Integrace kontaktních a bezkontaktních karetních čteček do systému WinPack

Integration of contact and contactless card readers in WinPack system

Juraj Jando

Bakalářská práce
2009

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektrotechniky a měření
akademický rok: 2008/2009

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Juraj JANDO**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Integrace kontaktních a bezkontaktních karetních čteček do systému WinPack**

Zásady pro vypracování:

1. **Seznamte se s technologií řešení kontaktních a bezkontaktních karet**
2. **Realizujte podrobný průzkum týkající se formátů karet u různých systémů, výrobců a užívaných komunikačních protokolů**
3. **Popište způsob připojení do WinPacku a programování panelů a dokumentujte ho na čtečkách v laboratoři D309**

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **WinPack – uživatelský manuál. Honeywell Access Systems. ADI Olympo. Brno. 425 s.**
2. **Instalační manuál k ústřednám GALAXY G3. Brno. ADI Olympo.**
3. **KŘEČEK S. a kol.: Příručka zabezpečovací techniky. 3.vydání. Praha. Criterius. 313 s.ISBN 80-902938-2-4.**
4. **Popis vlastností čipu Micro RWD. Poslední revize 5.3.05. Dostupné z www.ibtechnology.co.uk/PDF/magswipe_dec.PDF**

Vedoucí bakalářské práce: **Ing. Stanislav Goňa, Ph.D.**
Ústav elektrotechniky a měření

Datum zadání bakalářské práce: **20. února 2009**

Termín odevzdání bakalářské práce: **20. května 2009**

Ve Zlíně dne 20. února 2009

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

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Předmětem bakalářské práce je seznámení se s technologií řešení kontaktních a bezkontaktních karet, průzkumu týkajícího se formátů karet u různých výrobců, systémů a užívaných komunikačních protokolů. Praktická část se zabývá přístupovým systémem WinPack. V této části je popsáno připojení, programování a konfigurace panelů, nastavení časových zón, oprávnění, podlažních map, karet a přidávání uživatelů karet.

Klíčová slova: Magnetický karty, čipový karty, formát karet, WinPack

ABSTRACT

The subject of bachelor thesis is familiarity with the technology solutions contact and contactless cards, the survey concerning formats for different card manufacturers, system and used communication protocols. The practical part deals with the access system WinPack. This section describes the connection, programming and panel configuration, set the time zones, privileges, storied maps, cards, and addition of user cards.

Keywords: Magnetic cards, chip cards, format of cards, Winpack

Poďakovanie

Úvodom by som chcel poďakovať vedúcemu mojej bakalárskej práce pánu Ing. Stanislavovi Goňovi, Ph.D., za cenné rady a pripomienky pri tvorbe bakalárskej práce.

Prohlašuji, že

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

Prohlašuji,

že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.

Ve Zlíně …….…….

podpis diplomanta

OBSAH

ÚVOD

S identifikačnou kartou sa už každý z nás stretol, či už sa jednalo o magnetickú kartu ktorá sa využíva hlavne ako bankomatovová a platobná karta, bezkontaktná karta ktorá sa využíva v prístupových systémoch pre ich jednoduchú, efektívnu a rýchlu manipuláciu, ďalej to mohla byť čipová karta ktorá sa používa vo verejnej doprave pre ich väčšiu kryptografickú ochranu ktorá slúži ako cestovný lístok a zároveň slúži ako elektronická peňaženka na ktorej sú uložené peniaze. Ďalším typom čipovej karty sú telefónne karty na ktorej je určitý obsah kreditu a pri volaní sa za prevolané minúty odpočíta určitá čiastka z uloženého kreditu, ktorá záleží na podmienkach volaní. Ďalej sa môžeme stretnúť s kartou pri platení v obchode kde sú to vernostné a členské karty. Pri používaní mobilného telefónu tiež používame identifikačnú kartu na ktorej sú uložené dáta o mobilnom čísle, mene vlastníka karty apod. Ide o špeciálny druh čipovej karty ktorá je navrhnutá pre mobilnú komunikáciu. V poslednom rade sa karty začali používať aj pri platení mýtneho za cestné úseky a pri hazardných hrách. S prvými kartami sa začalo experimentovať už na začiatku 20 storočia ale prvé použitie kedy ľudom zjednodušili život bolo až v 60 rokoch minulého storočia kde zrýchlili kontrolu cestovných lístkov a zároveň urýchlili prepravu osôb v Londýnskom metre. Postupne začali prenikať aj do ostatných častí priemyslu a stali sa našou dennou potrebou a ovplyvňujú náš každodenný život. Neodmysliteľnou súčasťou kariet sú čítačky kariet. Týchto čítačiek existuje niekoľko základných druhov medzi ktoré patria: čítačka magnetických kariet, čítačka kontaktných a bezkontaktných kariet s frekvenciou 125 KHz a 13,56 MHz, čítačka čipových kariet. Tieto čítačky sa ďalej rozlišujú podľa toho, aký formát čítačka je schopná prečítať. Čítačky sa používajú v závislosti od typu použitia identifikačnej karty. Ďalšou časťou ktorá súvisí s identifikačnými kartami sú prístupové a dochádzkové systémy. Väčšinou sa jedná o počítačom riadené systémy ktoré zjednodušujú, zefektívňujú, obmedzujú a kontrolujú prístup do určitého vymedzeného priestoru a kontrolujú dochádzku. Vstup do týchto priestorov môže byť vymedzený iba určeným osobám a to vo vymedzených časových intervaloch. Túto problematiku sa budem snažiť bližšie popísať a rozobrať v bakalárskej práci.

I. TEORETICKÁ ČÁST

1 TECHNOLÓGIA RIEŠENIA KONTAKTNÝCH A BEZKONTAKTNÝCH KARIET / ČÍTAČIEK

Identifikačná karta je predmet ktorý slúži od uchovávania informácii na identifikáciu osoby až po zložitý kryptografický prostriedok, ktorý je kľúčom k bezpečnostnému prístupu k informačným a komunikačným technológiám. Identifikačné karty delíme na *karty s magnetickým prúžkom*, *bezkontaktné karty*, *kontaktné čipové karty* a *bezkontaktné čipové karty*. V systémoch kontroly vstupu sú najčastejšie využívané bezkontaktné karty, kontaktné a bezkontaktné čipové karty. V súčastnej dobe sú častejšie používané bezkontaktné čipové karty pre ich pohodlnejšiu manipuláciu.

Typické aplikácie pre využitie kariet:

- Elektronická kontrola vstupu
- Dochádzkový systém
- Elektronická peňaženka
- Verejná doprava (cestovné lístky)
- Vernostné, členské karty
- ID karty
- Hazardné hry
- Elektronické kľúče
- Logistika
- Spoplatnenie ciest
- Telefóne karty

1.1 Magnetické karty

Karty s magnetickým prúžkom používame už niekoľko desaťročí. Magnetické karty boli prvý krát použité na začiatku roku 1960 firmou The London Transit Authority ktorá ho použila v Londýnskom metre. Tato karta obsahovala magnetický prúžok ktorý bol na papieri a až neskôr firma IBM (International Business Machines Corporation) vytvorila plastovú kartu s magnetickým prúžkom pre americkú vládu. Americká vláda využívala túto kartu pre bezpečnostný systém. Ku koncu 70 rokov sa magnetický prúžok dostal aj na kreditné karty. V súčasnosti sa najviac používajú magnetické karty v bankovníctve, dochádzkových systémoch, elektronickej kontrole vstupu a ako cestovné karty. Magnetické

karty sú jednoduchým nosičom dátových informácii. Dnes sú nahradzované čipovými kartami pre ich malú kryptografickú ochranu a väčšiu náchylnosť na poškodenie oproti čipovým kartám.

Obr. 1. Magnetická karta.

1.1.1 Normy

Pre magnetické karty existujú normy vydané International Organization for Standardization ktoré definujú fyzikálne vlastnosti kariet, veľkosti, miesto pre magnetický pásik, magnetickú charakteristiku. (ISO 7810, ISO 7811, ISO 7812, ISO 7813, ISO 4909).

1.1.2 Princíp činnosti

Údaje na karte sa zapisujú na magnetický prúžok, ktorý je tvorený z množstva magnetických častí kovového základu, schopných svojou orientáciou uchovávať údaje. Pri zapisovaní údajov na kartu sa na magnetickom pásiku vytvoria krátke úseky s rôznou polaritou, ktoré vznikajú pri magnetickej indukcii. Pri čítaní karty prechádza čítacie zariadenie po zmagnetizovanom povrchu a malý permanentný magnet je buď priťahovaný alebo odpudzujúci magnetickou silou a tým dochádza k indukcií kladného alebo záporného napätia [1].

Na magnetickom prúžku sa nachádzajú celkom tri stopy, každá z nich má svoj špecifický význam a na každú sa ukladajú rozdielne elektronické údaje.

1. *stopa (IATA)* – Prvá stopa bola definovaná už v roku 1969 Medzinárodnou asociáciou leteckých dopravcov (International Air Transportation Association). Karta slúžila pri automatickom odbavení cestujúcich. Výsledkom bolo

zjednodušenie a urýchlenie odbavovania. Do bankového sektoru sa dostala v roku 1970. Prvá stopa obsahuje 79 alfanumerických znakov. Pre číslo karty bolo vyhradených 18 numerických znakov a pre meno vlastníka karty 26 alfa numerických znakov. Ostatné znaky sú vyhradené pre kontrolné znaky.

2. *stopa (ABA)* – Druhá stopa bola vytvorená Americkou Bankovou Asociáciou (American Bankers Association) pre on-line finančné transakcie. Táto stopa obsahuje 40 numerických znakov z toho je 19 vyhradených pre číslo karty.

3. *stopa (THRIFT)* – Tuto stopu vytvorili banky špeciálne pre finančné transakcie. V tejto stope je možné nielen čítať údaje ale aj údaje zapisovať na kartu. Pri výbere hotovosti z bankomatu sa prepísal finančný limit ktorý bol stanovený buď na deň alebo iné časové obdobie, ktoré bolo definované podľa potrieb zákazníka. Po uplynutí tejto doby sa limit znova navŕšil na pôvodnú úroveň. Ďalej bolo možné zmeniť PIN kód. Tretia stopa obsahuje 107 numerických znakov ktoré sú vyhradené pre číslo karty, kód štátu, kód meny, PIN, dátum platnosti karty, finanční limit atd. [2].

