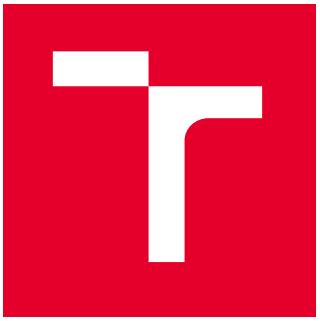


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ

DEPARTMENT OF TELECOMMUNICATIONS

LABORATORNÍ ÚLOHA SYSTÉMU BIOMETRICKÉ KONTROLY VSTUPU

LABORATORY EXERCISE OF THE BIOMETRIC ACCESS CONTROL SYSTEM

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **Jakub Volf**
AUTHOR

VEDOUCÍ PRÁCE — **doc. Ing. Karel Burda, CSc.**
SUPERVISOR

BRNO 2023

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní program **Informační bezpečnost**

Ústav telekomunikací

Student: Jakub Volf ***ID:*** 222277

Ročník: 3 ***Akademický rok:*** 2022/23

NÁZEV TÉMATU:

Laboratorní úloha systému biometrické kontroly vstupu

POKYNY PRO VYPRACOVÁNÍ:

Nastudujte a popište problematiku systémů biometrické kontroly vstupu. Následně zpracujte detailní popis a provozní možnosti dodaných komponent. Z těchto komponent navrhněte a prakticky zrealizujte systém kontroly vstupu v podobě výukového panelu. Pro navržený systém zpracujte laboratorní úlohu a technickou dokumentaci. V laboratorní úloze se studenti mají seznámit s konfigurací a s provozem vytvořeného systému. U konfigurace se požaduje možnost správy systému z biometrické čtečky i ze správního počítače a to jak přes webový prohlížeč, tak i přes specializovaný software. Správní počítač má mít podobu virtuálního počítače na platformě VMware. Z hlediska provozu výukového systému se požaduje možnost autentizace osob geometrií obličeje, otiskem prstu i kartou.

DOPORUČENÁ LITERATURA:

DOPORUČENÁ LITERATURA:

[1] Burda K.: Základy elektronických zabezpečovacích systémů. CERM, Brno 2018.

[2] -: DS-K1T671 Series Face Recognition Terminal - User Manual. Hikvision, Hangzhou 2020.

Termín zadání: 6.2.2023 ***Termín odevzdání:*** 26.5.2023

Vedoucí práce: doc. Ing. Karel Burda, CSc.

doc. Ing. Jan Hajný, Ph.D.
předseda rady studijního programu

ABSTRAKT

Tato práce se zabývá tématem biometrické kontroly vstupu. V teoretické části práce je nejprve popsána elektronická kontrola vstupu obecně a posléze samotná kontrola vstupu na základě biometrických rysů člověka. Okrajově je zmíněna legislativa a vývoj zastoupení biometrické kontroly na trhu. V rámci praktické části je na základě dodaných komponent navržen a vyroben panel. Na panelu jsou umístěny jednotlivé komponenty a zapojeny dle manuálu. Tento celek tak tvoří funkční systém pro biometrickou kontrolu vstupu, který bude využit jako jedna z laboratorních úloh do výuky. Pro účely laboratorní úlohy je sepsán postup laboratorní úlohy pro studenta a dokumentace pro vyučujícího k obsluze tohoto systému.

KLÍČOVÁ SLOVA

biometrická kontrola vstupu, geometrie obličeje, laboratorní úloha, otisk prstu, terminál

ABSTRACT

This thesis deals with the topic of biometric access control. The theoretical part of the thesis first describes electronic access control in general, followed by access control based on human biometric traits. Legislation and the development of biometric control representation in the market are briefly mentioned in this work. Based on the provided components, a panel is designed and manufactured in the practical part. The individual components are implemented in the panel and connected according to the manual. This assembly thus forms a functional system for biometric access control, which will be used as one of the laboratory tasks in educational classes. There is a written method, based on the laboratory task, specifically designed for student and a documentation for the teacher on how to operate this system.

KEYWORDS

biometric access control, facial geometry, fingerprint, laboratory exercise, terminal

VOLF, Jakub. *Laboratorní úloha systému biometrické kontroly vstupu*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2023, 61 s. Bakalářská práce. Vedoucí práce: doc. Ing. Karel Burda, CSc.

Prohlášení autora o původnosti díla

Jméno a příjmení autora:	Jakub Volf
VUT ID autora:	222277
Typ práce:	Bakalářská práce
Akademický rok:	2022/23
Téma závěrečné práce:	Laboratorní úloha systému biometrické kontroly vstupu

Prohlašuji, že svou závěrečnou práci jsem vypracoval samostatně pod vedením vedoucí/ho závěrečné práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené závěrečné práce dále prohlašuji, že v souvislosti s vytvořením této závěrečné práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

podpis autora*

*Autor podepisuje pouze v tištěné verzi.

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu bakalářské práce panu doc. Ing. Karlu Burdovi, CSc. za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Obsah

Seznam obrázků

Úvod

V dnešní době se lidé potýkají s problémem konvenčního zabezpečení vstupu do kontrolovaných oblastí. Dnešní standardní zabezpečení bývá pomocí hesla či různé číselné kombinace. Zabezpečení provází člověka odjakživa a hledáním a aplikací nových metod zabezpečení přispívá k ochraně nejen člověka, ale i budov, zařízení a citlivých informací. Díky potenciálu dnešních technologií existují možnosti zabezpečení i jinými způsoby, které jsou mnohdy bezpečnější a využívají i biometriky člověka.

Hlavním cílem bakalářské práce je navržení laboratorní úlohy systému biometrické kontroly vstupu. Ke splnění hlavního cíle práce byly stanoveny dílčí cíle teoretické a praktické části. Mezi dílčí cíle teoretické části se řadí objasnění a přiblížení problematiky elektronické kontroly vstupu v závislosti na biometrických systémech. Význam těchto dílčích cílů spočívá v zasazení architektury, principu fungování a rozboru typů autentizace elektronické kontroly vstupu. Zakončení teoretické části je věnované stručnému nastínění vývoje zastoupení biometrické autentizace na trhu, legislativního rámce a normám ČSN, dle kterých se biometrické systémy navrhují. Mezi dílčí cíle praktické části se řadí návrh panelu, jeho výroba, osazení komponenty, následné zpracování samotné laboratorní úlohy ve formě postupu pro studenta a dokumentace pro vyučujícího. Tyto dílčí cíle mimo jiné pokrývají výkresovou dokumentaci, popis hardwarových a softwarových komponentů a bližší popis laboratorní úlohy. Metody zpracování bakalářské práce směřují k literární rešerši s prvky srovnávání a navrhování.

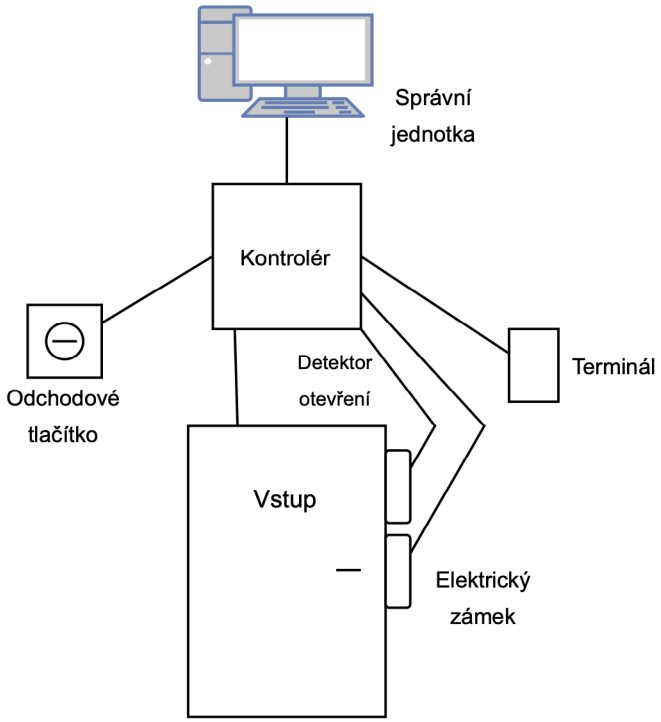
1 Systémy elektronické kontroly vstupu

Systémy pro elektronickou kontrolu vstupu (EKV) slouží k ochraně majetku a řízení přístupu pověřených osob v kontrolované oblasti na základě přístupových práv, které jsou jim předem přiděleny. Nahrazuje tak klasický klíčový systém, kdy klíč při jeho ztrátě či odcizení mohla využít neoprávněná osoba a vstoupit tak do zájmových prostor. Pokud dojde ke ztrátě prostředku, kterým se osoba prokazuje u systému EKV, lze v řídící jednotce lehce zamezit případnému zneužití identifikačního prostředku [2, 14].

1.1 Architektura systémů EKV

Mezi základní prvky systému EKV patří kontrolér, vstup, terminál a správní jednotka. Kontrolér je tzv. řídící jednotka celého přístupového systému. Vstup lze popsat jako uzavíratelný průchod, který je ovládán kontrolérem a slouží k zamezení průchodu nepovolaným osobám. Nejčastěji se jedná o dveře, které jsou opatřeny elektrickým zámkem. Terminál je zařízení, které umožňuje komunikaci osoby s přístupovým systémem. Mezi zařízení typu terminál můžeme považovat čtečku karet, čtečku biometriky, klávesnici pro vložení hesla, či kombinaci dvou zmíněných. Správní jednotka je zařízení, skrze které se ovládá a spravuje přístupový systém. Nejčastěji se jedná o počítač, na kterém je nainstalován software pro správu takového systému. Součástí prvků můžou být i detektor otevření a odchozí tlačítko. Detektor otevření detekuje neoprávněné otevření vstupu či stav, ve kterém není vstup uzavřen. Odchozí tlačítko se nachází v kontrolované oblasti a osoba jeho stisknutím požádá kontrolér o otevření vstupu, aby mohla opustit daný prostor. V některých případech může být odchozí tlačítko nahrazeno například detektorem PIR [3, 18].

Jednotlivé prvky jsou mezi sebou propojeny následujícím způsobem. Na řídící prvek celého systému, tedy kontrolér, jsou připojeny všechny ostatního prvky systému viz obrázek 1.1. Správní jednotka se na něj připojuje lokálně přes USB či RS-232 nebo vzdáleně přes LAN či sběrnici RS-485. Dále musí být správní jednotka připojena také k terminálu, nejčastěji přes LAN, aby mohl autentizovat ověřovací seznam. Co se týče dalších prvků, ty bývají připojeny dvoudrátovou smyčkou ke kontroléru [2, 3].



Obr. 1.1: Přístupový systém (vlastní zpracování)

1.2 Fungování systémů EKV

Nejprve vloží autorita prostřednictvím správní jednotky do systému přístupový a ověřovací seznam. Žadatel o přístup se autentizuje pomocí terminálu. Na základě prokázané identity kontrolér prověří, zda má žadatel nějaká práva, případně jaká, v přístupovém systému. Po vyhodnocení kontrolér vstup odemkne prostřednictvím elektrického otvírače, nebo ponechá vstup zamčený. V případě pokusu o násilné otevření vstupu či ponechání otevřeného vstupu tento stav rozpozná detektor otevření a spustí patřičné opatření, nejčastěji vyhlásí poplach. Odchozí tlačítko, jak již bylo zmíněno, se umisťuje v kontrolované oblasti na zdi a jeho použitím si osoba vyžádá o otevření vstupu [2, 3].

1.3 Typy autentizace

Autentizace neboli ověření identity žadatele se provádí při vstupu osoby do kontrolované oblasti. Žadatel o přístup se prokazuje tzv. nosičem dokazovacího faktoru, kterým může být autentizační předmět nebo žadatel samotný. Nosič dokazovacího faktoru obsahuje tzv. dokazovací faktor DF, kterým žadatel prokazuje svou identitu.

Mezi dokazovací faktory patří tajné informace, např. heslo, nebo unikátní charakteristické rysy žadatele či předmětu. Součástí přístupových systémů s výpočetně náročnou autentizací je na straně žadatele specializované zařízení, jež obtížný výpočet provádí a na autentizátor je na straně přístupového systému. V systémech s méně náročnou autentizací se je autentizátor součástí přístupové ústředny. Autentizátor disponuje tzv. ověřovacími faktory OF (např. hash hesla), kterým prostřednictvím autentizačního protokolu ověřuje, zda se žadatel o přístup prokazuje dokazovacím faktorem osoby, za kterou se vydává [5].

1.3.1 Autentizace heslem

Autentizace heslem spočívá ve znalosti žadatele určitého kódu, který je unikátní, nejčastěji posloupnost čísel nebo znaků a měl by ho znát pouze žadatel. Žadatel takové heslo zadává při autentizaci do přístupového terminálu na klávesnici ve správném pořadí. Dokazovací data DD, kterými je v tomto případě heslo, se porovnávají s ověřovacím faktorem OF. Kritérium pro úspěšnou autentizaci je DD = OF. Pokud je vyhodnoceno jako shodné, žadatel je úspěšně autentizován. V případě této autentizace zaniká potřeba nosit fyzický identifikační předmět, což snižuje náklady na pořízení a provoz takového přístupového systému. Mezi nevýhody patří například riziko odpozorování hesla útočníkem nebo zapomenutí hesla uživatelem [3, 13].

1.3.2 Autentizace průkazem

Žadatel o přístup se při autentizaci průkazem prokazuje nepadělatelným předmětem, na němž je uvedena jeho identita. Nejprve ověřovatel prostřednictvím ochranných prvků ověří, zda se nejedná o padělek. Pokud je předmět posouzen jako originál, tak je osoba autentizována a je jí umožněn přístup. U tohoto typu autentizace následující: DF = nepadělatelné ochranné prvky průkazu, OF = znalost ochranných prvků průkazu, kritérium úspěšné autentizace = průkaz není padělán ani modifikován. Mezi ochranné prvky využívající se u průkazů patří symboly viditelné pod UV světlem, hologramy atd. Výhodou tohoto typu autentizace je nepotřebnost jakékoliv techniky pro ověření DF, stačí pouze pověřená osoba. Jako velkou nevýhodu je důležité uvést riziko ztráty či krádeže průkazu a velké pořizovací náklady kvůli ochranným prvkům [3, 13].

1.3.3 Autentizace biometrikou

Tato metoda ověřuje charakteristické rysy osoby. Jedná se o morfologii osoby (např. obrazec papilárních linií) nebo chování osoby (např. způsob chůze). Není zde potřeba nosit fyzický identifikační předmět, nebo si pamatovat heslo. Tyto rysy jsou tak

unikátní a nelze je padělat. Z těchto důvodů je biometrika oblíbeným způsobem pro autentizaci osob. Podrobněji je tento typ autentizace popsán v kapitole 2 [3, 13].

1.3.4 Autentizace hardwarem

Autentizace hardwarem spočívá v autentizaci osoby pomocí paměťového úložiště nebo mikropočítače. Jako paměťové úložiště lze použít kartu s magnetickým proužkem, Wiegandovu kartu či RFID kartu. Mikropočítačem jsou pak smartphone nebo mikroprocesorová karta. Identifikační a autentizační údaje se na magnetické karty ukládají a čtou speciálními jevy souvisejícími s magnetismem. Příkladem takových karet jsou právě Wiegandovy karty a karty s magnetickým proužkem [3].

Karta s magnetickým proužkem

Informace sloužící k autentizaci se zapisují na magnetický pásek o velikosti 3 stop. Jednotlivé stopy se magnetizují po úsecích o délce Δ a $2*\Delta$. Tyto stopy lze nazvat jako ploché permanentní magnety, neboť jsou zmagnetizovány pouze jedním směrem. Sousedící magnety totožné stopy mají opačné směry magnetizace, to znamená, že po magnetu s orientací S-J (S = sever, J = jih) následuje vždy magnet s orientací J-S a naopak. Každý bit má ve stopě přidělen úsek o délce $2*\Delta$, jedná se tedy o bitový úsek. Nulový bit se kóduje jako jediný magnet o délce $2*\Delta$ a jedničkový bit je reprezentován dvojicí opačně orientovaných magnetů o délce Δ [3, 5].

