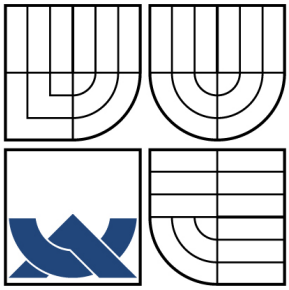
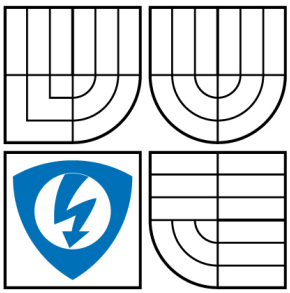


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

LABORATORNÍ ÚLOHA KARTOVÉHO PŘÍSTUPOVÉHO SYSTÉMU

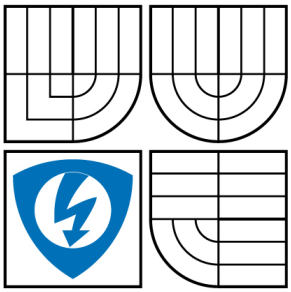
LABORATORY TASK OF THE CARD ACCESS SYSTEM.

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — PETER MINÁRIK
AUTHOR

VEDOUCÍ PRÁCE — doc. Ing. KAREL BURDA, CSc.
SUPERVISOR

BRNO 2008



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student:	Minárik Peter	***ID:***	77932
Ročník:	3	***Akademický rok:***	2007/2008

NÁZEV TÉMATU:

Laboratorní úloha kartového přístupového systému

POKYNY PRO VYPRACOVÁNÍ:

V rámci práce popište principy, technická řešení a základní prvky soudobých kartových přístupových systémů. Dále popište zapojení a obsluhu přiděleného kartového přístupového systému. Pro tento systém navrhněte laboratorní úlohu v délce 90 minut. Volbu dílčích úloh a postup úlohy zdůvodněte. K praktickému provádění laboratorní úlohy zpracujte podrobný a metodický návod.

DOPORUČENÁ LITERATURA:

[1] SMITH, R. E.: Authentication. Addison Wesley, Boston 2002.
[2] KŘEČEK, S. a kol.: Příručka zabezpečovací techniky. Blatenská tiskárna, Blatná 2003.

Termín zadání:	11.2.2008	***Termín odevzdání:***	4.6.2008

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

prof. Ing. Kamil Vrba, CSc.
předseda oborové rady

LICENČNÍ SMLOUVA
POSKYTOVANÁ K VÝKONU PRÁVA UŽÍT ŠKOLNÍ DÍLO

uzavřená mezi smluvními stranami:

1. Pan/paní

Jméno a příjmení: Peter Minárik
Bytem: Žitavská 68, 94103, Úľany nad Žitavou
Narozen/a (datum a místo): 2.7.1986, Nové Zámky

(dále jen "autor")

a

2. Vysoké učení technické v Brně

Fakulta elektrotechniky a komunikačních technologií
se sídlem Údolní 244/53, 60200 Brno 2
jejímž jménem jedná na základě písemného pověření děkanem fakulty:
prof. Ing. Kamil Vrba, CSc.

(dále jen "nabyvatel")

Článek 1
Specifikace školního díla

1. Předmětem této smlouvy je vysokoškolská kvalifikační práce (VŠKP):
   - ☐ disertační práce
   - ☐ diplomová práce
   - ☑ bakalářská práce

   jiná práce, jejíž druh je specifikován jako .....

(dále jen VŠKP nebo dílo)

Název VŠKP: Laboratorní úloha kartového přístupového systému
Vedoucí/školitel VŠKP: doc. Ing. Karel Burda, CSc.
Ústav: Ústav telekomunikací
Datum obhajoby VŠKP: .....

VŠKP odevzdal autor nabyvateli v:

- ☑ tištěné formě - počet exemplářů 1
- ☑ elektronické formě - počet exemplářů 1

2. Autor prohlašuje, že vytvořil samostatnou vlastní tvůrčí činností dílo shora popsané a specifikované. Autor dále prohlašuje, že při zpracovávání díla se sám nedostal do rozporu s autorským zákonem a předpisy souvisejícími a že je dílo dílem původním.
3. Dílo je chráněno jako dílo dle autorského zákona v platném znění.
4. Autor potvrzuje, že listinná a elektronická verze díla je identická.

Článek 2

Udělení licenčního oprávnění

1. Autor touto smlouvou poskytuje nabyvateli oprávnění (licenci) k výkonu práva uvedené dílo nevýdělečně užít, archivovat a zpřístupnit ke studijním, výukovým a výzkumným účelům včetně pořizovaní výpisů, opisů a rozmnoženin.
2. Licence je poskytována celosvětově, pro celou dobu trvání autorských a majetkových práv k dílu.
3. Autor souhlasí se zveřejněním díla v databázi přístupné v mezinárodní síti
   - ☑ ihned po uzavření této smlouvy
   - ☐ 1 rok po uzavření této smlouvy
   - ☐ 3 roky po uzavření této smlouvy
   - ☐ 5 let po uzavření této smlouvy
   - ☐ 10 let po uzavření této smlouvy

   (z důvodu utajení v něm obsažených informací)
4. Nevýdělečné zveřejňování díla nabyvatelem v souladu s ustanovením § 47b zákona č. 111/1998 Sb., v platném znění, nevyžaduje licenci a nabyvatel je k němu povinen a oprávněn ze zákona.

Článek 3

Závěrečná ustanovení

1. Smlouva je sepsána ve třech vyhotoveních s platností originálu, přičemž po jednom vyhotovení obdrží autor a nabyvatel, další vyhotovení je vloženo do VŠKP.
2. Vztahy mezi smluvními stranami vzniklé a neupravené touto smlouvou se řídí autorským zákonem, občanským zákoníkem, vysokoškolským zákonem, zákonem o archivnictví, v platném znění a popř. dalšími právními předpisy.
3. Licenční smlouva byla uzavřena na základě svobodné a pravé vůle smluvních stran, s plným porozuměním jejímu textu i důsledkům, nikoliv v tísni a za nápadně nevýhodných podmínek.
4. Licenční smlouva nabývá platnosti a účinnosti dnem jejího podpisu oběma smluvními stranami.

V Brně dne: .....

....

Nabyvatel Autor

ABSTRAKT

Práca sa zaoberá vytvorením laboratórnej úlohy kartového prístupového systému. V prvej časti tejto práci sú popísané princípy, technické riešenia a základné prvky súčasných kartových prístupových systémov. V druhej časti je navrhnutá laboratórna úloha, zameraná na zoznámenie sa s kartovým prístupovým systémom, jeho nastavením a funkciami.

KĽÚČOVÉ SLOVÁ

Kartový prístupový systém, riadiaca jednotka HUB Pro, program SKYLA Pro II, bezkontaktný identifikátor, Wiegand.

ABSTRACT

The Bachelor´s thesis is based on creating laboratory task of the card access system. Principles, technical solutions and primary parts of card access system are described in the first part of the project. The laboratory task is designed in the second part. It's focused on getting familiar with card access systems, their setup and function.

KEYWORDS

Card access system, controller HUB Pro, program SKYLA Pro II, contactless identifier, Wiegand.

MINÁRIK, P. *Laboratorní úloha kartového přístupového systému.* Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2008. 28 s. Vedoucí bakalářské práce doc. Ing. Karel Burda, CSc.

PREHLÁSENIE

Prehlasujem, že svoju bakalársku prácu na tému "Laboratórna úloha kartového prístupového systému" som vypracoval samostatne pod vedením vedúceho bakalárskej práce a s použitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor uvedenej bakalárskej práce ďalej prehlasujem, že v súvislosti s vytvorením tohto semestrálneho projektu som neporušil autorské práva tretích osôb, nezasiahol som nedovoleným spôsobom do cudzích autorských práv osobnostných a som si plne vedomí následkov porušení ustanovení § 11 a nasledujúcich autorského zákona č. 121/2000 Sb., vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovení §152 trestného zákona č. 140/1961 Sb.“

V Brně dne …… ……..

(podpis autora)

POĎAKOVANIE

Ďakujem vedúcemu bakalárskej práce Doc. Ing. Karlu Burdovi, CSc., za veľmi užitočnú metodickú pomoc a cenné rady pri spracovaní bakalárskej práce.

Obsah

Úvod

Kartový prístupový systém slúži k zabezpečeniu a ochrane objektov, v ktorom sú klasické kľúče nahradené čipovými kartami, v prevedení ako bezkontaktné alebo čipové. Principiálne nám určuje kto sa kam a kedy dostane. Elektronická forma kontroly a evidencie vstupov si našla svoje uplatnenie v chránených zónach, strážených parkoviskách a v neposlednom rade ako forma evidencie návštev vďaka dynamickej možnosti prideľovania oprávnení. Obsluhe ponúka prehľady udalostí v systému - snímanie priechodu osôb cez jednotlivé dvere je samozrejmosťou, pričom je tiež možné filtrovanie dát podľa času, osôb či kontrolovaných zón.

Ak je táto kontrola vstupu navyše pripojená k počítačovej sieti, majú užívatelia k dispozícii omnoho širšie spektrum funkcií. Systém kontroly vstupu umožňuje uchovávať a spracovávať základné informácie o osobách a poskytuje tiež informácie týkajúce sa ich dochádzky.

Tento prístupový systém môže byť prepojený s ďalšími systémami a to napr. s nadradeným podnikovým informačným systémom, so systémom riadenia dopravy a inými.

1. Princípy kartových prístupových systémov

V dnešnej dobe je snáď samozrejmosťou každých podnikov alebo objektov, v ktorých sa má zamedziť voľnému pohybu osôb v rámci kontrolovaných zón použitie kartového prístupového systému. Vytvoríme tak kontrolovaný priestor, v ktorom je možné v každom okamihu presne vedieť kto sa nachádza v kontrolovanej zóne.

Princípom takejto elektronickej kontroly vstupu je počítačom riadený súbor prvkov kontrolujúci prístup do určitého priestoru. Ten býva zabezpečený zámkom a nejakou formou kľúča. Vstup do takéhoto chráneného priestoru je potom povolený len oprávneným osobám v určitých, dopredu definovaných časových intervaloch. Určiť kto a v akom časovom okamihu bude mať do chráneného priestoru prístup, je vďaka použitiu počítača jednoduché a ľahko meniteľné.

Slabinou u klasických zabezpečení pomocou zámku a kľúča je nutnosť existencie fyzického kľúča. Ten sa dá pomerne ľahko duplikovať a umožňuje vlastne prístup komukoľvek, kto je jeho vlastníkom. Navyše informácie kedy a kým bol kľúč použitý sa neevidujú. V prípade straty alebo odcudzenia kľúča spolu s nákladnou výmenou zámku takýto systém výrazne predražuje.