1.1.3 LiCo a HiCo karty

Magnetické karty rozdeľujeme ďalej podľa koercivity. Jedná sa o schopnosť pernamentného magnetu odolávať demagnetizácii externým magnetickým polom a tiež svojím vlastným demagnetizačným polom. Koercivita sa udáva Oerstedech (Oe).

LiCo (Low Coercivity) 300 Oe - sú charakteristické nízkou kapacitou záznamu, malou životnosťou, sú náchylnejšie na poškodenie a vyznačujú sa svetlo hnedým magnetickým prúžkom. Pri kódovaní magnetických stôp nevyžadujú taký vysoký výkon ako HiCo karty. V súčasnosti sa moc nepoužívajú pre ich nízku životnosť a náchylnosť na poškodenie.

HiCo (High Coercivity) 4000 Oe – sú charakteristické väčšou kapacitou záznamu, dlhou životnosťou, sú ťažie poškoditeľné a vyznačujú sa čiernym magnetickým prúžkom. Využívajú sa hlavne ako bankomatové karty a pri elektronickej kontrole vstupu [1,2].

1.2 Čipové karty

S čipovou kartou v rôznych formách sa stretávame už niekoľko rokov a väčšina ľudí sa s ňou už stretla. Prvá možnosť kedy sme sa s ňou mohli zoznámiť boli karty do verejných telefónnych automatov. Išlo o predplatenú telefónu kartu na ktorej bol kredit v určitej hodnote. Pri telefonovaní sa kredit zmenšil o stanovenú hodnotu, ktorá závisela od počtu predvolaných minút a tarife za prevolanú minútu. Prvé hromadné použitie kariet pre verejné telefóne automaty bolo vo Francúzku v roku 1983. Dovtedy boli telefóne búdky vystavované častým útokom zlodejov. Zároveň to bolo aj prvé hromadné rozšírenie čipových kariet. V súčasnosti sa môžeme stretnúť s čipovou kartou pri platobných kartách. Platobné karty s magnetickým prúžkom sú nahradzované čipovými kartami, pre ich väčšiu kryptografickú ochranu. Ďalej sa stretávame s kartami pri elektronickej kontrole vstupu, pri dochádzkových systémoch, v mobilných telefónoch kde sa nachádza SIM karta, v dopravných prostriedkoch, kde sú využívané ako cestovné lístky a v ďalších aplikáciách. V poslednej dobe sú zvyšované nároky na bezpečnosť, rýchlosť a presnosť čipových kariet a zaujímajú dôležité postavenie všade tam, kde je treba kontrolovať, odbavovať veľké množstvo zamestnancov, cestujúcich apod. Spoločným faktorom týchto kariet je vysoká bezpečnosť a vysoká odolnosť proti poškodeniu.

Obr. 2. Čipová karta.

1.2.1 Zloženie čipovej karty

Základom každej čipovej karty je polovodičový čip, ktorý je vložený do plastovej karty. Najčastejšou technológiou vloženia čipu do karty je vyfrézovanie dutiny v karte, ktorá má rozmer čipu a následne vlepenie čipu do dutiny. V prípade bezkontaktných čipových kariet

sa často zalieva čip spolu s anténou priamo do karty. Rozmer karty je daný normou ISO 7816-1. Táto norma obsahuje dva rozmery karty. Veľký rozmer majú platobné karty, identifikačné karty atd., malý rozmer majú SIM karty v mobilných telefónoch. Najjednoduchšie čipové karty obsahujú iba pamäťové registre, ktoré je možné nastavovať, pripočítať a odpočítať nejakú predefinovanú hodnotu (napr. telefóne karty do verejných telefónnych automatov). Zložitejšie sú procesorové karty ktoré majú okrem pamäte aj procesor vykonávať príkazy. Pre využitie v bezpečnostných systémoch sú najzaujímavejšie mikroprocesorové (smart) karty, ktoré obsahujú podobné komponenty ako celý počítač – procesor, špecializované kryptografické koprocesory, rôzne typy pamätí a vstupné/výstupné kanály integrované v jedinom čipe. Moderné čipy majú implementovanú radu bezpečnostných mechanizmov, ktoré sťažujú rôzne typy útokov na bezpečnosť. Ďalšou dôležitou časťou čipovej karty je zabudovaný software – operačný systém, ktorý je z pravidla umiestňovaný v pamäti ROM čipu. Práve kombinácia možností čipu a funkcií operačného systému je podstatou čipovej karty. Ide o špecializovaný miniatúrny kryptografický počítač, ktorý komunikuje s PC alebo terminálom prostredníctvom kontaktného alebo rádiového prenosu a bezpečne realizuje kryptografické a dátové operácie [3,4].

1.2.2 Druhy kariet

- Pamäťová čipová karta (chip card)
- Pamäťová čipová karta so špeciálnou logikou (PIN, čítače apod.)
- procesorová čipová karta (smart card)
- kontaktná čipová karta
- bezkontaktná čipová karta
- hybridná čipová karta
- duálna čipová karta
- PKI čipová karta

Kontaktná čipová karta:

Kontaktná čipová karta má kontaktnú plôšku s ôsmimi kontaktmi, ktorých funkcia je

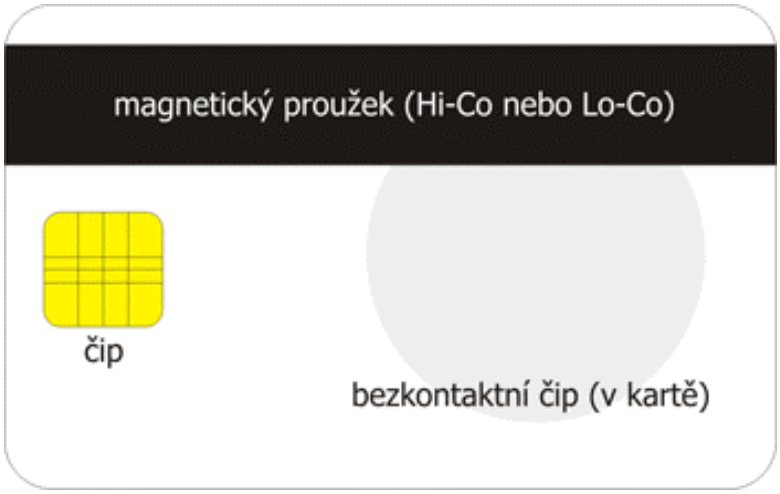
umiestnená na čipovej karte a je štandardizovaná normou ISO/IEC 7816-2. Jednotlivé kontakty slúžia pre napájanie čipu, sériovou komunikáciou, privedenie externého taktovacieho signálu a programovacieho napätia. Rozšírenie komunikačných možností čipovej karty špecifikuje štandard ISO/IEC 7816-12. Na jeho základe sú dnes vyrábané karty s integrovaným USB rozhraním priamo do čipu, označované USB-ICC. Hlavnou výhodou je možnosť eliminácie čipových kariet, ktorá je nahradzovaná štandartným USB rozhraním počítača, ku ktorému je pripojený adaptér obsahujúci čipovú kartu v SIM formáte.

Bezkontaktná čipová karta:

Bezkontaktná rádiová komunikácia s čipovou kartou na krátku vzdialenosť (do desiatich centimetrov) využíva frekvenciu 13,56 MHz a je definovaná štandardom ISO/IEC 14443. Vysoká prenosová rýchlosť je nutná pre rýchly zápis a čítanie väčších objemov dát, hlavne v oblasti biometrickej identifikácie a verifikácie. V minulosti bola hlavná prekážka využitia sofistikovaných kryptografických možností čipových kariet prostredníctvom rádiového prenosu príliš vysoká energetická náročnosť čipov. V súčastné dobe je možné realizovať i komplexné kryptografické operácie založené na algoritmoch RSA alebo ECC s využitím rádiového prenosu. Avšak nastávajú nové bezpečnostné rizika spojené s rádiovým prenosom (neoprávnené čítanie, odpočúvanie, presmerovanie).

Hybridná čipová karta:

Hybridná karta je kombinácia čipovej a magnetické karty. Obsahuje čip a magnetický prúžok. Tieto karty sa využívajú v bankovníctve a postupne nahrádzajú magnetické karty. Niekedy sú nazývané skratkou EMV. Táto skratka je zložená z asociácií Europay, MasterCard a Visa, ktoré definovali štandardy pre čipovú platobnú kartu.



Obr. 3. Hybridná čipová karta.

PKI čipové karty:

PKI čipová karta je procesorová čipová karta, ktorá je schopná uskutočňovať príkazy v asymetrickej a symetrickej kryptografii a často i výpočet odtlačku (hash). PKI karty obsahujú tiež kryptografické koprocesory pre skrátenie času pri kryptografických operácií [3,4].

1.2.3 Komunikácia čipovej karty s čítačkou kariet

Čipová karta nemá vlastný zdroj elektrickej energie a pri komunikácii s čítačkou kariet je závislá na dodávke elektrickej energie od čítačky kariet. U bezkontaktnej karty sa energia prenáša vo forme indukcie elektromagnetického poľa z čítačky do antény čipovej karty. Pri bezdrôtovej komunikácii sa používa nosná frekvencia 13,56 Mhz a maximálna vzdialenosť sa udáva 10 cm. Energie indukovaná v anténe karty nabije čip. Pri spätnom prenose informácii karta využíva princíp záťažovej modulácie. Karta odoberá väčšie alebo menšie množstvo energie z elektromagnetického poľa čítačky a reprezentuje tak logickú 0 a logickú 1. Čítačka detekuje zmeny odberu energie v jej elektromagnetickom poly a následne ich vyhodnocuje [3,4].

1.2.4 Bezpečnosť kariet

Ochrana dát pred neoprávneným prístupom je riešiteľná pomocou rôznych opatrení, medzi najúčinnejšie patrí správne implementovaná kryptografická ochrana. Potrebné hlavné kľúče sú generované a uložené v bezpečnom systéme pre správu kľúča a následne importované na čipovú kartu pre každodenné používanie. Čipová karta a programové vybavenie

umožňuje bezpečne šifrovať a dešifrovať pracovné kľúče, ktoré sú následne využité k vlastnému šifrovaniu alebo dešifrovaniu dát. Pri poruche alebo strate je možné hlavné kľúče importovať na náhradnú kartu [3,4].