Magnetický proužek na kartě protáhne žadatel o přístup v blízkosti čtecí hlavy. O bit 0 se jedná v případě, kdy napěťová špička způsobená rozhraním dvou magnetů je vzdálena úsek $2*\Delta$. Bit je 1 v případě, kdy je napěťová špička uprostřed úseku $2*\Delta$. Výhodami magnetických karet jsou nízká cena a spolehlivost. Nevýhodou je nedostatečná bezpečnost, jelikož jdou snadno duplikovat [3, 5].

Wiegandova karta

Wiegandova karta obsahuje dvě řady krátkých drátů o rozměrech 1 mm x 10 mm, které jsou do ní zataveny. Horní řada představuje bit 1 a spodní řada představuje bit 0. Každá karta disponuje jedinečnou posloupností 26 bitů, kterou se osoba zároveň identifikuje a autentizuje. Dráty jsou vyrobeny ze slitiny několika kovů a jádra s pláštěm drátu mají odlišnou magnetickou tvrdost [3, 5].

Čtení binární posloupnosti na Wiegandově kartě umožňuje tzv. Wiegandův jev. V klidovém stavu mají jádro a plášť stejný směr magnetizace. Prvním pohybem karty ve čtečce dojde k vystavení drátů silnému nastavovacímu magnetu, což způsobí přemagnetování jádra i pláště. Následným pohybem karty ve čtečce dojde k vystavení drátů překlápěcímu magnetu a jsou přemagnetována pouze jádra drátů. Čtečka Wiegandových karet obsahuje snímací cívku, která detekuje, ve které řadě se v daný

moment nachází drát. Tím je zjištěna celková posloupnost bitů dané karty. Výhodou je nízká cena a velmi obtížné pořízení duplikátu [3].

RFID karta

RFID kartu lze zjednodušeně popsat jako paměťové úložiště pro tajné Wiegandovo slovo WS. Mezi přední a zadní desku karty je zatavena cívka a čtečka obsahuje cívku druhou. Čtečka nepřetržitě vysílá signál o frekvenci f, který se indukuje v cívce karty. V případě RFID karet se jedná o kmitočet 125 kHz a pro bezdrátovou komunikaci mezi kartou a čtečkou využívá rozhraní podle standardu ISO 14443. Tento typ karet obsahuje EEPROM paměť, která umožňuje i zápis informace vedle klasického čtení informace. Moderní verze RFID karet disponují ochranou před neoprávněným čtením. To je dosaženo skrytím části paměti s Wiegandovým slovem a dostupností jen se znalostí tajného hesla. Nevýhodou je riziko odposlechu komunikace mezi kartou a čtečkou, tedy zjištění tajné hodnoty Wiegandova slova [3]. Mezi běžné problémy RFID karet lze zařadit chybné přenosy mezi čtečkou a kartou, riziko naklonování karty a potenciální zneužití tohoto klonu či mechanické poškození. V případě mechanického poškození karty okamžitě přestanou fungovat, a to z důvodu změny identifikace na specifické rádiové frekvenci [10]. Vzhled karty je k vidění na obrázku 1.2.

Obr. 1.2: RFID karta
(vlastní zpracování)

Mikroprocesorová karta

Mikroprocesorová karta je v principu samostatný počítač, ve kterém je dokazovací faktor bezpečně uložen a představuje jej klíč symetrického kryptosystému nebo soukromý klíč asymetrického kryptosystému. Kryptoprocesor provádí obtížné kryptografické výpočty, mezi které patří například generování dvojice veřejný a soukromý klíč. Mikroprocesorová karta se využívá za účelem zajištění maximální bezpečnosti [3, 18].

Smartphone

Smartphone neboli chytrý telefon je autentizační hardware, který denně využívá obrovské množství lidí. Právě proto z důvodu možnosti využít jej také jako autentizační hardware nabyl takové oblibě. Velký výkon smartphonů umožňuje provádět autentizaci na základě asymetrické kryptografie. Smartphone nabízí i další typy bezdrátových přenosových technologií, kterými je možné autentizaci provádět [3, 18].

Velmi oblíbeným rozhraním je NFC (Near field communication), jenž je rozšířením standardu ISO/IEC 14443. Další využívanou technologií je Bluetooth. Ta oproti NFC, které má dosah jen v řádech centimetrů, umožňuje autentizovat se na vzdálenost několika metrů. Jako příklad lze uvést situaci, kdy se terminál nachází až za překážkou v kontrolované oblasti a osoba se autentizuje na vzdálenost několika kroků před vstupem. Snižuje se tedy nebezpečí sabotáže terminálu [3].

2 Biometrické systémy EKV

Biometrika je charakteristický rys osoby, který odlišuje jednotlivce podle jejich morfologických (např. obličej) nebo behaviorálních (způsob chování) znaků. Biometriky se vyznačují svou unikátností pro každého jednotlivce a obtížným padělaním. Systémy EKV využívající biometrické metody k ověření identity žadatelů se nazývají biometrické přístupové systémy [5].

Biometrická autentizace je způsob ověření identity, kdy je samotná osoba, která požaduje přístup, považována za dokazovací faktor. Při žádosti o přístup jsou žadateli změřeny biometrické údaje (tzv. biometrický obraz). Autentizátor přístupového systému pak porovná tyto naměřené hodnoty s důvěryhodně získaným záznamem biometrických údajů žadatele (tzv. biometrický vzor). Pokud mají biometrický obraz a biometrický vzor dostatečnou vzájemnou podobnost, je identita osoby prokázána. Biometrický vzor vytváří autorita při autorizaci osoby [5].

2.1 Typy biometrické autentizace

Mezi typy biometrické autentizace lze zařadit veškeré unikátní biometrické prvky nacházející se na těle člověka. Mezi takové prvky lze zařadit:

- otisk prstu,
- cévní řečiště,
- rozpoznání obličeje,
- skenování duhovky,
- rozpoznání hlasu,
- DNA [5].

V závislosti na typu biometrické autentizace lze přiřadit dobu trvání vyhodnocení a případné autorizování požadavku. Vyhodnocení některých typů (např. otisk prstu, rozpoznání obličeje) je řádově v sekundách. Oproti tomu DNA se pohybuje řádově v dnech až týdnech. Z tohoto důvodu je nutné brát ohledy na konkrétní typy biometrické autentizace a v závislosti na potřebě ochrany vybrat správný typ biometrie [16].

2.1.1 Autentizace podle otisku prstu

Jednou z nejpoužívanějších biometrických metod autentizace je skenování otisků prstů. Tento typ autentizace je založen na jedinečných obrazcích utvářených papilárními liniemi na povrchu kůže prstů viz obrázek 2.1. Tyto obrazce jsou utvářeny střídáním vyvýšených linií (tzv. lišty) a snížených linií (tzv. rýhy). Pro jedinečnost otisků každé osoby se tak využívají v přístupových systémech [5, 14].

Obr. 2.1: Lidský otisk prstu (Zdroj: [20])

Ke snímání těchto obrazců se používá několik druhů snímačů: optické snímače, kapacitní snímače a ultrazvukové snímače. Každý typ snímače funguje na jiném principu a má své výhody i nevýhody [5].

Optické snímače skenují obrazec papilárních linií jako fotoaparát. Žadatel o přístup položí svůj prst na stěnu optického hranolu, který je nasvícen světelným zdrojem. Pokud fotony dopadajícího světla dopadnou na místo, kde se papilární lišta dotýká stěny hranolu, tkáň prstu fotony pohltí. Pokud naopak fotony dopadajícího světla dopadnou na místo, kde se nachází rýha, jsou odraženy směrem k obrazovému snímači. Tento obrazový snímač (nejčastěji CCD nebo CMOS snímač) vytvoří z fotonů, které byly odraženy, obrazec papilárních linií. Výhodou tohoto druhu snímače jsou levné náklady na pořízení a jeho odolnost. Nevýhodou je potřeba udržovat snímač čistý, protože v případě špinavého snímače či prstu nedojde k autentizování osoby a zanechaný mastný otisk může být využit k oklamání systému [5, 14].

Kapacitní snímače zkoumají papilární linie měřením kapacity. Kapacitní snímače obsahují velmi drobné vodivé destičky, které jsou uspořádány matice a zality do plátu. Dvě vedle sebe sedící destičky jsou deskou kondenzátoru, kterému se měří kapacita. V místě, kde se po přiložení prstu nachází papilární lišta, sníží se kapacita mezi vodivými destičkami. V místě, kde se po přiložení prstu nachází papilární rýha, kapacita mezi vodivými destičkami vzroste. Výhodou tohoto druhu snímače je bezproblémová autentizace osoby, která se autentizovala špinavým prstem. Nevýhodou je riziko poškození snímače elektrostatickým výbojem [5, 14].

Ultrazvukové snímače zkoumají papilární linie prostřednictvím pulzů. Piezoelektrický krystal, který je umístěn pod snímací destičkou, vysílá a přijímá ultrazvukové pulzy. Snímaná plocha se skládá z bodů, do kterých jsou vysílány velmi krátké akustické pulzy. Krystal vysílá pulzy směrem k destičce. Část vlnění se odrazí zpět od spodní části destičky a přijímač rozpozná první odraz. Část vlnění, která nebyla odrazena, projde skrz materiál destičky až do místa horní plochy destičky. V tomto místě, kde se nachází rozhraní dvou odlišných prostředí, vznikne druhý

odraz, jenž je opět rozpoznán přijímačem. V případě výskytu papilární lišty ve snímaném bodě dojde k pohlcení vlnění tkání prstu a nejde k dalšímu odrazu. Pokud se v místě snímaného bodu vyskytuje papilární rýha, tak vlnění postupuje až do bodu, kdy se dotkne kůže prstu. V tomto bodě je uskutečněn třetí odraz, přijímač jej opět detekuje a zbylé vlnění je pohlceno tkání prstu. Kombinací mnoha odrazů po celé ploše snímací destičky je vytvořen papilární obrazec prstu žadatele o přístup. Ultrazvukové snímače mají vyšší pořizovací náklady, avšak odpadá potřeba čistit snímač či se autentizovat čistým prstem. Poškození systému elektrostatickým výbojem taktéž nehrozí [5, 14].

Následně po získání biometrického obrazce z otisku prstu žadatele je obrazec zpracováván. Zpracování spočívá v hledání útvarů zvaných markanty a jejich porovnání s markanty v dříve uloženém biometrickém vzoru. Markaty lze popsat jako útvary v obrazci papilárních linií, které jsou od sebe lehce rozpoznatelné. Těchto útvarů je několik variant, např. jádro, rozdvojení, konec linie atd. Na základě míry shody právě získaných markantů a markantů ze vzoru se rozhoduje o potvrzení nebo zamítnutí identity žadatele [5, 14].

2.1.2 Autentizace podle cévního řečiště prstu/dlaně

Tato metoda autentizace zkoumá cévní řečiště prstu a dlaně osob. Cévní řečiště je shluk cév, kterými proudí krev. Žadatel o přístup vloží prst do komůrky, kde je vyzařováno infračervené záření. Poté je prst vyfotografován kamerou, jež funguje v IR spektru. Fotony záření jsou pohlceny hemoglobinem vyskytujícím se v lidské krvi, tím pádem jsou na fotografii cévy tmavší barvy oproti okolní tkáni. Následným digitálním zpracováním fotografie je tento rozdíl navýšen. Výsledný obraz cév je porovnán s obrazem cév na biometrickém vzoru a je rozhodováno o potvrzení či zamítnutí identity žadatele. Stejným způsobem jako u prstu se provádí autentizace cévního řečiště u dlaně či hřbetu ruky, jelikož tam také proudí cévy v určitém shluku a hemoglobin pohlcuje fotony [4, 5].

2.1.3 2D autentizace podle obličeje

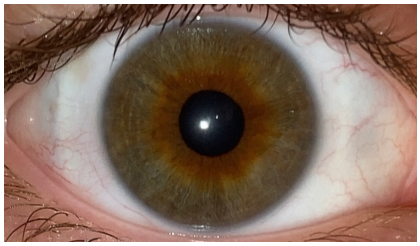
Tento způsob autentizace se provádí kamerou s dostatečným rozlišením. Žadatel o přístup si nejprve nechá vyfotografovat obličej. Následně se pořízený obraz obličeje zpracovává. Metodou obličejové metriky se najdou v obraze významné body (např. špička nosu, kraje očí či úst) a změří se mezi nimi vzdálenost. Naměřené vzdálenosti se porovnají se vzdálenostmi u biometrického vzoru a rozhodne se, zda je žadatel autentizován či nikoliv. Z důvodu snadného oklamání systému fotografií či videem je tento způsob autentizace nespolehlivý. Proto vznikly čtečky pro 3D autentizaci obličeje viz 2.1.4 [4, 5].

2.1.4 3D autentizace podle obličeje

3D autentizace obličeje stejně jako předchozí způsob autentizace spočívá v měření vzdálenosti mezi významnými body. Z důvodu odlišných zakřivení objektu se fotony odráží v různých úhlech, což způsobí deformaci obrazu obličeje. Obličej žadatele je při autentizaci nasvícen pravidelným rastrem složeným z několika desítek tisíc bodů. Nasvícení obličeje se provádí IR zářením odolným proti špatným světelným podmínkám. Odraz paprsků od obličeje způsobí nepravidelnost bodů rastru. Nepravidelnosti odraženého rastru se vyhodnotí a dojde k vytvoření 3D modelu obličeje žadatele, na kterém se změří vzdálenosti mezi významnými body. Naměřené hodnoty se porovnají s hodnotami z biometrického vzoru a žadatel je buď úspěšně, nebo neúspěšně autentizován [4, 5].

2.1.5 Autentizace duhovkou

Autentizace duhovkou spočívá v porovnávání u každého jedince odlišného rozmístění a tvaru skvrn vyskytujících se na duhovce oka. Terminál opatřený kamerou vyfotografuje oči žadatele o přístup a z pořízené fotografie vytvoří biometrický obrazec duhovky žadatele. Biometrický obrazec je poté porovnán s předem vytvořeným biometrickým vzorem. Stejně jako u autentizace otiskem prstu se vyhodnocuje míra shody a podle ní je identita žadatele potvrzena nebo zamítnuta [5]. Na obrázku 2.2 je vidět fotografie lidského oka.

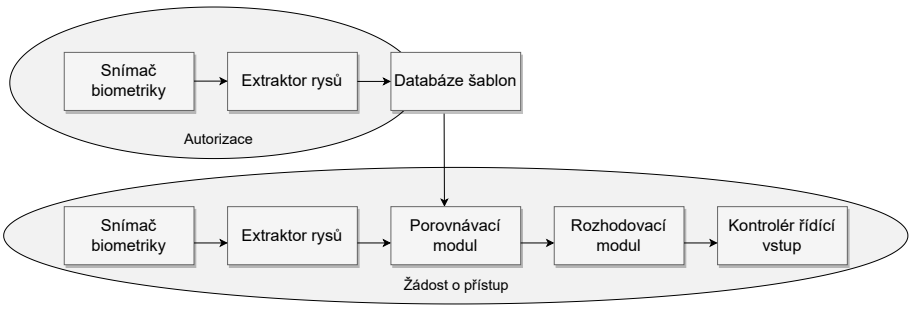


Obr. 2.2: Duhovka lidského oka
(vlastní zpracování)

2.2 Vlastnosti biometrické autentizace

Při autorizaci žadatele změří autorita biometrické údaje žadatele a uloží je do databáze šablon. Při žádosti o přístup se znovu změří biometrické údaje žadatele a porovnají se se šablonou uloženou v databázi. Pokud je míra shody dostatečně velká,

žadateli je umožněn přístup [4]. Schéma řízení přístupu pomocí biometriky je k vidění na obrázku 2.3.



