Systémy kontroly vstupu pro kombinované a integrované systémy

Access control systems for combined and integrated systems

Bc. Daniel Fojtík

Diplomová práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

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

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Daniel FOJTÍK**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Systémy kontroly vstupu pro kombinované a integrované systémy**

Zásady pro vypracování:

1. **Vysvětlete technický vývoj těchto systémů v rámci ČR a Evropy.**
2. **Zpracujte normy pro kontrolu vstupu a integrované systémy zahrnující ACCESS.**
3. **Proveďte konkrétní návrh pro zvolený komerční objekt.**
4. **Odhadněte další vývoj integrovaných systémů.**

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **Český normalizační institut. ČSN CLC/TS 50398. [s.l.] : [s.n.], 2005. 20 s.**
2. **Český normalizační institut. ČSN EN 50133-7 (334593) Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích. [s.l.] : [s.n.], 2000. 13 s.**
3. **KINDL, Jiří. Projektování bezpečnostních systémů . 1. vyd. Zlín : [s.n.], 2004. 134 s. ISBN 80-7318-165-7.**
4. **UHLÁŘ, Jan. Technická ochrana objektů . 1. vyd. Praha : [s.n.], 2001. 205 s. ISBN 8072510762.**
5. **LAUCKÝ, Vladimír. Technologie komerční bezpečnosti I . 3. vyd. Zlín : [s.n.], 2010. 81 s. ISBN 978-80-7318-889-4.**

Vedoucí diplomové práce: **Ing. Rudolf Drga**
Ústav bezpečnostního inženýrství

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

Termín odevzdání diplomové práce: **7. června 2010**

Ve Zlíně dne 19. února 2010

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Cílem diplomové práce je zhodnocení současného stavu na trhu se systémy kontroly vstupu a identifikačními médii. Dále řešitel prostuduje a zpracuje normy ČSN EN 50133-7 a ČSN CLC/TS 50398 a provede konkrétní návrh pro zvolený komerční objekt.

Klíčová slova: Systémy kontroly vstupu, přístupové systémy, ACCESS, docházkové systémy, identifikační média.

ABSTRACT

The thesis aims to assess the current state of the market with access control systems and identification media. Further study investigator and process standards ČSN EN 50133-7 and ČSN CLC / TS 50398 and make a concrete proposal for selected commercial building.

Keywords: Access control systems, access systems, Access, attendance systems, identification media.

Tímto bych chtěl poděkovat Ing. Rudolfu Drgovi, za odborné vedení, ochotně poskytnuté rady a čas, který mi věnoval při vypracování mé diplomové práce. Dále bych chtěl poděkovat Ing. Jiřímu Alexovi z firmy SKS s.r.o. Blansko za ochotu a odborné rady při vypracování práce.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/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 diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/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 diplomovou/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 – diplomovou/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 diplomové/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 diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/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 diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně dne 2.6.2010 …….

Daniel Fojtík

OBSAH

ÚVOD

Jak fyzické, tak právnické osoby si čím dál tím víc uvědomuji potřebu chránit svůj majetek. Ať už se jedná o movitý majetek, nebo o cenné informace, data údaje apod. Lidé si sice uvědomovali hodnotu svého majetku, ale nevěnovali patřičnou potřebu jeho ochrany. K ochraně majetku nám slouží spousta bezpečnostních systémů, ať už se jedná o PZTS, MZS nebo systémy kontroly vstupu(ACS).

Systémy kontroly vstupu sice majetek přímo nechrání, ale umožňují nám omezit přístup do prostor s ním, kontrolovat přístup osob k němu a jednoznačně určit přístupová práva. Hlídané prostory je třeba nejen hlídat, ale i evidovat, monitorovat a řídit přístup do určitých části na základě přístupových práv. Díky těmto přístupovým oprávněním je buď přístup povolen nebo zamítnut.

Systémy kontroly vstupu v poslední době už nejsou chápany jako jednotlivé systémy, ale hrají významnou roli v mnoha dalších bezpečnostních systémech. Bývají použity v kombinaci se zabezpečovacími nebo docházkovými systémy. Jednotlivé systémy už nebývají užívány jako samostatná a jediná řešení, ale jsou integrovány a kombinovány do flexibilních celků.

Všechny tyto systémy jsou sice stále ještě finančně náročné na jejich instalaci, provoz apod., ale každý, ať už se jedná o fyzickou či právnickou osobu, by si měl uvědomit, že instalace systému kontroly vstupu, popřípadě jiných zabezpečovacích systémů není rozmar, ale účinně pomáhají ke snížení krádeží, úniku cenných dat a mnohdy dokáží ochránit majetek a informace daleko vyšší hodnoty.

V neposlední řadě musíme brát v úvahu i to, že ochrana majetku je důležitým aspektem i pro Českou asociaci pojišťoven, která si klade podmínky na zajištění budov při uzavírání pojistných smluv.

1 OBJEKTOVÁ OCHRANA

Vezmeme-li ochranu v obecné rovině, jde o to, abychom vytvořili bezpečné prostředí pro subjekt, který má být chráněn. Budeme-li navrhovat konkrétní ochranu musíme znát základní věci, mezi které patří:

- **předmět ochrany** (co se má chránit s popisem daného předmětu, subjektu)
- **cíl ochrany** (proti čemu budeme chránit, definovat předpokládané nebezpečí)

Budeme-li realizovat ochranu, jde o návrh a sladění prostředků, které máme dostupné , zajišťující bezpečnost, jenž požadujeme nebo je definována.

K realizaci ochrany používáme prostředky, které nazýváme bezpečnostní systém. Bezpečnostní systém představuje integrovaný celek, který nám zajišťuje bezpečnost:

- **osobní** (jde o ochranu osob, na tuto bezpečnost je kladen nejvyšší důraz)
- **informační** (jde o ochranu informaci a dat, které pro nás určitou hodnotu)
- **majetkovou** (je o ochranu majetku, movitých a nemovitých věcí)

U každé bezpečnostní oblasti používáme ochranu:

- **mechanickou** (mechanické zábranné systémy a prostředky)
- **elektronickou** (poplachový zabezpečovací a tísňový systém)
- **režimovou** (technicko organizační opatření)

Při navrhování ochrany objektu musíme však brát v potaz tři základní pravidla, kterými bychom se měli řídit nebo je alespoň mít pořád na mysli.

1) Každou ochranu jde překonat, tudíž neexistuje absolutní ochrana.
2) Je třeba propojovat více skupin ochran. Jedna skupina ochrany není dostačující.
3) Člověk je nenahraditelný – technické prostředky člověka nenahradí. Dojde-li k poplachu, je na člověku, zda opravdu došlo k překonání ochrany. [1]

1.1 Základní rozdělení objektové ochrany

Abychom ochránili objekt před jeho narušením, bylo zapotřebí vypracovat různé formy ochrany objektu, se kterými se musíme seznámit.

a) ***Klasická ochrana*** – je založena na zajištění objektu pomocí takových mechanických zařízení, která ho umožňují chránit a znemožňuji jeho odcizení nebo poškození, jejich částí, nebo k ochraně cenných předmětů uvnitř objektu. Tato ochrana patří mezi nejstarší způsob zajištění objektu a tudíž se s ní můžeme potkat v různé podobě prakticky na každém objektu. Je velmi rozšířená a používá se jako základní forma ochrany objektu. Avšak prostředky klasické ochrany, nejsou schopny stoprocentně chránit zabezpečené objekty. Jedná se o tzv. *zpožďovací faktor*, který nám udává, jaký čas je zapotřebí k překonání (kvalifikovanému napadení dostupnými nástroji a metodami) prostředku klasické ochrany. Proto se v dnešní době prostředky klasické ochrany kombinují s jinými druhy ochrany, se kterými se navzájem doplňuje.

b) ***Fyzická ochrana*** – je taková ochrana, která je prováděna „živou sílou“. Jedná se o fyzickou ochranu objektů pomocí vrátných, hlídačů, strážných, hlídací službě, policie apod. Budeme-li to brát z finančního hlediska, tak se jedna o nejdražší způsob ochrany objektů. Ostatní druhy ochrany objektu mají sice vysoké počáteční náklady (zakoupení, zapojení, montáž atd.), ale jejich provoz je již většinou finančně nenáročný. Kdežto u fyzické je tomu naopak. Počáteční náklady minimální (výzbroj, oděv, školení atd.) avšak na provoz jsou kladeny vysoké finanční nároky (vyplácení mzdy).

c) ***Režimová ochrana*** - je soubor organizačně administrativních opatření a postupů, které vedou k zajištění správných funkcí zabezpečovacího systému a jejich sladění s provozem chráněného objektu. Její princip je založen na fungování stanovených bezpečnostních směrnic, které se obecně nazývají tzv. *režimová opatření*. U režimové ochrany dělíme na:

- <u>*Vnější režimová opatření*</u> – týkají se především vstupních a výstupních prostor chráněného objektu, kudy se dostávají vozidla, osoby, věci do objektu. Jedná se zejména o vchody, vjezdy apod., kde dochází ke kontrole vozidel, osob, věcí při vstupu a výstupu z chráněného objektu (prostoru).

- *Vnitřní režimová opatření* - týkají se především pohybu uvnitř chráněného objektu. Např. omezení pohybu osob a vozidel vně objektu (prostoru) , nebo jeho částí. Dále se může jednat o monitorování pohybu materiálu, výrobků, cenností apod., zajištění dostatečného osvětlení v určitých částech objektu atd.

d) ***Technická ochrana*** – používá se jako podpora klasické ochrany. Jedná se o nejvíce spolehlivou ochranu, která jde zároveň nejhůře překonat z hlediska dnešních požadavků i technických možností. Jedná se o detekční systémy, které „monitorují" objekt pomocí technických prostředků objektové bezpečnosti. Zajišťuje informace v objektu, prostoru, jenž je chráněn a o případném narušení prostoru. Cílem technické ochrany je zvýšení efektivity klasické a fyzické ochrany z důvodu rychlé reakce na nastalou situaci a k jejímu rychlému řešení. K zabezpečení objektu se u technické ochrany využívají:

- *mechanické prvky bezpečnosti* – využívají se zde mechanické zábranné prostředky a systémy, jenž pachateli znesnadňuji, popř. zamezují vniknutí do chráněného objektu či prostoru. Patří zde:
  - mechanické zábranné systémy obvodové ochrany (různé bezpečnostní oplocení, brány, závory, branky, ploty apod.)
  - mechanické zábranné systémy plášťové ochrany (mříže, rolety, okna, balkónové dveře, bezpečnostní fólie, bezpečnostní skla, ochranné fólie apod.)
  - mechanické zábranné systémy předmětové ochrany (zámkové pokladničky, trezory, schránky apod.)
- *elektronické prvky bezpečnosti* – k ochraně majetku a osob je využito elektronických (elektrických) prvků, a to:
  - poplachový zabezpečovací a tísňový systém (PZTS , dříve EZS)
  - přístupové a docházkové systémy (ACCESS)
  - elektrická a požární signalizace (EPS)
  - uzavřené televizní okruhy (CCTV)

- biometrické identifikační systémy
- ochrana dat a informací
- průmyslová havarijní signalizace
- elektronická ochrana zboží
- zdravotní a nouzová signalizace

- *kombinované (mechatronické) prvky bezpečnosti* – jedná se o kombinaci mechanických zábranných systémů a elektronické ochrany jako jednoho funkčního celku (např. el. blokování dveří)
- *speciální prvky bezpečnosti* – je zde využito speciální (specifických) prostředků k zajištění ochrany objektu (chemická ochrana apod.)

[1,2]

2 SYSTÉMY KONTROLY VSTUPU A DOCHÁZKY

Systémy kontroly vstupu a docházky nám určují, kdo může kam jít, kdy tam může jít a zároveň tento proces evidují, včetně identifikace jak tyto činnosti probíhaly. Hlavní činností SKV je, aby zabránili přístupu nepovolaným osobám do míst, kde nemají dané přístupové právo. SKV umožňují sledovat pohyb osob v daných úsecích, jejich kontrolování, vyhledávání, včetně pokusů o neoprávněný vstup.

Systémy kontroly vstupu

SKV řídí přístup k prostorům, které mají být chráněny, zařízením, aktivům, informacím a datům na základě jednoznačně předepsaných pravidel.

Docházkové systémy

DS kontrolují oprávnění vstupu na kontrolním místě při vstupu a mohou následně provádět sběr informací o osobě, čase a důvodu průchodu daným místem vstupu.

Systém kontroly vstupu a docházkový systém jde integrovat v jeden celek, který se na nazývá *integrovaný identifikační systém kontroly vstupu.* [3]

Významným parametrem SKV je autentizace, to znamená, že dojde k ověření, že osoba, která požaduje vstup do objektu, prostoru je opravdu tou osobou, za kterou se vydává. SKV nám slouží k lepší informovanosti o pohybu vlastních i externích zaměstnanců v daných prostorách a mají za úkol ovládání elektrického zámku dveří. Na základě ověření identity a přístupových práv se dveře otevřou či nikoliv.