1.3 Karty využívajúce wiegand efekt

Wiegand efekt dostal meno po svojom objaviteľovi John R. Wiegand. Bol vytvorený ako špeciálna technológia na komunikáciou medzi kartou a čítačkou kariet. Wiegand karty sa používajú v bezpečnostných systémoch pri elektronickej kontrole vstupu a dochádzkových systémoch. Je charakteristický pomalou prenosovou rýchlosťou oproti čipovým a magnetickým kartám. Prenosová rýchlosť je okolo 1000 bit/s.

1.3.1 Dátový rámec

V wiegand formáte existuje niekoľko rôznych typov protokolov. Najčastejšie sa vyskytuje formát pozostávajúci z 26 bitov. 26 bitový mód pozostáva z počiatočného párneho paritného bitu, 24 bitov z údajmi a jedného vypínacieho nepárneho paritného bitu.

```
Converted BCD data:      00 00 04 60 22 12 75  (14 digits)
Truncated BCD data:         04 60 22 12 75  (10 digits)

Wiegand 26 bit sequence:-  E   (b0 --------- b11)  (b12 -------- b23)  O

                           E   (  0    4    6      0    2    2  )  O

                           1    0000 0100 0110   0000 0010 0010    1
```

Obr. 4. Príklad 26 bitového wiegand módu.

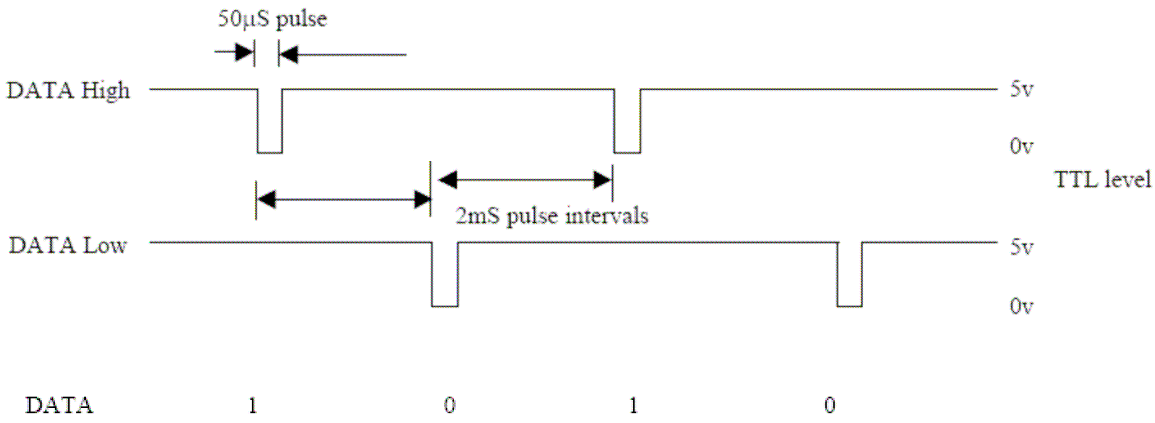
E – je párny paritný bit pre bity od 0 – 11

O – je nepárny paritný bit pre bity od 12 – 23

1.3.2 Kódovanie logickej nuly a jednotky

Wiegand rozhranie používa na generovanie logickej 0 a logickej 1 tri výstupy, z ktorých jeden je uzemnenie a ďalšie dva sa označujú ako DATA 0 (niekedy sa používa ozn. DATA High) a DATA 1 (niekedy sa používa ozn. DATA Low). Ak na čítačke nie je žiadna aktivita na DATA 0 a DATA 1 sa privádza napätia o hodnote 5V. Ak sa generuje logická

1, napätia na DATA 1 klesne k nule ale napätia na DATA 0 sa nemení. Tento impulz trvá 50 μs. Ak sa generuje logická 0, napätie na DATA 0 klesne k nule a napätie na DATA 1 ostáva rovnaké. Interval medzi dvoma impulzmi trvá 2 ms [5].



Obr. 5. Wiegand protokol časový diagram.

2 FORMÁTY KARIET U RÔZNYCH VÝROBCOV A SYSTÉMOV

Táto kapitola pojednáva o prístupových systémoch, čítačkách kariet a formátov kariet.

2.1 Prehľad prístupových systémov v Českej Republike a Európe

Systém pre kontrolu vstupu je počítačom riadený súbor prvkov kontrolujúci prístup do určitého priestoru. Ten býva zabezpečený zámkom a nejakou formou kľúča. Vstup do takto chráneného priestoru je potom povolený len zodpovedným osobám v určitých, vopred definovaných časových intervaloch. Určenie, kto bude mať do chráneného priestoru prístup, je vďaka použitia počítača jednoduché a ľahko meniteľné. Slabinou klasického zabezpečenia pomocou zámku a kľúča je práve nutnosť existencie fyzického kľúča. Ten sa dá pomerne ľahko duplikovať a umožňuje prístup komukoľvek, kto ho vlastní. Navyše neexistuje evidencia, kedy a kým bol kľúč použitý. Nebezpečenstvo straty alebo odcudzenia kľúča spolu s nákladnou výmenou zámkov takýto systém značne predražujú. Systém kontroly vstupu je dostupnou a efektívnou alternatívou predošlého. Všetci ľudia, ktorí sa budú v sledovaných priestoroch pohybovať, dostanú kartu alebo číselný kód umožňujúci vstup do jednotlivých oblastí iba zodpovedným osobám v určených časoch. Malý programovateľný riadiaci panel potom na základe identifikácie človeka vstup povolí alebo nepovolí. Ak dôjde k strate alebo odcudzenie karty, možno riadiaci panel jednoducho a rýchlo preprogramovať. Ak je navyše aj kontrola vstupu pripojená k počítačovej sieti, majú používatelia k dispozícii oveľa širšie spektrum funkcií. Systém môže v takom prípade obsahovať CCTV prvky pre vzdialené monitorovanie priestor, môže zaznamenávať a poskytovať informácie o používaní kariet aj kódov, ponúknuť obsluhe prehľady udalostí v systéme alebo generovať správy z databáz. Okrem toho umožňuje systém kontroly vstupu uchovávať a spravovať základné informácie o tisícovkách zamestnancov. Dôležitým znakom takýchto systémov je schopnosť tvorby a správy identifikačných preukazov zamestnancov so základnými personálnymi údajmi a fotografií [6].

2.1.1 Concept Access 4000 – Zabezpečovací a prístupový systém

Systémy Concept 3000 a Access 4000 patria medzi obľúbené a často používané zabezpečovacie a prístupové systémy, najmä vo veľmi rozsiahlych inštaláciách. Concept vyniká najmä počtom priestorov (nezávislých podsystémov), ktorých môže byť až 250, počet používateľov môže dosahovať až 4000 (počet používateľov, ktorí sú determinovaný

iba kartou, môže byť viac ako 24 000). Veľmi zaujímavý je aj počet zón (slučiek), ktorý môže dosahovať až 4000 (vylúčením systémové vstupy strážiaci stav I&HAS), počet programovateľných výstupov môže dosahovať maxima 3800. Concept umožňuje riešiť nielen zabezpečenia objektu, ale poskytuje aj funkcie pre vytvorenie prístupového systému. Evidenciu prístupu osôb možno ľubovoľne napojiť sa zabezpečovacím systémom, čím sa pre užívateľov značne zjednodušuje ovládanie a samozrejme tiež klesajú náklady na určené na inštaláciu. Veľmi žiadanú vlastností je aj možnosť spolupráca s dochádzkovým systémom - vďaka použitie štandardného komunikačného formátu Wiegand možné pripojiť ľubovoľný dochádzkový terminál, ktorý poskytuje dáta v tomto formáte. Užívateľ tak nie je viazaný na použitie jediného typu dochádzkového terminálu a príslušného programového vybavenia. Možnosti nasadenia však siahajú ďalej, pretože Concept ponúka ďalšie nad štandartné funkcie, ako napríklad riadenie a zabezpečenie výťahov. Náročných užívateľov určite zaujme možnosť automatického riadenia klimatizácia a kúrenie, pričom nie sú zanedbané ani bežné funkcie pre riadenie jednoduchších elektrospotrebičov. Medzi unikátne vlastnosti patrí možnosť snímania a vyhodnocovanie "analógových" veličín (napr. teplota, intenzita osvetlenia, atď.) Jednou z najdôležitejších vlastností každého zabezpečovacieho zariadenia sú jeho komunikačné schopnosti. Concept nezaostáva ani v tejto oblasti, pretože ústredňa umožňuje komunikovať s množstvom zariadenia, medzi ne patrí v prvom rade PCO, ďalej potom aj prostriedky výpočtovej techniky, mobilný GSM telefóny alebo možné dáta prenášať po LAN s protokolom TCP / IP (napr. Internet). Ústredňa umožňuje paralelné spracovanie komunikačných úloh, takže je možné súčasne prenášať informácie na niekoľko rôznych typov zariadení (súčasne možno prenášať správu na PCO, rovnakú udalosť tlačiť na tlačiarni, zobrazovať v PC, zasielať formou SMS na mobilný telefón, ...). Concept 4000 možno cez sériové rozhranie pripojiť k PC, na ktorom beží softvér AcceptNet. Pomocou tohto programu je možné ľahko konfigurovať a kontrolovať stav viac ústrední, pričom toto ovládanie a nastavenie môže byť robené z viac koncových staníc (z tzv. recenzie). Program AcceptNet umožňuje pripojenie ďalších programových alebo hardvérových modulov, ktoré môžu podstatne rozširovať funkčnosť systému (riadenie CCTV prvkov, zasielanie upozornenia emailom alebo pomocou SMS, komplexná správa užívateľských kariet atd.). Z predchádzajúcich vlastností je zrejmé, že sa jedná o dynamický a progresívny systém, ktorý je pripravený riešiť nielen požiadavky pre zabezpečenie a riadenie prístupu do objektu, ale aj riadenia technologických procesov [7].

