Systémy kontroly vstupu pro komerční objekty

Access control systems for commercial objects

Lukáš Sucháček

Bakalářská práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2009/2010

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Lukáš SUCHÁČEK**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Systémy kontroly vstupu pro komerční objekty**

Zásady pro vypracování:

1. **Popsat systémy kontroly vstupu a jejich funkci.**
2. **Stanovit požadavky na systémy podle norem.**
3. **Popsat úkoly komplexní ochrany před vloupáním a požárem.**
4. **Zvolit komerční objekt a prakticky ho systémem kontroly vstupu zabezpečit.**

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **Laucký, V., Technologie komerční bezpečnosti I., Zlín: vyd. Univerzita Tomáše Bati ve Zlíně, 2003. ISBN 80-7318-119-3.**
2. **Laucký, V., Technologie komerční bezpečnosti II., Zlín: vyd. Univerzita Tomáše Bati ve Zlíně, 2004. ISBN 80-7318-231-9.**
3. **Křeček a kol., Stanislav. Příručka zabezpečovací techniky. Marie Bubníková; Dagmar Kubešová. 3 vydání Blatná; Cricetus, 2006. 313 s. ISBN 80-902938-4.**
4. **Kindl, Jiří: Projektování bezpečnostních systémů I. 1. vyd. UTB Zlín 2004.ISBN 80-7318-165-7.**
5. **Laucký, V., Řízení technologických procesů v průmyslu komerční bezpečnosti. 1. vyd. Zlín :Univerzita Tomáše Bati ve Zlíně, 2005. 101 s. ISBN 80-7318-329-3.**

Vedoucí bakalářské práce: **JUDr. Vladimír Laucký**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **19. února 2010**

Termín odevzdání bakalářské práce: **19. května 2010**

Ve Zlíně dne 19. února 2010

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

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

Tato bakalářská práce probírá základní teorii o používaných systémech kontroly vstupů. V práci je podrobně rozebrána struktura těchto systémů, požadavky, úkoly, používané komponenty a komunikace mezi jednotlivými prvky. Zvyšování efektivnosti systému se realizuje integrací s jinými systémy a mechanickými prostředky. Dále jsou popsány identifikační metody a prostředky identifikace osob, v neposlední řadě pak biometrická identifikace. Na závěr je proveden návrh zabezpečení konkrétního objektu.

Klíčová slova: Systémy kontroly vstupu, přístupový systém, identifikace, čtečka, kontrolér

ABSTRACT

This thesis discusses the basic theory used in the access control system. The work is detailed structure of these systems, requirements, tasks, components used and the communication between components. Increasing the effectiveness of the scheme is implemented by integrating with other systems and mechanical means. The following describes the identification method and means of personal identification, not least the biometric identification. In conclusion, then made a proposal security of a particular object

Keywords: Access control systems, identification, card reader, controller

Poděkování:

Touto cestou bych rád poděkoval vedoucímu mé bakalářské práce JUDr. Vladimíru Lauckému za připomínky, cenné rady, poskytnuté materiály a vstřícný přístup nejen při zpracovávání této 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.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….……

podpis diplomanta

OBSAH

ÚVOD

Od nepaměti se snaží majitel svého pozemku nebo objektu zabezpečit vstup tak, aby se dovnitř nedostala osoba, která tam nemá co dělat. Až do druhé poloviny 20. století to bylo řešeno pomocí dveří a vrat, ale s lidským faktorem – strážným, který rozhodoval o vpuštění nebo nevpuštění osoby do prostoru. Snaha odbourat lidský faktor v této oblasti vedla k zavádění systémů kontroly vstupů s návazností na automatickou bariéru, která propustí pouze identifikovanou osobu.

Existuje mnoho způsobů jak identifikovat člověka, respektive prokázat jeho oprávnění k přístupu do určitého prostoru. V dnešní době se využívá různých způsobů jako: kontrola průkazu totožnosti, ověření pomocí předmětu (karty, čipu atd.), ověření pomocí informace uložené v paměti (hesla), a v neposlední řadě ověření pomocí biometrických údajů. Poslední zmiňovaná metoda se v dnešní době začala hodně rozšiřovat, jedná se v podstatě o nejspolehlivější identifikační metody, spočívá totiž v ověřovaní fyziologických vlastností, které jsou pro každého člověka jedinečné a nosičem informace je tedy samo lidské tělo. Biometrické systémy se v dnešní době také zabudovávají i do počítačů nebo telefonů.

Využití systémů kontroly vstupů je poměrně široké a aplikací stále přibývá. Setkat se s nimi můžeme všude tam, kde je nutné zabezpečit vstup proti nepovolaným osobám, ochránit osobní data, v docházkových systémech, v lékařství při identifikaci pacienta, v neposlední řadě pak ochrana know – how. Důležité je nastavení přístupových práv, kterými se řídí pohyb osob v objektu např. časovým omezením vstupu do prostoru či úplného zamezení přístupu. Celý pohyb osob se pak ukládá do systému, ze kterého se dá jednoduše zjistit kdo se kdy a kde pohyboval v objektu zabezpečeném tímto systémem.

Cílem mé práce je popsat funkci těchto systémů, požadavky a v neposlední řadě možnosti které se nabízí. V praktické části pak budu aplikovat systém kontroly vstupu na konkrétní objekt.

I. TEORETICKÁ ČÁST

1 FORMY ČINNOSTI V PRŮMYSLU KOMERČNÍ BEZPEČNOSTI

Formy soukromé bezpečnosti v průmyslu komerční bezpečnosti dělíme z hlediska použitých metod ochrany na:

a) Ochrana osob

b) Ochrana majetku

Ochrana osob, zejména pak ochrana života a zdraví má vždy v činnosti průmyslu komerční bezpečnosti přednost před ochranou majetku.

Formy ochrany osob a majetku dělíme na:

a) Fyzickou ochranu

b) Režimová opatření

c) Technické prostředky ochrany objektu

1.1 Fyzická ochrana

Jedná se o nejčastější formu ochrany osob a majetku. Jedná se o ochranu prováděnou živou silou (vrátní, hlídači, strážní, hlídací služba, policisté). Na její úrovni závisí výsledná činnost všech ostatních druhů ochrany. Nejjednodušší a nejefektivnější bývá pokud je prováděna profesionálně. Její největší výhodou je že lze v případě potřeby provést okamžitý zásah na ochranu osob či majetku a odvrátit případné hrozící nebezpečí chráněnému zájmu nebo alespoň snížit riziko škody na minimum. [2, 6]

1.2 Režimová opatření

Režimová opatření představují stanovený soubor procedur, které zahrnují režim vstupu a výstupu osob, vjezdu a výjezdu dopravních prostředků, režim pohybu osob, dopravních prostředků a chráněných informací v objektu a jeho jednotlivých částech v pracovní a mimopracovní době, režim manipulace s klíči, identifikačními prostředky a médii, které se používají pro systémy zabezpečení vstupů, režim manipulace s technickými prostředky a jejich používání.

Režimová opatření jsou zpravidla popsána v provozním řádu objektu, zavazujícím všechny osoby, které jsou oprávněny vstupovat do objektu.

Vedle jiných náležitostí obsahují režimová opatření i seznamy osob oprávněných vstupovat do chráněných prostorů objektu, seznam dopravních prostředků oprávněných vjíždět do objektu, způsob kontroly prokazování oprávněnosti k vstupu nebo vjezdu do objektu, pokyny, nařízení a příkazy k určitému chování a jednání v chráněných objektech, často vydaných písemně, většinou formou tabulek, nápisů na budovách, či stěnách uvnitř objektu. [8]

1.3 Technické prostředky ochrany objektu

Slouží ke zvýšení účinnosti fyzické ochrany objektů, ale sama o sobě, bez přímé vazby na fyzickou ochranu, nemůže být efektivní. Tvoří jen dočasnou překážku bránící nepovolaným osobám vniknout do objektu. Při použití pultu centralizované ochrany obvykle stačí zásahová jednotka o určitém počtu zaměstnanců (podle velikosti objektu) , která je připravená rychle reagovat na případný poplachový signál. Při tomto způsobu střežení objektu stačí několik pracovníků střežit více objektů mnohem efektivněji, než dokáže fyzická ostraha přímo v objektech.

Technická ochrana objektů se dělí na:

Obvodovou ochranu – signalizuje narušení obvodu objektu. Obvodem objektu obvykle rozumíme jeho katastrální hranici, obvykle tvořenou přírodními nebo umělými bariérami (potoky, zdi, ploty…).

Plášťovou ochranu – signalizuje narušení pláště objektu. Plášťová ochrana je zpravidla zajišťovaná elektrickou zabezpečovací signalizací (dále EZS).

Prostorovou ochranu – signalizuje změny v chráněném prostoru.

Předmětová ochrana – signalizuje napadení nebo neoprávněnou manipulaci s chráněnými předměty.

Technická ochrana využívá k zabezpečení objektů prvků:

- mechanických
- elektronických (elektrických)
- smíšených a speciálních

- **Mechanická ochrana**

Je ochrana majetku a osob za využití mechanických zábranných systémů, které zamezují nebo znesnadňují proniknutí do chráněného objektu, případně ke chráněné osobě.

Mezi mechanické prvky zabezpečení patří:

- mechanické zábranné systémy obvodové ochrany (klasické a bezpečnostní oplocení, vrcholové zábrany, brány, branky, závory, turnikety atd.),
- mechanické zábranné systémy plášťové ochrany (okna, mříže, rolety, žaluzie, bezpečnostní skla, bezpečnostní dveře, přídavné zámky atd.),
- mechanické zábranné systémy předmětové ochrany (komorové trezory, úschovné objekty, ohnivzdorné skříně, příruční pokladničky atd.).

- **Elektronická ochrana**

Je ochrana majetku a osob pomocí elektrických prvků. Patří sem zejména:

- elektrická zabezpečovací signalizace (EZS),
- elektrická požární signalizace (EPS),
- uzavřené televizní okruhy (CCTV),
- přístupové a docházkové systémy (ACCESS),
- biometrické identifikační systémy,
- elektronická ochrana zboží,
- ochrana dat a informací,
- satelitní vyhledávání vozidel
- zdravotní a nouzová signalizace.

- **Smíšená a speciální ochrana**

Smíšená ochrana osob a majetku, využívá kombinaci mechanických zábranných systémů a elektronickou ochranu jako celek (elektronické blokování dveří, závor, turniketů atd. Kombinované elektromechanické zámky a zámkové systémy, elektronické otvírače dveří. Mezi speciální ochranu řadíme individuální technickou ochranu a chemickou ochranu předmětů a dokumentů. [2]

2 VŠEOBECNÝ POPIS SYSTÉMŮ KONTROLY VSTUPU

2.1 Seznámení se systémy kontroly vstupu

Systém pro elektronickou kontrolu vstupu je počítačem řízený soubor prvků kontrolující přístup do určitého prostoru. Ten bývá zabezpečen zámkem a nějakou formou klíče. Vstup do takto chráněného prostoru je potom povolen pouze oprávněným osobám v určitých, předem definovaných časových intervalech. Určení, kdo a kdy bude mít do chráněného prostoru přístup, je díky použití počítače jednoduché a snadno měnitelné.

Slabinou klasického zabezpečení pomocí zámku a klíče je právě nutnost existence fyzického klíče. Ten lze poměrně snadno duplikovat a umožňuje přístup prakticky komukoliv kdo jej vlastní. Navíc neexistuje evidence kdy a kým klíč použit.

Systém elektronické kontroly vstupu je mnohem efektivnější alternativou předešlého. Všechny osoby, které se budou ve sledovaných prostorách pohybovat, obdrží kartu nebo číselný kód, umožňující vstup do jednotlivých oblastí pouze povolaným osobám v určených časech. Programovatelný řídící panel pak na základě identifikace osoby vstup povolí nebo nepovolí. Pokud dojde ke ztrátě nebo odcizení karty, lze řídící panel jednoduše a rychle přeprogramovat. Pokud je navíc kontrola vstupu připojena k počítačové síti, mají uživatelé k dispozici mnohem širší spektrum funkcí. Systém může zaznamenávat a poskytovat informace o používání karet i kódů, nabídnout obsluze přehledy událostí v systému nebo generovat zprávy z databází. Kromě toho umožňuje systém kontroly vstupu uchovávat a spravovat základní informace o tisícovkách zaměstnanců a poskytovat informace týkající se jejich docházky. [1, 7]

Obecně se dá systém kontroly vstupů shrnout do tří bodů:

KDO se dostane **KAM** a **KDY**.

Přístupové systémy se instalují podle stupně důležitosti. Bezpečnostní oblasti strategických podniků, bank, výpočetních center, trezorových místností apod., mají přístupové systémy důmyslnější a mnohdy s vícenásobnou kontrolou a jištěním. U méně náročných realizací jako je například střežení panelového domu, rodinného domu, provozoven apod., se instaluje systém méně náročný, ale přesto bezpečný pro daný druh ochrany.

Nejdůležitějším řídícím faktorem přístupových systémů je přidělování přístupového práva, které se vystavuje konkrétním osobám na základě stupňů oprávnění podle prostorových, časových, personálních a jiných dispozic. U vyšších systémů se tak děje formou přidělení identifikačního média – nosiče. [2]

2.2 Úkoly systému kontroly vstupů

Především ve spolupráci s ostatními mechanickými a elektronickými systémy plní základní dva úkoly:

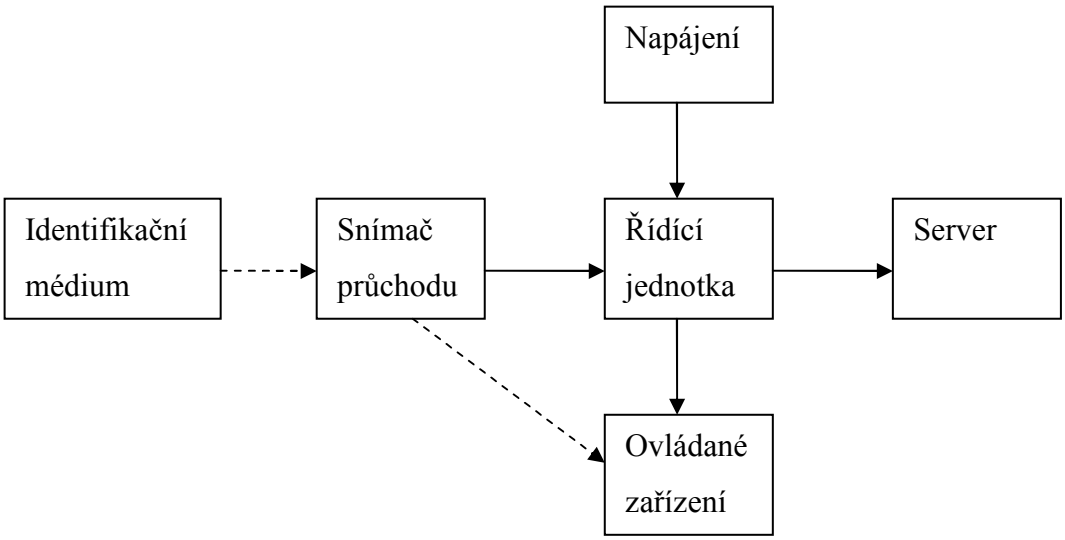
1. Řídí pohyb osob v objektu v denním režimu, to jest v době kdy je systém EZS zpravidla odblokován, nebo jeho část je odblokována a nestřeží.
2. Poskytují informace o pohybu osob v objektu, trvale tyto informace zaznamenávají a sledují a zaznamenávají místo pohybu a čas. Tím přispívají k ochraně objektu i režimovým opatřením. Plněním těchto funkcí pak je jasná komplexní funkce elektronické kontroly vstupu z hlediska logiky nasazení.

Další úkoly které musí systém plnit:

- omezení přístupu nepovolaných osob do určitých prostor objektu (sklady, výpočetní centra, velíny, kanceláře, nebezpečné provozy, utajované provozy, ochrana know - how),
- omezení přístupu mimo určité časové úseky (zaměstnanci, návštěvníci, noční, denní, úklid, zásobování),
- registrace délky pobytu, doby pobytu, místa a účelu, čítání doby pobytu na pracovišti (fungují jako elektronické píchací hodiny),
- sledování a dokumentování pohybu, místa a času osob a zařízení, monitorování stavu objektu, měření návštěvnosti, vytíženosti pracovníků, objektu, využívání zdrojů, materiálu (kopírky, výtahy), vytížení dalších kapacit, zvýšení bezpečnosti technologických provozů, dohled, využívání pracovní doby, zamezení zbytečného a nepovoleného pohybu po objektu, sledování odběru strav, dodržování technologických přestávek a činnost provozu atd. [2]

2.3 Struktura systému kontroly vstupu

Celý systém pro kontrolu vstupu se z pravidla skládá ze dvou základních částí, a to hardwarové a softwarové. Hardwarovou část tvoří řídící jednotky a prvky pro přenos dat a komunikaci (PC, převodníky RS-232/485, kabeláž, sběrnice atd.). Část softwarovou potom představují dvě části ovládacího programu – serverová a klientská (uživatelská).



Obr. 1: Topologie systému kontroly vstupu

Do hardwarové části tedy patří:

- **Identifikační médium**

Identifikační médium je prakticky nejdůležitějším prvkem bez kterého se do objektu zabezpečeného systémem kontroly vstupu osoba nedostane. Vyrábí se v různých provedení, nejčastěji to však bývají karty, přívěsky, etikety atd. Můžou být kontaktní, bezkontaktní, magnetické, čárové kódy, čipové, rádiové. V dnešní době se stále více používá jako nosič informace samo lidské tělo – biometrie.

- **Snímač průchodu**

Jedná se o zařízení, které čte a dekóduje data z identifikačního média. Musí vždy odpovídat typu nosiče – čtečky, klávesnice, terminály atd. Z důvodu že je snímač před zabezpečeným objektem, musí být odolný proti vnějším vlivům, stupeň krytí či sabotážní bezpečnost. Snímač průchodu by dále měl být snadno ovladatelný.

- **Ovládané zařízení**

Jedná se o koncové prvky vstupního systému, jsou to zařízení otevírající (příp. uzavírající) přístup do objektů. Patří zde různé elektrické zámky odblokování vstupu, uvolnění turniketu, otevření závory atd.