Systémy kontroly vstupu zahrnují tyto funkce:

- **Systém snímaní průchodu** - Systém snímání průchodů je tvořen elektronickými snímači osazenými ve struktuře vycházející z topologie míst, která je třeba alespoň monitorovat průchody a případně řídit přístup osob (tj. vchody do objektů či kanceláří, vjezdy objektů, parkovišť apod.)
- **Přístupový terminál** - Přístupový terminál je specializované zařízení zajišťující veškeré přístupové funkce. Je tvořen základní jednotkou, umísťovanou do nepřístupné oblasti uvnitř chráněné zóny, k níž lze připojit:
    - Vstupní snímač bezkontaktních karet
    - Výstupní snímač bezkontaktních karet

- Kontakt sledování otevřených dveří
- Tlačítko pro otevření dveří
- Sirénu pro hlášení alarmu
- Spínaný kontakt pro otevření přístupových mechanismů (závory, vrata, turnikety, elektromagnetické dveřní zámky)

- **Definování přístupových modelů** - Pro účely definování funkce přístupového systému jsou pomocí účinných nástrojů vytvářeny přístupové modely pro skupiny či jednotlivce, které se při konfigurování systému přiřazují konkrétním osobám a terminálům.
- **Sledování průchodů přes zámky** - Při normální funkci přístupového systému, kdy je povolen zápis průchodů do databáze, lze na základě zaznamenaných údajů trasovat průchody a kontrolovat přítomnost vybraných osob v zadaném časovém intervalu pro konkrétní terminál.
- **Systém anipassback** – hlídá opakované vstupy v jedné zóně – na každý vstup jeden výstup. [4]

Rozdělení autentizačních přístupů je založené na:

- *informaci uložené v paměti (nejčastěji znalost hesla, PIN kódu)*
- *předmětu, určenému k autentifikaci (tokeny, identifikační průkazky apod.)*
- *biometrickém rysu člověka (otisky prstů, dlaní, nehtu apod.)*

Na základě tohoto rozdělení rozlišujeme:

- **autentizaci heslem** – jedná se o nejpoužívanější metodu, která je založena na znalosti uživatelské jméno, hesla. Označuje se také jako sdílené tajemství mezi systémem a samotným uživatelem. Identifikace i autentifikace probíhá tak, že systém vyzve uživatele k zadání uživ. jména, hesla a systém jej porovná s údaji, které má uložené ve své databázi. Služba, zajišťující tento proces se nazývá authentication service a uživatelem zadané údaje (credentials) předává autentizační autoritě (authentization authority).
- **autentizaci předmětem** – tento typ je založen na vlastnictví nějakého identifikačního předmětu. Obecně tyto předměty, které potvrzují identitu svého

vlastníka nazýváme TOKEN. Autentizační předměty (tokeny) by měli být především jedinečné (unikátní) a těžko padělatelné, popř. aby nebylo možno je duplikovat. Mezi hlavní výhody tokenů patří právě obtížná padělatelnost. Dražší tokeny dokonce chrání sebe sama před násilným vniknutím a šifrovací klič, který je v nich uložen, je při pokusu o násilné vniknutí do tokenu zničen. Mezi nevýhody jednoznačně patří možnost odcizení nebo případná ztráta. Z tohoto důvodu bývají autentizační přístupy založené na autentizaci předmětem doplněny v kombinaci s autentizaci heslem. Z pohledu užívaných autentizačních předmětu můžeme tokeny dělit na:

- *tokeny paměťové* - magnetické, elektronické, resp. optické karty, které představují analogii mechanickým klíčům, jejich paměť obsahuje jednoznačný identifikační řetězec.
- *tokeny udržující heslo* - u těchto tokenů je výstupem po zadání jednoduchého uživatelského hesla přístupový klíč.
- *tokeny s logikou* – tyto tokeny umožňují zpracovat jednoduché příkazy (př. vydej následující klíč atd.)
- *inteligentní tokeny* – můžou obsahovat vlastní vstupní zařízené pro komunikaci s uživatelem, vlastní časovou základnu, jsou schopny šifrování, generace náhodných čísel apod.

- **biometrickou autentizaci –** U této autentizace můžeme rozlišit dle. fyziologické charakteristiky (otisk prstu, dlaně apod.) a behaviorální charakteristiky (rozpoznání hlasu, dynamika podpisu apod.). U autentitzace pomocí behaviorálních charakteristik máme větší jistotu, že autentizaci provádí opravdu daná osoba – ale i zde je možnost zneužití donucením osoby, popř. napodobením charakteristiky. Proto je vhodné doplňovat biometrickou autentizaci přítomnosti ostrahy(kontrola co a jak je ke snímači přikládáno, jestli nedochází k nežádoucí manipulaci se zařízením) popř. kamerovým systémem.

Třídy identifikace

Třída O – tato identifikace nevyžaduje přímou identifikace. Přístup je umožněn pomocí tlačítek. U vstupních prostor je přítomna fyzická ostraha pro vizuální kontrolu průkazky (povolení, vstupka apod.) opravňující ke vstupu.

Třída 1 - tato identifikace vyžaduje znalost informace, kódu, PIN kódu apod. Po zadání hesla dojde k porovnání s údajem v paměťové jednotce.

Třída 2 - třída identifikace, která vyžaduje užití pevného identifikačního předmětu, přístupové karty, tokenu nebo biometrického prvku osoby, která vstupuje. Uživateli je tak přiřazena jednoznačná identita. Tato třída identifikace zamezuje použití identifikačních prvků viditelných lidským okem (snadná tvorba kopie).

Třída 3 – u této třídy se využívá znalost PIN kódu, hesla apod. (Třída 1) v kombinaci s identifikačním prvkem a nebo biometrické metody (Třída 2).

Třídy přístupu

Třída A – U této třídy není vyžadován žáden časový filtr, přístup není časově omezen a ani není vyžadováno ukládání přístupových informací.

Třída B – Systémy třídy B musí užívat časový filtr a ukládat přístupové informace. Lepší systémy ukládají do paměti informace při napadení systému, dojde-li k otevření bez oprávnění, včetně odmítnutých přístupů.

Typy vstupních oprávnění

Generální oprávnění ke vstupu – přístup je umožněn kdykoliv a kamkoliv.

Omezení generálního oprávnění – přístup je umožněn kdykoliv a kamkoliv jen v přítomnosti další osoby k tomu oprávněné.

Časově omezené oprávnění – přístup je umožněn kamkoliv, ale jen v určité době.

Prostorově omezené oprávnění – přístup je umožněn kdykoliv, ale jen do určitých prostor.

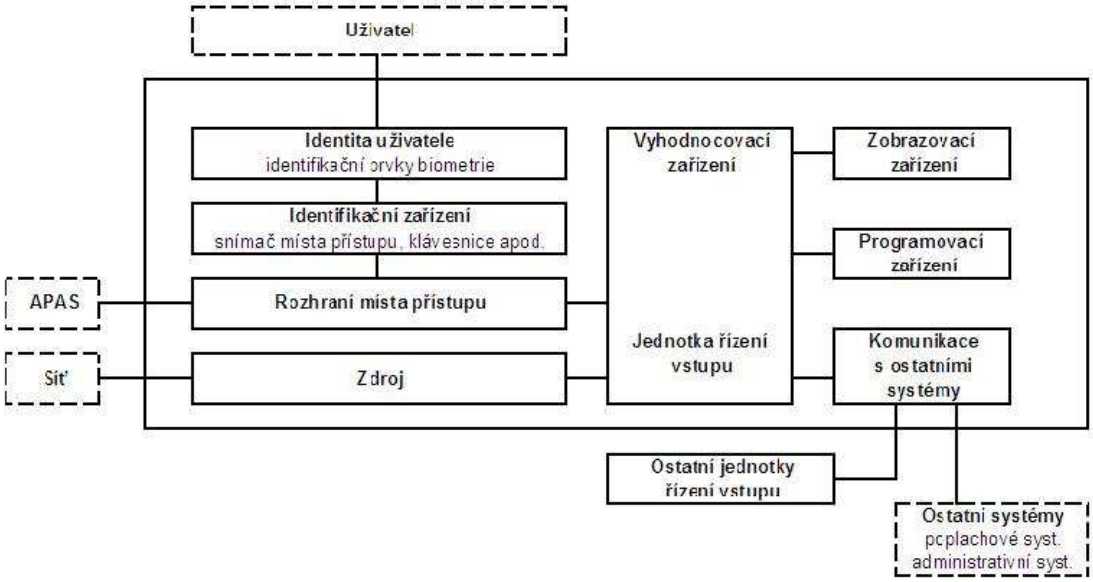
Prostorově a časově omezené oprávnění – přístup je umožněn jen v určitém čase a jen do určitých prostor.

Oprávnění vstupu s omezením – Omezení vstupu z jiných důvodů (je li v prostoru méně nebo více než x počet osob, byla-li osoba před tím v určitém prostoru apod.) [3]

2.1 Struktura systémů kontroly vstupu

- Čtecí a snímací zařízení.
- Vyhodnocovací jednotka.
- Výstupní prvek (zámek, indikátor.)
- Napájecí zdroj.
- Dohledové a správní pracoviště.

[3]



Obr. 1 Struktura SKV

2.2 Integrace systémů kontroly vstupu s jinými systémy

SKV (systémy kontroly vstupu) jsou používány buď samostatně, nebo se kombinují s dalšími systémy (poplachové systémy apod.). V této kombinaci tvoří společně jednu bezpečnostní aplikaci. V současnosti se používají tyto kombinace:

- **Kombinace přístupového systému a docházkového systému**

V téhle kombinaci je nejen hlídán vstup do objektu, ale jsou zaznamenávány údaje pro další zpracováni zaměstnavatelem. Docházkový systém eviduje příchody a odchody do práce, odchody na obědy, k lékaři, služební cesty, přerušení práce, druh směny, práce ve svátečních dnech, o víkendu, dovolenou a pod. Při používání docházkového systému dochází k menší chybovosti při zpracování informací o docházce, zvýšení pracovní morálky a efektivnější práci.

- **Kombinace přístupového systému a systému pro výdej stravy**

Kombinace, umožňující přístup do zařízení zaměstnavatele a odběr stravy, nápojů a jiných potravin. Zároveň umožňuje bezhotovostní platbu za nakoupené potraviny, stravu, nápoje.

- **Kombinace přístupového systému a systému pro výdej pracovních pomůcek**

Podobný princip jako u systému pro výdej stravy. Umožňuje vstup do zařízení a prostor zaměstnavatele a odběr, nákup pracovních pomůcek, oděvů, nářadí potřebné k výkonu zaměstnáni. Zároveň umožňuje bezhotovostní platbu za nakoupené pracovní pomůcky a eviduje vydané pracovní pomůcky pro potřeby zaměstnavatele.

- **Kombinace systému kontroly vstupu s Poplachovým zabezpečovacím a tísňovým systémem (PZTS)**

Tato kombinace umožňuje vstup do prostor oprávněné osobě a dochází k odkódování (odalarmování) systému PZTS, aby nedošlo k planému poplachu. Zároveň dochází k evidenci vstupu osob a umožňuje časově sledovat pohyb osob po pracovišti nebo v daných prostorách. Používá se tam, kde nestačí pouze SKV, ale je nutné zabezpečit objekt, prostory nebo jejich části PZTS.

- **Kombinace systému kontroly vstupu s EPS**

Je jednou z nejčastěji používaných kombinací. Je zároveň nejjednodušší aplikací. Užívá se k zajištění automatického otevření únikových východu, dojde-li k detekci požáru EPS. Aby docházelo k rychlé a spolehlivé reakci je integrace prováděna zapojením napájení elektr. zámků přes kontakt signalizačního relé systému EPS.

- **Kombinace systému kontroly vstupu s CCTV**

Umožňuje vstup do prostor oprávněné osobě a systém CCTV umožňuje kontrolovat nejen pohyb osob, zaměstnanců po objektu, ale i jejich vykonávanou činnost. Používá se tam, kde potřebujeme mít neustálý dohled veškerého pohybu v objektu, nebo jeho částech s možností včasné reakce na nežádoucí situaci.

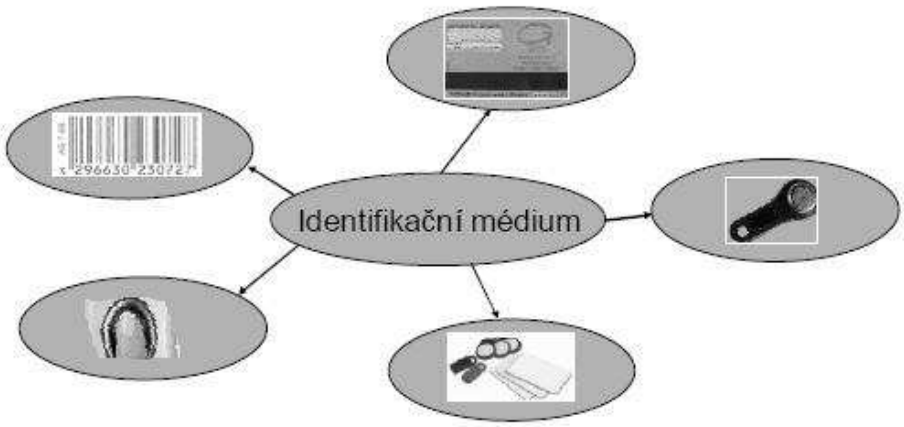
- **Kombinace systému kontroly vstupu do informačních technologií**

S nárůstem využívání informačních technologií je zároveň i potřeba přístupu k nim. Musíme brát na vědomí, že ne všechny informace jsou přístupné všem. Tímto požadavkem došlo ke vzniku integrace SKV s informačními technologiemi. Vzhledem k omezeným možnostem pamatovat si hesla, kódy apod. je požadováno, aby byl přístup umožněn po schválení vstupu a vydání přístupového média (přihlašování do počítačové sítě, k samotnému počítači, elektronický podpis apod.). Hlavními prvky, které tvoří vazbu mezi systémy kontroly vstupu pro fyzickou kontrolu přístupu a prvky řízení přístupu k informacím jsou:

  - *Identifikační karty* – Většinou se používají kombinované karty (bezkontaktní karty, které obsahují identifikační část, která zároveň obsahuje výkonný bezpečnostní procesor s normalizovaným kontaktním polem – ISO 7816). Na identifikační kartě bývají uloženy informace o uživateli včetně jména a hesla.
  - *Biometrické prvky* – K identifikaci dochází pomocí biometrických prvků dané osoby (odtisk prstu, podle oční duhovky, podle nehtu apod.). Nutnost začlenění biometrické čtečky do existujících softwarových aplikací. Zabezpečená informace jev IS (informační systém) chráněna na prostředky operačního systému a šifrováním. K zpřístupnění zabezpečené informace dojde po věření shody mezi uloženým vzorem a nově sejmutým vzorkem biometrického údaje. [5]

3 ZÁKLADNÍ TYPY IDENTIFIKAČNÍCH MÉDIÍ U SKV

Systémy kontroly vstupu nám umožňují otevírání dveří, kontrolu a registraci vstupu osob do objektu či jeho části. SKV je jednotný systém přístupu do objektu dle oprávnění. Při vstupu oprávněné osoby systém otevře elektromagnetický dveřní zámek. Do paměti se uloží číslo uživatele, datum, čas a místo kde došlo ke vstupu do objektu, prostoru. Díky tomuhle máme přehled o počtu a pohybu zaměstnanců. Při ukládání dat do paměti nová data přepisují ty staré. Tuto funkci lze deaktivovat a až bude paměť plná údaji se vstupy, dojde k zablokování zámku do doby, než dojde k vyčtení údajů z paměti. Mezi hlavní výhody patří dlouholetý provoz bez nutnosti zásahu, velká přizpůsobivost potřebám majitele, detekce pokusu o zneužití identifikačního prvku, pohyb osob apod. Naopak nevýhodou jsou pořizovací náklady a nároky na bezpečnostního správce.