Obr. 2.3: Schéma řízení přístupu pomocí biometriky (vlastní zpracování)

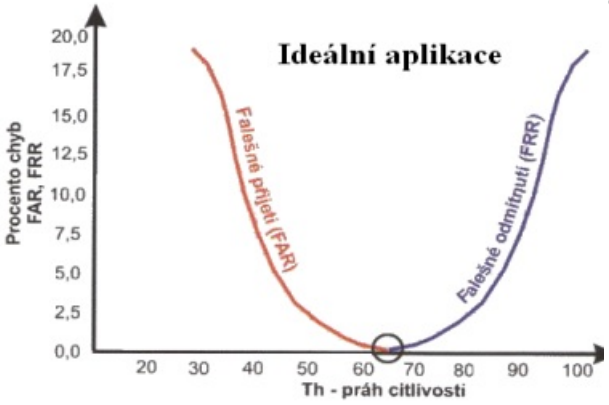
2.2.1 Přesnost biometrické autentizace

Tak jako u jiných bezpečnostních systémů může dojít i u biometrických systémů k chybám při ověření identity osoby. Může dojít ke dvěma chybným případům: chybné odmítnutí autentizované osoby nebo naopak její chybné přijetí. Hodnoty chybného odmítnutí a chybného přijetí se udávají jako relativní míra vzhledem k celkovému počtu pokusů o autentizaci. Jsou označovány jako míra chybného odmítnutí (FRR – False Rejection Rate) a míra chybného přijetí (FAR – False Acceptance Rate). Parametry FRR a FAR je možné hodnotit spolehlivost autentizačního systému a srovnávat jednotlivé systémy mezi sebou. Takovéto hodnocení lze provést na základě hodnot viz tabulka 2.1.

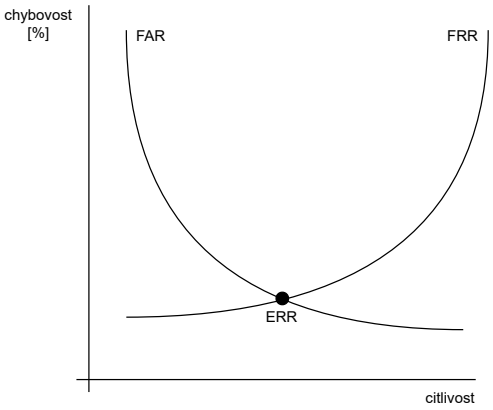
Tab. 2.1: Typické hodnoty FAR a FRR pro jednotlivé autentizační metody založené na typu biometriky (Zdroj: [1, 15])

Název biometriky	**FRR**	**FAR**	**Čas verifikace**
Otisk prstu	0,5%	0,01%	0,2 - 1 sekunda
Sken obličeje	14%	0,01%	3 sekundy
Otisk ruky	10%	0,05%	1 - 3 sekundy
Sken sítnice	10%	0,0001%	2 sekundy
Na základě chůze	3%	3%	-
Na základě psaní	10%	10%	-

Hodnoty FRR a FAR se mění na základě nastavení parametrů autentizační metody, ale vždy platí, že zvýšení FRR vyvolá zmenšení FAR a naopak. Stav, ve kterém jsou obě hodnoty FRR a FAR stejné, se nazývá EER (Equal Error Rate) [1]. Graf těchto hodnot se nachází na obrázku 2.5. Na obrázku 2.4 je znázorněna ideální aplikace k porovnání vůči reálnému vztahu FRR a FAR.



Obr. 2.4: Graf ideálního vztahu FRR a FAR (Převzato z: [18])



Obr. 2.5: Graf reálného vztahu FRR a FAR (Převzato a upraveno z: [1])

2.2.2 Výhody a nevýhody biometrické autentizace

Největší výhodou biometrické autentizace je její vysoká bezpečnost, kterou lze zvýšit pouze vícefaktorovým ověřováním. Jako vícefaktorové ověření lze považovat kombinaci dvou a více biometrických autentizací. Biometrické ověřování je velmi rychlý a efektivní proces. Mimo jiné přináší komfort a uživatelskou přívětivost, jelikož se po uživateli nevyžaduje zapamatování si hesla či potřebu nosit nějaké fyzické tokeny [9]. Z toho vyplývají následující výhody:

- Biometrické rysy jsou nedílnou součástí osoby, není tedy potřeba nosit cokoliv dalšího u sebe.
- Postupem času roste na popularitě, protože se jedná o moderní a uživatelem lehce ovládaný způsob zabezpečení.
- Rychlost a efektivita autentizace [4].

Mezi nevýhody biometrických údajů lze zařadit finanční náročnost, nemožnost dodat vždy stejný vzorek pro kontrolu či hygienické aspekty terminálů ověřující právě biometrické údaje. Dále se naráží na úskalí kompromitace biometrických údajů. V případě kompromitace těchto údajů je velmi náročné biometrické údaje změnit či aktualizovat. Další limity vychází z etických, náboženských či sociálních důvodů.

Mimo jiné je nutné zohledňovat legislativu a normy ČSN [9, 16, 19]. Shrnutím z toho vyplývají následující nevýhody:

- Biometrická ochrana je obvykle nákladná.
- Nikdy není 100% shodnost aktuálně sejmuté biometriky s biometrikou změřenou při autorizaci (např. nečistý prst, razantní změna vzhledu, tlak/poloha prstu při měření). Je nutné tedy akceptovat menší odchylky.
- Riziko padělání (např. kopie otisku prstu) [4].
- Legislativní rámec [19].

2.2.3 Útoky na biometrickou autentizaci

Systémy na bázi biometrické autentizace využívající fyziologické a behaviorální znaky jsou v dnešní době čím dál populárnější. S tím přichází i větší riziko napadení nějakým druhem útoku na tyto biometrické zabezpečení [12]. Možné způsoby útoků na systém biometrické autentizace:

- podvrh biometrického objektu (např. kopie otisku prstu),
- použití starých dokazovacích dat (záznam z dřívější autentizace),
- úprava extraktoru (např. úprava programu),
- použití starých dat z extraktoru,
- úprava bloku porovnání,
- úprava záznamu v databázi,
- úprava přenášené šablony,
- změna výsledku [4].

Mimo zmíněné způsoby útoků lze útoky dělit i na přímé a nepřímé. Přímé útoky jsou založeny na principu neznalosti modelu algoritmu, který je využíván pro autentizaci. Jako takový útok lze považovat například falešný prst imitující otisk prstu pro obelstění vyhodnocovacího algoritmu. Obdobně lze uvažovat nad imitací obličeje. Nepřímé útoky jsou založeny na znalosti identifikačního systému, a to konkrétně na znalosti modelu vyhodnocovacího algoritmu [12].

2.3 Legislativní rámec a normy ČSN

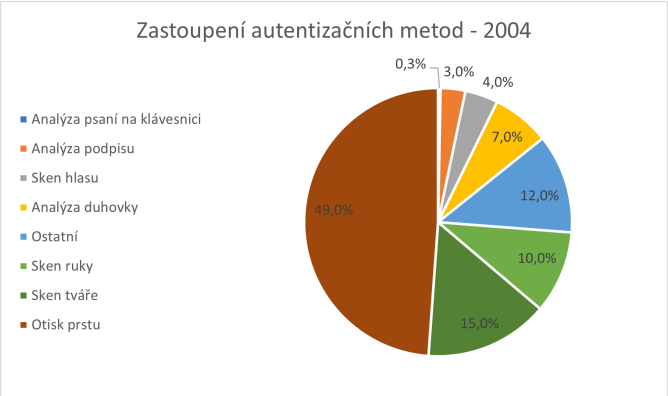
Do roku 2019 se v České republice uplatňoval zákon č. 101/2000 Sb. o ochraně osobních údajů, který v § 4 písm. b) určil biometrický údaj jako citlivý, v případě, že *„umožňuje přímou identifikaci nebo autentizaci subjektu údajů“* [8]. Tento zákon byl dne 24.04.2019 zrušen a nahrazen zákonem č. 110/2019 Sb. o zpracování osobních údajů, který vznikl na základě nařízení Evropského parlametu a Rady (EU)

2016/679. V tomto zákoně je biometrický údaj ukotven v § 66 odst. 6 [7]. Škop pojednává o zřízení speciální technické komise ISO/IEC JTC 1 *Information technology* obsahující subkomise pro jednotlivé obory IT. Mezi těmito subkomisemi existuje i subkomise SC 37 *Biometrics*, která zpracovává tvorbu norem a dokmumentů v této oblasti. Mezi takové normy a dokumenty se řadí:

- ČSN ISO/IEC 2382-37 *Informační technologie – Slovník – Část 37: Biometrika*;
- ČSN ISO/IEC 19785-2 *Informační technologie – Společný rámec formátů biometrické výměny – Část 2: Postupy pro činnost Biometrické registrační autority*;
- ČSN ISO/IEC 19785-4 *Informační technologie – Společný rámec formátů biometrické výměny – Část 4: Specifikace formátu bezpečnostního bloku*;
- ČSN ISO/IEC 19794 *Informační technologie – Formáty výměny biometrických dat*;
- ČSN ISO/IEC 19795 *Informační technologie – Testování a hodnocení výkonnosti biometrik*;
- ČSN ISO/IEC 30107 *Informační technologie – Detekce biometrického prezentačního útoku* [19].

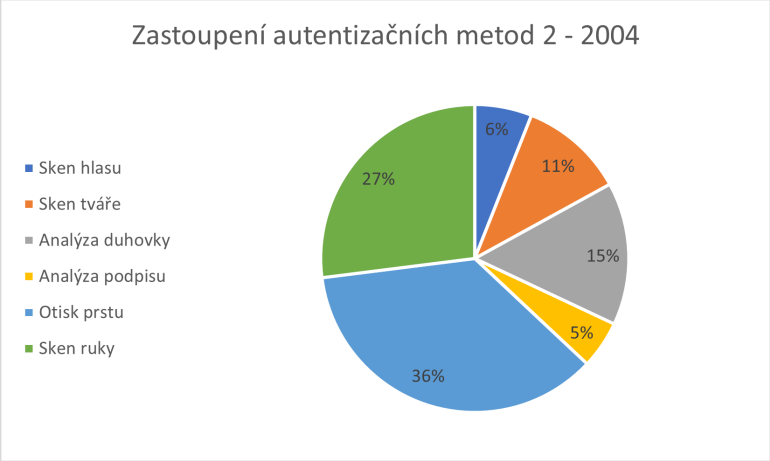
2.4 Vývoj zastoupení biometrické autentizace na trhu

Biometrická autentizace, jak je již zmíněno výše, je nejoptimálnějším způsobem autentizace z hlediska bezpečnosti. Z tohoto důvodu je tohle odvětví na trhu velmi průbojné s meziročním růstem více než 25 %. Velikost trhu s biometrikou byla dle Vaňka v roce 2010 až 4,2 miliardy USD. V roce 2015 pak 11,3 miliardy USD [21]. Zastoupení jednotlivých metod biometrické autentizace od roku 2004 je značně



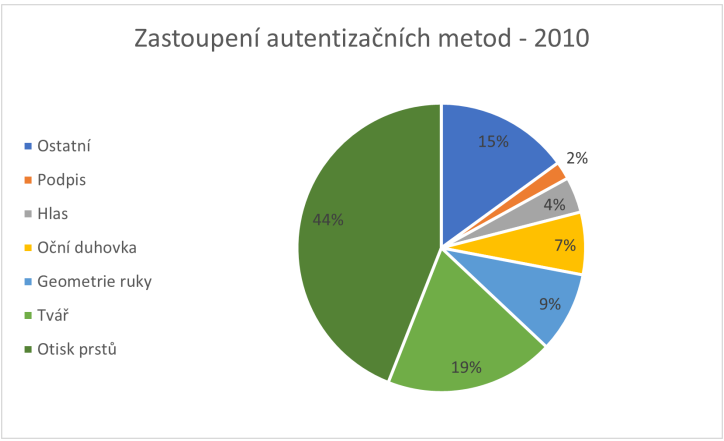
Obr. 2.6: Zastoupení autentizačních metod v roce 2004 (Převzato a upraveno z: [1])

proměnlivé viz porovnání grafů na obrázcích 2.6, 2.7 a 2.8. Z grafu vyobrazeného na obrázku 2.6 znázorňující zastoupení autentizačních metod v roce 2004 je zřejmé, že dominující všem biometrickým identifikačním systémům je otisk prstu. Zbylé metody jsou méně rozšířené, druhou nejčastěji používanou metodou je rozpoznávání tváře [1]. Graf z jiného zdroje, znázorněn na obrázku 2.7, podepírá otisk prstu jako nejčastěji používaný biometrický autentizační prvek.



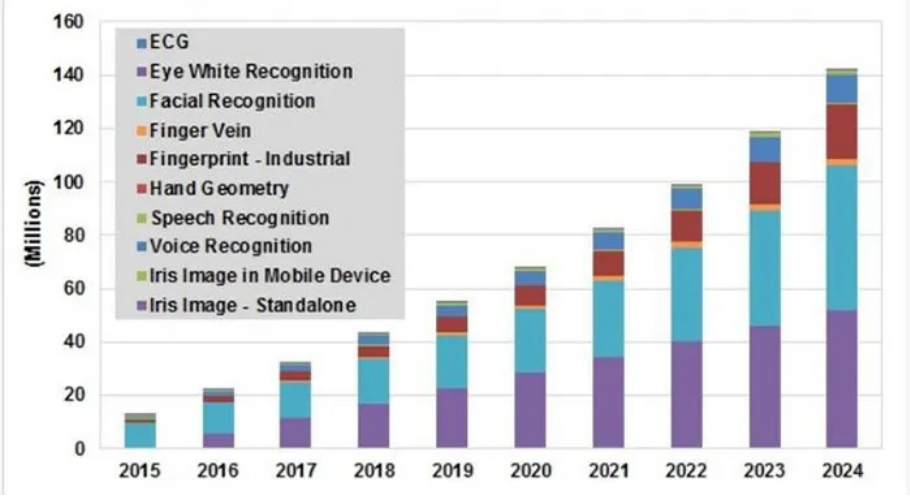
Obr. 2.7: Zastoupení autentizačních metod v roce 2004 v jiném zdroji (Převzato a upraveno z: [17])

Graf znázorněný na obrázku 2.8 poukazuje na změnu zastoupení využívání otisku prstu a rozpoznávání obličeje jako autentizační metody v souvislosti s vývojem technologií. Oproti roku 2004 lze vidět i znatelný pokles využívání analýzy podpisu a hlasu. Neutrálně se jeví analýza duhovky, která je dle obrázku 2.6 na stejném procentuálním zastoupení avšak oproti obrázku 2.7 je nižší.



Obr. 2.8: Zastoupení autentizačních metod v roce 2010 (Převzato a upraveno z: [21])

S vývojem mobilních telefonů a implementace takzvaného face ID do zařízení od společnosti Apple byl zaznamenán pokles využití otisku prstů a navýšení využívání rozpoznávání obličeje. Mobilní telefony jsou v dnešní době hojně využívané k placení nákupů bezkontaktní metodou. Cerny tak v souvislosti autorizacemi plateb poukazuje na nárůst v oblibě využívání autorizace obličejem než dříve využívané otisky prstu. Na obrázku 2.9 je znázorněn vývoj trhu od roku 2015 do roku 2023 s předpovědí na rok 2024 [6].



Obr. 2.9: Vývoj trhu dle jednotlivých modalit (Převzato z: [6])

3 Praktická část

Praktická část práce se zaobírá sestavením laboratorní úlohy na biometrické kontroly vstupu, která bude sloužit pro výuku. Komponenty dodané a použité při sestrojení systému včetně softwaru pro ovládání jsou popsány dále v této kapitole.

