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 ELEKTRONICKÉ KONTROLY VSTUPU

LABORATORY TASK OF THE ELECTRONIC ACCESS CONTROL SYSTEM

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE — Tomáš Maňásek

AUTHOR

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

SUPERVISOR

BRNO 2022

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní program **Telekomunikační a informační systémy**

Ústav telekomunikací

Student: Tomáš Maňásek ***ID:*** 221283

Ročník: 3 ***Akademický rok:*** 2021/22

NÁZEV TÉMATU:

Laboratorní úloha systému elektronické kontroly vstupu

POKYNY PRO VYPRACOVÁNÍ:

Nastudujte a popište problematiku systémů elektronické kontroly vstupu (EKV). Na základě dodaných komponent navrhněte a prakticky realizujte systém EKV na výukovém panelu. Pro vytvořený systém navrhněte laboratorní úlohu v trvání 90 minut. Pro tuto úlohu zpracujte dokumentaci pro studenty a také pro vyučujícího. Řídící software úlohy poběží v podobě virtuálního stroje typu VMware.

DOPORUČENÁ LITERATURA:

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

[2] Příručka k uvedení systému NetAXS-123 do provozu. Honeywell, Brno 2010.

Termín zadání: 7.2.2022 ***Termín odevzdání:*** 31.5.2022

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

prof. Ing. Jiří Mišurec, CSc.
předseda rady studijního programu

ABSTRAKT

Cílem této bakalářské práce je nastudovat a popsat problematiku elektronické kontroly vstupu. Na základě dodaných komponent navrhnout a realizovat EKV systém na výukovém panelu. Pro vytvořený systém navrhnout laboratorní úlohu v trvání 90 minut. Pro tuto úlohu zpracovat dokumentaci pro studenty a vyučujícího.

KLÍČOVÁ SLOVA

Zabezpečovací systémy, Laboratorní úloha, Elektronická kontrola vstupu

ABSTRACT

The aim of this bachelor thesis is to study and describe access control systems. Based on the supplied components, design and implement an EKV system on the teaching panel. Design a laboratory task lasting 90 minutes for the created system and prepare documentation for students and the teacher for this task.

KEYWORDS

Security systems, Laboratory exercise, Access control system

MAŇÁSEK, Tomáš. *Laboratorní úloha systému elektronické kontroly vstupu*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2022, 44 s. Bakalářská práce. Vedoucí práce: doc. Ing. Karel Burda, CSc.

Prohlášení autora o původnosti díla

Jméno a příjmení autora:	Tomáš Maňásek
VUT ID autora:	221283
Typ práce:	Bakalářská práce
Akademický rok:	2021/22
Téma závěrečné práce:	Laboratorní úloha systému elektronické 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 prof. Ing. Karlu Burdovi, CSc. za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Obsah

Úvod **10**

1 Teoretická část **11**
1.1 Řízení přístupu v EKV . . . 11
1.2 Docházkové systémy . . . 11
1.3 Autentizace a její typy . . . 12
1.3.1 Autentizace heslem . . . 12
1.3.2 Autentizace předmětem . . . 12
1.3.3 Autentizace biometrikou . . . 13
1.4 Autentizační předměty . . . 13
1.4.1 typy úložiště . . . 14
1.4.2 Typy komunikačního rozhraní . . . 16
1.5 Biometrické metody autentizace . . . 17
1.5.1 Autentizace otisky prstů . . . 17
1.5.2 Autentizace geometrií obličeje . . . 18

2 Praktická část **20**
2.1 Použité komponenty . . . 20
2.1.1 Ústředna Honeywell NetAXS-123 . . . 20
2.1.2 rozšiřující modul NXD1 . . . 20
2.1.3 RFID čtečka karet HIDD iclass . . . 20
2.1.4 Odchodové tlačítko Rosslare EX-06 . . . 21
2.1.5 Elektrický dveřní zámek FAB Profi 1211 . . . 21
2.1.6 RFID karta HID iClass GP . . . 21
2.1.7 PoE přepínač Tenda . . . 21
2.2 Použitý software . . . 21
2.2.1 VMWare Workstation 15 Player . . . 21
2.3 Návrh výukového systému . . . 22
2.3.1 Návrh zapojení . . . 22
2.3.2 Návrh výukového panelu . . . 22

3 Návod k laboratorní úloze **26**
3.1 Teoretický úvod . . . 26
3.1.1 Zapojení úlohy . . . 26
3.2 Návod k vypracování úlohy . . . 28
3.2.1 Spuštění virtuálního stroje . . . 28
3.2.2 Přihlášení do webového rozhraní . . . 28

3.2.3 Resetování konfigurace 29
3.2.4 Nastavení času a časových zón 30
3.2.5 Nastavení dveří 1 32
3.2.6 Nastavení dveří 2 33
3.2.7 Přidání přístupových úrovní 35
3.2.8 Přiřazení čipových karet 36
3.2.9 Ověření laboratorní úlohy 37
3.2.10 Sledování událostí 38
3.2.11 Ukončení laboratorní úlohy 38

4 Návod k laboratorní úloze pro vyučující **39**
4.1 NetAXS-123 obnovení základní konfigurace 39
4.1.1 Plný reset ústředny 39
4.1.2 Nastavení ústředny pro konfiguraci přes webové rozhraní . . . 40
4.1.3 Nahrání základní konfigurace 40

Závěr **42**

Literatura **43**

Seznam symbolů a zkratek **44**

Seznam obrázků

1.1 Konektor technologie i-Button 16
1.2 Papilární obrazce 17
2.1 Schéma zapojení 23
2.2 Konstrukční výkres panelu. 24
2.3 Rozmístění prvků na výukovém panelu. 25
2.4 Realizace výukového panelu. 25
3.1 Blokové schéma zapojení laboratorní úlohy. 27
3.2 Rozmístění prvků na přípravku. 27
3.3 RUN LED umístění. 28
3.4 Nastavení aktuálního času. 30
3.5 Časové zóny - výchozí tabulka. 31
3.6 Časové zóny - výsledná tabulka. 31
3.7 Dveře 1 čtečka A nastavení. 32
3.8 Dveře 1 nastavení výstupu. 33
3.9 Dveře 1 nastavení vstupu pro odchod. 33
3.10 Dveře 2 čtečka A nastavení. 34
3.11 Dveře 2 nastavení výstupu. 34
3.12 Přidání přístupové úrovně „Plný přístup“. 35
3.13 Přidání přístupové úrovně „Výroba“. 36
3.14 Přidání přístupové úrovně „Úklid“. 36
3.15 Přidání nových karet. 37
4.1 Umístění DIP switche. 39
4.2 Umístění RUN LED. 39

Úvod

Tato bakalářská práce se zabývá problematikou elektronické kontroly vstupu. Dále je na základě dodaných komponent navržen výukový systém pro účely laboratorní úlohy. Tento návrh je následně realizován v podobě přípravku pro laboratorní úlohu. K laboratorní úloze je také navržen jak návod a dokumentace k vypracování úlohy pro studenty, tak návod pro vyučující obsahující postupy k řešení nejčastějších problémů které by mohly nastat.

V teoretické části se práce věnuje výše zmíněné problematice elektronické kontroly vstupu (EKV). Popisuje jejich fungování, dále se věnuje autentizaci a jejímu typovému rozdělení, autentizačními předměty a jejich dělení podle typu úložiště a typu komunikačního rozhraní. Dále jsou v práci popsány metody biometrické autentizace pomocí otisku prstů a geometrie obličeje.

Praktická část se v prvním bodě zabývá použitými komponenty k realizaci výukového panelu. Jedná se o kontrolér NatAXS-123, dvě čtečky karet iClass R10, čtyři RFID karty HID iClass GP, odchodové tlačítko Rosslare EX-06, dva elektrické zámky FAB Profi 1211 a PoE přepínač Tenda. Dále se věnuje návrhu a realizaci výukového panelu a celé laboratorní úlohy.

K laboratorní úloze je vypracován návod s pracovním postupem pro její plnění v rámci výuky a také návod pro dohlížející vyučující.

1 Teoretická část

Elektronická kontrola vstupu EKV je elektronický systém, sloužící k automatizovanému řízení vstupu do kontrolované oblasti [7].

EKV eliminuje potřebu užívání klasických klíčů, které jsou nahrazeny jiným způsobem rozpoznání osoby, například čipovou kartou nebo specifickým heslem. Systémy EKV umožňují omezovat vstup neautorizovaných osob, selektivně řídit přístup autorizovaných osob, sledovat příchod a odchod osob a časově tento přístup omezit.

1.1 Řízení přístupu v EKV

Řízení přístupu je proces regulace přístupu osob a jiných zařízení do řízených prostor. Je důležité, aby přístup do kontrolované oblasti měly pouze vybrané osoby.

Aby osoba mohla používat vstupy do kontrolované oblasti, musí být nejprve autorizována autoritou (např. správcem budovy). V průběhu autorizace autorita osobě sdělí přístupová práva (tj. jaké vstupy v jakou časovou dobu smí používat). Dále autorita přiděluje každé osobě tzv. identifikátor ID, což je jednoznačná informace vyjadřující tuto osobu. Rovněž s osobou sjedná dvojici údajů potřebné k její identifikaci, ověřovací faktor OF a dokazovací faktor DF. DF jsou data kterými bude osoba prokazovat svoji identitu. Tyto data má osoba u sebe k dispozici. OF jsou data, podle kterých bude systém ověřovat identitu osoby. Tyto data jsou naopak s ID uložena do databáze systému [7].

Pro vstup nebo výstup z kontrolovaného prostoru musí osoby projít určeným přístupovým místem. Tato přístupová místa jsou obvykle opatřena nějakým typem zábrany, nejčastěji dveřmi, nebo přístupovými terminály. Pro průchod přístupovým místem do chráněné oblasti musí osoba prokázat svou identitu pomocí dokazovacího faktoru DF. Poté co osoba uvede svůj DF, systém podle něj zjistí z databáze přidělená přístupová oprávnění a na jejich základě osobu propustí do prostoru, nebo žádost o průchod zamítne. Při výstupu z oblasti se kontrola oprávnění osoby provádí jen v případech, kdy je vyžadována vysokým stupněm zabezpečení. V ostatních případech je v blízkosti zábrany umístěno tlačítko pro odchod, jehož stiskem se zábrana otevře a osoba může opustit objekt bez nutnosti se znovu autentizovat [8].