Systém elektronickej kontroly je omnoho efektívnejšia alternatíva ako klasický spôsob zabezpečenia. Všetky osoby, ktoré sa budú v sledovaných priestoroch pohybovať, obdržia identifikačnú kartu alebo číselný kód umožňujúci vstup do jednotlivých oblastí len povolaným osobám v určenom čase. Malý programovateľný riadiaci panel následne na základe identifikácie človeka vstup buď povolí alebo nepovolí. V prípade straty alebo odcudzenia karty, stačí riadiaci panel jednoducho a rýchlo preprogramovať.

Riadenie vstupov do objektov spočíva v znemožnení priechodu bez jednoznačnej identifikácie média (*karty*) s platným právom pre vstup. To znamená, že pred identifikáciou osoby s oprávnením pre vstup do objektu sú prístupové mechanizmy (*dvere, závory, turnikety, apod.*) zavreté a uzamknuté. Po priložení identifikačnej karty k snímaciemu zariadeniu (môže byť samostatné alebo zabudované v prístupovom termináli) je bez ohľadu na práva držiteľa karty vždy vykonaný záznam o tejto udalosti do systému. Potom je na základe údajov uložených v systéme overované v časových, topologických a ďalších procesných súvislostiach oprávnenie držiteľa karty k priechodu či vstupu do objektu alebo zóny. Pokiaľ je daná osoba autorizovaná pre vstup, systém následne zabezpečí odomknutie alebo otvorenie prístupových mechanizmov. Okrem riadenia prístupových mechanizmov môže

systém iniciovať aj činnosť iných bezpečnostných systémov, v najjednoduchšom prípade napríklad spúšťať alarm.

Prístupový systém môžeme využiť aj pre kontrolovanie vjazdu áut na parkoviská, do garáží alebo do areálov firiem. Takto využívaný prístupový systém zahŕňa širokú paletu mechanických zariadení s elektrickými pohonmi závor, brán a blokovačov s rôznym príslušenstvom a množstvo elektrických jednotiek pre riadenie prístupu, detekciu vozidiel, zber dát a komunikáciu. Podľa potrieb a použitých zariadení, je možné prístupy automaticky povoľovať po identifikácii vodiča napr. magnetickou alebo čipovou kartou.

1.1. Funkcia anti-passback

V mnohých prípadoch je snaha o zámerné zneužitie identifikačných prvkov. Príkladom môže byť vstupná zábrana, pri ktorej si viacej osôb predáva jedinú kartu, s pomocou ktorej sa všetky dostanú dovnútra. V takýchto prípadoch sa požíva funkcia, ktorá týmto viacnásobným priechodom zabráni. V odborných literatúrach sa väčšinou označuje ako ***anti-passback***. Základnou myšlienkou anti-passbacku je kontrola smeru dvoch po sebe nasledujúcich priechodov. Vždy musí byť dodržaná sekvencia ***príchod – odchod – príchod***. V praxi to teda znamená, že držiteľ karty musí sledovaný priestor najskôr opustiť a až potom mu bude umožnený opätovný prístup. Riadiace jednotky pracujúce s anti-passbackom budú vo väčšine prípadov nastavené do tzv. jednodverového režimu. V tomto režime sú všetky čítania kariet na jednej čítačke brané ako príchody a všetky čítania na druhej čítačke zase naopak ako odchody. Aby však anti-passback fungoval na takejto jednotke správne, je nutné zaistiť, aby všetky osoby, ktoré cez ňu budú mať prístup, mali u svojej prístupovej úrovni povolený priechod na oboch stranách.

Prístupový systém môže používať tzv. ***globálny anti-passback***, u ktorého sa kontrolujú všetky vstupy do a výstupy zo strážených priestorov bez ohľadu na miesto priechodu. Aby toto riadenie fungovalo efektívne, je rozhodovanie posunuté na úroveň riadiaceho počítača s dátovým serverom. V prípade pozitívneho vyhodnotenia dáva príslušnej riadiacej jednotke pokyn k uvoľneniu priechodu. Z princípu funkcie je zrejmé, že v tomto prípade je trvalé pripojenie a činnosť komunikačného a dátového serveru nevyhnutná.

Okrem tohto globálneho sa používa i lokálny anti-passback, ktorý však funguje len v rámci jednej riadiacej jednotky. Ďalším rozdielom oproti globálneho je kontrola len viacerých vstupov – bráni opakovanému načítaniu tej istej karty na vstupnej čítačke. Na výstupnej čítačke môže byť platná karta čítaná i viackrát po sebe a vždy dôjde k zopnutiu príslušného relé.

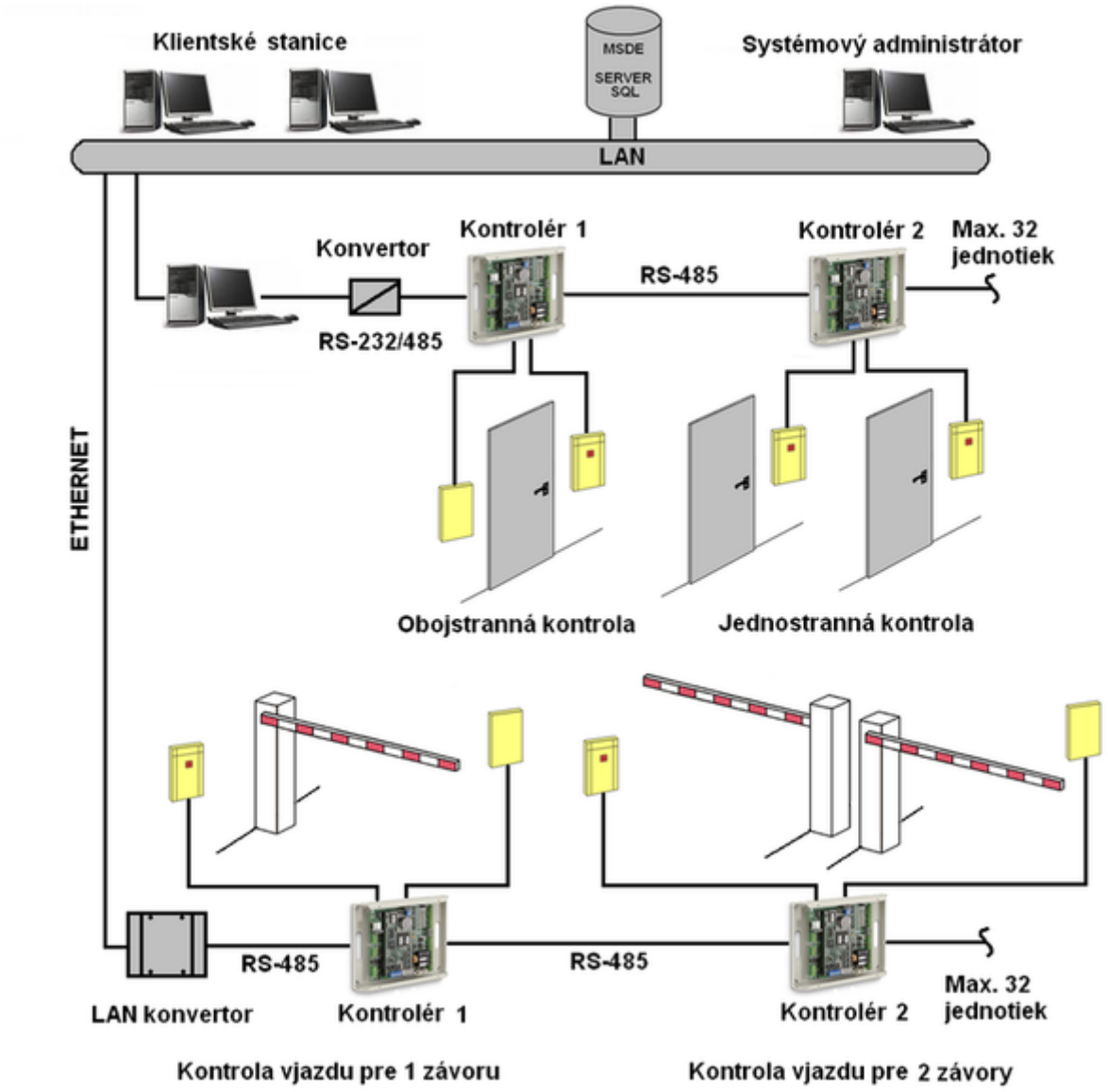
Kontroluje teda poradie vstup – odchod, ale len u jednej riadiacej jednotky. Nedá sa ním ale zabrániť druhému vstupu do objektu na inej jednotke.

V mnohých prípadoch u pomerne veľkého systému čítajúcom i viac zberníc, nie vždy môže úspešne zabrániť viacnásobnému priechodu. V prípade, že bežní užívatelia poznajú jeho základné režimové obmedzenia, môžu ľahko nájsť spôsob, ako túto funkciu obísť. Príkladom môže byť turniket, u ktorého sa na vstupnej strane načíta karta oprávneného užívateľa a povolí mu vstup. Následné načítanie karty na výstupnej čítačke – pretočenie turniketu „naprázdno“ a podanie karty inej (neoprávnenej) osobe na vstupnej strane. Takejto situácii sa dá úspešne predísť použitím tzv. ***časového anti-passbacku***. Okrem spomenutých obmedzení sa k ním pridáva ešte kontrola času, ktorý uplynul medzi dvoma poslednými čítaniami tej istej karty.

2. Technické riešenia

Pokiaľ chceme zaviesť elektronický prístupový systém (napr. do svojej firmy), bude potrebné zaopatriť vchodové dvere sledovaných miestností elektronickými zámkami, prístupovými terminálmi so snímacími zariadeniami a autorizované osoby vybaviť magnetickými alebo čipovými identifikačnými kartami. Doporučuje sa v rámci grafickej potlače karty, uviesť na nej údaje presne identifikujúce jej držiteľa (*fotografia, meno, rodné číslo, apod.*).

Údaje z prístupového systému sa spracovávajú centrálne na jednom počítači alebo sieťovo *(viď. obr.1)*. Čítacie jednotky sú zapojené v sieti čítacích jednotiek s nadriadeným riadiacim centrom. Riadiace miesto spracováva a vyhodnocuje načítané údaje podľa stupňa bezpečnosti. Výhodou sieťového spracovania (využíva SQL databázu na serveri) je, že informácie sú prístupné na ľubovoľnej klientskej stanici siete. Ďalšie výhody vyplývajú zo všeobecných vlastností SQL databáz. Výhodou lokálneho spracovania dát je jednoduchosť a nižšia cena systému. V tejto variante sú dáta ukladané na disku jedného počítača, ktorý je zároveň riadiacim počítačom pre terminály a jediným klientom.