3.1 Hardwarové komponenty

Pro potřeby sestrojení systému pro biometrickou kontrolu vstupu byl dodán spojovací materiál (obrázek 3.1) včetně terminálu a dalších elektrotechnických zařízení (obrázek 3.2). Spojovací materiál nebyl však použit, jelikož byly dostupné i jiné, vhodnější spojovací prvky.

Obr. 3.1: Spojovací materiál (vlastní zpracování)

Obr. 3.2: Terminál s elektrotechnickými zařízeními (vlastní zpracování)

3.1.1 Terminál Hikvision DS-K1T671MF

Terminál od firmy Hikvision je hlavním komponentem celého sestrojovaného systému [11]. Je vybaven čtečkou pro snímaní otisků prstu a kamerou s rozlišením 2 Mpx pro obličejovou autentizaci. Dále je možné připojit k terminálu externí Wiegandovu čtečku, která může sloužit k dalšímu způsobu autentizace. Terminál lze

nastavit tak, aby po žadateli o přístup požadoval jeden ze zmíněných typů autentizace, ale také kombinaci více autentizací za účelem zvýšení bezpečnosti. Kapacita terminálu pro biometrické vzory a události je 6 000 vzorů obličeje, 5 000 vzorů otisku prstu, 6 000 osob a 50 000 událostí.

Z pozice běžného uživatele se terminál ovládá 7palcovým dotykovým displejem. Ve většině případů ale ani není potřeba se terminálu jakkoliv dotýkat. Velkým benefitem je totiž stav, ve kterém terminál nepřetržitě čeká na případný pokus o autentizaci. Žadateli o přístup tak stačí v případě autentizace obličejem pouze přistoupit k terminálu v doporučované vzdálenosti a terminál sám rozpozná pokus o autentizaci. V případě pokusu o autentizaci otiskem prstu to funguje velmi podobně. Osoba rovnou přiloží otisk na čtečku a terminál taktéž ihned rozpozná pokus o autentizaci.

Terminál je možné jakožto správce přístupů 3 způsoby. Přímo na dotykovém displeji, stejně jak jej ovládá obyčejný uživatel. Dále z pohodlí řídící místnosti prostřednictvím specializovaného softwaru či webového rozhraní.

3.1.2 Elektrický zámek dveří Fermax

Zámek spínaný elektřinou přiváděnou z kontroléru, v tomto případě terminálu. Jakmile je do něj přivedeno napájení 12V, dojde k jeho odblokování. V opačném případě bez přicházejícího napájení je v poloze zablokováno.

3.1.3 Bezkontaktní karta Mifare

Bezkontaktní karta o ISO rozměrech, sloužící jako identifikační médium s frekvencí 13,56 MHz. Umožňuje zápis a přepis dat na čipu.

3.1.4 Webkamera Niceboy

Webkamera od značky Niceboy, sloužící k pořízení fotografie obličeje studenta a následnému použití fotografie jako záznam geometrie obličeje.

3.2 Softwarové komponenty

Softwarové komponenty se řadí mezi základní stavební kameny, díky kterým fungují moderní aplikace a systémy. Mezi ně se řadí i softwary umožňující uživatelům interagovat se zařízením.

3.2.1 VMware Workstation 17 player

WMware je software umožňující uživatelům na svém stávajícím OS vytvářet, spouštět či konfigurovat virtuální verzi jakéhokoliv operačního systému. Například na PC s OS Windows, lze prostřednictvím tohoto softwaru provozovat OS Linux, MacOS, atd.. Zejména je velmi využíván k testovacím účelům, jelikož díky němu odpadá nutnost mít více zařízení s různými verzemi OS. Proto byl tento software zvolen jako vhodný nástroj k provozování softwaru od firmy Hikvision.

3.2.2 Hikvision iVMS-4200

Hikvision je software pro ovládání a správu většiny zařízení od značky Hikvision [11]. Umožňuje správci mnoho užitečných funkcí. Správce systému skrze něj může například sledovat aktuální dění před terminálem prostřednictvím kamery terminálu. Dále umožňuje správu přístupů, jako je například vytvoření, smazání nebo úprava přístupových práv osob. Disponuje také možností spravovat docházkový systém, kde správní autorita vidí veškeré úspěšné i neúspěšné pokusy o autentizaci. A to včetně data a časů provedení dané akce. Vedení firmy používající tento software tak může jednoduše kontrolovat docházku svých zaměstnanců. Samozřejmostí je možnost skrze tento software kompletně nastavovat terminál a jeho funkce vzdáleně.

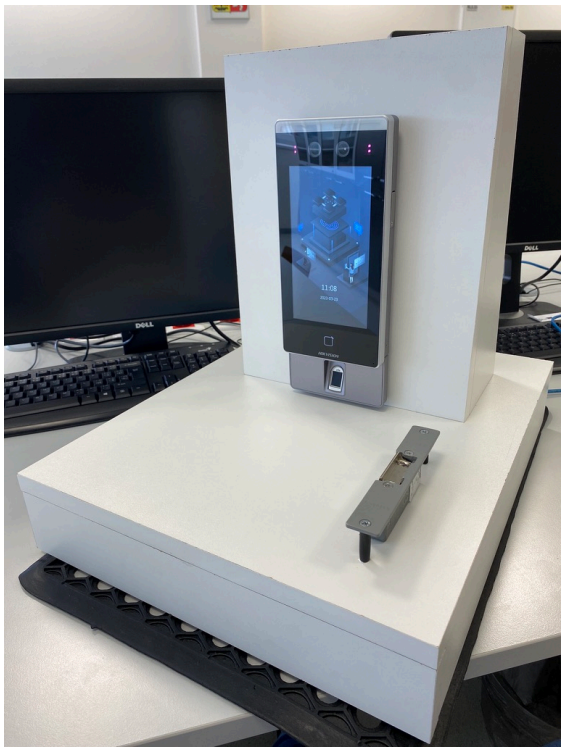
3.3 Návrh systému biometrické kontroly vstupu

Celý systém bude řízen samotným terminálem. Terminál bude umístěn na svislé desce představující stěnu. Na základě vyhodnocování konkrétních situací bude provádět příslušné úkony. Jako příklad, lze uvést odemčení elektrického zámku v případě úspěšné autentizace osoby. Ze strany pohledu osoby žádající o přístup je přístupný pouze terminál a elektrický zámek viz obrázek 3.3. Z opačné strany panelu, tedy pohledu správce systému, lze přistupovat k napájení terminálu, napájení zámku a jednotlivým vodičům viz obrázek 3.4.

Terminál bude připojen UTP kabelem k internetu, aby jej bylo možné spravovat vzdáleně pomocí specializovaného softwaru nainstalovaného na správním PC.

3.3.1 Návrh zapojení

Panel, který je osazen systémem pro biometrickou kontrolu vstupu, se skládá ze dvou desek a podstavy. Napájen je přívodním kabelem flexi 3x1,5mm2 ukončeným vidlicí pro zapojení do zásuvky 230 V/AC. Terminál umístěný na svislé desce je napájen



Obr. 3.3: Pohled na panel zepředu (vlastní zpracování)

Obr. 3.4: Pohled na panel zezadu (vlastní zpracování)

adaptérem 12 V/DC, který je zapojený do zásuvky 230 V/AC. Jednotlivé vodiče terminálu jsou vyvedeny otvorem ve svislé desce na stranu přístupnou pouze správci. Elektrický zámek umístěný na vodorovné desce na přední straně terminálu je také napájen adaptérem 12 V/DC, který je také zapojen do zásuvky 230 V/AC. Napájení zámku je vedeno pod vodorovnou deskou v prostoru mezi podstavnými deskami, aby nebylo přístupné běžnému uživateli a bylo tak zabráněno případnému poškození kabeláže. UTP kabel je veden pod vodorovnou deskou a prostupy veden do terminálu.

Terminál a zámek jsou s napájecími adaptéry propojeny pomocí svorkovnice. Aby bylo zamezeno možnosti vytrhnout vodiče ze svorkovnice, nebo je nějak poškodit, je svorkovnice s vodiči umístěna do ochranné krabičky a upevněna na svislou desku. Nepoužité vodiče jsou umístěny do druhé ochranné krabičky a upevněny také na zadní stěně panelu. Schéma zapojení je k vidění na obrázku 3.6.

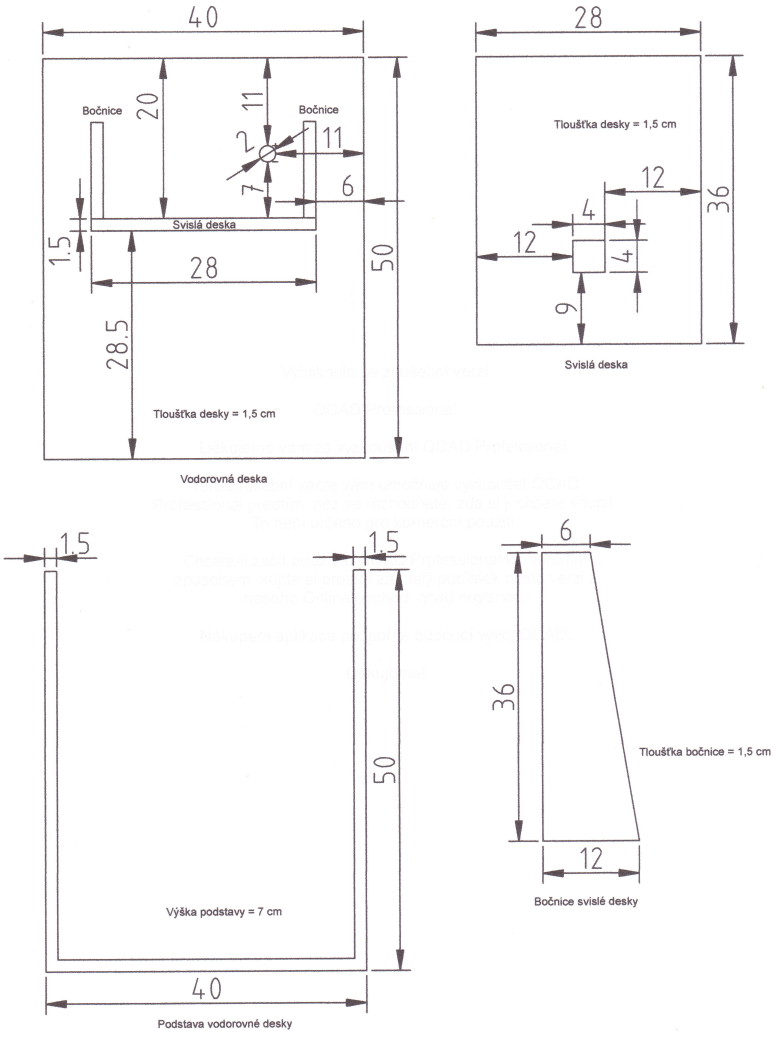
3.3.2 Návrh panelu

Koncept výukového panelu byl vytvořen na základě dodaných komponent a předpokládaného využití prostoru pro kabeláž. Tento koncept, znázorněný na obrázku 3.5,

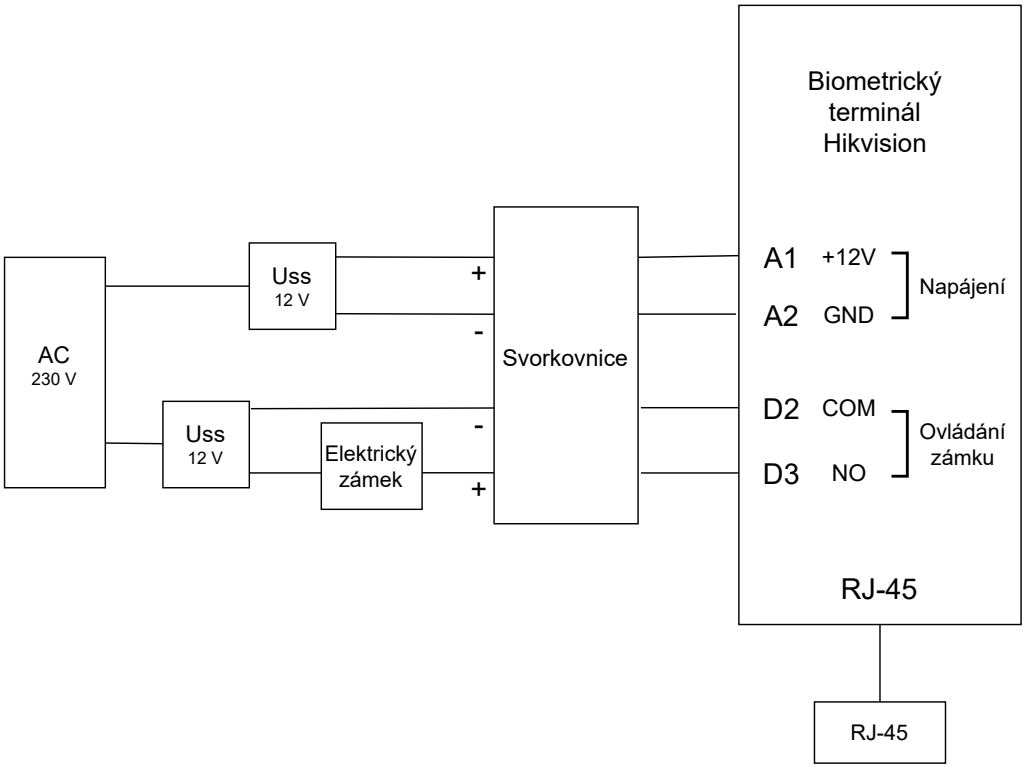
je pouhým náčrtem, který byl použit pro vytvoření prototypu výukového panelu. Po sestrojení výukového panelu a zhodnocení rozměrů potřebných pro uložení veškeré kabeláže včetně terminálu, byla vytvořena výkresová dokumentace, skládající se z:

- Výkres podstavy,
- Výkres svislé desky a bočnice,
- Výkres sestavy s kusovníkem,

podrobněji znázorněno viz příloha C.



Obr. 3.5: Návrh výkresu k výrobě panelu
(vlastní zpracování)



Obr. 3.6: Schéma zapojení systému (vlastní zpracování)

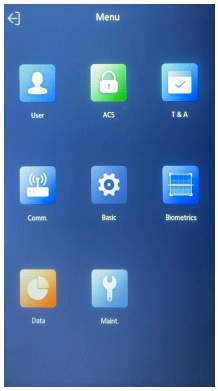
4 Laboratorní úloha

4.1 Laboratorní úloha - návod pro studenta

Úkolem této bakalářské práce bylo sestavit laboratorní úlohu umožňující studentům vyzkoušet si správu systému z biometrické čtečky a správního počítače prostřednictvím webového rozhraní a specializovaného softwaru. Proto je úloha rozdělena na 3 části podle toho, jakým způsobem se správa systému provádí. Funkcí a možností systému je velké množství, ale pro splnění časové náročnosti úlohy 90 minut byly zvoleny a představeny ty nejdůležitější. Mezi ně patří vytvoření osoby v databázi osob, přidání autentizace kartou, otiskem prstu a geometrií obličej. Nechybí ani více faktorová autentizace, tedy kombinace 2 zmíněných autentizací pro zvýšení bezpečnosti. Ve 2. a 3. části, kdy se sytém ovládá vzdáleně ze správního počítače, byly představeny dostupné moduly/záložky, k čemu slouží a jednoduchá ukázka. Kompletní znění laboratorní úlohy se nachází v příloze A.