1.2 Docházkové systémy

Docházkový systém je velmi blízký k systému přístupovému. Docházkový systém zajišťuje evidenci pohybu osob v kontrolovaných prostorech. Na rozdíl od přístupového systému neprovádí regulaci průchodu osob přístupovými místy ale pouze průchody zaznamenává [8].

Díky své blízkosti, docházkové systémy často bývají kombinované se systémy přístupovými.

1.3 Autentizace a její typy

Autentizace se provádí při vstupu osoby do kontrolovaného prostoru. Autentizace je ověření identity osoby žádající o vstup (tzv. žadatel). Za účelem autentizace žadatel předkládá tzv. nosič dokazovacího faktoru, což může být autentizační předmět (např. čipová karta), nebo osoba samotná (např. otisk prstů). Nosič dokazovacího faktoru obsahuje tzv. dokazovací faktor DF, kterým žadatel může prokázat přístupovému systému svou identitu. Dokazovací faktor mohou být buď charakteristické rysy žadatele, či autentizačního předmětu, nebo nějaké tajné informace. Autentizaci provádí tzv. autentizátor. U přístupových systémů s výpočetně náročnou metodou je autentizátor součástí přístupové jednotky. autentizaci provádí pomocí tzv. dokazovacího procesoru, který je také součástí jednotky. V případě méně náročné metody se autentizátor nachází na ústředně přístupového systému. Autentizátor má k dispozici tzv. ověřovací faktor OF (např hash hesla), kterým může pomocí autentizačního protokolu ověřit zda se jedná o oprávněnou osobu. Dokazovací faktor a ověřovací faktor jsou sjednávány v rámci autorizace.

1.3.1 Autentizace heslem

Metoda autentizace heslem předpokládá, že uživatel má znalost jedinečného hesla, které je ideálně známé jen uživateli samotnému. Autentizaci uživatel provádí tak, že své jedinečné heslo zadá ve správné posloupnosti na klávesnici přístupového terminálu. Hash hesla se následně porovná s hash hesly v paměti ústředny. Pokud je hash zadaného hesla shodný s hash heslem v přístupovém seznamu, uživatel je úspěšně autentizován.

Výhoda této metody spočívá v tom, že uživatel nepotřebuje žádný fyzický identifikační předmět, což snižuje pořizovací a provozní náklady přístupového systému.

1.3.2 Autentizace předmětem

Tato metoda předpokládá, že má uživatel při sobě určitý identifikační předmět. Tento předmět má v sobě zapsanou jedinečnou informaci, která uživatele identifikuje. Autentizační předměty se pohybují v mnoha různých typech a tvarech. Jejich principy a rozdělení jsou popsány v sekci 1.4.

1.3.3 Autentizace biometrikou

Autentizace biometrikou využívá jedinečné tělesné rozměry a vlastnosti osoby. U této metody není nutné nosit identifikační předmět, nebo si pamatovat heslo. Jako dokazovací faktor slouží tělo osoby žádající o autentizaci.

Pro použití této metody si musí každý uživatel nejprve projít procesem získávání co nejpodrobnějšího referenčního vzoru zvolené biometriky který slouží jako ověřovací faktor. Tento sňatý vzor biometriky osoby je následně uložen do paměti zařízení. Pro požádání o přístup žadatel nechá změřit své biometrické údaje a autentizátor přístupového systému tyto změřené údaje porovná s biometrickým vzorem dříve vloženým do ověřovacího seznamu.

V praxi využívané biometriky:

- Otisky prstů
- Obličej
- Oční duhovka
- Oční sítnice
- Geometrie ruky

Biometrické metody využívající otisku prstů a geometrie obličeje jsou podrobněji vysvětleny v sekci 1.5.

1.4 Autentizační předměty

Autentizační předmět je předmět, sloužící k prokázání identity osoby které patří. Předmět může být buď nějaký průkaz, nebo paměťové úložiště. Autentizace průkazem je založena na unikátních rysech specifických pro daný typ průkazu jako např. identifikační údaje držitele a ochranné prvky. Tento typ autentizace se používá téměř výhradně při autentizaci osobou (např. pracovník ostrahy). Důvodem je to, že pravost průkazu lze poměrně rychle ověřit lidmi, zatímco strojová kontrola ochranných prvků vyžaduje speciální techniku která je nákladná. Proto se v přístupových systémech založených na autentizátorech strojového typu používají téměř výhradně autentizační předměty paměťové. Autentizační předměty paměťové lze rozdělit podle:
a) tvaru a velikosti:
   - karty
   - přívěšky
   - náramky
b) typu úložiště:
   - magnetová páska
   - Wiegandův drát
   - paměťový čip

- mikroprocesor

c) komunikačního rozhraní:
   - snímač magnetického záznamu
   - galvanické rozhraní
   - rádiové rozhraní

Na velikosti a tvaru autentizačního předmětu záleží pouze z hlediska lidské manipulace. Je důležité aby předmět osobám nepřekážel, byl dobře manipulovatelný a aby nebyl náchylný na ztrácení. Z těchto důvodů jsou nejpoužívanější zejména karty a přívěšky kdy karty lze lehce přenášet například v peněžence a přívěšky se dají bezpečně připnout např. na klíče nebo na batoh. Z technického hlediska je tvar a velikost autentizačního předmětu nepříliš podstatný [8].

1.4.1 typy úložiště

Karta s magnetickým proužkem

Základem karty je magnetický proužek složený z kovových zmagnetizovatelných částeček. Pomocí standardní magnetické zapisovací a čtecí hlavy lze do magnetického proužku zapisovat a číst data ve třech paměťových stopách. První stopa může nést až 76 7 bitových znaků, druhá stopa umožňuje 37 5 bitových znaků a třetí stopa 104 numerických 5 bitových znaků [9]. K zápisu a čtení údajů na kartě se většinou používá protahovací čtečka karet.

Magnetické karty jsou velmi levné a spolehlivé. Jsou však zastaralé a snadno klonovatelné což je dělá málo bezpečnými.

Wiegandova karta

Základem Wiegandovy karty jsou dva řádky 10 mm dlouhých drátků o průměru 1 mm, které jsou do karty zalisovány. Dráty v horním řádku reprezentují bit s hodnotou 1 a dráty v řádku spodním bit s hodnotou 0. Každá karta má unikátní posloupnost 26 bitů, která je použita k identifikaci uživatele a zároveň k autentizaci. Dráty jsou vytvořené ze speciální slitiny kobaltu, železa a vanadu a jejich jádro a plášť mají různou magnetickou tvrdost. Jde o tzv. Wiegandův drát. Jádro drátu je magneticky měkčí než jeho plášť, proto vyžaduje značně menší intenzitu magnetického pole k přemagnetování než plášť.

Čtení dat z Wiegandovy karty umožňuje tzv. Wiegandův jev. V klidovém stavu stavu má jádro a plášť stejnou polaritu, protože magneticky tvrdý plášť přemagnetuje magneticky měkké jádro na souhlasnou polaritu. Pohybem ve čtečce se dráty postupně ocitají v blízkosti dostatečně silného nastavovacího magnetu aby přepolarizoval jádro i plášť drátu na určenou polaritu. Dále se dráty ocitnou v blízkosti

překlápěcího magnetu, který je schopný přepolarizovat pouze magneticky měkké jádro drátu. Při přemagnetování jádra nastane tzv. Wiegandův jev, kdy na snímací cívce umístěné blízko překlápěcího magnetu lze detekovat napěťový impulz. Ve čtečce jsou tyto cívky dvě, jedna v blízkosti horní řady drátů a druhá v blízkosti řady dolní. Pokud je impulz na horní snímací cívce, zaznamená se bit s hodnotou 1, pokud na cívce dolní, půjde o bit s hodnotou 0.

Výhodou tohoto typu karet je poměrně komplikovaná tvorba duplikátu a jejich nízká cena.

Karta s paměťovým čipem

Tyto karty jsou založeny na paměťovém čipu (zpravidla paměť typu EEPROM). Podporují pouze autentizační metodu založenou na předání hesla. V momentě kdy autentizátor detekuje připojení paměti, tak kartě vyšle výzvu k zaslání svého obsahu. Karta na výzvu reaguje zasláním požadovaných dat autentizátoru, který je poté porovná s daty ze svého ověřovacího seznamu. Aby se zvýšila bezpečnost popsaného autentizačního protokolu, používají se paměťové čipy, které před odesláním dokazovacího faktoru vyžadují heslo pro zpřístupnění jejich obsahu. Heslo autentizátor posílá s výzvou k zaslání dat.

Karta s mikroprocesorem

Jde o karty obsahují vlastní mikropočítač. Mikropočítač umožňuje provádění kryptografických operací. Toho je využito pro šifrované ověření dokazovacího faktoru neseného kartou. V mikroprocesorových kartách se zpravidla využívá symetrická kryptografie. Obě strany sdílejí stejnou tajnou hodnotu, tzv. klíč K. Tato hodnota slouží jako dokazovací faktor DF i jako ověřovací faktor OF. platí tedy že K = DF = OF. Identifikace karty probíhá následovně [7]:

1. Přiblížením karty k terminálu se aktivuje přenosový kanál.
2. Karta vyšle svůj identifikátor ID.
3. Terminál nalezne v ověřovacím seznamu klíč K odpovídající tomuto ID.
4. Terminál vygeneruje náhodné číslo R, které zašle kartě.
5. Karta toto číslo zašifruje svým klíčem K a pošle jej v zašifrované podobě zpět.
6. Terminál dešifruje přijatý kryptogram a výsledné číslo porovná s číslem R.
7. Pokud se dešifrované číslo rovná číslu R, mikroprocesor karty má k dispozici tajný klíč K který byl přidělen identitě ID jako její dokazovací faktor.
8. Hodnotu ID terminál pošle kontroleru který ji standardně zpracuje.

Karty s mikroprocesorem mají vysokou úroveň bezpečnosti na úkor vyšší pořizovací ceny.