Obr. 1: Bloková schéma systému

V mnohých prípadoch je možná previazanosť prístupového s dochádzkovým systémom, oba systémy sú na to logicky predurčené. Týmto spojením môžeme, v najjednoduchšom prípade, zabezpečiť jediným načítaním identifikačnej karty zamestnanca, zápis do knihy dochádzky a zároveň umožniť jeho vstup do objektu otvorením dverí či odblokovaním zábrany.

3. Základné prvky

V súčasnej dobe máme k dispozícii široké spektrum produktov špičkových svetových výrobcov pre realizáciu systému elektronickej kontroly vstupu. V závislosti od konkrétnych požiadaviek a finančnej náročnosti je možné si zadovážiť rôzne druhy komponentov. Dôležité je individuálne posúdenie pre každú aplikáciu.

K základným prvkom patria identifikačné zariadenia (čítačky), prevažne bezkontaktné, ďalej prístupové riadiace jednotky, elektrické a elektromagnetické zámky, softwarové prostriedky pre právu systému ale tiež podporné prvky a technológie (napr. tlačiarne pre podtlač plastových kariet).

3.1. Bezkontaktné čítačky kariet

Existuje množstvo rôznych typov čítačiek odlišujúcich sa nielen dizajnom a odolnosťou ale hlavne ich konfiguráciou, čítacím dosahom alebo frekvenciou s ktorou pracujú.

Väčšinou sú navrhované pre montáž na kovové rámy dverí alebo stĺpiky, ďalej pre interné alebo externé použitie, ale aj pre odolnosť proti úmyselného poškodeniu. Pracujú s frekvenciou 125 kHz alebo 13,56 MHz. Môžu byť nakonfigurované pre výstup dát buď vo formáte *Wiegand* [1] alebo vo formáte ABA Track II [2]. Tak môže byť aplikácia využívajúca klasický Wiegand alebo magnetické prúžky upravená na bezkontaktnú pri využití zostávajúcej kabeláži. V súčasnosti sú vybavené vyspelými funkciami napr. *QuickFlash* pre okamžitú odozvu čítania užívateľom, *SelfTest* pre uľahčenie oživovania pri inštalácii, výstupný *WatchDog* pre aplikácie vyžadujúce vyšší stupeň zabezpečenia alebo tiež zvukový výstup a troj - stavová LED.

Čítačky EM kariet (EM Series spoločnosti Indala) sú riešené ako multiprotokolové. Výhodné sú napr. v prípade, kedy užívateľ prechádza z jedného prístupového systému na iný s požiadavkou o zachovaní súčasných EM kariet užívateľov. Bez problémov sa prispôsobia väčšine nadväzujúcich technológií.

[1] Wiegandova karta obsahuje zabudované vodiče s magnetickými vlastnosťami, ktoré je obtiažné napodobniť a ktoré tak nesú informácie ako napr. číslo karty, číslo účtu, identifikácia zamestnanca a pod. Karta je čítaná jej priblížením alebo priložením k Wiegandovmu snímaču.

[2] ABA Track II je vlastne emulácia formátu magnetických pásikov.

3.2. Identifikačné prvky

Medzi tie najpoužívanejšie patria bezkontaktné (bezdotykové) karty (vďaka variante SmartCard) a prívesky. Tieto sa nemusia vkladať do čítačky kariet, stačí byť iba v dosahu rádio - frekvenčnej čítačky.

Skladajú sa z antény, transceivera a transpondéra. Anténa slúži na príjem a vysielanie signálu, transceiver umožňuje komunikáciu s čítačkou a transpondér najzložitejšia časť obsahuje samotné funkcie, ktoré má daný prvok plniť. Čipy sú k dispozícii vo vyhotovení na čítanie alebo čítanie a zápis. Dáta, ktoré sú uložené v čipe, sú prenášané pomocou zaliatej antény frekvenčným kmitaním, pričom prenos týchto dát sa pohybuje v rozmedzí nízkofrekvenčného 125 kHz a vysokofrekvenčného kmitočtu 13,56 MHz. V niektorých štátoch sa dajú používať aj ďalšie frekvencie ako 868 MHz (v Európe) a 915 MHz (v Amerike).

Možno ich dodávať s identifikačnými údajmi vo väčšine používaných formátov (najčastejšie Wiegand 26 bit) a s požadovanými hodnotami kódov užívateľa a rozsahom rady ID čísel jednotlivých kariet podľa zadania užívateľa. Z výroby je potom zaistené presné dodržanie sekvencie čísel bez výpadkov a presahov.

Vďaka veľmi malej hrúbke karty a použitej výrobnej technológii možno priamo tlačiť na čelnú stranu karty digitalizované fotografie a ľubovoľnú grafiku.

Existujú aj karty, ktoré obsahujú dve alebo viac čipových technológií - tzv. hybridné karty. Naproti tomu sú známe aj karty kombinované tzv. karty "dual-interface". Tieto karty majú jeden čip, ku ktorému sa dá pristúpiť buď pomocou kontaktného poľa, alebo bezdrôtovo, prostredníctvom zaliatej antény.

3.3. Prístupové riadiace jednotky

Riadiaca jednotka pre systémy kontroly vstupu tiež nazývaná kontrolér je určená k ovládaniu dverí v sledovanom priestore, v rôznych typoch inštaláciách. Použitie týchto jednotiek závisí na potrebe zabezpečenia priestoru. Záleží koľko dverí chceme zabezpečiť a akým spôsobom. Väčšinou sa používajú jednotky, ktoré sú schopné ovládať kontakty buď dvoch samostatných dverí (dvojdverový režim) alebo do jedných dverí, ale rôznymi smermi (príchod/odchod – jednodverový režim). Skladajú sa z tzv. podsystémov. Okrem rozhrania pre pripojenie čítačiek je každý z podsystémov osadený vstupmi pre pripojenie dverového snímača a odchodového tlačítka.

Riadiace jednotky môžu pracovať okrem priameho prepojenia (RS-232) s riadiacim počítačom taktiež v sieťovej prevádzke. V takejto prevádzke spolu komunikuje viacero kontrolérov prepojených spoločnou zbernicou RS-485. Jednotka môže pracovať i celkom autonómne – bez nutnosti komunikácie s riadiacim PC alebo ostatnými jednotkami.

Kapacita pamäti záznamov kontroléru závisí od konkrétneho typu riadiacej jednotky. Jednotka sa môže dodávať ako doska plošného spoja alebo ako modul v kovovom kryte – jeho neoprávnené otvorenie signalizuje tamper kontakt integrovaný na DPS, pridávaný je tiež záložný zdroj.

3.4. Softwarové prostriedky

O konfiguráciu jednotiek a ich monitorovanie sa stará príslušný *program*. Kombináciou bezpečnostných technológií s modernými sieťovými funkciami prináša plnohodnotné riešenie otázok bezpečnosti prístupu vhodné pre inštalácie akéhokoľvek rozsahu.

Je koncipovaný ako aplikácia typu klient – server. Pre užívateľa tento koncept prináša predovšetkým možnosť súbežnej činnosti viacerých operátorov. Jednotlivé klientske aplikácie komunikujú so serverom prostredníctvom TCP/IP protokolu – systém je tak možné spravovať odkiaľkoľvek. Prístup všetkých operátorov je chránený heslom, administrátor môže navyše každému z nich povoliť prístup len do niektorých častí programu. Heslom sa dá taktiež chrániť prístup dátového serveru k SQL databázam.

Podpora viacnásobných účtov dovoľuje operátorom rozdelenie kariet a ich držiteľov do samostatných skupín, s ktorými sa pracuje oddelene. Navyše majú operátori k dispozícii rôzne nástroje pre diagnostiku – užitočných pre oživenie systému alebo lokalizáciu hardwarových problémov, ďalej pre sledovanie pohybu osôb, návrh podtlače kariet alebo vytváranie prehľadných správ.

4. Popis prideleného kartového prístupového systému

4.1. Popis zapojenia

Pridelený kartový prístupový systém je zobrazený v *Prílohe 1*. Tvorí ho zdroj napätia, ktorý napája hlavnú riadiacu jednotku kontroly vstupu. Táto riadiaca jednotka je vlastne srdcom celého prístupového systému. Vyrobená je firmou *Honeywell* a jej názov je HUB Pro. Možnosti tejto jednotky budú popísané neskôr. K nej sú ďalej pripojené dve identifikačné zariadenia - bezkontaktné čítačky kariet značky *Indala* rady ASR-605 s čítacím dosahom do 13 cm a výstupným formátom *Wiegand 26-bit*. Imitujú vstupné čítačky dverí, kde každá z nich v prípade potreby otvára elektromagnetický zámok dverí značky BeFo.

Tento systém disponuje taktiež odchodovým tlačítkom s nápisom Emergency, používaným ako núdzové tlačítko pri poruche či inej neočakávanej situácii. Celý prístupový systém je prostredníctvom riadiacej jednotky a rozhrania RS-232 priamo prepojený s počítačom na ktorom beží komunikačný server. Súčasťou tohto systému sú bezkontaktné identifikačné kartičky a prívesky *Indala* s formátom 26b Wiegand.

Užívateľsky príjemné prostredie programu SKYLA Pro II, nainštalovaného na počítači, umožňuje obsluhu a rýchle programovanie riadiacej jednotky HUB Pro.

4.2. Časti systému

Celý systém pre kontrolu vstupu sa skladá z dvoch základných častí:

Hardwarová časť' – je reprezentovaná riadiacou jednotkou a prvkami pre komunikáciu. (PC, kabeláž zbernice atď.)

Softwarovú časť' – predstavujú dve spolupracujúce časti programu SKYLA Pro II – serverová a klientska (užívateľská).

4.2.1. Hardwarová časť

Riadiaca jednotka HUB Pro (*viď. Príloha 2*) je zariadenie, ktoré na základe informácií zo vstupných prvkov (najčastejšie čítačiek kariet) rozhoduje o poskytnutí alebo odmietnutí prístupu do sledovaného priestoru. Povolenie prístupu sa deje odblokovaním pripojeného elektrického zámku.