4.1.1 Část 1. - Nastavení prostřednictvím terminálu

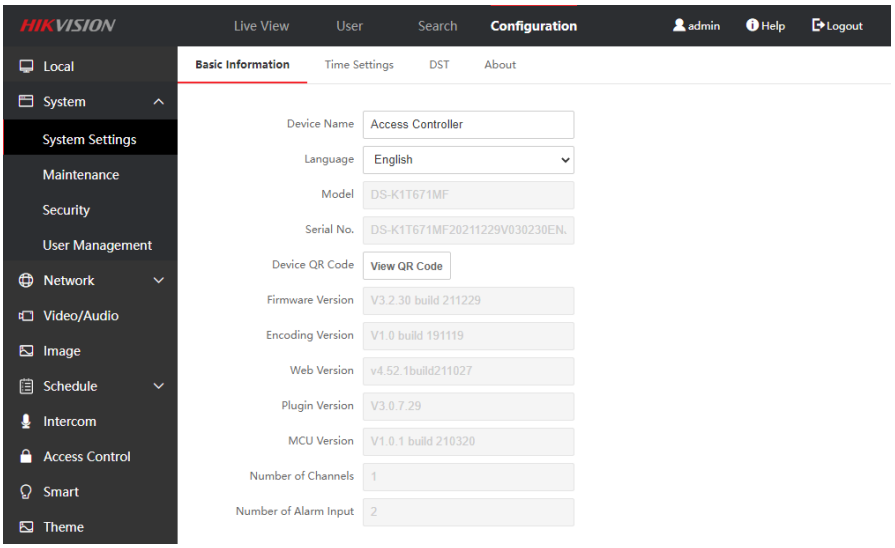
V první části postupu laboratorní úlohy si student vyzkouší ovládání systému přímo v prostředí terminálu. Postupně vytvoří v databázi osob 3 osoby, každou s lehce odlišnými vlastnostmi. Nejprve vytvoří osobu Admin, která bude mít přístup do nastavení terminálu a bude se autentizovat pomocí karty nebo otisku prstu. Dále vytvoří osobu Zaměstnanec, která nedisponuje oprávněním vstoupit do nastavení terminálu. Autentizovat se bude kombinací otisku prstu a geometrií obličeje. Studentovi je tedy představena více faktorová autentizace. Třetí osobou bude Uklízečka autentizující se pouze prostřednictvím karty a bez oprávnění vstoupit do nastavení terminálu. Po vytvoření všech 3 osob si student otestuje jak jednotlivé způsoby autentizace fungují. Na obrázku 4.1 níže, je zobrazeno hlavní menu terminálu.



Obr. 4.1: Hlavní menu terminálu (vlastní zpracování)

4.1.2 Část 2. - Nastavení prostřednictvím webového rozhraní

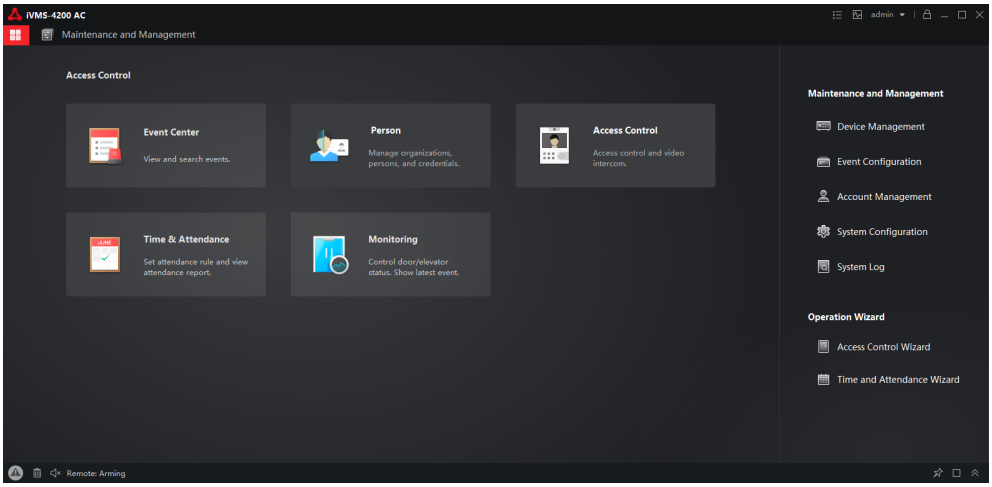
V druhé části postupu se student seznámí s ovládáním systému vzdáleně prostřednictvím webového rozhraní na správním počítači. Po přihlášení do rozhraní si prohlédne rozložení stránky a provede několik úprav v databázi osob. Smaže vytvořenou osobu Uklízečka a místo ní vytvoří novou osobu Dělník. Nová osoba se bude autentizovat kartou Uklízečky a geometrií obličeje. Pro přidání záznamu geometrie obličeje použije přiloženou webkameru. Provedené změny si ověří na terminálu a provede vyhledání akcí podle parametru Name v záložce Search. Prostředí webového rozhraní je k vidění na obrázku 4.2.



Obr. 4.2: Webové rozhraní (vlastní zpracování)

4.1.3 Část 3. - Nastavení prostřednictvím programu iVMS 4200

V poslední části provede student správu terminálu opět vzdáleně ze správního počítače. Po spuštění a přihlášení do softwaru je nejprve nutné terminál přidat. Následně po jeho přidání smaže databázi osob na terminálu a vytvoří nové osoby. Veškeré úpravy provedené v programu je nutné ručně importovat do terminálu. V předchozí části u webového rozhraní se změny importují automaticky ihned. Dále si student vyzkouší přidat jeden z mnoha parametrů osob – počet povolených autentizací. Jako poslední provede student základní úkony v modulech Event Center a Monitoring. Oba moduly slouží k monitorování a kontrole zaznamenaných akcí. Na obrázku 4.3 je zobrazeno hlavní menu softwaru s jednotlivými moduly.



Obr. 4.3: Hlavní menu iVMS 4200 (vlastní zpracování)

4.1.4 Otázky a reset zařízení

Po dokončení všech tří částí postupu si student projde otázky a připraví si na ně odpovědi. Účelem otázek je ověřit získané znalosti studentů a také jejich pozornost. Své odpovědi sdělí vyučujícímu. Po jeho odsouhlasení uvedou zařízení do původního stavu dle kroků v úloze.

4.2 Časová náročnost úlohy a postup

Délka cvičení, pro kterou bude laboratorní úloha využívána, je 90 minut. Proto jsem časovou náročnost úlohy otestoval na jednom z mých bývalých spolužáků. Vypracovat úlohu mu trvalo 75 minut, což je dle mého uvážení ideální délka. I v případě pomalejšího tempa vypracovávání úlohy by tedy student měl úlohu stihnout vypracovat v časovém limitu cvičení. Pro přehledné vypracovávání a snadnou orientaci je postup úlohy orientován v krocích. Některé kroky jsou doplněny obrázky pro snadnější pochopení.

4.3 Dokumentace pro vyučujícího

Dokument určený výhradně pro vyučujícího a poskytující zásadní informace o úloze i komponentech. Nejprve je v něm popsán způsob napájení komponent. Dále jsou vypsány všechny komponenty využívané v úloze a jak uvést celý systém do chodu.

Pro případ potřeby jsou uvedeny přístupové údaje a síťové nastavení terminálu. Pokud by nastala situace, kdy student pozmění nastavení terminálu a naruší tím jeho fungování, je v dokumentaci popsáno jak terminál uvést do výchozího nastavení a jaké parametry pozměnit pro správné fungování. Následně jsou stručně popsány jednotlivé části úlohy, co si v nich student vyzkouší. Poslední částí dokumentace jsou otázky, na které student odpoví vyučujícímu. Prověří se tak, co se student při vypracovávání úlohy naučil a zapamatoval. Kompletní znění dokumentace je k nalezení v příloze B.

4.4 Možnosti rozšíření

Možností, jak rozšířit tuto úlohu, se nabízí několik. Nejjednodušší variantou je využití funkcí terminálu a softwaru, které nebyly z důvodu časového limitu použity. Mezi tyto funkce patří například docházkový systém, který po jeho zavedení eviduje příchody, odchody, přestávky, pozdní příchody a přesčasy. Další možností rozšíření je připojení podporované externí čtečky otisku prstu do správního PC. Bylo by tak možné vytvářet záznam otisku prstu bez nutnosti použití terminálu. Terminál také podporuje připojení dalších komponent, které nebyly využity. Například odchodové tlačítko, sirénu pro signalizaci poplachu a Wiegandovu čtečku karet.

Závěr

Biometrická kontrola vstupu je v dnešní době velmi vyhledávaným tématem, které si zaslouží svoji pozornost. V souvislosti s tím bylo vypracováno téma „Laboratorní úloha systému biometrické kontroly vstupu“, ve kterém bylo vytyčeno několik zásadních bodů ke splnění.

Teoretická část se zabývá rešerší systémů elektronické kontroly vstupu, a to konkrétně architekturou systémů EKV, fungováním systémů EKV a základními typy autentizace, mezi které se řadí autentizace heslem, průkazem, biometrikou a hardwarem. Podstatně rozšířenější dílčí částí jsou pak biometrické systémy EKV, které se zabývají jednotlivými typy biometrické autentizace, a to podle otisku prstu, cévního řečiště prstu, autentizací dle obličeje a duhovky. Vlastnosti biometrické autentizace jsou pak nedílnou součástí teorie, kde byla znázorněna její přesnost, výhody a nevýhody společně s hrozbami vyplývajícími z využívání těchto zabezpečovacích systémů. Okrajovou dílčí částí pak je stručné nastínění legislativního rámce s výčtem norem ČSN společně s historickým zastoupením a srovnáním biometrické autentizace na trhu s předpovědí do roku 2024.

Praktická část obsahuje dílčí cíle, jimiž jsou hardwarové komponenty, softwarové komponenty, návrh systému biometrické kontroly vstupu a laboratorní úloha. Součástí je i zpracování technické dokumentace pro výrobu panelu. Jednotlivé kapitoly popisují osazení a propojení jednotlivých komponent na základě vytvořeného schématu. Na základě funkčnosti terminálu byla zpracována laboratorní úloha popisující nastavení prostřednictvím terminálu, webového rozhraní a programu iVMS 4200. Laboratorní úloha také zahrnuje otázky pro studenta a postup pro reset zařízení. Zhodnocuje také časovou náročnost úlohy a možnosti rozšíření dalšími zařízeními či moduly, které jsou kompatibilní s tímto systémem.

Bakalářská práce je vhodná jako studijní a doprovodná literatura pro biometrické zabezpečení elektronické kontroly vstupu. V praktické části by za normálních okolností byla žádaná ekonomická analýza pro výrobu výukového panelu s terminálem, avšak z důvodu zajištění potřebných materiálů fakultou nebyla zpracována. Vzhledem k rozmanitosti biometrických kontrolních systémů je práce vhodná jako vstupní dokument pro návrhy jiných zabezpečovacích systémů na této bázi.

Literatura

[1] BENEŠ, Radek. *Autentizační metody založené na biometrických informacích* [online]. 2010 [cit. 06.01.2023]. ISSN 1214-9675. Dostupné z: http://access.fel.cvut.cz/view.php?cisloclanku=2010110002.

[2] BURDA, Karel. *Základy elektronických zabezpečovacích systémů*. Brno: Akademické nakladatelství CERM, 2017. ISBN 978-80-7204-967-7.

[3] BURDA, Karel. *Elektronická kontrola vstupu* [online]. [b.r.] [cit. 23.01.2023]. Dostupné z: https://moodle.vut.cz/pluginfile.php/245372/mod_resource/content/1/BZSY%2007d.pdf.

[4] BURDA, Karel. *Biometrické systémy EKV*. [online]. [b.r.] [cit. 11.12.2022]. Dostupné z: https://moodle.vut.cz/pluginfile.php/248941/mod_resource/content/1/BZSY%2008d.pdf.

[5] BURDA, Karel a Ivo STRAŠIL. *Zabezepečovací systémy* [online]. Brno, 2011 [cit. 23.01.2023]. Dostupné z: https://moodle.vut.cz/mod/resource/view.php?id=124517.

[6] CERNY, Jan. *Mobile payments in 2024? Biometrics about to secure $2.5 trillion.* Everly.eu [online]. 2020 [cit.07.05.2023]. Dostupné z: https://everly.eu/2020/02/10/mobile-payments-in-2024-biometrics-about-to-secure-2-5-trillion/

[7] ČESKO. *Zákon č. 110 ze dne 24. dubna 2019 o zpracování osobních údajů*. 2019, částka 47. Dostupné také z: https://www.zakonyprolidi.cz/cs/2019-110

[8] ČESKO. *Zákon č. 101 ze dne 25. dubna 2000 o ochraně osobních údajů a o změně některých zákonů*. 2000, částka 32. Dostupné také z: https://www.zakonyprolidi.cz/cs/2000-101

[9] FRĄCKIEWICZ, Marcin. *Špičkové technologie biometrické autentizace: Komplexní průvodce.* TS2 SPACE, 2023 [online]. [cit. 17.03.2023]. Dostupné z: https://ts2.space/cs/spickove-technologie-biometricke-autentizace-komplexni-pruvodce/

[10] HANY, Umma et al. *Design and Development of a Litho-code ID based electronic entry-control system.* International Journal of Electrical and Computer Engineering (IJECE). 2012, 2(4) [cit 07.05.2023]. Dostupné z: DOI: https://doi.org/10.11591/ijece.v2i4.705

[11] HIKVISION. *Hikvision DS-K1T671 manual* [online]. Manua.ls, [b.r.] [cit. 06.01.2023]. Dostupné z: https://www.manua.ls/hikvision/ds-k1t671/manual.

[12] JAIN, Rubal a Chander, KANT. *Attacks on biometric systems: an overview.* International Journal of Advances in Scientific Research, 2015, 1.07: 283-288 [online]. [cit. 13.02.2023]. ISSN: 2321-0613. Dostupné z: https://pdfs.semanticscholar.org/dc91/bd3e5780ceb475f82c33af0b83592eb3c468.pdf

[13] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management I.* Zlín: VeRBuM, 2011. ISBN 978-80-87500-05-7.

[14] MAŇÁSEK, Tomáš. *Laboratorní úloha systému elektronické kontroly vstupu* [online]. Brno, 2022 [cit. 06.01.2023]. Dostupné z: https://www.vut.cz/www_base/zav_prace_soubor_verejne.php?file_id=242634. Bakalářská práce. Vysoké učení technické v Brně.

[15] PAVLÍK, Pavel. *Biometrie jako základ současné i budoucí identifikace a autentizace. Kontakt.* 2007; 9(2):427-430 [cit. 06.01.2023]. Dostupné z: DOI: https://doi.org/10.32725/kont.2007.066

[16] PŘIBYL, Tomáš. *Výhody a nevýhody biometrických systémů* . Science World, 2008 [online]. [cit. 07.05.2023]. Dostupné z: https://www.scienceworld.cz/biologie/vyhody-a-nevyhody-biometrickych-systemu-1-515/

[17] PUŽMANOVÁ, Rita. *Biometrické systémy v praxi.* In: www.systemonline.cz [online]. 2004 [cit. 16.05.2023]. Dostupné z: https://www.systemonline.cz/clanky/biometricke-systemy-v-praxi.htm

[18] RAK, Roman, Vašek MATYÁŠ a Zdeněk ŘÍHA. *Biometrie a identita člověka ve forenzních a komerčních aplikacích.* Praha: Grada Publishing, 2008. Profesionál. ISBN 978-80-247-2365-5

[19] ŠKOB, Miroslav. Biometrické systémy a jejich slabá místa. TZB-info, 2020 [online]. [cit.11.05.2023]. Dostupné z: https://www.tzb-info.cz/bezpecnost/20337-biometricke-systemy-a-jejich-slaba-mista

[20] ŠURKALA, Milan. *Turisté budou v Japonsku platit otiskem prstu.* In: Svět hardware [online]. 11.04.2016 [cit. 28.03.2023]. Dostupné z: https://www.svethardware.cz/turiste-budou-v-japonsku-platit-otiskem-prstu/42164.

