se zabývá základními metodami verifikace uživatelů v rámci elektronického systému kontroly vstupu. Teoretická část práce se věnuje vysvětlení základní problematiky bezpečnostních systémů, resp. kamerových systémů a elektronickým systémům kontroly vstupu. Kromě klíčových parametrů jsou uvedeny aktuální trendy v obou oblastech. Praktická část se věnuje tvorbě experimentální sestavy, kombinujícího kamerové systémy a přístupové systémy, včetně popisu použitého hardwarového vybavení a konfiguraci zapojení. Následuje popis implementace jednotlivých funkcí, včetně ověření funkčnosti. V závěru je popsána designová stránka prototypu a testování celé sestavy, stejně jako zhodnocení výsledků diplomové práce.

Klíčová slova: kamerový systém, kontrola vstupu, video detekce, zabezpečení, integrace

ABSTRACT

This work deals with the basic methods of user verification within the electronic access control system. The theoretical part of the work is devoted to the explanation of the basic issue of security systems, or camera systems and electronic access control systems. In addition to key parameters, current trends in both areas are presented. The practical part is devoted to the creation of an experimental set-up, combining camera systems and access systems, including a description of the hardware equipment used and the connection configuration. The following is a description of the implementation of individual functions, including functionality verification. In the conclusion, the design side of the prototype and the testing of the entire assembly are described, as well as the evaluation of the results of the thesis.

Keywords: camera system, access control, video detection, security, integration

Děkuji vedoucímu mé diplomové práce Ing. Stanislavu Kováři, Ph.D za přínosné rady, ochotu a trpělivost při konzultacích. Dále děkuji Ing. Hynku Rafajovi za pomoc s 3D návrhem a následným tiskem krabičky pro má zařízení. Děkuji své rodině za podporu v průběhu celého studia.

OBSAH

ÚVOD

V dnešní době je bezpečnost v oblasti řízení přístupu do chráněných prostor a objektů. Hlavním bodem zájmů nejen pro organizace ale také pro různé instituce. S rostoucím výskytem hrozeb a také s požadavky na zefektivnění a zlepšení zabezpečení vzniká potřeba vyvíjet a implementovat pokročilejší systémy kontroly vstupu. Tyto systémy využívají moderní technologie k ověření a identifikaci uživatelů před udělením nebo zamítnutím přístupu do chráněného prostoru. Tato práce se zaměřuje na problematiku duální verifikace osob v systémech ESKV (Elektronický systém kontroly vstupu) pomocí kombinace různých metod jako je identifikační karta, biometrické údaje spolu s osobním přístupovým heslem. Duální verifikace zahrnuje ověření identity uživatele pomocí dvou nezávislých metod. To zvyšuje spolehlivost, a hlavně bezpečnost celého systému kontroly vstupu. Cílem této práce je navržení experimentální sestavy, která bude kombinovat různé metody přístupu. Sestavu bude možné kombinovat s aplikací pro detekci obličeje, se základním rozpoznáním obličeje podle naučených vzorů. Teoretická část práce se zabývá rešerší současného stavu ESKV a funkcí, které nabízí systémy kamerového dohledu (VSS). Praktická část se věnuje výběru komponentů pro experimentální sestavu, softwarovou implementaci a propojení jednotlivých komponent do funkčního celku. Následně je provedeno ověření funkce experimentální sestavy. Následně jsou navrženy body, ve kterých zařízení fungovalo spolehlivě a také body, které mohou být použity při případném budoucím vylepšení experimentální sestavy.

I. TEORETICKÁ ČÁST

1 VIDEO SURVEILLANCE SYSTEM

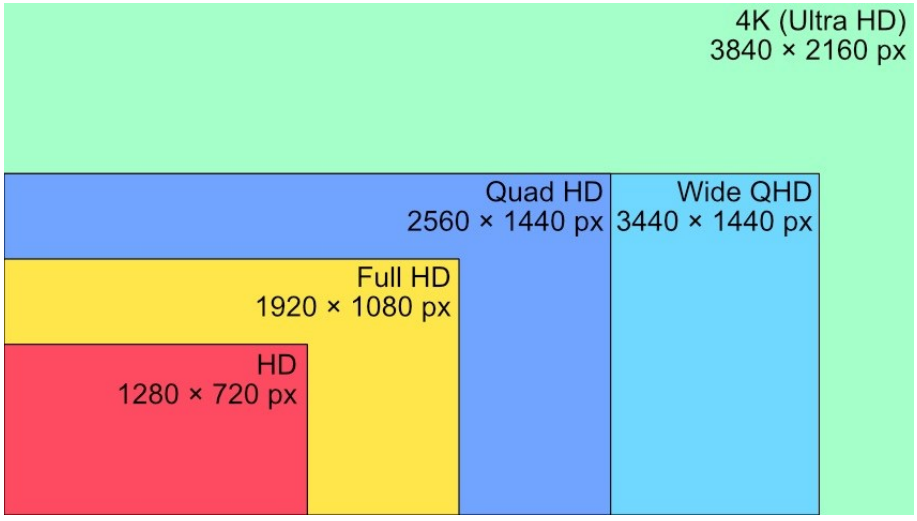
1.1 Základní parametry kamer

Mezi základní parametry kamer, které jsou důležité při jejich porovnání a výběru patří:

- Rozlišení – počet obrazových bodů výška (V) x šířka (Š)
- Citlivost – světelné podmínky záznamu
- Objektiv – přiblížení, zorné pole
- Rychlost snímání – počet snímků
- Komprese videa – ztrátová, bezztrátová

1.1.1 Rozlišení

Jedná se o parametr, který udává počet pixelů, které je kamera schopna zachytit a zpracovat, čím je hodnota větší, tím je obraz detailnější a kvalitnější. Nejběžnější dnes rozšířené rozlišení u kamer je SD – Standart Definition běžně označován jako 480p. Jedná se o rozlišení použité u starších a levnějších zařízení, kde není kladen důraz na vysokou kvalitu pořizovaného záznamu – kamera v průchodu apod. Dalším zástupcem je rozlišení označované jako HD – High Definition. Typicky se jedná o rozlišení 720p (1280x720 px) popřípadě 1080p, kdy se jedná u Full HD obraz s rozlišením 1920x1080 px. Další dnes už pomalu převládající rozlišení je UHD – Ultra HD, jedná se o video ve velmi vysokém rozlišení označovaném jako 4K, 3840x2160 – jedná se o čtyřnásobný počet pixelů oproti Full HD. [1]



Obrázek 1. Porovnání rozlišení [2]

1.1.2 Citlivost

Udává schopnost kamery, resp. objektivu, zachytávat obraz za různých světelných podmínek, vysoká citlivost dokáže zachytit kvalitní a detailní obraz i za velmi špatných světelných podmínek, naopak nízká citlivost povede k nízké kvalitě, rozmazání a šumu v obraze. Světelnost můžeme ovlivnit zvolením vhodné apertury, jako je objektiv s clonou, která může regulovat množství světlat dopadajícího na světlo citlivý prvek – senzor. Dále je citlivost samotného senzoru ovlivněna technologií použitou pro zhotovení senzoru samotného, kdy moderní senzory využívají mimo jiné zpětné osvětlení snímače, kdy dochází k odrazu přijatého světla za účele zvýšení světelnosti snímku. V případech, kdy není možné zvýšit světelnost snímku pomocí externího zdroje světla je možné zvýšit světlost snímku pomocí digitální techniky, toto zesvětlení scény vede ke zvýraznění šumu samotného senzoru, a proto senzory s nízkým vlastním šumem jsou používané tam, kde se předpokládá, že budou použity při zhoršených světelných podmínkách. V opačném případě, by mohla výsledná scéna být překryta šumem. [3]

1.1.3 Objektiv

Hlavním parametrem u objektivů je ohnisková vzdálenost, která je udávána v mm, kratší vzdálenost znamená širší zorné pole zachyceného obrazu, naopak větší vzdálenost se používá pro objektivy s funkcí přiblížení – zoom. Kromě toho může být objektiv vybaven manuálním nebo automatickým ostřením obrazu, které slouží pro zaostření požadovaného objektu, který je předmětem zájmu – typicky příklad na fotografii kdy je osoba v popředí krásně ostrá a pozadí za ní je rozostřené. Další funkcí je automatická stabilizace obrazu, která se stará o minimalizaci rozmazání obrazu z důvodu pohybu nebo třesu snímacího zařízení. Kromě samotných funkcí je také důležitý způsob upevnění objektivu na těle zařízení. Montáž může být univerzální, pro několik typů zařízení a objektivů, popřípadě atypická, kdy je omezené množství kompatibilních objektivů pro dané zařízení – speciální případy, potažmo restrikce ze strany výrobce. [4]

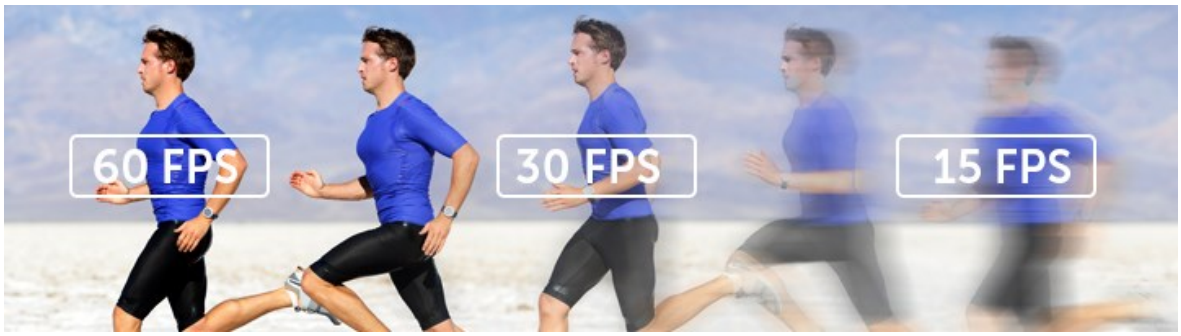
Obrázek 2. Rozdíl mezi ohniskovými vzdálenostmi [5]

1.1.4 Rychlost snímání

Rychlost snímání neboli počet snímků za vteřinu FPS (Frame per Second) je důležitý parametr, který uvádí počet snímků, které jsou potřeba pro trvání videa přehrávaného normální rychlostí po dobu jedné vteřiny. Počet snímků se nejčastěji pohybuje od 15 do 120, ale vyšší hodnoty nejsou výjimkou. Pro běžné bezpečnostní kamery se rychlost pohybuje mezi 15 a 30 snímky.

Nižší počet snímků vede k trhání a neostrosti videa během dynamických scén – pohybu, kde se pohyb zdá trhaný až poskakující, to je dáno velkým rozdílem pozic daného objektu mezi snímky.

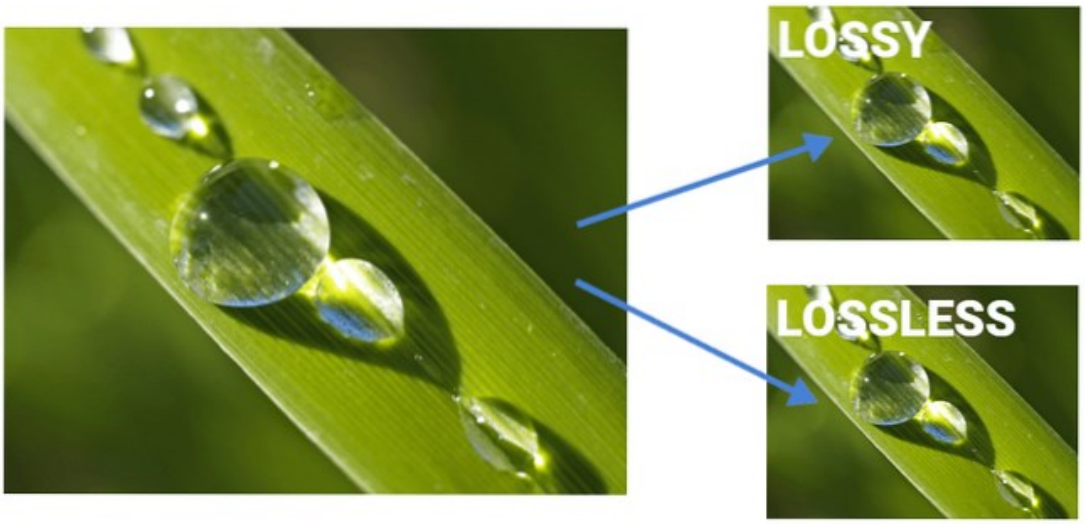
Při vyšší snímkovací frekvenci je dynamický pohyb při přehrávání plynulý a detailnější. Nevýhodou je ovšem větší výpočetní náročnost na zpracování obrazu a také náročnost na kapacitu uložiště, kdy video s 15 FPS při porovnání s videem s 30 FPS při stejném rozlišení a barevné hloubce bude mít téměř poloviční velikost při stejné délce. Tento negativní dopad lze řešit pomocí komprese videa, ale za cenu vyšších požadavků na výkon. [6]



Obrázek 3. Porovnání rychlosti snímání [7]

1.1.5 Komprese

Existuje několik různých typů kompresních algoritmů, jejichž společným cílem je zredukovat velikost, kterou daná data zabírají. Hlavní dělení kompresních algoritmů je na ztrátové a bezztrátové algoritmy. Bezztrátové algoritmy, jak jejich název napovídá, pracují tak aby nedocházelo ke snížení kvality vstupních dat. U ztrátové komprese je upřednostňována menší velikost na úkor kvality dat. Ztrátové algoritmy mohou pracovat například na principech průměrování, nebo redukcí barevné hloubky, a tedy snížením použitelných barev v obraze. Při redukci z 16 bit barevné hloubky, na 8 bit je rozdíl v počtu barev 281 475 miliard vs 16,77 milionů barev. [8]



Obrázek 4. Příklad ztrátové a bezztrátové komprese obrazu [9]

1.2 Kamery a jejich funkce

V této kapitole se čtenář seznámí s aktuálním stavem kamerových systémů, inteligentních funkcí a technologií které jsou při jejich implementaci použity. V současné době lze na poli bezpečnostních kamer pozorovat rostoucí využívání moderních technologií, jako jsou kvalitnější optické snímače s vyšším rozlišením, spolu s používáním sofistikovaných softwarových funkcí, které umožnují mimo jiné vylepšení obrazu, redukci šumu nebo rozšíření obrazu o zajímavé údaje v rámci rozšířené reality (AR).

1.2.1 Aktuální stav

V dnešní době kamery disponují celou řadou smart funkcí, které umožnují automatizaci v rámci dohledových center, proto odpadá nutnost několika pracovníků sledujících několik monitorů současně. V dnešní době postačí jedna osoba ovládající SW spojený s analytickými funkcemi, které přepínají kamery podle toho, jestli se na nich děje aktivační událost. Typickým příkladem může být postupné cyklické přepínaní mezi kamerami, kdy v případě detekce pohybu/narušitele/, nebo jiné události dojde k přenesení dané kamery s událostí do popředí a ostatní jsou upozaděny. Než dojde k ukončení dané situace, nebo nevznikne situace nová na jiné kameře. V tom případě jsou všechny kamery s událostí přeneseny do popředí, aby daná situace měla dostatek pozornosti – není potřeba věnovat pozornost kamerám kde se nic neděje a zároveň je vhodné poukazovat na kamery se spuštěným alarmem. [10]

1.2.2 Smart funkce VSS

Detekce pohybu – tato funkce umožnuje spuštění dané rutiny v případě, že je v obraze detekován pohyb. Základním principem detekce pohybu je vytvoření statického obrazu, který je použit jako šablona a vůči ní je porovnáván živý obraz (video). V případě, že je v obraze změna oproti šabloně – byl detekován pohyb, moderní kamery umožnují nastavovat velikost změny pro detekci pohybu. Díky tomu je možně minimalizovat množství falešných poplachů na minimum, také je možné nastavit parametry tak, aby v obraze detekoval pohyb člověka – změna musí být větší a poměrově je lidské tělo vyšší než širší.

Detekce obličeje (face recognition) – funkce, která vyhledává specifické prvky v daném uspořádání v obraze, v případě obličeje mezi hlavní znaky, které se hledají patří: oči, nos, ústa a jejich vzájemná vzdálenost. Kromě toho je možné detekovat smích. Možnosti detekce jsou závislé na komplexnosti modelu, čím komplexnější model tím vyšší přesnost a menší chybovost při detekci.

Noční vidění – umožnuje použití kamer při zhoršených světelných podmínkách, kdy je snímaný prostor přisvícený infračerveným světlem. Díky tomu se prostor na první pohled jeví jako temný, ale na obrazu kamery dojde pouze ke přechodu z barevného obrazu na stupně šedi.

Funkce virtuálního plotu (geofencing) – jedná se o možnost vztyčit virtuální bariéru ve snímaném prostoru, kdy je v tomto prostoru spuštěna detekce pohybu. Tato kombinace slouží pro detekování pohybu v „zakázané“ oblasti, ale nedetekuje jej jinde – např. kamera

snímající prostor před domem s přesahem na silnici, budeme detekovat pohyb na pozemku a ignorovat pohyb na silnici – redukce planých poplachů ve spojení s tím, že není potřeba nahrávat celou dobu, ale postačuje jen nějaký úsek před detekcí událostí, během ní a nějakou dobu po.

Možnost vzdáleného ovládání (Tilt, Pan, Zoom) – umožnuje ruční nebo automatické natáčení kamery v prostoru a přiblížení obrazu bez ztráty kvality a tím zvětšit plochu snímanou kamerou. Díky tomu je možnost zredukovat potřebné množství kamer a popřípadě kameru natočit tak, aby zachycovala konkrétní situaci. [10]

1.2.3 Budoucí vývoj

Do budoucna se dá předpokládat, že kamerové systémy budou doplněny o další smart funkce ve spojení s rostoucím využitím umělé inteligence (AI). Již nyní umožňují kamery detekovat různé typy chování, jako poflakování, ztrátu nebo zahození předmětu. Tyto funkce by mohly být propojeny napříč několika nezávislými kamerovými systémy a vyhodnocovat tak potenciálně nežádoucí chování. Mimo jiné, může být propojeno s docházkovými systémy – analytika pracovní výkonosti a možnosti optimalizace výkonu pomocí detekce a následné redukce prostojů. [11]

2 ELEKLTRONICKÉ SYSTÉMY KONTROLY VSTUPU

Jedná se o zařízení nebo systém, který slouží pro monitorování a řízení přístupu v dané oblasti nebo prostoru. Tyto systémy využívají různé elektronické zařízení, jako jsou čtečky ID karet, klávesnice nebo biometrické snímače.