2.1.2 RON – dochádzkový a prístupový systém

Dochádzkový a prístupový systém bol vytvorený firmou RON Software spol. s. r. o.. Hlavným cieľom firmy je vývoj aplikačného softvéru. Dochádzkový a prístupový systém je elektronický zbernicový systém, ktorého hlavnou funkciou je evidovanie dochádzky, kontrola, ovládanie prístupových častí (dvere, závory, turnikety atd.), sledovanie pohybu zamestnancov. Princíp práce s týmto systémom prebieha tak, že každý zo zamestnancov obdrží identifikačné médium (plastová karta, prívesok ku kľúčom). V programe sa dá nadefinovať 90 rôznych operácií pre prechod terminálom (príchod do práce, odchod k lekárovi, služobná cesta, dovolenka, odchod na iné pracovisko, atd.). Zamestnanec pri vstupe alebo výstupe z objektu zvolí operáciu a priloží identifikačné médium k terminálu a následne mu je umožnený alebo zamietnutý vstup do objektu. Spojenie s terminálom a počítačom je realizované pomocou zberníc RS485, RS232 alebo pomocou TCP/IP. Pri rozšírení systému o modul AMO – Kontrola vstupu je možné monitorovať stav jednotlivých prístupových miest pomocou grafického zobrazovania. Medzi štandardné vlastnosti tohto modulu patrí grafické zobrazenie výkresov objektu a možnosť prepínať medzi nimi (rôzne poschodia), zobrazenie jednotlivých zariadení na výkrese (terminály, sirény), zobrazenie poplachu s vlastným textom (napr. „otvorené dvere v sklade!“), grafické zobrazenie stavu dverí [8].

2.2 Prehľad výrobcov čítačiek a kariet

Medzi najvýznamnejších výrobcov kontaktných a bezkontaktných kariet patria spoločnosti HID, Gemalto, Philips, EM Marin. Dôležitou súčasťou kariet sú čítačky kariet. Čítačka čipových kariet sa správne označuje ako terminál. Jedná sa o zariadenie, ktoré sprostredkúva komunikáciu s čipovou kartou. Čítačka (terminál) môže byť ako samostatné zariadenie, alebo môže byť prepojená napríklad s počítačom. Pre prepojenia čítačky s počítačom sa často využíva iný komunikačný protokol, ako ktorý využíva čítačka pre komunikáciu s kartou.
Test na signalizáciu vytiahnutia karty z čítačky. Ide o jeden z najzákladnejších parametrov čítačky. Napríklad v prípade prihlasovanie do systému Windows pomocou čipovej karty je veľmi dôležité, aby čítačka bezpečne signalizovala, že došlo k vytiahnutiu karty z čítačky. V takom prípade totiž automaticky dôjde k zablokovaniu stanice. Čítačky, ktoré nemajú túto signalizáciu garantovanú, zamestnanec môže pred odchodom svojho pracoviska obísť

jednoduchým trikom: do čítačky pod čipovú kartu vloží vizitku a z čítačky vytiahne len kartu (v čítačke ponechá vizitku). Práve test na signalizáciu vytiahnutia karty odlišuje profesionálne čítačky od domácich čítačiek. Trik s vizitkou možno mnohokrát úspešne vykonávať až po určitom opotrebení čítačky, preto je potrebná garancia výrobcu, že čítačka bola testovaná proti tomuto útoku.
Ovládač čítačky je SW knižnica, pomocou ktorej operačný systém komunikuje s čítačkou [4].

2.2.1 AR6111-MX Čítačka MIFARE kariet

Jedná sa o čítačku kariet od spoločnosti Siemens vhodnú pre rôzne typy prístupových systémov. Je špeciálne navrhnutá pre čítanie sériového čísla karty - CSN (card serial number), kľúčenky s použitím 13,56 MHz technológie, spĺňajúc normy ISO14443-A, ISO14443-B a ISO15693 ako sú Mifare, my-C alebo my-D karty [9].

Obr. 6. Čítačka kariet AR6111-MX.

Vlastnosti čítačky:

- Pracovná frekvencia 13,56 MHz
- Podporované technológie kariet:
  - Mifare Standard 1k a 4k,

- Mifare Ultra-Light,
- Mifare DESfire

- Dosah čítania do 7 cm, v závislosti od vonkajších podmienok, technológie a typov kariet
- Indikácia stavov: 2x LED – diódy (zelená, červená), bzučiak
- Napájanie čítačky - z napájacieho zdroja pre dverový modul
- "Touch and Go" rýchla odozva
- Napájacie napätie 9 V - 15 V DC
- Spotreba el. energie Max. 2,6 W
- Pracovná teplota -25°C do +60°C

2.2.2 Bezkontaktná karta EM4450/4550

Jedná sa o bezkontaktnú kartu od spoločnosti EM MICROELECTRONIC – Marin SA. V karte je CMOS integrovaný obvod určený pre použitie na čítanie a zápis v elektronických RF transpondérov. Čip obsahuje 1 kbit EEPROM pamäte, ktorá môže byť nakonfigurovaná pomocou užívateľov. Pamäť môže byť zabezpečená pomocou 32 bytového hesla pri všetkých čítacích a zapisovacích operácií. Heslo môže byť aktualizované ale nikdy nie čítané. Sériové číslo a identifikačné číslo sú pevne naprogramované a každý čip unikátne. V EM4450/4550 posiela dáta do čítačky kariet ktorá vyhodnocuje zmenu amplitúdy v elektromagnetickom poly, prijaté dáta a povely sú čítané podobnou cestou. Jednoduchými príkazmi je možné zaplniť EEPROM, aktualizovať heslo, prečítať konkrétne pamäťové oblasti a spraviť reset [10].

Základné funkcie EM4450/4550:

- pracovná frekvencia 100 - 150 KHz
- čítacia vzdialenosť 100 - 150 mm
- 1 Kbit programovateľnej pamäte
- 32 bitové sériové číslo
- bezkontaktný čip R/W (read/write)

- pracovná teplota od -40 do +80
- životnosť 10 rokov, 100 000 cyklov
- rýchlosť prenosu dát 2,4 kbits/s
- vyhovuje normám ISO

2.3 Používané formáty kariet

Používané technológie pri kartách:

- Mifare
- DesFire
- Hitag
- Cotag
- HID Prox
- ICODE
- PKI
- EM Marin
- Indala
- iCLASS

2.3.1 Technológia MIFARE

S rozvojom a čoraz častejším používaním bezkontaktných kariet vznikali nové požiadavky na bezpečný a rýchlejší zápis. Jedno z riešení priniesla firma Philips ktorá vyvinula technológiu Mifare, ktorá bola špeciálne navrhnutá ako elektronická peňaženka vo verejnej doprave pre používanie bezkontaktných kariet a zároveň dodržiavala štandard ISO 14443. Postupne sa táto technológia uplatňovala v bankovom sektore, v systémoch súvisiacich so zábavou a voľným časom, v elektronickej kontrole vstupu, dochádzkových systémoch, stravovacích systémoch a u dopravcov kde slúžia ako cestovné lístky. Začiatkom roku 2006 už bolo vo svete viac ako 500 miliónov kariet a 5 miliónov komunikačných zariadení. V súčasnosti bolo predaných viac ako bilión kariet a viac ako 7 miliónov čítačiek. Výrobcom samotného čipu je u vyšších typov kariet z bezpečnostných dôvodov výhradne firma Philips. Technológia Mifare je založená na rovnakých princípoch ako iné bezkontaktné technológie. Umožňuje však aj rýchly a bezpečný zápis dát.

Medzi základné vlastnosti MIFARE technológie patria:

- Pracovná frekvencia 13,56 MHz
- Antikolíznosť, to znamená, že do poľa čítacieho zariadenia môže byť vložených viac transpondérov. čítacie zariadenie potom vie komunikovať s každým transpondérom samostatne
- Vysoká prenosová rýchlosť. Prenosové rýchlosti sa pohybujú v rozmedzí 106kbit/s až po 848 kbit/s
- Bezpečnosť. Pri čítaní a zápise dát sa používa proces autentifikácie. K dispozícii sú dva typy kľúčov, funkcia ktorých je voliteľná
- Viac aplikácií na jednom transpondéri. Počet a veľkosť aplikácií je závisí od typu a veľkosti transpondéra
- Čítacia vzdialenosť do 100 mm (závisí od typu transpondéra a prostredia)

Základne štandardy kariet Mifare:

- MIFARE Ultralight
- MIFARE Standard 1k
- MIFARE Standard 4k
- MIFARE DESFire
- MIFARE PROX
- MIFARE SmartMX

	MIFARE Ultralight	MIFARE Standard 1k	MIFARE Standard 4k	MIFARE DESFire	MIFARE PROX	SmartMX
velikost paměti	64 B	1024 B	4096 B	4096 B	16384 B	73728 B
délka čísla karty	56 bitů	32 bitů	32 bitů	56 bitů	56 bitů	56 bitů
počet zápisů do paměti	1000	100.000	100.000	100.000	100.000	100.000
doba uchování dat	2 roky	10 let	10 let	10 let	10 let	10 let
doba vykonání typické transakce	31,4 ms	164 ms	164 ms	105 ms	105 ms	105 ms
elektronická peněženka	není	32 bitů, plný kredit	32 bitů, plný kredit	plný i omezený kredit	Uživatelsky programovatelná	Uživatelsky programovatelná
metoda šifrování dat	žádná	CRYPT1	CRYPT1	DES, 3DES AES*	DES, 3DES, RSA	DES, 3DES, RSA, ECC
počet aplikací	1	16	40	28		
vhodné použití	jednorázové jízdenky	jednoduchá elektronická peněženka pro drobné platby, časová jízdenka	jednoduchá elektronická peněženka pro drobné platby, časová jízdenka	e-ticketing, věrnostní programy, elektronická peněženka	e-business	e-business

Obr. 7. Prehľad technických parametrov štandardov Mifare.

MIRAFE Ultralight *(64 byte):*

Mifare Ultralight majú odlišnú štruktúru ako štandardy 1k a 4k. Pamäť pozostáva zo 64 bitov ktorá je organizovaná ako 16 blokov zo 4 bitmi na každej z nich. Prvé štyri bloky obsahujú sedem bitov sériového čísla spolu s dvoma kontrolnými bytmi. Ostatné byty sa používajú pre zamknutie kartových funkcií. Zvyšných 12 blokov (48 bitov) môže byť použité na základné čítanie a zapisovanie dát. Napriek odlišnej štruktúre, používajú rovnaký komunikačný protokol. Pri používaní sa nepožaduje žiadny typ overenia a preto neobsahuje žiadne bezpečnostné kľúče. Kvôli malej pamäti, nízkej zriaďovacej cene sa zvyčajne používajú pre nízko nákladové operácie.