- **Server**

Je to zařízení pro správu, monitorování a evidenci přístupových systémů.

- **Řídící jednotka**

Řídicí jednotky jsou zařízení, která na základě informací ze snímače (nejčastěji čteček karet) rozhodují o poskytnutí nebo odmítnutí přístupu do zabezpečeného prostoru. Povolení přístupu se děje nejčastěji odblokováním připojeného elektrického zámku nebo turniketu, zvednutím závory apod. Systém pracuje s distribuovanými databázemi. To znamená, že obsahy databází jsou rozesílány na jednotlivé řídicí panely, které pak pracují zcela autonomně, tedy bez nutnosti spolupráce s ostatními prvky v síti (PC, další jednotky). Mohou tak lokálně vyhlašovat poplachy při násilně otevřených nebo nedovřených dveřích, samy rozhodnout, zda osobu s konkrétní kartou do chráněného prostoru vpustí nebo ne apod. Velkou výhodou je, že pokud nastane výpadek komunikace s počítačem neohrozí to nijak funkčnost systému, systém bude pracovat naprosto stejně, jen záznamy o proběhlých událostech se budou ukládat ve vnitřní paměti. Pro jejich naprogramování a plné využití všech vlastností je však nutné alespoň dočasné propojení se softwarovou částí - ovládacím programem.

Pokud je jednotka jen jediná a umístěna dostatečně blízko počítači s ovládacím programem (cca. 10 m), postačí komunikace přímo přes sériové rozhraní RS-232. Pokud je jednotka instalována od počítače dále anebo jich je v systému více, je potřeba k propojení počítače a řídicích jednotek použít tzv. sběrnici RS-485. Signály sběrnice v takovém případě generuje převodník 232/485 připojený na sériový port počítače. Spojení s jednotkami navíc nemusí být realizováno nutně jen lokálně pomocí metalické sběrnice; na velké vzdálenosti můžete využít i existující počítačové sítě, po níž se budou informace přenášet v podobě TCP nebo UDP paketů. Vzdálenost mezi řídicím počítačem a vlastními jednotkami pak není prakticky ničím limitována. Stejně tak při připojení jednotek po síti nejste omezeni počtem dostupných sériových portů počítače. Technologii IP rozeberu dále.

Systémy kontroly vstupů ale kromě vlastní funkce kontroléru přístupu umí sledovat i důvody průchodů. Vedle prostých příchodů a odchodů tak mohou zaznamenat i to, zda pracovník odchází k lékaři, na dovolenou, služební cestu apod. Zaznamenaná docházková data lze automaticky přenášet do databáze systému. [7]

Softwarová část:

Softwarovou stránku systému představují dvě části programu, serverová a klientská. Serverovou část tvoří hned několik aplikací - datový server, komunikační server a služby pro automatické spouštění naplánovaných akcí a kopírování popisu událostí na sériový port.

Hlavním úkolem datového serveru je zajištění a sjednocení přístupu k databázím pro všechny připojené klienty. Komunikační server pak obstarává veškerou komunikaci s hardwarovými zařízeními. Musí tedy být spuštěn na počítači, k němuž je sběrnice s jednotkami buď fyzicky připojena nebo který je připojen k počítačové síti, po níž se má s jednotkami komunikovat. Databáze s datovým serverem mohou být nainstalovány na jednom počítači a na jiném počítači, umístěném např. blíže kontrolérům, může běžet server komunikační.

Klientská část poskytuje uživatelské rozhraní, z něhož je možné systém monitorovat a ovládat. Se serverem komunikuje pomocí TCP/IP protokolů, může proto být nainstalován prakticky kdekoliv, kde je k dispozici přístup k TCP/IP síti. Server tedy může komunikovat najednou i s více klienty, kteří pak pracují zcela nezávisle, ale nad společnými databázemi. Správa systému je tak možná z více libovolných míst současně. [7]

Přenos dat:

Komunikace mezi oběma popsanými částmi - hardwarovou a softwarovou probíhá podle následujícího scénáře.

Jednotky na sběrnici zaznamenávají události do svých vnitřních pamětí. Paměť každé z jednotek má kapacitu 10.000 takových událostí. Pokud je komunikační server spuštěn a správně nakonfigurován, provádí tzv. polling - cyklicky vyčítá ze všech aktivních jednotek zaznamenané události. V každém cyklu takto server obvolá všechny jednotky na sběrnici a z každé vyčte 1 událost (pokud na jednotce nějaká zaznamenaná je), což při obsazení sběrnice 31 jednotkami trvá maximálně cca 3-4 sekundy. V případě, že komunikační server spuštěn není, nebo je vyčítání událostí obsluhou záměrně pozastaveno,

zůstávají záznamy pouze v pamětech jednotek, kde čekají na vyčtení, po přečtení události ji komunikační server doplní o všechny nezbytné informace - kde a kdy k ní došlo, jméno a příjmení osoby, číslo karty apod. – a zobrazí ji v okně uživatelského rozhraní (klienta). Pokud je klientů připojeno více, rozešle ji všem.

V opačném směru probíhá přenos dat také, např. při programování jednotek nebo manuálním ovládání vstupů kontrolérů přímo z programu. V takových případech posílá komunikační server konkrétní jednotce rámec s požadovanou informací a jednotka mu správné přijetí, a případně i úspěšné provedení příkazu potvrdí. Pokud server potvrzení nedostane, několikrát požadavek zopakuje. Jestliže ani jeden z těchto pokusů není úspěšný, oznámí v uživatelském rozhraní obsluze, že jednotka nekomunikuje. [7]

Funkce ANTI-PASSBACK:

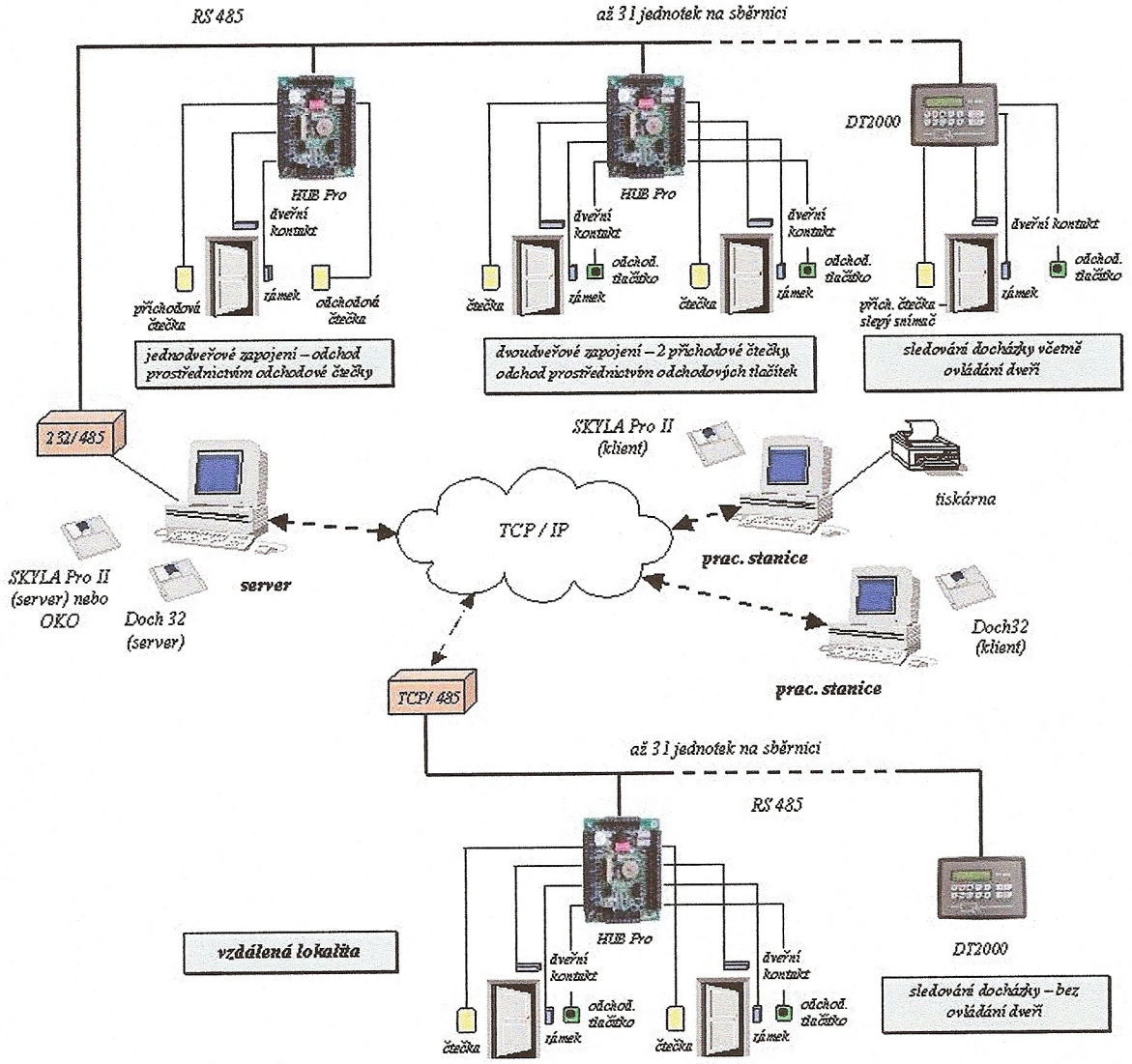
Jde o funkci, která brání opakovaným vstupům na jednu kartu. K tomu aby tato funkce mohla fungovat musí být nastavena část čteček pro vstup do objektu (vstupních), a část čteček pro opuštění objektu (výstupních). Zjednodušeně řečeno anti-passback sleduje, zda při načtení karty na některé vstupní čtečce, bylo předcházející čtení provedeno na čtečce výstupní. Jinými slovy řečeno zda osoba před dalším vstupem objekt nejprve opustila. Pokud tato podmínka není splněna systém vyhodnotí identifikaci jako neplatnou a neumožní tak vstup do objektu. Tak může zabránit situaci, kdy si více osob před vstupem předává kartu pro získání přístupu. Funkce dále sleduje čas uběhlý od poslední čtení této karty. Pokud je kratší než přednastavený interval, vstup opět není umožněn.

- **Globální Anti-passback:**

Rozhodování zde provádí řídící počítač s datovým serverem. Ten shromažďuje data o průchodech anti-passbackovými čtečkami a rozhoduje zda dotyčné kartě vstup umožní. V tomto případě je nezbytné trvalé připojení a činnost komunikačního i datového serveru.

- **Lokální Anti-passback:**

Funguje pouze v rámci jedné řídící jednotky, kontroluje pouze více vstupů, na níž se aktivuje zapnutím příslušného systémového příznaku. Na výstupní čtečce může být platná karta čtena i vícekrát po sobě, a vždy dojde k sepnutí příslušného relé. Protože se ale pořadí vstup-odchod kontroluje pouze uvnitř jedné jednotky, nelze zabránit druhému vstupu do objektu na jiné jednotce. [5, 7]



Obr. 2: Funkční schéma programu Skyla Pro od Honeywellu

2.4 Kombinace systému kontroly vstupu s jinými systémy

Systémy kontroly vstupu mohou být používány samozřejmě i v kombinaci s dalším poplachovým systémem, potom tvoří společně jednu bezpečnostní aplikaci. Kombinace pochopitelně zvyšuje efektivitu přístupových systémů, a v mnoha případech se používá.

V současné době se většinou používají tyto kombinace systémů kontroly vstupu:

- **Kombinace přístupového systému a docházkového systému**

Tato kombinace umožní vstup do objektu a zároveň zaznamená datové údaje pro potřeby zaměstnavatele, respektive personálního útvaru, tím je umožněn nejen vstup do

objektu, ale i evidována docházka tj. příchod a odchod do zaměstnání, odchod na svačinu, oběd, k lékaři, soukromí výstup z objektu, služební odchody, přerušení práce, ranní, odpolední, noční práce, práce o svátcích a dnech pracovního volna a podobně. Sledování a evidence pracovní doby je dána ustanoveními Zákoníku práce, v jehož novele jsou promítnuty relevantní směrnice Evropského společenství do českého pracovního práva.

- **Kombinace přístupového systému a systému pro výdej stravy, pracovních pomůcek nebo materiálu**

  Umožňuje další kombinaci přístupu do zařízení zaměstnavatele a odběr stravy, nápojů, nářadí a jiných pracovních pomůcek, přičemž umožňuje bezhotovostní platby např. za stravu, nebo umožňuje evidenčně podchytit vydávané pracovní pomůcky, nástroje, nářadí a podobně.

- **Kombinace systému kontroly vstupu a EZS**

  Často používaná kombinace, která umožní vstup do objektu oprávněné osobě a současně na trase přístupu, či v místnostech, kam má osoba umožněn přístup nebo průchod odalarmuje"(odkóduje)"systém EZS tak, aby nevyvolal nežádoucí poplach. Přitom eviduje a má možnost i časově sledovat pohyb oprávněné osoby po pracovišti. Používá se všude tam, kde nestačí pouze přístupový systém, ale je nutno ještě zajistit objekt, nebo jeho část elektrickou zabezpečovací signalizací.

- **Kombinace systému kontroly vstupu a CCTV**

  Používá se tam, kde je nutno kontrolovat nejen pohyb osob po objektu, ale i sledovat celkovou činnost osoby nebo osob v objektu a mít permanentní kontrolu veškerého pohybu v objektu s možností včasné reakce na nežádoucí situaci, která může vzniknout např. ve věženích, vojenských skladech., letištích, jaderných elektrárnách, chemických provozech apod. Kamerový systém může být z důvodu úspory energie vypnutý a zapne se až po identifikaci osoby přístupovým systémem. Kamery se umisťují taky často aby měli v záběru identifikační zařízení (terminál, čtečku atd.), a to nejčastěji z důvodu vandalismu či jiného poškození.

- **Kombinace systému kontroly vstupu a EPS**

  Je jednou z nejčastějších a nejjednodušších aplikací. Používá se k zajištění automatického otevření únikových východů v případě detekce požáru systémem EPS. Z

důvodu rychlosti reakce, spolehlivosti a univerzálnosti je integrace prováděna zapojením napájení elektrických zámků přes kontakt signalizačního relé systému EPS. V neposlední řadě je taky důležité aby se při vzniku požáru vědělo kolik osob se nachází v prostorách zabezpečených systémem kontroly vstupu. Právě proto je důležité aby opravdu každý zaměstnanec prováděl identifikaci před vstupem do objektu. Otázkou samozřejmě zůstává jak je to dodržováno, dalo by se to nazvat takovou formou režimového opatření.

- **Kombinace systému kontroly vstupu s informačními technologiemi**

Rostoucí využití informačních technologií vyžaduje samozřejmě i přístup k nim. Ne všechny informace je však možno sdělovat každému a kdykoliv. Tím vznikl požadavek na integraci systému kontroly vstupu a informační technologie. Vzhledem k omezeným možnostem zapamatovat si kódy a hesla se požaduje, aby přístup byl umožněn po schválení vstupu a vydání přístupového média (přihlašování k PC, do sítí a různých SW, aplikacím, elektronický podpis atd.). Vazebními prvky mezi systémem elektronické kontroly vstupu pro fyzickou kontrolu přístupu a prvky řízení přístupu k informacím jsou:

- identifikační karty

  Většinou ve formě kombinovaných karet, to jest. bezkontaktní karta obsahující bezkontaktní identifikační část která současně obsahuje výkonný bezpečnostní procesor s normalizovaným kontaktním rozhraním dle ISO 7816, informace uživatele jména a hesla je v tomto případě převážně uschována na Id kartě.

- biometrické prvky

  Otisk prstu, charakteristiky duhovky oka zpracovávané pomocí programového modulu (API) umožňujícího začlenění biometrické čtečky do existujících softwarových aplikací. U tohoto způsobu je zabezpečená informace uložená v informačním systému chráněna prostředky operačního systému a šifrováním a k jejímu zpřístupnění dochází po ověření shody mezi uloženým vzorem a nově sejmutým vzorkem biometrického údaje. [2]

2.5 Docházkový systém PASSPORT

Systém PASSPORT je určen k evidenci a automatickému zpracování docházky na základě dat o průchodech na čtečkách identifikačních prvků a dat o definicích směn, kalendářů a dalších nastavení. Systém docházku nejen vyhodnocuje, ale i kontroluje podle předem definovaných modelů pracovní doby a umožňuje editovat a zavádět nové akce přímo z klávesnice PC jednotlivých uživatelů. Zpracovaná data o docházce lze přehledně tisknout pomocí různých sestav nebo exportovat do navazujících systémů, zejména mzdových a personálních. Každá osoba provádí značení docházkových akcí na čtečkách identifikačních karet, které jsou podle požadavků umisťovány do vstupních prostor či do prostor jednotlivých pracovišť.

Základními docházkovými akcemi jsou:

- Běžná pracovní činnost,
- Přestávka na oběd,
- Dovolená,
- Nemoc,
- Případně další programovatelné akce.

Výhody systému:

- usnadnění a zpřesnění zpracování dat,
- zamezení falšování údajů,
- usnadnění přepisovaní údajů o docházce a následného výpočtu odpracované doby,
- rychlá informace o aktuálním stavu docházky, přítomnost osob,
- zpřístupnění základních informací o odpracované době v rámci měsíce na čtečkách identifikačních karet.

Vyhodnocování odpracované doby se provádí podle tzv. modelu pracovní doby. Model pracovní doby definuje základní údaje a řídí výpočet a zpracování docházky. [12]

2.6 Evidence návštěv VISIT

Programový modul VISIT je určen k evidenci osob vstupujících do prostor, kde je požadována přesná evidence všech procházejících osob včetně návštěv, které nemají trvalé oprávnění ke vstupu. Systém je instalován na PC v recepci či vrátnici, jehož prostřednictvím se registrují základní osobní údaje o návštěvě. Dále lze tento systém vhodně využít pro registraci vjíždějících vozidel, kde se vedle údajů o posádce vkládají rovněž základní údaje o vozidle.