1.4.2 Typy komunikačního rozhraní

Magnetické rozhraní

Tato rozhraní jsme již popsali u magnetických a Wiegandových karet. V případě magnetických karet tvoří komunikační rozhraní magnetický pásek karty a čtecí hlava přístupového terminálu. Karta s magnetickým páskem je protažena přístupovým terminálem se čtecí hlavou, ta umožní přečíst dokazovací faktor a identifikační údaje držitele karty. Komunikační rozhraní Wiegandových karet tvoří 26 Wiegandových drátů zalisovaných v kartě a čtecím zařízením již popsaným u Wiegandových karet.

Galvanické rozhraní

Mezi nejpoužívanější galvanická rozhraní patří např. rozhraní typu USB (Universal Serial Bus). Toto rozhraní se však pro účely autentizace nepoužívá. Důvodem je skutečnost, že pro galvanické připojení je nutné předmět připojit na přesně danou pozici, což je pro časté používání nepohodlné. Rozhraní technologie i-Button tento problém vyřešilo svým speciálním konektorem. Připojení zařízení ke konektoru je rychlé a spolehlivé [8] viz. obrázek 1.1.

Obr. 1.1: Konektor technologie i-Button.

Rádiové rozhraní

Asi nejpoužívanější rádiové rozhraní pro bezdrátovou komunikaci je rozhraní pro karty s vazbou na vzdálenost do 10 cm. Popisuje jej standard ISO/IEC 14443 [6]. Tyto karty mají v sobě zalisovanou cívku, která funguje jako anténa a paměťový nebo mikroprocesorový čip. Rozhraní pracuje na kmitočtu 13,56 MHz. Bezdrátové karty mohou mít buď napájení aktivní, nebo napájení pasivní. U aktivního napájení je karta napájena např. baterie, zatímco karta s napájením pasivním získává energii elektromagneticky ze čtečky. Karty s pasivním napájením jsou mnohem rozšířenější, protože jsou levnější a nepotřebují měnit baterie. Napájení karet bez vlastního zdroje funguje následujícím způsobem. Čtečka karet generuje magnetické pole o kmitočtu

13,56 MHz. Pokud se cívka karty přiblíží dostatečně k cívce čtečky, vytvoří transformátor. Přes transformátor se část energie generované cívkou čtečky přenese na cívku karty, ta je poté usměrněna a přivedena na kondenzátor, sloužící jako zdroj napájení karty. Karta následně odešle uložené informace pomocí tzv. zátěžové modulace, kdy tranzistor odpojuje a připojuje paralelní zátěžový rezistor k cívce karty. Pokud je zátěžový rezistor odpojen, na cívce bude poměrně nízký proud, což odpovídá vysílanému stavu H. Pokud je zátěž připojena, proud cívkou karty vzroste. Z důsledku transformátorové vazby zároveň naroste i proud v cívce čtečky. Měřením tohoto proudu čtečka zjistí stavy vysílané kartou.

1.5 Biometrické metody autentizace

1.5.1 Autentizace otisky prstů

Tato metoda autentizace je jednou z nejrozšířenějších biometrických metod. Vychází z existence papilárních linií na povrchu kůže (viz obr. 1.2). Identifikace je založena na snímání charakteristických obrazců tvořených z těchto linií.

Obr. 1.2: Papilární obrazce.

Nejpoužívanější metoda snímání papilárních linií je **metoda optická**. Tato metoda je založena na pořizování fotografií snímaného povrchu. Pomocí algoritmů se následně hledá, kde na povrchu jsou prohlubně a kde hřebeny. Tyto algoritmy analyzují, kde na pořízeném snímku jsou tmavá a kde světlá místa. Papilární linie budou světlejší než rýhy mezi nimi. Protože povrch přiložený ke snímači zakrývá většinu vnějšího světla, je nutné mít u snímače nějaký způsob přisvětlení, např. LED diody. Výhoda optických snímačů je jich nízká cena a odolnost. Nevýhodou je nutnost čištění snímače a nemožnost pořízení kvalitního snímku pokud je prst špinavý [8].

Další metodou snímání je metoda založená na **kapacitním snímání**. Kapacitní snímače hledají papilární linie měřením kapacity. Kapacitní snímače jsou složeny z

velkého množství vodivých ploch, poskládaných do matice a umístěných za izolační destičkou. Sousední vodivé plošky tvoří desky kondenzátoru. Na místech, kde je papilární linie v kontaktu s izolační vrstvou kapacita mezi vodivými ploškami poklesne. Na místě kde se nachází vzduchová mezera kapacita vzroste. Měřením těchto kapacit zjistíme kde se nachází papilární linie, což nám umožní utvořit obraz otisku. Výhodou kapacitního snímání je skutečnost, že dokáže sejmout obrazec papilárních linií i u špinavého nebo zamazaného prstu. Nevýhodou je jejich náchylnost na poškození elektrostatickým výbojem [8].

Následující metodou je metoda **snímání ultrazvukem**. Pod snímací destičkou je umístěn piezoelektrický krystal, generuje a zároveň přijímá ultrazvukové pulzy. Pro každý bod snímané plochy je vygenerován krátký akustický pulz. Část tohoto pulzu se odrazí od spodní části snímací destičky zpět. Přijímač tento odraz detekuje. Neodražená čast pulzu pokračuje materiálem snímací destičky dokud nedosáhne jejího povrchu kde se odrazí. Tento odraz je detekován. Pokud se na snímaném bodě nachází linie, další odraz již nenastane protože tkáň prstu zbytek vlnění pohltí. Pokud se na snímaném bodě nachází rýha, pokračuje vlnění vzduchem až ke kůži, kde se odrazí a následně je detekováno jako třetí odraz. Toto měření se provádí po celé ploše snímače. Podle počtu odrazů v každém bodě se následně vytvoří kompletní papilární obrazec přiloženého prstu. Výhodou ultrazvukového snímače je jeho nenáročnost na údržbu, jeho odolnost proti elektrostatické elektřině a schopnost správného snímání zašpiněných prstů. Nevýhodou je jeho vyšší cena [8].

Po sejmutí otisku prstu následuje jeho zpracování. Pro porovnání otisků prstu se používají tzv. markanty. Markanty jsou lehce rozpoznatelné útvary v obrazci papilárních linií. Tyto markanty se v obrazci vyhledávají a poté se ukládají jejich souřadnice s jejich typem a případně i úhel pod kterým rýha nebo line od daného markantu pokračuje. Takto zjištěné údaje se následně porovnávají s údaji biometrického vzoru. Podle míry jejich podobnosti se následně určí, zda je otisk žadatele přijat nebo zamítnut [8].

1.5.2 Autentizace geometrií obličeje

Další populární metoda autentizace. Princip spočívá v pořízení snímku obličeje žadatele, který je následně porovnáván s biometrickým vzorem. Podobnost obličejů se vyhodnocuje na základě tzv. obličejové metriky. Na snímku obličeje se vyhledají základní body obličeje (např. koutky očí, brada, koutky úst atp.), mezi kterými se následně měří vzdálenost. Tyto vzdálenosti jsou biometrikou snímané osoby. Ta se následně porovnává s biometrickým vzorem z databáze. Pokud systém nalezne dostatečnou shodu pořízeného snímku se vzorem v databázi, osoba dostane udělen

přístup do objektu.

2 Praktická část

2.1 Použité komponenty

Seznam dodaných komponentů k účelu realizace laboratorní úlohy:

- 1x Ústředna Honeywell NetAXS-123
- 1x rozšiřující modul NXD1
- 2x RFID čtečka karet HIDD iclass
- 1x Odchodové tlačítko Rosslare EX-06
- 2x Elektrický dveřní zámek FAB Profi 1211
- 1x RFID karta HID iClass GP
- 1x PoE přepínač Tenda

2.1.1 Ústředna Honeywell NetAXS-123

Ústředna NetAXS-123 je základem naší laboratorní úlohy. V základní konfiguraci ústředna umožňuje ovládat jeden vstup a připojit:

- Až dva terminály pro vstup
- odchodové tlačítko a kontrolu polohy dveří
- Zamykací nebo pomocná zařízení

Ústřednu lze napájet buď připojením 12 V vodiče nebo pomocí technologie PoE (Power over Ethernet). Připojení terminálu je provedeno přes rozhraní Wiegand sedmi vodiči. Pro připojení dvou terminálů pak osmi vodiči. K ústředně se lze připojit přes Ethernet pomocí TCP/IP protokolu nebo přes Micro USB-B kabel. Dále má ústředna pro potřeby návazného připojení svorky na připojení sběrnice RS 485. Tímto způsobem lze k ústředně navázat až 30 panelů kde pouze bránový panel má vlastní IP adresu [10].

2.1.2 rozšiřující modul NXD1

Rozšiřující modul umožňuje ústřednou ovládat další vstup. Modul umožňuje, stejně jak základní ústředna, připojení až dvou vstupních terminálů, připojení odchodového tlačítka snímače polohy dveří a zamykací nebo pomocná zařízení.

2.1.3 RFID čtečka karet HIDD iclass

RFID čtečka pracuje na frekvenci 13,56 MHz. K ústředně se připojuje sedmi vodiči. S ústřednou komunikuje na základě Wiegandova rozhraní.

2.1.4 Odchodové tlačítko Rosslare EX-06

Tlačítko s piezoelektrickým spínačem a LED indikací stavu. Tlačítko umožňuje nastavení délky sepnutí po stisknutí. Tlačítko komunikuje s ústřednou přes dvojici vodičů. Tlačítko slouží k opuštění kontrolovaného prostoru bez nutnosti autentizace.

2.1.5 Elektrický dveřní zámek FAB Profi 1211

Zámek ovládaný kontrolérem. Technické parametry:

- Napájení 8 - 12 V AC/DC
- Odběr cívek
- 12V AC = 300 mA
- 12V DC = 600 mA
- maximální doba držení cívek pod napětím: 60 s

V klidovém stavu je zámek v poloze BLOKOVÁNO. V poloze ODBLOKOVÁNO je jen po dobu, kterou je přivedeno napájení.

2.1.6 RFID karta HID iClass GP

Karta pracují na frekvenci 13,56 MHz

2.1.7 PoE přepínač Tenda

PoE přepínač umožňuje pomocí technologie Power over Ethernet napájet připojená zařízení přes UTP kabely. Náš přepínač disponuje čtyřmi PoE porty s maximálním povoleným odběrem 1,2 A a přenosovou rychlostí 100 Mb/s. Přepínač je využít k napájení a ke konfiguraci naší ústředny [11].