MIFARE Štandard 1k (1024 byte):

Mifare štandard 1k pozostáva z 1024 bitov ktoré sú organizované do 16 sektorov, každý z nich pozostáva zo 4 blokov a každý blok je 16 bitov dlhý. Prvý blok v pamäti (Block 0) je iba na čítanie. Obsahuje 4 bytové sériové číslo, kontrolné byty a výrobné údaje. Posledný blok v každom sektore (Block 3, 7, 11, 15...59, 63) obsahuje dva bezpečnostné kódy (KeyA a KeyB) a prístupové bity ktoré definujú ako má byť sektor prijatý. Pre užívateľa je poskytnutých 752 bitov pre voľné zapisovanie dát.

MIFARE Štandard 4k (4096 byte):

Mifare štandard 4k pozostáva z 4096 bitov. Dolných 2048 bitov (sektory 0 – 31)sú organizované rovnakou cestou ako štandard 1k. Avšak horných 2048 bitov sú organizované ako 8 veľkých sektorov a každý obsahuje 16 blokov (sektory 32 – 39). Výhoda oproti predchádzajúcemu štandardu je vo veľkosti využiteľnej pamäte ktorá je 3440 bitov.

MIFARE DESFire:

Mirafe DesFire pozostáva z 4096 bitov. Obsahuje trojitú kryptografickú ochranu. Na tento štandard sa dá uložiť 28 rozdielnych aplikácií a za každú aplikáciu 16 zložiek. Veľkosť každej zložky je definovaná v čase svojho vzniku. Pre vysokú kryptografickú ochranu sa využíva v bezpečnostných systémoch, verejnej doprave kde slúžia ako cestovné lístky a elektronická peňaženka atd.

Rádiofrekvenčné rozhranie:

- bezkontaktný prenos dát, napájanie elektromagnetickým poľom (prevádzka bez batérií)
- prevádzková vzdialenosť až 100 mm (v závislosti od geometrie antény a výkonu vysielača)
- prevádzková frekvencia 13,56 MHz
- prenosová rýchlosť 106 kbit/s, 212 kbit/s alebo 424 kbit/s
- integrita dát: 4 Byte MAC (message authentication code), 16 bit CRC, parita, bitové kódovanie, bitový počet
- antikolizná vlastnosť (možnosť práce viac kariet súčasne v poli antény)
- prenosový protokol podľa ISO 14443-4

Stála pamäť:

- 4 kB stálej (udržujúci si obsah aj bez prítomnosti napájacieho napätia) pamäti, v novej verzii až 8 kB
- obdobie zápisu 2 ms na blok (1 ms mazanie predchádzajúcich dát, 1 ms vlastný zápis)
- doba uchovávania dát 10 rokov
- trvanlivosť 100 000 zapisovaných cyklov

Organizácia stálej pamäte:

- flexibilné súborový systém (u starších typov kariet sa používali pamäťové bloky o pevnej veľkosti)
- 28 úplne nezávislých aplikácií na karte
- 16 súborov pre každú aplikáciu
- 14 kryptografických kľúčov pre každú aplikáciu

Bezpečnosť:

- 7-bajtové jedinečné číslo karty
- 3-kroková autentifikácia
- hardwarovo podporované šifrovacie algoritmy DES/3DES (v novej verzii aj AES)
- zabezpečenia dát 4-bajtovým MAC (Message authentication code)
- autentizácia na aplikačnej úrovni

Výhody proti MIFARE Standard:

- plne multyaplikační systém, každú z aplikácií má jej vlastník plne pod kontrolou
- väčšiu pamäť (daná lepším využitím pamäti)
- výrazne rýchlejšie čítanie a zápis
- predpoklad rozvoja do budúcnosti s kompatibilným protokolom ISO 14443-4
- významne dokonalejšie kryptografické zabezpečenia (3DES)

MIFARE PROX a SmartMX:

Sú vyspelé duálne procesorové karty (s kontaktným aj bezkontaktným rozhraním), ktorých funkcia sa dá programovať v jazyku JAVA. Umožňujú tak naprogramovanie zložitých a veľmi bezpečných aplikácií so širokým spektrom použitia, preto sú vhodné pre systémy ktoré potrebujú vysokú kryptografickú ochranu. Proti ich častejšiemu využívaniu hovorí vysoká výrobná náročnosť, vysoká cena (asi osemnásobne oproti MIFARE Štandard 1K a päťnásobne oproti MIFARE DESFire) a sofistikovanejšie vytváranie softvéru [11].

2.3.2 Technológia EM Marin

Technológia EM Marin od firmy EM MICROELECTRONIC – Marin SA patrí medzi najviac rozšírené v Českej Republike. Od roku 1989 sa firma špecializuje na vývoj, konštrukciu a výrobu aktívnych a pasívnych RFID obvodov. Ide o bezkontaktné karty ktoré pracujú na frekvencií 125 KHz a 13,56 MHz [10].

Typ:	Frekvencia [MHz]:	Čítacia pamäť [bit]:	Zapisovacia pamäť [bit]:	Antikolíznosť:	Rýchlosť prenosu [kbits/s]:
EM4200	125 KHz	128	-	-	2,4
EM4205/4305	125 KHz	64	512	-	2 - 16
EM4450/4550	125 KHz	64	1024	-	2,4
EM4033	13,56	64	-	X	6,69 26,69
EM4133	13,56	64	306	X	6,69 26,69
EM4233	13,56	64	1664	X	6,69 26,69

Tab. 1. Základné štandardy kariet EM Marin.

2.3.3 Technológia FeliCa

FeliCa je technológia vyvinutá pre bezkontaktné karty spoločnosťou Sony. Komunikácia medzi čítačkou kariet a kartou funguje na princípe elektromagnetických vĺn na frekvencii 13,56 MHz. Rýchlosť prenosu je okolo 212 kbit/s. Karta je rozdelená do 8 blokov a každý blok pozostáva zo 16 bajtov. Felica používa štandartné bezpečnostné algoritmy, ktoré zaisťujú vysokú úroveň bezpečnosti. Šifrovací kľúč je automaticky generovaný pri overovaní. Posielanie informácií a zmeny kľúčových informácií sú šifrované do tzv. „balíkov“, aby boli bezpečne vymieňané medzi kartou a čítačkou kariet [12].

Základné vlastnosti technológie FeliCa:

- Pracovná frekvencia 13,56 MHz
- Rýchlosť prenosu 212 kbit/s
- operačný čas do 100 ms
- šifrovanie dát
- anitkolízny systém
- vyhovuje normám ISO

2.3.4 Technológia iCLASS

Technologia iCLASS od firmy HID bola špeciálne navrhnutá tak, aby prístupový systém bol odolnejší, všestrannejší a bezpečnejší. Všetky dátové prenosy medzi kartou a čítačkou sú šifrované pomocou bezpečných algoritmov. Pomocou štandartnej kryptografickej ochrany, iCLASS znižuje riziko ohrozenia dát na karte alebo duplikovania kariet. Pre väčšiu bezpečnosť dát na karte, môžu byť dáta chránené DES alebo 3DES šifrovaním. Bezpečnostné mechanizmy, ako aj vzájomné overovanie a šifrovanie sú účinne kombinované s rýchlim spracovaním a prenosom dát, výsledkom čoho je čas pri transakcií kratší ako 100 ms [13].

Základné vlastnosti technologie iCLASS:

- Pracovná frekvencia 13,56 MHz
- Šifrovanie dát pomocou 64-bitových generovaných kľúčov pre čítanie a zápis
- pracovná teplota od -40 do +70
- čítacia vzdialenosť 50 – 100 mm (záleží od inštalačných podmienok)
- operačný čas do 100 ms
- životnosť 10 rokov, 100 000 cyklov
- bezkontaktný čip R/W (read/write)
- veľkosť pamäte: 2k bit, 16k bit alebo 32k bit
- pre 2k bit iCLASS technológiu: pozostáva z 256 bajtov ktoré je možné rozdeliť na dve aplikácie
- pre 16k bit iCLASS technológiu: pozostáva z 2 kbajtov ktoré je možné rozdeliť na 2 až 16 aplikácií
- pre 32k bit iCLASS technológiu: pozostáva z 2k bajtov ktoré je možné rozdeliť na 2 až 16 aplikácií plus 16k bajtov voľne konfigurovatelné pamäte
- vyhovuje normám ISO

2.3.5 Technológia Indala

Technológia Indala, vytvorená firmou HID, poskytuje pridanú úroveň prístupového zabezpečenia prostredníctvom overovania na čítačke kariet. Toto dodatočné overenie je možné zabezpečiť dvomi cestami:

- všetky dáta na karte sú chránené šifrovaním pred programovaním karty. Bez dekódovania nie je možné zistiť údaje na karte
- kartu a čítačku je možné naprogramovať pre každú stránku, potom bude karta chránená pred neoprávneným použitím na inom zariadení [14].

Základné vlastnosti technológie Indala:

- Pracovná frekvencia 125 KHz
- 172 bitov definovaných užívateľom (číslo zamestnanca, číslo oddelenia, atd.)
- overenie heslom
- pracovná teplota od 0 do +50
- čítacia vzdialenosť 120 mm
- vyhovuje normám ISO

II. PRAKTICKÁ ČÁST

3 PRIPOJENIE KARTOVÝCH ČÍTAČIEK DO SYSTÉMU WINPACK

Táto kapitola pojednává o prístupovom systéme WinPack.

3.1 WinPack, základné informácie

WinPack je moderný riadiaci softvér navrhnutý pre prácu v prostredí Windows 2000 a novšie verzie, Windows NT 4.0 a Windows 98 (iba užívateľské rozhranie) tak, aby v maximálnej miere využíval rýchlosti, spoľahlivosti a flexibity sieťových systémov. Obsahuje celú radu funkcií určených pre rozsiahle inštalácie. Prostredie je možné nakonfigurovať tak, aby v maximálnej možnej miere vyhovovalo personálu pri monitorovaní poplachov, vydávania kariet a prevádzania ďalších bežných činností. WinPack podporuje funkcie sledovania a prehľadu pre zobrazovanie miest pohybu osôb zo zabezpečených alebo bezpečných dôvodov. Umožňuje pre ostrahu objektu definovať obchôdzky určené čítačkami a vstupmi, a to ako v predpísanom tak i v náhodnom poradí. Ďalej ponúka kontrolu priestorov pomocou CCTV s prenosom obrazu v reálnom čase, podporuje rozhranie Burle, Dedicated Micros, Geutebruck, Javelin, JavQuest, NCI CCTV, Panasonic, Pelco a Vicon.