Obr. 2 Typy identifikačních médií

3.1 Elektronický zámek

Je blokovací zařízení, které pracuje pomocí elektrického proudu. Elektronické zámky jsou buď nezávislé s elektronickým ovládáním, namontovaným přímo na zámku, nebo v většině případů jsou napojeny na systémy kontroly vstupu (access control system).

Elektronické zámky používají magnety, elektromagnety nebo motory pro ovládání zámku. Ovládání zámku může být jednoduché jako používání přepínače například u Intercomu pro uvolnění bytových dveří nebo složité, založené na biometrickém ovládání systému dveří.

3.1.1 Druhy elektrických zámků

3.1.1.1 Magnetické zámky

Jedná se o nejzákladnější typ elektronického zámku. Velký elektromagnet je namontován na rám dveří a odpovídající armatura (protikus) se montuje na rám dveří. Když je magnet napájen a dveře jsou uzavřeny, tak armatura je pevně přidržována magnetem. Magnetické zámky jsou velmi jednoduché na instalaci a jsou i velmi odolné proti útoku. Velkým problémem může být ovšem výpadek el. proudu, kdy dojde k pádu magnetického pole a prodleva umožní volný přístup do dveří. Což je velkým problémem, kdy je v dnešní době bezpečnost prvořadým zájmem.

Obr. 3 Elektromagnetický zámek

3.1.1.2 Elektrické západkové zámky

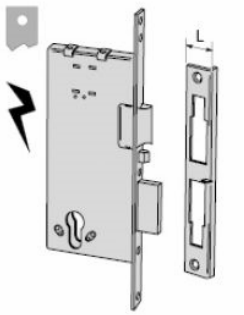
Nahrazuje klasické západkové zámky. Obvykle jsou ve dvou variantách a to:

- *Fail secure* – zámek bez napájení zamčený. Klika ve směru úniku je funkční trvale (antipanic), vnější klika je funkční po přivedení napájení z ovládacího zařízení, např. čtečky. Nebo Obě kliky jsou funkční po přivedení napájení z ovládacího zařízení, např. čtečky.
- *Fail safe* – zámek bez napájení zamčený. Klika ve směru úniku je funkční trvale (antipanic), vnější klika je funkční po odpojení napájení z ovládacího zařízení, např. čtečky. Nebo Obě kliky jsou funkční po odpojení napájení z ovládacího zařízení, např. čtečky.

Obr. 4 Elektrický západkový zámek

3.1.1.3 Elektrické zadlabávací zámky

Nahrazuji klasické mechanické zámky. Do dveří se musí vyvrtat díra pro přívod elektrických drátů. Jsou nejlevnější a nejčastěji používanou metodou elektronických zámků.



Obr. 5 Elektrický zadlabávací zámek

3.1.2 Metody ověřování přístupu pro elektronické zámky

Pomineme-li otevírání pomocí klíče, nabízí elektronické zámky řadu prostředků autentizace.

- **Číselné kódy, hesla a přístupová hesla**

Jedná se o nejrozšířenější metodu. Pro otevření je nutno zadat číselný kód, aby byl zámek deaktivován. Kombinace délky kódu hesla se pohybuje mezi 4-6 číslici.

Obr. 6 Zámek s číselným kódem

- **Bezpečnostní žetony**

Pro otevření dveří je nutno přiložit bezpečnostní žeton, token, čipovou kartu ke snímači na zámku dveří.

Obr. 7 Kombinace zámku se čtečkou

- **Biometrické elektronické zámky**

Některé nové elektronické zámky využívají biometrii k ověření identity uživatele. Po shodě biometrických údajů s uloženými daty dojde k deaktivaci zámku.

Obr. 8 Biometrický elektronický zámek s PIN vstupem

- **RFID zámky**

Radio-frekvenční identifikace. tato technologie se používá u moderních a nových elektronických zámků. Pomocí radiových vln, je sledováno, zda se v okolí nenachází osoba (popř. zvíře) s RFID čipem určeným k otevření elektronického zámku. Dosah někdy bývá i několik metrů.

3.2 Optická média

Do optických médií řadíme karty s čárovým kódem. Jedná se o nejrozšířenější metodu automatické identifikace. Čárový kód je tvořen černotiskem tištěnými pruhy (u některých novějších verzí mozaikou) definované šířky a světlých mezer, ve kterých jsou zakódovány určité informace (jméno osoby, cena, číslo výrobku, skladové informace, přístupová práva apod.) Ke čtení a dekódování čárového kódu slouží snímače (čtečky pro jednorozměrné kódy a skenery pro jedno a více rozměrné kódy), které na principu světla dokáží převést informace v podobě čísel a znaků do počítače či jiného zařízení, kde s těmi informacemi můžeme dále pracovat.

Karty s čárovým kódem mají spoustu výhod a předností. Mezí hlavní přednosti jednoznačně patří:

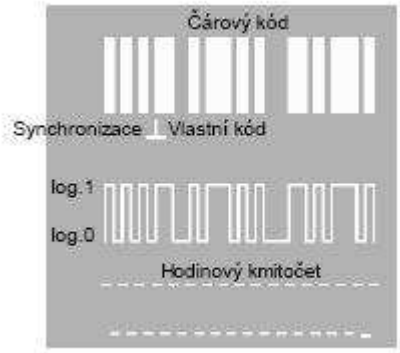
- **Přesnost** – Budeme-li kód, heslo, jméno zadávat ručně může dojít při jejich zadávání k chybě, používáním karet s čárovým kódem eliminujeme chybnost zadávání údajů. Ke kontrole správnosti čárového kódu navíc slouží kontrolní číslice, která je vypočítána z předchozích číslic kódu.
- **Rychlost** - Když budeme zadávat data, údaje klávesnicí, zjistíme že i nejlepší pisatelé jsou pomalejší než pořizování dat z čárového kódu jakýmkoliv snímačem.
- **Flexibilita** – Čárové kódy mohou být tištěny na jakýkoliv materiál odolný proti kyselinám, vysokým teplotám, mrazu, vlhkosti, obroušení apod. Jejich velikosti mohou být upraveny potřebám zákazníka.
- **Cena** – Náklady na nosič informace jsou zcela zanedbatelné, budeme-li je srovnávat s jinými médii.

Avšak pozor, kvůli možnosti snadného zkopírování se už nepoužívají v bezpečnostních systémech, kde je zapotřebí určité ochrany, ale např. v knihovnách, obchodech, supermarketech apod.

3.2.1 Konstrukce čárového kódu

Čárové kódy jsou tvořeny sekvencí čar a mezer s definovanou šířkou. Ty jsou při čtení transformovány podle své sytosti na posloupnost elektrických impulsů různé šířky a porovnávány s tabulkou přípustných kombinací. Pokud je posloupnost v tabulce nalezena, je prohlášena za odpovídající znakový řetězec. Nositelem informace je nejenom tištěná čára, ale i mezera mezi jednotlivými dílčími čárami. Krajní skupiny čar mají specifický význam - slouží jako synchronizační pro čtecí zařízení, které podle nich generuje signál Start/Stop. Technická specifikace pak vyžaduje ochranné světlé pásmo bez potisku před a za synchronizačními čarami.

[7]



Obr. 9 Čárový kód

3.2.2 Základní prvky čárového kódu

- **X - šířka modulu** - jde o nejužší element kódu. Tedy nejmenší přípustnou šířku čáry nebo mezery.
- **R - světlé pásmo** - doporučeno minimálně desetinásobek šířky modulu, nejméně však 2,5 mm.

- **H - výška kódu** - nám udává svislý rozměr pásu kódu. Doporučeno je minimálně 10 % délky pásu pro ruční čtení, pro čtení skenerem se doporučuje 20 % délky pásu, minimálně však 20 mm, pro kód EAN je doporučeno 75 % délky pásu.
- **L - délka kódu** – nám udává obsazenou délku pásu od první značky Start po poslední značku Stop, ale bez světlého pásma.
- **C - kontrast** - je poměr rozdílu jasu odrazu pozadí a odrazu čáry k jasu odrazu pozadí a pro uspokojivě čitelný kód by měl přesahovat 0,7.

[7]

3.2.3 Typy nejčastěji používaných čárových kódů

a) Čárový kód EAN

Tento kód je využíván státy zapojených do sdružení EAN (European Article Number). Kóduje se pomocí čísel 0-9, kde každá číslice kóduje dvě čáry a dvě mezery. Objevují se ve dvou variantách a to EAN 8 a EAN 13 (číslo 8 a 13 označuje počet čísel, obsažených v čárovém kódu. První dvě nebo tři číslice nám vždy určují stát původu (např. ČR má číslo 859), další čtyři až šest číslic nám určují výrobce a zbývající číslice (kromě poslední) určují konkrétní zboží. Poslední číslice je kontrolní , to nám ověřuje správnost dekódování.

Obr.10 Čárové kódy EAN 13 a EAN 8

b) Čárový kód Code 128

Jedná se o univerzální, volně použitelný čárový kód ke kódování. Jeho název napovídá, že je schopný zakódovat 128 znaků (spodní polovinu ASCII tabulky). Tento kód umí jako jeden z mála rozlišovat a zachovat velikosti písmen v kódu. Má 3 znakové sady (A, B, C). Tyto sady se jedním, ze speciálních znaků na začátku kódu nastaví a je možno mezi nimi v průběhu kódu přepínat. Znaková sada A obsahuje mimo jiné spodních 32 (řídících) znaků

ASCII tabulky, druhá sada B obsahuje ASCII znaky s kódy 32 až 128, třetí sada C umí pojmout dvojciferná čísla od 00 až 99. Poslední znaky, které jsou většinou stejná pro všechny sady, mají většinou speciální význam.

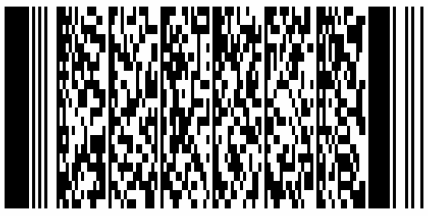
[7]

Obr. 11 Čárový kód CODE 128

c) Čárový kód PDF 417 (Portable data file)

Jedná se o 2D kód. Má velmi vysokou informační kapacitu se schopnosti detekce a opravy chyb, dojde li k poruše kódu. Název PDF 417 vychází ze struktury kódu. Každé zakódované slovo se skládá ze čtyř čar a čtyř mezer o šířce minimálně jednoho a maximálně šesti modulů. Ve slovo je vždy použito celkem 17 modulů přesně. Rozdíl od klasických jednorozměrových čárových kódů (které obvykle slouží jako klíč k vyhledávání údajů v databázi) je v tom, že čárový kód PDF 417 si nese všechny potřebné informace s sebou a je tak nezávislý na jiném systému. Kód PDF 417 umožňuje nejen zakódovat běžný text, ale umožňuje kódování grafiky, speciálních programovacích instrukcí atd. Velikost datového souboru může být až 1,1 kB. Při generování symbolu jde zvolit úroveň korekce chyb, což nám umožňuje zabezpečit čitelnost i při částečném poškození kódu.

[9]



Obr. 12 Čárový kód PDF 417

d) Další čárové kódy

- Kód typu 2 z 5
- Codabar
- Datamatrix
- QR Code
- Kruhový kód
- Code 39
- GS1 Databar

3.2.4 Snímače čárových kódů

Snímače čárových kódů nám slouží k bezchybnému čtení čárových kódů a předání jeho obsahu uživateli. V závislosti na principu snímání čárového kódu rozdělujeme snímače na laserové a digitální. Klasické laserové snímače vyzařují červené světlo, které je pohlcováno tmavými čarami a odráženo světlými mezery. Snímač pak sleduje rozdíly v reflexi a ty jsou přeměňovány v elektrický signál, který odpovídá šířce čar a mezer. Přijaté signály jsou převáděny v číslice, písmena, které obsahuje čárový kód. V posledních letech se začali využívat kromě klasických laserových snímačů i snímače digitální. Ty fungují podobně jako digitální fotoaparáty. Zde dochází k vyfocení čárového kódu. Následně se jeho obsah dekóduje pomocí dekodéru, jenž je součástí samotného snímače. Velkou výhodu u digitálních snímačů je, že umožňuje mnohosměrné čtení jak 1D, tak i 2D symbolů.

Obr. 13 Čtečky čárových kódů

3.3 Magnetická média

Jsou to identifikační karty o velikosti kreditních karet, na kterých je magnetický proužek. V něm jsou uloženy všechny potřebné informace. Magnetický proužek funguje na principu magnetického záznamu, který se používá u magnetofonových kazet nebo počítačových disket. Proužek obsahuje množství magnetických částic, které jsou kovového základu.Tyto magnetické částice jsou schopny dle své orientace uchovávat údaje. Po zmagnetizování se vytvoří množství malých permanentních magnetů, které tvoří binární rozhodování:

- Zmagnetizování – logická 1
- Nezmagnetizování – logická 0

Informace jsou na magnetické karty kódovány zařízením do tří stop. každá z těchto tří stop má své specifické parametry kódování, které jsou dány normou (ISO 7811).

1. stopa (IATA) – 79B – je na ní možno uložit 79 alfanumerických znaků. Hustota kódování je 210 bpi.

2. stopa (ABA) – 40B – je na ní možné umístit 40 numerických znaků (pouze čísla 0-9 a rovnítko). Hustota kódování je 75 bpi.

3. stopa (THRIFT) – 107B – je na ní možné umístit 107 numerických znaků (pouze čísla 0-9, rovnítko a dvojtečka). Hustota kódování je 210 bpi.