Systém pracuje s distribuovanými databázami čo znamená, že obsahy databáz sú rozosielané na jednotlivé riadiace panely. Tie potom pracujú celkom autonómne – bez nutnosti spolupráce s ostatnými prvkami v sieti ako je PC alebo ďalšie jednotky. Jednotka tak môže lokálne vyhlasovať poplachy pri násilne otvorených alebo nedovretých dverách, sama rozhodnúť, či osobu s konkrétnou kartou do chráneného priestoru postí alebo nie. Ďalšou výhodou je, že prípadný výpadok komunikácie s počítačom neohrozí funkčnosť systému. Pracovať bude rovnako, ale záznamy o prebehnutých udalostiach budú uschované vo vnútornej pamäti jednotky. Pre plné využitie všetkých vlastností a naprogramovanie je potrebné zaistenie komunikácie jednotky s ovládacím programom SKYLA Pro II.

Každá jednotka disponuje vlastnou pamäťou konfigurácie, kariet, i transakcií. Skladá sa z dvoch identických **podsystémov**, každý z nich môže ovládať jedny dvere celkom nezávisle od druhých. Používa pomocné relé, ktorými ovláda prepínacie kontakty. Stavy všetkých výstupov sú indikované pomocou LED. Obidve hlavné, zámkové relé môžu pracovať v niekoľkých režimoch – bežnom, prepínacom (pre ovládanie EZS), zatváracom alebo v režime anti-passback *(viď. kapitola 1.1. Funkcia anti-passback)*. Má dvojitú symetrickú štruktúru – na doske plošných spojov nájdete dve rovnaké svorkovnice pre pripojenie jednotlivých častí. Podobne je zdvojená i pamäť konfigurácie a kariet, tzn. v každom z podsystémov môžete uložiť úplne iné nastavenia a iné čísla kariet. Spoločná je len vnútorná pamäť udalostí.

Máme k dispozícii dva režimy, v ktorých môže jednotka pracovať – jedno alebo dvojdverový režim. Menia sa prepnutím DIP prepínača č.6. Pri zmene režimu je však vždy nutné jednotku reštartovať. V ***jednodverovom*** (obojstrannom) ***režime*** jednotka ovláda len jedny dvere, avšak obojstranne. Zaznamenáva príchody a odchody, tzn. slúži ako prístupový kontrolér pre jedny dvere v oboch smeroch s príchodovou a odchodovou čítačkou. V tomto prípade sa uplatňujú nastavenia len pre podsystém 1. Ak modul pracuje v ***dvojdverovom*** (jednostrannom) ***režime*** (čítačky len na vstupných stranách), ovláda dvoje dvere nezávisle na sebe. Používa obidva podsystémy.

Táto jednotka môže slúžiť ako riadiaca jednotka vstupu pre dvoje nezávislé dvere – so samostatnými databázami kariet a nastavením pre jednotlivé dvere.

HUB Pro sníma stavy z niekoľkých možných vstupov: kontaktov dverí, odchodových tlačítiek, pomocných vstupov a čítačiek s rozhraním Wiegand. Autonómne prevádza naprogramované činnosti a správy o vzniknutých udalostiach a posiela ich po linke RS-232 (alebo RS-485) do nadriadeného počítača. V prípade ak nie je spojenie s počítačom aktívne tzn. režim off-line, záznamy o udalostiach sa ukladajú do pamäti transakcie jednotky.

4.2.2. Softwarová časť

Tvoria ju už vyššie zmieňované dve časti programu SKYLA Pro II – serverová a klientska.

Serverová časť je reprezentovaná niekoľkými aplikáciami: dátovým serverom, komunikačným serverom a službami pre automatické spustenie naplánovaných akcií a kopírovanie popisov udalostí na sériový port.

Úlohou dátového serveru je zjednotenie a zaistenie prístupu k databázam pre všetkých pripojených klientov.

Komunikačný server zaobstaráva všetku komunikáciu s hardwarovým zariadením. Je preto nutné aby bol spustený na počítači, ku ktorému je linka (zbernica) s jednotkou fyzicky spojená alebo ktorý je pripojený k počítačovej sieti, po ktorej sa má komunikovať. V našom prípade kedy máme pripojený len jeden počítač, sú dátový aj komunikačný server nainštalované a prevádzkované na jedinom počítači.

Klientska časť – poskytuje užívateľské rozhranie, z ktorého je možné systém ovládať a monitorovať. So serverom komunikuje pomocou TCP/IP protokolu a preto môže byť nainštalovaný prakticky kdekoľvek, kde je k dispozícii prístup k TCP/IP sieti. Z predchádzajúceho odstavca, môže server komunikovať naraz i s viacerými klientmi, ktorý potom pracujú celkom nezávisle, avšak nad spoločnými databázami. Správa systému je tak možná i z viacerých miest súčasne.

4.3. Obsluha systému

Obsluha prístupového systému sa vykonáva prostredníctvom programu SKYLA Pro II, ktorá je vybavená sadou podporných nástrojov pre uľahčenie a spohodlnenie obsluhy. Patrí sem napr. automatické zálohovanie všetkých databáz v nastavených intervaloch alebo samočinné programovanie kariet do pamäti jednotky.

Program umožňuje podrobné sledovanie jednak vlastnej činnosti prístupového systému (príchody, odchody, narušenie režijných opatrení atď.), ale tiež spätné sledovanie operácií a zásahov všetkých operátorov. Základnou úlohou programu je nastavenie prístupového systému tak, aby čo najviac vyhovoval požiadavkám užívateľa. K tomu používa sadu databáz tzv. tabuľky. Pomocou nich sa nastavujú parametre systému kontroly vstupu. Jednoducho a prehľadne nadefinujete parametre jednotky HUB Pro, časové zóny, prístupové úrovne pre prideľovanie oprávnení osobám kedy a kde majú povolený prístup, ďalej môžete nastaviť oprávnenia pre operátorov, ktorý majú s programom pracovať.

V ponuke sú aj rôzne diagnostické nástroje užitočné pre oživenie systému alebo lokalizáciu hardwarových problémov – od mapovania zbernice až po podpornú diagnostiku jednotky.

K dispozícii sú tiež rôzne servisné nástroje ako napr. zálohovanie alebo obnovenie databázy, import alebo export dát, mapovanie zberníc, hromadné pridanie osôb, parametre jednotiek atď.

5. Zdôvodnenie voľby jednotlivých úloh

Mojou úlohou bolo vytvoriť laboratórnu úlohu. K dispozícii som mal pridelený kartový prístupový systém popísaný v predchádzajúcej kapitole. Pre vytvorenie konkrétnych častí laboratórnej úlohy som sa rozhodol preto, aby si študenti vyskúšali obsluhu takéhoto kartového prístupového systému, keď budú v úlohe administrátora resp. operátora. Do úvahy som bral i to, že úloha je časovo obmedzená dĺžkou vyučovania 90 min. Z tohto dôvodu sa nedali prebrať všetky dostupné možnosti takéhoto prístupového systému. Zvolil som preto len tie najzákladnejšie a najčastejšie vykonávané úkony, ktoré administrátor či operátor používa. Použitý prístupový systém môže teda pracovať v dvoch režimoch. Ja som zvolil jednostranný – *dvojdverový režim*, čo znamená, že použité čítačky budú nezávisle na sebe ovládať dvoje dvere (len na vstupných stranách). Študenti budú mať teda za úlohu vytvoriť prístupový systém modelového podniku a vytvoriť konkrétne osoby - zamestnancov a prideliť im prístupové práva do určitých oblastí v areály podniku. V laboratórnej úlohe vystupuje celkom päť osôb, patriacich do iného oddelenia. Sú im pridelené identifikačné zariadenia pre prístup do systému.

Postup konkrétnych úloh je zvolený tak, aby sa študenti naučili veľmi rýchlo a bez komplikácií nastaviť systém a obsluhovať ho. Pri nastavovaní systému postupne vypĺňajú potrebné informácie jednotlivých databáz – tzv. tabuľky. Pomocou nich vytvárajú časové úrovne, počas ktorých má byť povolené – uvoľnenie dverí. Sú potrebné pri vytváraní prístupových úrovní. Ďalej vytvoria novú lokalitu. Jedná sa o priame prepojenie kontroléru s počítačom pomocou zbernice RS-232. V tabuľke Jednotky sa uchovávajú všetky potrebné nastavenia týkajúce sa riadiacej jednotky HUB Pro. Definujú sa tu jednotlivé podsystémy – dvere *(záleží na čísle podsystému)*, ich časové zóny, časovače, systémové a denníkové príznaky. Systémové príznaky nastavujú režimy chovania jednotky a denníkové príznaky určujú, ktoré typy udalostí sa budú ukladať do pamäti jednotky – tým pádom aj zobrazovať v okne História programu. Správca systému taktiež využíva nástroj pre diagnostiku jednotky. Umožní mu sledovať v reálnom čase aktuálne stavy vstupov, výstupov jednotky, meniť stavy výstupov, kontrolovať veľkosť napájacieho napätia alebo na diaľku vymazávanie databáz na jednotke. Analógové hodnoty môžu pomôcť odhaliť tie situácie, v ktorých slučky nepracujú správne, napr. v prípade problému s prechodovými odpormi kontaktov alebo kabeláže.

Ďalšou používanou je tabuľka Oblasti. Slúži pre definovanie užívateľských oblastí, v ktorých sa má sledovať prítomnosť osôb. Môžu byť do seba vnorené alebo úplne nezávislé. Pre správcu majú praktické využitie hlavne v prehľade prítomnosti osôb. V okamihu kedy bude zaznamenané čítanie karty osoby na čítačke z inej oblasti, bude táto osoba preradená do aktuálnej oblasti. Nástroj, pomocou ktorého sa prideľujú prístupové práva celým skupinám naraz sa nazýva Prístupové úrovne. Prideľovanie určitej prístupovej úrovne naraz skupinám osôb sa deje preto, lebo sa nepredpokladá žeby každá osoba mala svoju jedinečnú sadu oprávnení. V reálnych systémoch sa vždy dá nájsť nejaká skupina osôb, ktoré budú mať rovnaké prístupové práva. Tabuľka oddelení je pomocnou štruktúrou. Neviaže sa k jednotke ani k lokalite, využíva sa pri triedení a vyhľadávaní osôb alebo pri vytváraní zostáv. Častou úlohou správcu prístupového systému je vytváranie nových osôb, ktorým nastaví určité práva prístupu do systému a prideľuje im nejaký identifikačný prvok (kartu, PIN, atď.). Typicky to bývajú zamestnanci, návštevy, dodávatelia apod. Tieto ale aj iné záznamy (organizačného a personálneho charakteru, fotografie alebo textové poznámky) združuje tabuľka Osoby.

Aby riadiaca jednotka fungovala podľa nadefinovaných tabuliek, musia sa tieto informácie preniesť do pamäti jednotky. Na to slúži funkcia programovanie jednotky, ktorá umožňuje vykonať programovanie manuálne alebo automaticky.