3.1.1 Správa databáz

WinPack umožňuje definovať časové zóny, komunikačnej slučky, panely, karty, držiteľov kariet a iné informácie nevyhnutné pre plnohodnotnú správu systému. Používa ako databázový stroj Microsoft SQL alebo MSDE. Podporuje filtrovanie poplachov podľa práve prihláseného operátora. Môže si tak určiť, aké poplachy môže konkrétne operátor monitorovať. Navyše je možné pre každú osobu z okruhu operátorov veľmi detailne definovať prvky, ktoré bude môcť ovládať (až na úroveň jednotlivých čítačiek, vstupov alebo poznámkových polí), čo vytvára takmer ideálny kompromis medzi ochranou citlivých údajov a užívateľskou prívetivosťou programu. WinPack pracuje s databázami, ktoré sa môžu jednoducho a prehľadne editovať, prehľadávať alebo triediť. Z obsahu databázy alebo zaznamenaných udalostí je možné generovať širokú škálu správ a ty následne prezerať, tlačiť alebo exportovať do externých súborov.

3.1.2 Správa kontroly vstupu

WinPack používa tzv. mapy pre monitorovanie a ovládanie bežných funkcií kontroly vstupu. Mapa zobrazuje v grafickej podobe jednotlivé zariadenia - dvere, panely, vstupy, výstupy alebo prvky CCTV systému. Grafická podoba najčastejšie zodpovedá pôdorysu budovy, štruktúre objektu alebo geografickému usporiadanie územia. Vďaka zobrazeniu systémových zariadení (abstraktné zariadenia - ADV) má užívateľ prehľad aj o stave systémového hardvéru a možnosť tieto zariadenia diaľkovo ovládať. Pomocou ADV v mape tak možno napríklad zamknúť alebo odomknúť dvere, pohľad z CCTV kamery môže používateľ prepnúť z jedného monitora na iný atď. Oblasti riadenia možno definovať pridaním zariadenia do mapy konania, ktorá tiež umožňuje zariadení diaľkovo ovládať. Mapa konania má, na rozdiel od vyššie uvedených máp, formu adresátového stromu, v ktorom sú jednotlivé zariadenia členené podľa typu, umiestnenie alebo iného užívateľom preferovaného kritériá. Okná udalostí a poplachov zobrazujú poplachy spolu s ostatnými systémovými informáciami vo forme zoznamu. Poplachy možno potvrdiť a vymazať z mapy podlaží, tak aj priamo z okna poplachov.

3.1.3 Okná máp a riadiace funkcie

Okná máp sú nakonfigurované užívateľom. Poskytujú okrem monitorovacích, tak aj riadiace funkcie pre panely, dvere, poplachy, vstupy, výstupy a iné zariadenia systému. Naraz možno prezerať aj viac máp – kliknutím myši sa otvárajú ďalšie. Natáčanie alebo prepínanie CCTV kamier možno tiež plne ovládať z okna mapy. Mapa riadenia poskytuje užívateľovi ďalší spôsob ovládania zariadenia. Užívateľ mapu definuje pridávaním zariadení do vetviacej sa stromovej štruktúry. Aj z tejto stromovej štruktúry možno monitorovať stav zariadenia a ovládať ju. Iné okná na obrazovke slúžia napríklad pre monitorovanie priestorov v reálnom čase pomocou CCTV kamier (on-line monitoring) alebo automatické zobrazenie karty s fotografiou a informáciami o držiteľovi, ktorý práve priložil svoju kartu k ľubovoľnej čítačke.

3.1.4 Abstraktné zariadenia

Abstraktné zariadenia (ADV) sú akýmsi zástupcom fyzického zariadenia (napr. komunikačného servera, riadiaceho panela, dverí alebo CCTV prepínača). Svojim vzhľadom na obrazovke sa podobá ikone zariadenia a i funkčne je ADV s konkrétnym

zariadením v systéme kontroly vstupu späté. Primárne slúži na zobrazovanie aktuálneho stavu spojeného prvku a na jeho ovládanie. ADV sú umiestnené na mapové pozadia a spolu s ním tak vytvárajú konkrétne mapu, ktorá je hlavným prvkom užívateľského rozhrania celého systému. Abstraktné zariadenia majú v celkovej koncepcii systému dôležitú úlohu - poskytujú užívateľské rozhranie pre ovládanie najrôznejších prvkov hardvéru bez toho, aby po užívateľovi vyžadovala detailnú znalosť ich konfigurácie. Napríklad po umiestnení do mapy umožňuje, ADV dverí, užívateľovi tieto dvere zamykať, odomykať, premostiť dverný kontakt alebo toto premostenie zrušiť, príp. zopnúť dverný zámok na nastavenú dobu. Z pohľadu užívateľa je pritom ľahostajné, či je ovládanie dverí realizované panelom N-1000 (PW-2000) alebo iným kontrolórom. Pri práci s mapou signalizujú ADV stav príslušného zariadenia farbou a blikaním. S ADV môže byť prehraný aj zvukový súbor - potom je obsluha na zmenu stavu upozornená aj akusticky. Každé ADV má riadiace menu, ktoré používateľovi dovoľuje realizovať funkcie dostupné u toho ktorého zariadenia. Kliknutím pravým tlačidlom myši na ADV sa toto menu otvorí. V niektorých prípadoch možno využiť aj funkciu preťahovania objektov (drag & drop) - napríklad objekt prislúchajúce kamere možno myšou presunúť na objekt monitora, čím sa vykoná prepnutie monitora na túto kameru. Farby, blikanie a ďalšie vlastnosti abstraktných zariadení možno editovať, meniť alebo otáčať pomocou utility pre vytváranie mapy podlaží.

3.1.5 Dátové stromy

WinPack používa pre organizáciu a zobrazenie niektorých databázových informácií formu grafických stromov. Tieto stromy uľahčujú organizáciu údajov do logických alebo geografických skupín. Každý zo stromov sa vytvára počas programovania systému, takže je už od základu navrhnutý tak, aby vyhovoval požiadavkám konkrétneho systému pre kontrolu vstupu. S výnimkou mapy zariadenia definujú stromy len hierarchiu zariadenia, nie zariadenia samotné. Napríklad prístupové úroveň je definovaný ako zoznam čítačiek bez ohľadu na ich fyzické prepojenie. Čítačky sa však zobrazujú nie v klasickom zozname, ale vo forme dátového stromu. Vetva na najvyššej úrovni môže predstavovať celý komplex budovy. Z nej sa potom vetvia jednotlivé miestnosti - kancelárie vedenia, účtovné oddelenie, dielňa, expedície atď. Odpovedajúce vchody sú potom pridávané do jednotlivých vetiev. Vchody, ktoré sú v určitej prístupovej úrovni dostupné, sa potom zobrazujú zelenou farbou. Letmý pohľad na strom tak rýchlo prezradí, ktoré vchody sa v

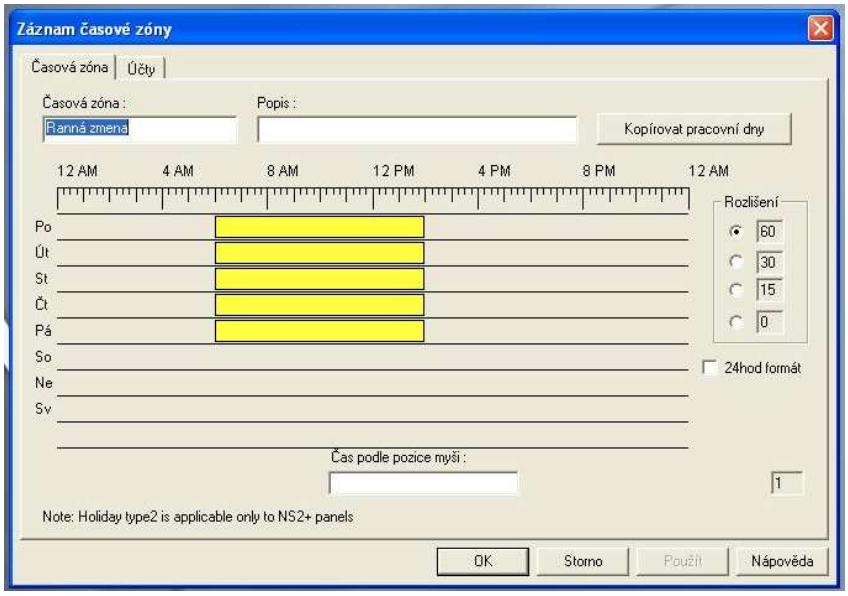
tejto prístupovej úrovni nachádzajú a ktoré z nich sú pre konkrétnu úroveň povolené. Mapa zariadenia sa zobrazuje aj v stromovej hierarchii, ale na rozdiel od iných stromovitých štruktúr u nej dochádza okamihom pridania zariadenia do mapy k jeho definícii. Okrem toho zobrazuje táto štruktúra zariadenia tak, ako sú fyzicky prepojené - používateľ si teda jeho podobu nemôže upravovať úplne ľubovoľne.

3.2 Nastavenie časových zón, užívateľov kariet, kariet, oprávnení, mapy podlaží

Prvotnou činnosťou pri nastavovaní systému kontroly vstupu by malo byť plánovanie, ktoré by malo predchádzať konfigurácií a programovaniu.