[3,10]

Obr. 14 Ukázka stop na kartě

3.3.1 Rozdělení magnetických karet:

Existují dva typy magnetických proužků:

- ***Karty s magnetickým pruhem HiCo (High Coercivity)* –** Vysoká hustota záznamu. Jsou odolnější proti vnějším vlivům než LoCo karty a téměř nedochází k žádnému znehodnocení karty.
- ***Karty s magnetickým pruhem LoCo (Low Coercivity)* –** Nízká hustota záznamu. Nízké pořizovací náklady, nevýhodou je, že se může poškodit magnetický pruh, necháme-li kartu v blízkosti magnetu

Karty se dají opticky rozlišit podle barvy magnetického proužku. Magnetické proužky LoCo karet jsou spíše hnědé. Oproti tomu proužky karty HiCo jsou spíše černé. Avšak existují i jiné barvy magnetických proužků – dle požadavků zákazníka (stříbrné, červené, modré, zelené, žluté)

[11]

3.3.2 Použití magnetických karet

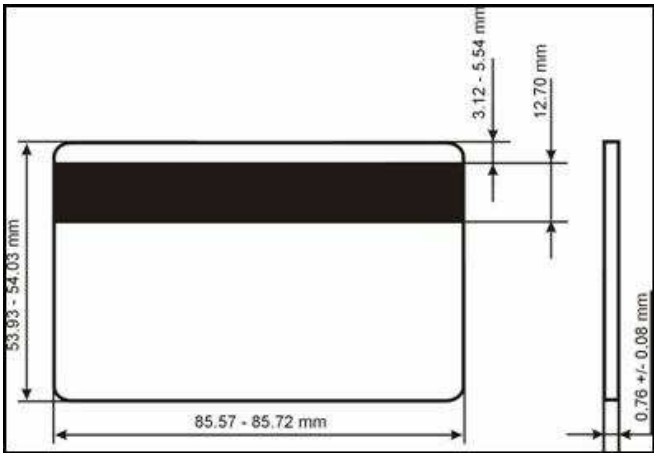
Karty s magnetickým pruhem jsou velmi rozšířené a to z těchto základních důvodů:

- magnetické karty jsou ekonomicky nenáročné
- životnost magnet. karet je vysoká (uvádí se 5-6 let)
- data magnetické karty jsou dynamické – tzn. že záznam, který je na kartě uložen, jde kdykoliv přepsat jiným záznam, lze údaje doplnit, či aktualizovat.

Velkou nevýhodou magnetických karet je jejich bezpečnost. Bez velkých problém lze kartu přečíst a vyrobit duplikát. Dále mezi nevýhody patří možnost poškození karty, omezená životnost snímacího zařízení (zhruba 10^6 protažení snímacím zařízením) nebo životnost karty v závislosti na agresivitě prostředí .

Magnetické karty bývají většinou doplněny jinou formou identifikace. Většinou to bývá zadáním hesla, kódu nebo PIN kódu. jsou velmi rozšířené v bankovnictví, kontroly docházky, u přístupových systému – tady se však v současné době přechází na modernější metody, jako jsou bezkontaktní karty nebo biometrická identifikace.

[5, 2]



Obr.15 Umístění magnetického proužku na kartě

3.3.3 Čtečky magnetických karet

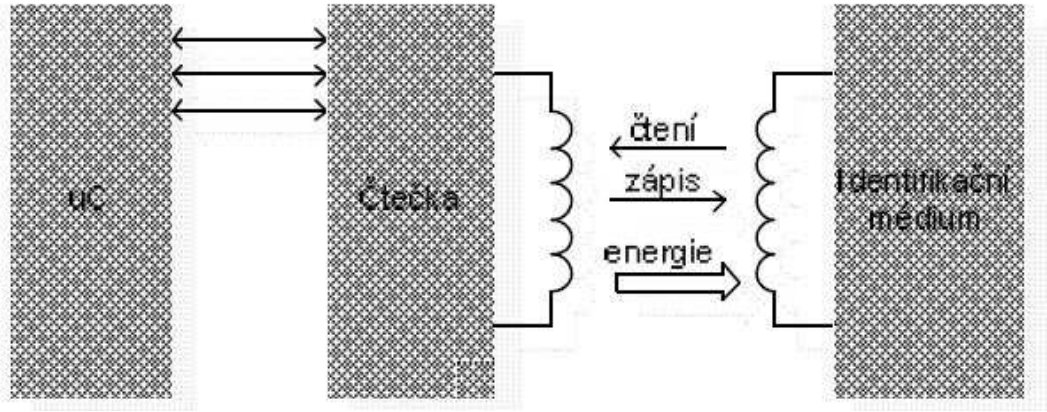
Čtečky magnetických karet snímají informace zakódované v magnetickém pruhu karty. Čtečky můžou snímat informace z různých stop, maximálně však ze tří stop. V závislosti na tom, ze které stopy je informace sejmuta, se rozlišují čtečky pro první, druhou, nebo třetí stopu. Dle toho, kolik stop současně je čtečka karet schopna současně dekódovat, rozlišujeme čtečky na:

- *jednostopé*
- *dvoustopé*
- *třístopé*

Obr. 16 Čtečky magnetických karet

3.4 Čipová média

Čipové karty (nazývané též Smart card – neboli chytrá karta), jsou plastové karty, které obsahují polovodičový čip (integrovaný obvod), který je schopen zpracovávat data. Jedná se o jedno z dnes nejdokonalejších médií, která jsou běžně rozšířena. V podstatě jde o miniaturní obvod s pamětí, do kterého jde zadat elektronický kód v digitální podobě. Čipové karty dokážou chovávat větší objem informací, uložená data jsou chráněna proti neoprávněné manipulaci a přístup k nim je chráněn bezpečnostní logikou.



Obr. 17 Blokové schéma čipových médií (bezkontaktní RFID)

Identifikačním médiem zpravidla bývá nejčastěji buď karta nebo média v podobě přívěsku na klíče, ve kterých je zakódována datová informace.

Existují dva druhy čipových médií, a to:

- *S kontaktními paměťovými prvky*
- *S bezkontaktními paměťovými prvky*

3.4.1 Kontaktní paměťové prvky

Čipová identifikační média obsahují kontaktní pole. K propojení dojde, zapojíme-li čip do obvodu. U těchto identifikačních médií muže probíhat oboustranná komunikace. Avšak velkou nevýhodou je životnost mechanických částí čtečky, která je závislá na počtu uživatelů a jejich přístupu k zařízení. K napájení dochází při kontaktu se čtečkou.

[2]

Čipová média s kontaktními prvky se nejčastěji vyrábějí ve formě karet a přívěšků.

3.4.1.1 Kontaktní čipová karta

Kontaktní čipová karta je velice rozšířeným druhem hardwarového klíče. Jedná se o plastikovou kartu rozměrů vizitky. Ve svém těle má karta vložen čip (do karty je vyfrézována dutina velikosti čipu a následní vlepení čipu do dutiny). K propojení čipové karty se čtecím zařízením dochází kontaktní ploškou, čímž dojde ke komunikaci mezi čipem a čtečkou.

Standart ISO/IEC 7810 definuje velikost karty na 85,60x53,98 mm a šířka 0,76 mm. Další ze standartu (ISO/IEC 7816-2) upravuje kontaktní plošku, která obsahuje osm kontaktů, jejich funkce a umístění na čipové kartě. Jednotlivé kontaktní plošky jsou určeny k napájení čipu, komunikaci, programovací napětí apod. Dva kontakty bývají volné, které jsou určeny pro budoucí využití. Ty se již v současnosti používají u některých druhů karet pro alternativní rozhraní USB.

Obr. 18 Popis čipu

VCC – Vstupní napájení čipu.

RST – Reset. Používají se buď samostatně (reset signálu napájeného z rozhraní zařízení) nebo v kombinaci s vnitřní reset řídící jednotkou. Je-li implementován vnitřní reset, tak napájecí napětí na VCC je povinné.

CLK – Časování signálu

GND – Uzemnění

VPP – Vstup programovacího napětí

I/O – Vstup nebo výstup pro sériová data do obvodu integrovaného uvnitř karty.

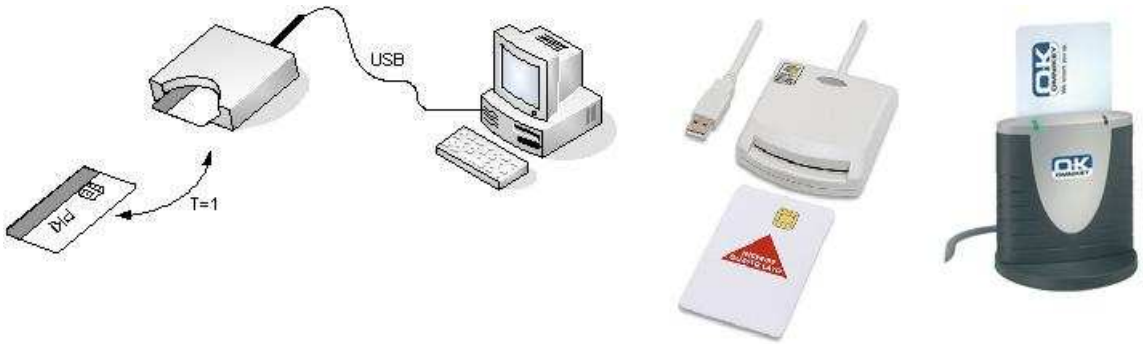
C4 a C8 jsou dva zbývající kontakty, které jsou rezervovány pro další užití.

Obr.19 Ukázka některých druhů čipů

Čtečka čipových karet

Čtečka čipových karet je zařízení, které zprostředkovává komunikaci s čipovou kartou. Čtečka může být buď samostatné zařízení, nebo může být propojena například s počítačem. Pro propojení čtečky s PC se často využívá jiný komunikační protokol, než který využívá čtečka pro komunikaci s čipovou kartou.

[12]



Obr. 20 Ukázka některých druhů čteček čipových karet

3.4.1.2 Kontaktní čipové přívěšky

Jednoznačným zástupcem kontaktních čipových přívěšku je osobní identifikační čip (nebo tzv. elektronický klíč) Dallas, který je založen na iButton technologii. Jedná se o přístupový systém, který je upraven požadavkům kontroly přístupu, identifikace osob při vstupu i opouštění objektu, daného prostoru. Přiložíme-li čip ke čtecí hlavě snímacího zařízení, dojde k přečtení kódu a tím i k identifikaci osoby. Výhodou těchto čipů je multifunkčnost, kdy jeden čip může být použit pro kontrolu vstupu, docházky, výdej stravy apod.

Výrobce kontaktních čipů Dallas (fa Dallas semiconductor) zaručuje, že nikdy nebudou vyrobeny dva naprosto stejné čipy, což nám zaručuje nezaměnitelnou identifikaci. V podstatě se jedná o polovodičové paměti uzavřené do kovového pouzdra o průměru 16 mm. Kromě základního provedení se vyrábějí čipy které jsou vybaveny paměti EEPROM, do které lze nahrát jakékoliv údaje a ty jsou při identifikaci přenášeny do čtecího zařízení.[13]

Kontaktní čipy jsou oblíbené pro svou spolehlivost a lehkou manipulaci. Čipy bývají usazeny v plastovém pouzdru, které si můžeme připnout ke klíčům, k opasku apod. čímž se nám omezuje i ztrátovost oproti přístupovým kartám. Při používání dochází k minimálnímu opotřebení, avšak nevýhodou je malá mechanická odolnost spodní plošky, která může být poškozena ku příkladu klíči.[5]

Obr. 21 Kontaktní čip Dallas

Čtečka kontaktních čipových přívěšků

Jedná se o elektronické zařízení, které umožňuje čtení čipů a přenos kódu do počítače. Zařízení bývají sestaveny z kontaktní čtecí plochy a procesoru, který zajišťuje obsluhu čtení kódu z čipu a data okamžitě vysílá do PC.

Obr. 22 Čtečka kontaktních čipů

3.4.2 Bezkontaktní paměťové prvky

V poslední době se stává čím dál tím rozšířenějším přístupovým médiem pro identifikaci osob vedle klasických kontaktních karet a čipů stávají bezkontaktní přístupová média. Přenos dat tak probíhá bez nutnosti napojení čtečky na kontakty (piny) karty. Bezkontaktní identifikační systémy jsou založeny na radiofrekvenční identifikaci – RFID.

Identifikační předměty bývají vybaveny datovým médiem, kterému se nazývá transpondér. Transpondér je elektronický obvod, který se skládá z vysílací a přijímací antény, nabíjecího kondenzátoru a paměti. Ke svému provozu nepotřebuje vlastní zdroj napájení – pasivní RFID čip. To znamená, že vysílač opakovaně vysílá do okolí pulsy. Objeví – li se v jeho blízkosti RFID čip, využije přijímaný signál k nabití svého kondenzátoru a odešle odpověď.

Čipy využívají převážně tyto nosné frekvence:

- 125 -134 KHz (LF – nízké frekvence) – nejběžněji používané frekvence.
- 13, 56 MHz (HF – vysoké frekvence) – díky mnoha přednostem se začíná více prosazovat nad LF. Má sice kratší dosah, ale zase rychlejší přenos dat, dokáže číst i zapisovat data na kartu, šifrování dat, využití jedné karty pro více účelů apod.

- 860-930 MHz (UHF – ultravysoké frekvence) - frekvence 868 MHz používané v Evropě a 915 MHz v Americe.

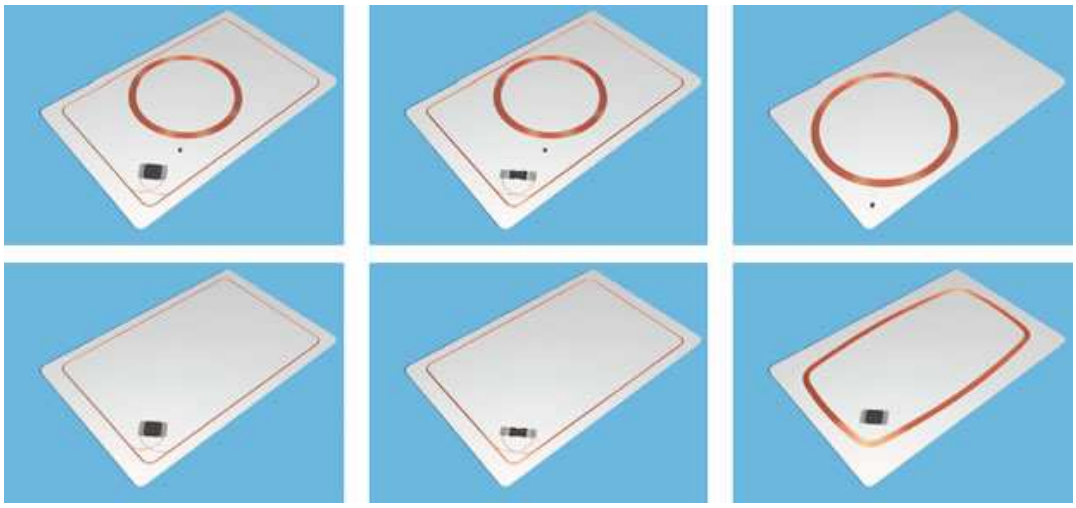
Provedení bezkontaktních přístupových systémů může mít různé provedení a to:

- Bezkontaktní plastové karty.
- Bezkontaktní plastové disky.
- Přívěšky na klíče.
- Bezkontaktní hodinky, náramky.
- A jiné.