2.1 Přístupové systémy

Přístupové systémy využívají technologie pro řízení, monitorování a regulaci přístupu do určitých prostor nebo k datům. K tomuto účelu můžeme přístupové systémy klasifikovat do dvou kategorií. První jsou fyzické systémy, kdy řízení přístupu probíhá pomocí fyzického klíče, který má oprávněná osoba k dispozici a na jehož základě je umožněn přístup do dané oblasti nebo k datům. Tato kategorie je v rámci diplomové práce méně podstatná, a proto se více zaměřuje na druhou kategorii. Tou je kategorie elektronických přístupových systémů, které jsou založeny na propojení několika dílčích částí jako elektronické zámky, klávesnice, čtečky karet, ať už kontaktní nebo bezkontaktní a autentizace pomocí biometrických údajů. Mnohdy jsou tyto systémy vícenásobné, kdy je potřeba splnit více podmínek pro vstup – vstupní karta spolu s uživatelským kódem. [12], [13]

2.1.1 Přístupový bod

Jedná se o místa, které jsou v přímém kontaktu s uživateli a případnými narušiteli systému vstupu. Umožnuje kontrolovaný přístup do systému – prostoru. Nejčastěji se jedná o dveře nebo brány vybavené elektricky ovládaným zámkem / mechanismem, tento zámek může být integrován do dveří jíž z výroby spolu se zařízením pro udělení přístupu – biometrická čtečka otisků prstů, klávesnice pro zadání kódu, popřípadě jiné používané zařízení. Druhou variantou jsou dveře, kde možnost elektrického ovládání byla doplněna dodatečně pomocí vložky zámku s potřebným elektrickým zařízením, které je nejčastěji propojeno s nějakou formou řídící jednotky, která se stará o řízení zámku podle vnitřního programu. [12], [13]

2.1.2 Identifikační prvky

Identifikační prvky jsou zařízení, která umožnují uživateli prokázat oprávněnost na vstup do systému – prostoru. Nejběžnější prvky jsou přístupová klávesnice, která slouží pro zadání přístupového kódu, který může být pro každého uživatele unikátní. V případě nižšího požadavku na zabezpečení, může být kód sdílený mezi více uživatelů. Tam kde jsou požadavky na zabezpečení větší je klasická klávesnice doplněna o čtečku identifikačních karet, případně

o čtečku otisků prstů. Tyto čtečky mohou samotnou klávesnici úplně nahradit, kromě nich se můžeme v praxi setkat se zařízeními na čtení krevního řečiště, kamerového rozpoznáni obličeje a dalšími zařízeními pro rozpoznání biometrických znaků uživatelů systému. [12], [13]

2.1.3 Úrovně ESKV

Jednotliví uživatelé mohou získat několik různých úrovní oprávnění, které ovlivňují, v jakém rozsahu a četnosti jim bude umožněn nebo znemožněn přístup do dané oblasti. Z pravidla se jedná o úrovně pro správu daného zařízení, tato úroveň je mnohdy označována jako servisní – umožnuje dělat zásahy do systému v plném rozsahu. Další je úroveň pro správu uživatelů, ta umožnuje upravovat jednotlivé uživatele, nastavovat jim oprávnění a podobně. Touto úrovní disponují vedoucí pracovníci, kteří mají na starosti hlavní řízení. Poté existují jednotlivé uživatelské úrovně tak, aby nebylo zapotřebí vytvářet vlastní úroveň pro každého zaměstnance, ale jsou vytvořeny např. podle pracovního zařazení. Úrovně jsou řazeny hierarchicky, od nejnižší po nejvyšší, kdy každá úroveň nad nejnižší umožnuje to, co úroveň pod ní a přidává něco navíc. Může také některá práva odebrat nebo je jinak modifikovat. [12], [13]

Elektronický systém kontroly vstupu, nabízí kromě řízení přístupu oprávněným osobám také monitorování jejich vstupu v reálné čase. Může sloužit jako náhrada systému jednotného klíče, kdy je klasická zámková vložka nahrazena elektronickou. Nejčastěji pomocí čipů nebo čteček otisků prstů. Systém může kombinovat řízení přístupu s docházkovým systémem, kdy je zaznamenána aktivita jako vstup do místnosti nebo její opuštění. Z těchto údajů lze vytvořit docházku za dané období – nejčastěji měsíční, kdy uživateli odpadá nutnost používat externí docházkový systém pro evidenci příchodů a odchodů na pracoviště. Kromě toho tyto systémy umožnují vytváření grafů návštěvnosti nebo vytíženosti jednotlivých vstupů a místností. [12], [13]

2.1.4 Současný stav

Současné systémy nabízejí několik různých způsobů ověření nároku uživatele na vstup do chráněného prostoru. Nejběžnější jsou čtečky magnetických pásků, různé technologie čipových karet jako RFID, NFC a podobně. Kromě externích čipů se rozšiřuje možnost používat mobilní telefon jako přístupové zařízení, kdy odpadá potřeba mít nějaký další identifikační prvek. Kromě toho se také používá biometrické rozpoznání, nejčastěji pomocí otisku prstů,

ve více zabezpečených provozech se vyskytují i čtečky umožňující snímat obraz krevního řečiště, popřípadě rozpoznání na základě snímání sítnice oka. Kromě jedné možnosti ověření uživatele se používá více faktorové ověření, kdy je potřeba splnit dva nebo více způsobů přihlášení – čipová karta v kombinaci s otiskem prstu nebo číselným heslem. Kromě přihlášení umožnují komerční systémy také možnost centrálního řízení jednotlivých zařízení od stejného výrobce případně SW integraci napříč několika zařízeními od různých výrobců. Kromě toho nabízí některé systémy i analytické nástroje, které lze spouštět nad jednotlivými daty a s jejich pomocí analyzovat situaci napříč systémy, případně podle rozpoznaných vzorů detekovat pokus o narušení v jeho počátku. [12], [13]

2.1.5 Identifikace a Autentizace

V elektronických systémech kontroly vstupu je důležité rozlišovat mezi identifikací a autentizací uživatele. Identifikace je proces, při kterém dochází k rozpoznání uživatele nebo jiné entity na základě poskytnutých údajů od uživatele. Mezi identifikační prvky se řadí různé identifikační karty jako RFID či karty s magnetickým proužkem. Biometrické čtečky mohou být také použity pro identifikaci.

Autentizace slouží pro ověření totožnosti, kterou se uživatel nebo jiná entita identifikovali. Mezi autentizační zařízení, patří mimo jiné uživatelské PIN kódy a biometrická data. Tato data jsou uložena v databázi a je vůči nim provedeno porovnání. Nejčastěji se autentizace vyskytuje v rámci dvou nebo více faktorového ověření, kdy se kombinují identifikační a autentizační metody dohromady tak, aby mohlo být zaručeno jednoznačného udělení nebo odmítnutí přístupu do chráněného prostoru. [12], [13]

2.2 Otisky prstu

Jedná se o jedinečné obrazce vzniklé z papilárních linií nazývaných markanty, tyto markanty jsou unikátní i pro jednovaječné dvojčata, které je mají rozdílné – je tedy možné je pomocí nich rozlišit. Vědní obor zabývající se otisky prstu se nazývá Daktyloskopie.

2.2.1 Typy obrazců papilárních linií

Papilární linie a vzory, které tvoří, se u lidí začínají vyvíjet již v děloze a zůstávají neměnné po celou dobu života, až na případy, kdy dojde k fyzickému poškození tkání vlivem úrazu nebo nemoci. Obrazce se obecně dělí do třech typů: obloukovité,

obloučkovité a smyčkovité. Toto základní dělení má několik podskupin, do kterých se řádí různé tvary a jejich typy. [14]

Oblouček – nejjednodušší tvar, linie mírně zakřivené do oblouku, probíhají přes celé bříško.

Stranový oblouček – podobný jako oblouček, ve středu navíc obsahuje triradius – trojcípou hvězdu, podobná znaku Δ

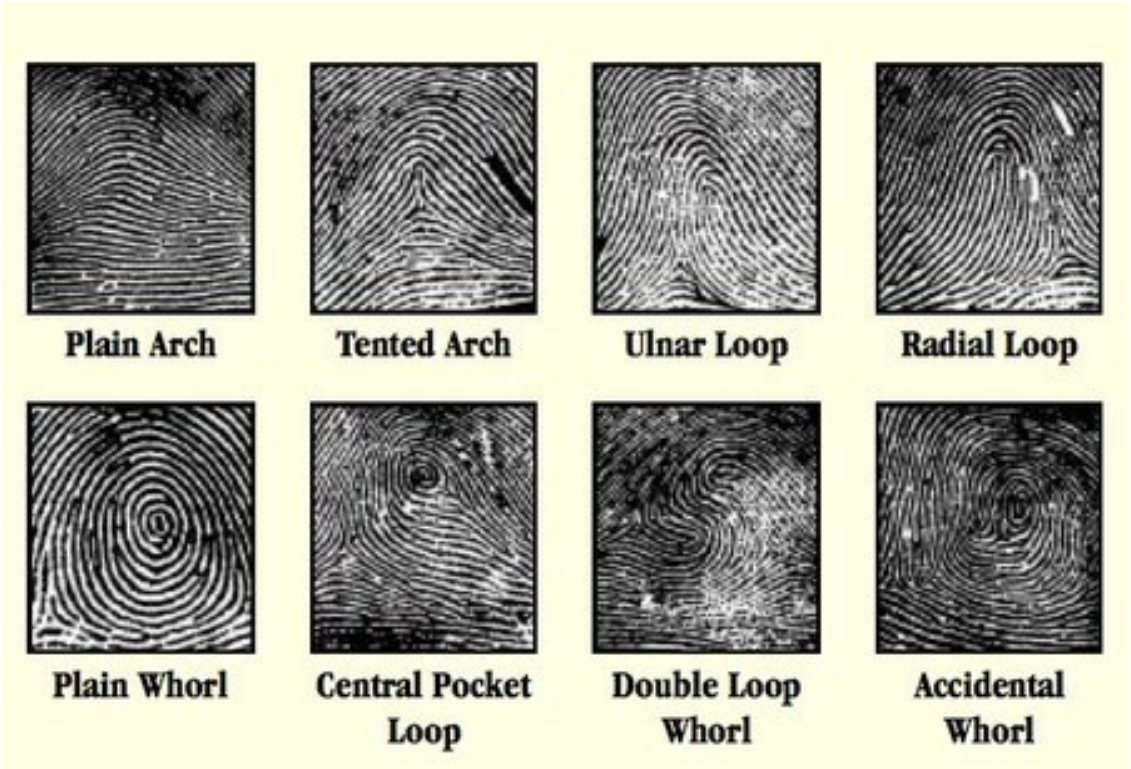
Smyčka – jeden tridius, smyčka se točí ostře kolem jednoho bodu, zbylá část tvořena paralelními liniemi, ta část, kde se otáčejí – **hlava** a část, kde vybíhají – **ocas.** Dále se dělí na **ulnární** – otevřené směrem k malíčku nebo **radiální** – otevřené k palci.

Vír – ohraničen dvěma tradiusy, linie probíhají v kruzích, elipsách nebo spirálově kolem jádra.

Centrální jádro – typicky vír uzavřený do systému linií která tvoří kuličku.

Laterální jádro – dvě do sebe zaklíněné smyčky, obě končící na stejné straně prstu.

Dvoj smyčka – stejně jako laterální jádro, jen smyčky končí na opačných stranách prstu.



Obrázek 5. Základní vzory papilárních linií [15]

2.2.2 Metody snímání

Historicky se otisky prstů získávaly pomocí inkoustu a karty. Inkoust se nanesl na otisky a poté se přenesl jejich obraz na papír. Tato metoda byla nejrozšířenější, až do doby, kdy nastoupily moderní snímací technologie, které umožnují rychlejší a přesnější identifikaci i z neúplných otisků – částečný otisk. Moderní snímače pracují na různých principech, jako optické porovnání, kapacitní nebo za pomoci ultrazvuku.

Optické snímače – zaznamená se obraz otisku prstu. Tento obraz je uložen, a následně je použit při porovnaní s dalšími snímky (starší uložený otisk vs. nový obraz ze snímače). [18]

Kapacitní snímače – není zde přímo snímán obraz prstu, ale dochází k vytvoření 3D obrazu papilárních linií při přiložení prstu na snímač. Díky různé výšce papilár dochází ke vzniku rozdílné kapacity mezi prstem a snímačem (princip kondenzátoru), z těchto rozdílu je vytvořen 3D model který je následně použit pro porovnání s dalšími otisky. [16]

Ultrazvukové snímače – v tomto případě je využíván zdroj ultrazvuku ve spojení s „mikrofonem“ kdy je ze snímače vyslán signál vůči přiloženému prstu a odraz zvukových vln se liší podle toho, jestli se zvuk odrážel od vrcholu papilární linie nebo od jejího údolí. Díky tomuto rozdílu, je možné vytvořit 3D model povrchu prstu – papilárních linií, tento model je dále použit pro porovnání s dalšími otisky. [16]

Termální snímače – podobně jako ultrazvukové snímače zaznamenávají výšku papilár. Pomocí termálního snímání jsme schopni měřit rozdíl teplot mezi vrcholem a údolím papilár a z těchto rozdílů vytvořit termální obraz, který je dále použit pro porovnání s jinými termálními obrazy vytvořených z otisků. [16]

2.3 RFID

Jedná se o technologii umožňující bezdrátovou identifikaci při použití rádiových vln na různých frekvencích. RFID neboli Radio Frequency Identification. Volba frekvence ovlivňuje rychlost, dosah a také přenos dat. Základní princip spočívá v umístění čipu – tagu, do blízkosti čtečky, která podporuje daný tag. Dojde k načtení dat z tagu a jejich následné zpracování – předání dál. RFID tag může být pasivní zařízení, kdy je napájen bezdrátově ze čtečky, díky tomu je potřebná menší vzdálenost pro úspěšné načtení tagu. Kromě pasivní verze existuje také aktivní verze, která disponuje vlastním zdrojem energie – typicky baterie. Díky externímu napájení je umožněn přenos dat na větší vzdálenost, výhoda/nevýhoda většího dosahu je dána aplikaci, kde je tag použit. [17]

2.3.1 Typy RFID

RFID tagy se běžně vyrábí ve velké škále tvarů a rozměrů. Volba použité komunikační frekvence tagu ovlivňuje minimální rozměry antény, která musí být umístěná na čipové kartě nebo klíčence. Velikost antény lze ovlivnit pomocí volby aktivního tagu, který je napájen pomocí externí baterie a není zde potřeba používat relativně velkou anténu, která slouží zároveň pro napájení v případě pasivní verze RFID. Pasivní verze je nejběžnější při použití jako přístupové karty nebo přívěšků na klíče. [17]

LF – Low Frequency

Frekvence 25 až 134 kHz, malý dosah, identifikace zvířat nebo předmětů v těsné blízkosti. Nízké ovlivnění vodou a kovy v prostředí, řádově jednotky cm max 10 cm

HF - High Frequency

Frekvence 13,56 MHz, malý dosah, platební karty, ID karty řádově cm do 1 metru

UHF – Ultra High Frequency

Frekvence v rozsahu 860-960 MHz, větší dosah, použití v logistice a přepravě. Dosah typicky 5-6 metrů

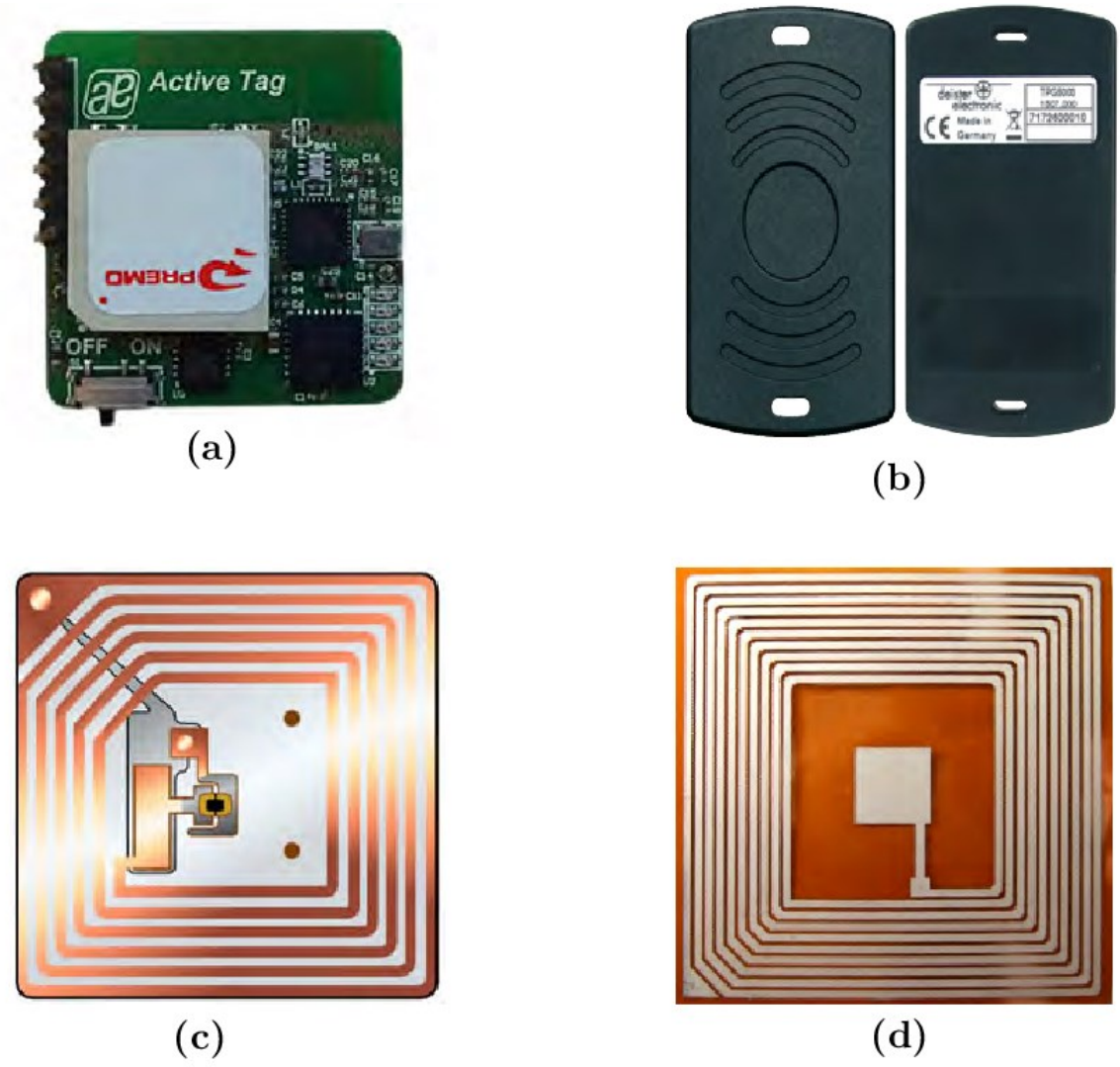
2.3.2 Principy aktivního RFID

Aktivní RFID se skládá ze tří hlavních částí (čtečka, anténa, tag) a napájecí části – typicky baterie. Díky externímu napájení může mít tag jednak o něco větší dosah komunikace, tak z pravidla mívá větší využitelnou kapacitu paměti. Pro aktivní tagy se používají zpravidla frekvenční pásma 433 a 915 MHz. Použitá frekvence se volí s ohledem na prostředí, ve kterém bude používán. Životnost tagu je hlavně ovlivněna kapacitou baterie a intenzitou – počtem čtení. Typická životnost se pohybuje mezi 3 až 5 roky. Existují v podstatě dva typy aktivních tagů, jeden se nazývá bacons a druhý transponders.

Bacons systém vysílá v pravidelných intervalech určité údaje, tento interval bývá 3-5 s. Použití této varianty je převážně v těžebním průmyslu nebo při zpracování pohonných hmot. Transponders systém na rozdíl od bacons neodesílá pravidelně data, ale odešle je až jako odpověď na přijatý signál ze čtečky – na vyžádání. Díky tomu je tato varianta šetrnější k baterii. Tento systém se používá v oblastech mýtných bran, případně bezpečnostních systémech. [18]

2.3.3 Princip pasivního RFID

V porovnání s aktivním tagem je pasivní co do počtu komponent jednodušší. Skládá se pouze ze dvou částí – antény a čipu. Čip je napájen pomocí čtečky, která slouží jak pro komunikaci tak i pro napájení.[18]



Obrázek 6. Příklady RFID zařízení (a) Aktivní tag, (b) Semi-Aktivní, (c) Pasivní s čipem, (d) pasivní bez čipu. [18]

II. PRAKTICKÁ ČÁST

3 REALIZACE EXPERIMENTÁLNÍ SESTAVY

Pro experimentální sestavu bylo definováno několik požadavků, které by měla splňovat. V rámci těchto požadavků byly vybrány jednotlivé součásti a komponenty včetně SW řešení.

3.1 Požadavky na sestavu

- Přístup pomocí číselného kódu
- Přístup pomocí bezkontaktní karty
- Přístup pomocí biometrického údaje
- Detekce obličeje s pokusem o rozpoznání
- Předání informace o přístupu nepoplachové aplikaci

Princip činnosti:

Zařízení čeká na vstup od uživatele, zadání kódu, přiložení karty nebo přiložení otisku prstu na čtečku. Po zadání/načtení kódu nebo známého otisku prstu dojde k předání informace na server. Pin kód je přenesen na server stejně jako údaje z karty. V případě otisku prstů bude přenášeno ID otisku, které je ve čtečce uloženo. Detekce obličeje a pokus o její rozpoznání je pomocí externího počítače vybaveného webkamerou, případně s dostupnou IP kamerou.

3.1.1 Seznam použitých komponent pro realizaci experimentální sestavy

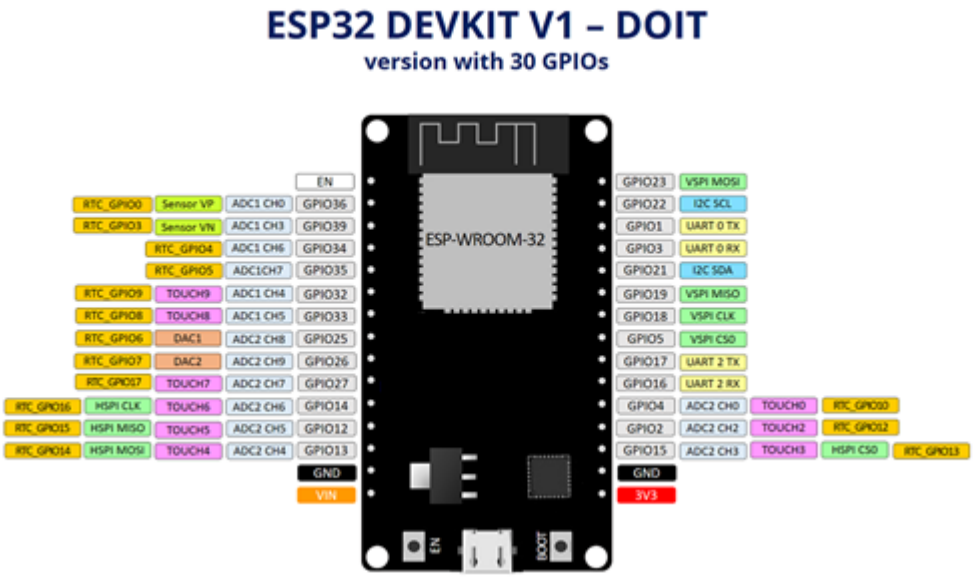
- ESP-32-WROOM [19]
- RFID čtečka MFRC-522 RC522 [22]
- Maticová tlačítková klávesnice 4x3 [21]
- Snímač otisků prstů s pamětí DY50 [23]

4 VÝBĚR HW

V rámci této části práce je čtenář seznámen s jednotlivými částmi, které jsou použity pro praktickou realizaci experimentální sestavy. V rámci realizace bylo voleno mezi několika více či méně podobnými zařízeními, která nabízejí různou funkcionalitu. Jednalo se například o předchůdce ESP-32 tedy ESP-8266 nebo alternativu jako Arduino UNO spolu s modulem pro WiFi komunikaci. Výběr HW byl ovlivněn jednak pořizovací cenou samotného zařízení, tak také funkcionalitou, kterou nabízí s ohledem na možnost budoucího rozšíření, jak po HW stránce, tak také po SW stránce.