3.2.1 Časové zóny

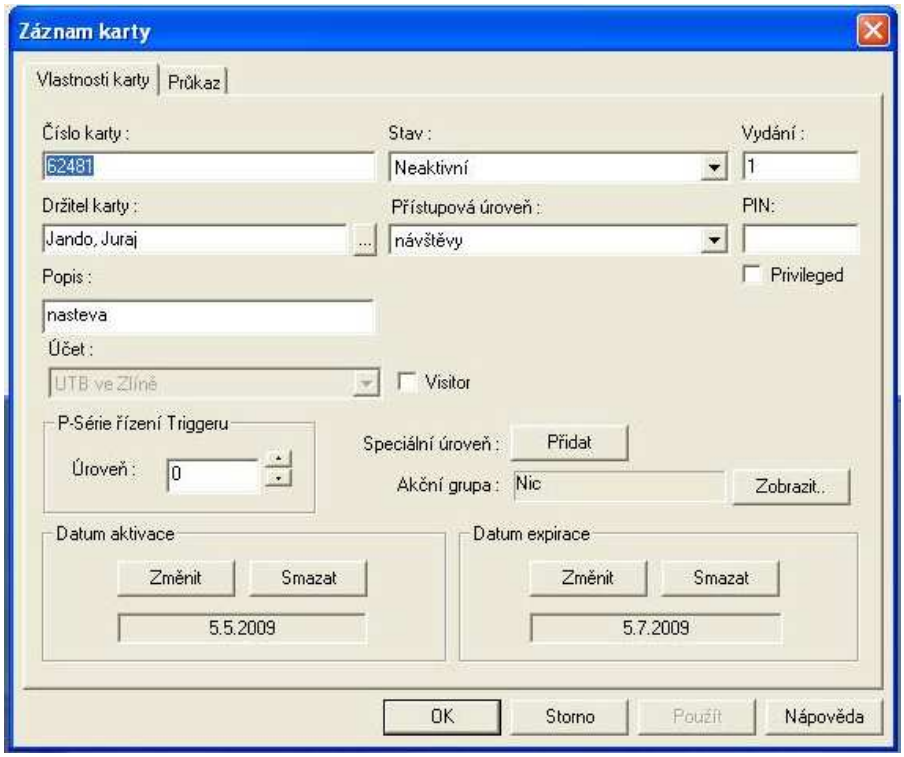
Jedná sa o časové intervaly, ktoré určujú, kedy a aké akcie sa budú odohrávať. Niektoré akcie je možné pre niektoré časové zóny povoliť alebo zakázať. Najčastejšie sa časová zóna využíva na obmedzenie prístupu a pohybu po objekte zamestnancami. V prístupovom systéme sa časová zóna myslí rozsah hodín a dní ku ktorému je priradená karta alebo určitý počet kariet. Následne sa časová zóna konfiguruje na panely, ktoré majú časovú zónu používať. Štandartne sa vytvára jedná časová zóna s neobmedzenou časovou platnosťou. Nastavuje sa na 24 hodín denne a na 7 dní v týždni vrátane sviatkov. Táto zóna sa prideľuje ku karte ktorých vlastník je správca alebo majiteľ a nastavuje sa na všetky panely. Ďalej sa definujú časové zóny podľa potrieb (ranná zmena viz obr. 8., odpoludňajšia, nočná, upratovanie, návšteva, atď.).



Obr. 8. Nastavenie rannej časovej zóny.

3.2.2 Užívatelia kariet, karty

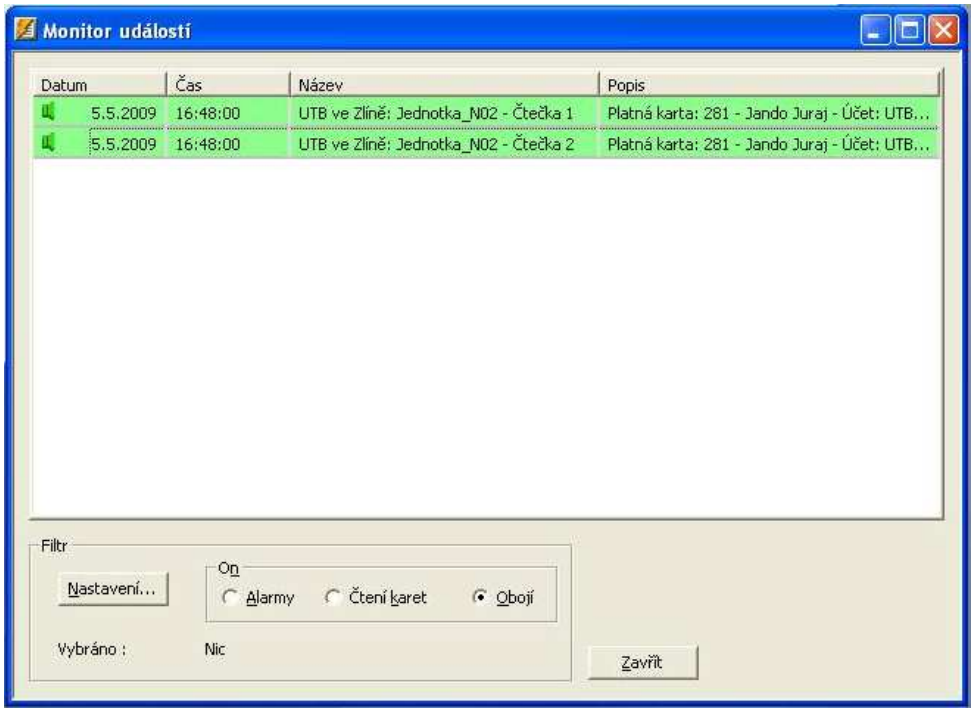
Jedná sa o osoby, ktorým sú karty vydávané a ktorý ich používajú. Údaje o užívateľoch kariet musia obsahovať minimálne meno a priezvisko ktoré sa nachádzajú v databázach. Ďalej je možné pridať osobné, pracovné a biometrické informácie. Keď je vytvorený užívateľ karty je možné k nemu pridať kartu a záznam o karte viz obr. 9. Karta je definovaná číslom karty, prístupovú úrovňou a statusom karty (aktívna, neaktívna, stratená, ukradnutá alebo sledovacia). Ďalej je možné nastaviť kartám dobu platnosti, priradiť PIN.



Obr. 9. Nastavenie karty pre návštevy s obmedzenou dobou platnosti.

3.2.3 Oprávnenia

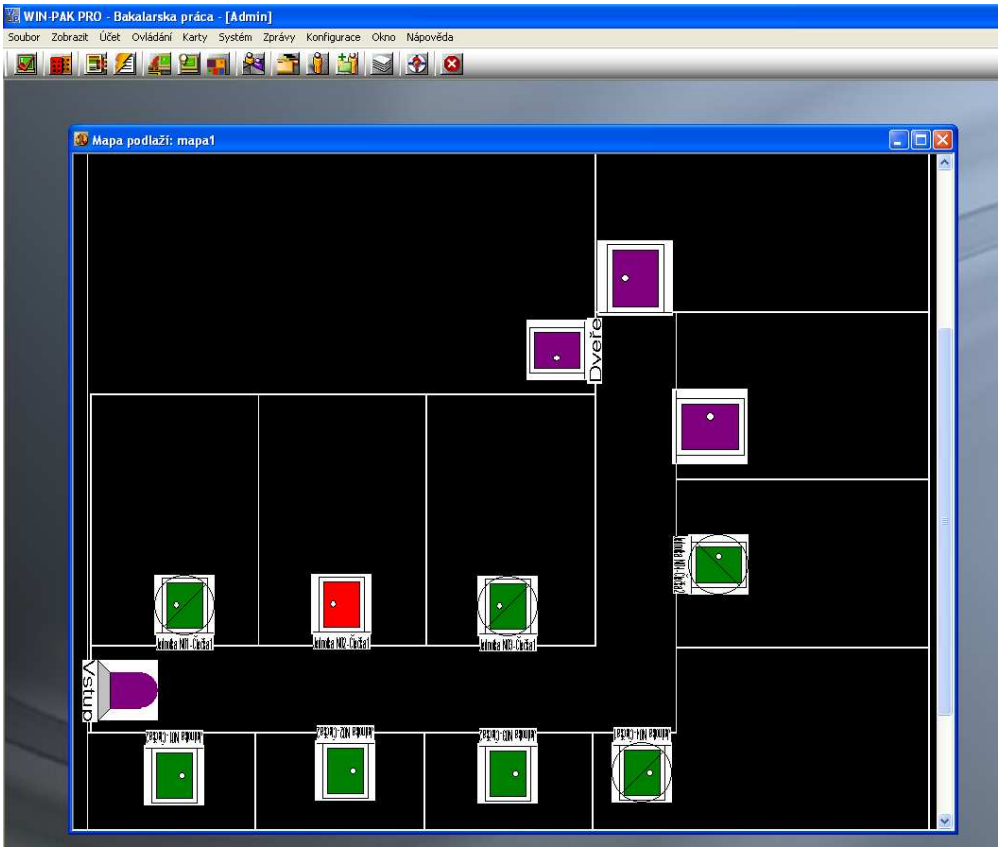
Najjednoduchšie nastavenie oprávnenia je nastavenie prístupových úrovní na karte alebo na skupine kariet, tie určujú kedy a kde bude karta vyhodnotená ako platná. Prístupová úroveň je tvorená časovými zónami ktoré sú pridelené čítačkám kariet. Prístupové úrovne definujú časové úseky podľa ktorých čítačky kariet povolia alebo odmietnu prístup karte a následne odblokovanie alebo zablokovanie dverí. Výhoda prístupových úrovní spočíva v tom, že sa nemusia nastavovať paneli pre jednotlivé karty ktorým bude prístup povolený alebo odmietnutý.



Obr. 10. Povolenie prístupu karty.

3.2.4 Mapy podlažia

Mapy podlažia slúžia na jednoduchú manipuláciu a prehľadnú prácu so systémom. Pozadie môže tvoriť pôdorys podlaží budovy alebo oblasti, kde sú zariadenia fyzicky umiestnené. Súbory s pozadím musia byť vytvárané ako metasoubory (.wmf). Okná máp je možné prispôsobiť špecifickým požiadavkám konkrétneho systému kontroly vstupu. Naraz môže byť otvorené a prezeraných aj niekoľko takýchto okien. Mapy môžu obsahovať odkazy na iné mapy pre iný alebo podrobnejší pohľad. V mape sa dajú po pridaní zariadení s ADV vlastnosťami prvkov povoľovať a blokovať prístupy, ovládať CCTV kamery, zobrazovať a vymazávať poplachy, atď. Zmenu udalosti prvky signalizujú zmenou farby a blikaním viz obr. 11.



Obr. 11. Zobrazenie poplachu na vstupe, zelená farba signalizuje pohotovostný stav, červená poplach, fialová nepriradené ADV

3.3 Programovanie panelov

Programovanie panelov predstavuje v prvom rade zozbieranie nezbytných informácií o hardwarovej konfigurácií a naplánovanie si akcií ktorý bude daný panel vykonávať. Hardwarová konfigurácia sa týka formátov kariet, typov použitých čítačiek alebo klávesníc a nastavenie poplachových vstupov a výstupov.