[5,14]

3.4.2.1 Bezkontaktní plastové karty

Bezkontaktní karty bývají vyráběny z plastu a uvnitř bývají hermeticky uzavřeny bezkontaktní technologie. Karty jsou velmi odolné vůči oxidaci kontaktů, prachu, špíně, vlhkosti, vibracím a mají velmi vysokou životnost. Velkou výhodou oproti kontaktním kartám je, že z karty nejsou vyvedeny žádné kontakty (piny) a tudíž nedochází k poškození funkce karty ať už úmyslně nebo z nedbalosti.



Obr. 23 Různé druhy usazení jedné nebo dvou bezkontaktních technologií na jedné kartě

3.4.2.2 Bezkontaktní přívěšky

Bezkontaktní přívěšek je náhradou za mechanické klíče, které ovládají systém uvolnění elektrického zámku. Uvnitř plastového pouzdra je osazen čip a navinutá cívka. RFID čip obsahuje identifikační číslo, které slouží k identifikaci uživatelů v přístupovém systému.

[15]

Obr.23 Bezkontaktní přívěšky

Obr.24 Ukázka bezkontaktních náramků a hodinek

Čtečka bezkontaktních médií

Čtečka nám funguje jako vysílač, který do okolí vysílá určitou frkvenci. její umístění je libovolné, mže být zabudována ve zdi, v nějakém rámu, popřípadě i za zdí (ochrana proti vandalismu). V závislosti na umístění čtečky a frekvenci nemusíme u některých typů vůbec bezkontaktní médium vytahovat a dojde i přesto k identifikace- tzv. Freehand systémy.

Obr. 25 Bezkontaktní čtečky

3.5 Biometrická identifikace

Biometrická identifikace je identifikace na základě jedinečných fyziologických znaků člověka coby „hesla“ pro získání přístupu do chráněné oblasti, prostoru k chráněné věci, či zařízení.

U biometrické identifikace je nutné porozumět základním pojmům:

Rekognice (rozpoznávání) – Jedná se o rozpoznávání člověka použitím vhodné tělesné vlastnosti.

Verifikace (ověření) – Je to proces, při kterém se biometrický systém pokouší potvrdit totožnost jedince, který se s ní prokazuje, srovnáním sejmutého vzorku se vzorkem, který je již zapsaný (tzv. šablona)

Identifikace – Jedná se o to, že biometrický systém se pokouší určit totožnost neznámého jedince. Biometrický údaj je sejmut a porovnává se s všemi uloženými vzorky (šablonami).

Autentifikace (autentizace) – Toto označní je slučitelné s rekognicí – akorát s tím rozdíloem, že na konci tohohle procesu získá uživatel určitý status, a to např. osoba má přístup/ nemá přístup, osoba rozpoznána/nerozpoznána atd.

[16]

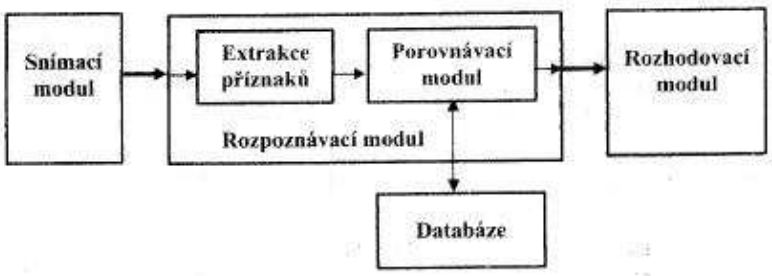
Biometrika je společný název pro všechny technologie, které jsou používány k identifikace, kontrole totožnosti osoby na základě fyzických či fyziologických znaků.

Obr. 26 Fyzické a fyziologické biometrické identifikátory.

[17]

Princip činnosti:

Biometrické identifikační systémy se skládají z několika logických (funkčních) bloků. Princip biometrických systému můžeme popsat pomocí následujícího schématu:



Obr. 27 Princip činnosti biometrických systémů

- *Snímací modul* – získává biometrická data osoby.
- *Rozpoznávací modul*

  - modul pro extrakci příznaků – K identifikaci osoby se nepoužívají veškeré snímané informace, ale jen některé jejich významné části – příznaky. S extrahovanými částmi se uskutečňují různé matematické operace. Díky těmto operacím se provádí identifikace osoby.
  - porovnávací modul – zde se na základě získaných příznaků porovnává s daty, které jsou uloženy v databázi.

- *Rozhodovací modul* – zde se provádí závěrečné rozhodnutí, jestli jsou snímané údaje shodné s daty, které jsou uloženy v databázi.

[2]

Mezi hlavní přednosti biometrických systémů jednoznačně patří ***jedinečnost*** (uniqueness). To znamená, že žádní dva lidé nemají stejné biometrické charakteristiky. Mezi další výhody biometrických systémů patří :

- ***Univerzálnost*** (universality) – každý člověk je nositelem biometrických charakteristik.
- ***Permanence*** (permanence) – biometrické charakteristiky lidí se nemění s časem (stárnutí).
- ***Jednoduchost*** (simplicity) – biometrické charakteristiky jsou měřitelné a získané charakteristiky jsou jednoduché a přesné.
- ***Přijatelnost*** (acceptability) – samotné snímaní charakteristik je nenáročné.

3.5.1 Identifikace podle otisku prstu

Identifikace podle otisku prstu je jednou z nejstarších, neznámějších a nejvíc rozšířených biometrických metod. Jedná se o nejvíc využívaný způsob pro identifikaci nejen v kriminalistice, ale i u různých bezpečnostních a přístupových systémů. Na základě referenčního vzorku dokáží velmi rychle identifikovat oprávněnou osobu a umožnit ji oprávněný přístup do objektu, prostoru, přístup do určitých systémů atd. Identifikace podle otisku prstu patří do skupiny daktyloskopických identifikací. Daktyloskopie je nauka o obrazech papilárních linií (papila = bradavka) na vnitřní straně článků prstů a dlaní člověka. U daktyloskopie se využívají tří základní neměnné faktory papilárních linií a ty jsou:

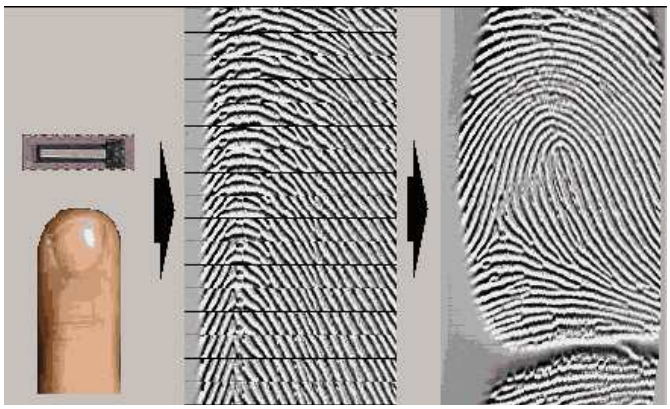
- na světě nenajdeme dva jedince se stejnými obrazci papilárních linií,
- papilární linie jsou po celý život relativně neměnné a
- obrazce papilárních linií jsou neodstranitelné (výjimkou je odstranění zárodeční vrstvy kůže).

3.5.1.1 Metody zachycení otisku prstu (roller finger)

a) Získání otisku pomocí papíru a inkoustu – jedná se o klasickou metodu získávání otisku prstů. Používá se ve forenzní oblasti. Prstem se roluje po papíře k získání otisku celého prstu.

b) Statické snímání – nejběžnější metoda snímání otisku. Prst se přitiskne na senzor a bez jakéhokoliv pohybování dojde k sejmutí otisku. Výhodou je jednoduché ovládání, avšak musíme dodržovat základní pravidla při snímání (moc netlačit na čočku, nepootáčet s prstem pří snímání – deformace linií apod.)

c) Snímání šablonováním – prstem se přejíždí po senzoru, který snímá prst. Obraz se skládá z pásů, které snímač následovně skládá k identifikaci. Ke snímání se používá křemíkový snímač. [16]



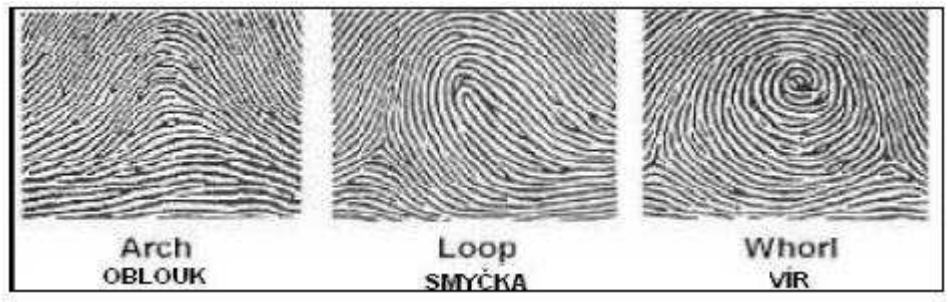
Obr. 28 Ukázka šablonového snímání

3.5.1.2 Klasifikace otisků prstů

Tzv. Henryho systém rozděluje otisky prstů do následujících tříd:

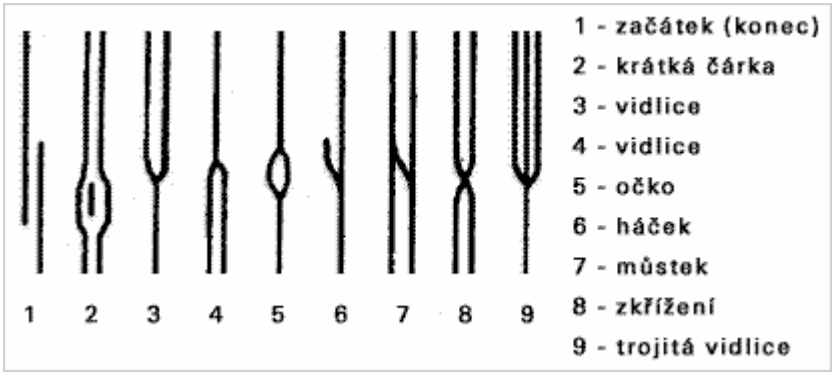
- Závit (Whorl)
- Levá a pravá smyčka (Loap)
- Oblouk (Arch)
- Špičatý oblouk (Tented Arch)

Tyhle se následně mohou dále dělit na další podskupiny, čímž při správném zařazení urychlíme porovnávání až o několik řádů (př. Loap – radial, ulnar; Whorl – plain, double loap, whorls, accidental whorl apod.).



Obr. 29 Ukázka některých tříd otisků

K samotné identifikaci osoby nám však nepostačuje určení třídy (vzoru) daktyloskopického otisku prstu. Aby došlo k individuální identifikaci, musíme ještě určit shodnost individuálních znaků, resp. zvláštností papilárních linií, které se obecně nazývají markanty.[2]



Obr. 30 Ukázka základních markant papilárních linií

3.5.1.3 Snímače otisků prstů

Ke snímání otisku prstu nám slouží mnoho desítek metod založených na nejrůznějších fyzikálních principech, které se neustále zdokonalují a nalézají se nové a nové metody. Pojďme se podívat na ty, co se již používají:

a) Optické snímače
   - na základě odrazu (reflexní)
   - reflexní se skládáním obrazu
   - bezdotykový odraz
   - transmisní

b) Elektroluminiscenční snímače

c) Kapacitní snímače
   - křemíkové čipy a kapacitní snímač
   - kapacitní snímač a TFT
   - TFT optické

d) Tlakové snímače
   - vodivá membrána na silikonu
   - vodivá membrána na TFT
   - dotekové mikro-elektro mechanické spínače

e) Rádiové snímače

f) Teplotní senzory

g) Ultrazvukové snímače

h) Fotonové krystaly

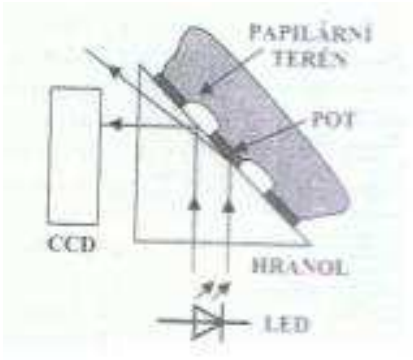
i) Snímače povrchové impedance

3.5.1.3.1 Optické snímače

Optické senzory využívají odlišných vlastností odrazu světelného paprsku v papilárním terénu snímaného otisku, kde vlivem potu v papilárním prostředí dochází ke změně optických vlastností optického hranolu a vytvoření snímaného obrazu na CCD snímačích. Korekce zkreslení a neostrostí obrazu, vzniklých v důsledku rozdílných optických drah paprsků vytvářejících obraz otisku prstu a vlivu vlhkosti na snímací ploše hranolu, se provádějí volbou indexu lomu materiálu snímacího hranolu, volbou úhlu pozorování snímací plochy a přídavnými korekčními optickými soustavami.

Aby byl při snímání otisku prstu eliminován vliv vlhkosti na kvalitu obrazu otisku prstu, je vhodné, aby snímací hranol byl navržen tak, aby hodnota úhlu mezi snímací plochou a průhledovou plochou, byla rovna, nebo větší než hodnota goniometrické fce arcsin podílu indexu lomu vody a indexu lomu materiálu snímacího hranolu. Pro zvýšení kontrastu a ostrosti obrazu otisku prstu je výhodný optický filtr. Jeho parametry jsou přizpůsobeny vlnové délce záření emitovaného světelným zdrojem a spektrální citlivosti CCD detektoru.