2.2 Použitý software

2.2.1 VMWare Workstation 15 Player

VMWare je program umožňující spustit jednu nebo více virtualizovaných instancí různých operačních systémů. Jednou z výhod virtualizovaných systémů je jejích jednoduché přenášení mezi různými zařízeními a jejich snadné zprovoznění, které víceméně spočívá pouze ve spuštění správných souborů VMWare programem. Mezi jejich praktické využití patří např. možnost spuštění starší verze operačního systému, pro účel používání programů které již na nové verzi operačního systému nejsou podporovány. Přesně pro tento účel budeme používat virtualizovanou instanci operačního systému Windows 7.

2.3 Návrh výukového systému

Na základě dodaných modulů a snaze o jejich optimální využití byl navržen dvoudveřový přístupový systém. Pro model prvního vstupu jsme použili jednu RFID čtečku karet, odchodové tlačítko a elektrický zámek. Elektrický zámek bude ovládán odchodovým tlačítkem a čtečkou karet. Jestliže bude ústředna správně nakonfigurována elektrický zámek by se měl stiskem tlačítka nebo načtením dodané karty otevřít. Model druhého vstupu bude vypadat podobně. Jediný rozdíl bude absence odchodového tlačítka, protože nám bylo poskytnuto jen jedno (což pro demonstraci jeho fungování stačí). Ústředna, do které budou všechny výše zmíněné komponenty zapojeny, bude propojena se správním počítačem přes PoE přepínač pomocí Ethernetového kabelu.

Ústřednu bude možné konfigurovat přes webové rozhraní.

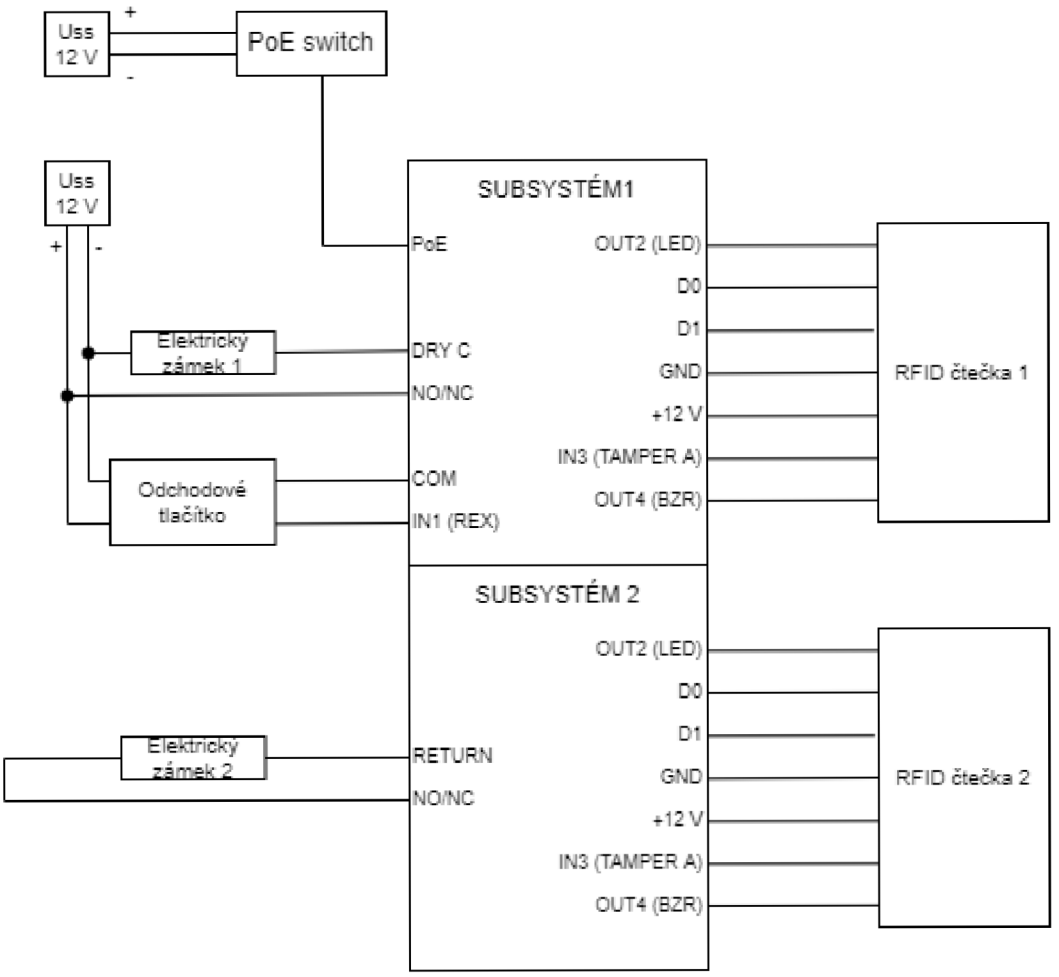
2.3.1 Návrh zapojení

Na obr. 2.1 jsou ústředna a její rozšiřující modul vyobrazeny jako dva spojené bloky. Ústředna je napájena pomocí PoE a rozšiřující modul z ústředny. PoE přepínač je napájen jedním ze dvou potřebných 12 V zdrojů. Druhý 12 V zdroj napájí první elektrický zámek a odchodové tlačítko. Druhý elektrický zámek je napájen z ústředny. Z ústředny je napájen pouze jeden elektrický zámek, protože oba zámky najednou ústředna napájet nezvládne. RFID čtečky jsou k ústředně zapojeny sedmi vodiči každá. Jsou to zemní vodič GND a napájecí vodič +12 V, datové vodiče D0 a D1, tamper kontakt IN 3(TAMPER A), kontakt bzučáku OUT4(BZR) a ovládací kontakt LED.

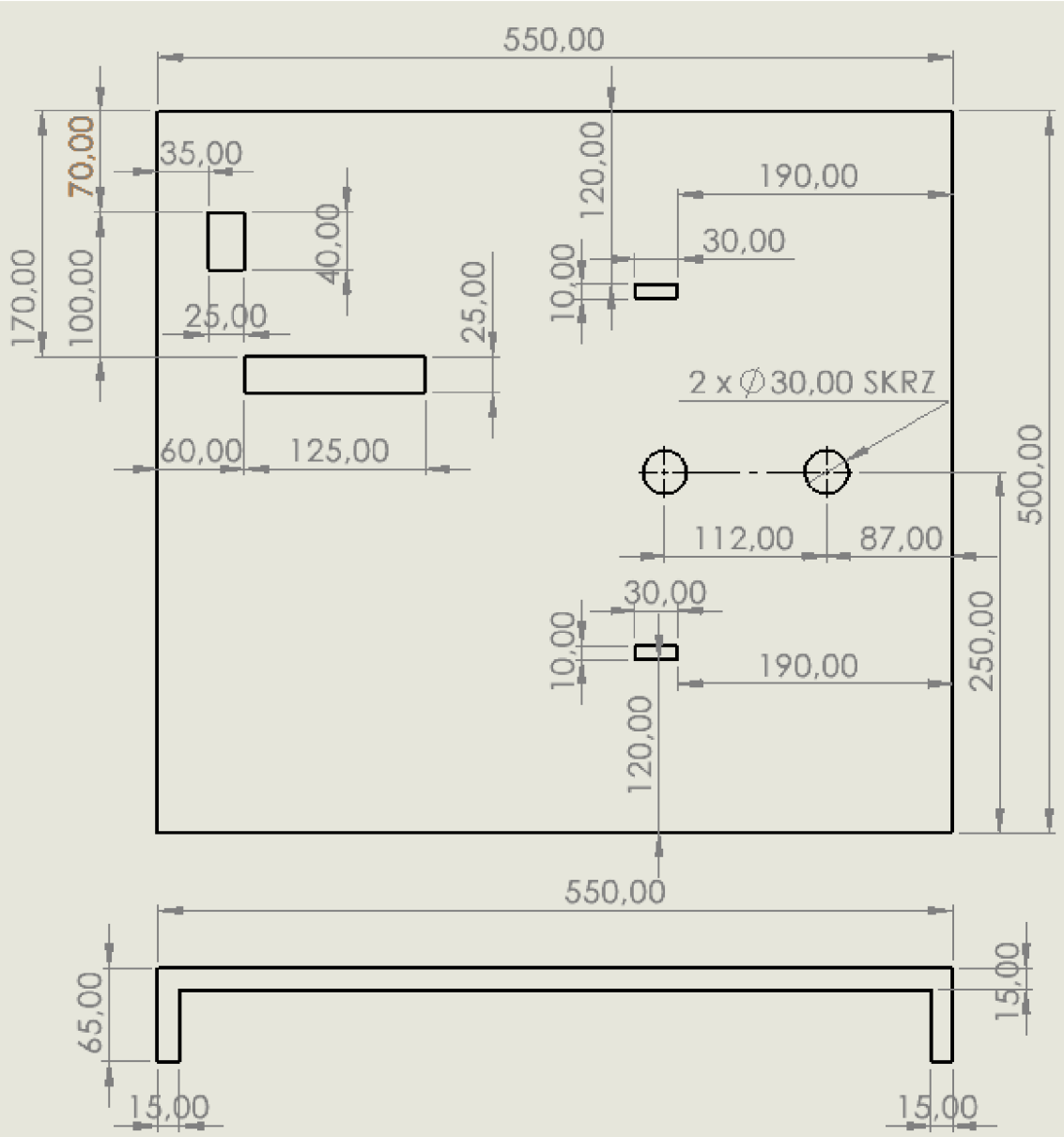
2.3.2 Návrh výukového panelu

Pro realizaci výukového panelu byl vytvořen návrh (obr. 2.2), podle kterého byla následně vyrobena výuková deska.