Ďalšie nástroje, ktoré sú v použitom programe dostupné slúžia na vytváranie prehľadu o udalostiach, ku ktorým dochádza na hardwarovej alebo softwarovej časti systému alebo pre zistenie, kde sa konkrétna osoba aktuálne nachádza. Správca tak môže veľmi rýchlo vyhľadať požadované informácie. Informácie o prebehnutých udalostiach alebo obsah tabuliek môže byť zobrazený, vytlačený alebo vyexportovaný použitím zostáv.

6. Laboratórna úloha kartového prístupového systému

6.1. Cieľ

Zapojenie a konfigurácia prideleného kartového prístupového systému. Jedná sa o konfiguráciu, ktorá obsahuje modul *HUB Pro*, ktorý je základným prvkom pre výstavbu prístupových systémov malého a stredného rozsahu. V spojení s prakticky ľubovoľnými čítačkami alebo klávesnicami s dátovým výstupom Wiegand umožňuje realizáciu užívateľsky efektívneho systému pre kontrolu prístupu.

6.2. Upozornenie

Pri zapájaní dbajte na farbu použitých káblov. Pri zapájaní napätí jednotlivých súčastí dodržujte túto farebnú kombináciu: červená pre + 12V a šedá pre – (GND) pre lepšiu prehľadnosť.

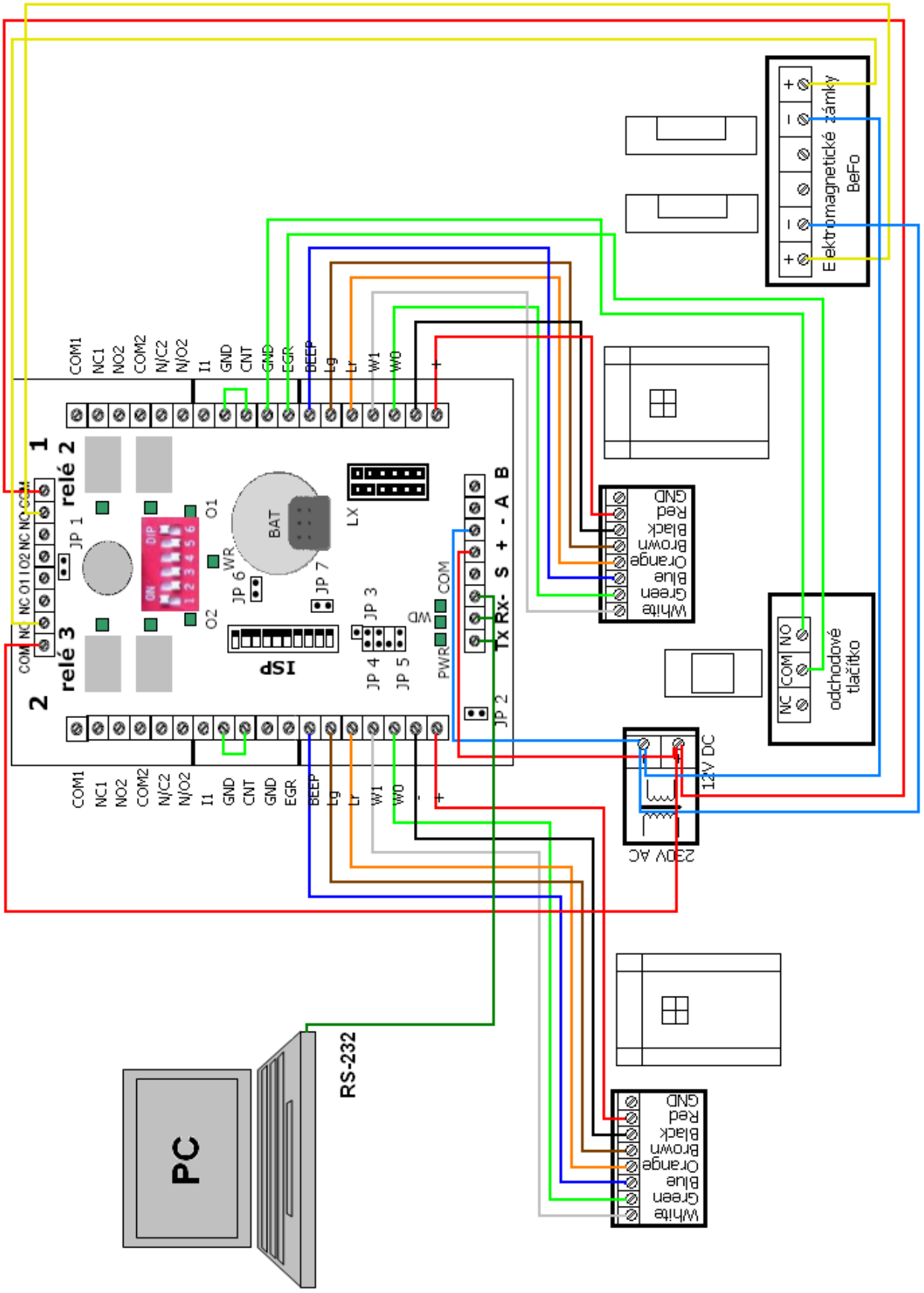
Aby kontrolér správne pracoval, nesmie sa napájacie napätie dostať mimo rozsah 11V ÷ 14V.

Pred zapojením do siete si nechajte zapojenie vždy najskôr skontrolovať vyučujúcim.

6.3. Zoznam zariadení

1. Riadiaca jednotka HUB Pro.
2. PC s programom SKYLA Pro II.
3. Odchodové tlačítko.
4. 2x bezdrôtové čítačky.
5. 2x elektrické zámky na dvere.
6. 3x ID karty a 2x ID prívesky
7. Zdroj napätia.
8. Svorkovnice a káble na prepojenie.

6.4. Schéma zapojenia



6.5. Zadanie

1. Oboznámte sa s predloženými prístrojmi, preštudujte si z priložených materiálov jednotlivé nastavenia a možnosti ústredni HUB Pro .

2. Zapojte ústredňu a prepojte ju s počítačom. Spustite program SKYLA Pro II a oboznámte sa z jeho prostredím.

3. Vytvorte prístupový systém modelového podniku. Naprogramujte hlavnú riadiacu jednotku a pridajte k nej jednotlivé podsystémy (dvere), ktoré ďalej pripojte k príslušným oblastiam podľa návodu. Vytvorte databázu užívateľov a prideľte im prístupové práva do systému.

4. Predveďte vyučujúcemu vytvorený prístupový systém. Overte funkciu odchodového tlačítka. Zobrazte si históriu prístupov do systému a zistite kde sa jednotlivé osoby nachádzajú.

5. Pred vypnutím ústredni vymažte nastavenie riadiacej jednotky a vytvorených užívateľov.

6.6. Návod

1. Po prevzatí zariadenia skontrolujte jednotlivé moduly a identifikujte ich.

2. Zapojte jednotlivé časti ústredni podľa uvedenej schémy zapojenia. Dodržujte pritom správnu farebnú kombináciu káblov. Po zapojení si nechajte zapojenie skontrolovať vyučujúcim. Po odsúhlasení pripojte ústredňu k sieťovému napájaniu. Pri štarte ústredni sa prevedie kontrola pripojených čítačiek zvukovou signalizáciou. Na riadiacej jednotke svieti zelená LED PWR – indikuje napájanie.
Ďalej prepojte riediacu jednotku kontroly vstupu HUB Pro s počítačom (pomocou sériového portu RS 232). Na počítači spustite program SKYLA Pro II pre konfiguráciu a správu systému kontroly vstupu. Prihláste sa ako ***Student*** a heslo zadajte ***student*** . Oboznámte sa s prostredím programu *(viď. obr.6.1, kapitola 6.9. Obrázky)*.

3. Pri realizácii dostupného kartového prístupového systému si treba uvedomiť že sú dostupné dve čítačky kariet a dva zámky dverí. Budete teda

realizovať prístupový systém s dvojdverovým (jednostranným) režimom – je nastavený ak je v riadiacej jednotke prepínač DIP č.6 v ***spodnej*** polohe.
Ďalšie nastavenia systému a programovanie jednotiek budete vykonávať v programe SKYLA Pro II. K zadávaniu a uchovávaniu informácií o tom ako má jednotka fungovať slúžia v programe samostatné databázy – tzv. ***tabuľky***. Naľavo v hlavnom menu. Aby ste mohli systém rýchlo a bez komplikácií nastaviť budete vyplňovať tabuľky v nasledovnom poradí.

- ***Časové zóny*** – Kliknite na tlačítko ***Nový***, ktoré nájdete na lište v ľavom hornom rohu okna tabuľky. V zozname záznamov v hornej časti okna naskočí nový riadok a v spodnej časti okna, v paneli detailov záznamu, sa objavia prázdne polia pre vyplnenie. Zadajte do všetkých polí požadované údaje a kliknite na tlačítko ***uložiť***, vytvorte tak tieto časové zóny:

Časové zóny

	Název	Popis	Čas zač	Čas uko	Pondě	Úterý	Středa	Čtvrtek	Pátek	Sobota	Neděle	Svátky
	Vždy		0:00	23:59	☑	☑	☑	☑	☑	☑	☑	☑
	Pracovná doba		8:00	16:00	☑	☑	☑	☑	☑	☐	☐	☐
	Víkendy + sviatky		8:00	16:00	☐	☐	☐	☐	☐	☑	☑	☑
▶	Upratovanie		17:00	19:00	☑	☑	☑	☑	☑	☐	☐	☐

Obr. 2: Časové zóny

Poznámka: Sviatky môžete pridávať a editovať v tabuľke ***Sviatky***.

- ***Lokality*** – Odpovedá zbernici (RS-232). Vytvorte novú lokalitu, kliknite na tlačítko ***Nový***, zadajte názov lokality ***Zbernica RS-232***, typ portu zvoľte ***RS-232***, zaškrtnite ***Aktívny*** (po reštarte komunikačného serveru bude zbernica aktívna), ďalej vyberte z ***Voľby pripojenia*** názov a rýchlosť sériového portu PC, cez ktorý sa bude s jednotkou komunikovať. Zatrhnite *checkbox* ***Pri uložení aplikovať zmeny***. Ten zaisťuje, že v okamihu uloženia záznamu lokality sa komunikačný server pokúsi aplikovať zmeny, ktoré ste nastavili. Lokalitu ***uložte***. *Pozor!* Pri pridávaní novej lokality môže pokus o spustenie komunikácie s lokalitou zlyhať (budete informovaný výstražným dialógom). V takom prípade v textovom menu ***Servis*** vyberte položku ***Reinicializácia komunikačného serveru*** *viď. obr. 6.4, kapitola 6.9. Obrázky*.