4.1 ESP-32

Jako zařízení, které se bude starat o prvotní zpracování a propojení jednotlivých částí jsem se rozhodl pro použití modulu ESP-32-WROOM-32 od firmy Espressif Systems. Jedná se o mikrokontroler nabízející dostatek HW pinů pro připojení jednotlivých modulů. Spolu s integrovanou podporou WiFi 4, Bluetooth Classic a BLE.[19]



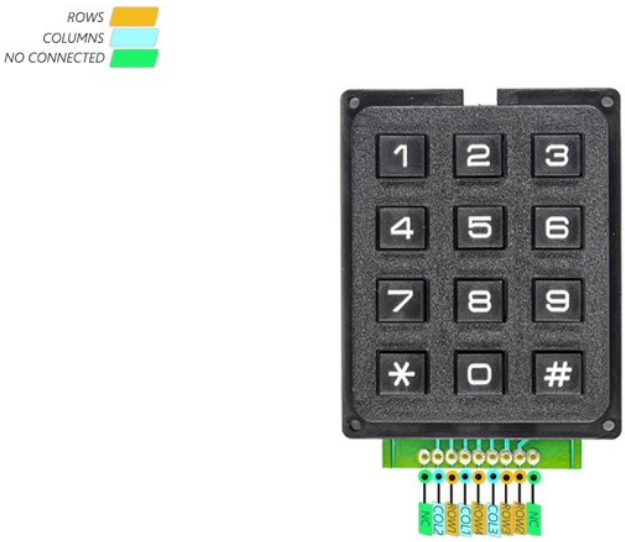
Obrázek 7. GPIO piny ESP-32 [20]

Technické parametry:

- 2x 8bitový DA převodník,
- 18kanálový 12bitový AD SAR převodník,
- 32 GPIO,
- dvoujádrový procesor Xtensa LX6, 160(240Mhz),
- 520 kB SRAM,
- podpora Wifi 802.11 b/g/n,
- podpora Bluetooth (classic + BLE),
- SPI,I^2C,I^2S,UART,CAN,IR,PWM,
- různé úsporné režimy,
- provozní teplota -40 až +125 ° C,
- napájecí napětí 2,3 až 3,6V. [19]

4.2 Membránová klávesnice

Pro možnost zadávání číselného kódu bylo rozhodnuto pro použití membránové klávesnice 4x3 která kromě číslic 0-9 nabízí také * a # které jsou použity pro reset zadaného kódu a pro jeho potvrzení. Z pohledu HW se jedná o řadu tlačítek, které spínají jednotlivé piny podle sloupce a řady dané klávesy. Je tedy potřeba použít obsluhu tlačítek pomocí MCU.



Obrázek 8. Membránová klávesnice a popis vývodů [21]

4.3 RFID čtečka

Jako další součást pro možnost duální verifikace byla zvolena technologii RFID, konkrétně tagy na frekvenci 13.56 MHz s podporou protokolu MIFARE Classic 1 K, které umožnují mimo jiné uživatelskou změnu obsahu paměti v tagu. Její velikost je 1024 Bajtů. Pracovní vzdálenost od čtečky může být až 10 cm.[22]

Obrázek 9. Čtečka RFID-RC522 s příkladem ID tagů [22]

4.4 Čtečka otisků prstů

Jako další možnost přístupu byla vybrána čtečka otisků prstů s vlastní pamětí DY50. Tato čtečka umožnuje, jednak komunikaci s ovládacím SW přes počítač za použití UART převodníku, tak po sériové lince předávat informace o načteném otisku. Jestli se nachází ve vnitřní paměti a s jakou shodou. Vnitřní paměť čtečky umožnuje pojmout až 162 jednotlivých otisků. Za předpokladu, že každý uživatel bude mít uložený pouze jeden prst, tak kapacita bude dostatečná pro až 162 unikátních uživatelů.[23]

Obrázek 10. Snímač otisků prstů DY50 [23]

4.5 Nepoplachová Aplikace

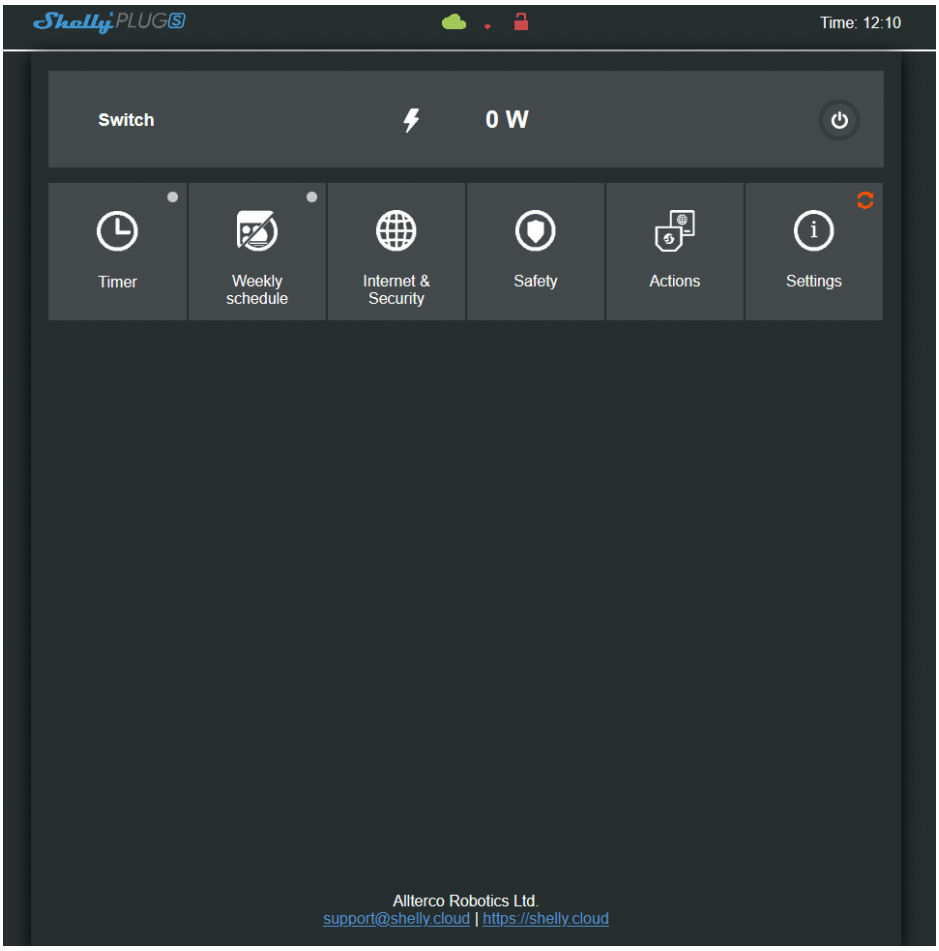
Nepoplachové aplikace jsou takové aplikace, které nejsou primárně určené k ochraně zdraví, života, majetku nebo prostředí. Mezi tyto aplikace řadíme mimo jiné systémy pro řízení topení, ventilace, řízení energetických systémů, správa budov. Může se jednat o regulaci topení, řízení osvětlení případně další aplikace, které nejsou přímo určené, jako poplachové dle aktuálně (2024) platné normy ČSN EN 50398-1 (334597) z roku 2018. [24]

Pro potřeby této práce bylo vybráno ovládání zařízení od firmy Shelly. Konkrétně se jedná o produkt Shelly Plug S. Jedná se v podstatě o standartní chytré zařízení do zásuvky 230 V/16 A. Které umožnuje monitorování spotřeby s ovládaným výstupem 230 V/16 A pomocí spínacího relé. Maximální spínaný výkon tímto zařízením je omezen na 2500 W, to při 230 V odpovídá 10,87 A. Pro ovládání je využito dostupné API, které umožnuje integraci zařízení do různých systémů jako je Home Assistant případně DIY řešeních založených na různých jiných systémech včetně podpory MQTT a dalších. [24], [25]

Obrázek 11. Shelly Plug [25]

4.5.1 Ovládání z prostředí Node Red

Zařízení umožnuje být řízeno pomocí webového rozhraní a také pomocí Web API. V dostupné dokumentaci k zařízení je možné zjistit jaké funkce a možnosti jsou pomocí API k dispozici. Pro účely této práce bylo použito pouze změny stavu v případě, že je výstup vypnut, nebo dojde k jeho zapnutí a naopak.[26]



Obrázek 12. Webové rozhraní Shelly Plug

Příkaz pro ovládání je sestaven z několika částí. Jedná se o IP adresu zařízení, volbu výstupu a co se s ním má provést. [26]

Příklad pro změnu stavu výstupu bez ohledu na aktuální stav:

192.168.89.10/relay/0?turn=toggle

Příklad pro zapnutí výstupu:

192.168.89.10/relay/0?turn=on

Příklad pro vypnutí výstupu:

192.168.89.10/relay/0?turn=off

5 DETEKCE OBLIČEJE SYSTÉMEM VSS

Pro možnost propojení systému s prvkem VSS, bylo rozhodnuto pro vytvoření aplikace, která bude umožnovat připojení na IP kameru. Nad video streamem bude provedena detekce obličeje s pokusem o rozpoznání obličeje vůči vytvořené databázi za použití open-source knihovny OpenCV.

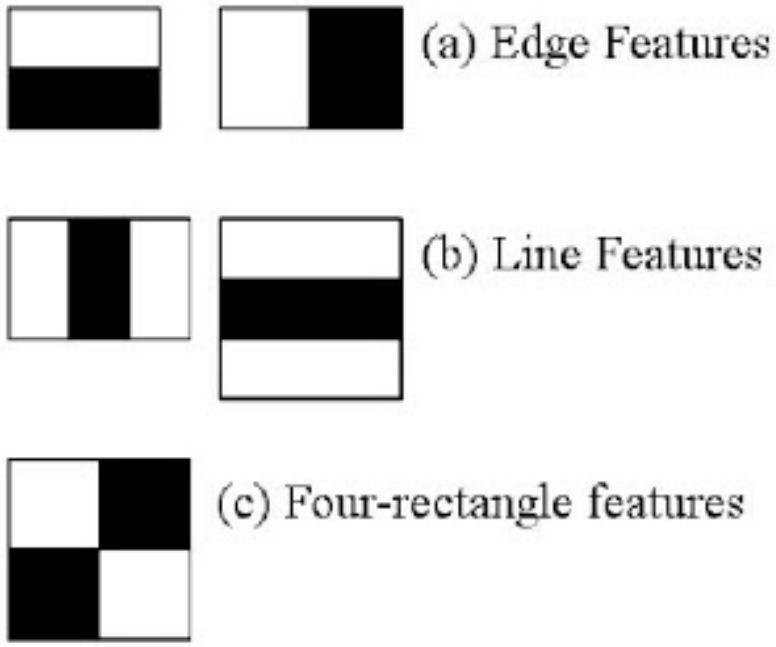
5.1 OpenCV

Jedná se o multiplatformní open-source knihovnu se zaměřením na práci s obrazem za účelem zpracování v reálném čase. OpenCV je zkratka několika slov Open Source Computer Vision. Knihovna nabízí několik funkcí pro zpracování obrazu, jako filtry pro změnu kvality obrazu, rozmazání a zvýraznění hran. V zásadě se dá říci, že umožnuje komplexní úpravu obrazu na úrovni středně pokročilého SW jen s tím, že k jejich ovládání a nastavení slouží funkce a argumenty ve vývojovém prostředí pří tvorbě aplikace. Mimo to nabízí možnost vkládat různé obrazce do obrazu jako takového. To je vhodné pro zvýraznění různých částí obrazu při detekci. Knihovna má několik funkcí pro detekci obrazců, jako jsou linie, čáry a obličeje. Díky jejich kombinaci lze detekovat dopravní značky, počítat výskyt daného vzoru a podobně. Většina funkci je k dispozici v rámci zpracování v reálnem čase a zanáší tedy minimální zpoždění mezi vstupem vstupního obrazu a výstupem analyzovaného. Samotná knihovna obsahuje sadu nástrojů, které lze využít při návrhu vlastní aplikace pro zpracování obrazu [27], [28], [29], [30]

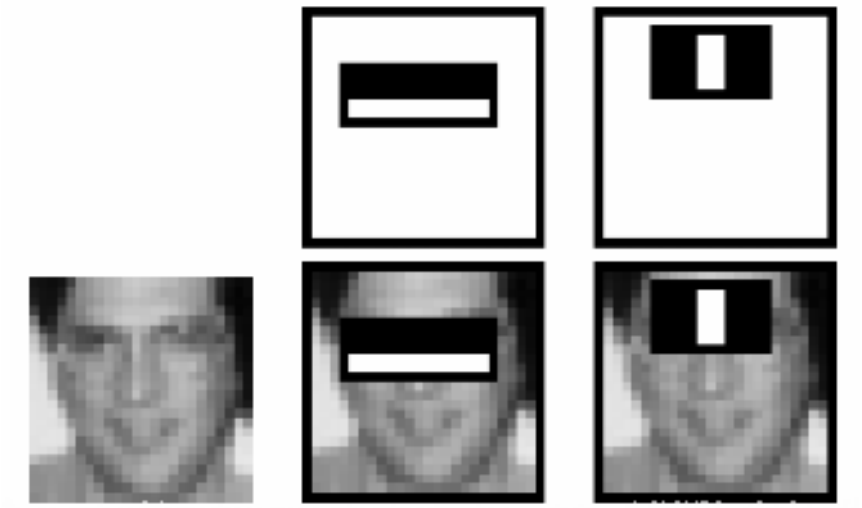
5.2 Detekce a rozpoznání obličeje

Pro doplnění experimentální sestavy o prvek VSS, byla vybrána možnost detekce obličeje, s možností rozpoznání pomocí knihovny OpenCV a vytvořeného matematického modelu založeném na algoritmu LBP (Local Binary Patterns). Pro tyto účely bylo vybráno použití Haar Cascade. Jedná se o techniku, která využívá detekce rysů v obraze. Tyto rysy jsou v podstatě různě velká okna, která se nachází v obraze a podle jejich rozmístění, velikosti a četnosti se rozhoduje, zdali požadovaný rys se v obraze nachází, čí nikoliv. Pro vyhledávání rysu se používá datový soubor, který je vytvořen pomocí vzorových souborů s pozitivním výskytem daného rysu. Trénovací proces pro vytvoření datového souboru se zaměřuje na to, aby klasifikátor byl schopen rozlišovat mezi oblastmi s pozitivním rysem a s negativním rysem. Jedná se o rychlou a vcelku spolehlivou metodu detekce objektů v obraze, kdy pro detekci daného obrazu je potřeba získat nebo vytvořit filtr obsahující pozitivní rysy daného

objektu. Pro potřeby této práce bude využit haarcascade, který je k dispozici v rámci OpenCV a slouží pro detekci obličeje zepředu. [27], [28], [29], [30]



Obrázek 13. Základní vlastnosti pro konvoluční filtr [28]



Obrázek 14. Příklad aplikace konvolučního filtru na obličej [28]

5.2.1 Detekce obličeje v jazyce Python

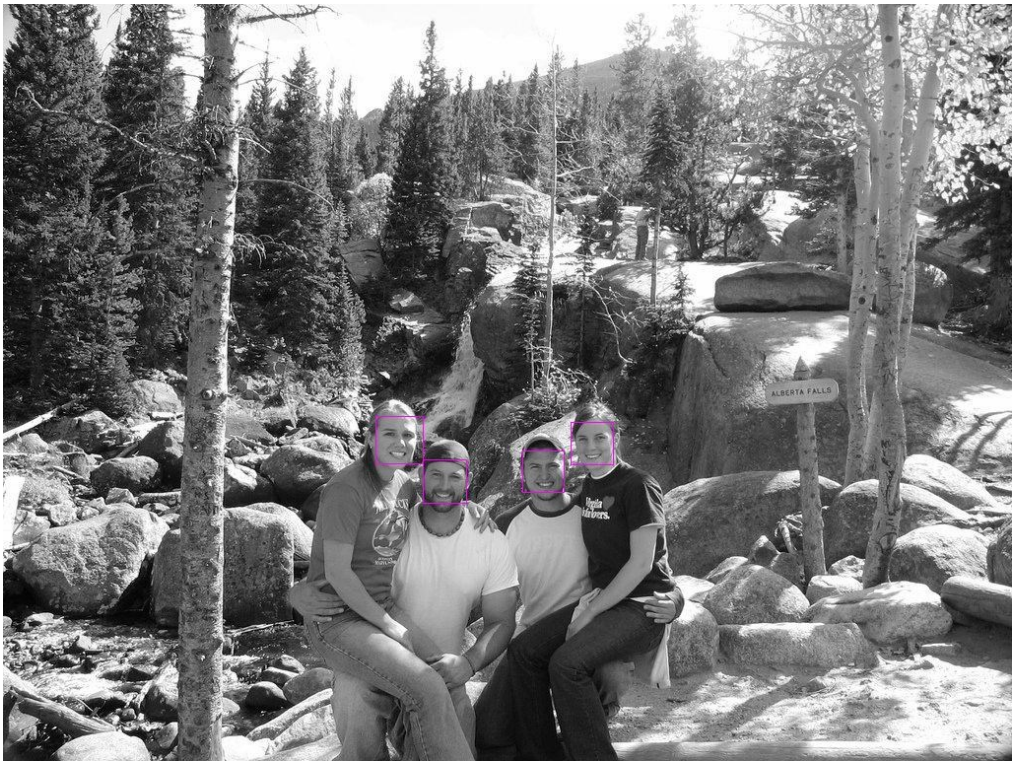
Pro detekci je potřeba importovat knihovny, které se budou používat. Jedná se o knihovnu OpenCV – cv2 a knihovnu pro práci s vektory, maticemi a vícerozměrnými poly – Numpy. Další potřebná knihovna je pro práci s obrazovými formáty v jazyce Python – PIL. Poslední

knihovna slouží pro práci s operačním systémem. Umožnuje využívat jeho funkce a zapisovat/číst soubory – os.

Dále je v programu potřeba uvést systémovou cestu k souboru obsahujícím natrénované rysy. V tomto případě obličeje z předního pohledu. V rámci této práce bylo vyzkoušeno více variant natrénovaných kaskádových filtrů. Kdy se jako nejvíce vhodný pro tuto aplikaci jeví použití haarcascade_frontalface_default.xml, který je k dispozici na stránkách projektu OpenCV a také v Github repositáři téhož projektu. Jedná se o předpřipravený model, který je dostačující pro základní detekci. Je potřeba nadefinovat vstupní obrazové zařízení. Může se jednat buďto o interní kameru na notebooku, externí USB kameru, popřípadě využít obrazový přenos z IP kamery, která je dostupná na síti, ke které je zařízení – PC připojené. Kromě fyzického kamerového zařízení je také možné použít pro vstup obrazu video soubor.