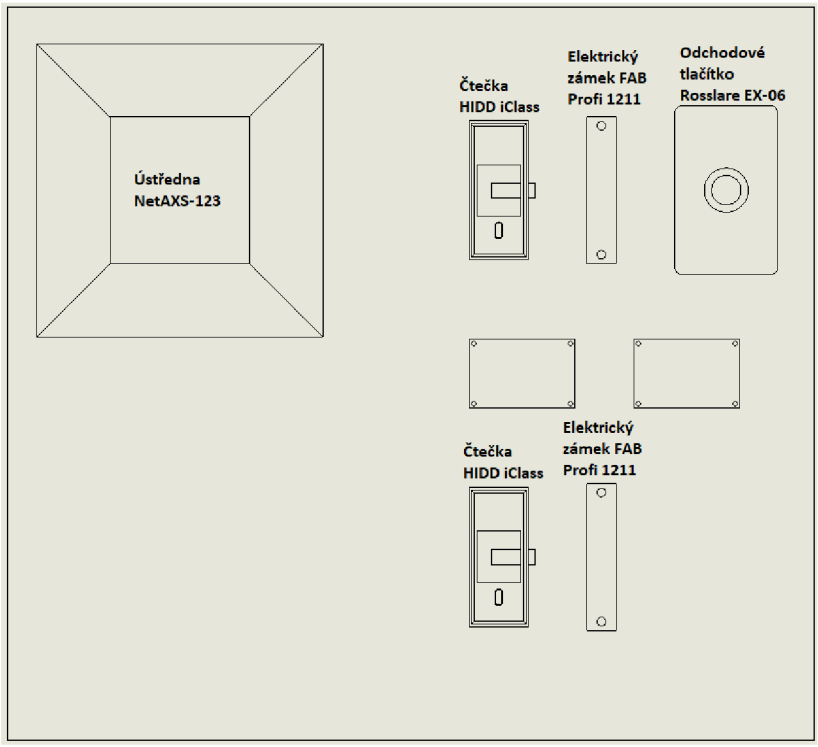
Moduly byly připevněny k panelu podle obr. 2.3.



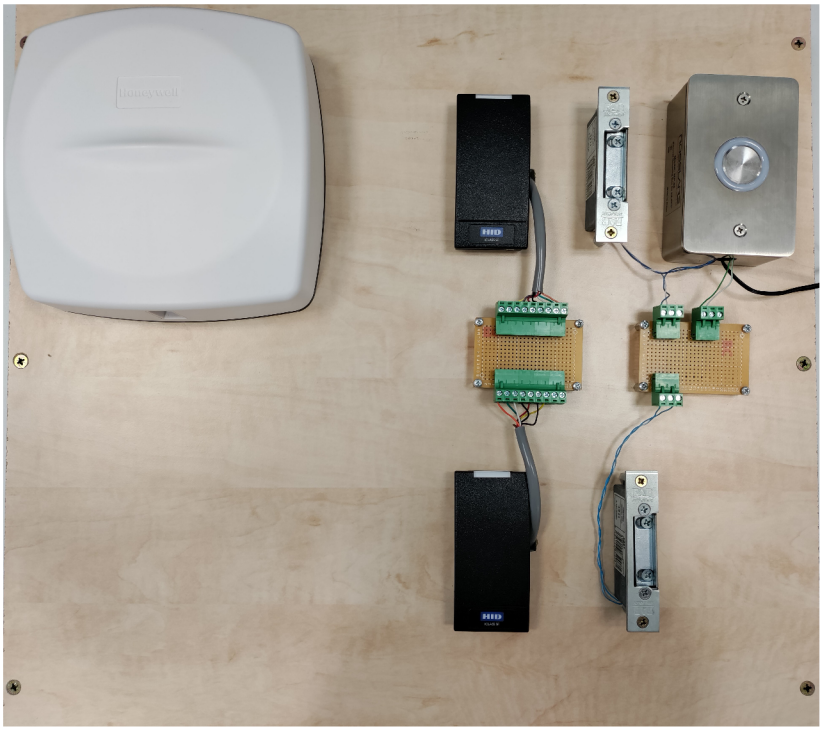
Obr. 2.1: Schéma zapojení úlohy.



Obr. 2.2: Konstrukční výkres panelu.



Obr. 2.3: Rozmístění prvků na výukovém panelu.



Obr. 2.4: Realizace výukového panelu.

3 Návod k laboratorní úloze

3.1 Teoretický úvod

Systémy elektronické kontroly vstupu (EKV) můžeme definovat jako elektronický systém, určený k automatizovanému řízení vstupů do kontrolované oblasti. Chování EKV systému definuje tzv. autorita. Ta určuje kdo a kdy může řízené vstupy používat. Pro správné fungování EKV systému je nutné spolehlivě zjistit identitu osoby žádající o vstup. K tomuto účelu se používají autentizační techniky.

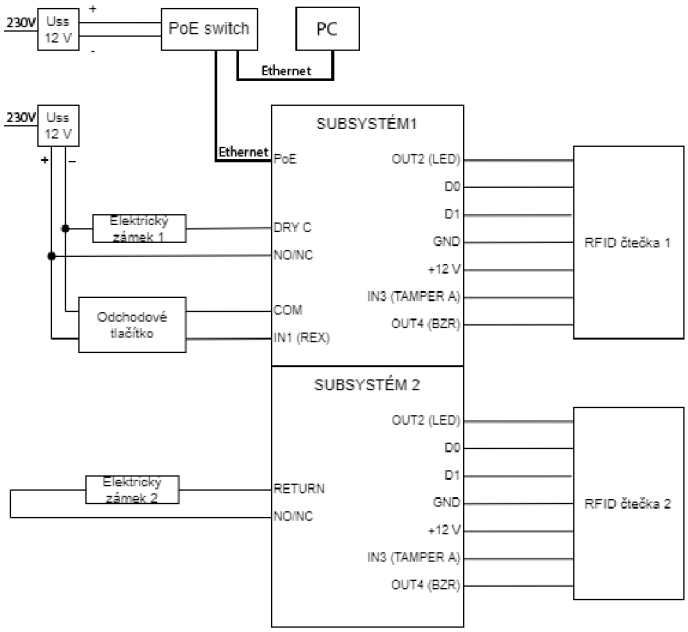
V případě této laboratorní úlohy žadatel prokazuje svou identitu pomocí RFID karty. K přečtení údajů z karty slouží čtečka karet. Žadateli jsou následně podle přečtených údajů přiřazena dříve definovaná oprávnění, v našem případě uvolnění nebo neuvolnění elektrického zámku pro požadovaný vstup.

3.1.1 Zapojení úlohy

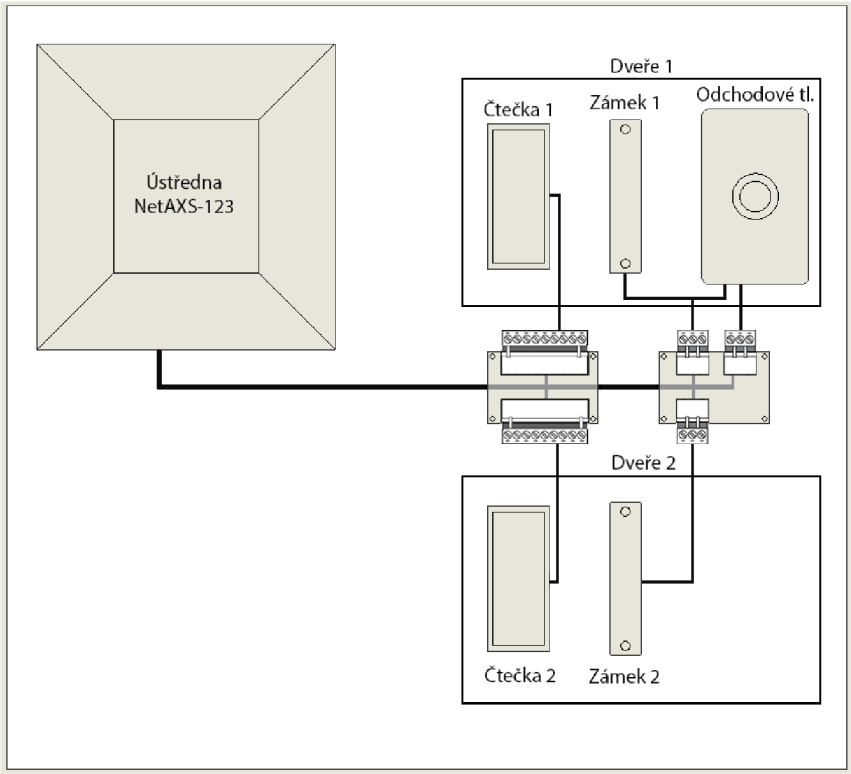
Z obrázku 3.1 můžeme vyčíst zapojení úlohy. PoE přepínač je napájen stejnosměrným 12V zdrojem zapojeným do sítě 230V. Stejně tak jsou napájeny elektrický zámek 1 a odchodové tlačítko které spolu sdílí 12V zdroj. Napájení tlačítka a zámku 1 ze zdroje je nutné, protože ústředna nepodporuje napájení odchodového tlačítka a maximální odběř přes PoE je nedostačující k provozu obou elektrických zámků najednou. Ústředna je napájena z PoE přepínače technologií PoE (Power over Ethernet) ke kterému je připojena ethernetovým kabelem. Elektrický zámek 2 je napájený přímo z ústředny. RFID čtečka 1 a 2 jsou každá připojeny k ústředně sedmi vodiči které zahrnují včetně přenosu dat a ovládání i napájení.

Na obrázku 3.2 je vyobrazené rozložení jednotlivých prvků na laboratorním přípravku. V levém horním rohu plochy se nachází ústředna NetAXS-123. V pravém horním rohu se nachází čtečka, zámek a odchodové tlačítko prvních dveří. V pravém dolním rohu pouze čtečka a zámek dveří druhých. Všechny periferie jsou navedeny na svorkovnice mezi nimi a skrz tyto svorkovnice do ústředny.
Použité zařízení:

- Ústředna Honeywell NetAXS-123 s rozšiřujícím modulem NXD1,
- dvě čtečky RFID karet HIDD iclass,
- odchodové tlačítko Rosslare EX-06,
- dva elektrické dveřní zámky FAB Profi 1211,
- čtyři RFID karty HID iClass GP,
- PoE přepínač Tenda.



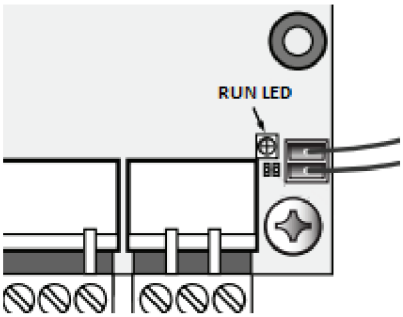
Obr. 3.1: Blokové schéma zapojení laboratorní úlohy.