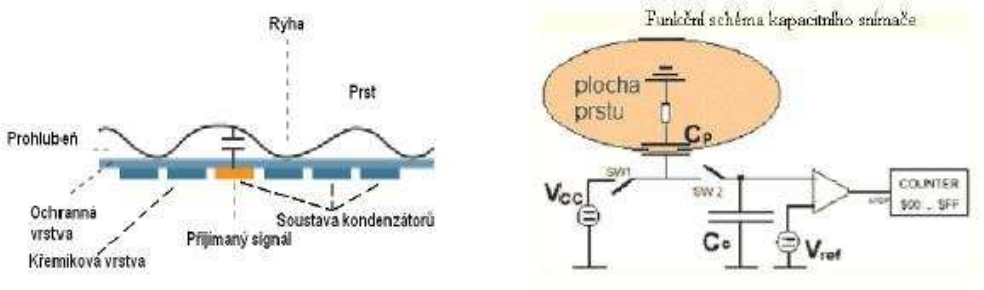
[2]



Obr.31 Optické snímání otisku prstu

3.5.1.3.2 Kapacitní snímače

Kapacitní snímače měří kapacitu mezi kůži prstu a aktivními pixely. Velikost měřeného elektrického pole se mění mezi rýhami a prohlubněmi struktury papilárních linií jako příčinna změny dielektrika mezi jednou deskou kondenzátoru – pixelem a druhou deskou kondenzátoru – prstem. Dielektrikem je v našem případě buď vzduchová vrstva (prohlubeň- pixel) nebo pokožka (rýha - pixel). Citlivá snímací plocha je tvořena tisíci kondenzátory.



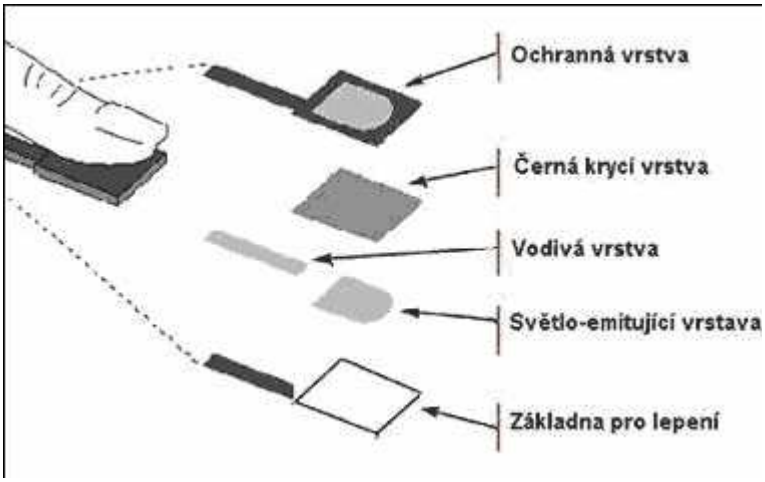
Obr. 32 Kapacitní snímání otisku prstu

3.5.1.3.3 Tlakové snímače

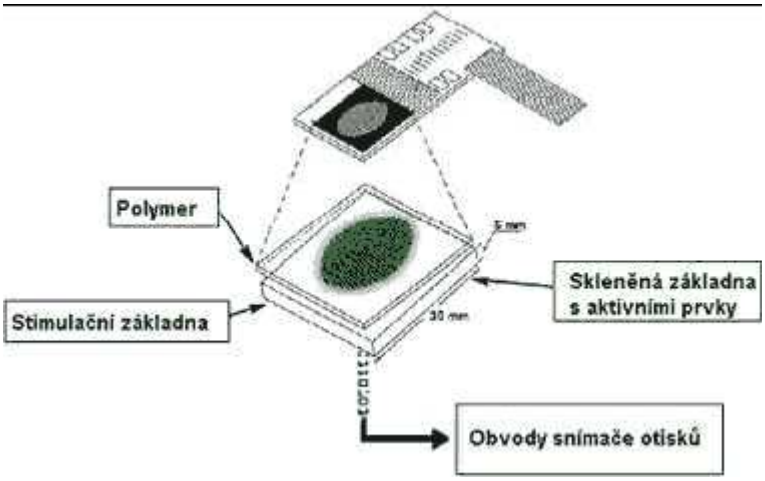
Tyto snímače reagují na tlak papilárních linií na povrch snímače a za pomocí miniaturních tlakových čidel, nebo mikrospínačů jej převádějí na elektrický proud. Papilární linie vyvolávají na snímané ploše lokální tlakové působení, zatímco tlak v rýhách je nižší. Výhodou je, že pracují dobře jak v suchém, tak i vlhkém prostředí.

3.5.1.3.4 Elektroluminiscenční snímače

Elektroluminiscenční senzory jsou jedny z nejnovějších mezi snímači otisku prstů. Snímací plochou je zde polymer, jenž se skládá z několika vrstev. Nejdůležitějsší vrstvou je vrstva, která emituje světlo v místech, kde na ní tlačí papilární linie prstu. Ve vrstvě polymeru se pak vytvoří vlivem tlaku papilárních linií obraz otisku prstu důsledkem emise světla. Obraz je následně detekován polem fotodiod, které jsou součásti skleněné základny. Obraz je pak transformován do digitálního formátu elektronikou, která je zabudována do skleněné základny. V konečné fázi je obraz zaslán do databáze v digitální podobě. Výhodou elektroluminiscenčních snímačů jsou malé rozměry, dobré rozlišení, relativně nízká cena, kvalita otisku se nesnižuje když je prst extrémně suchý. Naopak však je méně odolný vůči mechanickému poškození či vůči znečištění.[2]



Obr. 33 Polymer, který tvoří snímací plochu snímače



Obr. 34 Konstrukce elektroluminiscenčního snímače

3.5.1.4 Požadavky na snímače prstů

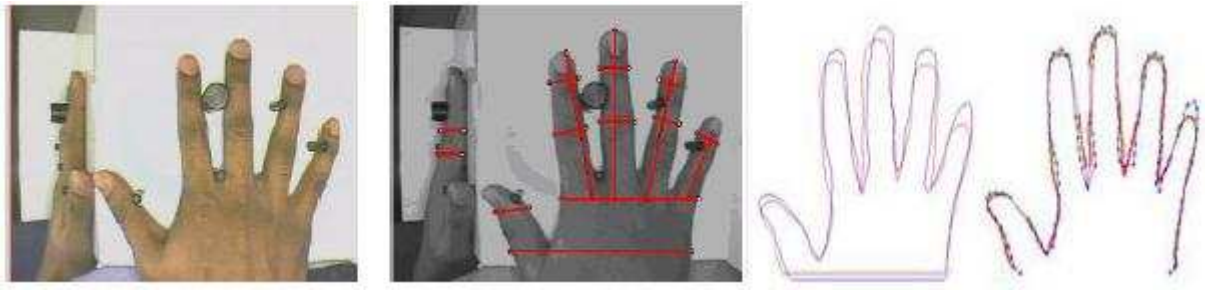
- Vyhovující celkové rozměry – Lehká splnitelnost u systému kontroly vstupu, které jsou určeny pro přístup do místností, budov apod. U přístupu do PC, notebooku je miniaturizace neodmyslitelná.
- Dostatečně velká snímací plocha – Aby bylo zaznamenáno co nejvíce identifikačních znaků – markant z otisku prstu.
- Dostatečné rozlišení – Kvalitní obraz by neměl být zkreslený, měl by mít dostatečný kontrast a měl by obsahovat co nejširší škálu rozsahu šedé barvy (kvůli vysokému jasovému rozlišení.

- Odolnost vůči mechanickému poškození – Snímače by měli být odolné vůči případnému mechanickému poškození.
- Uživatelská přívětivost – Jedná se o základní požadavek na systém vůči uživateli a ergonomii snímače.
- Životnost snímačů – Jde hlavně o konstrukční prvky snímačů, u kterých je vlivem opotřebení omezena životnost. Jsou to především materiály chránící snímací plochu proti poškození.
- Opakovatelnost dosažené kvality obrazu otisku prstu – Aby bylo dosaženo dobrých výsledků při autentizaci z hlediska hodnot chyby prvního a druhého druhu je důležitá opakovatelnost kvality obrazu otisku.
- Dostatečná ochrana vůči napodobeninám – Snímače v dnešní době nezabezpečují dostatečnou ochranu vůči napodobeninám. Řešením tohohle problému je v dodatečné ochraně kamerovým systémem, nebo přítomností ostrahy.

[16]

3.5.2 Identifikace podle morfologie ruky (geometrie ruky)

Tato metoda je založena faktu, že každý člověk má jedinečný tvar ruky, který je od určitého věku osoby neměnný. Snímače využívají jednoduchého principu měření a 3D snímání délky, šířky, tloušťky a povrchu ruky konkrétního člověka umístěné na podložce s pěti polohovými kolíky pomocí CCD kamery.



Obr. 35 Ruka se zrcadly snímaná CCD kamerou a příklad měření vzdáleností

Spíše než k identifikace se tato metoda užívá k verifikaci, protože není natolik přesná jako kupř. otisky prstů. Je vhodná pro větší databáze uživatelů, nebo pro uživatele s malým

přístupem. Biometrické systémy založené na verifikaci ruky jsou používány v různých aplikacích docházkových a přístupových systémů, kde jsou velmi rozšířené.

Mezi nevýhody patří, že lidé s onemocněním kloubů, popřípadě podobnými vady, můžou mít potíže s přiložením ruky ke snímači. Mezi další patři proměnlivost velikosti ruky z důvodu zhubnutí nebo přibrání na váze uživatele.

Obr. 36 Snímací zařízení morfologie ruky

3.5.3 Identifikace podle oční duhovky

Duhovka je sval, který je uvnitř oka, který reguluje velikost čočky na základě světla dopadajícího na oko. Ke snímání duhovky je zapotřebí velice kvalitní digitální kamery a infračerveného osvětlení oka. Během mapování se duhovka mapuje do fázorových diagramů, které obsahují informaci o orientaci, četnosti a pozici specifických plošek. Tyto informace pak slouží k vytvoření duhovkové mapy a šablony pro identifikaci.

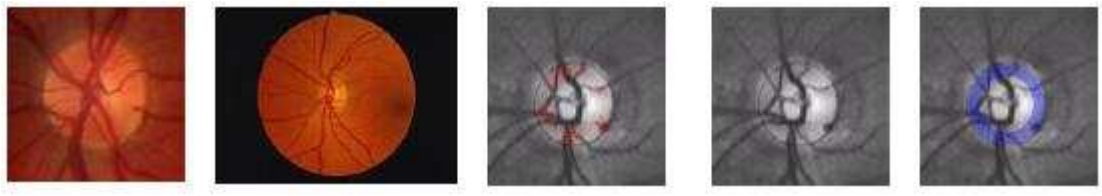
Obr. 37 Popis duhovky a snímání biometrických dat duhovky

Nenalezneme lepší biometrickou charakteristiku, která by poskytovala více rozlišovacích možností. U každého člověka se duhovky liší, stejně tak se liší i pravá a levá duhovka u jedince. Mezi výhody patří, že je to bezkontaktní metoda, velmi rychlá a především přesná.

Obr. 38 Snímač oční duhovky

3.5.4 Identifikace podle oční sítnice

Pro identifikaci osoby podle její sítnice oka, se užívá obraz struktury cév na pozadí lidského oka v okolí slepé skvrny. Pro získání obrazu se používá zdroj světla s nízkou intenzitou záření a opto-elektrický systém (kvůli riziku nebezpečného ozáření se používá jen jedna IR LED dioda). verifikace sítnice je velmi přesnou metodou identifikace. Její používání vyžaduje od uživatele, aby se díval do přesně vymezeného prostoru, což může být pro některé osoby nepříjemné a někdy až nemožné, pokud používají brýle. Z těchto důvodů nemá tato metoda rozšířenou oblast používání a její použití se vztahuje na oblasti vůbec nejvyššího stupně zabezpečení. [16]

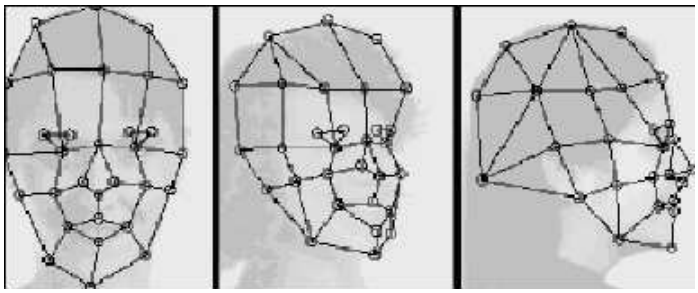


Obr. 39 Lokalizace sítnice a ukázka některých charakteristik sítnice

3.5.5 Identifikace podle geometrie tváře

Rozpoznávání na základě geometrie tváře je založeno na srovnávání obrazu, který je sejmut kamerou s obrazem, jenž je uložen v databázi. Po rozpoznávání se používají tzv.

šedé obrazy. Jako příznaky pro rozpoznávání slouží většinou tvar obličeje a poloha opticky významných míst na tváři (oči, nos, ústa, obočí) a vzájemná vzdálenost mezi nimi. Neuchovává se přesná poloha jednotlivých významných míst, ale ukládá se vzdálenost očí, vzdálenost rtů od nosu, úhel mezi špičkou nosu a okem apod. Software nejdříve vyhledá oči jako temné body v horní polovině obrazu a odtud se pak pokouší najít další významné charakteristiky. Nedojde-li k určení pozice očí, další rozpoznávání již neprovádí, protože by bylo zbytečné. Mezi výhody patří, že je to bezkontaktní systém. Nevýhodou jsou problémy, které mohou nastat při identifikaci dvojčat.[16]



Obr. 40 Síť vytvořená elastickým mapováním obličeje

3.5.6 Identifikace podle hlasu

Je založena na analýze řeči identifikované osoby. Lidská řeč je charakterizována svou akustickou strukturou (amplitudově frekvenční spektrum měnící se v čase), lingvistickou strukturou (gramatika a skladba řeči) a subjektivním projevem osoby (inotace, rytmus, barva halsu apod.). Zdrojem řečníkových kmitů jsou řečové orgány, tzv. vokálový trakt. Ten se skládá z hlasivek, dutiny hrdelní, ústní a nosní, měkkého a tvrdého patra, zubů, jazyka. Tvar těchto orgánů nám způsobuje, že rezonance vokálního traktu je u každé osoby odlišná.

Rozlišujeme dva přístupy u identifikace podle hlasu a to:

- textově závislé (text dependent) – osoba musí říct předem danou, definovanou frázi.
- textově nezávislé (text independent) – osoba může říct jakoukoliv frázi.