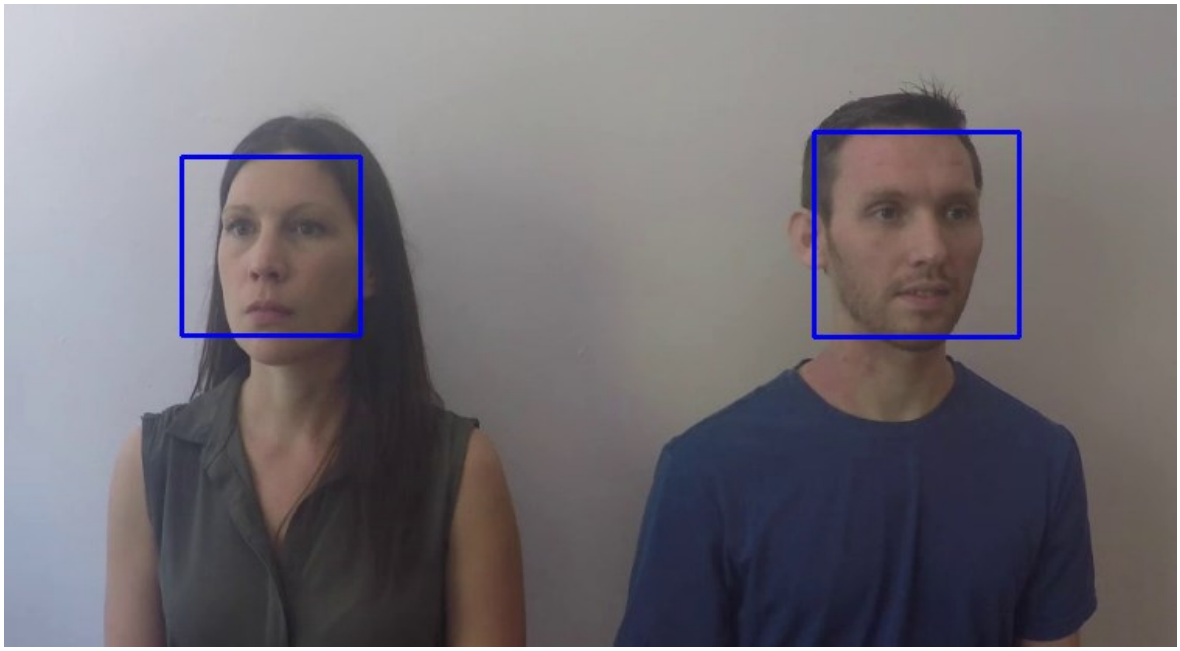
Samotné zpracování obrazu probíhá po jednotlivých snímcích. Kdy je každý snímek převeden na stupně šedi, aby jej bylo možné použít v rámci OpenCV knihovny. Poté jsou nastaveny parametry pro detekci. Specifikuje se minimální a maximální velikost. Vše mimo rozsah se ignoruje. Také se nastaví tzv. minNeighbors, změnou velikosti se značně redukuje počet falešných detekcí viz. Obrázek 15 a Obrázek 16. [27], [28], [29], [30]

Obrázek 15. Falešná detekce způsobená malou hodnotou minNeighbors [31]



Obrázek 16. Detekce s nastavenou optimální hodnotou minNeighbors [31]

Po úspěšné detekci obličeje dojde k uložení výstřižku obličeje pro potřeby vytvoření modelu rozpoznání. Schopnost rozpoznání je závislá od počtu snímku, na kterých se daný obličej vyskytuje. V případě nízkého počtu vstupních snímků může být výsledný model značně nepřesný. Vzhledem k použité metodě je výsledný model použitelný pouze za ideálních světelných podmínek. V případě zhoršených podmínek dochází ke značnému zhoršení rozpoznávacích schopnosti, zvyšuje se míra falešného rozpoznání a přiřazení obličeje k jiným osobám.Jako ukázkové soubory jsou použity data z projektu Intel IoT DEVKIT, které jsou dostupné pod licencí CC-BY-4.0 [32]



Obrázek 17. Detekce obličejů na vzorových datech [32]

6 IDENTIFIKACE UŽIVATELE

V rámci této kapitoly je čtenář seznámen s použitými SW prostředky, které jsou použité pro implementaci jednotlivých částí identifikačního procesu v rámci experimentální sestavy.

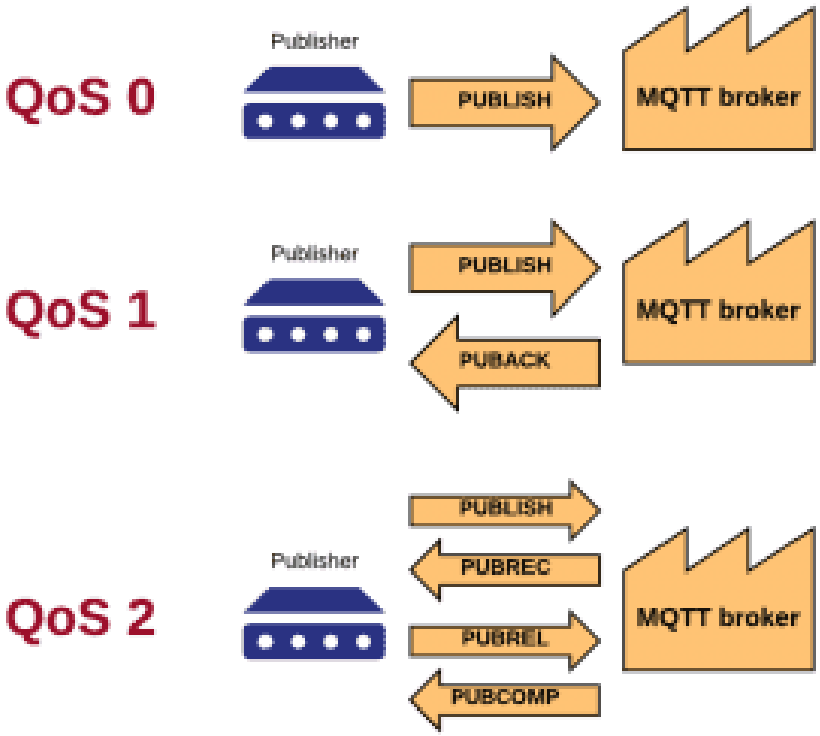
6.1 MQTT

MQTT neboli Message Quering Telemetry Transport je komunikační protokol, který byl navržen pro použití v IoT – Internet of Things. Tento protokol funguje na principu klient-server a je vhodný pro aplikace vyžadující malou spotřebu el. energie a spolehlivou komunikaci i ve stižených podmínkách – výpadky signálu [33]

6.1.1 Princip činnosti

Komunikace se skládá minimálně ze dvou prvků. Broker neboli server, jedná se o centrální bod sítě, který komunikuje se všemi klienty a podle nastavených pravidel předává zprávy od ostatních klientů. Klienti se tedy připojují k Brokeru a posílají mu zprávy, nebo je naopak pouze přijímají. Klient se tedy může provozovat ve třech režimech. Prvním je pouze odesílání dat na broker. Typicky se jedná o senzory, spínače nebo cokoliv co pouze udává svůj stav nebo hodnotu. Druhým režimem je pouze přijímání dat od brokeru, zde se jedná o různé akční členy, které přijímají vstupní data, se kterými dále pracují, např. reléový modul, který reaguje pouze na On/Off. Třetím režimem je kombinace prvních dvou. Jedná se tedy o zařízení, která jednak zprávy odesílají tak také přijímají. Může se jednat o složitější zařízení, jako chytré termostaty, kdy vzdálený senzor pošle změřenou teplotu, termostat ji příjme a na základě její hodnoty pošle zprávu pro zapnutí nebo vypnutí topení dalšímu klientovi v sítí. Veškerá tato komunikace probíhá prostřednictvím brokeru. Komunikace probíhá pomocí zpráv, které jsou řazené do skupin podle témat – topiců, kdy každý topic se může skládat z několika subtopiců. Pro lepší pochopení je vhodný případ topicu MujDum kdy subtopic může být mujdum/obyvaci pokoj, ve kterém může být několik dalších subtopicu jako MujDum/ObyvaciPokoj/svetlo apod. Kdy každý klient se může přihlásit k odběru daného topicu který jej zajímá, případně několika různých topiců. Není teda potřeba odebírat vše a následně to třídit, ale můžeme odebírat pouze potřebný subtopic, který nebude třeba dále upravovat, např. teplota, ovládání světla apod. Díky možnosti nastavit QoS Quality of Service pro jednotlivé zařízení v síti je možné garantovat, že daná zpráva dorazí všem klientům podle jejich potřeb. Pro MQTT existují tři úrovně QoS, kdy jsou očíslovány od 0 do 2, kdy 0 (at most once) reprezentuje odeslaní jednou, kdy příjemce nemusí přijetí potvrdit. Druhým krokem

je úroven 1 (at least once), kdy je příjem zprávy potřeba potvrdit – garance doručení. Poslední režim je nejnáročnější, co se týká režie pro zprávy, úroveň 2 (exactly once) – zpráva je doručena právě jednou. [33], [34]



Obrázek 18. Úrovně odpovědi na zprávu MQTT [34]

Kromě QoS umožnuje MQTT také dynamické připojování a odpojování klientů ze sítě. Díky tomu může broker udržovat přehled o klientech a v případě jejich znovu připojení jim poslat všechny zprávy, které zmeškali v době nepřipojení – zde hraje roli správné nastavení QoS pro jednotlivé témata. [33], [34]

6.1.2 Propojení se sestavou

Experimentální sestava využívá několik vláken, do kterých posílá zprávy ze sestavy. Vždy po zadání kódu a jeho potvrzení je do vlákna pro číselný kód odeslán zadaný kód, který je následně ověřen vůči databázi. Komunikace není v rámci experimentální sestavy šifrovaná. V rámci sestavy to není potřeba. Pokud by byla nutnost komunikaci šifrovat, tak je to možné přidáním šifrovacího algoritmu do FW kdy by před odesláním zprávy došlo k jejímu zašifrování. Na straně serveru by přijatá zpráva nabyla hned zpracována, ale bylo by ji potřeba

nejprve dešifrovat. Obdobně pro RFID čtečku. Po načtení karty je přečten řetězec, který je na ní uložený poslaný na server. Řetězec může být forma textu – hesla případně pouze číselný řetězec jako obdoba kódu. V případě snímače otisků je využita vnitřní paměť, kdy je nasnímaný otisk porovnán s vnitřní databází a v případě schody je na server odesláno ID z vnitřní databáze. Na serveru je tedy potřeba udržovat aktuální identifikátory, které jsou ve čtečce používány.[33], [34]

6.2 Příprava SW

V rámci práce je použito několik HW součástí, které obsahují SW pro jejich řízení. Může se jednat o operační systém s aplikačními doplňky, pro doplnění funkcionality případně její rozšíření až po FW, který slouží pro obsluhu HW zařízení v rámci experimentální sestavy.

6.2.1 MQTT broker Mosquitto

Pomocí příkazové řádky jsou nainstalovány dva balíčky Mosquitto a mosquitto-clients pomocí příkazu

sudo apt install -y mosquitto mosquitto-clients

Automatické spuštění služby po startu se nastaví pomocí příkazu

sudo systemctl enable mosquitto.service

Ověření verze brokeru pomocí příkazu

mosquitto -v

Nastavení brokeru pro přístup za pomoci uživatelského jména a hesla – neautorizovaná osoba nebo zařízení nebude moct posílat případně dostávat zprávy od autorizovaných zařízení nebo osob.

Příkaz pro nastavení uživatelského jména je

sudo mosquitto_passwd -c /etc/mosquitto/passwd POZADOVANE_JMENO po potvrzení příkazu nás systém vyzve k zadání uživatelského hesla, které chceme používat ve spojení s daným jménem. Poté je potřeba upravit konfigurační soubor samotného brokeru. To provedeme pomocí příkazu.

po potvrzení příkazu nás systém vyzve k zadání uživatelského hesla, které chceme používat ve spojení s daným jménem. Poté je potřeba upravit konfigurační soubor samotného brokeru. To provedeme pomocí příkazu.

sudo nano /etc/mosquitto/mosquitto.conf

Ten otevře konfigurační soubor v textovém editoru, kde je potřeba editovat několik parametrů. Prvním je napsat na první řádek řetězec

per_listener_settings true

a dále potřeba zapsat následující řádky:

allow_anonymous false

listener 1883

password_file /etc/mosquitto/passwd

První deaktivuje anonymní uživatele. Druhý definuje port, na kterém budou přijímány zprávy a třetí je umístění souboru obsahujícího uživatelské jméno a heslo. Po těchto úpravách uložíme soubor pomocí klávesové zkratky CTRL+X poté Y pro potvrzení. Nyní stačí restartovat službu brokeru pro aplikování změn a tím je broker připraven k používání.

Příkaz pro restartování služby

sudo systemctl restart mosquitto

ověření běhu brokeru pomocí příkazu

sudo systemctl status mosquitto

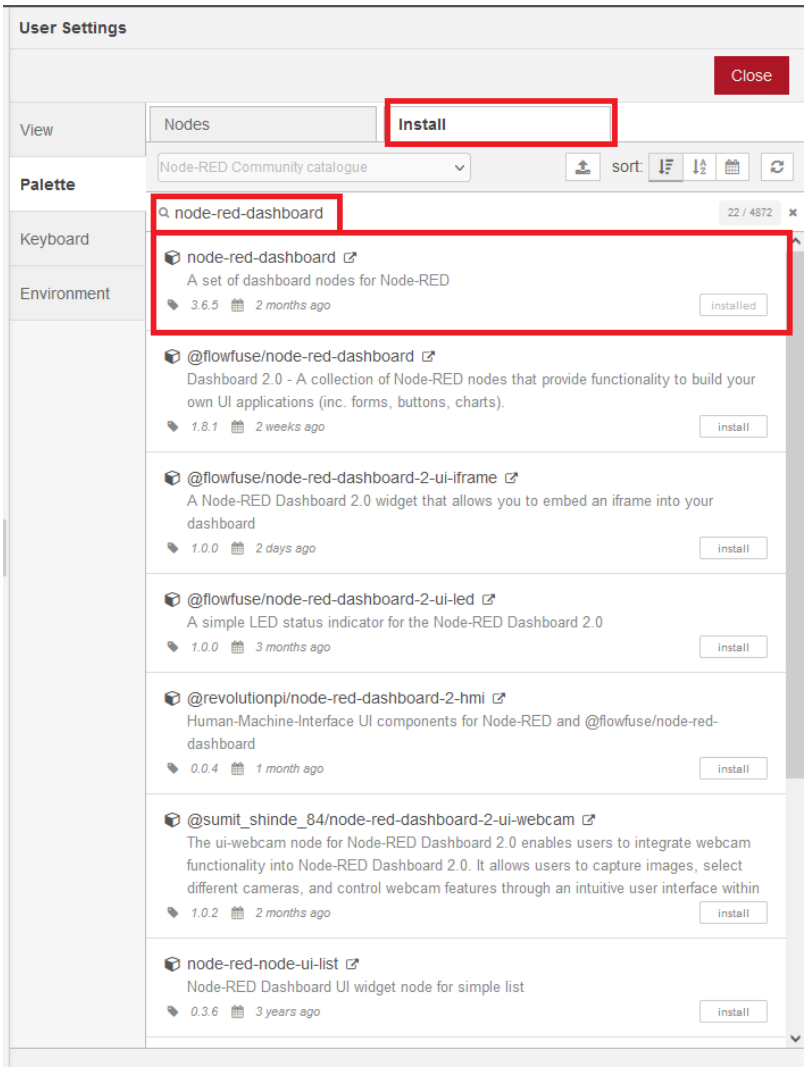
6.2.2 Instalace NodeRed

Instalace prostředí NodeRed je provedena pomocí připraveného skriptu, který je k nalezení v dokumentaci na stránkách nodered.org

Příkaz do terminálu pro instalaci

bash <(curl -sL https://raw.githubusercontent.com/node-red/linux-installers/master/deb/update-nodejs-and-nodered)

Kromě základních balíčků je v rámci práce použito i několik doplňků, které umožnují/usnadňují práci s některými funkcemi, jako připojení k SQL databázi, rozšíření, které přidá možnost zobrazení/vytvoření rozhraní na webu – dashboard apod. Instalace balíčků probíhá z webového prostředí, kdy pomocí klávesové zkratky Alt+P je vyvoláno okno ze kterého je možné instalovat a mazat požadované doplňky. Jak je možné vidět na Obrázku 19, je možné procházet jak nainstalované balíčky, tak vyhledávat balíčky nové.



Obrázek 19. Instalace přídavných balíčků Node Red

6.2.3 MySQL,Apache,PHP,PHP My admin

Instalace SQL databáze spolu s webovým server probíhá prostřednictvím příkazové řádky. Před jakoukoliv instalací je vhodné provést opětovnou aktualizaci repozitářů a systému pomocí příkazu

sudo apt update && sudo apt upgrade -y

Poté je možné přistoupit k instalaci samotného webového serveru Apache za pomoci příkazu

sudo apt install apache2 -y

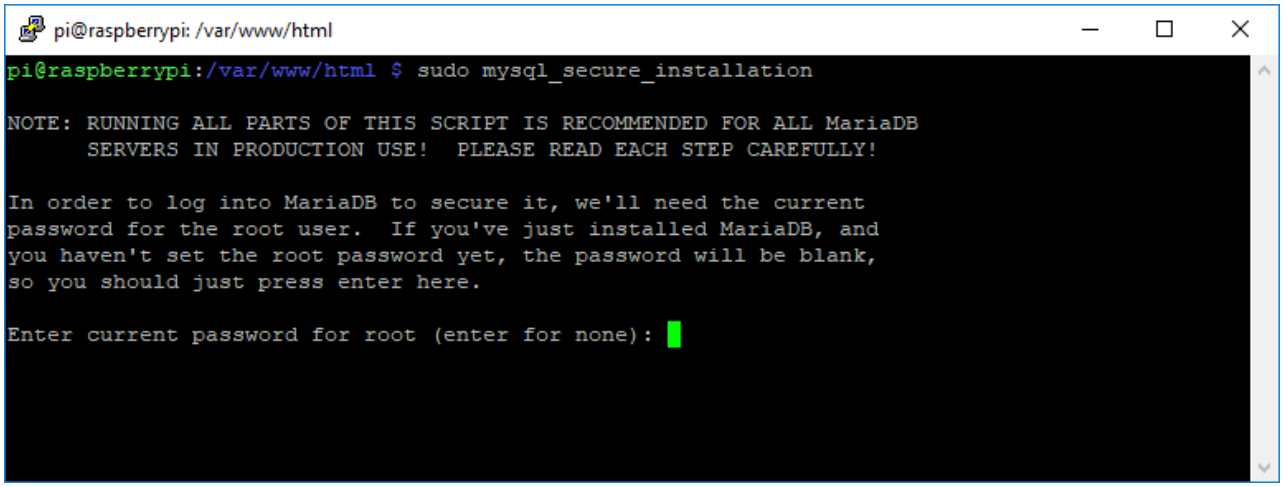
proces instalace je automatizovaný, takže po nainstalování ověříme, zdali funguje, a to tak že otevřeme webový prohlížeč a do pole pro URL adresu zadáme IP adresu zařízení případně IP adresu 127.0.0.1. Jedná se o adresu localhost, která vede vždy zpět na zařízení.

Instalace PHP probíhá obdobně. Na rozdíl od Apache je potřeba provést ještě nějaké úpravy pro zobrazení webové stránky s PHP. Instalace pomocí příkazu sudo apt install php -y

Po proběhnutí instalačního procesu můžeme smazat soubor index.html, který se nachází ve složce /var/www/html. Poté pomocí textového editoru vytvoříme soubor s názvem index.php do kterého vložíme řetezec <?php echo "hello world"; ?>. Po uložení souboru provedeme restart služby webového serveru pomocí příkazu sudo service apache2 restart. Nyní opět otevřeme webový prohlížeč a ověříme funkčnost PHP načtením adresy localhost, která by nyní měla obsahovat zprávu, kterou jsme vložili do souboru index.php – hello world

Instalace samotného SQL pomoci příkazu sudo apt install mariadb-server php-mysql -y.