Obr. 3.2: Rozmístění prvků na přípravku.

3.2 Návod k vypracování úlohy

1. Zkontrolujte správné propojení všech komponent.
2. Zapojte napájecí zdroje PoE switche a odchozího tlačítka do elektrické zásuvky 230V.
3. Vyčkejte než kontrolní dioda **RUN LED** v pravém dolním rohu ústředny začne pravidelně jednou za sekundu blikat.



Obr. 3.3: RUN LED umístění.

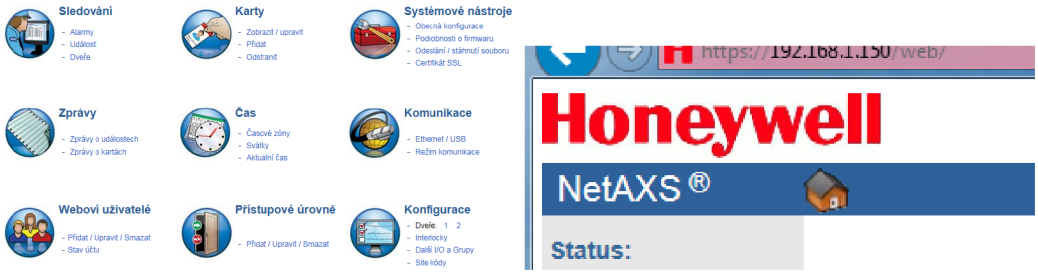
3.2.1 Spuštění virtuálního stroje

1. Na laboratorním PC spusťte program **VMWare Workstation 15 Player**.
2. V otevřeném okně klikněte na **Open a Virtual Machine**.
3. Vyberte soubor **Windows 7 Ultimate SP1 (x64)** nacházející se ve složce *D:/VirtualMachines/BPC-ZSY-Windows 7 Ultimate SP1 (x64)* a klikněte na tlačítko **Otevřít**.
4. Přidaný virtuální stroj spusťte kliknutím na **Play virtual machine**.

3.2.2 Přihlášení do webového rozhraní

1. Ve virtuálním stroji spusťte program **Internet Explorer** ve kterém následně otevřete url: *https://192.168.1.150*
   Je důležité url napsat včetně *https://*
2. Objeví se okno o chybě certifikátu stránky, klikněte na odkaz **Continue to this website (not recomended).**
3. Po načtení stránky se přihlaste do webového rozhraní pomocí následujících přihlašovacích údajů:
   - Jméno: admin
   - Heslo: Pasw2021!

4. Po úspěšném přihlášení se zobrazí tzv. „cílová stránka“, do které je možné se navrátit kliknutím na ikonu domečku, jež se objeví na levé stranně modré horní lišty po opuštění cílové stránky.



3.2.3 Resetování konfigurace

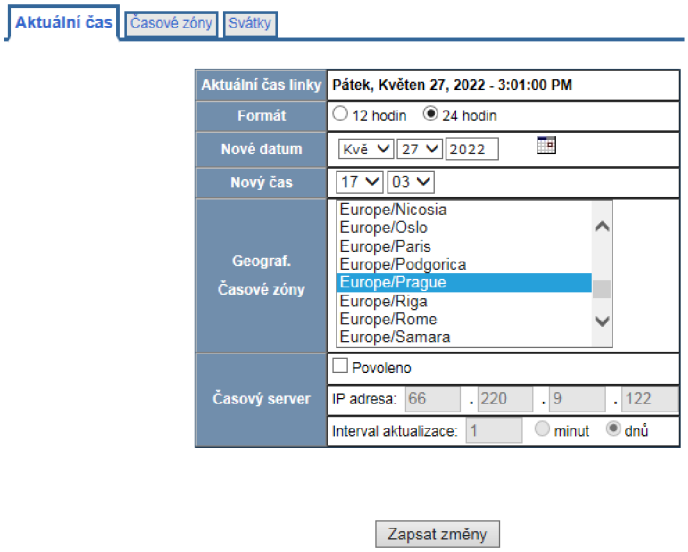
1. Na cílové stránce pod menu položkou **Systémové nástroje** najděte a klikněte na položku **- Odeslání / stáhnutí souboru**.

2. Klikněte na tlačítko **Browse** pod nadpisem **Stáhnout**.
3. Vyberte soubor **NetAXSDefaultConfig** nacházející se ve složce */Desktop/NetAXSConfiguration* a potvrďte tlačítkem **Open**.
4. Následně klikněte na tlačítko **Stáhnout** a vyskakovací okno potvrďte tlačítkem **OK**.
5. Po chvíli se objeví další vyskakovací okno které také potvrďte tlačítkem **OK**.
6. Zobrazí se načítací panel, tím se však neřiďte. Vyčkejte asi minutu, dokud nezačne kontrolní dioda **RUN LED** na ústředně pravidelně jednou za sekundu blikat.
7. Stránku znovu načtěte stiskem tlačítka **F5** na klávesnici a přihlaste se stejnými přihlašovacími údaji.
8. Přivolejte vyučujícího pro ověření provedení resetu základní konfigurace.

3.2.4 Nastavení času a časových zón

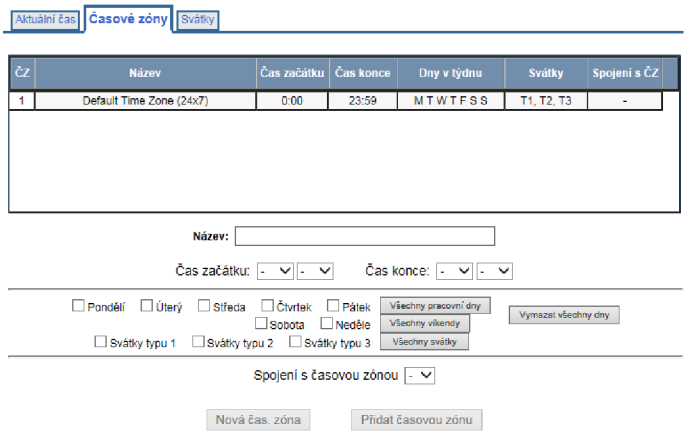
1. Pod položkou **Čas** klikněte na **- Aktuální čas**.

2. Nastavte časový formát na **24 hodin**.
3. Datum a aktuální čas nastavte podle aktuálního data a času do políček **Nový datum** a **Nový čas**.
4. Časové pásmo zvolte například **Europe/Prague**.



Obr. 3.4: Nastavení aktuálního času.

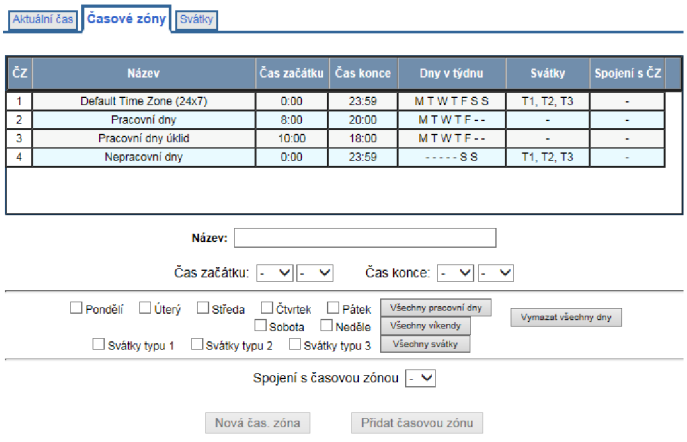
5. Ostatní nastavení ponechte a potvrďte tlačítkem **Zapsat změny**.
6. Následně na horní liště najděte a klikněte na **Časové zóny**. V tabulce by se měla nacházet pouze jedna časová zóna se jménem „Default Time Zone (24/7)“. Tato časová zóna zahrnuje všechny dny v týdnu 24 hodin denně.
7. Pro demonstrační účely vytvořte tři další časové zóny. Časové zóny se používají např. k omezení platnosti oprávnění pouze na zvolenou časovou zónu.
8. První časovou zónu pojmenujte v políčku **Název** na „Pracovní dny“. **Čas začátku** zvolte 8:00 a **Čas konce** nastavte na 18:00.
9. Stiskem tlačítka **Všechny pracovní dny** zaškrtněte dny pondělí až pátek.
10. Potvrdíme tlačítkem **Přidat časovou zónu**.



Obr. 3.5: Časové zóny - výchozí tabulka.

11. Druhou časovou zónu pojmenujte v políčku **Název** jako „Pracovní dny úklid“. **Čas začátku** zvolte 9:00 a **Čas konce** nastavte na 19:00.
12. Stiskem tlačítka **Všechny pracovní dny** zaškrtněte dny pondělí až pátek.
13. Potvrdíme tlačítkem **Přidat časovou zónu**.

14. Třetí časovou zónu pojmenujte v políčku **Název** na „Nepracovní dny“. **Čas začátku** zvolte 0:00 a **Čas konce** nastavte na 23:59.
15. Stiskem tlačítka **Všechny víkendy** a **Všechny svátky** zaškrtněte dny sobota, neděle a všechny tři typy svátků.
16. Potvrdíme tlačítkem **Přidat časovou zónu**.

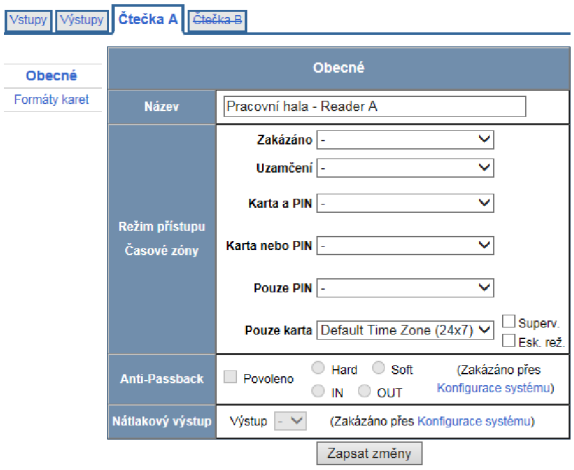


Obr. 3.6: Časové zóny - výsledná tabulka.