[21] VANĚK, Tomáš. *Autentizace - Biometrika*. rantos.cz [online]. [b.r.] [cit. 28.04.2023]. Dostupné z:http://rantos.cz/IBE-prezentace/P09a_Biometrika,_verze_1.0.3.pdf

Seznam symbolů a zkratek

EKV	Elektronická kontrola vstupu
PIR	Passive Infra Red
USB	Universal Serial Bus
LAN	Local Area Network
DF	Dokazovací faktor
OF	Ověřovací faktor
DD	Dokazovací data
RFID	Radio Frequency Identification
Δ	značka pro odchylku
EEPROM	Electrically Erasable Programmable Read-Only Memory
NFC	Near Field Communication
CCD	Charged Coupled Device
CMOS	Complementary Metal Oxide Semiconductor
IR	Infra Red
FRR	False Rejection Rate
FAR	False Acceptance Rate
EER	Equal Error Rate
OS	Operační systém
UTP	Unshielded Twisted Pair
V/AC	Alternating Voltage
V/DC	Direct Voltage
ZSY	Zabezpečovací systémy

Seznam příloh

A Laboratorní úloha systému biometrické kontroly vstupu

A.1 Úvod

Cílem této laboratorní úlohy je seznámit studenty se systémem biometrické kontroly vstupu, který si vyzkouší nastavit a spravovat třemi odlišnými způsoby. Proto je tato laboratorní úloha rozdělena na 3 části. Nejprve si vyzkouší ovládat biometrický terminál přímo v jeho integrovaném rozhraní. V následující části si studenti vyzkouší ovládat terminál vzdáleně prostřednictvím webového rozhraní. Poslední část spočívá v ovládání terminálu vzdáleně pomocí programu iVMS 4200, který je od stejného výrobce jako terminál. Po absolvování úlohy bude mít student lepší představu, jak systém biometrické kontroly vstupu funguje, jak probíhá jeho správa a jaké komponenty je možné v systému využít.

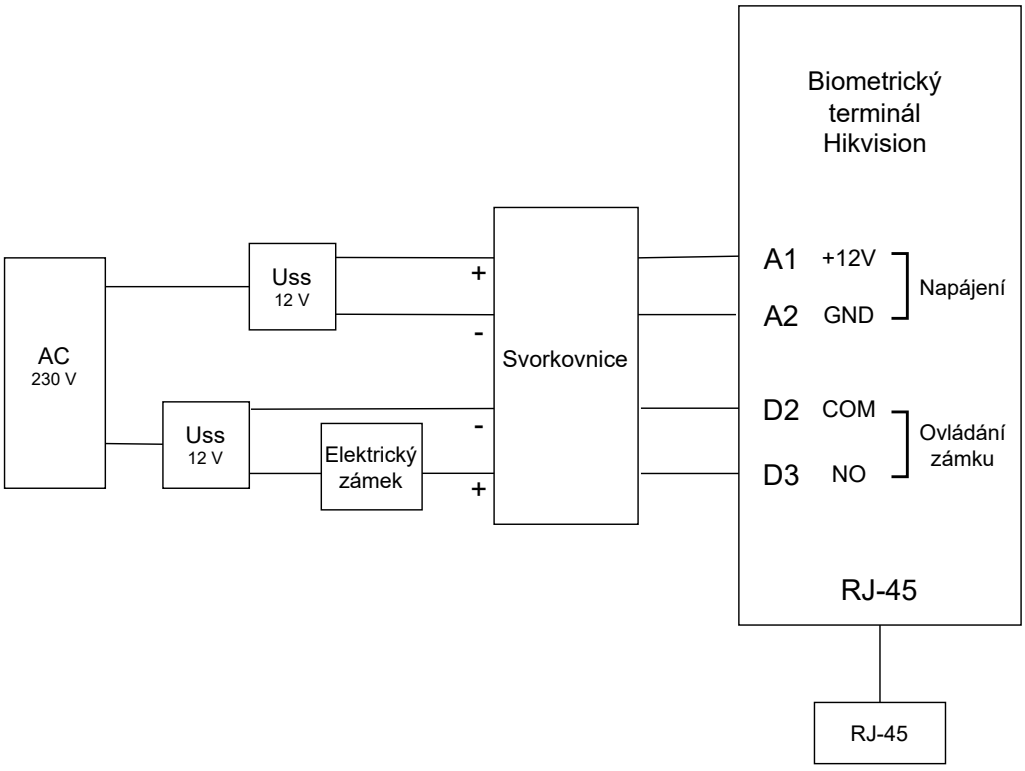
Terminál využívaný v této úloze je od firmy Hikvision, a slouží k řízení přístupu osob do určitého objektu. Je vhodný pro vnitřní i venkovní použití a jeho ovládání je uživatelsky velmi jednoduché a moderní. Terminál nabízí několik variant autentizací – otiskem prstu, obličejem a kartou. Možností je také vícefaktorová autentizace ve formě kombinace výše zmíněných 3 autentizací. Dále je možné k terminálu připojit externí čtečku karet pomocí Wiegand nebo RS-485 protokolu. Kapacita terminálu je 6 000 osob, 6 000 vzorů obličeje, 6 000 karet, 5 000 vzorů otisků prstu a 50 000 událostí.

A.2 Seznam komponent

- Terminál Hikvision DS-K1T671MF
- Elektrický zámek dveří Fermax
- 2x Bezkontaktní karta Mifare (4036375414 a 4124954550)
- Webkamera Niceboy
- PC s virtualizovaným operačním systémem Windows 10
- Software iVMS 4200

A.3 Schéma zapojení

Jednotlivé komponenty jsou na panelu propojeny dle schématu viz obr. A.1. Označení AC je pro zdroj napájení adaptérů. Horní Uss značí adaptér pro napájení terminálu a spodní Uss napájení pro elektrický zámek. Vše je propojeno pomocí svorkovnice, která je umístěna do ochranné krabičky vlevo. Vodiče od terminálu, které nebyly použity, jsou schovány do ochranné krabičky vpravo. Označení RJ-45 je pro konektor síťového kabelu.



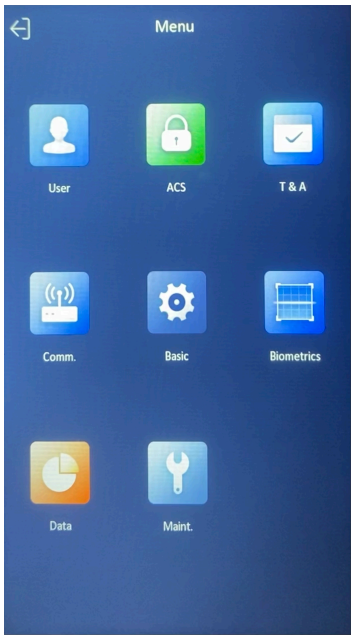
Obr. A.1: Schéma zapojení systému

A.4 Postup

A.4.1 Část 1. – Nastavení prostřednictvím terminálu

První část laboratorní úlohy se zabývá nastavením prostřednictvím integrovaného prostředí terminálu. Nejprve je zapotřebí uvést komponenty systému do chodu zapojením přívodního kabelu od zásuvek do napájení. Poté vyčkejte, než se vše aktivuje. Databáze osob terminálu je prázdná a úkolem tedy bude přidat do databáze osoby a k nim jednotlivé způsoby autentizace. Jako první vytvoříte osobu Administrátor, která bude mít přístup i do správy terminálu. Postupujte dle následujících kroků:

1. Podržte prst 2-3 sekundy na displeji terminálu a posuňte přiložený prst do levé či pravé strany pro vstup do nastavení terminálu.
2. Zadejte heslo „Adminpristup123“ a potvrďte *OK*. Dejte pozor na velká/malá písmena, pokud dojde k zadání špatného hesla 5x po sobě, terminál bude uzamknut na 30 minut.
3. Po zadání hesla se zobrazilo hlavní menu terminálu, viz obr. A.2, které si později blíže projdete. Zvolte první modul – *User*. Jak můžete vidět, v databázi terminálu se nenachází žádná osoba. Stiskněte symbol + a zobrazí se menu pro přidání osoby viz obr. A.3.

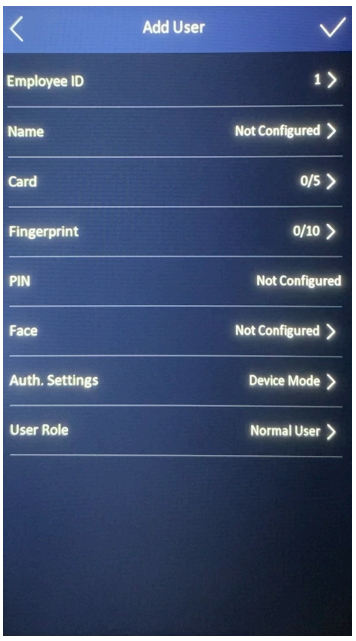


Obr. A.2: Hlavní menu terminálu

4. *Employee ID* zůstane 1, stiskněte *Name* a napište „Admin“.
5. Zvolte *Card* pro přidání karty, symbol +, stiskněte *Card No.* (číslo karty) a přiložte jednu ze dvou karet ke čtečce na terminálu (symbol čtverečku pod dis-

plejem). Tím dojde k načtení čísla karty, *Type* ponechejte na Normal Card, potvrďte *OK*, uložte symbolem ✓ a vraťte se šipkou zpět.

6. Kartu máte přidanou a nyní přidáte záznam otisku prstu. Zvolte *Fingerprint* pro přidání otisku prtu, symbol +, a opakovaně přikládejte bříško jednoho z prstů na ruce, dokud nedojde k návratu do předchozího menu. V případě úspěšného přidání se vraťte šipkou zpět. Pokud nebyl prst úspěšně přidán, tak pokus opakujte. Zvažte také možnost výběru jiného prstu. Doporučení: palec či prostředníček.
7. Stiskněte *User role* a zvolte možnost *Administrátor* pro přidělení oprávnění spravovat terminál.
8. Vše uložte stisknutím symbolu ✓.

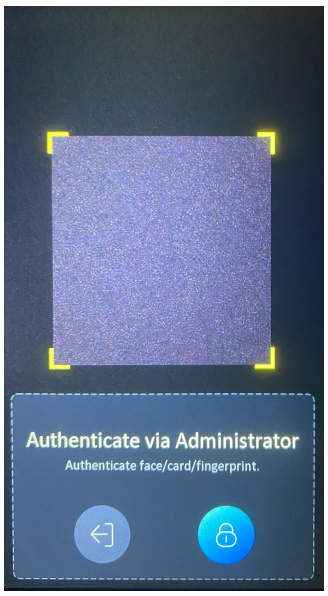


Obr. A.3: Menu přidávání osoby

9. Nyní vytvoříte druhou osobu. Stiskněte symbol + pro přidání osoby.
10. *Employee ID* opět nechejte na hodnotě 2, stiskněte *Name* a napište „Zamestnanec“.
11. Zvolte *Fingerprint* pro přidání záznamu otisku prstu, symbol +, a stejným způsobem jako u předešlé osoby přikládejte opakovaně bříško prstu, dokud nedojde k návratu do předchozího menu. S jediným rozdílem, musíte vybrat odlišný prst, než byl dříve uložen, aby nedošlo k duplicitnímu záznamu. Terminál duplicitu ihned pozná a opětovné přidání daného prstu zruší.
12. Poté zvolte *Face* pro přidání záznamu obličeje a snažte se umístit hlavu před terminálem tak, aby byla přesně ve vyznačeném kruhu. Stiskněte ikonku fotoaparátu a potvrďte ✓, čímž dojde k vytvoření záznamu geometrie obličeje.

13. Terminál disponuje možností vícefaktorové autentizace, proto se Zaměstnanec bude muset prokázat geometrií obličeje i otiskem prstu. Stiskněte pole *Auth. Settings*, poté klepněte na *Mode*, zvolte *Custom*, klepněte na *Type* a zvolte *Multiple Credentials*, a jako poslední stiskněte *Method* a vyberte *Face* a *FP*. Potvrďte *OK* a jděte zpět šipkou.
14. Jelikož jde o normálního zaměstnance, který nesmí mít přístup do správy terminálu, tak políčko *User role* ponechejte na hodnotě *Normal user*.
15. Uložte osobu symbolem ✓ do databáze.
16. Třetí osobu vytvoříte následujícím způsobem. Stiskněte symbol + pro přidání osoby.
17. *Employee ID* nechejte na hodnotě 3, stiskněte *Name* a napište „Uklizecka“.
18. Zvolte *Card* pro přidání karty, symbol +, *Card No.*, přiložte druhou kartu ke čtečce na terminálu pro načtení čísla karty, potvrďte *OK*, uložte symbolem ✓ a vraťte se symbolem šipky zpět.
19. Pole *User role* nechejte opět na hodnotě *Normal User*, protože jde pouze o uklízečku.
20. Uložte symbolem ✓, a vyjeďte ven ze správy terminálu opětovnými stisky šipky zpět.

Všechny 3 osoby jsou v databázi uložené a nyní si ověřte funkčnost vyzkoušením všech možností autentizace pro všechny osoby. Admin – karta nebo otisk prstu, Zaměstnanec – otisk prstu + geometrie obličeje (nejprve otisk a poté geometrie obličeje), Uklízečka – karta.



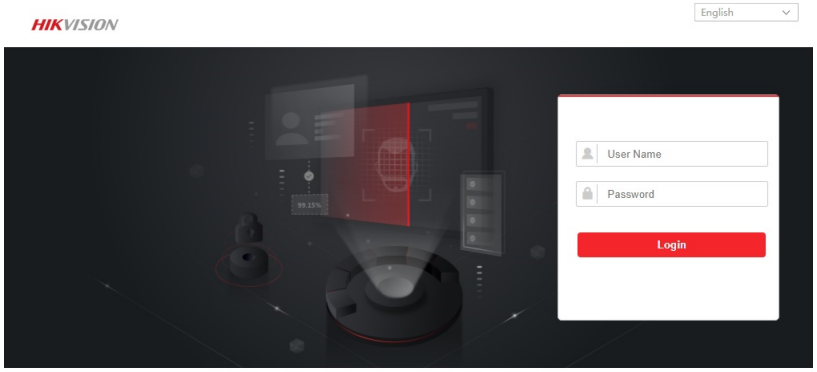
Obr. A.4: Admin login

Pokud budete chtít vstoupit do správního menu terminálu, tak po podržení prstu na displeji a posunutí do strany není potřeba zadávat heslo, ale je možné se prokázat jako Admin, tedy otiskem prstu nebo kartou Admina viz obr. A.4. V případě, že bysme chtěli opět heslem, tak stiskneme symbol zámku a napíšeme heslo.

A.4.2 Část 2. – Nastavení prostřednictvím webového rozhraní

V této části budete ovládat nastavení terminálu prostřednictvím webového rozhraní. Webové rozhraní nabízí ze všech 3 způsobů nastavení nejméně funkcí, avšak ty základní funkce ano.

1. Zapněte PC příslušný k této laboratorní úloze. Po jeho načtení spusťte na ploše program *WMware Workstation 16 Player*. Zvolte *Windows 10 x64* a spusťte. Pokud se objeví dotaz na síť 2, zvolte možnost *Ano*.
2. Otevřete prohlížeč *Edge* a do vyhledávače zadejte IP adresu terminálu, kterou si najdete přímo na terminálu v nastavení (*Comm.* – *Wired Network* – *IP address*). Po načtení se zobrazí se přihlašovací stránka viz obr. A.5, kde zadejte uživatelské jméno „admin“ a heslo „Adminpristup123“.