[2]

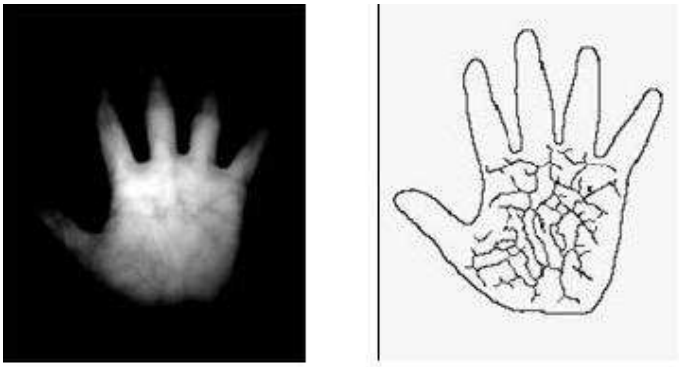
3.5.7 Identifikace podle dynamiky podpisu

Každá osoba má jedinečnou dynamiku podpisu při psaní. K identifikaci podle dynamiky podpisu je zapotřebí speciálního pera a speciální podložky na provedení podpisu. Biometrický systém pak porovnává podpis osoby s uloženým podpisovým vzorem v databázi. Mezi míru dynamických charakteristik patří napětí, tlak pera, zrychlení v jednotlivých částech podpisu, sklon jednotlivých znaků, rychlost psaní, dráha a doba pohybu pera na papíře.

Obr. 41 Ukázka biometrického pera s podložkou

3.5.8 Identifikace podle žil na rukách

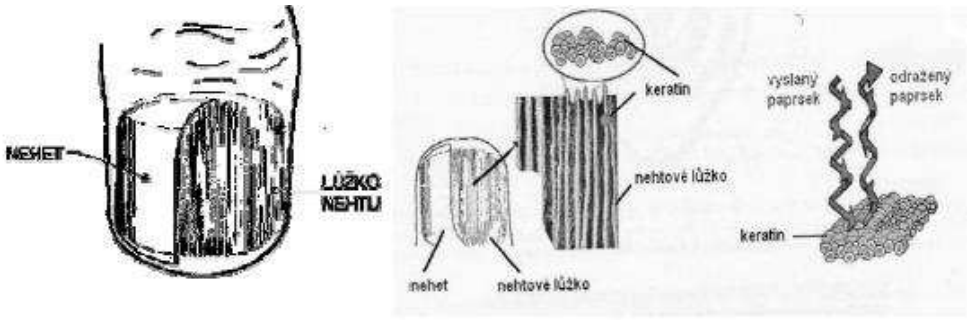
Identifikace podle žil na rukách spočívá ve snímání hřbetu ruky speciální kamerou v IR světle. Tak lze získat černobílý obraz stromové struktury žil, které tvoří zřetelný vzorec. Struktura krevního řečiště se navíc v dospělém věku příliš nemění, je velice výrazná a je jedinečná i mezi jednovaječnými dvojčaty, což prokázaly i některé vědecké studie. Výhodou je také bezkontaktní princip (uživatel se nemusí dotýkat povrchu snímače, což zvyšuje hygienu a pravděpodobnost správného přijmutí uživatele).[16]



Obr. 42 IR snímek dlaně a extrahované žíly dlaně

3.5.9 Identifikace podle nehtu

Nehet má na svém povrchu určité nerovnosti, které kopírují strukturu lůžka nehtu. Ta je unikátní u každého člověka a na každém prstu. Lůžko nehtu je tvořeno paralelní podkožní strukturou, která se nachází pod nehtem. Ta se skládá z podélných vrstev různých šířek. V prostoru mezi nehtem a nehtovým lůžkem se nachází keratin, což je přírodní polymer, který mění orientaci dopadajícího světla. Když necháme dopadat paprsek polarizovaného světla na nehet pod určitým úhlem, na odraženém paprsku je možné sledovat fázové změny paprsku na přijímači. Po zpracování signálu získáme číselnou sekvenci čárového kódu, který lze porovnat v databázi.



Obr. 43 Struktura nehtu a identifikace podle podélného rýhování

3.5.10 Další biometrické identifikační systémy

- Identifikace podle DNA
- Identifikace termovizními obrazy
- Verifikace podle způsobu pohybu očí
- Verifikace podle vrásnění článků prstů
- Verifikace podle tvaru článků a pěstí
- Identifikace podle dynamiky klávesových úderů
- Verifikace a identifikace podle pachu
- Biometrie ušního boltce
- Verifikace osob podle tvaru a pohybu rtů
- Identifikace podle spektroskopie kůže
- Verifikace podle biometrických vlastnosti zubů

4 NORMY ČSN

Základní normou, která se zabývá Systémy kontroly vstupu je norma ČSN EN 50133 a pak norma ČSN CLC/TS 50398, která se zabývá kombinovanými a integrovanými systémy.

4.1 ČSN EN 50133-7

Tato norma nám udává pokyny k použití automatizovaných systémů kontroly vstupů a komponentů uvnitř a vně budov na základě souboru norem EN 50133. Zahrnují návrh systému, instalaci, předávání, provoz a údržbu systémů kontroly vstupů. Pokyny jsou určeny pro systémy kontroly vstupů pro použití v bezpečnostních aplikacích. Zahrnuje oblasti od jednoduchých systémů pro řízení jednoho přístupového místa až po složité systémy s mnohanásobnými přístupovými místy. Systém kontroly vstupu umožňuje ovládat a monitorovat výstupní ovládací prvky a senzory přístupového místa (apas), které však nejsou zahrnuty do těchto pokynů. Systém kontroly vstupů může být propojen s jinými systémy (například: Elektrické zabezpečovací systémy). Tato norma však neurčuje, zda má nebo nemá být v daných objektech instalován automatizovaný systém kontroly vstupů. [17]

Systém kontroly vstupů zahrnuje všechny konstrukční a organizační náležitosti společně se zařízením požadovaným k ovládání vstupů.

Posláním systému kontroly vstupů je:

a) rozhodnout

- kdo má poskytnutý vstup
- kde může být přístup získán
- pokud systém funkci poskytuje, kdy je přístup povolen

b) minimalizovat riziko nepovoleného vstupu

Pozornost je věnována zvláště minimalizaci omezení oprávněného uživatele.

Zavedení systému kontroly vstupů se řídí následujícím pořadím:

a) projekt (návrh) systému

b) instalace systému

c) předání systému

d) provoz systému

e) údržba (servis) systému

Podle informací získaných od zákazníka a na základě výsledku analýzy rizik je nutno vzít v úvahu pro každé přístupové místo následující:

- klasifikace zabezpečení vstupu a výstupu (identifikace, časový filtr, ukládání dat),
- četnost průchodu uživatelů (počet osob v časovém úseku),
- vztah k ostatním systémům (např. EZS, CCTV, administrativnímu systému atd.),
- bezpečnostní požadavky (např. nouzové východy, požární ochrana atd.),
- požadavky na hlášení (např. displeje, ukládaní dat, výstraha atd.),
- provoz systému kontroly vstupů v poruchových podmínkách (např. potřeba náhradního zdroje napájení, selhání zařízení nebo kabelu atd.),
- charakter prostředí instalačního místa,
- další důležité podmínky (riziko vandalizmu atd.),
- počet uživatelů a úrovní přístupu s přihlédnutím jak k současné, tak i předpokládané budoucí potřeby,
- umístění zařízení,
- snadnost provozu (používání, ovládání, obsluhovatelnost atd.),
- spolupráce s uživateli (motivování, školení atd.),
- mechanická pevnost přístupového místa a konstrukce budovy korespondující se stupněm zabezpečení,
- nezbytnost zajištění průchodu pouze jedné osoby v daném čase apas,
- způsob návratu přístupového místa do uzavření (např. automatické zařízení zavírání dveří),
- kabelové trasy, typ kabelu, maximální délka kabelu,
- vhodnost identifikačního zařízení (životnost zařízení, průchodu uživatelů, prostředí atd.),
- provozní uspořádání pro přístupové místo (bezrizikový režim při poruše, zabezpečení při

poruše atd.),

- opatření pro tělesně postižené osoby,

- opatření pro zásilky a zavazadla,

- správa (ovládání) systému (programování, ohlašování).

Navíc k výše uvedeným údajům je nutno vzít v úvahu pro systém s více místy přístupu:

- stupeň zabezpečení přístupových míst vedoucích do stejného zabezpečeného prostoru,

- celkový počet uživatelů a úrovní přístupu beroucích v úvahu jak současnost, tak i předpoklad budoucích potřeb,

- kapacita zařízení k ukládání do paměti,

- komunikační spoje (dosažitelnost, spolehlivost, bezpečnost) mezi různými montážními místy a/nebo dalšími systémy,

- koordinace ohlašovacích funkcí (místo, postup, způsob atd.).

Norma nám dále udává požadavky na:

a) **Instalaci** - Způsoby elektrické projekce se řídí stávajícími národními a místními předpisy. Dříve než se zahájí práce, je nutno vzít v úvahu veškeré bezpečnostní požadavky.Komponenty se instalují v místech se známou a definovanou úrovní zabezpečení provozu a přístupnosti pro údržbu a servis.

- Zařízení - Zařízení se instaluje podle pokynů výrobce. Při výběru místa instalace se zohledňuje přístupnost a snadnost používání.
- Napájecí zdroj
- Kabeláž
- Revize

b) **Předávání** - Předmětem předávání je převedení odpovědnosti z projektové a instalační firmy na kupujícího. Podmínky předání mezi těmito stranami se jasně definují.

c) **Provoz** - Provoz a ovládání systému kontroly vstupů je v odpovědností kupujícího.

Odpovědností správce je zajistit:

- školení uživatelů,
- poskytnutí písemných instrukcí uživatelům, ovládání systému a záloha dat,
- seznamování a motivování uživatelů ke správnému využívání systému,
- aktualizování databáze systému,
- odezvu na jakoukoliv výstrahu,
- organizování údržby systému,
- plnění národních předpisů týkajících se databází.

d) **Údržbu** - K zajištění správné funkce systému jsou prováděny v dohodnutých intervalech údržba, prověrky, prohlídky a servis.

e) **Dokumentaci** - Dokumentace nezbytná pro instalaci, provoz, schvalování a údržbu systému kontroly vstupu je přizpůsobena rozsahu a složitosti instalovaného systému.

[18]

4.2 ČSN CLC/TS 50398

Tato norma nám uvádí všeobecné požadavky a typy struktur kombinovaných a integrovaných poplachových systémů. Norma zajišťuje integraci jedné nebo více aplikací do jednoho integrovaného systému. Tento dokument poskytuje další informace týkající se prvotního návrhu (projektu) systému, plánování, instalace, předávání, provozu a údržby (servisu) kombinovaného a integrovaného systému. Norma specifikuje požadavky na poplachové systémy, které jsou kombinovány nebo integrovány s jinými systémy, které mohou a nemusí být poplachovými systémy. Dále definuje požadavky týkající se pravidel integrace s cílem zdůraznit význam jednotlivých aplikačních poplachových norem a objasňuje případné rozpory. [21]

Norma nám specifikuje tři konfigurace nebo typy integrovaných poplachových systémů:

- *Typ 1* – aplikovatelný pro kombinaci a integraci jednoúčelových poplachových systémů.
- *Typ 2A* – aplikovatelný pro kombinaci a integraci poplachových systémů a nepoplachových systémů, používající společné přenosové trasy, společná zařízení a společná vybavení. Porucha v kterékoliv aplikaci nemá žádny negativní účinek na

jakoukoliv další poplachovou aplikaci. K dosažení tohoto stavu je potřebné znásobení (nadbytečnost).

- *Typ 2B* – aplikovatelný pro kombinaci a integraci poplachových systémů a nepoplachových systémů používajících společné přenosové trasy, společná zařízení a společné zařízení. Porucha v jedné aplikaci může mít negativní účinek na jinou poplachovou aplikaci.

[20]

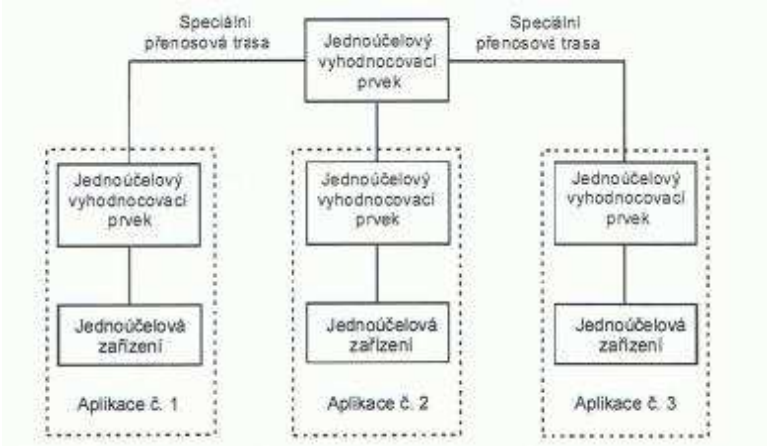
Typ 1

Konfigurace typu 1 je kombinací dvou nebo více jednoúčelových systémů. Tyto jednoúčelové systémy jsou připojeny ke společnému doplňkovému zařízení, například propojením přes doplňkovou přenosovou trasu.

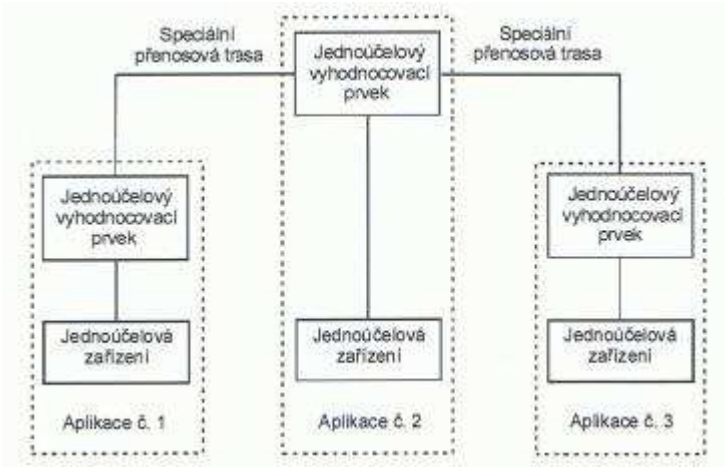
Zařízení v konfiguraci typu 1 vyžadované normou v poplachové aplikaci nesmí být v žádném provozním stavu nepříznivě ovlivněno jakýmkoli dalším jednoúčelovým systémem nebo jakýmkoli doplňkovým zařízením.