Poté je potřeba znovu restartovat službu webového serveru a poté spustit instalaci MySQL pomocí příkazu sudo mysql_secure_installation



Obrázek 20. Instalace MySQL z příkazové řádky

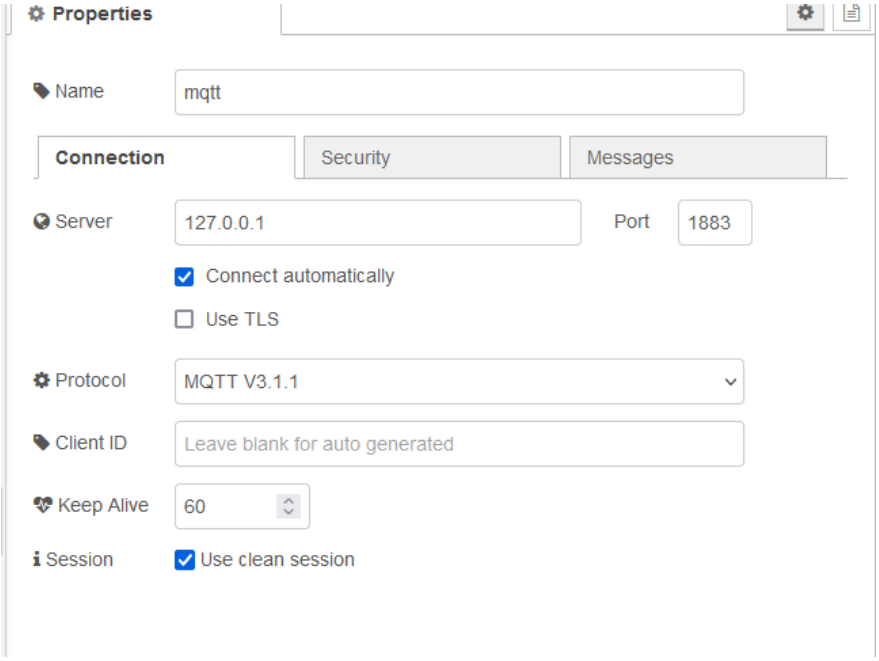
6.3 Node Red

Jedná se o open-source platformu pro vizuální programování, kterou vyvinula firma IBM. Základ je postaven na jazyce Node.js, který poskytuje přívětivé grafické rozhraní pro vytváření toků dat za pomocí uzlů (nodes) a propojovacích linií. Uzly představují různé funkce pro práci s daty. Složitější a funkční celky se v NodeRed označují za tok dat (Flow). Kromě aplikací na práci s daty umožnuje NodeRed rozšíření pomocí tzv. palet. Jedná se o rozšiřující moduly, které mohou přidávat rozšířené funkce, popřípadě umožnují přidání grafické

nadstavby nad jednotlivými celky. Kromě toho je možné na jedné stanici vytvořit danou aplikaci a exportovat ji včetně jejich parametrů ve formátu JSON do jiného zařízení ve kterém jsou nainstalované potřebné moduly, které jsou v dané aplikaci použity. [35]

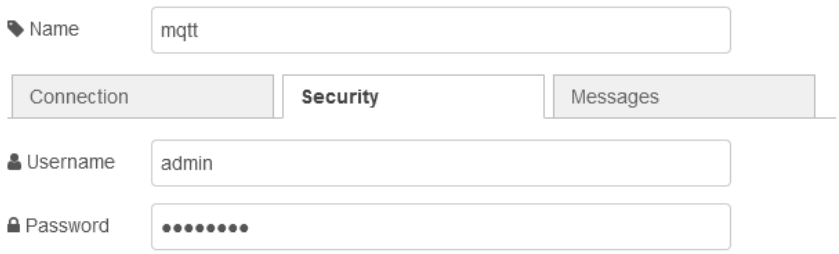
6.3.1 Nastavení MQTT brokeru v Node-Red

Data, která jsou posílána pomocí protokolu MQTT je potřeba v prostředí získat, aby bylo možné s nimi dále pracovat. Node Red obsahuje v základu podporu pro příjem a odesílání zpráv pomocí protokolu MQTT. Stačí tedy tyto připravené bloky použít a doplnit do nich parametry Brokeru, přes který bude probíhat komunikace. Vzhledem k faktu že broker běží na stejném zařízení jako aplikace Node Red, stačí uvést IP adresu jako localhost a výchozí port pro připojení (je použito defaultního portu pro komunikaci). [34][35]



Obrázek 21. Node Red připojení k MQTT broker

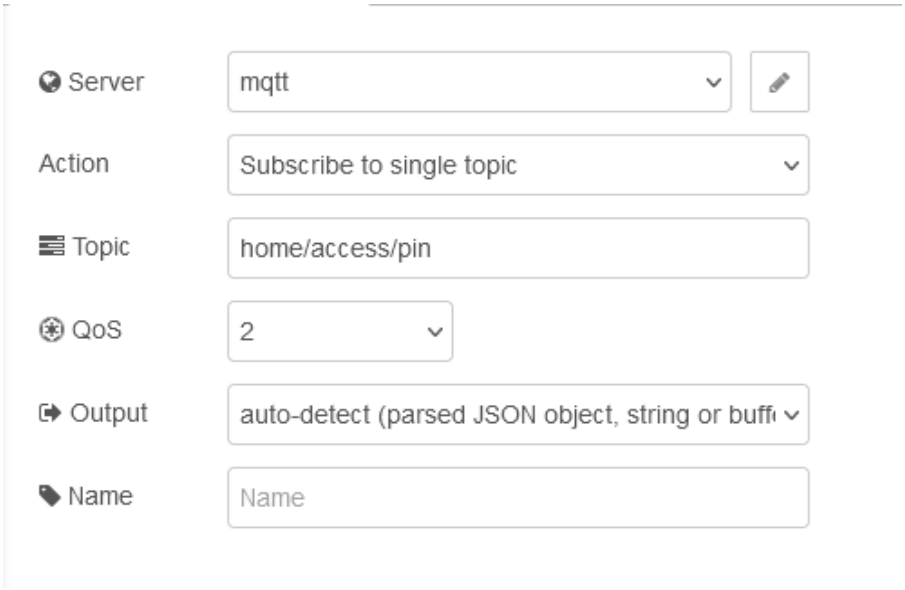
Kromě nastavení údajů o brokeru je také potřeba vyplnit přihlašovací údaje. Bez toho by broker odmítl připojení a nebylo by možné přijímat nebo posílat data. Pod záložkou Security vyplníme přihlašovací údaje pro broker, které jsme nastavili při jeho instalaci.



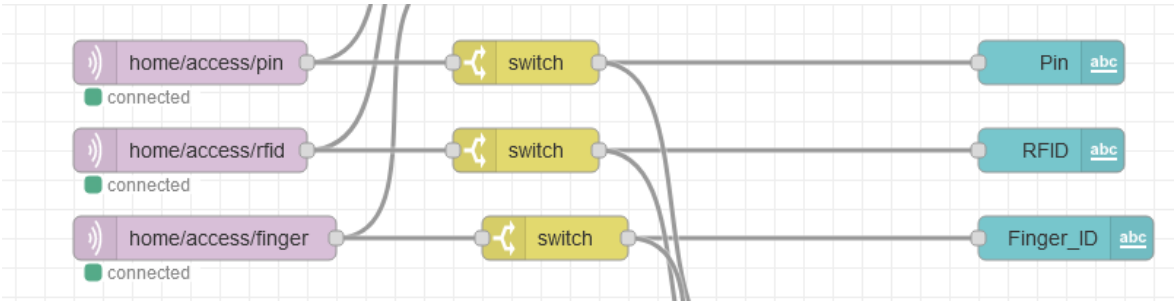
Obrázek 22. Node Red Nastavení přístupových údajů pro MQTT

6.3.2 Příjem dat z experimentální sestavy

Experimentální sestava posílá upravená data z jednotlivých modulů (Membránová klávesnice, Čtečka RFID, Snímač otisků) do samostatných vláken MQTT. Tyto vlákna jsou přijímána do prostřední Node Red pomocí bloků na příjem dat z přednastaveného MQTT serveru. Nastavení MQTT serveru bylo nastíněno v předchozí části. V rámci této podkapitoly je popsáno nastavení příjmu jednotlivých vláken a zpracování přijatých dat je popsáno v rámci další podkapitoly. Zobrazení přijatých dat je realizováno pomocí bloků, které přijaté hodnoty zobrazí ve webovém prostředí. Jedná se pouze o zobrazení pro testovací účely a není nezbytné pro funkci sestavy. [33][35]



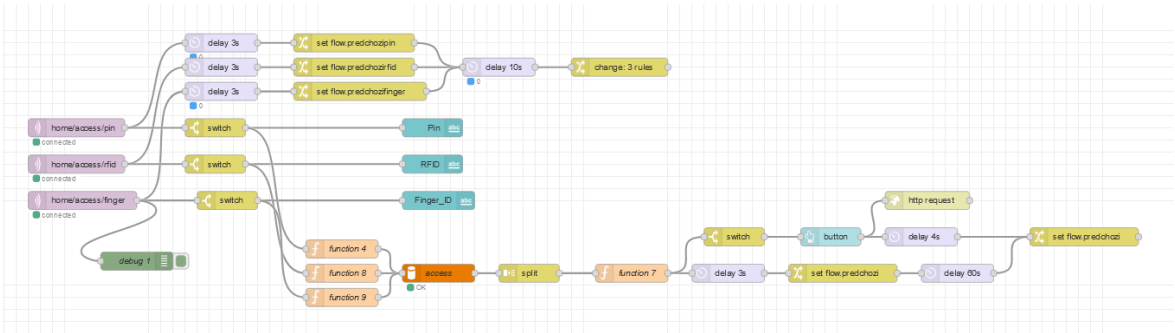
Obrázek 23. Nastavení MQTT pro příjem vlákna, do kterého je posílán číselný kód



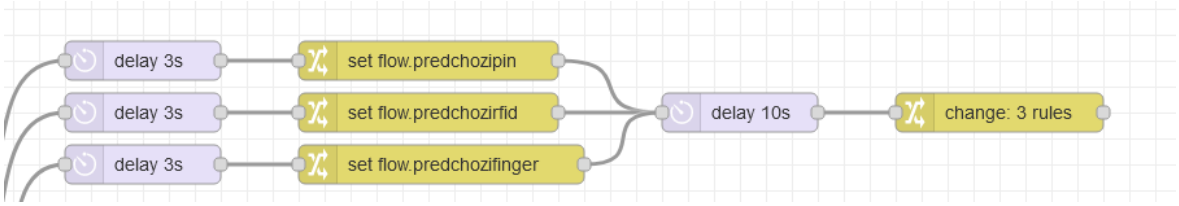
Obrázek 24. Bloky pro příjem dat a jejich zobrazení (popis v následující podkapitole)

6.3.3 Zpracování přijatých dat

Po přijetí dat z MQTT je provedeno několik kroků. Prvním je provedení porovnání v bloku switch, kde je porovnána přijatá hodnota s hodnotou uloženou v paměti. Pokud je hodnota v paměti jiná od hodnoty přijaté je provedeno další zpracování. Ve stejnou dobu běží 3sekundové zpoždění, po kterém je přijatá hodnota uložena do paměti pro další porovnání. Hodnota je v paměti uložena zhruba po dobu 10-ti sekund, kdy dojde k jejímu opětovnému přepisu na výchozí hodnotu. Jedná se o netisknutelný znak (Alt+255). Tato přechodná změna je v programu z důvodu eliminace použití stejného způsobu přihlášení dvakrát po sobě. Kdy by při absenci této části bylo možné dvojnásobným přihlášením pomocí jedné metody docílit nežádoucího přístupu – případ úniku kódu, ztráta tagu apod. Zároveň po uplynutí 10-ti sekund je možné opakovat pokus o přístup. [35]

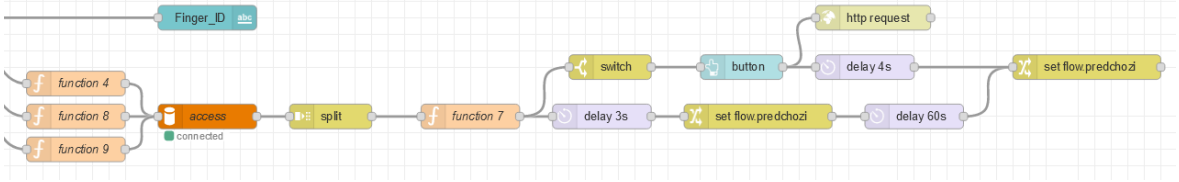


Obrázek 25. Zpracování přijatých zpráv, jejich zobrazení a ověření vůči databázi celkový pohled.



Obrázek 26. Bloky pro nastavení načtených dat, eliminace přihlášení jedním způsobem

Po přijetí údajů, je pomocí bloku pro přístup do SQL tabulky sestaven dotaz pro vyhledání daného číselného kódu, RFID řetězce nebo ID ze snímače. V případě že se v databázi nachází pozitivní shoda je vráceno ID uživatele z databáze. Toto ID je porovnáno s pamětí pro ID, pokud je v paměti výchozí hodnota (-1) je vloženo do paměti, kde zůstane po dobu 60 sekund, nebo do přihlášení, podle toho, co nastane dříve. V případě, že je v paměti uložené stejné ID jako právě získané, jedná se o situaci druhého přístupu a je umožněn přístup. Tato skutečnost je signalizována pomocí změny stavu výstupu na nepoplachové aplikaci (např. zapnutí/vypnutí osvětlení).



Obrázek 27. Procedura pro ověření že všechny použité metody patří stejnému uživateli

6.4 Obsluha membránové klávesnice

Pro obsluhu membránové klávesnice, byla použita open source knihovna keypad.h, která vychází ze stejnojmenné knihovny od autora Mark Stanley a Alexander Brevig která byla komunitou upravena a dále udržována.

Pro použití knihovny je potřeba definovat počet řádků a sloupců klávesnice kterou používáme. Nejpoužívanější je 4x3 a 4x4. V tomto případě je použita klávesnice 4x3, definujeme tedy počet řádků na 4 a počet sloupců na 3. Také je potřeba si definovat vícerozměrné pole pro jednotlivé znaky klávesnice (vhodné, pokud si chceme udělat vlastní rozložení/layout kláves i s vlastním potiskem).

```
#define ROW_NUM     4 // four rows
#define COLUMN_NUM  3 // three columns
```

```
char keys[ROW_NUM][COLUMN_NUM] = {
  {'1', '2', '3'},
  {'4', '5', '6'},
  {'7', '8', '9'},
  {'*', '0', '#'}
};
```

Dále je potřeba definovat na jakých pinech jsou připojené jednotlivé piny klávesnice. V našem případě používáme piny 21,22,32 a 12 pro řádky a piny 25,4 a 33 pro sloupce (piny voleny s ohledem na další moduly).

```
byte pin_rows[ROW_NUM] = {21, 22, 32, 12}; // GPIO21, GPIO22, GPIO32, GPIO12 connect to the row pins
byte pin_column[COLUMN_NUM] = {25, 4, 33};  // GPIO25, GPIO4, GPIO33 connect to the column pins
```

Dále je potřeba vytvořit pole, pro zaznamenané znaky a instanci samotné klávesnice, které se v argumentech předá mapování jednotlivých kláves, pole pinů se sloupci a řádky a jejich počet.

```
char znaky[60];//pole pro stisknuté znaky
Keypad keypad = Keypad( makeKeymap(keys), pin_rows, pin_column, ROW_NUM, COLUMN_NUM );// instance klávesnice s nemapovanými znaky a GPIO piny
```

Nyní je možné používat funkci knihovny getKey(), která vrací namapovaný znak v případě, že bylo stisknuto dané tlačítko, v opačném případě vrací nulový znak (‘\0‘).

Když máme načtený stisknutý znak je potřeba jej vyhodnotit. Na to je vytvořená rutina, kdy každý znak, který neodpovídá # nebo * je vložen do pole znaky [] ve kterém jsou uloženy dokud nedojde ke stisku řídících znaků (#,*), nebo k dosažení maximálního počtu znaků, který je nastaven na 60. V případě stisku znaku * je tomuto znaku přiřazena procedura reset. Dojde tedy k vymazání stisknutých znaků z paměti – pro případ chybného zadání/oprava. V případě stisku # je tomuto znaku přiřazeno potvrzení OK. Dojde tedy k předání/odeslání uložených znaků na server a jejich vymazání z paměti pro potřeby dalšího zadání.

```
char key = keypad.getKey(); // uložení stisknutého znaku do proměnné
    if (key) {
      if(key == '#'){ // hashtag je zástupný znak pro potvrzení, po jeho stisku dojde k odeslání pole znaků
        Serial.println(znaky);
        client.connect(clientID, mqtt_username, mqtt_password);
        client.subscribe(stopic,1);
        client.loop();
        connect_MQTT();
        String ts=String(znaky);
```

```
        if (client.publish(pin_topic, String(ts).c_str())) {
          Serial.println("pin sent!");
          client.disconnect();
        pozice = 0;
        memset(znaky, 0, sizeof(znaky));

      }
      else if(key == '*'){ // star je zástupný znak pro reset, vymazání za-
daných znak z paměti
        pozice = 0;
        memset(znaky, 0, sizeof(znaky));
      }
      else {
        znaky[pozice] = key;//uložení stisknutého znaku do pole a inkremen-
tace pole
        pozice++;
        if(pozice == 59){ // při dosažení maximální délky znaku dojde k vý-
mazu a uvolnění paměti, ekvivalent stisku reset
          Serial.println(znaky);
          pozice = 0;
        memset(znaky, 0, sizeof(znaky));
        }
      }
  }
```

6.5 Obsluha RFID čtečky

Zvolená RFID čtečka využívá komunikační rozhraní SPI (Serial Peripherial Interface). Pro komunikaci je využita knihovna, která umožnuje značné zjednodušení komunikace.

Inicializace RFID čtečky s pomocí knihovny je potřeba definovat piny použité pro RESET a přenos dat. Poté je vytvořena instance třídy rfid a následně instance komunikačního klíče.

```
#define SS_PIN 5 //SDA
#define RST_PIN 15 //RESET
MFRC522 rfid(SS_PIN, RST_PIN); // třída rfid
MFRC522::MIFARE_Key key; // třida klíče
byte nuidPICC[4]; //identifikátor RFID
int blockNum = 2;  //velikost bloků pro data
byte blockData [16] = {"testovaci_heslo"}; //testovací data - heslo
byte bufferLen = 18; // zásobník pro čtení dat
byte readBlockData[18]; // pole přečtených dat
MFRC522::StatusCode status; // stav RFID
```

Před zahájením komunikace je provedena inicializace komunikace po sběrnici SPI a inicializována instance RFID. Následně je vygenerován komunikační klíč, který má délku 6 bitů.

```
SPI.begin(); // Inicializace SPI rozhraní
  rfid.PCD_Init(); // Inicializace MC552
  for (byte i = 0; i < 6; i++) { // generování klíče komunikace FF FF FF FF
FF FF
    key.keyByte[i] = 0xFF;
  }
 // Přeskočení smyčky pokud není karta přítomná u čtečky
    if ( ! rfid.PICC_IsNewCardPresent())
      return;
    // Ověření zdali byla karta už jednou načtena nebo nikoliv - opakované
použití
    if ( ! rfid.PICC_ReadCardSerial())
      return;
    //Serial.print(F("PICC type: "));
    MFRC522::PICC_Type piccType = rfid.PICC_GetType(rfid.uid.sak); // na-
čtení typu RFID karty
    //Serial.println(rfid.PICC_GetTypeName(piccType));
    //  ověření zdali se jedná o kartu typu PICC nebo Classic MIFARE
    if (piccType != MFRC522::PICC_TYPE_MIFARE_MINI &&
      piccType != MFRC522::PICC_TYPE_MIFARE_1K &&
      piccType != MFRC522::PICC_TYPE_MIFARE_4K) {
      Serial.println(F("TAG není typu MIFARE Classic."));
      return;
    }
```

6.5.1 Čtení

```
 // načtení NUID karty
      for (byte i = 0; i < 4; i++) {
        nuidPICC[i] = rfid.uid.uidByte[i];
      }
        Serial.println("Načtení dat z karty...");
        ReadDataFromBlock(blockNum, readBlockData);
        Serial.print("Data :");
        Serial.print(blockNum);
        Serial.print(" --> ");
        char text[18];
        for (int j=0 ; j<16 ; j++) // zkopírování dat do textového pole pro
další manipulaci
        {
          Serial.write(readBlockData[j]);
          text[j]= readBlockData[j];
        }
        client.connect(clientID, mqtt_username, mqtt_password); // Připojení
MQTT
        client.subscribe(stopic,1);//odběr vlákna pro řídící data - nevyu-
žito
        client.loop(); // obsluha příjmu zprávy
```

```
        connect_MQTT(); // připojení k MQTT
        String ts(text);
        if (client.publish(rfid_topic, String(ts).c_str())) { // odeslání
přečtených dat na server ve formátu stringu
          Serial.println("rfid sent!");
          client.disconnect();  // odpojení od MQTT brokeru
        }
```

6.6 Obsluha snímače otisků prstů

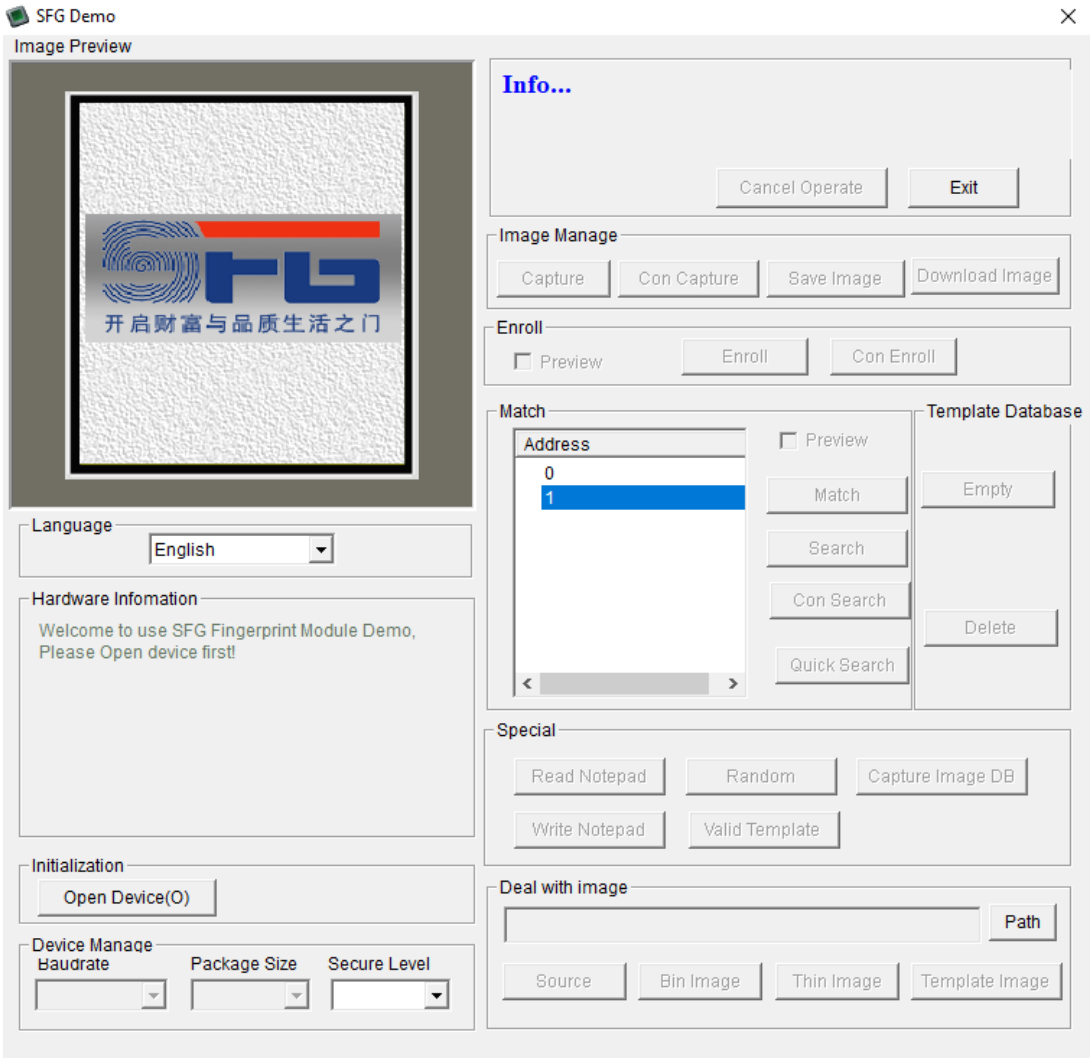
Použitý snímač otisků prstů je v rámci experimentální sestavy použit ke dvěma samostatným funkcím. První funkce slouží pro zaznamenání nového uživatele do paměti pomocí řídícího počítače. V tomto případě je nutno čtečku připojit pomocí rozhraní na experimentální sestavě a přepnou přepínač režimů na pozici 1. Po přepnutí přepínače na pozici 0 je komunikace s PC ukončena a čtečka přechází do režimu porovnávání přiložených otisků vůči své paměti. V případě shody vrací vnitřní ID uživatele.