Systém VISIT pracuje:

- jako autonomní systém
- v rámci systému kontroly vstupu ACCESS
- v rámci systému evidence docházky PASSPORT

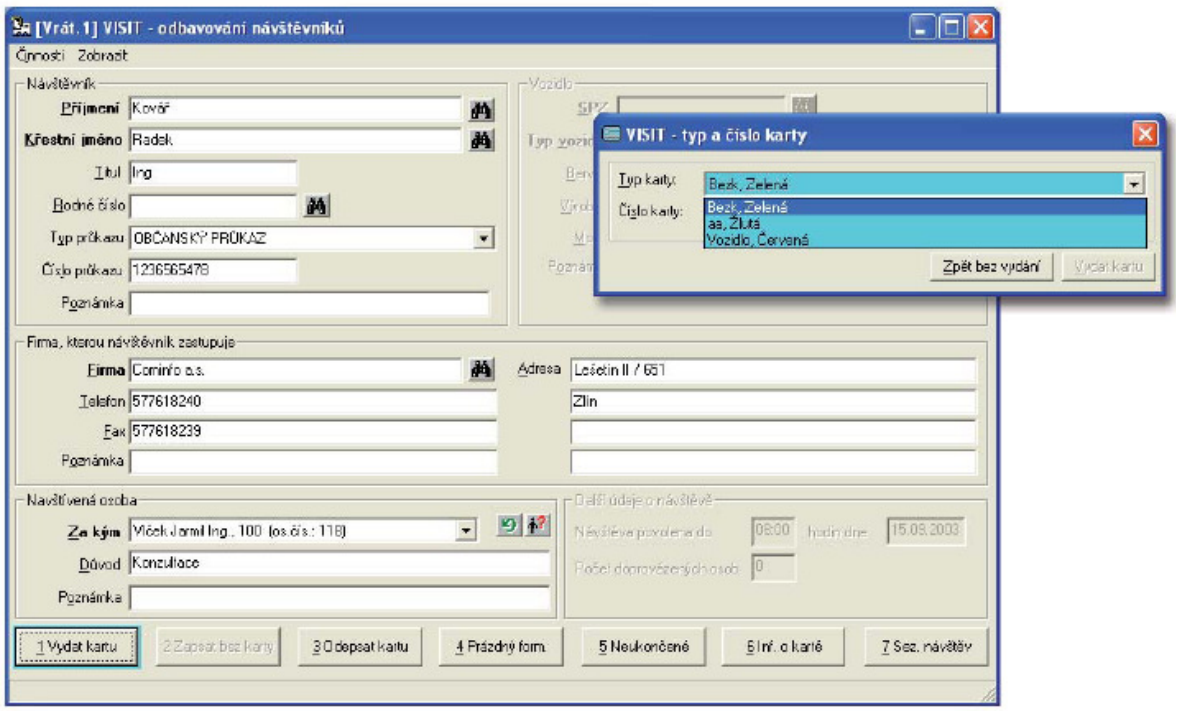
Je-li systém evidence návštěv propojen se systémem kontroly vstupu Access, je možno návštěvě vydat platnou identifikační kartu. Tato identifikační karta může mít předem definováno oprávnění vstupu a přesně tak určit, do kterých prostor je návštěvě povolen vstup.

Vrácení návštěvní karty lze realizovat dvěma způsoby:

- osobně – vrácení identifikační karty obsluze recepce či vrátnice,
- automaticky – vhozením návštěvní karty do zásobníkového snímače, kde tyto karty zůstávají uschovány pro účely dalšího použití.

Systém obsahuje následující základní možnosti práce:

- vyhledávání dat o předchozích návštěvách osob,
- příchod návštěvy – osobní údaje, datum a čas příchodu a číslo vydané karty,
- odchod – doplní záznam časem odchodu a uvolní návštěvní kartu pro další použití,
- prohlížení – přehledné zobrazení na monitoru počítače,
- vyhledávání – akce vyhledá záznamy o již provedených návštěvách,
- archiv – měsíční uložení dat do archivu. [12]



Obr 3: Program evidence návštěv VISIT

2.7 Stravovací systém CARDPAY

Jednou z hlavních oblastí nasazení systému je jeho implementace do prostředí podnikového stravování. Platební systém CARDPAY představuje řešení pro lokální bezhotovostní platební místa spojená do jednoho centra, kde probíhá centrální správa účtů karet. Při nasazení systému pro podnikové stravování (objednávkové i restaurační) tak zcela nahrazuje a plně automatizuje standardní „stravenkový“ systém. Umožňuje evidovat primární údaje o jednotlivých strávnících a hlavně provádět výpočet skutečných nároků na dotaci stravného na základě dat o odpracované době z docházkového systému. [12]

Ke společným vlastnostem patří:

- společná matriční data a uživatelská správa s jinými aplikacemi,
- definice různých typů účtů a strávníků, jejich parametrů,
- vazba na docházkový systém,
- vazby na různé firmy, provádějící přípravu jídel,
- vazba na mzdový systém.

2.8 Hotelový přístupový systém

Hotelový přístupový systém spolupracuje s hotelovým rezervačním systémem. Na recepci obdrží host svou platnou identifikační hotelovou kartu, která má nastavenou platnost použití a práva přístupu. Vstup do pokoje spočívá pouze v přiblížení identifikační karty s příslušnými oprávněními ke čtečce karet. Pro využití hotelové karty, jako karty platební, se také nastaví typ účtu a možnosti plateb za služby a zboží.

Bezkontaktní identifikační karty mohou být:

- jednorázové – zůstávají hostům jako suvenýr,
- vratné, které po skončení pobytu host navrátí.

Hotelový přístupový systém plní tyto funkce:

- přístup hostů do hotelových pokojů,
- ovládání výtahů,
- přístup na parkoviště a do sportovních zázemí.

Systém je řešen v režimu provozu on-line, takže vždy jsou k dispozici informace:

- obsazení pokojů,
- možnost energetických úspor,
- využití hotelových služeb,
- zabezpečení proti násilnému vniknutí do pokojů. [12]

Obr. 4: Čtecí hlava pokojových karet

3 SYSTÉMOVÉ POŽADAVKY

Tyto požadavky popisuje norma ČSN EN 50 133-1, tato norma popisuje všeobecné požadavky na systémy kontroly vstupů pro použití v bezpečnostních aplikacích. Pokud některá část systému kontroly vstupů (například rozhraní přístupného místa) tvoří část zabezpečovacího poplachového systému, musí tato část splňovat současně i příslušné požadavky norem na zabezpečovací systémy.

Norma se zabývá zabezpečovacími aplikacemi pro každé přístupové místo. Systém kontroly vstupů se může skládat z libovolného počtu přístupových míst. Různé úrovně důvěrnosti při identifikaci uživatelů žádajících vstup místem přístupu vedly k definování tříd rozpoznání. Dále jsou definovány požadavky na automatizované systémy kontroly vstupů a komponenty uvnitř a vně budov.

Zahrnuje:

- systémovou architekturu a všeobecné požadavky na systém kontroly vstupů pro zabezpečovací aplikace,
- funkční požadavky,
- definice podmínek okolního prostředí a elektromagnetické kompatibility,
- požadavky na komunikaci kontroly vstupů s ostatními systémy, jako jsou například ovládací prvky místa přístupu a detektory, poplachový systém atd.

3.1 Klasifikace zabezpečení

Zabezpečení systému kontroly vstupu je založeno na klasifikaci identifikace a na klasifikaci přístupu.

- *Klasifikace = třídění, hodnocení, řazení informací podle určitých kriterií*
- *Identifikace = zjištění totožnosti uživatele, předmětu*

3.2 Klasifikace identifikace

- je založena na úrovni důvěrnosti při identifikaci oprávněných uživatelů (Uživatel = osoba žádající průchod místem přístupu),
- vyjadřuje jakost vztahu mezi identifikací použitou daným systémem a oprávněným uživatelem,

- bere v úvahu riziko prozrazení oprávnění vlastního uživatele bez ztráty vlastního práva zachovat si výhodu vlastního přístupu,
- systém kontroly vstupu musí mít v každém místě přístupu jednoznačnou identifikaci alespoň v jednom směru,
- pro specifické přístupové místo se může v průběhu času třída identifikace měnit.

Třída identifikace 0 - žádná přímá identifikace.

Založena na prostém požadavku o přístup bez identity uživatele (tlačítko, kontakt, detektor pohybu aj.)

Třída identifikace 1 - informace uložené v paměti.

Založena na heslech, osobních identifikačních číslech aj.

Třída identifikace 2 - identifikační prvek nebo biometrie.

Založena na používání identifikačních prvků, karet, fyzických klíčů, otisku prstů aj.

Třída identifikace 3 - identifikační prvek nebo biometrie spolu s informací uloženou v paměti. Založena na používání kombinace identifikačního prvku nebo biometrie a informace uložené v paměti

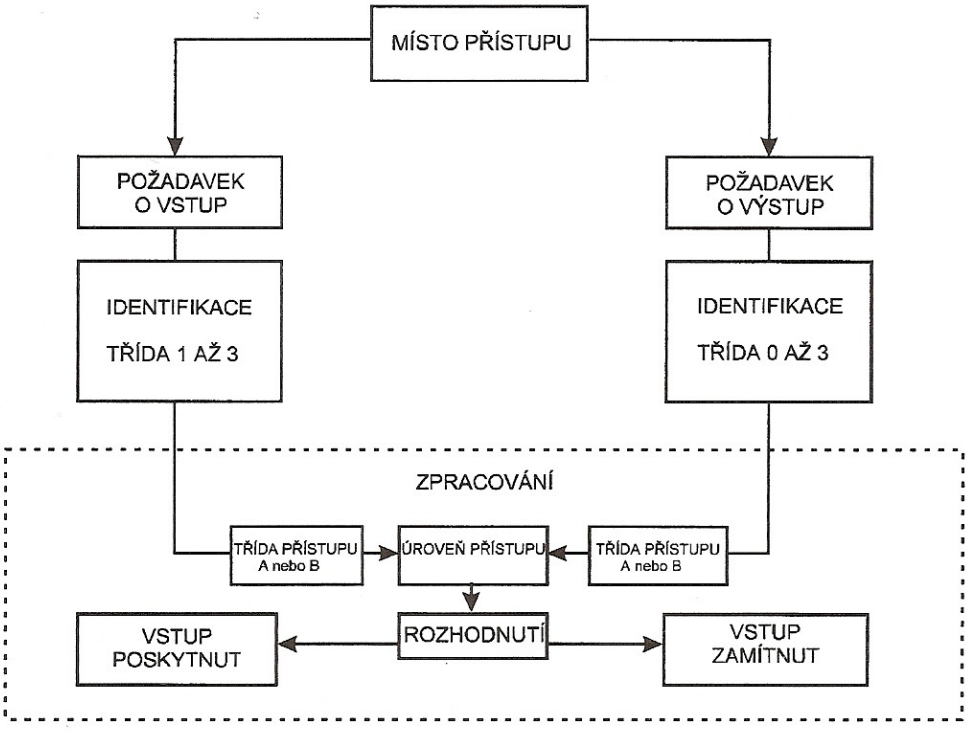
3.3 Klasifikace přístupů

- **Třída přístupu A**

Tato třída platí pro místo přístupu, ve kterém požadovaný stupeň zabezpečení nevyžaduje ani časový filtr, ani ukládání přístupové transakce. (Transakce = událost která odpovídá uvolnění přístupového místa poté, co byla rozpoznána identita uživatele)

- **Třída přístupu B**

Tato třída platí pro místo přístupu, které zahrnuje časové filtry a funkce ukládání. Zahrnuje také podtřídu, která se vztahuje na místo přístupu zahrnující časové filtry ale bez funkcí ukládání dat.(uvolnění přístupového místa poté, co byla rozpoznána identita uživatele).



Obr. 5: Tradiční postup povoleného přístupu

3.4 Společné funkční požadavky pro třídu přístupu A a B

3.4.1 Zpracování

Požadavky na zpracování jsou použitelné pro všechny třídy identifikace. Pokud jsou postupy zpracování uloženy ve snímači místa přístupu a nastavení jsou viditelná, nebo je možné jednotku vyměnit bez účasti správce systému, musí být v dokumentaci uvedeno, že tento výrobek je vhodný pro použití na hranicích přístupového pásma s nižším stupněm bezpečnosti. Uživateli musí být možno přiřadit časový filtr. U postupů musí být možno definovat minimálně dva časové úseky uvolnění, jeden 5 sekund a druhý 60 sekund, a dva povolené časové úseky otevření apas, jeden 10 sekund a druhý 60 sekund. (Apas = výstupní ovládací prvky a detekční prvky míst přístupu). V neposlední řadě zde patří i požadavek, který říká že systém, který se automaticky restartuje po připojení napájení, musí uchovat naprogramované přístupové postupy nejméně po dobu 120 hodin po výpadku napětí.

Dále pak platí pro třídu identifikace 1, že u systému který využívá informaci uloženou v paměti, nesmí být možné po sekvenci 5 za sebou nesprávně zadaných informací umožněn přístup dříve než po 5 minutách.

Pro třídu identifikace 3 platí, že systém, který používá kombinaci identifikačního prvku (tokenu) nebo biometrie a informace uložené v paměti, musí vyslat výstrahu po 5 sekvencích za sebou nesprávně zadaných informací při stejném identifikačním prvku nebo biometrii.

3.4.2 Napájení

Při připojení nebo odpojení napájení nesmí v žádném případě dojít k chybnému uvolnění vstupu. Nepožaduje se však, aby systém kontroly vstupu napájel apas.

3.4.3 Vnitřní zabezpečení

- neoprávněná osoba nesmí mít možnost bez použití nástrojů si zajistit přístup, to platí pro třídy identifikace 1 až 3.

3.4.4 Ochrana programování

- musí být k dispozici zabezpečovací prostředky k zabránění neoprávněné změny předvolených postupů. Poměr počtu různých kombinací kódu k počtu oprávněných osob musí být nejméně 1000:1,
- minimální počet kombinací musí být 10 000,
- správce systému musí mít možnost změnit tento přístupový kód.

3.4.5 Ovládání míst přístupu

- systém kontroly vstupů musí být vybaven rozhraním pro spojení s apas. Toto rozhraní musí zahrnovat ovládání apas a monitorování stavu zabezpečení apas. (Apas = výstupní ovládací prvky a detekční prvky míst přístupu),
- svorkovnice rozhraní místa přístupu musí být umístěna uvnitř skříňky, která musí při otevření normálním způsobem detekovat sabotáž,

- při dodržení montážních pokynů výrobce nesmí být možno získat přístup ze strany s nižší úrovní zabezpečení k obvodu uvolnění,
- systém kontroly vstupů musí monitorovat stav apas, zda je nebo není apas uzavřen,
- ovládací výstup rozhraní místa přístupu musí mít nejméně jeden bezpotenciálový kontakt s jmenovitým zatížením nejméně 30 VA,
- ovládací výstup rozhraní místa přístupu musí být sepnut, pokud je přístup povolen, a musí být zrušen, pokud nastane jedna z následujících událostí:
  - uběhl předvolený časový úsek uvolnění apas,
  - monitorování apas indikuje, že apas je otevřen.

3.4.6 Identifikace

Úroveň zabezpečení je ovlivněna řadou faktorů, z nichž nejdůležitější jsou počet kombinací a snadnost zhotovení duplikátu.

Pro třídu identifikace 1 platí:

- poměr počtu různých kombinací kódů k počtu identifikovatelných uživatelů musí být nejméně 1000:1,
- minimální počet kombinací v systému musí být 10 000.

Pro třídu identifikace 2 a vyšší platí:

- každému uživateli musí být v jednom systému přiřazena jednoznačná identita,
- struktura kódování identifikace musí být poskytovat nejméně 1 000 000 kombinací a každá informace identifikace předaná do systému musí být s touto strukturou porovnána,
- četnost chybných povolení nesmí být větší než 0,01 %. Míra chybných odmítnutí musí být menší než 1 %,
- identifikační prvek s kódovacími systémy, které jsou viditelné samotným lidským okem, a tudíž je při normálních podmínkách možné snadno zhotovit jeho duplikát, nesmějí být použity,

- pokud je identifikační prvek označen identifikačním číslem, nesmí být přímým zobrazením celého kódu identifikačního prvku.

Pro třídu identifikace 3 platí:

- informace uložené v paměti používané současně s identifikačním prvkem nebo biometrií musí mít minimálně 10 000 kombinací.

3.4.7 Hlášení

Systém kontroly vstupu musí mít prostředky pro hlášení ve formě výstrahy a zobrazení událostí tykající se detekce sabotáže, nastane-li situace že je místo přístupu otevřeno bez poskytnutí přístupu, nebo proběhlo otevření místa přístupu po uplynutí povolené periody pro poskytnutí přístupu.

Každá požadovaná výstraha musí být ohlášena s maximálně 10sekundovým zpožděním.

3.4.8 Komunikace s jinými systémy

Každé místo přístupu systému kontroly vstupu musí mít výstup, který avizuje okamžik oprávněného přístupu. Pokud je tímto výstupem binární spínač, musí být galvanicky oddělen a sepnut při poskytnutí přístupu a rozepnut, když nastane jedna z následujících událostí:

- místo přístupu je otevřeno a zavřeno,
- povolená doba pro uvolnění apas uběhla, nedošlo k otevření místa přístupu,
- místo přístupu zůstalo otevřené i po uběhnutí povolené doby pro otevření.

Pokud jsou pro tento výstup použity alternativní prostředky, musí poskytovat stejné logické informace. Pokud připojené systémy mají vybavení pro změny postupů daného systému kontroly vstupů, potom musí splňovat požadavky ochrany programování. Připojením nebo odpojením komunikačních linek nesmí dojít k poskytnutí přístupu. [5]

4 IP TECHNOLOGIE A SYSTÉMY KONTROLY VSTUPU

Komunikační sítě využívající protokoly TCP/IP se v posledních letech rozšířila do mnoha oborů a zařízení a elektronické systémy pro kontrolu vstupu nejsou výjimkou. Vyhrazená media jako jsou třeba metalické sběrnice propojující přístupové kontroléry jsou stále ve velké míře používány i v systémech budovaných v současnosti, protože mají řadu opodstatnění. Nicméně dovolují komunikovat s připojenými prvky jen na omezené vzdálenosti. Například u nejpoužívanějšího typu sběrnice RS-485 je to max. 1200m. Tuto vzdálenost lze samozřejmě zvyšovat pomocí opakovačů, ale i tak bude vzdálenost v řádu několik kilometrů, což např. pro správu přístupového systému zahrnujícího několik měst není dostatečné. Proto se začínají nahrazovat právě IP technologií, která nemá s propojením na větší vzdálenost problém.