- ***Jednotky*** – Nastavenie týkajúce sa riadiacej jednotky HUB Pro. Tá je zostavená z dvoch podsystémov, ktoré umožňujú pripojenie dvoch nezávislých čítačiek (dverí). Kliknite na tlačítko ***Nový***. V spodnej časti okna sa objavia prázdne políčka pre nastavenie parametrov. Aktívna bude záložka ***Detail***, ktorá združuje parametre spoločné pre celú jednotku. Tu zadajte ***Názov***, pod ktorým bude jednotka vo všetkých častiach programu vystupovať (napr. *HUB Pro*). Zo zoznamu v poli ***Lokalita*** vyberte vami vytvorenú lokalitu

Zbernica RS-232. Ide o zbernicu, na ktorej bude jednotka pripojená. V poli ***Typ jednotky*** nastavte typ pripojeného modulu – vyberte možnosť ***HUB Pro***. V riadku ***Adresa*** zadajte adresu jednotky, ktorá musí byť v rámci lokality jedinečná (napr.***1***). Ďalším nastavovacím prvkom na tejto záložke je checkbox ***Aktívny***. Zatrhnite ho, aby mohla fyzicky pripojená jednotka na zbernici komunikovať s počítačom. Druhý checkbox ***Pri uložení aplikovať zmeny do komunikačného serveru*** opäť zatrhnite ako v predchádzajúcom prípade. Ako posledný bod na tejto záložke je nastaviť v poli ***Formát karty*** dátový formát, s ktorým budú pracovať karty a čítačky pripojené k jednotke. Zvoľte implicitný formát ***Wiegand*** s dĺžkou ***26*** bitov.

Poznámka: Tlačítko ***Diagnostika***, ktoré sa nachádza tiež na tejto záložke, bude aktívne až v okamihu uloženia záznamu a zahájení komunikácie s jednotkou.

Kliknite na záložku ***Podsystémy***. Na nej budete definovať čítačky (dvere) pripojené k jednotke. Kliknite na tlačítko ***Pridať*** uprostred pravého okraja okna programu. V poli ***Podsystémy pripojené k jednotke*** naskočí prázdny riadok pre zadanie názvu nového podsystému. Bude označený ako ***Číslo 0*** – ide o prvý podsystém na HUBu Pro. Kliknite do prázdneho riadku v stĺpci ***Názov***. Tu zadajte názov (jedinečný v rámci celého systému), pod ktorým bude podsystém v programe figurovať. Ide teda o meno čítačky (dverí), napr. ***Kancelárie***. Nezabudnite zatrhnúť políčko ***Dochádzková***. To spôsobí, že priechody osôb cez túto čítačku budú automaticky kopírované do databáze programu Dochádzka. V spodnej časti okna by mala byť aktívna podzáložka ***Časové zóny*** s prehľadom všetkých doposiaľ zadaných časových zón. Označte všetky časové zóny. Tie sa potom objavia u tohto podsystému v okne pri nastavovaní prístupových úrovní. Funkcia ***Autoodomknutie*** znamená, že po celú dobu trvania príslušnej časovej zóny budú dvere odomknuté. Nechajte preto zvolenú možnosť ***Nie***. Kliknutím na podzáložku ***Príznaky*** aktivujete pohľad na nastavenia systémových a denníkových príkazov. *Systémové* príznaky nastavujú režimy chovania jednotky, zatiaľ čo *denníkové* príznaky určujú, ktoré typy udalostí sa budú ukladať do pamäti jednotky a tým i zobrazovať v okne História programu. Obidva sú prednastavené tak, aby vyhovovali väčšine aplikácií. Nastavenie si prezrite. Poslednou podzáložkou sú ***Časovače***. Tu sa nachádza nastavenie troch systémových časovačov. Implicitne nastavené na ***Otvorenie – 4s***, ***Poplach – 10s***, ***Nedovretie – 15s***.

Obdobným spôsobom definujte druhý podsystém – druhú čítačku (dvere) s jedinečným názvom napr. ***Výroba***, opäť zatrhnite všetky časové zóny.

Takto nastavené všetky parametre zapíšte do databáze tlačítkom ***Uložiť***, ktoré nájdete na lište v ľavom hornom rohu okna Jednotky. Pri pridaní novej jednotky sa doporučuje ***reinicializácia komunikačného serveru***, túto položku nájdete v textovom menu ***Servis*** *viď. obr. 6.4, kapitola 6.9. Obrázky*.

Súčasťou tejto tabuľky je už zmieňované tlačítko ***Diagnostika*** v záložke ***Detail***, ktoré slúži pri oživovaní alebo stopovaní závad, umožňuje sledovať v reálnom čase aktuálne stavy vstupov, výstupov alebo slučiek jednotky, kontrolovať veľkosť napájacieho napätia, meniť stavy výstupov alebo na diaľku mazať databázy na jednotke. Prehliadnite si záložku ***Prehľad***, ktorá ponúka rýchly prehľad aktuálneho stavu jednotky.

- ***Oblasti*** – Slúži na nadefinovanie užívateľských oblastí, v ktorých sa má sledovať pohyb osôb.

Poznámka: Praktické využitie definovania oblastí v tejto tabuľke sa skrýva pod ikonou *Prítomnosť osôb* v *Hlavnom menu*, ku ktorej sa dostanete neskôr.
Po otvorení tabuľky *Oblasti* uvidíte v ľavom paneli štruktúru už nadefinovaných oblastí. Správne by tam mala byť (ak nie vytvote ju!) iba najvyššia oblasť s názvom ***Východisková úroveň***, do ktorej vytvoríte vnorené oblasti. Novú oblasť vytvoríte tak, že kliknete na tlačítko ***Nový,*** ktoré nájdete na lište v ľavom hornom rohu okna tabuľky. Zadajte názov novej oblasti (napr. ***Administratívna budova***) označte ju kurzorom a pridajte k nej jeden z dostupných podsystémov (napr. ***Kancelárie***) – dvojklik na vybratý podsystém. Takto vytvorte ďalšiu vnorenú oblasť do oblasti ***Východisková úroveň***. Nazvite ju napr. ***Výrobná hala***, označte ju a dvojklikom pridajte druhý podsystém ***Výroba***.

- ***Prístupové úrovne*** – Tu si najskôr nadefinujete prístupové oprávnenia jednotlivých skupín a pri pridávaní osôb (kariet) do systému už len vyberiete, do ktorej skupiny bude dotyčná osoba patriť. Použite tlačítko ***Nový*** a vytvorte prístupovú úroveň s názvom ***Vedenie podniku***. V záložke ***Prístupy*** vidíte stromovú štruktúru vytvorenej lokality, k nej priradenú jednotku a jej podsystémy a časové zóny. Zatrhnite tie časové zóny, počas ktorých majú byť príslušné dvere pre vytváranú úroveň prístupné. Vedenie podniku bude mať prístup všade a vždy, takže zatrhnite časovú zónu ***Vždy*** u oboch podsystémoch . Na pravej strane okna nechajte označený ***Režim osoby – Normálny*** a ***Podmienku príchodu – Karta***. Vytvorenú úroveň nezabudnite ***uložiť***. Podľa nasledujúcej tabuľky vytvorte ďalšie prístupové úrovne:

Tab.1: Prístupové úrovne

Prístupová úroveň	**časové zóny**	
	Podsys. 0 - Kancelárie	**Podsys. 1 - Výroba**
Vedenie podniku	Vždy	Vždy
Personálne	Pracovná doba, víkendy+sv.	-
Výroba	-	Pracovná doba, víkendy+sv.
Upratovanie	Upratovanie	Upratovanie
Návšteva	Pracovná doba	Pracovná doba

- ***Oddelenie*** – pomocná štruktúra, ktorá slúži pre potreby organizácie osôb (triedenie a vyhľadávanie osôb). Vytvorte nasledovné oddelenia: ***Vedenie, Personálne, Výroba, Upratovanie a Návšteva.***

- ***Osoby*** – Tu vytvoríte celkom päť osôb, ktorým nastavíte určité prístupové práva a pridelíte identifikačný prvok – kartu alebo prívesok (*viď. obr.3*). Najskôr vymažte prípadné pred vami vytvorené osoby. Kliknite na ***Nový***, v aktuálnej záložke ***Detail*** vyplňte požadované údaje. Jedinečné osobné číslo, pod ktorým bude osoba identifikovaná v rámci dochádzkového systému. Číslo karty sa zadáva v podobe *facility kód* medzera *ID (viď. obr. 6.5, kapitola 6.9. Obrázky)*. Formát karty zvoľte ***Wiegand 26b***. Keďže sú použité iba čítačky, PIN kód nebudete generovať. Ďalšia záložka ***Foto*** – pre pridanie fotografie osoby. Dôležitejšou je však záložka ***Prístupové úrovne***. Zatrhnite jednu z dostupných úrovní, ktorá bude osobe priradená a osobu ***uložte***.

Osoby

	Os. číslo	Příjmení	Jméno	Titul	Příst.úroveň	Oddělení	Číslo karty
	1	Šťastný	Peter	Ing	Vedenie podn	Vedenie	201 11049
	2	Skúpý	Miroslav		Výroba	Výroba	189 12716
	3	Nováková	Jana		Personálne	Personálne	201 11050
	4	Malíková	Lucia		Upratovanie	Upratovanie	189 12715
▶	5	Forman	Petr	Ing	Návšteva	Návšteva	189 12717

Obr. 3: Ukážka vytvorených osôb

Poznámka: Prístupová úroveň by mala logicky zodpovedať oddeleniu, do ktorého je daná osoba pridelená.
Takýmto spôsobom môžete vytvárať, vymazávať alebo editovať takmer ľubovoľný počet osôb (záleží od verzii programu).

Týmto je konfigurácia tabuliek hotová. Zostáva už len tieto informácie preniesť do pamäti jednotky. Na to slúži v ***Hlavnom menu*** ikona ***Programovanie***. Táto položka sprístupňuje ručné i automatické programovanie jednotky. Vykonajte ***Manuálne*** programovanie. Označte vami vytvorenú jednotku v príslušnej lokalite. Ďalej označte tabuľky, ktoré sa naprogramujú do pamäti jednotky (***Osoby, časové zóny, sviatky***). Zatrhnite tiež možnosť ***Najprv vymazať osoby*** a spustite programovanie. Otvorí sa vám okno ***Priebeh operácie***, ktoré indikuje stav programovania. Úspešne dokončené programovanie všetkých záznamov je zobrazené stavom ***Dokončené*** v stĺpci ***Stav***.
Poznámka: V prípade stavu ***Chyba*** skontrolujte komunikáciu medzi komunikačným serverom a jednotkou *viz. Príloha*. Po odstránení prípadných problémov spustite programovanie znovu.