3.2.5 Nastavení dveří 1

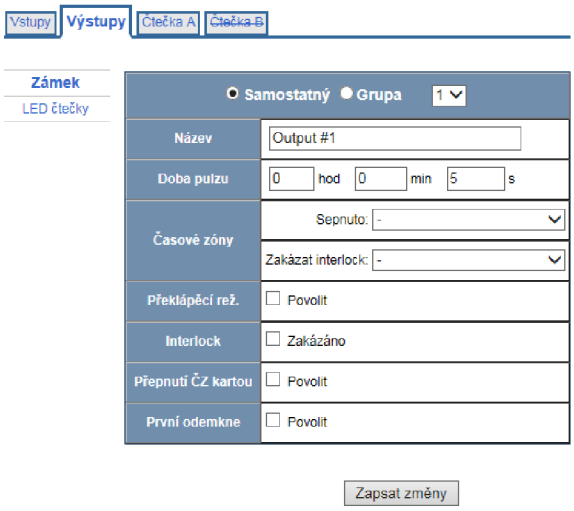
1. Pod položkou **Konfigurace** klikněte na **- Dveře[1]**.

2. Čtečku přejmenujte na „Výrobní hala - Reader A“.
3. U **Pouze karta** přístupového módu ponechte časovou zónu „Default Time Zone (24x7)“. Čtečka tedy bude v režimu **Pouze karta** po dobu zvolené časové zóny (v našem případě 24/7).
   Změny potvrďte tlačítkem **Zapsat změny**.

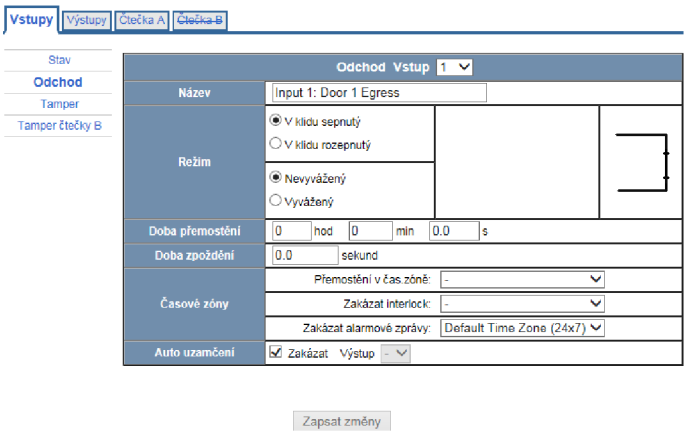


Obr. 3.7: Dveře 1 čtečka A nastavení.

4. Na horní liště klikněte na položku **Výstupy**.
5. Zkontrolujte zda je vybrán výstup číslo 1, což je výstup ke kterému je připojený elektrický zámek 1. Pokud ne, tak jej vyberte.
6. Nastavte **Doba pulzu** na 5 sekund. Zbytek nastavení ponechte a klikněte **Zapsat změny**.
7. Dále na horní liště klikněte na **Vstupy** a v levé poličce vyberte položku **Odchod**.
8. Zkontrolujte zda je **Odchod Vstup** na „1“ což je vstup ke kterému je připojeno opouštěcí tlačítko. Pokud ano, ponechte nastavení jak je. Pokud ne, nastavte jej na „1“ a potvrďte tlačítkem **Zapsat změny**.



Obr. 3.8: Dveře 1 nastavení výstupu.



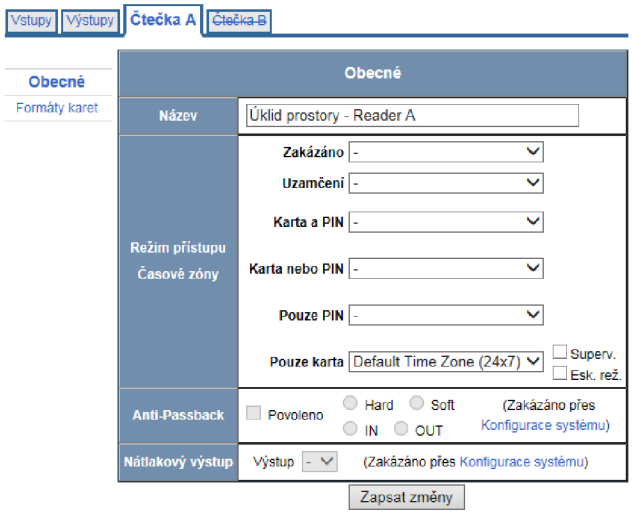
Obr. 3.9: Dveře 1 nastavení vstupu pro odchod.

3.2.6 Nastavení dveří 2

1. Pod položkou **Konfigurace** klikněte na **- Dveře[2]**.

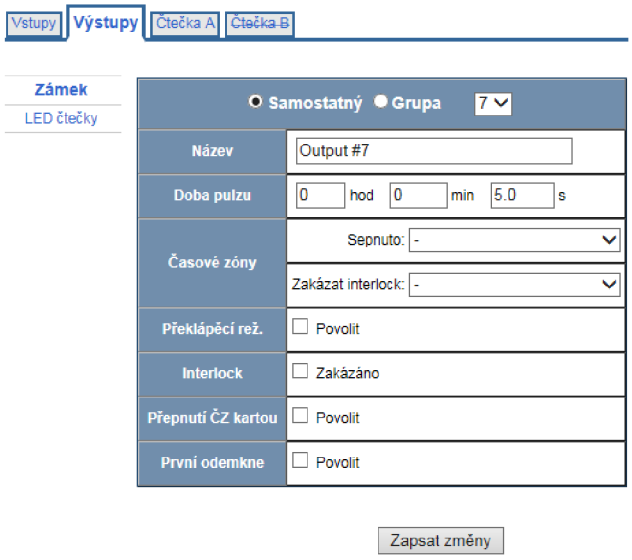
2. Čtečku přejmenujte na „Úklid prostor - Reader A“.
3. U **Pouze karta** přístupového módu ponechte časovou zónu „Default Time Zone (24x7)“. Čtečka tedy bude v režimu **Pouze karta** po dobu zvolené

časové zóny (v našem případě 24/7).
Změny potvrďte tlačítkem **Zapsat změny**.



Obr. 3.10: Dveře 2 čtečka A nastavení.

4. Klikněte na položku **Výstupy**.
5. Zkontrolujte zda je vybrán výstup číslo 7 což je výstup ke kterému je připojený elektrický zámek 2. Pokud ne, tak jej vyberte.
6. Nastavte **Doba pulzu** na 5 sekund. Zbytek nastavení ponechte a klikněte **Zapsat změny**.



Obr. 3.11: Dveře 2 nastavení výstupu.

3.2.7 Přidání přístupových úrovní

Přístupové úrovně nám umožňují definovat oprávnění k přístupu a následně jej přiřadit čipovým kartám a tím i jejich nosičům.

1. Pod položkou **Přístupové úrovně** klikněte na **- Přidat/Upravit/Smazat**.

2. Zaklikněte obě **Čtečka A** políčka a pod nadpisem **Název** pojmenujte stupeň „Plný přístup“.
   Potvrďte tlačítkem **Přidat úroveň**.

Obr. 3.12: Přidání přístupové úrovně „Plný přístup“.

3. Tlačítkem **Nová úroveň** vytvořte další přístupovou úroveň.
4. Zaklikněte **Čtečka A** políčko pod **Výrobní hala - Reader A [1]** a zvolte **Časovou zónu** „Pracovní dny“.
   Pod nadpisem **Název** pojmenujte stupeň „Výroba“.
   Potvrďte tlačítkem **Přidat úroveň**.
5. Tlačítkem **Nová úroveň** vytvořte další přístupovou úroveň.
6. Zaklikněte **Čtečka A** políčko pod **Úklid prostor - Reader A [2]** a zvolte **Časovou zónu** „Pracovní dny úklid“.
   Pod nadpisem **Název** pojmenujte stupeň „Úklid“.
   Potvrďte tlačítkem **Přidat úroveň**.

Obr. 3.13: Přidání přístupové úrovně „Výroba“.

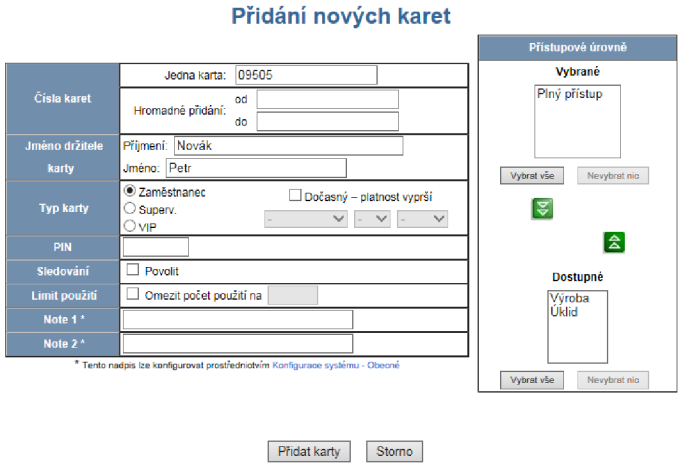
Obr. 3.14: Přidání přístupové úrovně „Úklid“.

3.2.8 Přiřazení čipových karet

1. Pod položkou **Karty** klikněte na **- Přidat**.

2. Kartu přidáte zadáním jejího čísla do políčka **jedna karta**.
   Číslo karty je natištěné na jejím povrchu. Hledáme pětimístnou číslici která je předcházena znaménkem „+“. Tedy například u karty s potiskem v podobě „4+09507 42101163121-7 SE“ to je číslo 09507.

3. Zadáním jména a příjmení nositele karty do políček **Jméno** a **Příjmení**.
4. Volbou přístupové úrovně, kterou zvolte z pravého seznamu **Dostupné** a následně ji přesuňte do seznamu **Vybrané** stiskem zeleného tlačítka s nahoru ukazujícími šipkami.



Obr. 3.15: Přidání nových karet.

5. Přidejte 3 karty. Ke každé z nich přiřaďte jednu z dříve vytvořených přístupových úrovní. Každá karta bude mít rozdílnou úroveň.
6. Následně ještě přidáme čtvrtou kartu. Této kartě změníme **Typ karty** na **VIP** a přiřadíme „Plný přístup“.
7. Poznačte si, nebo zapamatujte jednotlivé karty a jejich oprávnění.