4.1 Využití IP sítě pro komunikaci v přístupových systémech:

- Nejjednodušším využitím těchto sítí je propojení současné lokální metalické sběrnice, která sdružuje prvky elektronického přístupového systému s počítačem pro správu systému prostřednictvím počítačové sítě používající pro komunikaci protokol TCP/IP. Toto propojení umožní síťový převodník mezi ethernetovým rozhraním a sběrnicí. V tomto případě se jedná v podstatě o prodloužení dotyčné metalické sítě pomocí IP sítě. Jako negativum se dá označit omezení komunikační rychlosti s přístupovými prvky na rychlost danou max. přenosovou rychlostí sběrnice, přesto že současné IP sítě dovolují daleko vyšší rychlosti.

- Sofistikovanějším využitím IP v přístupových systémech je přímá síťová komunikace mezi programem pro správu přístupového systému a dílčími prvky, které jsou osazeny převodníkem na ethernetové rozhraní. Zde už je možné využívat plně komunikační rychlost kterou síť poskytuje. Fyzické umístění prvků může být v rámci sítě kdekoliv.

- Třetí případ by se dal označit za podskupinu předchozího. V předchozím případě šlo o to aby aplikace byla nainstalována alespoň na jednom počítači, zde se správa přístupových prvků provádí přes webové rozhraní, za využití protokolu http, respektive https. Velkou výhodou je tedy nezávislost na zařízení pros správu (nemusí jít o klasické PC, ale jakýkoliv přístroj s vestavěným webovým prohlížečem např.

PDA, smartphone nebo iPod), a na operačním systému (Windows, Mac OS, Linux, Symbian). Přístupový systém lze tedy v podstatě spravovat odkudkoliv. [4]

4.2 Přístupové prvky využívající IP technologie

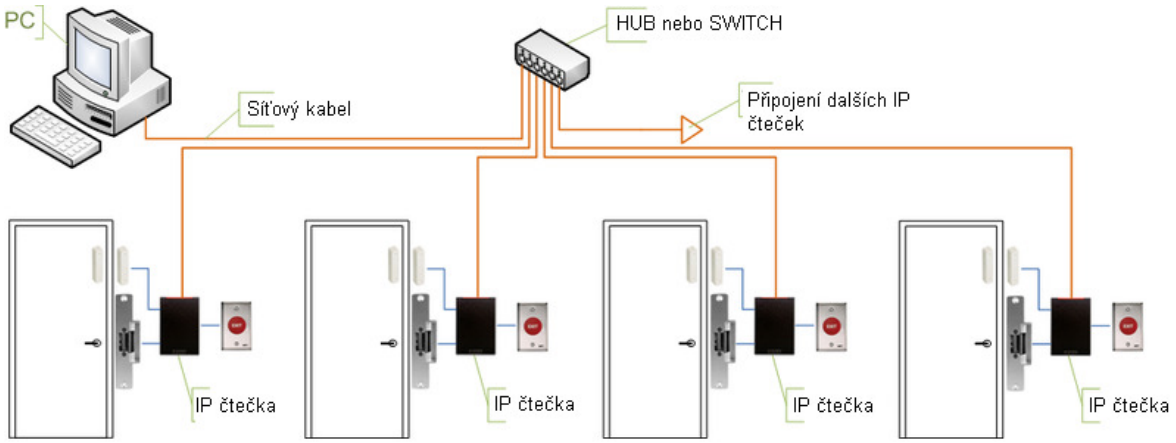
I když přístupové systémy ve své standardní podobě obsahují celou řadu prvků, z hardwarových komponent má smysl osazení ethernetovým rozhraním prakticky jen u kontrolérů a identifikačních zařízení (čteček).

1) Čtečky s IP rozhraním

Vybavení čtečky ethernetovým rozhraním pro přímou komunikaci po IP síti je v některých případech uživatelem vyžadováno a má své klady. Například možnost instalace čtečky kdekoliv v dosahu sítě, bez ohledu na její vzdálenost od přístupového kontroléru, který data posílaná čtečkou vyhodnocuje. Na druhé straně to znamená v důsledku nutnosti implementace ethernetového převodníku vyšší cenu čtečky ve srovnání s běžnými modely vybavenými standardními rozhraními - Wiegand, RS-232 nebo RS-485. Klady takového nasazení navíc mohou být zhodnoceny jen v instalacích, kde je v IP síti zajištěna dostatečně krátká odezva a spolehlivý přenos dat bez výpadků, jinak může uživatel na uvolnění přístupového místa čekat i neakceptovatelných několik sekund.

Protože se v tomto případě jedná o přenos identifikační informace mezi čtečkou a kontrolérem ještě před jejím vyhodnocením, a také protože je čtečka prvkem umístěným na nechráněné straně sledovaného prostoru, je velmi důležitá ochrana proti podvržení falešné identifikace neoprávněnou osobou. A to buď možností odpojení čtečky od IP sítě a připojení vlastní čtečky nebo zařízení, které bude její činnost emulovat (což je událost, již by měla čtečka v každém případě detekovat pomocí sabotážního kontaktu) nebo cestou podvržení paketu s falešnou identifikací osoby kdekoliv v síti. Druhý jmenovaný postup bude pro případného útočníka určitě obecně jednodušší a z jeho pohledu bezpečnější, protože umožňuje vypustit paket do sítě směrem k přístupovému kontroléru prakticky kdekoliv, bez rizika vlastního odhalení při manipulaci se čtečkou. Proto je při takovém využití IP technologie v přístupových systémech důležitější více než kde jinde dostatečné zabezpečení komunikace mezi čtečkou a kontrolérem proti případným útokům, ať už v podobě implementace dostatečně silného, a přitom rychlého šifrování dat, vytvoření VPN nebo jiných adekvátních mechanismů.

Z výše uvedených důvodů se v současné době spojení mezi kontrolérem a čtečkou prostřednictvím IP sítí zatím příliš nerozšířilo a z bezpečnostních i cenových důvodů stále převažují v současných systémech klasické komunikační kanály. [4]



Obr. 6: Použití IP čteček v systému

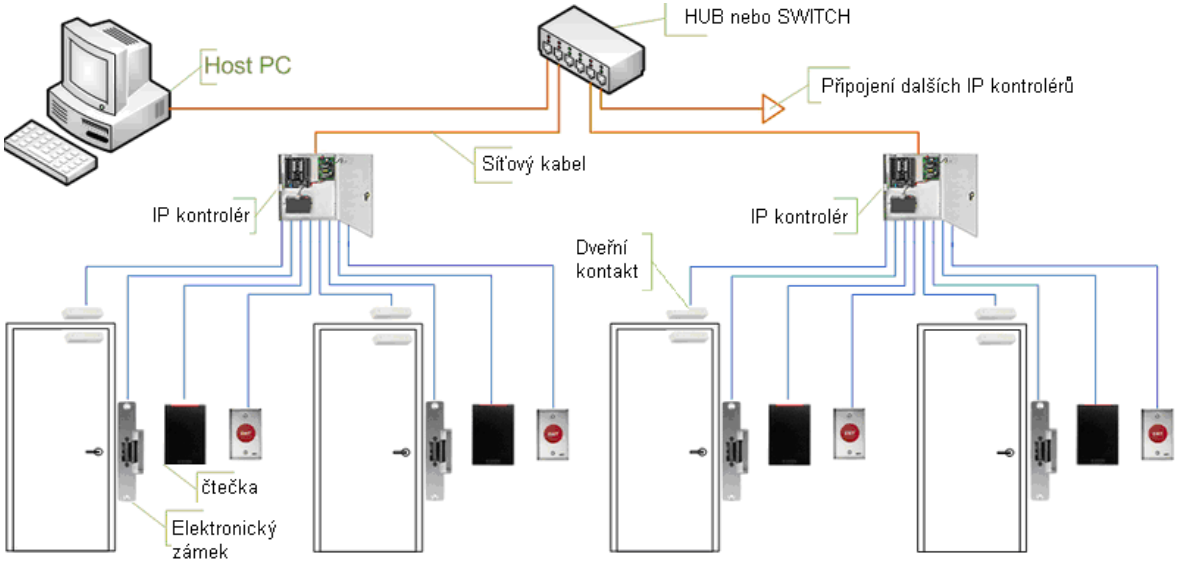
2) Přístupové kontroléry s IP rozhraním

Na rozdíl od čteček jsou kontroléry vybavené ethernetovým rozhraním daleko více rozšířené. Kontrolér je totiž z pohledu funkce přístupového systému již prvkem, který rozhoduje o povolení nebo zamítnutí přístupu osoby do konkrétního místa na základě její identifikace. Není tak závislý na rychlé výměně informací s jinými prvky přístupového systému, aby mohl být dotyčnému člověku přístup poskytnut v dostatečně krátké době. Spojení s dalšími prvky, ať už počítačem shromažďujícím události v systému nebo s jinými kontroléry, samozřejmě probíhat může a v naprosté většině případů i probíhá. Nicméně zde není rychlost předání informace tak kritická a mírné zdržení způsobené např. vyšším aktuálním zatížením IP sítě nebo krátkodobý výpadek nemají vliv ani na přesnost vyhodnocování identifikačních informací, ani na komfort běžného uživatele systému, který jeho čtečky denně používá pro průchody do chráněných oblastí.

Dá se dokonce říci, že většina novějších přístupových kontrolérů je již nějakou formou ethernetového rozhraní osazena nebo takové rozšíření velice jednoduše umožňuje, proto je v nově budovaných systémech poměrně často využíváno. Protože přístupový kontrolér by měl být bez ohledu na povinnou vybavenost sabotážním kontaktem standardně instalován na zabezpečené straně dveří, není v tomto případě tak vysoké riziko

neoprávněné manipulace osobou,která se do chráněného prostoru teprve snaží přístup získat.

Samozřejmě i zde je ale na místě zajištění bezpečnosti komunikačního kanálu i dálkového ovládání kontroléru vůči neoprávněnému útoku ve formě podvržení paketů nebo využití webového rozhraní pro ovládání přístupových míst neoprávněnou osobou. [4]



Obr. 7: Použití IP kontrolérů v systému

4.3 Obecné výhody a nevýhody řešení přístupových systémů na IP technologiích

Výhody:

- **Neomezený počet zařízení/kontrolérů**

Princip komunikace přes IP adresy na rozdíl od klasického připojování kontrolérů, případně jejich podřízených modulů na sběrnici s omezeným počtem prvků dovoluje použití prakticky neomezeného počtu systémových prvků. Počet může být omezen jen softwarem či počtem dostupných volných IP adres v síti. I tento teoretický nedostatek bude ale do budoucna řešen IP protokolem 6, s vyššími počty využitelných adres, než je tomu u aktuální nejčastěji používané verze protokolu 4.

- **Využití různých fyzických médií pro přenos dat**

IP protokol může být přenášen různými kanály a komunikačními médii. Není tak problém zesíťovat rozsáhlý objekt např. pomocí optických vláken, která můžou značně prodloužit běžnou ethernetovou kabeláž, a to bez omezení rychlostí. Dále můžou být data přenášena formou WiFi sítě. I to je komunikační kanál, kterým se mohou přístupové prvky, jsou-li vybaveny (třeba i externě připojeným) WiFi přístupovým bodem, využít ke komunikaci se softwarem pro správu systému.

- **Využití výhod stávajících IP sítí**

Síťová uspořádání, zde ethernetové sítě totiž mohou používat, a v řadě případů používají, redundance a záložní komunikační trasy pro případ výpadku primárního kanálu. Přesměrování paketů na jinou dostupnou trasu dnes mohou automaticky realizovat samy aktivní síťové prvky a to řádově stovek milisekund. IP sítě se považují za poměrně spolehlivý komunikační prostředek, velmi zřídka se stává, že by vypadla z provozu kompletně celá síť.

- **Integrace s ostatními systémy**

Díky obecně velice jednoduché dostupnosti dat z přístupového systému prakticky kdekoliv v dotyčné síti se otvírá integrace se systémy jinými, ať už bezpečnostními nebo třeba personálními. Pokud pro propojení požadovaných systémů, stačí výměna dat přes IP infrastrukturu - a v mnoha případech stačí, potom je jejich propojení otázkou nasměrování paketů na příslušný síťový prvek nebo komunikačního propojení jednotlivých programů, opět s využitím prostředků IP sítí.

Nevýhody:

- **Omezení spojená se síťovým provozem**

Zde by se daly uvést aspekty vyplývající z komunikace přes IP sítě. A to již zmíněné delší odezvy při výměně informací mezi prvky přístupového systému, a to zejména v okamžiku vyššího zatížení sítě. Řešením by bylo oddělit IP síť od zbytku síťové infrastruktury a realizovat provoz na zcela vyhrazené síti. Ale toto řešení už samozřejmě znamená dodatečné náklady.

- **Možná bezpečnostní rizika**

Jak už bylo naznačeno, díky propojení infrastruktur IP sítí se otvírá cesta potencionálním útočníkům ke zneužití systémů. Z tohoto důvodu je potřeba při projektování a implementaci takového přístupového systému klást velký důraz na zabezpečení komunikace i přístup k síťovým prostředkům

Z pohledu projektanta se pak jako největší výhoda že se nemusí v mnoha případech zabývat projekcí komunikačních tras. V projektech pro tyto systémy tak není potřeba zakreslovat dvojí kabeláž – strukturovanou pro IP síť a vyhrazenou sběrnicovou pro přístupové kontroléry, využije se právě stávajících nebo nově projektovaných tras strukturovaná kabeláže. Proces přípravy projektu se tím může zjednodušit a urychlit. Nevýhodou jsou zde omezení daná strukturou ethernetových sítí. Zde patří pokud pomineme vyšší nároky kladené na projektanta IP přístupových systémů, hlavně z důvodu nutnosti znalosti parametrů sítí, jejich topologie atd., mezní délku ethernetového segmentu mezi aktivním síťovým prvkem čtečky, která je dána hranicí 100 m.

Z pohledu instalačního technika i zde najdeme většinou pozitiva, ale existuje samozřejmě i několik nedostatků. Mezi výhody patří určitě zjednodušení a zlevnění instalace kabeláže. To bude pro instalačního technika asi největší přínos, protože díky využití již vybudované strukturované kabeláže tak rozvod komunikačních sítí neřeší vůbec. Zbývá mu jen klasické natažení kabeláže mezi čtečkou a kontrolérem (pokud není čtečka taky vybavena pro přímou IP komunikaci) a pak mezi kontrolérem a standardními dveřními prvky. Komunikaci kontroléru s nadřazenými systémovými prvky vyřeší připojením kontroléru do nejbližší ethernetové síťové zásuvky. Další výhodou jsou definované parametry kabeláže. U strukturované kabeláže pro ethernetové rozvody je poměrně snadné zajistit dodržení požadovaných parametrů. Výraznou úlevou pro technika pak určitě bude eliminace zemních smyček, ručení a zakončování. [4]

PoE (Power of Ethernet)

Systém napájení PoE (Power of Ethernet – napájení přes ethernet) lze určitě brát jako jeden z největších přínosů systémů postavených na IP technologiích. Po jediném kabelu, navíc jednoduše a levně dostupném a často už i předpřipraveném, totiž lze přenášet jak

komunikační data tak i napájení koncových prvků. Podmínkou samozřejmě je aby koncový prvek byl osazen PoE rozhraním, které umožní napájení po ethernetovém kabelu nejen jeho ale i k němu připojených prvků (čtečky, signalizační zařízení, dveřní zámek, atd.) Určitou nevýhodou systému PoE je relativně malý výkon, který lze přenášet. Podle standardu IEEE 802.3af je to cca 15 W, z čehož je pro koncové zařízení garantováno 12,95 W. To postačí pro provoz malého 1-2 čtečkového kontroléru, většinou i pro napájení nízko odběrového zámku. Tento stav se v blízké budoucnosti začne lepšit, a to díky standardu IEE 802.3at, s ním kompatibilní prvky budou moci využívat příkonu až 25 W, což bude stačit i pro větší výkonnější kontroléry. [4]

Obr. 8: IP čtečka na principu PoE

5 IDENTIFIKAČNÍ METODY

Kvalita jakéhokoliv automatizovaného přístupového systému je závislá téměř výhradně na kvalitě identifikačního mechanismu. Je-li identita autorizovaného uživatele ověřena v rozsahu povolené odchylky, je systémem zprostředkován přístup do prostředí s řízeným přístupem, v opačném případě je přístup zamítnut. Existuje velké množství metod zabezpečujících identifikaci uživatele a tvořících základ přístupových systémů. Mechanismus ověřování identity uživatele je obecně založen na tom,

- co zná pouze uživatel - například heslo,
- co uživatel vlastní- například identifikační předmět, a nebo na tom,
- co je pro uživatele charakteristické - například otisk prstu.

Ve stejném duchu pak říkáme, že je použita

- identifikace heslem (identifikace založená na znalosti hesla),
- identifikace předmětem (identifikace založená na vlastnictví předmětu) a
- biometrická identifikace (identifikace založená na biometrických charakteristikách člověka)

5.1 Identifikace heslem

Tradiční metoda pro identifikaci uživatele je tajné heslo, které musí uživatel sdělit přístupovému systému, žádá-li o povolení vstupu do prostředí s řízeným přístupem. Výhoda identifikace založené výhradně na hesle je, že může být po technické i programové stránce realizována velice jednoduše, a tím i levně. Nicméně, identifikační systém na heslo má mnoho nevýhod, které v praxi omezují jeho použití na aplikace s minimálními bezpečnostními požadavky.

Identifikace založená výhradně na hesle velice často selže z mnoha důvodů. Například je-li uživateli dovoleno, aby si je utvořil sám, má snahu zvolit si takové heslo, které se mu lehce pamatuje - a pak je lehce uhádnutelné. Nebo je-li uživateli heslo vygenerováno z náhodné kombinace znaků, velmi často si takové heslo někam poznamená, a pak je obtížně zapamatovatelné. Identifikační systémy založené výhradně na hesle musí mít solidně zabezpečený mechanismus pro generaci, distribuci a užití hesel.