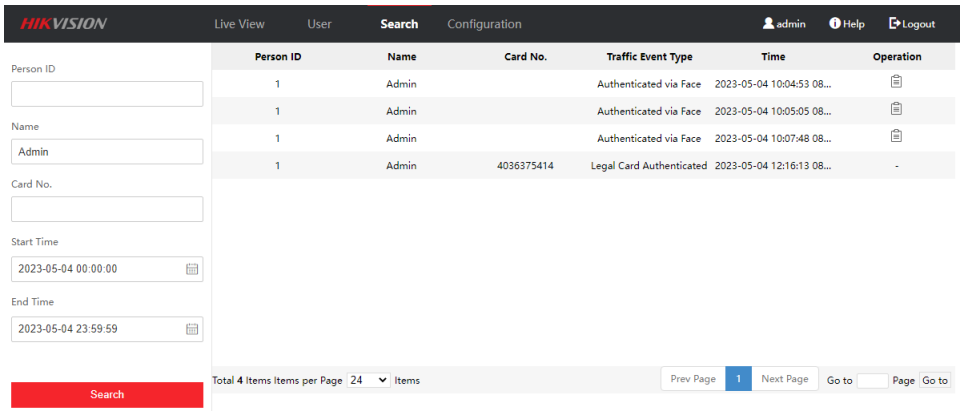


Obr. A.5: Přihlášení do webového rozhraní

3. Po přihlášení se dostanete do systémového nastavení terminálu, kde jsou také vypsány informace o verzích či kapacitě terminálu. Odtud je možné nastavit parametry ohledně sítě a systému, nastavení autentizace, biometrických parametrů atd.
4. V horní liště se nachází několik záložek. Záložka *Live View* slouží k živému přenosu záznamu kamery na terminálu. Potřebný Plug-in ke zprovoznění této záložky funguje pouze na prohlížeči Internet Explorer, který již není podporovaný Windows 10. Záložka *User* pro správu databáze osob, záložka *Search* k prohlížení zaznamenaných akcí na terminálu a záložka *Configuration*, která se zobrazila při přihlášení do webového rozhraní terminálu.

5. Přepněte se do záložky *User* a vyzkoušíte si několik úprav.
6. Nejprve odstraníte osobu Uklízečka z databáze zvolením políčka vedle jejího ID a tlačítkem *Delete* vlevo nahoře.
7. Nyní vytvoříte novou osobu kliknutím na symbol + v levém horním rohu a otevře se nabídka pro nastavení jednotlivých parametrů přidávané osoby. *Person ID* napište 3, *Name* napište „Dělník“, *Gender* zvolte *Male*, *Floor* a *Room No.* (číslo patra a místnosti) napište například 1 a 1, *Start* a *End Time* (začátek a konec trvání oprávnění k přístupu) nechejte na výchozí hodnotě. Dělník nesmí mít práva jako Admin, proto políčko *Administrator* nechejte prázdné.
   Záznam geometrie obličeje pořídíte pomocí přiložené webkamery. Připojte webkameru do PC pomocí USB konektoru. Zvolte *Connect to a virtual machine* a potvrďte 2x *OK*. Dále ve virtualizovaném OS spusťte aplikaci *Kamera* přes hledání v levém dolním rohu. Nasměrujte webkameru na úroveň svého obličeje tak, aby byl celý v záběru a pořiďte fotografii kliknutím na symbol fotoaparátu v aplikaci *Kamera*. Aplikaci zavřete a ve webovém rozhraní u vytváření osoby klikněte na symbol +. V otevřeném okně najděte fotografii v umístění *Obrázky/Z fotoaparátu*, vyberte ji a dejte otevřít.
   Nyní přidělte osobě kartu jako další způsob autentizace přes tlačítko *Add Card*. Použijte číslo karty, která byla použita pro Uklízečku. Potvrďte *OK*.
8. Úpravu osoby v databázi provedete kliknutím na symbol ve sloupečku *Operation*. Otevře se stejné menu jako při vytváření osoby a změníte požadovaný údaj. Pro Vaši potřebu ale nic měnit nebudete.
9. Nyní si autentizací kartou Uklízečky ověřte, že tato karta má nového majitele - Dělníka. Případně si můžete provedené změny ověřit v databázi osob na terminálu.
10. Další záložkou ve webovém rozhraní je záložka *Search*. Ta slouží k zobrazení všech akcí zaznamenaných terminálem. Přepněte se do této záložky. Ve výchozím stavu jsou zobrazeny všechny akce dohromady. Vlevo je možné vyhledávat akce podle *Person ID*, *Name*, *Card No.*, nebo v určitém časovém úseku. Pro ukázku napište například do políčka *Name* „Admin“ a dejte *Search*. Vypíší se Vám všechny akce spojené s osobu Admin viz obr. A.6.
11. Jak již bylo zmíněno, záložka *Configuration* slouží k nastavení systémových parametrů terminálu, síťového nastavení terminálu, či parametrů autentizace, dveří a biometriky.

Přes webové rozhraní není možné vytvářet záznam otisku prstu. To lze pouze přímo na terminálu nebo ve specializovaném softwaru s použitím podporované čtečky otisku prstu viz další část laboratorní úlohy.

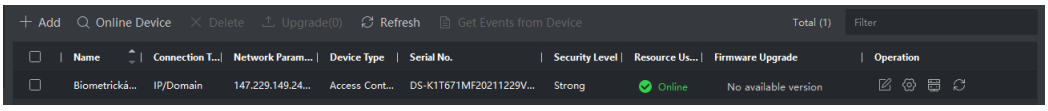


Obr. A.6: Výpis akcí dle parametru Name

A.4.3 Část 3. – Nastavení prostřednictvím programu iVMS 4200

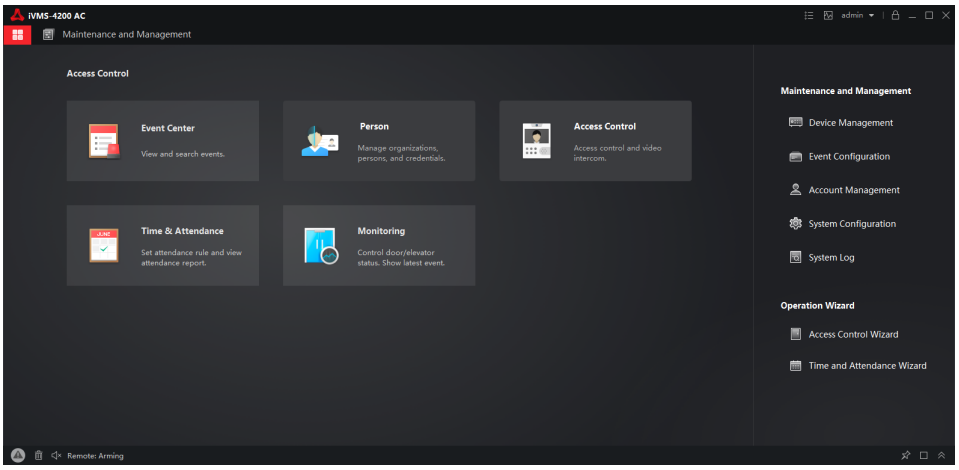
V poslední části laboratorní úlohy si vyzkoušíte nastavit a ovládat terminál prostřednictvím specializovaného programu iVMS 4200, jenž je oficiální software přímo od výrobce terminálu určený k ovládání a správě terminálu vzdáleně.

1. Na ploše virtuálního stroje spusťte program *iVMS-4200 AC 1.7.0.5 Client*. Po načtení bude program vyžadovat zadání přístupových údajů správce. Tyto údaje naleznete na ploše v textovém souboru *Přístupové údaje*. Zadejte údaje a přihlaste se do programu.
2. Nejprve je nutné přidat zařízení (terminál) do programu. To provedete přes tlačítko *+Add*, do políčka *Name* napište název zařízení, například „Biometrická čtečka“. Dále do políčka *Address* napište IP adresu terminálu, kterou jste použili i ve webovém rozhraní. *User Name* a *Password* budou také stejné jako u webového rozhraní, tedy „admin“ a „Adminpristup123“. Potvrďte tlačítkem *Add*. Pokud bylo zařízení přidáno správně, bude u sloupečku *Resource Usage* svítit zeleným písmem *Online* viz obr. A.7.



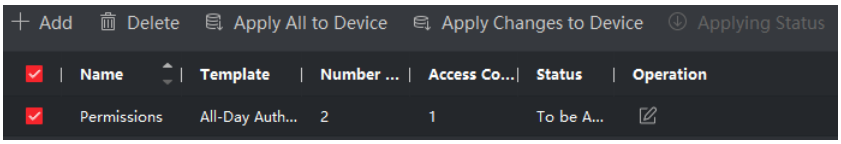
Obr. A.7: Výpis přidaných zařízení

3. Před prováděním následujících kroků smažte osoby z databáze přímo v terminálu. Jděte do nastavení, *Data*, *Delete data*, *User data* a potvrďte *OK*.
4. Vlevo nahoře v programu iVMS klikněte na ikonu čtyř čtverečků, která slouží pro přepnutí do hlavního menu programu. Program se skládá opět z několika modulů pro správu terminálu podobně jako webové rozhraní viz obr. A.8.



Obr. A.8: Hlavní menu programu iVMS 4200

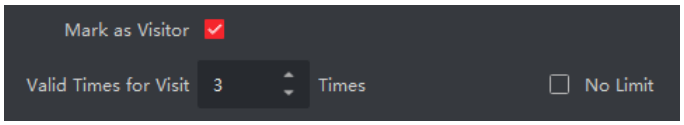
5. Jděte do modulu *Person*, kde si vytvoříte několik osob. Klikněte na *+Add*, hodnotu *Person ID* smažte a přepište na „1“, do políčka *Name* napište „Admin“. Dále klikněte na *+Add Face*, *Upload*, vyberte fotografii v umístění *Obrázky/Z fotoaparátu* a potvrďte *OK*. Tato osoba bude disponovat 2 způsoby autentizace – kartou a geometrií obličeje. Kartu přidělíme osobě kliknutím na symbol + u nápisu *Card* v sekci *Credential*, napíšeme číslo jedné ze 2 karet a potvrdíme. Záznam obličeje osoby je již nahraný. Pro přidání záznamu otisku prstu je zapotřebí připojit k PC podporovanou externí čtečku otisku prstů, kterou však tento panel není vybaven. Níže v dalších sekcích je možné přidat další parametry osoby, například její oprávnění, datum narození, datum nátupu, atd. V sekci *Access Control* zaškrtněte políčko *Device Operator*, které umožní osobě přistupovat do nastavení terminálu. Vytvoření osoby potvrďte kliknutím na *Add*.
6. Podobným způsobem vytvořte osobu Dělník. *Person ID* osoby bude 2, *Name* Delnik, foto nepřidávejte, a jako způsob autentizace přidejte pouze kartu. Pokud zadáte stejné číslo karty jako u předchozí osoby, tak nebude karta přidána za účelem zamezení duplicity karet.
7. Osoby, které byly nyní vytvořeny, nejsou uloženy do databáze osob v terminálu. Jděte do hlavního menu a do modulu *Access Control*, kde si vytvoříte skupinu a naimportujete data do terminálu. Rozklikněte *Authorization* a klikněte na *Access Group*, poté na *+Add*, *Name* napište „Permissions“ a zaškrtněte políčka *New Organization* a *Biometrická čtečka*. Provedené změny uložte tlačítkem *Save*. Zaškrtněte políčko u vytvořené skupiny a klikněte na *Apply Changes to Device* viz obr. A.9. Tím se osoby propíšou do databáze terminálu. Okno se zprávou o propsání můžete zavřít.
8. Nyní si vyzkoušejte autentizaci vytvořených osob na terminálu, tedy geometrií



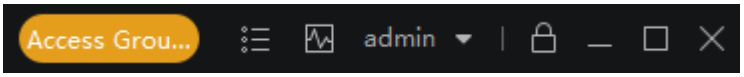
Obr. A.9: Access Group

obličeje a kartami.

9. Na terminálu přidejte autentizaci otiskem prstu osobě Dělník. Pokud nevíte jak, podívejte se na postup v 1. části laboratorní úlohy. Poté ověřte funkčnost.
10. Přepněte se zpět v programu do modulu *Person*, otevřete dvojklikem nebo tlačítkem *Edit* osobu Delnik a v sekci *Access Control* zaškrtněte *Mark as Visitor* a hodnotu *Valid Times for Visit* nastavte na 3 viz obr. A.10. Potvrďte *OK*. Nahoře se zobrazil žlutý nápis *Access Group to Be Applied* viz obr. A.11, na který klikněte a dejte *Apply Now*, což propíše provedené změny do terminálu. Tento parametr *Mark as Visitor* udává počet povolených autentizací dané osoby. Vyzkoušejte se tedy na terminálu 5x autentizovat jako osoba Dělník. Od 4. pokusu bude přístup zamítnut, protože byly povoleny jen 3 přístupy. Každá změna v programu se musí přes žlutý nápis propsat do terminálu.

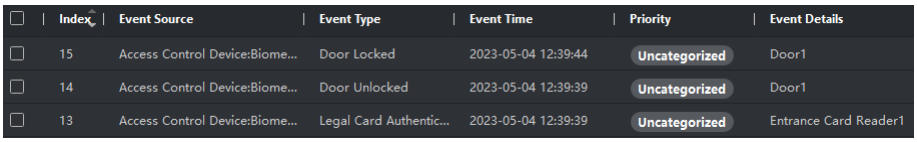


Obr. A.10: Mark as Visitor



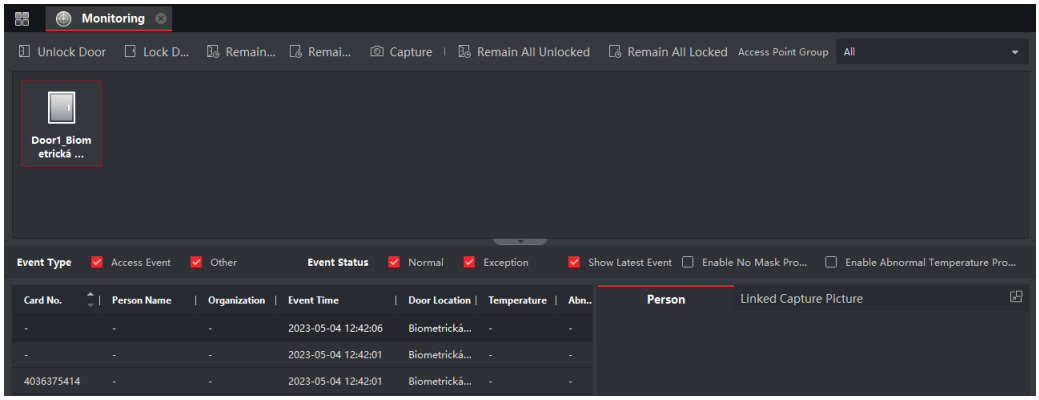
Obr. A.11: Upozornění na nepropsané změny

11. Jděte do hlavního menu v programu iVMS a přepněte se do modulu *Event Center*. Tento modul se skládá ze 2 sekcí a slouží k monitorování událostí. V první sekci se události zobrazují Real-time, tedy ihned po jejich zaznamenání. Vyzkoušejte si provést autentizaci na terminálu a vidíte, jak se ihned propsaly 2 zaznamenané akce a 3. akce po pár vteřinách (autentizace, odemčení zámku, zamčení zámku) viz obr. A.12. Přepněte se do druhé sekce *Event Search*, která slouží k vyhledávaní událostí na základě zadaných parametrů. V kolonce *Time* zvolte dnešní datum, *Start Time* zadejte o 10 minut pozdější aktuální čas a dejte *Search*. Vypsaly se události, které byly zaznamenány v zadaném časovém úseku. Proveďte jakoukoliv autentizaci a vidíte, že nebyla do výpisu připsána. Je nutné dát znovu *Search* pro aktualizování dat.



Obr. A.12: Výpis událostí v modulu Event Center

12. Jděte do hlavního menu a přepněte se do modulu *Monitoring*. Tento modul je velice podobný sekci *Real-time* v *Event Centru*, opět zobrazuje zaznamenané akce ihned bez nutnosti aktualizování. Dále je odtud možné vzdáleně ovládat zámek bez potřeby autentizace. Zvolte dostupný zámek (*Door1_Biometrická čtečka*) a zobrazí se jednotlivé možnosti viz obr. A.13. K dispozici je možnost otevřít nebo zavřít zámek na krátký časový interval a otevřít nebo zavřít zámek na dobu neurčitou. Dále je možné pořídit fotografii kamerou na terminálu či otevřít/zavřít všechny zámky naráz. Ve spodní části modulu se nachází výpis akcí s informacemi o autentizované osobě. V případě zájmu si můžete jednotlivé prvky ovládání zámku vyzkoušet.