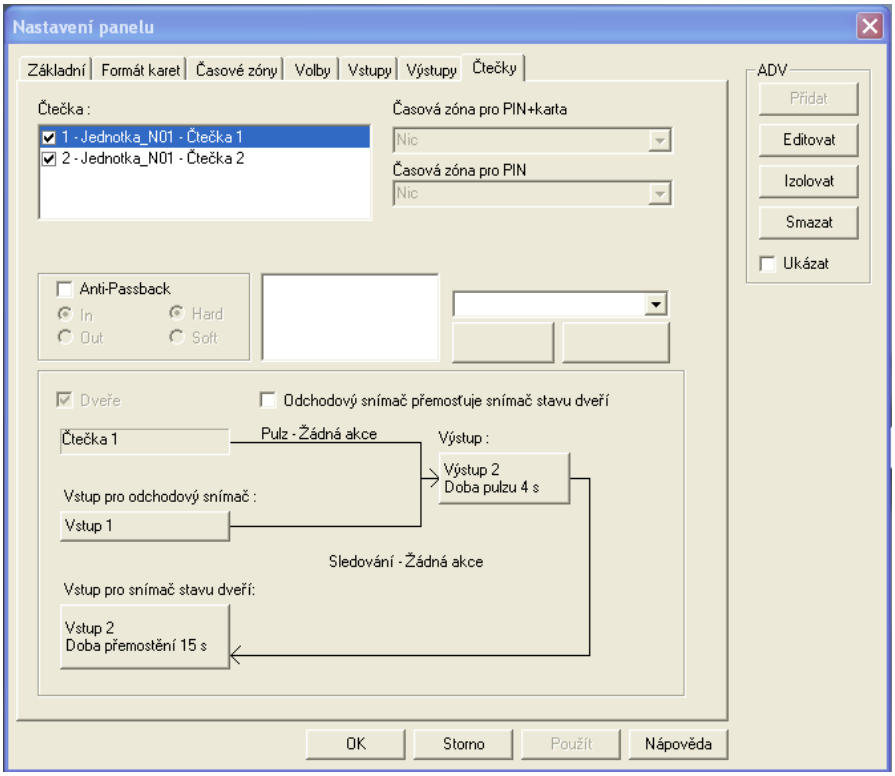
3.3.1 Pridávanie panelov

Panely sa pripájajú v mape zariadení na komunikačný server do komunikačných smyčiek. Vo WinPacku je možné pridať dva druhy panelov a to z rady PW-2000 alebo panely série P.

3.3.2 Konfigurácia panelov

Konfigurácia panelov zahrňuje základné informácie o jeho type, formáte kariet s ktorým panel pracuje, časových zónach, grupy sviatkov, čítačiek (viz obr. 12.), nastavenie

poplachových vstupov a výstupov, klávesníc, anti-passback, PIN, priebežné čítanie kariet, site kódy.



Obr. 12. Nastavenie panelu – čítačky

ZÁVĚR

Identifikační karty se staly součástí našeho každodenního života. Nahrazují klasické klíče, lístky v dopravě, peněženky, doklady atd.. Jsou zaváděné všude tam kde je potřeba zrychlit pohyb osob a je při tom důležitý určitý stupeň bezpečnosti. V budoucnu budou mít velký význam čipové karty (zejména v Evropské unii - největší počet čipových karet a čteček čipových karet ve světě), které mají větší kryptografickou ochranu jako ostatní karty. V současnosti nahrazují magnetické karty které slouží jako bankomatové a platební karty. Velkou zásluhu mají na tom německý vědci Jürgen Dethloff a jeho kolega Helmut Grötrupp, který jsou vynálezci čipových karet. Postupně budou čipový karty pronikat i do jiných systémů pro jejich klesající cenu, lepší bezpečnost a dostupnost.

V mé práci jsem se zaměřil na identifikační karty které se nejčastěji vyskytují v elektronické kontrole vstupu a docházkových systémech. V práci jsem popsal jejich složení, princip činnosti, jak komunikují s čtečkou karet, formáty karet a jejich nejčastějších výrobců. Dále jsem se zaměřil na přístupové systémy a čtečky karet. V přístupových systémech se nejčastěji vyskytuje wiegand formát. Z tohoto důvodu výrobci čteček karet pro přístupové systémy obsahují wiegand výstupy s wiegand protokoly. V praktické části jsem se zaměřil na přístupový systém WinPack. V tomto systému jsem prakticky odzkoušel komunikaci karty se čtečkou karet, přidal jsem karty do systému, které byly podmíněné přidáním uživatele karet. Dále jsem nastavil abstraktní zařízení, přidal panely na kterých jsem nastavil časové zóny a oprávnění. Nakonec jsem si vytvořil mapu podlaží, ke které jsem přiřadil jednotlivé panely s abstraktními zařízeními a odzkoušel jsem chod celého systému při použití identifikační karty.

ZÁVĚR V ANGLIČTINĚ

Identity cards have become part of our daily lives. They replace traditional keys, tickets for transport, wallet, documents, etc. They are implemented everywhere where there is a need to accelerate the movement of people and is important in that some degree of safety. In the future, will have great importance to the chip card (especially in the European Union - the largest number of smart cards and smart card readers in the world), with more cryptographic protection as other cards. At present, they replaced by a magnetic card, which serves as an ATM and credit cards. A credit of it, have Germans scientists Jürgen Dethloff and his colleague Helmut Grötrupp who are inventors of smart cards. Gradually, smart cards will penetrate into other systems for their declining cost, improved safety and availability.

In my bachelor thesis I focused on the identification cards that are most commonly found in access control systems and attendance systems. At theses I have described their composition, principles of operation, how to communicate with card reader, card of format and the most common manufacturers. I also focused on access control systems and card readers. The access systems are the most frequently used wiegand format. For this reason, manufacturers of card readers for access control systems include wiegand outputs with wiegand protocol. In practical part, I focused on the access system WinPack. In this system, I practically tested communication card with card reader, I have added cards, which were subject to the addition of users cards. I also set up an abstract device, added to the panel; I set the time zone and permission. Finally, I have created a floor map, which was assigned to the panels with abstract devices and I tested access control system with using an identification card.

SEZNAM POUŽITÉ LITERATURY

[1] .CCUMINN.. *Www.soom.cz : Bezpečnost magnetických karet* [online]. 2003-2009 [cit. 2009-10-02]. Dostupný z WWW: <http://www.soom.cz/index.php?name=articles/show&aid=427>.

[2] *Pandatron.cz, elektrotechnický magazín : Karty s magnetickým pruhem* [online]. 2000-2009 [cit. 2009-02-15]. Dostupný z WWW: <http://pandatron.cz/?535&karty_s_magnetickym_pruhem>. ISSN 1803-6007>.

[3] IVO, Rosol. *OKsystem : Technologie čipových karet* [online]. 2008 [cit. 2009-03-10]. Dostupný z WWW: <http://www.oksystem.cz/o-nas/servis-pro-novinare/napsali-o-nas/2005/07-business-world>.

[4] Siemens. *Siemens IT Solutions and Services : Multifunkční čipové karty* [online]. 2007 [cit. 2009-03-15]. Dostupný z WWW: <http://www.itsolutions.siemens.cz/web/topics/main_topic7>.

[5] Popis vlastností čipu Micro RWD [online]. 2005 [cit. 2009-03-22]. Dostupný z WWW <http://www.ibtechnology.co.uk/PDF/magswipe_dec.pdf>.

[6] WinPack – uživatelský manuál. Honeywell Access Systems. ADI Olympo. Brno. [cit. 2009-04-02]. 425 s.

[7] *EUROSAT CS* [online]. 2006 [cit. 2009-04-05]. Dostupný z WWW: <http:// www.eurosat.cz/UserFiles/Marketing/Concept/concept2006_katalog_web.pdf>.

[8] *RON SOFTWARE* [online]. c2003-2007 [cit. 2009-04-09]. Dostupný z WWW: <http://www.ron.cz/_cze/cze_dochazka_02princip.php>.

[9] *Siemens Building Technologies* [online]. c2006 [cit. 2009-04-20]. Dostupný z WWW: <http://www.cee.siemens.com/web/slovakia/sk/corporate/portal/produkty/divizie/technologie/ponuka/systemy/Documents/AR6111-MX-sk_2000001547567.pdf>.

[10] EM Microelectronic-Marin SA,. *1 KBit Read/Write Contactless Identification Device* [online]. c2003 [cit. 2009-04-19]. Dostupný z WWW: <http://www.emmicroelectronic.com/webfiles/Product/RFID/DS/EM4450_DS.pdf>.

[11] *Micro RWD MF (Mifare) "24/32 Wiegand" Output Version* [online]. 2007 [cit. 2009-04-21]. Dostupný z WWW: <http://www.ibtechnology.co.uk/PDF/MFprot_wdax.pdf>.

[12] Sony Corporation. *The FeliCa System* [online]. c2009 [cit. 2009-04-19]. Dostupný z WWW: <http://www.sony.net/Products/felica/abt/dvs.html>.

[13] HID Global. *ICLASS Card* [online]. c2008 [cit. 2009-04-20]. Dostupný z WWW: <http://www.hidglobal.com/documents/iclass_card_ds_en.pdf>.

[14] HID Global. *Indala FlexISO Imageable Card* [online]. 2007 [cit. 2009-04-21]. Dostupný z WWW: <http://www.hidglobal.com/documents/indala_flexiso_card_ds_en .pdf>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ID card	Identification card
IBM	International Business Machines Corporation
ISO	International Organization for Standardization
IATA	International Air Transportation Association
ABA	American Bankers Association
PIN	Personal Identification Number
Oe	Oersted
LiCo	Low Coercivity
HiCo	High Coercivity
SIM	Subscriber Information Module
ROM	Read only memory
PC	Personal computer
USB	Universal Serial Bus
MHz	Mega Hertz
KHz	Kilo Hertz
RSA	Rivest -Shamir - Adleman
ECC	Elliptic curve cryptography
EMV	Standard for interoperation chip cards
CCTV	Closed circuit TV
I&HAS	Intruder and Hold-up Alarm System
PCO	Pult centralizované ochrany
GSM	Global System for Mobile communications
LAN	Local Area Network
SMS	Short Message Service

TCP/IP	Transmission Control Protocol / Internet Protocol
SW	Software
CSN	Card serial number
LED	Light Emitting Diode
CMOS	Complementary metal–oxide–semiconductor
EEPROM	Electrically Erasable PROM
R/W	READ/WRITE
MAC	Message authentication code
DES/3DES	Data Encryption Standard/ Triple Data Encryption Standard
AES	Advanced Encryption Standard
RFID	Radio Frequency Identification
SQL	Structured Query Language
MSDE	Microsoft SQL Server Desktop Engine
ADV	Abstrakční zařízení
wmf	Windows Metafile

SEZNAM OBRÁZKŮ

SEZNAM TABULEK