4. Vytvorený kartový prístupový systém predveďte vyučujúcemu. Predveďte možnosti prístupu jednotlivých osôb do systému, v závislosti na definovaných časových zónach, oblastiach a prístupových úrovní. Vyskúšajte si tiež funkciu ***odchodového tlačítka***, ktorá spočíva v použití ako núdzové tlačítko, kedy sa po jeho stlačení odomkne zámok dverí.
Ako správca takéhoto systému si určite budete chcieť zobraziť históriu prístupov do systému alebo zistiť kde sa určitá osoba práve teraz nachádza. Vyskúšajte si preto funkcie dostupných nástrojov v tomto programe. Zobrazte a prehliadnite si históriu prístupov do systému. V ***Hlavnom menu*** kliknite na ikonu ***História*** – ***Prehľad***. Tu sa uchovávajú informácie o udalostiach, ku ktorým prichádza na hardwarovej časti systému, teda u riadiacej jednotky (príchody, odchody, výpadky komunikácie, pokusy o čítanie neznámych kariet atď.). Môžete si nadefinovať vlastný filter alebo tiež nastaviť farby jednotlivých udalostí.
Vykonajte ***Archiváciu histórie***, ktorá sa doporučuje. ***Vyčistíte*** si tak tabuľku histórie a nenecháte ju narastať *„donekonečna ”* – čo spôsobuje spomaľovanie reakcií pri manipulácii.
Zistiť kde sa momentálne osoby nachádzajú umožňuje funkcia ***Prítomnosť osôb***, ktorá sa tiež nachádza v ***Hlavnom menu***. Prezrite si ju. Práve tu sa uplatní definovanie oblastí.
Poznámka: V našom prípade sa zaznamenáva len príchod osoby do oblasti.
Pre zaznamenávanie odchodu by sa musela použiť odchodová čítačka.

Všetky tieto a iné informácie môžete vytvoriť aj vo forme ***Zostáv***, ktoré sú určené pre tlač alebo export.

5. Pred ukončením programu a vypnutím ústredni najskôr **vymažte všetky** vaše nastavenia. V menu ***Tabuľky*** postupne vymažte všetky vami definované informácie. Začnite od poslednej tabuľky ***Osoby***, smerom hore – predídete tak kolíziám. Program ukončite a rozpojte všetko čo ste zapojili.

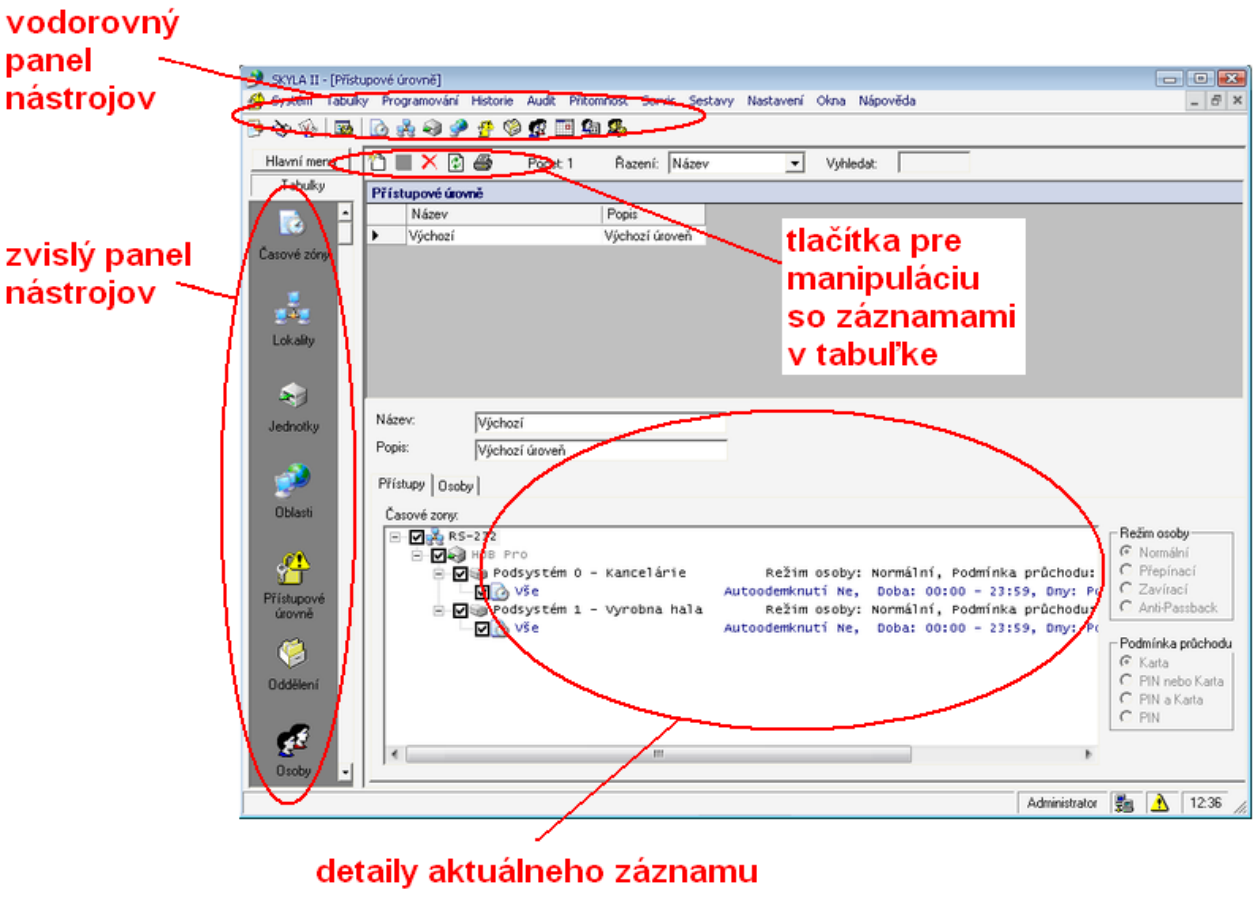
6.7. Rozvrhnutie hodiny

a) dochádzka študentov + vydanie zariadení (5 minút)
b) popis materiálu a pomôcok (5 minút)
c) samostatná práca študentov + priebežná kontrola a hodnotenie (80 minút)

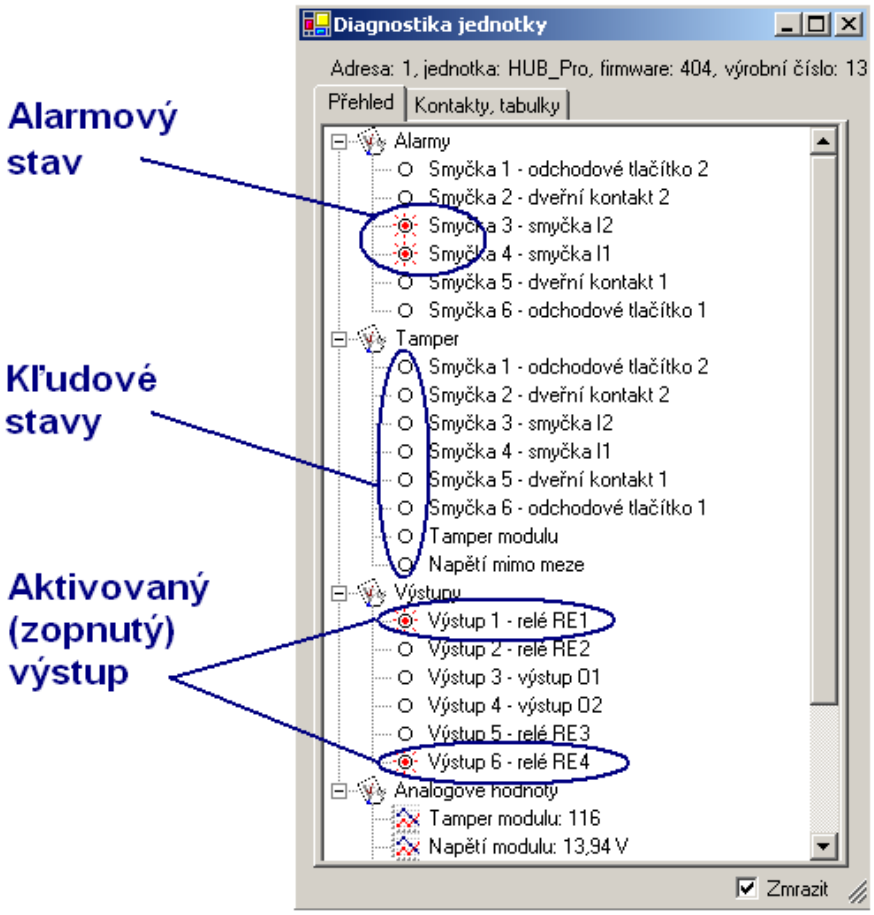
6.8. Zoznam literatúry

1. Užívateľský manuál riadiacej jednotky – HUB Pro
2. Inštalačný manuál k softwaru – SKYLA Pro II

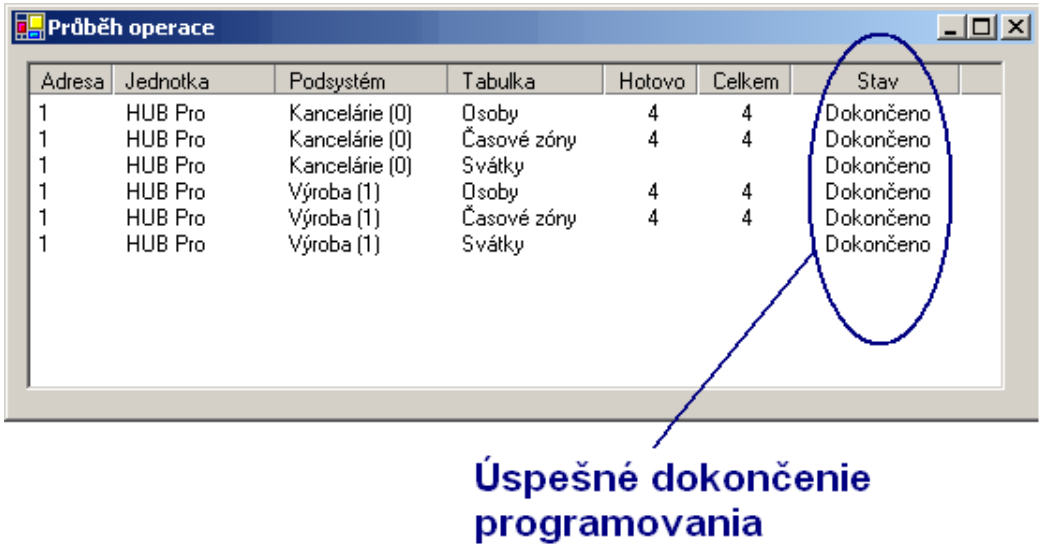
6.9. Obrázky



Obr. 6.1: Panely nástrojov v programe SKYLA Pro II



Obr. 6.2: Diagnostika jednotky (Prehľad)



Obr. 6.3: Priebeh operácie programovania

Reinicializácia komunikačného serveru:

Znamená znovu spustenie procesu komunikácie s jednotkou. Väčšinou sa vykonáva v prípade pridania novej lokality alebo jednotky, po obnovení databáze zo zálohy.

a) Textové menu – V menu ***Servis*** kliknite na voľbu ***Reinicializácia komunikačného serveru***.