Charakteristika dobrého hesla:

- je distribuováno zabezpečeným způsobem,
- obsahuje malá i velká písmena, číslice a další znaky dostupné na klávesnici,
- má dostatečnou délku - alespoň 6 znaků,
- nejde o obvyklé slovo nebo známou frázi,
- je nepravděpodobné - nelze jej odvodit ze znalosti osoby vlastníka,
- je často obměňované - alespoň každé dva měsíce,
- není nikde poznamenáno.

Z uvedené charakteristiky je zřejmé, že požadavky kladené na správu kvalitního hesla jsou značné a že identifikace heslem může být účinná pouze tehdy, je-li heslo řádně spravováno. A to je v praxi poměrně vzácný případ.

Vzhledem k tomu, že heslo může být zachyceno při přenosu k cílovému uzlu, a také proto, že časté změny hesla jsou pro uživatele zatěžující, je vhodnější, když systém zašle výzvu v podobě náhodné zprávy a uživatel jako heslo vrátí správnou reakci na tuto zprávu - např. její zašifrování tajným klíčem apod.

5.2 Identifikace předmětem

Obecné označení pro identifikační předmět, který potvrzuje identitu svého vlastníka, je token. Token musí být jedinečný a obtížně padělatelný. Tokeny používané v automatizovaných identifikačních systémech jsou vybaveny informací, která je používána při provádění identifikačního protokolu. Vzhledem k tomu, že informace uložená na identifikačním předmětu je jedinečná, musí být zabezpečena proti duplikaci nebo krádeži.

Největší hrozba pro bezpečnost takovéhoto typu systému spočívá v tom, že identifikační předmět může být ukraden nebo padělán. Tato hrozba může být zmírněna tím, že identifikační systém požaduje nejen token, ale i heslo (v případě výhradně číselné kombinace je to PIN - personal identification number). Jedná se tedy o kombinaci dvou identifikačních metod - identifikaci heslem a předmětem. Bez znalosti hesla je ukradený nebo padělaný token identifikačním systémem odmítnut.

Používané identifikační předměty jsou:

- Tokeny pouze s pamětí (magnetické, elektronické nebo optické karty) - jsou obdobou mechanických klíčů; paměť obsahuje jednoznačný identifikační řetězec,
- Tokeny udržující hesla - vydají určený kvalitní klíč po zadání jednoduchého uživatelského hesla,
- Tokeny s logikou - umějí zpracovávat jednoduché podněty typu: vydej následující klíč, vydej cyklickou sekvenci klíčů,
- Inteligentní tokeny (smart cards) - mohou mít vlastní vstupní zařízení pro komunikaci s uživatelem, vlastní časovou základnu, mohou šifrovat, generovat náhodná čísla apod.

I přes nesporné výhody, které používání identifikačních předmětů s sebou přináší, je stejně jako u hesel hlavní nevýhodou jejich přenositelnost. Tato vlastnost má u obou identifikačních metod za následek, že pouhá znalost hesla či vlastnictví identifikačního předmětu umožňuje komukoli vydávat se za někoho jiného, než ve skutečnosti je.

5.3 Biometrická identifikace

Biometrická identifikace je založena na automatizovaném zjišťování a porovnávání jedinečných biologických charakteristik uživatelů přístupového systému. Biometrické charakteristiky (biometriky) jsou měřitelné fyziologické nebo chování se týkající vlastnosti, které mohou být využitelné pro ověření identity jednotlivce.

Biometrické charakteristiky nejčastěji zahrnují:

- otisky prstů
- tvar ruky
- obličej
- hlas
- podpis
- obraz sítnice
- obraz duhovky atd.

Původně byly biometrické techniky používány ve specializovaných zabezpečovacích aplikacích, avšak v současné době nacházejí stále širší uplatnění i ve veřejném sektoru (bankomaty, vyplácení sociálních dávek, apod.).

5.4 Porovnání identifikačních metod

Hesla lze použít pouze pro nejnižší stupeň zabezpečení. Vyžadují poměrně komplikovanou správu a lze se jich relativně snadno zmocnit. Jsou přenositelná.

Tokeny lze použít pro vyšší stupeň zabezpečení. Lze se jich však relativně snadno zmocnit. Jsou přenositelné.

Kombinace tokenu a hesla (PIN) lze použít pro poměrně vysoký stupeň zabezpečení. Tato kombinace je značně odolná při odcizení nebo ztrátě tokenu, avšak není odolná vůči zapůjčení tokenu a vyzrazení hesla - jsou přenositelné.

Biometriky lze použít pro nejvyšší stupeň automatizovaného zjišťování a porovnávání zabezpečení. Nelze je ztratit ani jednoduše přenášet a představují jedinečný identifikátor uživatele - jsou nepřenositelné.

Souhrnně však hesla, identifikační tokeny i biometriky mohou být podrobeny útokům. Heslo může být uhodnuto, token může být ukraden a biometrika může být sofistikovaně napodobena. Tyto hrozby mohou být výrazně zmenšeny použitím jednotlivých identifikačních metod ve vzájemné kombinaci.

Vzhledem k tomu, že biometrická zařízení je obtížné oklamat, je ověření identity uživatele pomocí biometrik mnohem spolehlivější než při pouhém používání hesel nebo identifikačních předmětů, případně kombinace tokenu a hesla. Vhodná příležitost pro integraci biometrik do identifikačních procesů se naskytne tehdy, podaří-li se zautomatizovat verifikační proces tak že uživatele příliš neobtěžuje.

Biometriky v žádném případě nepředstavují všelék pro všechny možné problémy spojené s identifikací jednotlivce. Svými možnostmi však představují prostředek, který je v identifikačních nástrojích nezastupitelný a bez něhož nelze v současné době realizovat zabezpečovací projekt nejvyšší úrovně. [4]

6 PROSTŘEDKY IDENTIFIKACE OSOB

6.1 Magnetický systém

Tento identifikační systém používá jako identifikační médium karty velikosti kreditních karet, jiné provedení zde není možné, protože pro čtení dat musí být karta protažena čtecí hlavou. Základem je klasický magnetický pásek, kdy se po zmagnetizování vytvoří množství malých permanentních magnetů. Stav těchto magnetů tvoří binární rozhodování:

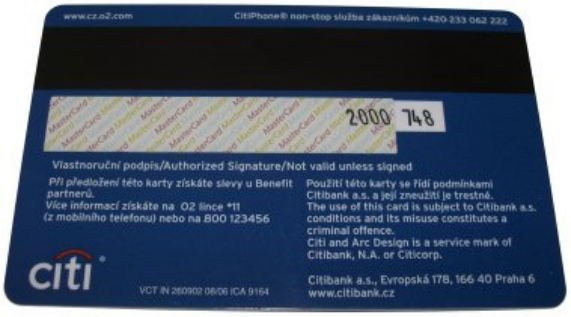
- Zmagnetováno - logická 1,
- Nezmagnetizováno – logická 0.

Standard ISO definuje 3 stopy záznamu

- 1.stopa - 79 B, numerické nebo alfanumerické znaky
- 2.stopa - 40 B, pouze numerické znaky
- 3.stopa - 107 B, pouze alfanumerické znaky

Výhodou magnetických karet je že data jsou dynamická, to znamená že uložený záznam lze později kdykoli přepsat nebo aktualizovat. Životnost uložených dat a karty je vysoká, udává se 5 až 6 let. Nevýhodou je možnost poškození dat při vystavení silnému magnetickému poli, nebo při poškrábání magnetické vrstvy, což se může stát velice snadno, poté se karta stane nečitelnou a je nutné ji vyměnit.

Obr. 9: Čtečka magnetických karet



Obr. 10: Magnetická karta

6.2 Optický systém

Jedná se v podstatě o identifikaci čárovým kódem. Princip identifikace je v tom, že v kódu je uložena číselná hodnota, podle které je pak nalezena v databázi. Čtení kódů probíhá pomocí laserového paprsku. Patří mezi nejlevnější a nejjednodušší médium. V podstatě je to seskupení černých proužků na bílém podkladu. Šířka v podélném směru představuje pro čtečku logickou informaci. Snímač vysílá světelný paprsek a sleduje, zda je odražen na bílém pozadí nebo pohlcen černým proužkem. První a poslední proužky slouží k synchronizaci. Pro snadné zkopírování nelze použít v bezpečnostních systémech, ale např. v knihovnách, supermarketech atd. Mechanické opotřebování karty je velmi malé, cena snímače, jeho umístění a použití je v podstatě stejné jako u magnetického systému.

Obr. 11: Čtečka čárových kódů

Obr. 12: Čárový kód typu EAN-13

6.3 Kontaktní systém

Jak už z názvu vyplývá tak k identifikaci je potřeba kontaktu identifikačního média a čtečky. Média mají podobu kovového pouzdra nebo kreditní karty a jsou opatřeny kontaktním polem. Propojením dojde k zapojení čipu do obvodu, může probíhat obousměrná komunikace. Nevýhodou je omezená životnost mechanických částí čtečky, která dost závisí na počtu uživatelů a jejich přístupu k zařízení. Jako identifikační média se používají čipové karty a kontaktní čipy Dallas.

Kontaktní čipová karta

Čipová karta je nejběžnějším druhem hardwarového klíče. Jde v podstatě o plastikovou kartu, která má ve svém těle vložen čip. Nejčastější technologií vložení čipu do karty je vyfrézování dutiny v kartě o rozměru čipu a následné vlepení čipu do dutiny. Dnes se zásadně využívají karty dle ISO 7816-1. Jedná se o dva rozměry karty. S oběma se běžně setkáváme. Velký rozměr mají platební karty a malý rozměr SIM - karty mobilních telefonů.

Čipové karty se dělí na paměťové, ty jsou osazené pouze paměťovými registry a na procesorové, které mají jednočipový procesor schopný vykonávat příkazy. Procesorové karty musí mít svůj operační systém, jinak by nebyli schopny příkazy vykonávat.

Kontaktní čipové karty mají na sobě zpravidla kontakty, pomocí kterých se propojují se čtečkou. Napájení rovněž obdrží ze čtečky. Čtečka čipových karet se správně označuje jako terminál.

Využití čipových karet:

- Autentizace držitele,
- Vytváření elektronického podpisu,
- Šifrování dat,
- Elektronická peněženka atd.

Obr. 13: Čtečka čipové karty s elektronickým zámkem

Obr. 14: Čipová karta

Kontaktní čip Dallas

Identifikační čip je kontaktní identifikační médium. Přiložením čipu ke snímací hlavě dojde k přečtení kódu a tím k jednoznačné identifikaci konkrétní osoby.

Použité ID čipy jsou produktem firmy Dallas Semiconductor. Obsahují jedinečný 64-bitový kód a výrobce garantuje, že nikdy nevyrobí dva identické čipy, což zaručuje nezaměnitelnost identifikace. Jsou odolné proti mechanickému poškození, vlhku, mrazu i mastnotě.

Obr. 15: Čip Dallas

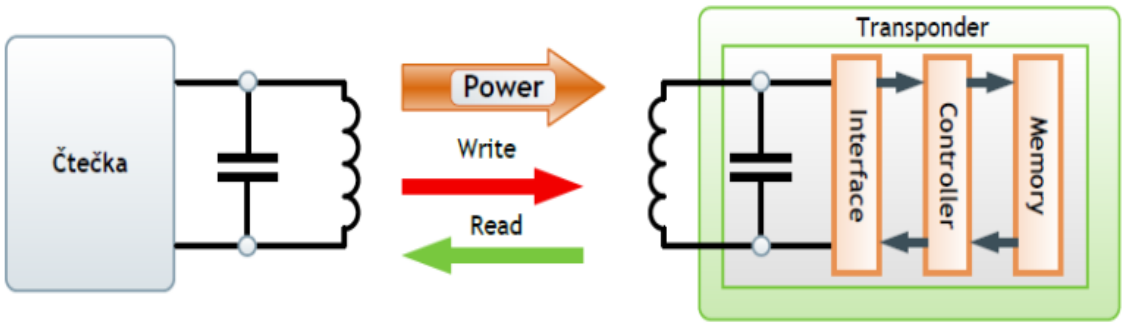
Obr. 16: Čtečka Dallas EDK2

6.4 Bezkontaktní systém

Jedná se o radiofrekvenční komunikaci, která je založena na radiovém přenosu dat mezi čtečkou a identifikačním médiem. Technologie se nazývá RFID. Identifikační systém se skládá z několika hlavních prvků, kterými jsou transpondéry (tagy), čtečky a podpůrné systémy (řídící počítače, databáze, komunikační sítě). Informace jsou v elektronické podobě ukládány do malých čipů-tagů, ze kterých je lze následně načítat a opakovaně přepisovat pomocí rádiových vln, současná čtecí zařízení dokážou najednou načíst až několik set tagů za minutu.

Bezkontaktní paměťové prvky se vyznačují tím, že nemají při identifikaci pevný kontakt s čtečkou, komunikace probíhá pouhým přiblížením. Standardní vzdálenost 5 - 10 cm, lze i větší, například na vzdálenost 25 cm, čtečky jsou standardně napájeny 12 V, pro větší vzdálenost mohou vyžadovat i 24 V.

Čtečka nejprve vysílá na svém nosném kmitočtu elektromagnetickou vlnu (stanovena většinou výrobců na 125 kHz), která je přijata anténou transpondéru. Indukované napětí vyvolá elektrický proud, který je usměrněn a nabíjí kondenzátor v transpondéru, tato akce trvá cca 50 milisekund. Uložená energie je použita pro napájení logických a rádiových obvodů transpondéru. Když napětí na kondenzátoru dosáhne minimální potřené úrovně, spustí se logický automat či mikroprocesor (tedy řídící obvody uvnitř transpondéru) a transpondér začne odesílat odpověď čtečce. Podle toho, zda vysílá logickou 1 nebo 0 se zatěžuje nebo odlehčuje indukční pole čtečky a tím vzniká amplitudová modulace indukčního pole vysílaného čtečkou. Čtečka signál upraví na plně digitální elektrický signál a předá do systému k dalšímu zpracování, kde se rozhodne o vpuštění osoby do objektu. Doba identifikace obvykle netrvá déle než 100 – 120 milisekund.



Obr. 17: Princip technologie RFID

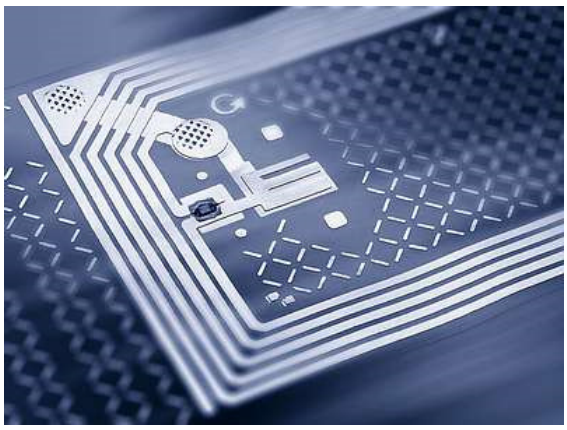
Jako základní nosič informace je použita pasivní identifikační karta (transpondér) nejčastěji formátu EURO o rozměrech 85 x 54 / 2,2 mm s hmotností okolo 5 g. Na čelní stranu je možno umístit text a fotografii a lze ji použít současně jako služební průkaz. Typy transpondérů se liší velikostí, tvarem, dosahem a funkcí. Mimo běžné velikosti identifikační karty EURO jsou vyráběny různé štítky, skleněná pouzdra apod. Hlavní verze transpondérů je typ R / O (read only) tedy nepřepisovatelné, do kterých je při výrobě vložen originální 64 bitový kód. Používá se jako průkaz jednoznačné identifikace. Typ R / W (read / write) je přepisovatelný v celém rozsahu možné kapacity paměti. Slouží jako programovatelný nosič dat. Umožňuje ukládat, číst a měnit identifikační kódy a jiné údaje. Programování se uskutečňuje na dálku, na vzdálenost danou dosahem čtecího zařízení. Vzdálenost na jakou je možno přeprogramovat transpondér R / W je zhruba polovička dosahu pro čtení.

Aktivní karty obsahují miniaturní baterii s dlouhou životností a mají zpravidla dvojnásobný čtecí dosah oproti kartám pasivním. Jsou i odolnější proti silným zdrojům VF rušení. Jejich pořizovací náklady jsou však vyšší.

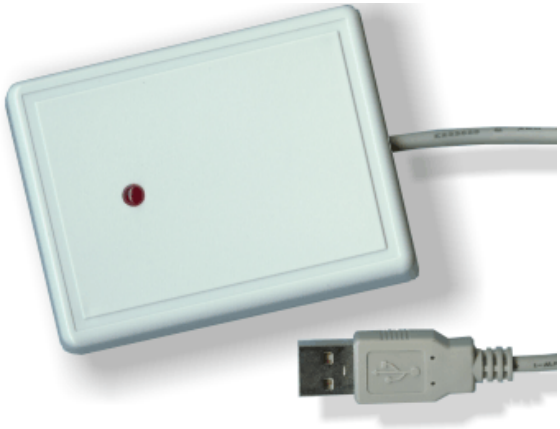
V současné době představuje technologie RFID nejdokonalejší uložení kódu - odolnost vůči pořízení kopie.

Vlastnost celého systému záleží na výběru antény, ty se vyrábějí v různém provedení. Každá anténa má vlastní vyzařovací charakteristiku elektromagnetického pole, které vytváří ve svém okolí.