6.6.1 Komunikace s PC

Vzhledem k tomu, že použitá čtečka otisků prstů DY50 disponuje vlastní pamětí pro uložené otisky prstů a vůči této paměti provádí porovnání nasnímaných otisků, je přínosné, že umožnuje zprostředkovaně přímou komunikaci s PC a obslužným SW na něm. Obslužný SW použitý v rámci této práce byl SFG Demo. Jedná se o testovací SW pro ovládání různých čteček otisků. V rámci tohoto SW je možné načíst informace o používané čtečce na daném COM portu. V případě DY50 je potřeba použít převodník UART pro komunikaci. Zde je použito ESP-32 jako převodník, kdy hlavní smyčka programu je rozdělena na dva funkční celky. První je pro autonomní činnost zařízení pro komunikaci se serverem a druhý se stará o zprostředkování komunikace na sériový port. V tomto režimu jsou ostatní funkce zařízení pozastaveny a pro opětovné rozběhnutí ostatních částí je potřeba opět přepnout režim. Komunikace s ESP-32 probíhá pomocí HW sériové linky, které ESP umožnuje (pokud by nebylo možné použít HW sériovou linku, bylo by potřeba vytvořit instanci sériové linky na SW bázi, kdy by obsluha byla o něco složitější a zabírala by více procesorového času).

```
if (runmode == 1){
    while (Serial.available())
      myserial.write(Serial.read());
    while (myserial.available())
      Serial.write(myserial.read());
  }
```

SW SFG Demo viz. Obrázek 28. Umožnuje načtení nových otisků do paměti. Porovnání čteného otisku s pamětí, přepsání/výmaz uložení otisků z paměti, případně export/zobrazení snímaného otisku. Paměť umožnuje uložit až 162 samostatných otisků.

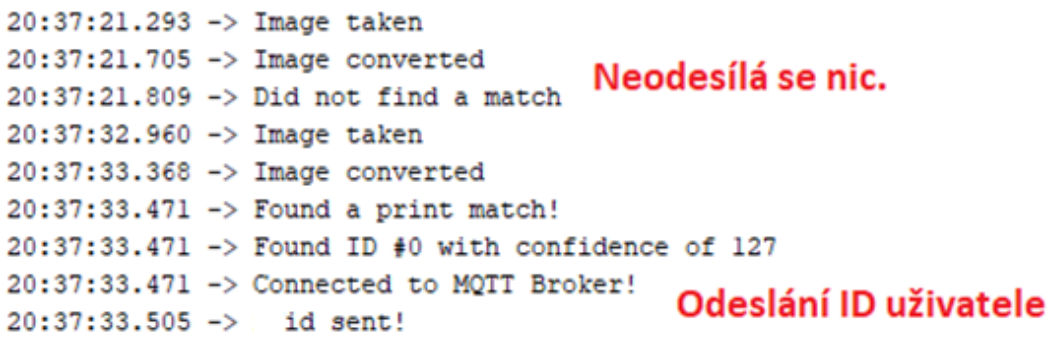


Obrázek 28. Rozhraní aplikace SFG

6.6.2 Komunikace s MCU

Pro komunikaci MCU se čtečkou DY50, je použita knihovna Adafruit-Fingerprint-Sensor-Library od společnosti Adafruit. Jedná se o knihovnu pod licencí BSD. Pro komunikaci jako takovou je potřeba vytvořit další HW sériovou linku, která se bude starat o komunikaci se čtečkou jako takovou. Dále je potřeba vytvořit instanci snímače a předat informace o použité sériové lince, na které je snímač připojen. Poté je potřeba inicializovat komunikaci a nastavit její rychlost (57600 baud/s). V programu se nachází dvě funkce, jejichž úkol je podobný. V případě detekování změny na snímači provést pokus o sejmutí otisku. V případě, že se na

snímači nachází otisk je provedeno porovnání s vnitřní pamětí snímače. Po nalezení shody je vráceno ID uživatele. Toto ID je následně odesláno na MQTT broker pro další zpracování.[19], [33]



Obrázek 29. Výstup sériové linky při neznámém otisku a při nalezení shody.

6.7 Komunikace sestavy se serverem

Pro možnost posílání dat na server, na kterém probíhá vyhodnocení přístupu, bylo rozhodnuto o použití bezdrátového spojení pomocí WiFi a odesílání dat pomocí MQTT protokolu na server. Díky použití MQTT je možná obousměrná komunikace se zařízením bez nutnosti dalšího vedení, kromě napájení, to je možné realizovat z jakéhokoliv USB zdroje schopného poskytnout až 500 mA proudu při 5 V napájení. Postačuje tedy jakýkoliv zdroj splňující požadavky na standart USB.

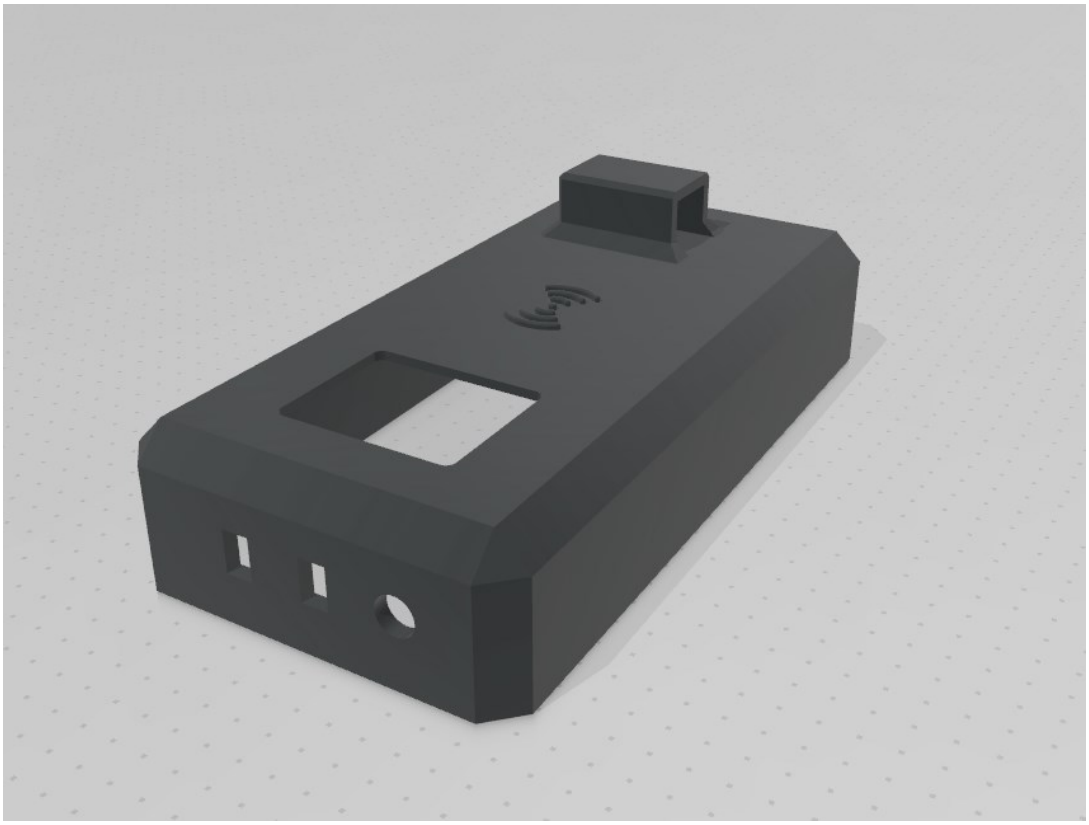
7 KRABIČKA SESTAVY

Experimentální sestava se skládá z několika elektronických součástek, které jsou vzájemně propojeny a z tohoto důvodu vznikl požadavek na vytvoření obalu, který bude tyto komponenty chránit před poškozením a zároveň bude fungovat jako jejich základna pro používání.

Krabička byla navržena tak, aby bylo umožněno umístění tlačítkové klávesnice. Vedle klávesnice je čtečka RFID karet a umístěn snímač otisků prstů. Kromě hlavních částí je na krabičce přítomno několik ovládacích prvků. Jedním je vypínač pro uvedení zařízení do provozu ON/OFF. Druhým je přepínač pro přepínání mezi režimy, kdy zařízení funguje tak, že vstupy od uživatele posílá na server. Druhý režim, při kterém je omezena funkce klávesnice a RFID čtečky a funguje pouze snímač otisků prstů, který komunikuje pomocí komunikačního portu s řídící aplikací na připojeném počítači. Návrh krabičky probíhal v SW Fusion 360 který je pro nekomerční použití k dispozici zdarma. Následně byl návrh vložen do SW PrusaSlicer, ve kterém byly dodělány podpory a proveden export do G-code pro vytištění na 3D tiskárně. Tisklo se na tiskárně Prusa XL.

Obrázek 30. Prusa XL [36]

Obrázek 31. Návrh krabičky pohled 1



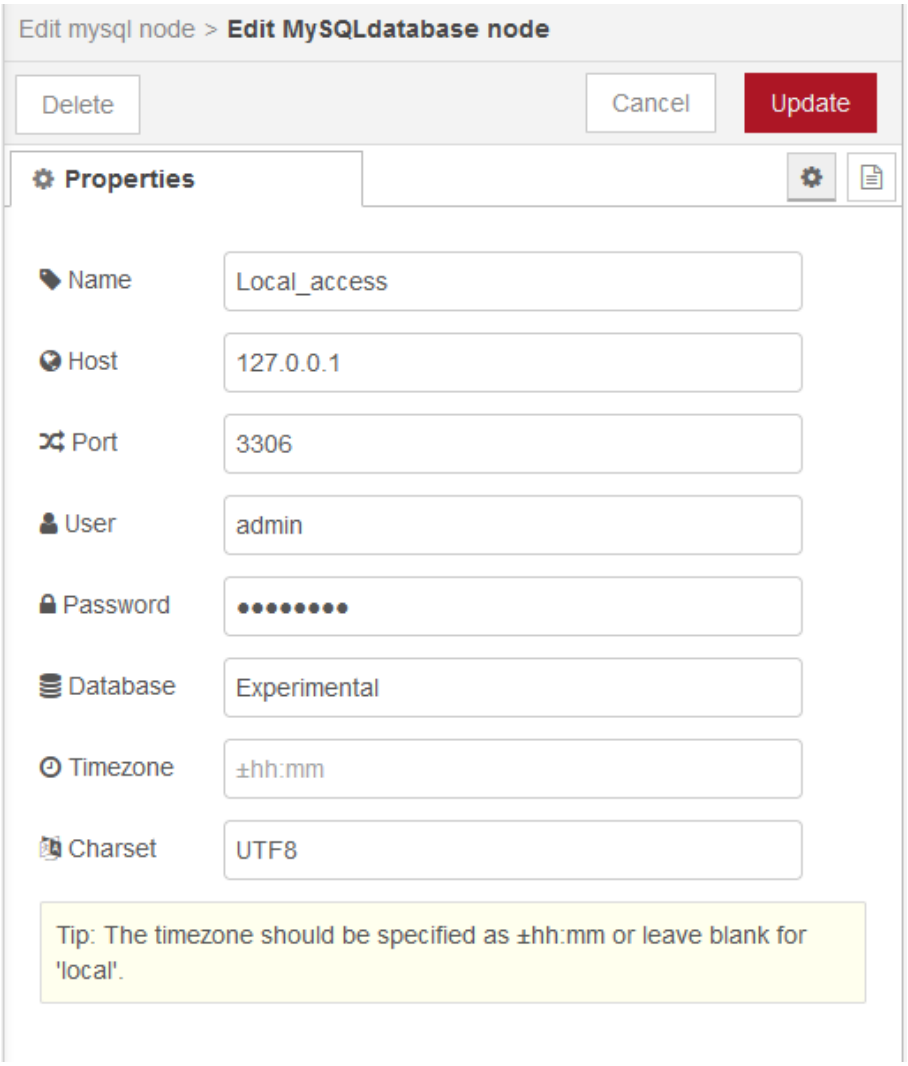
Obrázek 32. Návrh krabičky pohled 2

Obrázek 33. Fotografie výsledného tisku s osazenými moduly

7.1 Formát uživatelských dat a práce s nimi

Uživatelská data jsou uložena v SQL databázi. Databáze obsahuje jednu tabulku, ve které se nachází celkem pět sloupců. Tyto sloupce obsahují unikátní identifikátor v rámci tabulky, číselný kód daného uživatele, řetězec, který je uložený na přidělené identifikační kartě, identifikátor uživatele ze snímače otisků prstů, a nakonec jméno uživatele kterému daný záznam náleží. Pro potřeby experimentální sestavy nejsou jednotlivé položky šifrovány. Jedná se o vlastnost, která je daná možností sledování jednotlivých kroků během práce se sestavou.

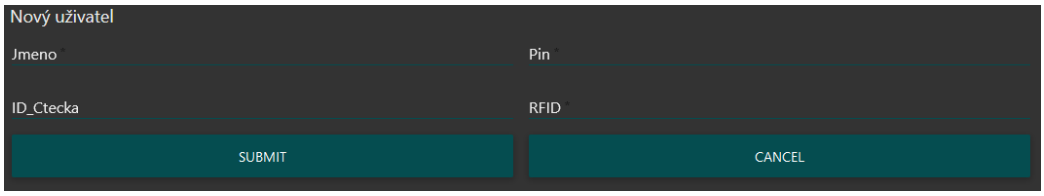
V prostředí Node Red je potřeba definovat údaje a parametry pro přístup k SQL databázi. Definování probíhá pomocí bloku SQL, ve kterém je adresa SQL serveru. V tomto případě je SQL služba spuštěna na stejném zařízení jako Node Red adresa je tedy localhost. Poté je použit výchozí port pro komunikaci a přihlašovací údaje k databázi s jejím názvem.



Obrázek 34. Fotografie výsledného tisku

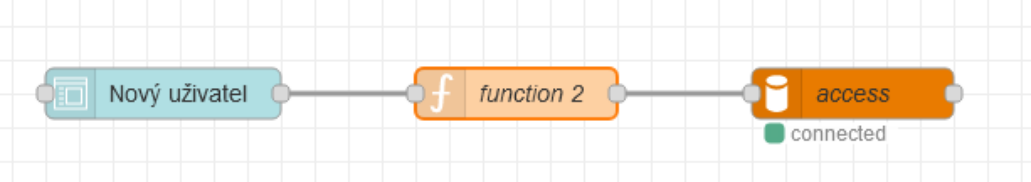
7.1.1 Vytvoření nového uživatele

Vytvoření nového uživatele probíhá z webového prostředí, které bylo vytvořeno pomocí Node Red a doplňku Dashboard. Od uživatele je přijat vstup ve formě výstupu z formuláře. Do formuláře jsou vyplněny údaje o uživateli, jako jeho jméno, číselný kód, řetězec uložený na identifikační kartě a případně identifikační číslo, pod kterým je uživatel veden v pamětí snímače otisků prstů.

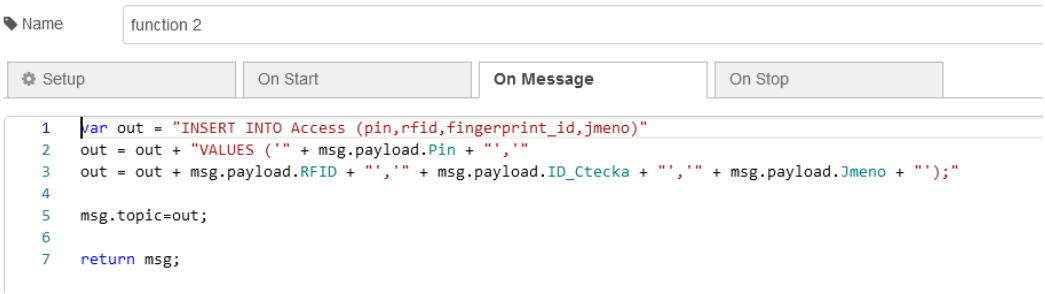


Obrázek 35. Formulář vložení nového uživatele

V rámci Node Red je procedura vytvoření nového uživatele implementována pomocí bloku formuláře. Kdy je výstup přiveden na vstup funkce pro vytvoření SQL dotazu, který je předán na samotnou databázi.



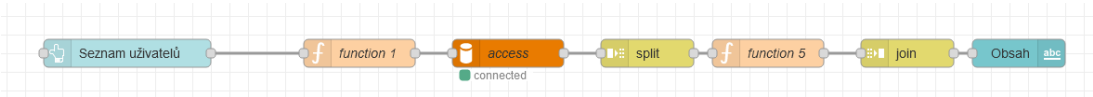
Obrázek 36. Node Red bloky vytvoření nového uživatele



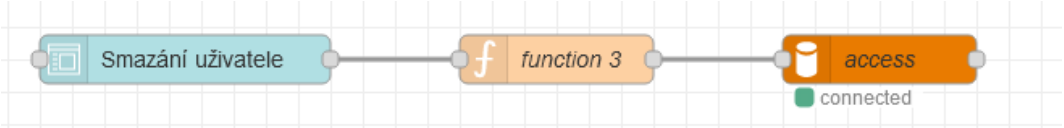
Obrázek 37. zpracování dat a vytvoření SQL dotazu pro vložení do databáze

7.1.2 Zobrazení uživatelů a Smazání existujícího uživatele

Na webové stránce je k dispozici možnost vypsání všech uživatelů, kteří jsou uloženi v databázi. Jedná se o zobrazení jejich unikátního identifikátoru tak jejich jména. V případě, že existuje více stejných jmen, je rozlišovací znak jejich identifikační číslo. Jedná se o inkrement, kdy první uživatelé mají číslo blíže k nule a u novějších uživatelů se identifikační číslo od nuly vzdaluje.