Obr. A.13: Modul Monitoring

A.5 Otázky

1. Jakým způsobem program iVMS 4200 upozornil, že došlo ke změnám a nejsou propsány do terminálu?
2. Je možné monitorovat ve webovém rozhraní a v programu iVMS 4200 události zaznamenané terminálem? Pokud ano, předveďte vyučujícímu.
3. Zjednodušeně popište princip správy databáze osob prostřednictvím každé ze všech 3 možností.

A.6 Uvedení do původního stavu

Reset terminálu:

1. Přejděte do hlavního menu terminálu.
2. Zvolte modul *Data*.
3. Zvolte možnost *Delete Data*, poté *User Data*.
4. Potvrďte *OK*.

Reset webového rozhraní:

- Neprovádí se, protože webové rozhraní čerpá aktuální data z terminálu.

Reset programu iVMS 4200:

1. Odeberte zařízení v *Device Management*.
2. Odeberte osoby v modulu *Person*.
3. Odeberte skupinu v *Access Control*.

Smažte svou fotografii ze složky *Obrázky/Z fotoaparátu* a odpojte webkameru od počítače.
Vypněte virtualizovaný operační systém a poté i samotný počítač.
Po provedení všech kroků pro reset odpojte přívod napětí do zásuvek.

B Laboratorní úloha systému biometrické kontroly vstupu – dokumentace pro vyučujícího

Tento dokument je určen výhradně vyučujícímu a poskytuje informace o způsobu napájení jednotlivých komponent, přípravě pracoviště a otázky, na které se vyučující při kontrole vypracování úlohy studentů zeptá.

B.1 Napájení komponent

Napájení vyžadují pouze 2 komponenty viz. následující podkapitoly. Na zadní straně panelu jsou umístěny 2 zásuvky na 230 V/AC pro napájení obou komponent. Do zásuvek je přiveden proud flexo šňůrou 3x1,5 mm^2 s vidlicí, která se zapojí do klasické 230 V/AC zásuvky. Jednotlivé vodiče jsou propojeny pomocí svorkovnice, která je umístěna do ochranné krabičky. Ochranná krabička se dá otevřít například malým plochým šroubovákem.

B.1.1 Terminál Hikvision DS-K1T671MF

Napájení terminálu zajišťuje síťový adaptér s napětím 12 V/DC. Kladný vodič adaptéru je pomocí svorkovnice spojen s kladným vodičem teminálu, označeným A1. Záporný vodič je opět pomocí svorkovnice spojen se záporným vodičem terminálu, označeným A2. Adaptér obsahuje LED diodu k indikaci funkčnosti napájení.

B.1.2 Elektrický zámek dveří Fermax

Zámek je v klidovém stavu bez napětí – uzamčen. V momentě, kdy terminál zaznamená úspěšnou autentizaci, je do zámku na cívku přivedeno napětí, a dojde tak k odemčení zámku. Adaptér zámku taktéž obsahuje LED diodu k indikaci funkčnosti napájení.

B.2 Příprava pracoviště

Laboratorní úloha se bude vypracovávat na stanovišti, které předem určí vyučující, a budou v ní používány následující komponenty:

- Terminál Hikvision DS-K1T671MF
- Elektrický zámek dveří Fermax
- 2x Bezkontaktní karta Mifare (4036375414 a 4124954550)

- Webkamera Niceboy
- PC s virtualizovaným operačním systémem Windows 10
- Software iVMS 4200

Student nejprve zapojí vidlici pro přívod napájení panelu do nejbližší zásuvky ve stole a UTP kabel do portu na konektor RJ-45 umístěný ve stole. Dále zapojí přichystané 2 adaptéry do zásuvek na panelu a tím uvede systém do provozu. Pro ovládání terminálu specializovaným softwarem si student zapne a připraví PC k tomu určený. Poté postupuje podle přichystaného návodu k vypracování laboratorní úlohy.

B.3 Přístupové údaje

Heslo k nastavení terminálu: Adminpristup123
iVMS 4200: Username – admin
iVMS 4200: Password – Pristup*

B.4 Síťové nastavení

Terminál je do školní sítě připojen LAN kabelem. V nastavení připojení terminálu je vypnuta funkce DHCP a nastavena tato statická adresa:

- IP adresa – 147.229.149.241
- Maska podsítě – 255.255.254.0
- Výchozí brána – 147.229.149.1

B.5 Další parametry nastavení terminálu

Tyto parametry slouží především pro případ, kdy student pozmění neoprávněně nastavení terminálu. Vyučující provede vymazání nastavení přes Menu – Maint. – Restore to Default Settings. Alternativou je Factory restore, který navíc smaže síťové nastavení a proto ho bude zapotřebí nastavit.

- Hlasitost terminálu: Menu – Basic – Voice Settings – Voice Volume – 1
- Doba otevření zámku po úspěšné autentizaci: Menu – ACS – Open Duration (s) – 5
- Interval mezi autentizacemi: Menu – ACS – Authentication Interval (s) – 5
- Přijatelná vzdálenost obličeje od terminálu: Menu – Biometrics – Recognition distance – 1 m

B.6 Průběh vypracování laboratorní úlohy

V první části si student vyzkouší ovládání přímo na terminálu. Nejprve vytvoří osoby v databázi a přidá způsoby autentizace. Poté si student vyzkouší, jak jednotlivé vytvořené autentizační metody fungují.

Ve druhé části bude student ovládat terminál z webového rozhraní prohlížeče, na který se připojí dle návodu. Zde si student vyzkouší opět přidání, úpravu, či smazání osoby v databázi. Dále si vyzkouší monitorovat akce na terminálu taktéž z webového rozhraní.

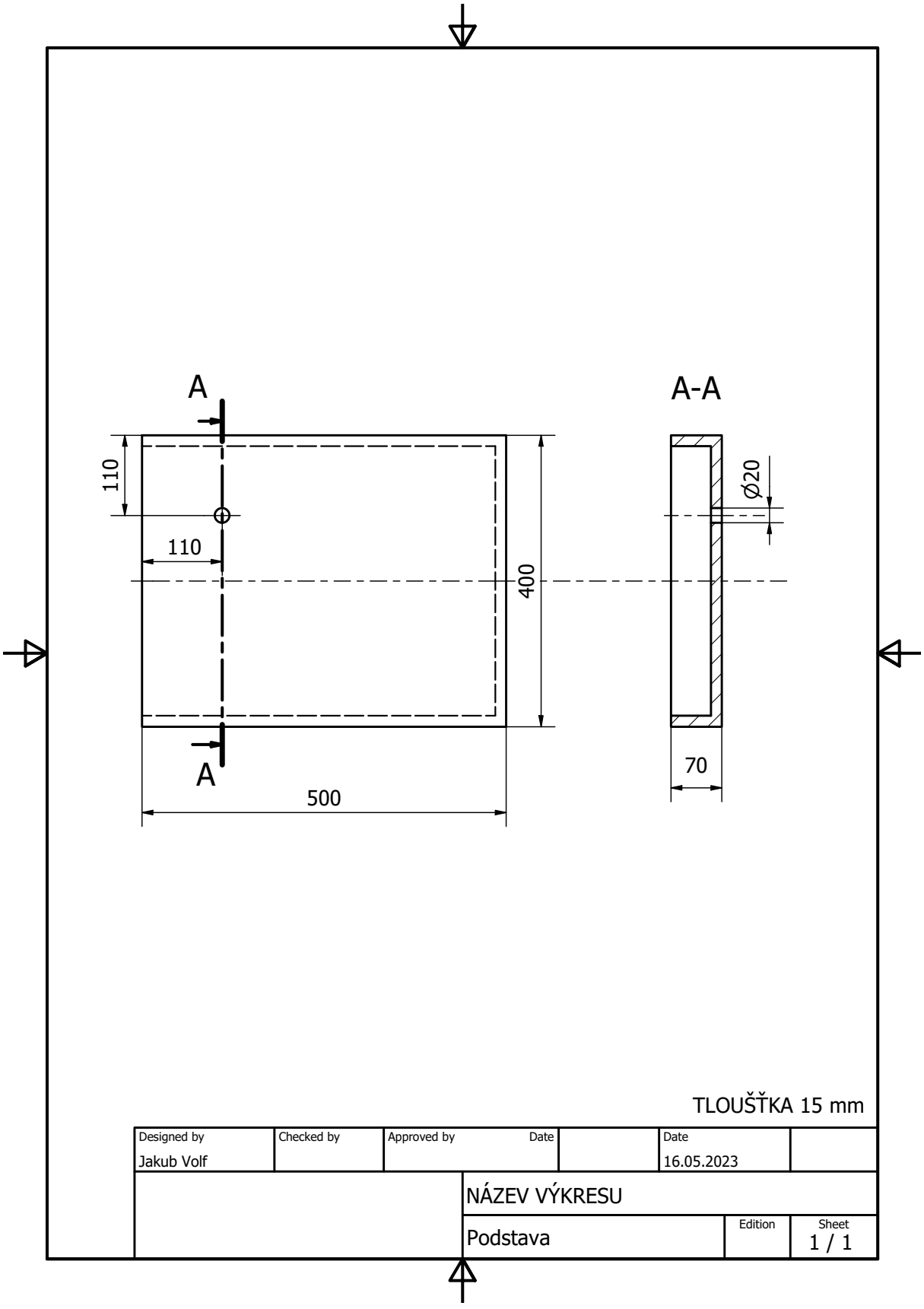
Ve třetí části si student vyzkouší ovládání terminálu z prostředí specializovaného softwaru. Software je přichystán na virtualizovaném operačním systému a dostane se k němu opět dle návodu. Ovládání terminálu pomocí softwaru je podobné webovému rozhraní, ale nabízí mnoho dalších funkcí, možností a je uživatelsky příjemnější.

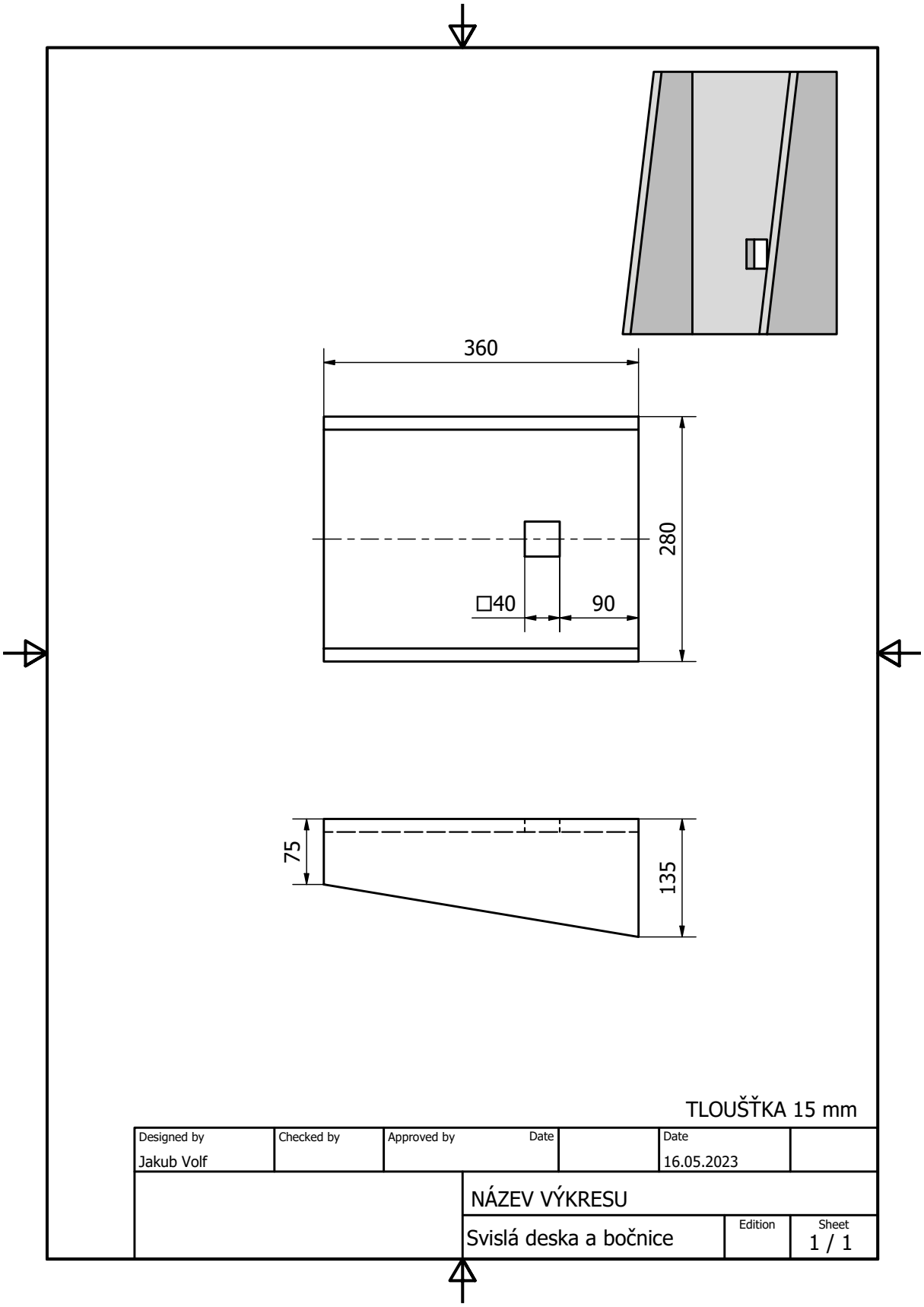
Po splnění všech tří částí a zodpovězení na otázky od vedoucího uvede student zařízení do původního stavu podle instrukcí obsažených v návodu.

B.7 Otázky pro studenty

1. **Jakým způsobem program iVMS 4200 upozornil, že došlo ke změnám a nejsou propsány do terminálu?** V horní liště se zobrazí žlutý nápis Access Group to Be Applied
2. **Je možné monitorovat ve webovém rozhraní a v programu iVMS 4200 události zaznamenané terminálem? Pokud ano, předveďte vyučujícímu.** Ano, je to možné.
3. **Zjednodušeně popište princip správy databáze osob prostřednictvím každé ze všech 3 možností.**

C Výkresová dokumentace



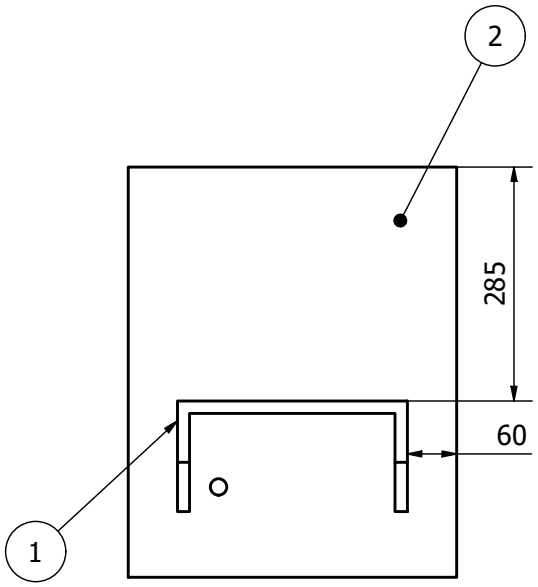


TLOUŠŤKA 15 mm

Designed by	Checked by	Approved by	Date	Date	
Jakub Volf				16.05.2023	

	NÁZEV VÝKRESU		
	Svislá deska a bočnice	Edition	Sheet 1 / 1

KUSOVNÍK			
DÍL	POČET	NÁZEV	POPIS
1	1	Svislá deska a bočnice	
2	1	Podstava	



Designed by	Checked by	Approved by	Date		Date	
Jakub Volf					16.05.2023	
		NÁZEV VÝKRESU				
		Sestava		Edition	Sheet	1 / 1