- Integrovaná anténa je pevnou součástí čtecího zařízení, dosah bývá desítky cm,
- Tužková anténa se používá pro skryté provedení zámkové jednotky. Dosah bývá cca 10 cm,
- Rámová anténa v provedení pod omítku nebo do výplně stěn má dosah 50 - 150 cm,
- Indukční smyčka, jejichž rozměr není omezen s dosahem 1 - 2 m. [10, 2]



Obr. 18: Struktura RFID



Obr. 19: RFID čtečka, 125 kHz

Obr. 20: Anténa pro RFID

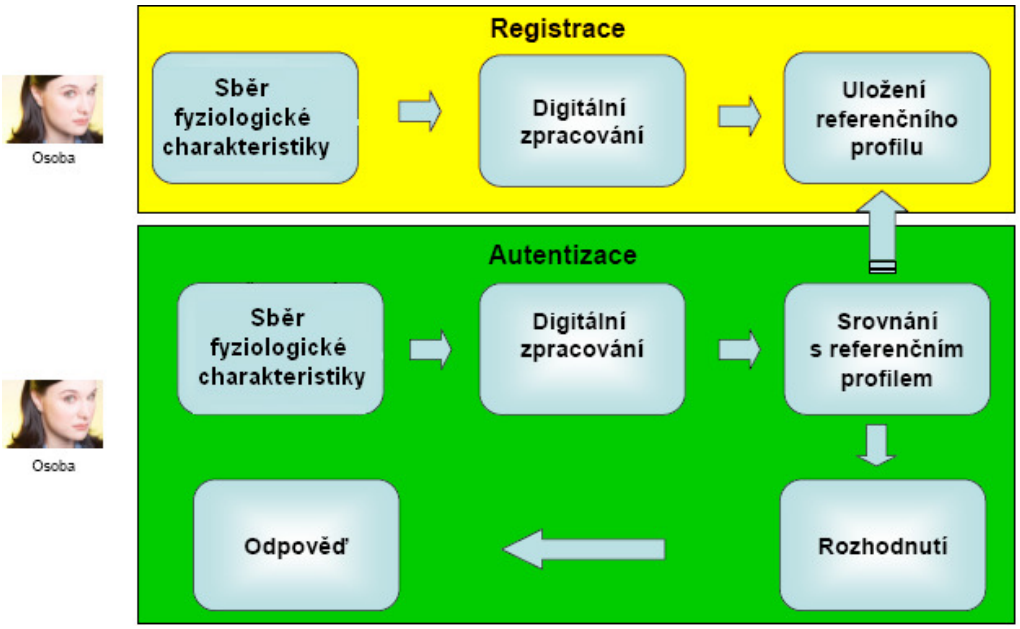
7 BIOMETRICKÁ IDENTIFIKACE

Využití biometrických systémů je poměrně široké a aplikací stále přibývá. Setkat se s nimi můžeme všude tam, kde je nutné zabezpečit vstup proti nepovolaným osobám, ochránit osobní data nebo identifikovat člověka například v biometrických pasech, v docházkových systémech, v lékařství při identifikaci pacienta. Biometrické systémy se v dnešní době také zabudovávají i do počítačů nebo telefonů.

Biometrických systémů je celá řada. Všechny ale vycházejí z nějaké fyziologické charakteristiky, která je pro každého člověka jedinečná a která se dá nějakým způsobem měřit (proto bio - metrie), zaznamenat a následně vyhodnotit. Biometrické prvky mohou být buď tzv. stabilní - např. otisk prstu, geometrie ruky, obraz sítnice nebo duhovky, vzorek DNA, a dokonce i tvar ucha, nebo dynamické, mezi které patří styl chůze, pohyby rtů, analýza dynamiky stisku kláves (např. psaní na klávesnici), apod.

Z nasnímaných dat vybere biometrický systém nejvýraznější rysy specifické pro uživatele (např. struktura papilárních linií na povrchu kůže prstu, uspořádání žilek na sítnici, výška a tón hlasu, aj.) a z nich pak vytvoří tzv. šablonu (etalon). Etalon se uloží do databáze a každé ověřování totožnosti pak probíhá jako porovnání nového měření s uloženým profilem.

Využití biometriky v zabezpečovacích systémech přináší vysokou míru jistoty a bezpečnosti. [4]



Obr. 21: Schéma biometrického autentizačního procesu

Možnosti ukládání etalonů:

- Uložení etalonu v biometrickém čtecím zařízení,
- Uložení etalonu ve vzdálené centrální databázi,
- Uložení etalonu v přenosných totenech například v čipové kartě,
- Libovolná kombinace předcházejících způsobů.

Výhodou první možnosti je rychlá reakce a nezávislost na externích procesech nebo datovém spojení při zpřístupnění etalonu. Nevýhodou je ovšem že etalony jsou svým způsobem zranitelné a jsou závislé na přítomnosti a funkčnosti daného čtecího zařízení. V případě závady je pak nezbytné znovu nainstalovat databázi etalonů nebo opětovně projít etapou zápisu.

Druhá možnost, uložení etalonu ve vzdálené centrální databázi, je možnost, která se zcela přirozeně nabízí pro IT systémy. V takovém případě je třeba myslet na to, že jakmile je síť mimo provoz, tak biometrický systém je vyřazen z činnosti.

Uložení etalonu v tokenu, je lákavé ze dvou důvodů. Předně nevyžaduje žádné lokální nebo centrální ukládání etalonů. Uživatel si nosí svůj etalon s sebou a může jej použít všude tam, kam má povolen autorizovaný přístup. Nevýhodou je vyšší cena a složitost biometrického systému z důvodu kombinace tokenového a biometrického čtecího zařízení na všech identifikačních místech.

Kombinace předcházejících řešení, může poměrně efektivně eliminovat nevýhody jednotlivých samostatných možností a používá se všude tam, kde je položen důraz na funkčnost systému za všech okolností. [4]

7.1 Měření biometrických metod

Pro měření biometrie se používá míra pravděpodobnosti chybného odmítnutí FRR - False Rejection Rate. To znamená, že správnou osobu vyhodnotíme chybně, neboli vyhodnocení dvou biometrických vzorků od stejné osoby dopadne odlišně.

FRR = počet neshodných vzorků/celkový počet

Míra chybného přijetí FAR - False Acceptance Rate znamená, že systém přijme odlišný vzorek jako správný. To znamená, že systém vyhodnotí dva odlišné vzorky jako totožné.

FAR = počet shodných porovnání rozdílných vzorků/celkový počet

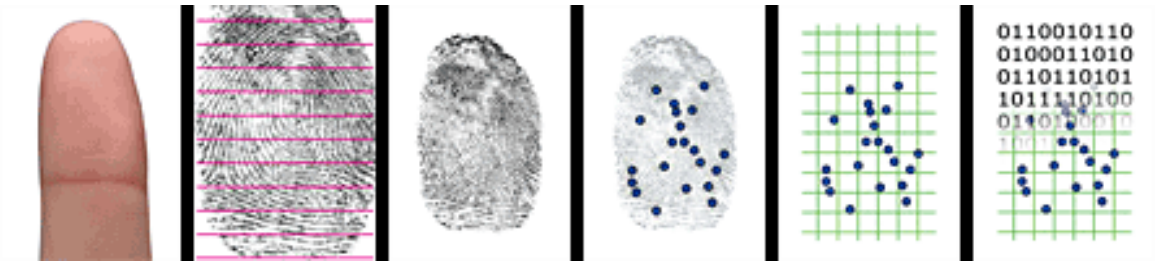
Biometrické systémy mají různé citlivosti nastavení. Pokud citlivost nastavíme jedním směrem, zařízení bude náchylné k odmítání i oprávněných osob. Pokud je nastavíme druhým směrem, bude propouštět osoby oprávněné, ale i osoby nežádoucí. Podle praktického použití, prostředí a požadavků použijeme správné nastavení, abychom eliminovali výše uvedené negativní vlivy. [4, 13]

7.2 Přehled základních biometrických metod

7.2.1 Otisk prstu

Jedná se o nejznámější a nejpropracovanější biometrickou metodu. Pro porovnání otisků prstů se používají identifikační body (markanty). Tyto body se nacházejí v rýhách vzoru. Identifikační bod se může skládat z některých následujících objektů: rozdvojení – konce dvou rýh vytvářejí vidličku, krátká rýha, ukončovací rýha, ohrazení – spojení dvou rýh vytvářející vidličku na obou koncích, izolované body, roztrojeni atd. Některé z těchto bodů se vyskytují častěji než ostatní. Při porovnání otisků se sleduje jak přítomnost markantů, tak i jejich umístění v daném otisku. Otisk prstu obsahuje v průměru 75 – 175 identifikačních bodů. V praxi není stanoven přesný počet bodů nutný k rozlišení mezi dvěma otisky.

Zásadou pro zabezpečovací techniku je, že se otisky uchovávají ve srovnávacím archivu pouze v digitální formě.



Obr. 22: Otisk prstu v digitální formě

Z obrázku naskenovaného článku prstu jsou expedovány speciální znaky a archivovány jako biometrický klíč. Žádné otisky prstů nejsou ukládány, nýbrž pouze přeměněny na binární kód, který nelze znovu proměnit na otisk prstu. Nejdůležitějším prvkem této metody jsou tedy snímače otisků prstů.

V dnešní době se na trhu pohybuje několik typů snímačů, jako jsou například optoelektronické, kapacitní, teplotní, elektroluminiscenční, radiofrekvenční a nově také možnost multispektrální analýzy otisku. Všechny tyto technologie poskytují poměrně širokou škálu možností, přičemž každý má své výhody a nevýhody, které je třeba zvážit. [4]

Optoelektronické snímače:

Jedná se o nejpoužívanější snímače v dnešní době, které umožňují jednoduché sejmutí otisku CCD detektorem, využívající osvětlení celé plochy prstu. Odrážené světlo pak prochází luminoforní vrstvou k CCD detektoru, kde se vytvoří obraz otisku. Výhodami této technologie je vysoká kvalita čtení, statická odolnost a rezistence vůči vlivům okolního prostředí. Na druhou stranu je třeba si dát pozor na některé nevýhody. Například znečištění nebo poškození prstu může způsobit jeho nekorektní vykreslení na otisku. Stejně tak otisk zůstávající na detektoru může zkreslit další pořizované otisky.

Kapacitní snímače:

Další rozšířená technologie, která využívá rozdílu kapacitního odporu mezi deskou snímače a povrchem prstu. Papilární linie jsou k podložce přilehlejší než mezery mezi nimi, mají tedy vyšší odpor. Poměrně jednoduchý princip přitom zajišťuje vysokou kvalitu čtení. Snímače také příjemně překvapí malým rozměrem a nízkou cenou. Bohužel doba jejich životnosti je relativně malá, vlivem statické elektřiny se postupně ničí a je nutné je v rozmezí přibližně tří let měnit. I když finančně tato okolnost může být nevýznamná, přece jen znamená potíže z organizačního hlediska.

Teplotní snímače:

Často používané jsou také teplotní snímače, které pořizují otisk prstu snímáním rozdílných teplot, které mají papilární linie a mezery mezi nimi. Uživatel při snímání přejíždí prstem přes citlivou plochu, obraz se skládá do digitálních pásů a poté do výsledného otisku. U této metody existuje nebezpečí, že při několikanásobném přejíždění prstem přes snímač bude sejmuta vždy jiná část prstu, což výrazně limituje možnost vytvoření databáze otisků. Navíc tyto snímače neposkytují dostatečně vysokou kvalitu obrazu otisku, a proto nejsou pro použití v přístupových systémech vhodné.

Absolutní špičkou mezi snímači otisků prstů je Americká firma Lumidigm. Systém využívající více osvětlovacích soustav o rozdílných vlnových délkách tak dokáže prosvítit

otisk prstu a porovnat i s otiskem pod povrchem kůže, krevní řečiště a teplotu prstu. Snímač je tak maximálně odolný proti falzifikátům otisku jako třeba silikonový prst. Tato technologie umožňuje čtení při extrémních podmínkách. Navíc vyhodnocovací software dokáže dotvořit otisk v případě neúplného přitisknutí prstu na snímač. Díky multispektrální analýze lze jasně detekovat v místě přitlačení i slabý odtok krve z prstu, a jasně tak oddělit falsifikát od skutečného prstu.

Obr. 23: Zámek se čtečkou otisku prstů

Obr. 24: Čtečka otisku prstů

7.2.2 Geometrie dlaně

Vlastní zařízení používá jednoduchého principu měření 3D rozměrů dlaně (délka, šířka, tloušťka a povrch) konkrétní osoby. Dlaň se pokládá na rovnou plochu obvykle s pěti distančními kolíky a je snímaná CCD kamerou. Obraz ruky poskytuje 31 000 polohových bodů a možnost provést až 90 různých délkových měření. Systém má relativně malé nároky na paměť zařízení. [4]

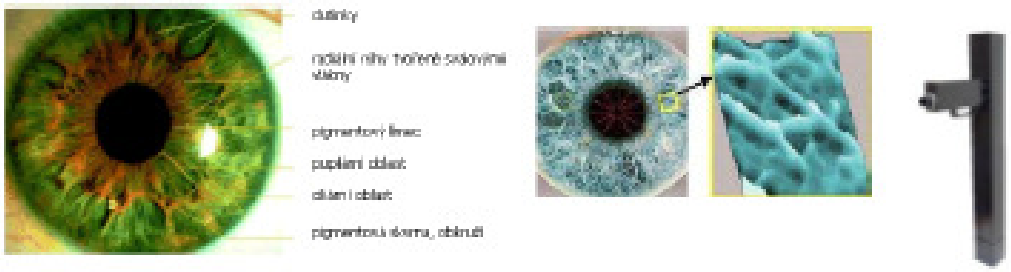
7.2.3 Geometrie obličeje

Princip je založen na srovnávání obrazu sejmutého kamerou a obrazem uloženým v paměti zařízeni. K jednoznačné identifikaci slouží tvar obličeje a poloha opticky výrazných orientačních míst obličeje, jako jsou nos, oči, obočí, lícní kosti a rty. Ukládají se pouze vzdálenosti těchto míst mezi sebou, např. vzdálenost očí, špičky nosu od jednoho oka apod. Správná technologie musí být nezávislá na změnách mimiky obličeje, změnách tváře, které přináší stárnutí, úpravy účesu apod. Algoritmy pro nalezení markantů ve spojení s

pokročilou optickou technologií umožňují identifikaci tváře v širokém rozsahu úhlů i při otočení hlavy až o 30° libovolným směrem. Systémy pracují s neviditelným infračerveným světlem, takže je tato obrazová technologie tolerantnější k okolním světelným podmínkám a v podstatě nezávislá na barvě pozadí, nalíčení tváře nebo špercích. [4]

7.2.4 Duhovka oka

Metoda je založena na snímání duhovky, kterou má každý člověk jedinečnou. Nalezení dvou identických duhovek náhodným výběrem je mnohonásobně méně pravděpodobné než nalezení dvou identických otisků prstů. Dokonce i obě duhovky jednoho člověka jsou rozdílné a jedinečné. Z tohoto pohledu neexistuje externí biometrická charakteristika člověka, která by byla spolehlivější. Snímače duhovky se používají pro vyšší bezpečnost. Duhovka obsahuje kolem 260 identifikačních znaků, ve srovnání s 30 - 50 znaky u otisku prstu. Používá se při ní konvenční CCD kamera, a nevyžaduje žádný intimní kontakt se snímacím zařízením. Jednotlivé konstrukce zařízení snímají duhovku buď jednoho nebo obou očí. [4, 13]



Obr. 25: Duhovka a snímač biometrických dat oční duhovky

7.2.5 Sítnice

Sítnice je povrch zadní strany oka, citlivá na světlo. Pro verifikaci sítnice se používá obraz struktury sítnice v okolí slepé skvrny získávaný pomocí zdroje světla s nízkou intenzitou a pomocí optoelektronického systému. Tento obraz je digitalizován a převeden na vzorek délky přibližně 40 bytů. Obrázky sítnice mají stejné charakterizační vlastnosti jako otisky prstů. Verifikace sítnice je velice přesná biometrická technika, avšak vyžaduje, aby se uživatel díval do přesně vymezeného prostoru a měl zaostřeno na daný bod. Tato metoda je kontaktní a její použití se redukuje jen pro vrcholně bezpečné kontrolní systémy. [4]

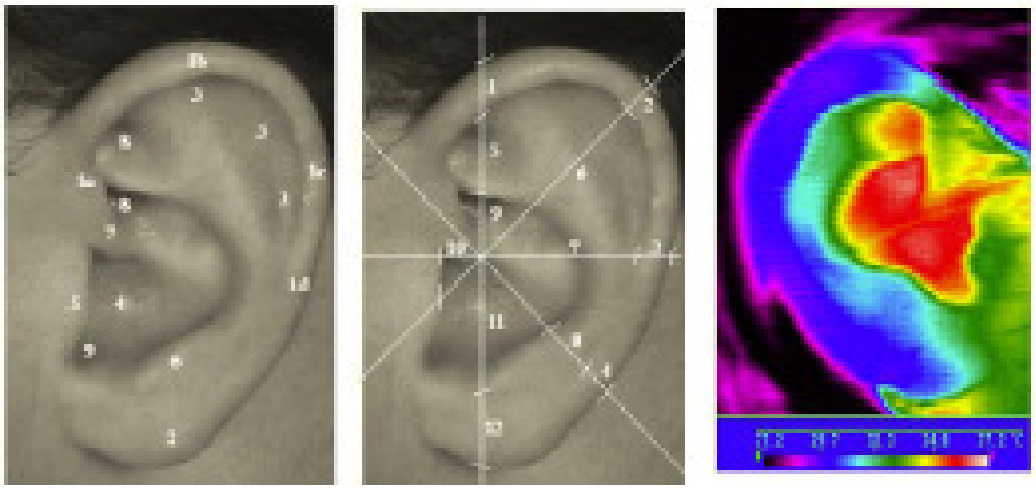
7.2.6 Krevní řečiště

Jedná se o snímání cévního uspořádání dlaně nebo hřbetu ruky. Opět je prokázáno, že obraz krevního řečiště, vytvořený cévním systémem, je pro každou osobu unikátní a relativně stabilní v průběhu jejího života. Dokonce i identická dvojčata mají rozdílná krevní řečiště. Snímání se provádí v infračerveném spektru světla, které je citlivé na vyzařované teplo, takže lze rozeznat oblasti s různou teplotou a teplé cévy zřetelně vystupují na pozadí snímku. [4]

7.2.7 Tvar ucha

Pro zpracování otisku ucha postačí snímek z černobílé CCD kamery s dostatečným rozlišením odstínů šedi. Počítačově se vytváří grafický model podle tzv. Vodorovného diagramu (způsob dekompozice metrického prostoru určený vzdálenostmi k dané diskrétní množině objektů v prostoru) - obdobně jako u grafiky obličeje. Pro identifikaci otisku ucha se používají tři metody. První metoda je podle morfologických vztahů - zjišťuje se 2D, případně 3D geometrie ušního boltce, další metodou je ověřování podle termogramu - pořizuje se termografický snímek, který mapuje rozložení tělesné teploty na boltci, poslední metoda - podle otisku struktur ušního boltce - metoda se velmi podobá metodě, která snímá otisky prstů, a proto se používá výhradně ve forenzní oblasti.