Obrázek 38. Node Red bloky pro vypsání uživatelů a jejich ID

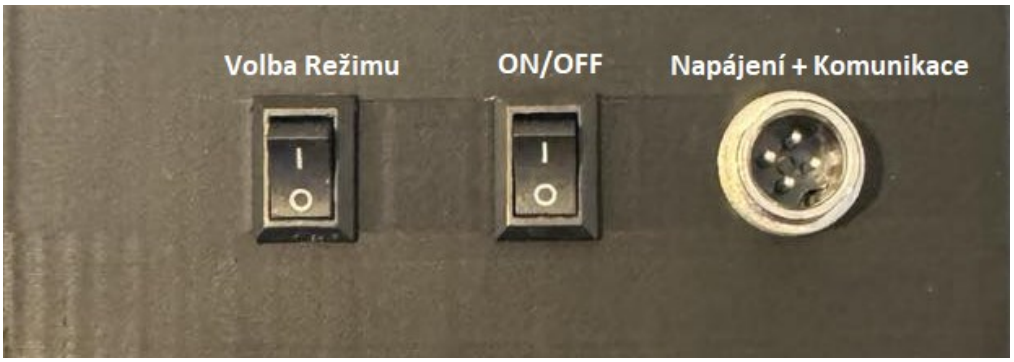


Obrázek 39. Node Red bloky pro smazání uživatele

8 OVĚŘENÍ FUNKCE SESTAVY

8.1 Seznámení s ovládacími prvky sestavy

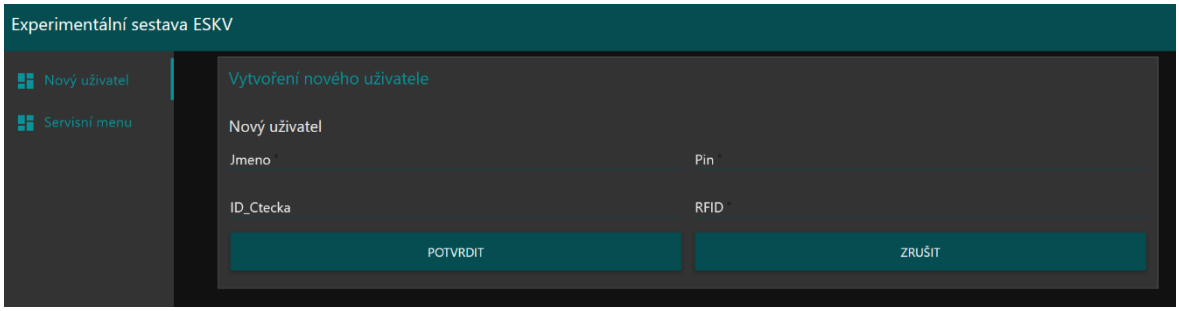
Experimentální sestava je vybavena komunikačním konektorem, který zároveň slouží pro její napájení. Vedle něj se nachází vypínač napájení, který slouží pro zapnutí nebo vypnutí napájení sestavy. Posledním ovládacím prvkem je přepínač režimů zařízení. Měnit režimy je možno jak při vypnutém, tak zapnutém stavu. Kromě těchto ovládacích prvků je na zařízení pouze k dispozici membránová klávesnice (RFID ani DY-50 nedisponují ovládacími prvky), klávesy * a # slouží jako reset resp. potvrzení zadání a jednotlivé klávesy reprezentují stejné znaky.



Obrázek 40. Ovládací prvky sestavy

8.2 Seznámení s webovým prostředím

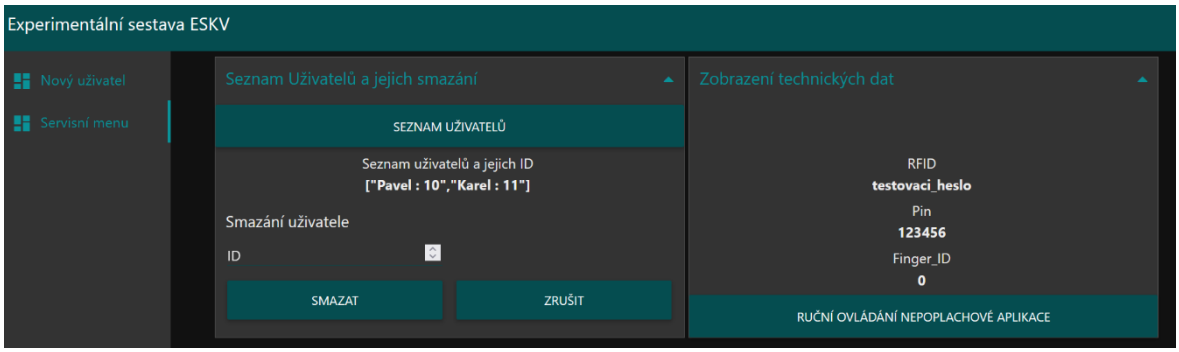
Webové prostředí je minimalistické a skládá se ze dvou záložek. První – výchozí záložka slouží pro vytvoření nového uživatele. Po vyplnění údajů uživatele a jejich potvrzení dojde k přidání uživatele do databáze.



Obrázek 41. Ovládací prvky sestavy

Druhá záložka nese název Servisní menu. V této záložce je možné zobrazit seznam uživatelů v databázi spolu s jejich ID. Pomocí tohoto ID je také možnost smazat uživatele z databáze.

Dále se zde nachází položka Zobrazení technických dat, kde se zobrazují přijaté údaje ze sestavy a také je zde tlačítko pro ruční ovládání nepoplachové aplikace.



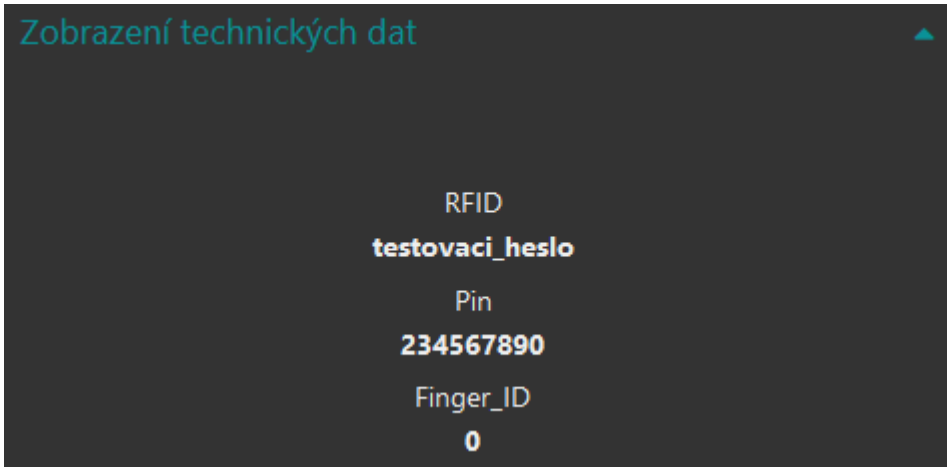
Obrázek 42. Ovládací prvky sestavy

8.3 Ověření komunikačního režimu 0

Pro ověření funkce je nejdříve nutné vyzkoušet správnou funkci jednotlivých modulů. V případě modulu klávesnice stačí vyzkoušet všechny čísla a provést potvrzení. Tím je ověřena funkce jednotlivých kláves, jejich pořadí a také potvrzovací tlačítko. Pro vyzkoušení tlačítka pro smazání stiskneme např. první klávesu poté reset a pokračujeme dále. Po přijetí by mělo první tlačítko být vynecháno. Ověření provádíme v servisním menu. V části Zobrazení technických dat. Tímto je tlačítková klávesnice ověřená a můžeme ji prohlásit za funkční.

Ověření správné funkce čtečky RFID karet je provedeno podobně. Použitím dvou RFID tagů, kdy alespoň na jednom jsou uloženy nějaká data. Po přečtení by se načtená hodnota měla zobrazit ve stejné sekci u hodnoty RFID. Tímto jsme ověřili funkci čtečky a můžeme ji prohlásit za funkční.

Ověření správné funkce snímače otisků prstů provedeme obdobně, vyzkoušíme nasnímat otisk uživatele, který je uložený ve vnitřní paměti zařízení a v položce Finger_ID by se mělo zobrazit ID ze čtečky. V případě otisku, který není ve čtečce nebude provedena žádná změna.



Obrázek 43. Načtené údaje z jednotlivých modulů.

Po ověření funkce jednotlivých částí je možné provést ověření funkce duální verifikace.

V databázi vytvoříme uživatele, který bude mít přiřazenu RFID kartu, zvolí si PIN a nasnímáme jeho otisk prstu do snímače DY-50. Uživatel má tedy k dispozici PIN, ID kartu a nahraný otisk pro přístup. Zároveň je k dispozici nepoplachová aplikace (světlo), které bude signalizovat úspěšný přístup. Budeme ověřovat všechny kombinace přístupových metod. Jednotlivé kombinace spolu s výsledkem jsou v tabulce 1.

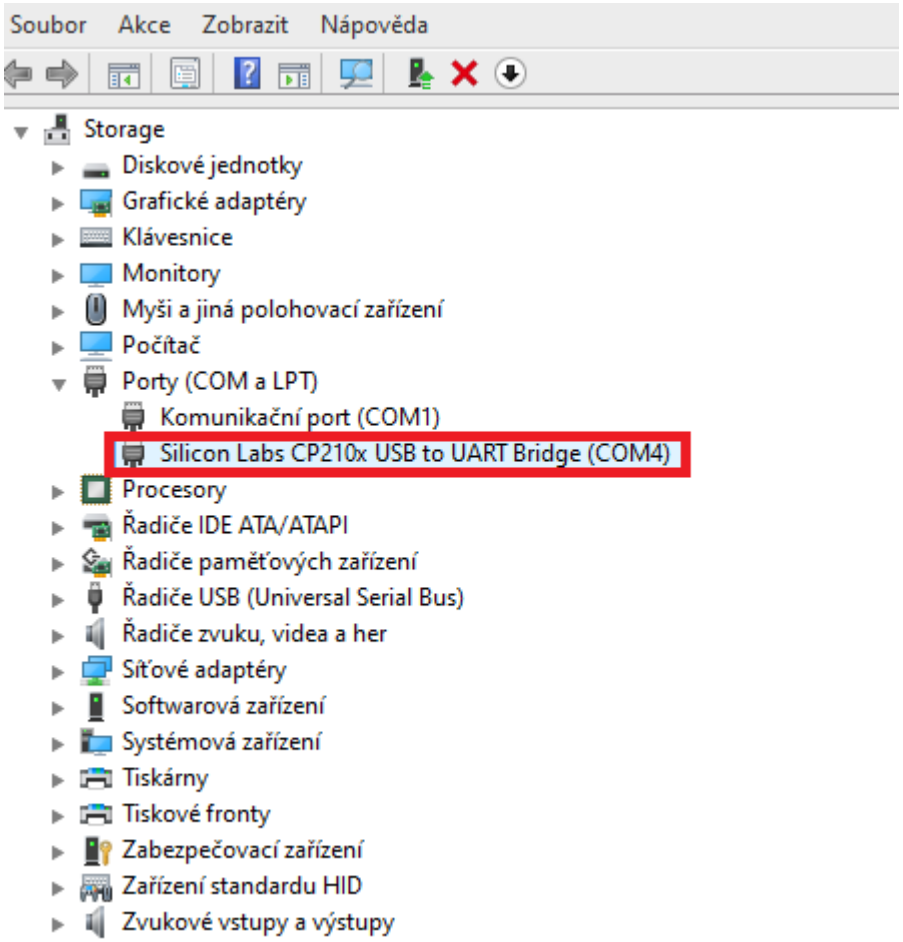
	PIN	RFID	Otisk
PIN	**Přístup nepovolen**	**Přístup povolen**	**Přístup povolen**
RFID	**Přístup povolen**	**Přístup nepovolen**	**Přístup povolen**
Otisk	**Přístup povolen**	**Přístup povolen**	**Přístup nepovolen**

Tabulka 1. Kombinace přístupových metod

Z tabulky 1. lze vyčíst, že sestava umožnila přístup při jakékoliv kombinaci přístupové metody. Přístup byl zamítnut pouze v případech, kdy byla použita stejná metoda dvakrát. Toto chování je korektní a na základě tohoto ověření funkčnosti můžeme konstatovat, že experimentální sestava splňuje požadované funkce. Ověření proběhlo také pomocí karty jiného uživatele, kdy systém korektně vyhodnotil nesoulad v identitě a přístup nebyl umožněn.

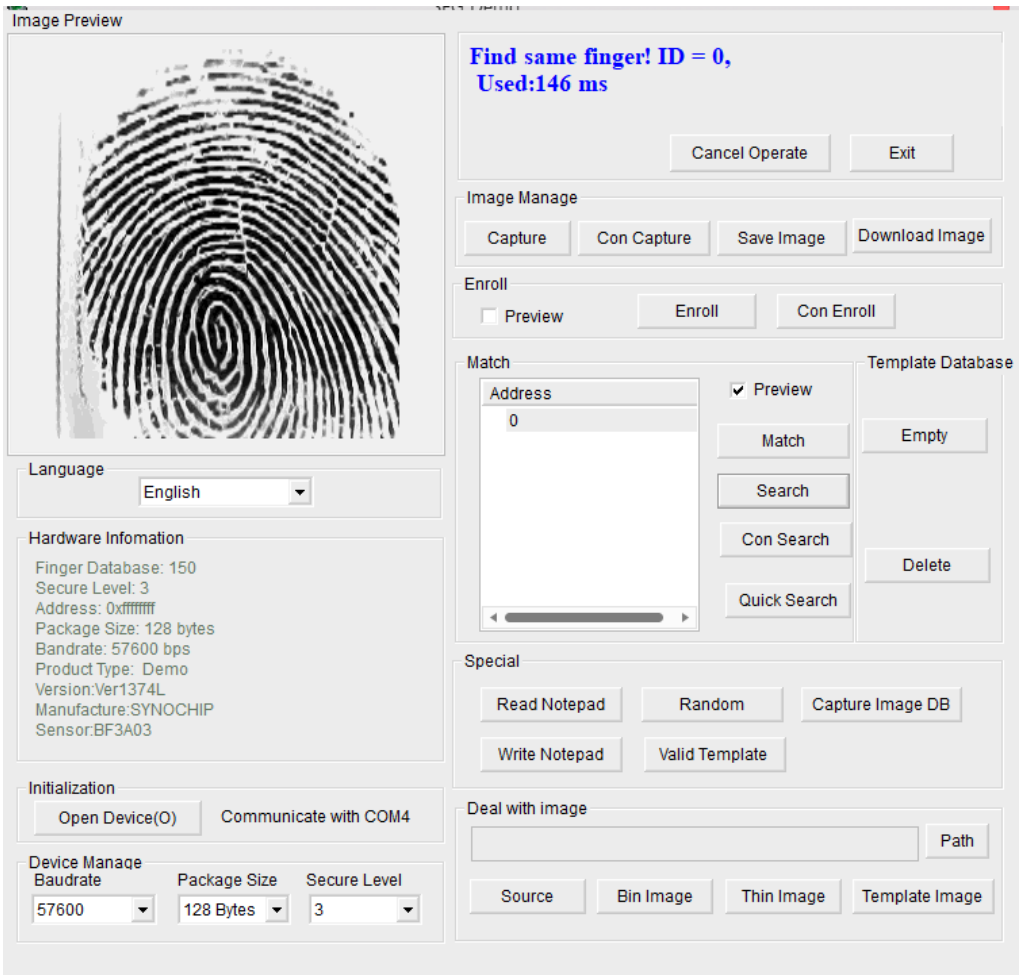
8.4 Ověření komunikačního režimu 1 (DY50 - PC)

Nejprve je potřeba na zařízení přepnout přepínač režimů na pozici 1, poté připojit sestavu k PC pomocí USB kabelu. Na PC ve správci zařízení pod položkou COM porty najít který COM port má sestava přiřazen. V tomto případě se jedná o COM4.



Obrázek 44. Správce zařízení

Otevřeme aplikaci pro obsluhu snímače otisků – SFG Demo. Otevřeme komunikaci na COM portu, na kterém je zařízení připojeno a potvrdíme. Po úspěšném připojení ke snímači dojde k načtení informací o snímači jako takovém spolu se známými otisky. Pro vložení nového záznamu stačí kliknout na tlačítko **Enroll** a zvolit ID nového uživatele. Poté uživatel přiloží požadovaný prst na snímač a postupuje podle instrukcí. Aplikace umožnuje kromě vložení nového uživatele jeho vyhledání v databázi, popřípadě ověření konkrétního záznamu. Mimo to je také možné smazat jednotlivé záznamy nebo celou databázi. Aplikace umožnuje také další funkce pro práci se snímačem. Tyto funkce jsou více popsány v uživatelském manuálu na stránkách vydavatele aplikace.



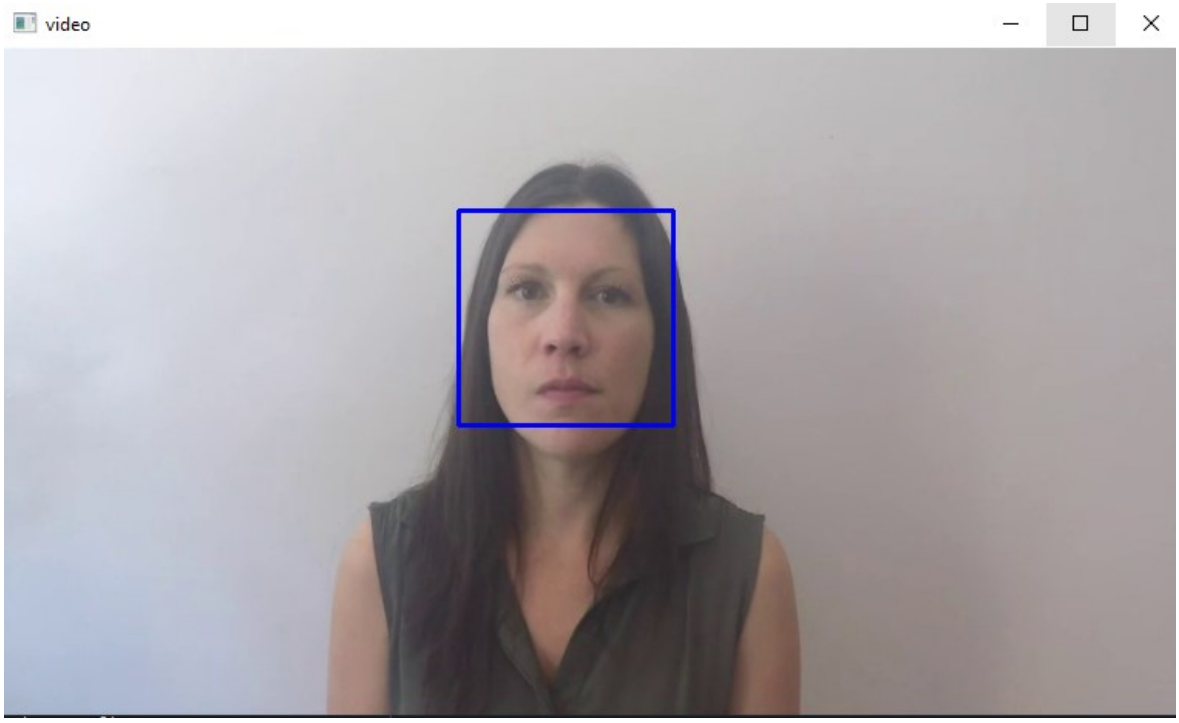
Obrázek 45. Aplikace SFG s připojeným snímačem.

Ověřením funkčnosti základních funkcí, byla zjištěna funkčnost této části experimentální sestavy. Během ověření se neprojevila žádná chyba nebo nežádoucí chování sestavy.