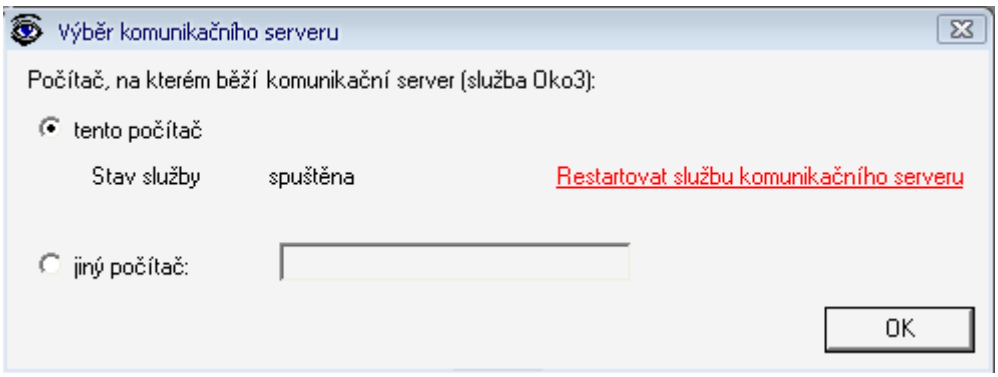
b) Systémová lišta – Tu je neustále indikovaný stav komunikačného serveru a súčasne stav spojenia s ním.

 symbol oka znamená, že server beží a bezproblémové spojenie s ním.

 znamená buď zastavenú službu komunikačného serveru alebo prerušenie spojenia s ním.

 znamená spojenie s kom. serverom, ale nie je detekovaný hardwarový kľúč (*zrejme ste pridali ďalšiu jednotku, na čo nemáte licenciu*).

Dvoj kliknutím na ikonu služby v systémovej lište sa otvorí okno pre výber a reštartovanie kom. serveru.



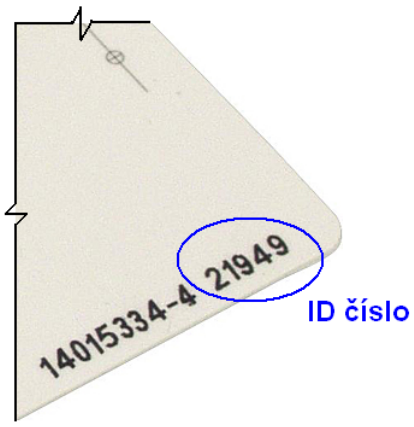
Obr. 6.4: Reštart komunikačného serveru

Kliknutím na pole s textom **Reštartovať službu komunikačného serveru** zaistíte reinicializáciu. Vo väčšine prípadov majú reštart a reinicializácia rovnaký efekt.

Formát kariet:

Dostupné karty, prívesky sú formátu **Wiegand 26b** u ktorých sa číslo zadáva v podobe *facility kód(FC) - medzera - ID číslo*.

Čísla kariet sú:	**189**	**12715**	Prívesky:	**201** **11049**
	189	**12716**		**201** **11050**
	189	**12717**		



Obr. 6.5: ID číslo karty

Záver

Na základe použitých literárnych zdrojov boli v tejto práci popísané princípy a technické riešenia súčasných kartových prístupových systémov, základné možnosti bežných prístupových ústrední a ich periférií. Popísané sú tiež časti prideleného prístupového systému a jeho obsluha. Na základe prideleného kartového prístupového systému a stanovených podmienok som navrhol konkrétne úkony laboratórnej úlohy, v ktorých sa študenti naučia konfiguráciu prístupového systému a vyskúšajú si úlohu správcu takéhoto systému. Postup úlohy bol smerovaný tak, aby bol prístupový systém vytvorený rýchlo a bez komplikácií.

Literatúra

[1] KŘEČEK, S. a kol.: Příručka zabezpečovací techniky. Blatenská tiskárna, Blatná 2003.

[2] SMITH, R. E.: Authentication. Addison Wesley, Boston 2002.

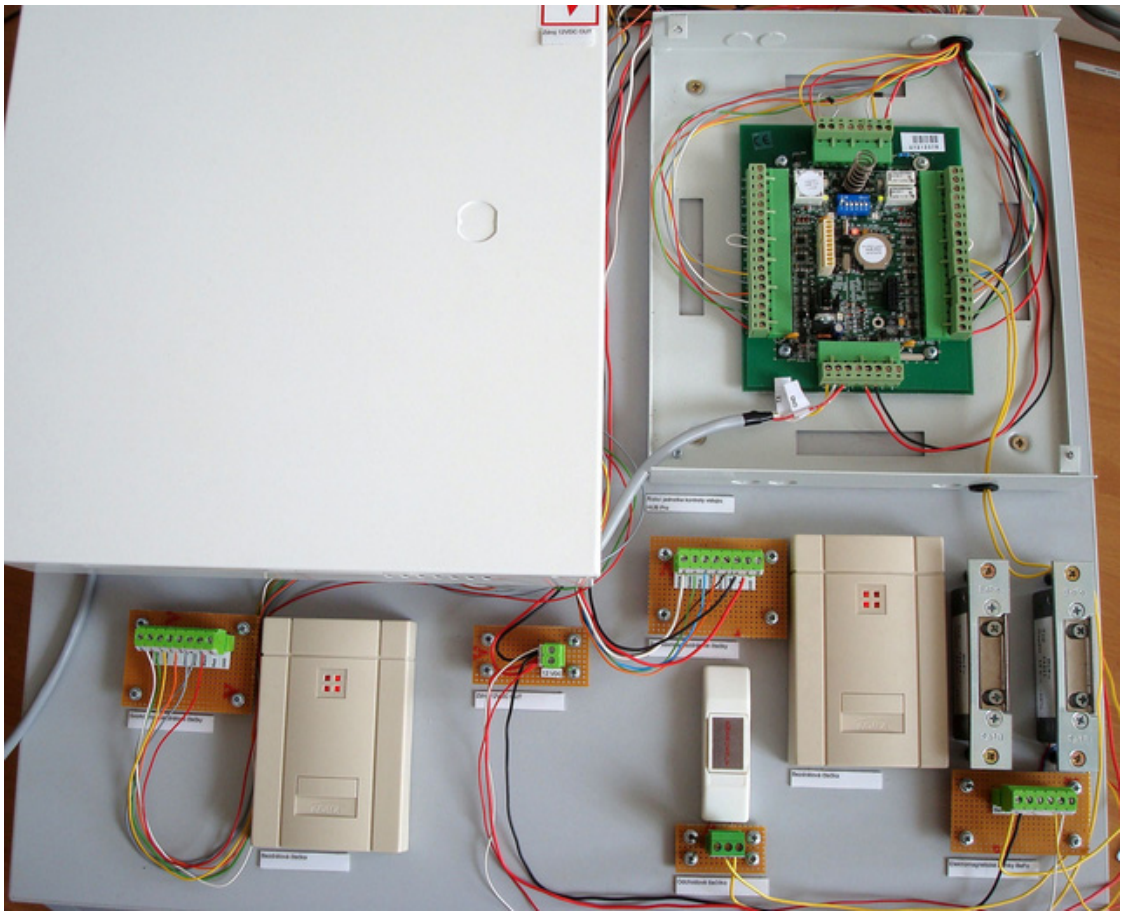
[3] HRIC, Branislav. Prístupový systém. [online], 2007.
Dostupný z: <http://arbe.sk/pdfs/Prez_pris.pdf>.

[4] Honeywell: *Inštalačný manuál HUB Pro.*
Dostupný z: <http://access.olympo.cz/pristupovka/pristupovka.htm>

[5] Honeywell: *Užívateľský manuál SKYLA Pro II.*
Dostupný z: <http://access.olympo.cz/pristupovka/pristupovka.htm>

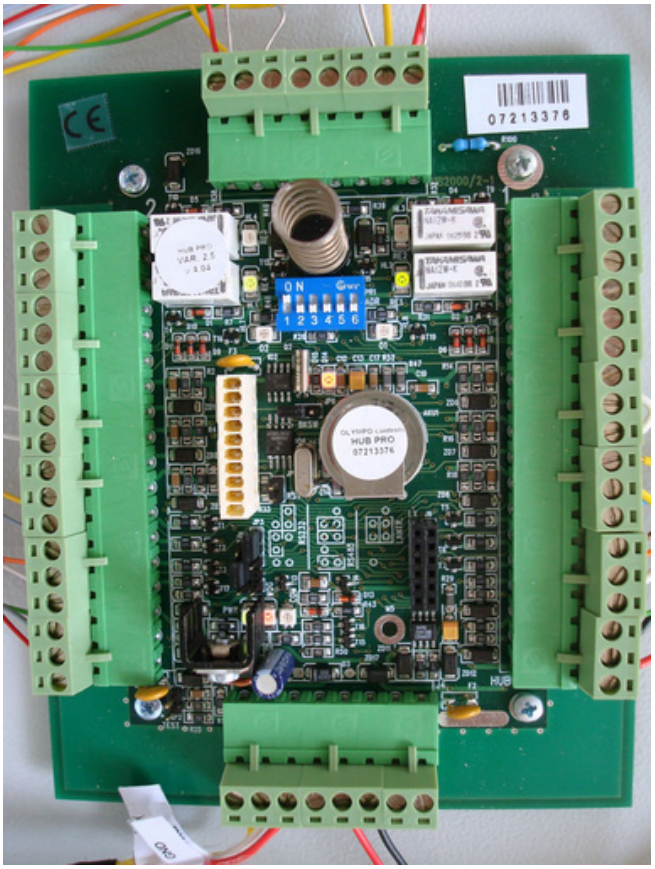
Zoznam príloh

Príloha 1: Pridelený kartový prístupový systém



Obrázok prideleného kartového prístupového systému

Príloha 2: Riadiaca jednotka HUB Pro



Obrázok riadiacej jednotky HUB Pro