3.2.9 Ověření laboratorní úlohy

1. Vyzkoušejte zda dveře správně reagují na stisk odchodového tlačítka.
2. Otestujte zda jsou karty správně schopné, nebo neschopné otevírat zámky dle konfigurace.
   Karta s oprávněním „Úklid“ by měla moct otevírat pouze dveře úklidových prostor, karta s oprávněním „Výroba“ naopak jen dveře výrobní haly. Karty s oprávněním „Plný přístup“ by měly být schopny otevírat oboje dveře.
3. Vraťte se do konfigurace přístupových úrovní kliknutím na
   - Přidat/Upravit/Smazat pod položkou **Přístupové úrovně**.

4. Pod políčkem **Úroveň** zvolte číslo odpovídající přístupové úrovni „Plný přístup“.
5. Pro obě čtečky změňte **Časovou zónu** z „Default Time Zone (24x7)“ na „Nepracovní dny“.
6. Po této změně by měla pouze karta typu **VIP** být schopná otevřít obě dveře. Je tomu tak, protože karty typu **VIP** ignorují většinu přístupových omezení.
7. Výsledky své práce prezentujte vyučujícímu.

3.2.10 Sledování událostí

Ústředna zaznamenává události v systému. Tyto události můžeme sledovat kliknutím na **Alarmy** pod položkou **Sledování**. Překliknutím z **Panel** na **Web** na horní liště můžeme sledovat informace o přihlášení k ústředně přes webové rozhraní. Klik-

nutím na **Alarmy** v levém horním rohu můžeme zobrazit historii potvrzených a nepotvrzených alarmů.

Kliknutím na **Dveře** v levém horním rohu zas můžeme zobrazit aktuální stav dveří. Můžeme zde i tlačítkem **Pulz** u položek **Output #1** a **#7** manuálně uvolnit elektrické zámky.

3.2.11 Ukončení laboratorní úlohy

1. Po kontrole vyučujícím **vyresetujte konfiguraci** stejně jako na začátku úlohy (podsekce 3.2.3) a vypněte virtuální stroj.
2. Odpojte napájecí zdroje PoE přepínače a odchodového tlačítka.
3. Vypněte laboratorní počítač.

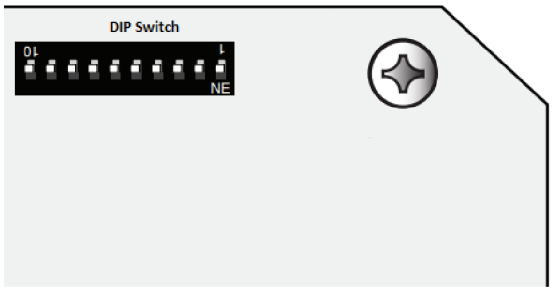
4 Návod k laboratorní úloze pro vyučující

4.1 NetAXS-123 obnovení základní konfigurace

4.1.1 Plný reset ústředny

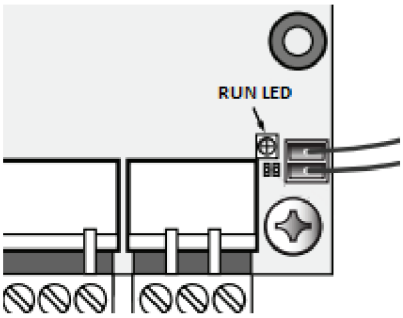
Pro obnovení továrního nastavení ústředny postupujte podle následujících kroků.

1. Poznačte si stávající nastavení DIP spínačů v pravém horním rohu ústředny.



Obr. 4.1: Umístění DIP switche.

2. Když je panel zapnut, nastavte všechny spínače DIP do polohy VYPNUTO.
3. Odpojte a znovu připojte napájení ústředny.
4. Vyčkejte dokud nezačne RUN LED (v pravém dolním rohu ústředny) rychle blikat zelenou barvou.



Obr. 4.2: Umístění RUN LED.

5. Vraťte DIP spínače na dříve poznačené pozice.
6. Znovu odpojte a připojte napájení ústředny.
7. Vyčkejte dokud RUN LED nezačne pravidelně jednou za sekundu blikat zelenou barvou.

4.1.2 Nastavení ústředny pro konfiguraci přes webové rozhraní

1. Ve virtuálním stroji spusťte program **Internet Explorer** ve kterém následně otevřete url: *https://192.168.1.150*
2. Objeví se okno o chybě certifikátu stránky, klikněte na odkaz **Continue to this website (not recomended).**
3. Po načtení stránky se přihlašte do webového rozhranní pomocí následujících přihlašovacích údajů:
   - Jméno: admin
   - Heslo: admin

4. Po prvním přihlášení budete donuceni nastavit nové heslo. To nastavte na „Pasw2021!“.
5. Na cílové stránce pod menu položkou **Communications** najděte a klikněte na položku **- Host/Loop**.
6. Přepněte nastavení **Host** na **Web Mode**. Potvrďte tlačítkem **Zapsat změny**.

4.1.3 Nahrání základní konfigurace

1. Na cílové stránce pod menu položkou **Systémové nástroje** najděte a klikněte na položku **- Odeslání / stáhnutí souboru**.

2. Klikněte na tlačítko **Browse** pod nadpisem **Stáhnout**.
3. Vyberte soubor **NetAXSDefaultConfig** nacházející se ve složce */Desktop/NetAXSConfiguration* a potvrdďte tlačítkem **Open**.
4. Následně klikněte na tlačítko **Stáhnout** a vyskakovací okno potvrďte tlačítkem **OK**.
5. Po chvíli se objeví další vyskakovací okno které také potvrďte tlačítkem **OK**.
6. Zobrazí se načítací panel, tím se však neřiďte. Vyčkejte asi minutu, dokud nezačne kontrolní dioda **RUN LED** na ústředně pravidelně jednou za sekundu blikat.

7. Ústředna je v základní konfiguraci. Stránku znovu načtěte stiskem tlačítka **F5** na klávesnici a přihlaste se přihlašovacími údaji:
   - Jméno: admin
   - Heslo: Pasw2021!

Závěr

V teoretické části bakalářské práce jsme obecně popsali problematiku elektronické kontroly vstupu. Popsali jsme použití těchto systémů a důvody jejich nasazení a principy jejich fungování. Dále jsme probrali autentizaci a její typy. Podrobněji jsme si přiblížili druhy autentizačních předmětu a principy jejich fungování. Dále jsme popsali komunikační rozhraní kontrolních systémů a zmínili jsme jejich pro a proti. Trochu podrobněji jsme se pak věnovali biometrickým metodám autentizace, kde jsme popsali různé metody snímání otisků prstu a jejich výhody a nevýhody.

V části praktické jsme na základě dodaných komponent navrhli zapojení výukového systému pro laboratorní úlohu EKV a zpracovali jsme jeho schéma. Navrhli jsme dvouvstupový kontrolní systém kde první vstup je řízen z jedné strany RFID čtečkou karet a z druhé odchodovým tlačítkem. Druhý vstup je řízen pouze čtečkou karet. Dále jsme navrhli výukový panel pro upevnění kontrolního systému. Celý výukový panel jsme realizovali.

Následně jsme pro realizovaný výukový systém vytvořili návod s pracovním postupem pro studenty a návod/manuál pro vyučující sloužící k řešení problémů které by mohly nastat.

Literatura

[1] VUT v Brně: *Úprava, odevzdávání a zveřejňování vysokoškolských kvalifikačních prací na VUT v Brně* [online]. Směrnice rektora č. 2/2009. Brno: 2009, poslední aktualizace 24. 3. 2009 [cit. 23. 10. 2015]. Dostupné z URL: <https://www.vutbr.cz/uredni-deska/vnitrni-predpisy-a-dokumenty/smernice-rektora-f34920/>.

[2] *ČSN ISO 690 (01 0197) Informace a dokumentace – Pravidla pro bibliografické odkazy a citace informačních zdrojů.* 40 stran. Praha: Český normalizační institut, 2011.

[3] *ČSN ISO 7144 (010161) Dokumentace – Formální úprava disertací a podobných dokumentů.* 24 stran. Praha: Český normalizační institut, 1997.

[4] BIERNÁTOVÁ, O., SKŮPA, J.: *Bibliografické odkazy a citace dokumentů dle ČSN ISO 690 (01 0197) platné od 1. dubna 2011* [online]. 2011, poslední aktualizace 2. 9. 2011 [cit. 19. 10. 2011]. Dostupné z URL: <http://www.citace.com/CSN-ISO-690.pdf>

[5] *Pravidla českého pravopisu.* Zpracoval kolektiv autorů. 1. vydání. Olomouc: FIN PUBLISHING, 1998. 575 s. ISBN 80-86002-40-3.

[6] *SO/IEC 14443-2:2020 Cards and security devices for personal identification — Contactless proximity objects — Part 2: Radio frequency power and signal interface platné od 1. července 2020* [online].

Dostupné z URL: <https://www.iso.org/standard/73597.html>

[7] BURDA, Karel. *Základy elektronických zabezpečovacích systémů.* CERM, Brno 2017.

[8] BURDA, Karel a Ivo STRAŠIL. *Zabezpečovací systémy* Brno, 2011. Dostupné z URL: <https://moodle.vut.cz/mod/resource/view.php?id=124517>

[9] BADIGER R. *Design a cost-effective magnetic card reader.* EDN Network, 2013. Dostupné z URL: <https://goo.gl/JSAbt8>

[10] *Honeywell. NetAXS-123: Access Control Unit Installation Guide, 800-05779V2.* 2013. [online] Dostupné z URL: <https://usermanual.wiki/Document/80005779V2NetAXS12350INSTALLGUIDE.1262409953.pdf>

[11] tenda_cz *Tenda TEF1105P-4-63W PoE AT Switch 63Watt* Dostupné z URL: <https://www.tenda.cz/article/tenda-tef1105p-4-63w-poe-switch-63watt>

Seznam symbolů a zkratek

EKV	Elektronická kontrola vstupu
ID	Jedinečný identifikátor
OF	Ověřovací faktor
DF	Dokazovací faktor
CCTV	uzavřený televizní okruh – Closed-circuit television
ZSY	Zabezpečovací Systémy
RFID	identifikace na rádiové frekvenci – Radio Frequency Identification
USB	Universal Serial Bus
PoE	Power over Ethernet
EEPROM	Elektricky Vymazatelná Paměť pouze pro čtení – Electrically Erasable Programmable Read-Only Memory