8.5 Ověření detekce a rozpoznání obličeje

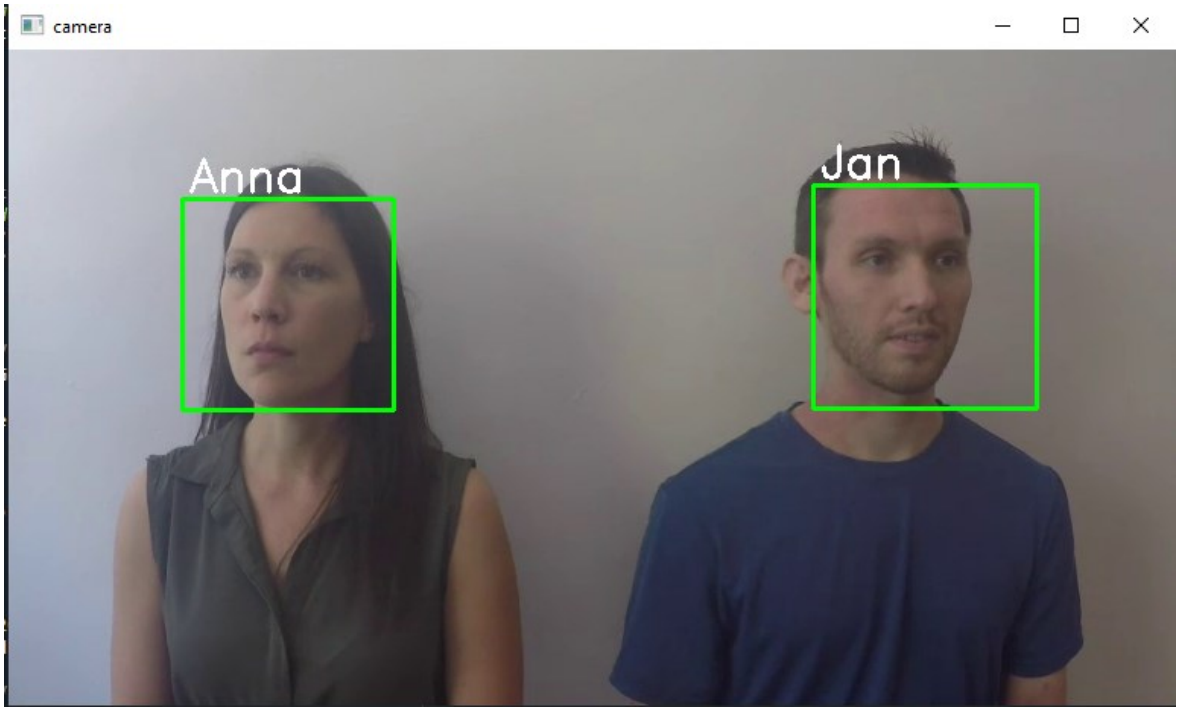
Pro ověření funkce rozpoznání obličeje, byly vybrány ukázkové soubory z projektu Intel IoT DEVKIT, které jsou dostupné pod licencí CC-BY-4.0 [32]

Detekce obličeje byla zkoušena na ukázkových videích a také na výstupu z webkamery. Když kamera zachytávala obraz obličeje z předního pohledu došlo k vykreslení ohraničení kolem detekovaného obličeje. Pro vyzkoušení možnosti rozpoznání obličeje, byly zvoleny dvě jména, která byla přiděleny jednotlivým účastníkům na ukázkových videích. Jedná se o jména Jan a Anna pro dva herce, další dva herci nejsou do modelu zahrnuti, pro možnost ověření detekce bez možnosti shody.

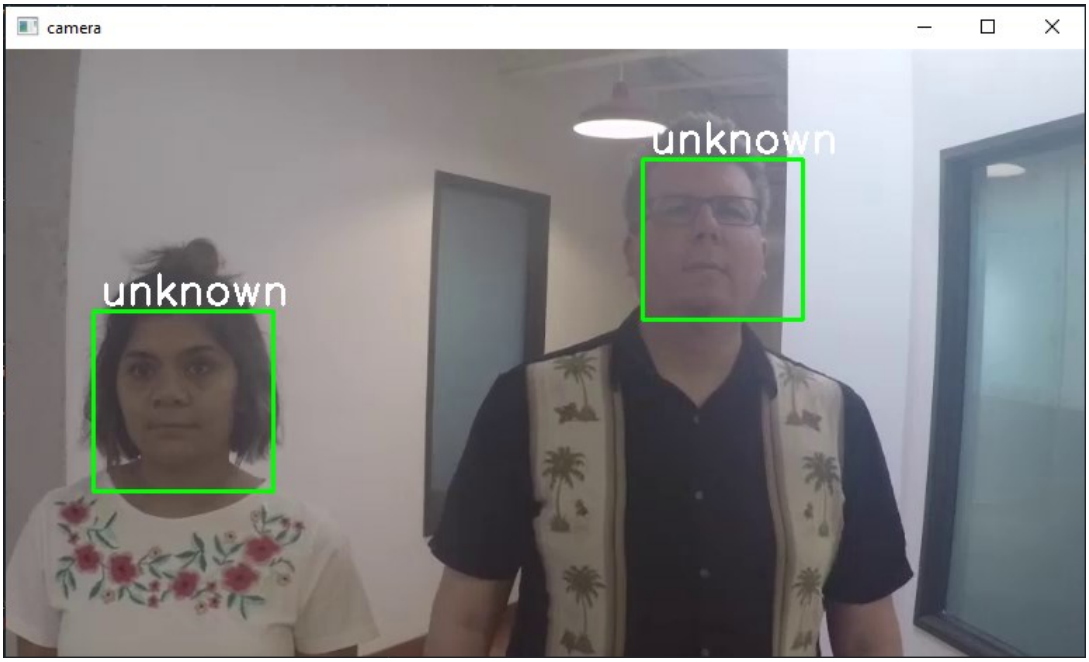


Obrázek 46. Detekce obličeje při vytváření modelu pro rozpoznání. [32]

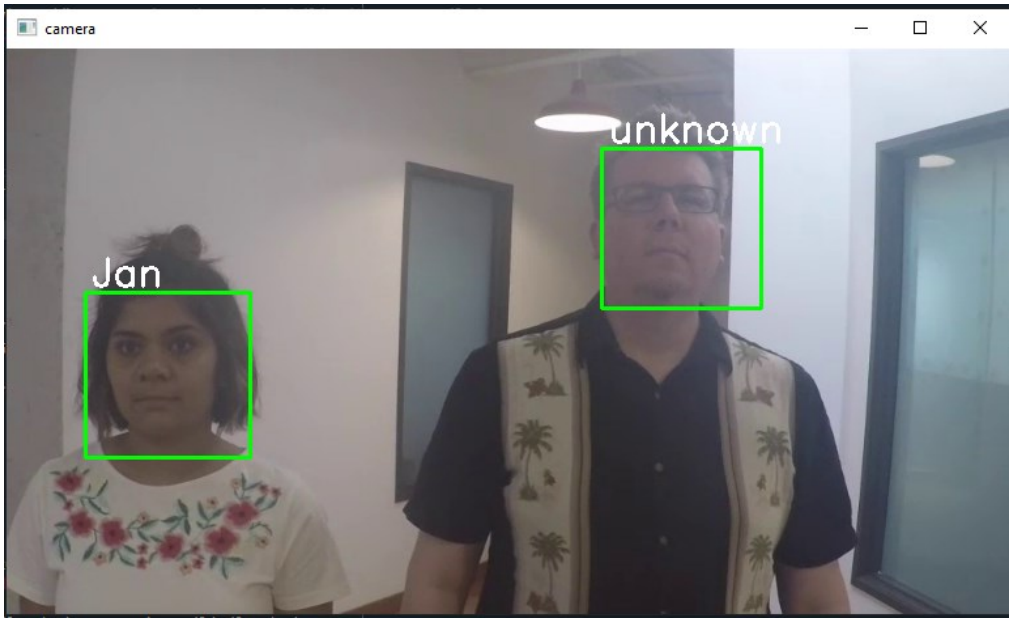
Po detekování samostatných herců a přidělení identifikačních čísel, bylo vyzkoušeno rozpoznání na jiném videu se stejnými herci. Jak je možné vidět na Obrátku 47. rozpoznání při dobrých světelných podmínkách funguje. Při pokusu o rozpoznání obličejů na jiných osobách, kde není nalezena shoda je zobrazeno označení unkown. V rámci testů při dobrých světelných podmínkách rozpoznání fungovalo dobře pouze při správném natočení obličeje vůči kameře. Při nevhodném natočení docházelo k falešnému rozpoznání, kdy byly jednotlivý uživatelé zaměnění mezi sebou, případně nedošlo k jejich rozpoznání.



Obrázek 47. Detekování obličeje – úspěšné rozpoznání se shodou. [32]



Obrázek 48. Detekování obličeje – úspěšné detekování bez shody. [32]



Obrázek 49. Detekování obličeje – špatné rozpoznání shody. [32]

ZÁVĚR

Cílem této diplomové práce bylo navržení experimentální sestavy, která zahrnuje prvky ESKV spolu s prvky VSS. Experimentální sestava obsahuje různé přístupové metody, jako klávesnice pro zadání číselného kódu, přístup pomocí identifikační karty a přístupu pomocí snímače biometrických dat – otisku prstu. Systém odesílá vstupní data od uživatele na server prostřednictvím Wi-Fi spojení. Na serveru dochází ke zpracování přijatých dat a ověření vůči databázi uživatelů pro ovládání nepoplachové aplikace. Na serveru běží kromě samotné databáze a zpracování přijatých dat, také webová služba. Webová služba umožnuje přidávat nové uživatele do databáze, případně mazat staré uživatele z databáze. Také umožnuje provedení výpisu uživatelů databáze a jejich unikátního identifikačního čísla. Mimo experimentální sestavu je práce doplněna o dvě aplikace v jazyce Python využívající knihovnu OpenCV, které slouží pro detekci a záznam obličeje. Kdy je nasnímán obličej, kterému je přiřazeno interní identifikační číslo. Při detekci obličeje je pořízeno několik snímků, tyto snímky jsou použity pro vytvoření modelu pro rozpoznání obličeje. Druhá aplikace využívá modelu pro rozpoznání obličeje, kdy vyhledává v obraze obličej a porovnává jej s modelem. V případě, že nalezne dostatek shodných rysů mezi obrazem a modelem přiřadí obličeji ID, které odpovídá shodnému ID v modelu. Podle tohoto ID je přiřazeno jméno uživatele, které je následně zobrazeno v okně přehrávajícího video/stream. Celá experimentální sestava je osazena v krabičce, která je vytištěna na 3D tiskárně. Po sestavení experimentální sestavy bylo provedeno ověření funkce jednotlivých částí, poté bylo provedeno ověření celkové funkce zařízení a vyzkoušeny různé kombinace přístupu, viz. Tabulka 1. Sestava v rámci přístupových metod byla v rámci testů funkční. Aplikace pro detekci a rozpoznání obličeje fungovala omezeně a s mírnou chybovostí.

SEZNAM POUŽITÉ LITERATURY

[1] *Formáty a rozlišení videa*. Online. C2010-2015. Dostupné z: https://av-navody.cz/?sekce=vrch_jaknaav-formatrozliseni. [cit. 2024-05-14].

[2] *Rozlišení 4K (Ultra HD): Vše, co potřebujete vědět*. Online. In: Rozlišení 4K (Ultra HD): Vše, co potřebujete vědět. 2020. Dostupné z: https://www.alza.cz/rozliseni-4k-ultrahd-art7638.htm. [cit. 2024-05-14].

[3] *ISO Explained in Detail – the Light Sensitivity of Cameras*. Online. C2024. Dostupné z: https://www.ifolor.ch/en/inspire/iso-explained-in-detail-the-light-sensitivity-of-cameras. [cit. 2024-05-14].

[4] PRATZNER, Felix. *The objective of a digital camera*. Online. 2021. Dostupné z: https://www.photocourse.info/the-objective-of-a-digital-camera.php. [cit. 2024-05-14].

[5] *Ohnisková vzdálenost*. Online. In: Moje.tajemno.net/. 2015. Dostupné z: https://moje.tajemno.net/ohniskova-vzdalenost/. [cit. 2024-05-14].

[6] *What is a High Frame Rate Camera? What are the Factors Affecting Frame Rate?* Online. C2001-2022. Dostupné z: https://www.technexion.com/resources/what-is-a-high-frame-rate-camera-what-are-the-factors-affecting-frame-rate/. [cit. 2024-05-14].

[7] SYDNEY, Roy. *Frame Rate: A Beginner's Guide for Live Streaming (Update)*. Online. In: Wowza.com. 2023. Dostupné z: https://www.wowza.com/blog/frame-rate-beginners-guide-live-streaming. [cit. 2024-05-14].

[8] KRISHNAN, Vignesh. *A Detailed Overview Of Popular Video Compression Techniques*. Online. 2023. Dostupné z: https://imagekit.io/blog/video-compression-techniques/. [cit. 2024-05-14].

[9] *Bezztrátový vs ztrátový obraz*. Online. In: Differbetween.com. 2015. Dostupné z: https://cs.differbetween.com/article/lossless_vs_lossy_image. [cit. 2024-05-14].

[10] *Funkce kamer*. Online. C2024. Dostupné z: https://www.ascz.cz/funkce-kamer-3/. [cit. 2024-05-14].

[11] *Umělá inteligence povyšuje funkci kamer na druhou*. Online. 2023. Dostupné z: https://retailnews.cz/2023/10/18/umela-inteligence-povysuje-funkci-kamer-na-druhou/. [cit. 2024-05-14].

[12] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management*. Zlín: Radim Bačuvčík - VeRBuM, 2015. ISBN 978-80-87500-57-6.

[13] ČSN EN 60839-11-1. Poplachové a elektronické bezpečnostní systémy - Část 11-1: Elektronické systémy kontroly vstupu - Požadavky na systém a komponenty. Praha: Český normalizační institut, 2014.

[14] SEMERA, Lukáš. *Daktyloskopie - historie , současnost a budoucnost*. Online, Diplomová Práce. Praha: Univerzita Karlova v Praze, 2015. Dostupné z: https://dspace.cuni.cz/bitstream/handle/20.500.11956/66042/DPTX_2013_1_11220_0_281952_0_142897.pdf?sequence=1&isAllowed=y. [cit. 2022-12-19].

[15] *Dermatoglyphics-and-Malocclusion-A-Forensic*. Online. In: Semanticscholar.org. 2016. Dostupné z: https://www.semanticscholar.org/paper/Dermatoglyphics-and-Malocclusion-A-Forensic-Link-Bhasin-Bhasin/7ecf4bf36b9bbfa319c3678afe3cf6a9e854a7c2/figure/0. [cit. 2024-05-14].

[16] *Otisk prstu*. Online. C2023. Dostupné z: https://www.safyid.com/otisk-prstu/. [cit. 2024-05-15].

[17] *Jak fungují RFID čtečky*. Online. C20210-2023. Dostupné z: https://esp.cz/cs/blog/funguji-rfid-ctecky. [cit. 2024-05-14].

[18] *Analysis of bit error rate performance of active and passive RFID communication systems with diversity*. Online. In: Semanticscholar.org. 2015. Dostupné z: https://www.semanticscholar.org/paper/Analysis-of-bit-error-rate-performance-of-active-Mahmud/41eef687b7d962618861e66366e80fb8b17f5982/figure/4. [cit. 2024-05-20].

[19] *Esp-32-wroom-32*. Online. Espressif.com. Shanghai: espressif, c2022. Dostupné z: https://www.espressif.com/sites/default/files/documentation/esp32-wroom-32_datasheet_en.pdf. [cit. 2022-05-05].

[20] *ESP-32 pinout*. Online. In: Random Nerd Tutorials. Lisabon: randomnerdtutorials, [2018]. Dostupné z: https://randomnerdtutorials.com/esp32-pinout-reference-gpios/. [cit. 2022-05-17].

[21] *Interfacing-4x3-membrane-matrix-keypad-with-arduino*. Online. In: Electropeak.com. 2020. Dostupné z: https://electropeak.com/learn/interfacing-4x3-membrane-matrix-keypad-with-arduino/. [cit. 2024-05-14].

[22] *RFID čtečka RC522*. Online. In: Rpishop.cz. C2024. Dostupné z: https://rpi-shop.cz/rfid/1327-rfid-ctecka-rc522.html?gad_source=1&gclid=CjwKCAjwl4yyB-hAgEiwADSEjeC-v8ZFO94k94XGOwjTivipJi3oDPX2S_qnez9Xqsxxw14PNPdFV2RoCTPYQAvD_BwE. [cit. 2024-05-14].

[23] *Snímač otisků prstů s pamětí DY50*. Online. In: Laskakit.cz. C2024. Dostupné z: https://www.laskakit.cz/snimac-otisku-prstu-s-pameti-dy50/?gad_source=1&gclid=CjwKCAjwl4yyBhAgEiwADSEjeIMOxoI-c-9WblaeqRyrKa_6sxeKlHzsdnkTXjPuZXg00KD6DDso2xoCrJkQAvD_BwE. [cit. 2024-05-14].

[24] ČSN EN 50398-1 (334597) Poplachové systémy - Kombinované a integrované poplachové systémy - Část 1: Obecné požadavky (2018)

[25] *Shelly Plug*. Online. In: Heureka.cz. C2007-2024. Dostupné z: https://zasuvky-pro-chytrou-domacnost.heureka.cz/shelly-plug/#prehled/. [cit. 2024-05-14].

[26] *API pro zařízení Shelly*. Online. Shelly-api-docs.shelly.cloud. C2024. Dostupné z: https://shelly-api-docs.shelly.cloud/gen1/#shelly1-1pm-status. [cit. 2024-05-16].

[27] *Dokumentace k OpenCV*. Online. 2024. Dostupné z: https://docs.opencv.org/4.x/. [cit. 2024-05-14].

[28] *Cascade Classifier*. Online. In: Docs.opencv.org. 2024. Dostupné z: https://docs.opencv.org/3.4/db/d28/tutorial_cascade_classifier.html. [cit. 2024-05-14].

[29] GEVORGYAN, Menua; MAMIKONYAN, Arsen a BEYELER, Michael. OpenCV 4 with Python Blueprints: Build creative computer vision projects with the latest version of OpenCV 4 and Python 3. Second Edition. Packt Publishing, 2020. ISBN 978-178980-181-1.

[30] HOWSE, Joseph; MINICHINO, Joe. Learning OpenCV 4 Computer Vision with Python 3: Get to grips with tools, techniques, and algorithms for computer vision and machine learning. Packt Publishing Ltd, 2020.

[31] *Opencv-detectmultiscale-minneighbors-parameter*. Online. In: Stackoverflow.com. 2014. Dostupné z: https://stackoverflow.com/questions/22249579/opencv-detectmultiscale-minneighbors-parameter. [cit. 2024-05-14].

[32] https://github.com/intel-iot-devkit/sample-videos?tab=CC-BY-4.0-1-ov-file

[33] *ESP-MQTT*. Online. Docs.espressif.com/. Shanghai: espressif, c2016-2022. Dostupné z: https://docs.espressif.com/projects/esp-idf/en/latest/esp32/api-reference/protocols/mqtt.html. [cit. 2022-05-16].

[34] MALÝ, Martin. *Protokol MQTT: komunikační standard pro IoT*. Online. In: Root. Praha 6: root.cz, [2016]. Dostupné z: https://www.root.cz/clanky/protokol-mqtt-komunikacni-standard-pro-iot/. [cit. 2022-05-17].

[35] *Node-Red Dokumentace*. Online. OpenJS Foundation and Node-RED contributors, [2021]. Dostupné z: https://nodered.org/docs/. [cit. 2022-05-05].

[36] *Prusa XL*. Online. In: Richvalsky.cz. C2024. Dostupné z: https://www.richvalsky.cz/3d-tiskarna-original-prusa-xl-s-peti-nastrojovou-hlavou--slozena-a-sestavena/. [cit. 2024-05-14].

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AD	Analog Digital
AI	Artificial Intelligece
API	Application Programming Interface
AR	Rozšířená realita
BLE	Bluetooth Low Energy
DA	Digital Analog
DIY	Do It Yourself
ESKV	Elektronický Systém Kontroly Vstupu
FPS	Frames Per Second
FW	Firmware
GPIO	General Purpose Input/Output
HD	High-Definition
HF	High Frequency
HW	Hardware
ID	Identifikace
IoT	Internet of Things
IP	Internet Protocol
JSON	JavaScript Object Notation
LBP	Local Binary Patterns
LF	Low Frequency
MCU	Micro Controller Unit
MQTT	Message Queuing Telemetry Trans – port
NFC	Near Field Communication
OpenCV	Open Computer Vision

PC	Personal Computer
PIN	Personal Identification Number
QoS	Quality of Service,
RFID	Radio Frequency Identification
SD	Standard Definition
SPI	Serial Peripheral Interface
SQL	Structured Query Language
SW	Software
UART	Universal Asynchronous Receiver/Transmitter
UHD	Ultra High-Definition
UHF	Ultra High Frequency
URL	Uniform Resource Locator
USB	Universal Serial Bus
VSS	Video Surveillance Systems
WiFi	Wireless Fidelity

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

Příloha P1 - CD

Obsah CD:

- Program pro detekci obličeje s vytvořením modelu pro rozpoznání v jazyce Python.
- Program pro rozpoznání obličeje z modelu v jazyce Python.
- Doprovodné soubory pro Python (kaskádový filtr pro detekci).
- .STP a .STL soubory krabičky pro 3D tiskárnu .
- Zdrojový soubor s FW pro ESP-32.
- Použité knihovny pro ESP-32.
- Vzorové videosoubory použité pro detekci.
- Videosoubor s ukázkou prostředí aplikace SFG.
- Videosoubor s ukázkou funkce detekce a rozpoznání obličeje.
- Videosoubor s ukázkou funkce sestavy v prostředí Node Red.
- Aplikace pro obsluhu snímače DY-50 pomocí PC – SFGDemoV2.0.
- Vyexportovaný obsah z prostředí Node Red.