Snímání morfologických vztahů je prováděno optickým snímacím zařízením (např. CCD kamerou) ze vzdálenosti cca 0,5 až 1 metru. Ke zhotovení termogramu se používá termovizní kamera a k otisku ucha se používají otiskové metody jako u pořízení otisku prstu. [4, 13]



Obr. 26: Biometrické měření parametrů ušního boltce

7.2.8 Hlas a řeč

Pro záznam hlasu se jedná o zjištění výšky tónu, zbarvení hlasu a plynulosti a frekvence mluvy. Pro ověření pravosti hlasu určité osoby slouží v paměti uložené vzory jeho hlasu - namluvené klíčové věty. Ověření identity hlasu spočívá ve specifice lidského hlasu, ale i ve flexibilitě klíčových vět. Ani nejlepší imitátor nemůže obelstít identifikační systém bez znalosti klíčové věty. Jistý problém je při identifikaci hlasu v reálném prostředí plném jiných řečí a zvuků. Pak se tato situace řeší postupným odfiltrováním jednotlivých frekvencí zvuků, přesto ale v současné době neexistuje zatím přesný systém k docílení čistoty a jednoznačnosti identifikace hlasu. [4, 13]

7.2.9 Chůze

Jedná o identifikaci chůze - odborně řečeno bipedální lokomoce. Rozlišovacím znakem je různý dynamický stereotyp pohybu celého těla.

Celá metoda spočívá v porovnávání křivek drah, které opisují určité body lidského těla, hlavně těžiště, pohyb kyčelního nebo kolenního kloubu, temene hlavy apod. Tyto křivky jsou unikátní, a tím i vhodné pro srovnávací analýzu. Bipedální lokomoce je nová metoda, a má perspektivní využití například při identifikaci pachatele procházejícího chodbou banky, kde vzápětí žádá s pistolí v ruce o vydání peněz a jeho siluetu s kuklou zaznamená kamera, eventuálně i jeho odchod z budovy. Celá disciplína se může rozvíjet díky tomu, že se v současnosti používá čím dál tím více sledovací bezpečnostní kamerový systém v bankách, institucích, na ulicích, na parkovištích apod. [4]

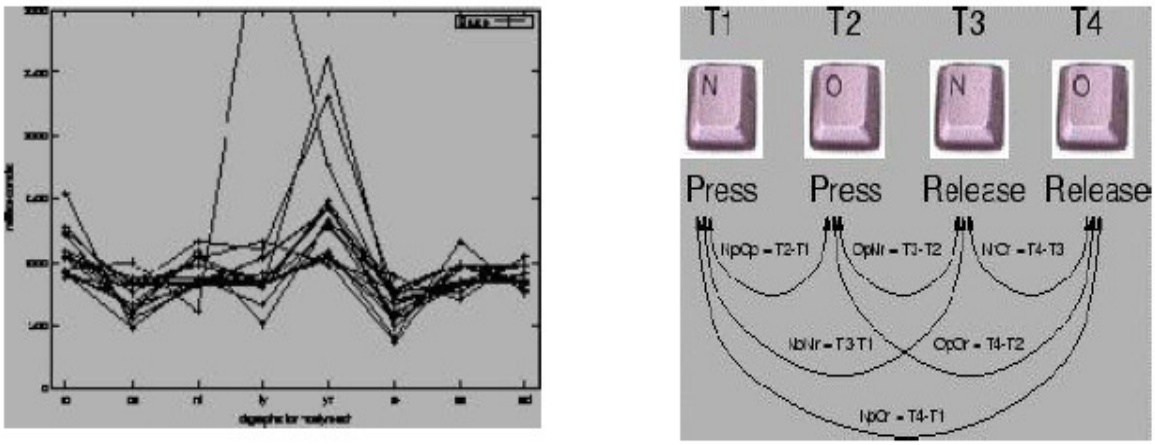
7.2.10 Podpis

Podstata spočívá v ověření identity osoby na základě jejího podpisu. K tomu je zapotřebí, aby se dotyčná osoba podepsala na speciální podložku pomocí speciálního pera. Systém ověřuje podpis osoby na základě porovnání s uloženým podpisovým vzorem, který popisuje, jak byl podpis napsán. Není tedy tak důležitá podoba podpisu či tvar písmen, ale důraz je kladen na dynamiku podpisu, provedení tahů, sílu, kterou se při psaní tlačí na podložku, rychlost psaní apod. To vše podává jednoznačnou charakteristiku libovolného podpisu. Technologie rozpoznávání je založena na porovnávání změny tlaku, zrychlení v jednotlivých částech podpisu, zarovnání jednotlivých částí podpisu, celkovou rychlost, dráhu a dobu pohybu pera na papíře a nad ním. [4]

Obr. 27: Tablet Wacom Graphire4 Classic pro zaznamenávání dynamiky podpisu

7.2.11 Psaní na klávesnici

Tato metoda je obdobou dynamického podpisu, přičemž sleduje stisk - dynamiku úhozů na klávesnici, která se u lidí liší. Sledují se časové údaje, kdy jsou klávesy drženy, a rovněž časová prodleva mezi jednotlivými stisky kláves. Dobře se hodí pro ochranu nežádoucích přístupů k osobním počítačům i ke vzdáleným informačním systémům pracujících v režimu on-line. [4, 13]



Obr. 28: Dynamika psaní na klávesnici a diagram, který jí zachycuje

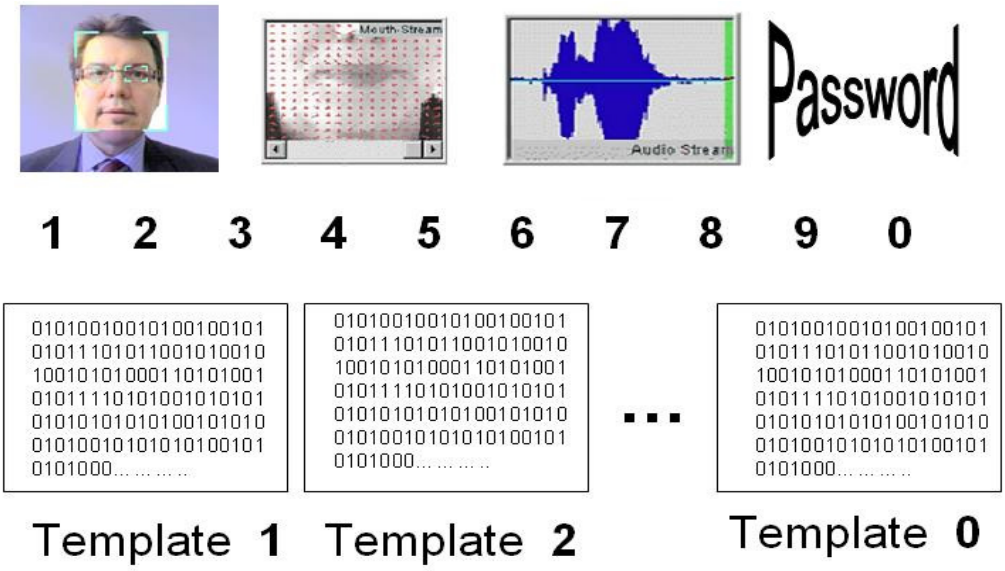
Existuje ještě mnoho dalších možností pro verifikaci a identifikaci osob, například: *Identifikace podle DNA* – vůbec nejpřesnější metoda, ale nejzdlouhavější, *plantogram* – otisk bosé nohy, *pohyb očí* - pomocí speciálních brýlí se sleduje pohyb očí, povrchové topografie rohovky a měří se intenzita odraženého světla od rohovky, *tvar článku prstu a pěsti* - jde o proměřování prstů sevřené pěsti, vrásnění článků prstů - spočívá v měření vrásek prstu mezi dvěma klouby, *pach* - lidský pach je složen asi ze 30 chemických

sloučenin, jejichž intenzita vytváří charakteristiku člověka, *odraz zvuku v ušním kanálu* - měří se intenzita pohlcení zvuku v ušním kanálku osoby, *tvar a pohyb rtů* - na obrazovce je sledována dynamika pohybu rtů při hovoru, *podélné rýhování nehtů* - metoda identifikuje nehtové lůžko.

7.3 Kombinovaná biometrie

Stále častější uplatnění nastavení přístupů jsou aplikace využívající kombinovaných metod biometrie. Pro vyšší stupeň zabezpečení a kvality vyhodnocení osob lze použít samotné kombinace biometrických metod nebo kombinace biometrických metod s metody znalostními (hesla) nebo v kombinaci s nějakým vlastnictvím (tokeny, RFID komponenty apod.).

Příklad kombinace biometrických metod pro vysoký stupeň zabezpečení:



Obr. 29: Příklad kombinované biometrie

Postup procesu je následující: Uživatel je rozpoznáván pomocí bezkontaktní metody rozpoznání obličeje, současně se automaticky vygeneruje heslo 4 číslic (možno písmena, barvy, slova apod.), uživatel postupně vysloví čtyři číslice tak, jak jdou za sebou. Při vyslovení se porovná hlas (každé číslo má v databázi svůj vzorek) a pohyb rtů (souvislost s čísly). Metoda rozpoznání kombinuje tedy čtyři procesy a výsledek je vynikající s téměř 100% jistotou identifikace dané osoby. [4]

8 MZS PRO SYSTÉMY KONTROLY VSTUPU

Používají se zejména blokovací zařízení, která provádí fyzické zablokování nebo uvolnění vstupních prvků do objektu zabezpečeného systémem kontroly vstupu. Jedná se o různé typy elektromagnetických a elektromotorických zámků, cylindrické vložky, turnikety, propusti atd. Používají se samozamykací zámky, to znamená že při každém zavření dveří se automaticky vysune závora zámku. Při výběru vhodného blokovacího zařízení jsou rozhodující funkční vlastnosti a spolehlivost, neboť tato část přístupového systému je nejvíc namáhaná. Propojení mechaniky s elektronikou umožňuje splnění všech požadavků, které uživatel od komplexního zabezpečení očekává. Tedy odolnost proti mechanickému překonání, kontrola průchodů, časové údaje, kontrola uzamčení atd.

8.1 Samozamykací elektromechanické zámky

Samozamykací elektromechanický zámek je instalován do dveří s vysokou bezpečnostní odolností. Z venkovní strany dveří je odemčen klíčem přes cylindrickou vložku nebo klikou a elektrickým impulzem. Klika zámku může být ovládána výstupním kontaktem ze čtečky karet, klávesnice, tlačítkem, apod. Tento typ zámku je určen pro vstupní, únikové, požární i průchodové dveře. Zámek může být pravolevý – obousměrná střelka.

Elektrický impulz na elektromagnetickou cívku zaaretuje pohyblivý mechanizmus v zámku a vnější klika je plně funkční pro otevření dveří. Není-li udělen tento elektrický impulz z přístupového systému je klika sice pohyblivá, ale bez možnosti otevření dveří. Na vnitřní straně dveří bývá použit systém panik. Pouhým stiskem kliky je zámek odemčen a dveře otevřeny bez použití klíče. Funkce panik je používána pro nouzové východy.

Samozamykací elektromechanický zámek je vždy po zavření dveří dvoubodově uzamčen. Po uzavření dveří je zajišťovací střelka zatlačena o protiplech v zárubni do zámku ve dveřích. Automaticky dojde k vysunutí závory a zablokování střelky zámku, a dojde k zamčení. Tyto zámky mají jednotné napájení 12 - 24 V DC. Používané zámky musí být odzkoušené Trezor testem. [11]

Možnosti nastavení zámku - ovládání prostupu:

"0" - fail secure - Klika ve směru úniku je funkční trvale (antipanic), vnější klika je funkční po přivedení napájení z ovládacího zařízení, např. čtečky.

"1" - fail safe - funkce EPS - Klika ve směru úniku je funkční trvale (antipanic), vnější klika je funkční po odpojení napájení z ovládacího zařízení, např. čtečky.

"2" - fail secure - Obě kliky jsou funkční po přivedení napájení z ovládacího zařízení, např. čtečky.

"3" - fail safe - funkce EPS - Obě kliky jsou funkční po odpojení napájení z ovládacího zařízení, např. čtečky.

Obr. 30: Samozamykací elektromechanický zámek

8.2 Samozamykací elektromotorický zámek

Elektromotorický zámek pracuje tak že po příchodu aktivačního signálu je motoricky zatažena závora dovnitř zámku a následně odblokována střelka. Zámek je odemčen a dveře je možné otevřít pouhým zatlačením.

Po uzavření dveří je zajišťovací střelka společně s hlavní střelkou zatlačena o protiplech do těla zámku a po vyskočení hlavní střelky do zárubně dojde k automatickému vysunutí závory a následnému zablokování střelky. Zámek je uzamčen ve dvou bodech a je elektromotoricky chráněn proti vysunutí závory mimo zárubeň.

V případě výpadku napájení zůstává zámek v uzamčeném stavu. Zámek je vždy možné odemknout cylindrickou vložkou z obou stran dveří nebo stiskem kliky z vnitřní strany dveří, tzv. antipanic funkce. Zámky mají jednotné napájení a to 12 - 24 V DC, 12 - 18 V AC. Nejznámějším výrobcem elektromechanických a elektromotorických zámků je firma Assa Abloy. [11]

Obr. 31: Samozamykací elektromotorický zámek ABLOY EL520

8.3 Digitální cylindrická vložka

Digitální cylindrická vložka se programuje dle potřeb zákazníka, je vhodná pro všechny Euro zámky, obsahuje paměť pro záznam přístupu, je vhodné pro síťové použití bez kabeláže. Má vysokou bezpečnost, flexibilitu, nízké provozní náklady. Digitální cylindrická vložka je zaměnitelná se standardní mechanickou vložkou.

Obr. 32: Digitální cylindrická vložka

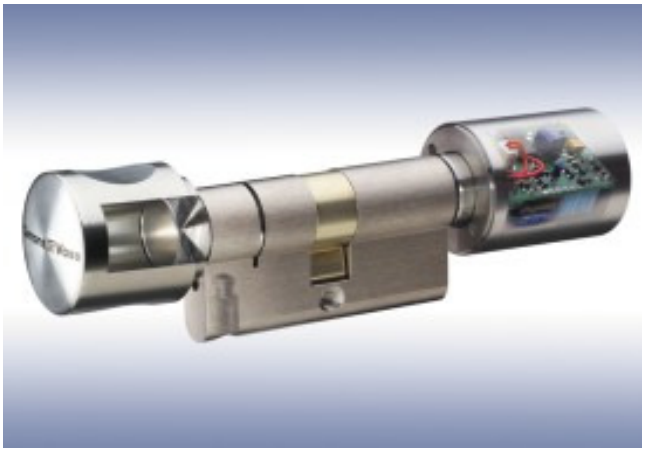
Digitální cylindrická vložka může také být kdykoli integrována do sítě. Není ovládána klasickým klíčem, ale programovatelným transpondérem pomocí radiového signálu. Jen jeden transpondér je třeba pro všechny cylindrické vložky v systému zabezpečení. Autorizace přístupu je poskytována použitím plánu zabezpečení.

Digitální cylindrická vložka je dostupná v následujících speciálních modelech:

- půl-cylindr, například pro garáže
- FH válec pro protipožární dveře a také jako volně točící se válec
- oboustranný, pro použití v vratech garáže nebo průchozích dveřích
- dále je cylindrická vložka dostupná ve verzi mosazi

Přenos dat je zabezpečený před kopírováním nepřetržitě měnícími se krypto kódy. Z bezpečnostních důvodů je veškerá elektronika umístěna na vnitřní straně dveří.

Ztracené transpondéry jsou jednoduše pro systém potlačeny (overlay-mode). Vysoký standard produktu je garantován certifikáty VdS (Sdružení německých pojišťoven). Digitální cylindrická vložka byla testována a BSI - Německý národní úřad pro bezpečnost a IT - ověřil výrobek k použití pro nejvyšší bezpečnost proti otevření.



Obr. 33: Digitální cylindrická vložka 3061

II. PRAKTICKÁ ČÁST

9 ZABEZPEČENÍ OBJEKTU SYSTÉMEM KONTROLY VSTUPU

9.1 Charakteristika objektu

Pro zabezpečení komerčního objektu systémem kontroly vstupu jsem vybral společnost zabývající se výrobou solárních systémů, zejména pak solárních panelů, půjde o zabezpečení prvního patra budovy, kde sídlí vedení firmy, projektanti a administrativní pracovníci.

Obr. 34: Zabezpečovaný objekt

V patře budovy se nachází patnáct kanceláří a zasedací místnost. Kanceláře jsou pak vybaveny osobními počítači a další drobnou elektronikou. Zabezpečení se provádí z důvodu omezení pohybu nepovolaných osob v objektu, zejména pak v souvislosti s ochranou dat, ať už ve formě psané nebo dat uložených v počítačích před případným odcizením či smazáním, a v neposlední řadě opatření na ochranu know - how. Pracovní činnost zde vykonává 40 osob, pracovní doba je od pondělí do pátku 8 – 16 hodin. Do prostoru je vstup možný pouze schodištěm na konci kterého se nachází vstupní dveře. Tyto dveře jsou tedy místem přístupu, které je předmětem zabezpečení. (viz. Obr.)

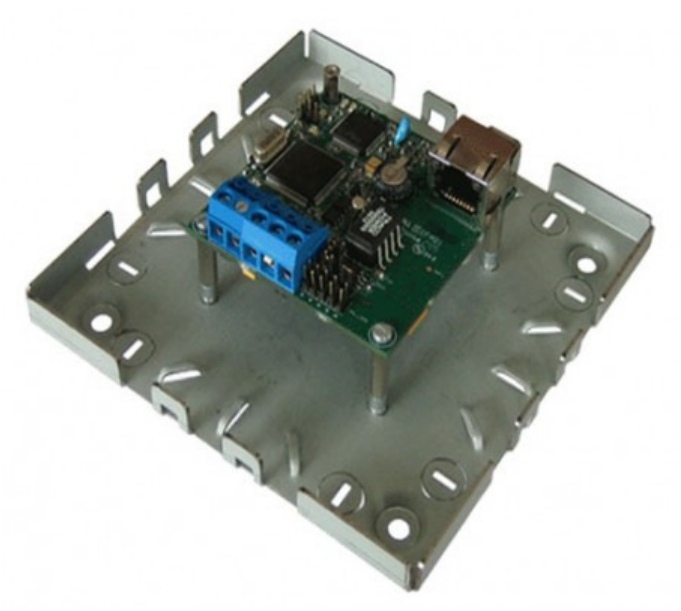
Obr. 35: Přístupové místo objektu

9.2 Použité komponenty

Pro zabezpečení jsem použil produkty firmy e-data. Půjde o zabezpečení ve třídě identifikace 3, která je založena na používání kombinace identifikačního prvku a informaci uložené v paměti. V tomto případě se bude jednat o kombinaci bezkontaktní karty a hesla. Třída přístupu je B. Použité komponenty:

1) Řídící jednotka TLC 200.8 MU

Tato řídící jednotka umožňuje připojení 1 až 8 čteček pro kontrolu vstupu, všech standardních typů. Obsahuje zabudovanou aplikaci pro kontrolu vstupu, správu systému, uživatelské nastavení a hlášení událostí. Informace jsou přístupné přes 10/100 Mbps síť Ethernet prostřednictvím libovolného standardního webového prohlížeče. Pro přístup k vestavěné aplikací pro kontrolu vstupu je třeba jednoduše vybrat síťové připojení Řídící jednotky TLC 200 MU v menu Síťová připojení ve Windows nebo napsat IP adresu řídící jednotky přímo do adresního řádku libovolného standardního web prohlížeče. Přihlášení do systému probíhá pomocí hesla a zobrazí se menu aplikace.



Obr. 36: Řídící jednotka TLC 200.8 MU

Technické údaje:

- Podporované čtečky: Legic (externí nebo interní), HID, Mifare, EM, Biometric
- Rozhraní:

Data čtečky: 1 x RS485 (max. 1400m), 2 x RS232 (max. 25m), 2 x Wiegand (max. 150m)

Řízení: RS485 (max. 400m celá síť od řídící jednotky ke všem připojeným dveřním jednotkám)

Vstupy/Výstupy (konfigurovatelné): 5 x výstupů, 2 x relé, 2 x rozhraní snímačů

- Napájení: 10 až 28V DC / 120mA
- Hmotnost: cca. 300g
- Provozní teplota: -10°C až +60°C (14 až 140F)
- Provozní vlhkost: 0 až 95%, nekondenzující
- Rozměry: 120 x 120 x 40 mm
- Temper: ANO
- Krytí: IP40
- Kryty: Kovová montážní deska s plastovým zaklepávacím krytem. Zadní a boční

kryty jsou přizpůsobeny pro připojení kabelů

2) Čtečka karet HID iCLASS RK40

Tato čtečka poskytuje vyšší stupeň zabezpečení přístupových systémů díky posílenému kódování a vzájemnému ověřování identifikační karty. Zároveň čtečka poskytuje vysoký uživatelský komfort. Čtečka je určena pro identifikační karty iClass.

Obsahuje klávesnici pro možnost zadávání PINu . Poskytuje vysoce bezpečné 64-bitové diverzifikované klíče pro vzájemné ověřování, šifrovaný přenos dat mezi kartou a čtečkou. Instalace je snadná, dále obsahuje tříbarevnou nastavitelnou indikaci a více tónový reproduktor umožňující rozlišení stavu i osobám nevidícím a neslyšícím.

Technické údaje:

- Pracovní frekvence: 13,56 MHz.
- Rozměry: 8,4 x 12,2 x 2,3 cm
- Napájení: 10 až 16V DC
- Spotřeba: 72mA max. 244mA při 12V DC
- Provozní teplota: -35°C až +65°C
- Provozní vlhkost: 5 až 95% bez kondenzace
- Hmotnost: 283,5g
- Rozhraní: Wiegand
- Krytí: IP40

Obr. 37: Čtečka HID iCLASS RK40

3) Elektromechanický úzký zámek ABLOY EL460

Po uzavření dveří se zámek automaticky uzamkne - vysune se závora a zablokuje se střelka. Stisknutím aktivované nebo panikové kliky je závora zatažena do těla zámku a následně odblokována střelka. Zámek je vždy možné odemknout cylindrickou vložkou z obou stran dveří nebo stiskem kliky z vnitřní strany dveří, tzv. antipanic funkce.

Technické údaje:

- Napájení: 12 - 24 V DC (-10%, +15%)
- Odběr: 0,13A (12 V), 0,065A (24 V), Max. 0,40 A
- Rozsah pracovních teplot: -20°C až +60°C
- Signalizace: závora zatažená, závora vysunutá, klíč odemyká/volný, klika stisknutá/volná, dveře otevřené/zavřené
- Výsun závory: 20mm, Šířka štítu: 24mm
- Povrchová úprava: štít zámku z nerez oceli

Certifikace:

Trezor test - Bezpečnostní třída 3, NBÚ - Ověření způsobilosti technického prostředku typu: 2, ČSN EN 1627 - Odolnost proti násilnému vniknutí , ČSN EN 179 - Pro únikové východy, ČSN EN 1125 - Pro panikové únikové východy , ČSN EN 1634-1 - Pro požárně odolné dveře

Obr. 38: Zámek ABLOY EL460

4) Napájení a záložní zdroj

Slouží pro společné napájení všech komponentů systému. Vnitřní zálohovací akumulátor zajišťuje nepřerušenou funkci systému i při výpadku síťového napájení. Zdroj vždy automaticky zajišťuje dobíjení akumulátoru. Pro zařízení bude stačit zálohovaný zdroj 12V-1,2 A, akumulátor 12V/1,3Ah.

5) Identifikační médium

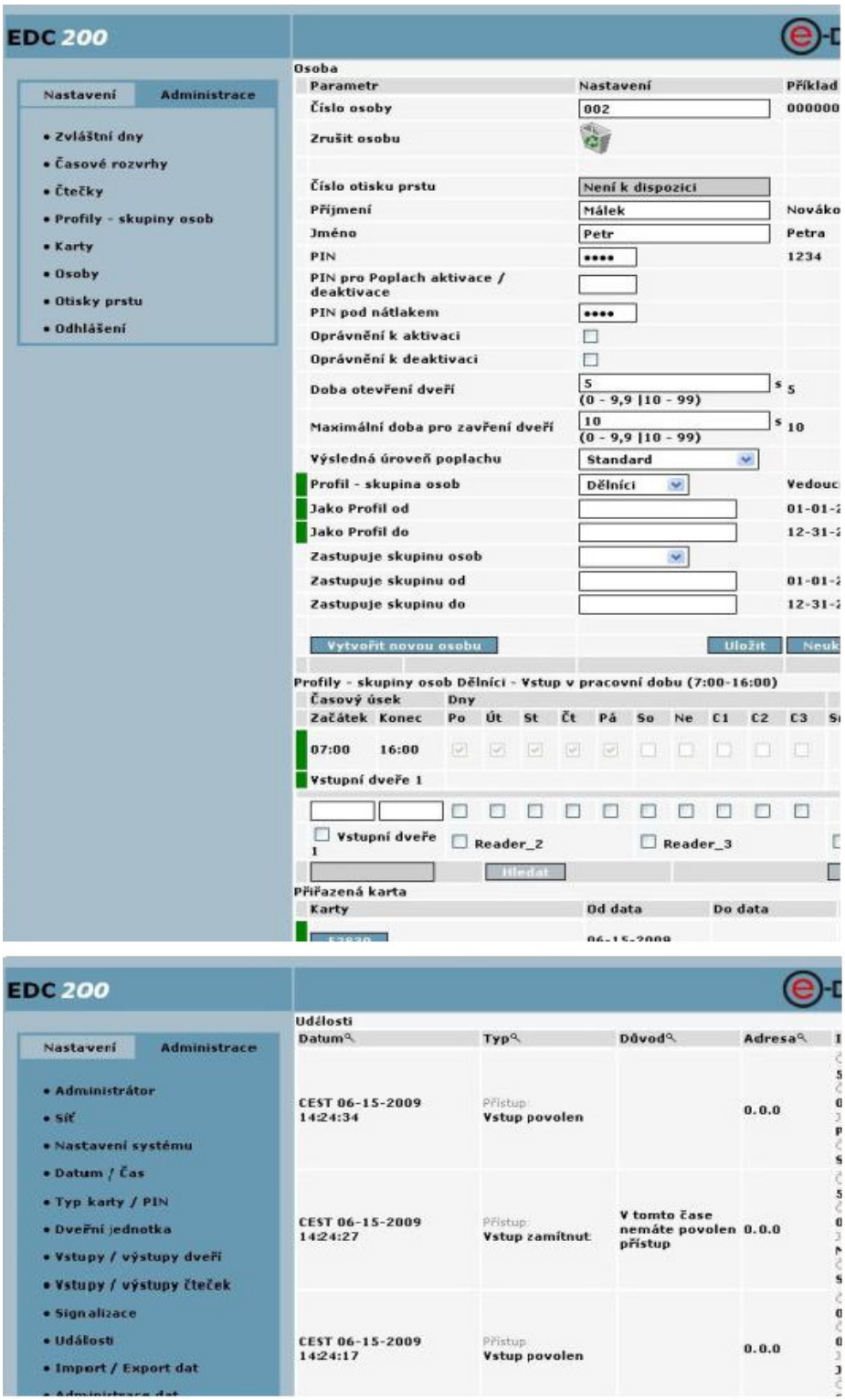
Jako identifikační médium jsem zvolil bezkontaktní karty MIFARE, které pracují na frekvenci 13,56kHz s čipem S50 ve standardním ISO formátu. Karta je vyrobena z bílého PVC materiálu s lesklým povrchem. Provozní teplota se pohybuje v rozmezí od -20 °C do 50 °C.

9.3 Zabezpečení

Řídící jednotka, napájecí a záložní zdroj budou umístěny uvnitř objektu v serverové místnosti, komunikace mezi čtečkou a řídící jednotkou bude probíhat přes rozhraní Wiegand ve vzdálenosti cca. 30m. Komunikace mezi řídící jednotkou a serverem bude realizována přes Ethernetové rozhraní. Každá osoba s oprávněním ke vstupu do objektu dostane identifikační kartu a kód. Přes libovolný webový prohlížeč se následně přiřadí tyto identifikační karty k jednotlivým osobám a jednoduše se nastaví časy a místa přístupu. Nastavení oprávnění vstupu je velmi variabilní a umožňuje povolit vstup např. pouze v určité dny, hodiny, zakázat vstup do objektu mimo pracovní dobu, o víkendu či o svátcích. Při vstupu do objektu přiloží osoba svoji kartu ke čtečce u dveří a následně zadá přístupový kód. Přístupový systém vyhodnotí přístupová práva, otevře dveře a zaeviduje datum a čas vstupu. V případě, že přístupová práva nesouhlasí, osoba se snaží vstoupit např. mimo pracovní dobu, tak přístupový systém zaeviduje datum a čas přiložení karty, ale dveře neotevře. Záznamy o všech vstupech a případně i výstupech z objektů se ukládají do databáze v přístupovém systému a na přání se mohou i automaticky odesílat přes internet. Přímo v přístupovém systému je možno přes standardní webový prohlížeč zobrazit přehled o tom, která osoba kdy v kolik hodin vstoupila. Dále je možno zobrazit pokusy o nepovolené vstupy do objektu a další události. Systém také monitoruje stav dveří. Jejich případné nezavření do určité doby, nebo násilné otevření vyvolá v nastaveném intervalu poplach. Jako organizační opatření bych doporučil pravidelnou změnu přístupového hesla.

Celková cena materiálu takového zabezpečení je cca. 35000 Kč, což je z hlediska bezpečnosti firmy přijatelné.

Po zadání IP adresy přístupového systému ve standardním webovém prohlížeči např. Internet Exploreru se zobrazí systémové rozhraní, ve kterém je možno vše nastavit:



Obr. 39: Nastavení přístupů

ZÁVĚR

Se systémy kontroly vstupu se setkáváme v běžném životě poměrně často a nejinak tomu bude i budoucnosti. Tyto systémy se jeví jako výhodná investice od základního použití například pro rodinné domky až po rozsáhlé objekty s přístupem pro tisíce osob. Tyto zařízení umožňují řídit pohyb osob v objektu, poskytovat informace o pohybu osob, tyto informace ukládat v reálném čase, a tím přispívat k ochraně objektu i režimovým opatřením. Samotný systém kontroly vstupu však nedokáže zabránit vstupu osob do objektu, proto je důležité systém vhodně integrovat do jiných systémů např. EZS či CCTV. Důležitá je pak zejména integrace s elektrickou požární signalizací, aby v případě požáru systém uvolnil únikové cesty.

V práci jsem popsal úkoly, které vykonávají tyto systémy, popsal strukturu a funkci jednotlivých prvků. Dále jsem uvedl základní požadavky, které stanovuje norma ČSN EN 50 133, což je norma pro použití systémů kontroly vstupu v bezpečnostních aplikacích. Obecně jsem popsal použití IP technologie pro komunikaci mezi komponenty, která se nyní stále častěji používá pro její jednoduchou instalaci a použití na vetší vzdálenosti. Podrobně jsem se zabýval identifikačními metodami a prostředky identifikace osob, zejména pak biometrickou identifikací, kde jsem popsal nejčastěji používané způsoby ověřování. Dále jsem uvedl a popsal mechanické prostředky používané v souvislosti s přístupovými systémy, zde se jednalo zejména o elektromechanické a elektromotorické zámky a cylindrické vložky, které tvoří důležitou součást systémů, která je prakticky nejvíce namáhaná. V praktické části jsem provedl návrh na zabezpečení konkrétního prostoru, za využití standardních zařízení pro třídu identifikace 3, používanou pro vyšší stupeň zabezpečení.

Cílem této práce bylo popsat systémy kontroly vstupů používané pro komerční objekty a stanovit požadavky na tyto systémy. Problematika v této oblasti je dosti rozsáhlá. V práci jsem postupoval tak aby čtenář pochopil jakým způsobem systém pracuje a jaké nabízí v současné době možnosti.

ZÁVĚR V ANGLIČTINĚ

With access control systems we encounter in everyday life quite often, too, it will be the future. These systems appear to be beneficial investment from the basic use such as individual houses to large buildings with access to thousands of people. These devices allow you to manage the movement of persons within the facility, provide information on movement of persons, stores this information in real time, and thereby contribute to the protection of building and lifestyle changes. Alone access control system, however, can prevent the entry of persons into the building, so it is important to properly integrate the system into other systems such as intrusion detection and CCTV. Particular importance is the integration with fire alarm, in case of a fire escape route system release. At work I have described the tasks carried out by these systems, described the structure and function of individual elements. I also pointed out the basic requirements, which sets the ČSN EN 50133, which is standard for the application of access control in security applications. Generally, I described how to use IP technology for communication between components, which are now increasingly used for its easy installation and use at greater distances. I dealt with in detail identification methods and means of personal identification, biometric identification in particular, where I described the most commonly used methods of verification. Then I said, and described the mechanical devices used in connection with the access systems, there were particular and electromotive electromechanical lock cylinders and which form an important part of the system, which is practically the most stressed. In the practical part, I made a specific proposal on the security space, using standard equipment for the class identification of 3, used for higher security level. The aim of this work was to describe the inputs used in control systems for commercial buildings and establish requirements for such systems. Problems in this area is quite large. At work I have progressed so that the reader understand how the system works, and what currently offers options.

SEZNAM POUŽITÉ LITERATURY

[3] Křeček a kol., Stanislav. Příručka zabezpečovací techniky. Marie Bubníková; Dagmar Kubešová. 3 vydání Blatná; Cricetus, 2006. 313 s. ISBN 80-902938-4.

[2] Lacký, V., Technologie komerční bezpečnosti II., Zlín: vyd. Univerzita Tomáše Bati ve Zlíně, 2004. ISBN 80-7318-231-9.

[3] Lacký, V., Technologie komerční bezpečnosti I., Zlín: vyd. Univerzita Tomáše Bati ve Zlíně, 2003. ISBN 80-7318-119-3.

[4] *Security magazín č.92*.(listopad/prosinec 2009) Praha 1 : Family media. 12 s. ISSN 1210-8723.

[5] ČSN EN 50133-1. *Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích - Část 1: Systémové požadavky*. Březen 2001, s. 28.

[6] Kindl, Jiří: Projektování bezpečnostních systémů I. 1. vyd. UTB Zlín 2004. ISBN 80-7318-165-7.

[7] Manuály a materiály firmy Honeywell

[8] ČERNÝ, JUDr. Josef ; IVANKA A KOL., Ing. Ján. *Systemizace bezpečnostního průmyslu I.*. Univerzita Tomáše Bati ve Zlíně : Univerzita Tomáše Bati , březen 2006. 135 s. ISBN 80-7318-402-8.

[9] Katalog produktů firmy AMBO. [online]. 2009, 6, Dostupný z WWW: <www.ambo,cz>.

[10] *Technologie RFID*. [online]., [cit. 2010-05-02]. Dostupný z WWW: <www.rfidportal.cz>.

[11] *Uzamykací dveřní systémy*.[online], [cit. 2010-05-02]. Dostupný z WWW: <www.assaabloy.cz>.

[12] *Materiály firmy Cominfo* [online]. [cit. 2010-05-02]. Dostupné z WWW: <www.cominfo.cz>.

[13] MGR. ING. ŠČUREK, Radomír . *Biometrické metody identifikace osob v bezpečnostní praxi : Studijní text* [online]. VŠB TU Ostrava, Červen 2008 [cit. 2010-05-06].

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

EZS	Elektrická zabezpečovací signalizace
EPS	Elektrická požární signalizace
CCTV	Uzavřený televizní okruh
ACCESS	Systém kontroly vstupu
MZS	Mechanické zábranné systémy
RS-232/485	Komunikační sběrnice
Wiegand	Komunikační sběrnice
PC	Osobní počítač
TCP/IP	Sada protokolů pro komunikaci v počítačové síti
http	Internetový protokol

SEZNAM OBRÁZKŮ