[20]

Obr. 44 Příklad konfigurace typu 1



Obr. 45 Příklad konfigurace typu 1, ústřední ovládací zařízení (CCF) třídy 1

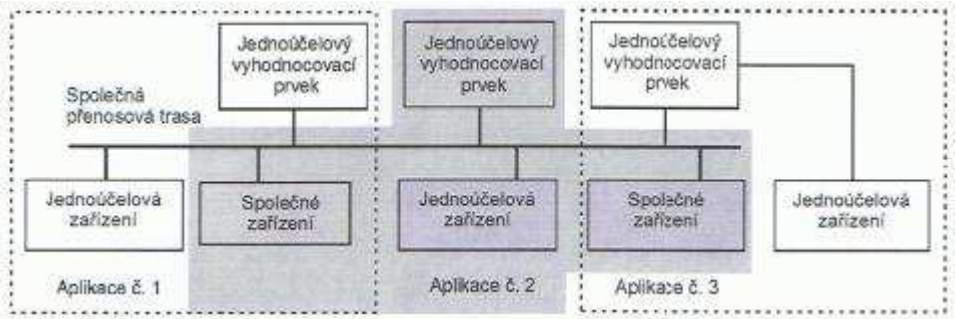


Obr. 46 Příklad konfigurace typu 1, ústřední ovládací zařízení (CCF) třídy 2

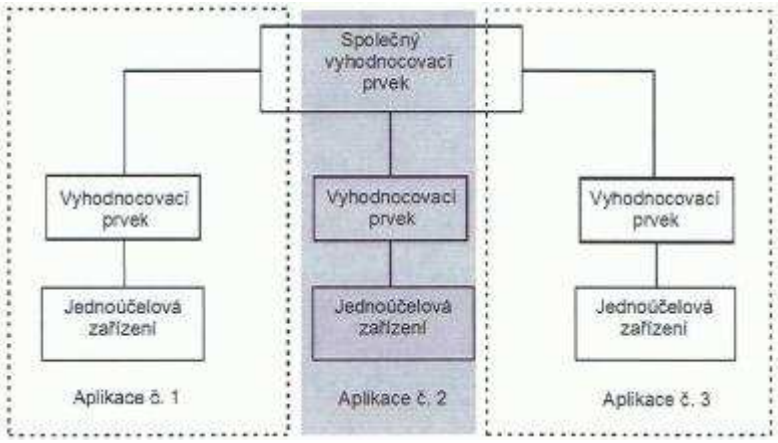
Typ 2

Konfigurace typu 2 je kombinací dvou nebo více jednoúčelových systémů, všechny využívají normou vyžadované zařízení společné nejméně pro jednu aplikaci.

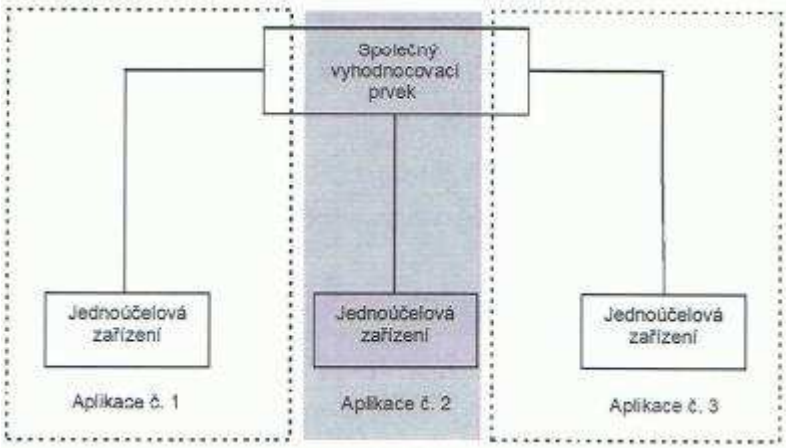
Konfigurace typu 2 jsou dále rozděleny na Typ 2A a Typ 2B. [20]



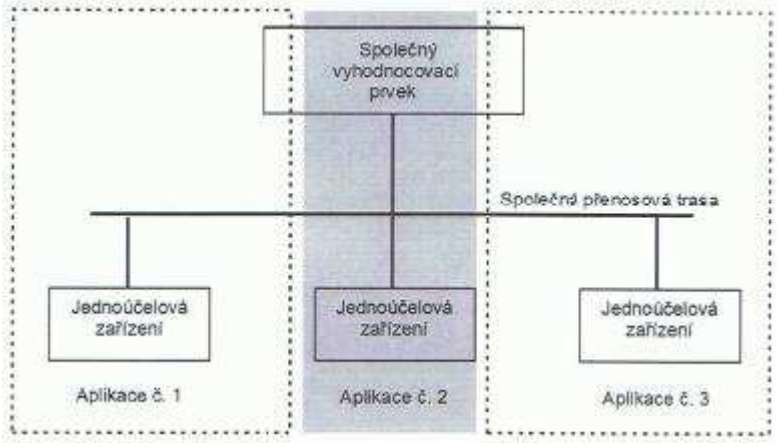
Obr. 47 První příklad konfigurace typu 2



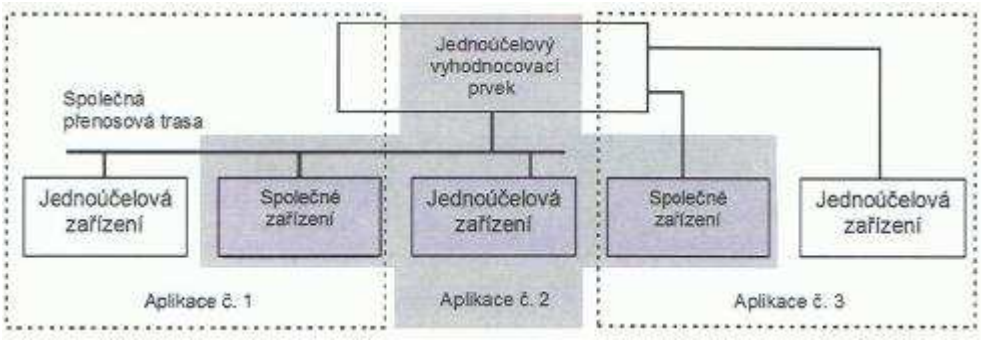
Obr. 48 Druhý příklad konfigurace typu 2



Obr. 49 Třetí příklad konfigurace typu 2



Obr. 50 Čtvrtý příklad konfigurace typu 2



Obr. 51 Pátý příklad konfigurace typu 2

Typ 2A

V konfiguraci typu 2A nesmí být integrita jakéhokoli normou vyžadovaného poplachového zařízení v jakékoli aplikaci být nepříznivě ovlivněna žádnou poruchou v jiné aplikaci.

Typ 2B

V konfiguraci typu 2B může být integrita jakéhokoli každého normou vyžadovaného poplachového zařízení v jakékoli aplikaci ovlivněna jedinou poruchou v jiné aplikaci.

[20]

Systémové požadavky a stanovení kompatibility

Integrovaný poplachový signál musí být navržen tak, aby nebyla žádná funkce aplikace v normálním stavu nepříznivě ovlivňována žádnou jinou aplikací.

V rámci kombinovaných a integrovaných systémů mohou být povelové signály přenášeny z jedné aplikace do jiné nebo z ústředního ovládacího zařízení (CCF) do dalších částí aplikace.

[20]

Norma nám dále udává požadavky na:

a) **Přístupové úrovně** – musí být v souladu s normou vyžadovanými úrovněmi pro každou aplikaci a nesmí umožnit neoprávněný přístup k jakékoli aplikaci.

b) **Návrh pro konfiguraci jednotlivých typů**

c) **Společné ovládací zařízení** – jakékoli manuální ovládání musí být jasné a jednoznačné.

d) **Společné signalizační zařízení**

- Požadavky na spolehlivost
- Signalizace informace
- Priority – Informace musí být signalizovány v pořadí priorit jasným a jednoznačným způsobem.

e) **Integritu normou vyžadovaných prvků pro zpracování poplachu**

f) **Připojení k poplachovému přenosovému systému** - jsou-li poplachové systémy připojeny k poplachovému přenosovému systému, musí tento systém splňovat odpovídající normy pro poplachové přenosové systémy..

g) **Propojení** – Jsou-li k zařízení splňujícím požadavky norem připojena zařízení nesplňující jednu nebo více aplikačních norem, musí splňovat požadavky dané touhle normou.

h) **Napájecí zdroje** – Speciální a/nebo společná zařízení nesmí ohrozit požadavky na napájení odpovídající příslušným aplikačním normám.

i) **Požadavky na časování**

j) **Současný výskyt událostí** - Systém musí být navržen tak, aby současný výskyt událostí každého typu v případě více než jedné aplikace neohrozil integritu žádné aplikace.

k) **Prověření provozuschopnosti**

l) **Centrální ovládací zařízení (CCF)**

m) **Dokumentace a školení** - dokumentace kombinovaného a integrovaného systému musí být stručná, úplná a jednoznačná. Poskytované informace musí být dostatečné pro montáž, uvedení provozu, vlastní provoz a údržbu systému.

5 DALŠÍ VÝVOJ INTEGROVANÝCH SYSTÉMŮ

Jednotlivé systémy se již nepoužívají jako samostatná řešení, ale jsou integrovány do flexibilních celků prostřednictvím architektury klient/server. Výsledkem je bezpečnostní koncept, který splňuje nároky na vysokou kvalitu a pružně se přizpůsobuje požadavkům zákazníka. Vývoj těchto systému se v posledních letech zaměřuje na požadavky zákazníka. Snaží se vyhovět jeho potřebám, potřebám zabezpečení jeho prostor apod.

Rozsáhlé systémové integrace s využitím běžných uživatelských rozhraní jsou jedním z klíčových prvků moderních bezpečnostních systémů. U kombinace sledování docházky, kontroly vstupu, poplachových a tísňových zabezpečovacích systémů už není funkční vzájemné propojení jediným hlediskem. Moderní systémy integrace vyžadují praktické ovládání, správu systému.

Do budoucna se bude zaměřovat na nadřazené dohledové systémy pro řízení rizik, které shromažďují informace z jednotlivých systémů do společného uživatelského rozhraní a je možné řídit celý systém z jediného počítače. To například umožňuje zobrazit informace ze systému kontroly vstupu o pohybu osob v v budově v jakoukoli dobu.

Potenciál pro integraci s využitím různých kombinací hardwarových a softwarových funkcí je obsažen v softwaru pro kontrolu přístupu. Vývoj stále nových softwarů, které by byly uživatelský přívětiví jde stále směrem dopředu.

6 PŘEDSTAVENÍ ŘEŠENÍ SYSTÉMU KONTOLY VSTUPU

Pro praktickou část své práce – návrh přístupového systému - jsem si vybral řešení od české firmy EFG CZ, spol. s r.o. Tato společnost působí na českém a slovenském trhu již 15 let a nabízí ucelený soubor produktů v oblasti bezpečnostních systémů. Od dodávky jednotlivých systémů přešla k systémové integraci v oblasti bezpečnosti, identifikace a komunikace. Největší podíl v působnosti firmy zaujímá vlastní přístupový a docházkový systém prezentovaný pod obchodním označením Aktion. SW i HW tohoto systému je vyvíjen přímo společností EFG CZ, spol. s r.o. a díky své otevřenosti je snadno integrovatelný do softwarových řešení třetích stran, jako jsou např. informační systém Lotus Notes, SAP, PERSIMS a Helios. Z oblasti bezpečnostních integračních a vizualizačních systémů jsou plně podporovány systémy C4, AlVis, kamerové systémy.

6.1 Výrobní program

Vlastní výrobní program společnosti EFG CZ, spol. s r.o. lze shrnout do těchto bodů:

I. docházkové terminály
   - řada SingleCon
   - řada MultiCon
   - řada ProfiCon

II. přístupové kontroléry
   - řada SingleCon
   - řada MultiCon

III. snímače
   - provedení APR
   - provedení .NEXT
   - provedení OEM

6.2 Docházkové terminály

Docházkové terminály jsou vyráběny ve třech řadách – SingleCon a MultiCon a ProfiCon.

6.2.1 SingleCon

Řada SingleCon je určena pro malé a střední aplikace. Provedení SingleCon představuje terminál TSC/E, který může fungovat na sběrnici systému Aktion nebo autonomně s přímým připojením do Ethernetu. Membránová klávesnice obsahuje 6 předdefinovaných tlačítek se symboly docházkových funkcí, 3 volně programovatelná tlačítka, 3 ovládací tlačítka a 2 tlačítka pro změnu průchodu. Terminál disponuje jedním programovatelným výstupním relé (dveřní zámek, siréna,..) a má integrovaný bezkontaktní snímač s dosahem 10-15 cm. Podporované formáty identifikačních médií jsou H4102 (Unique, EM Marin), High Security a Mifare. Dále umožňuje připojení externích snímačů (formát Wiegand 26b nebo Wiegand 46b), odchodového tlačítka či snímačů stavu dveří. LCD displej má 4x20 znaků

Obr. 52 Terminál TSC/E

6.2.2 MultiCon

Provedení MultiCon je již určeno pro střední a velké aplikace. Spolupracuje pouze ve spojení s řídící jednotkou (kontrolérem) MultiCon. Řada Multicon je reprezentována

terminály TMC/L s membránovou klávesnicí a TPC/L s dotykovým displejem. Funkce a vlastnosti jsou shodné s terminálem TSC/E.

Obr. 53 Terminál TPC/L

6.2.3 ProfiCon

Řada ProfiCon reprezentovaná terminálem TPC/E je postavená na bázi průmyslového PC s barevným dotykovým TFT displejem. Terminál funguje autonomně s přímým připojením do Ethernetu. Je vybaven bezkontaktním snímačem a volitelně může být doplněn biometrickým snímačem otisku prstů. Stejně jako u předchozích řad je ovládání výstupních zařízení umožněno volně programovatelným relé a obsahuje vstupy pro připojení odchodového tlačítka a snímaní stavu dveří.

Obr. 54 Terminál TPC/E

6.3 Přístupové kontroléry

Přístupové kontroléry slouží k přímému budování systému kontroly vstupu.

6.3.1 SingleCon

Podobně jako u docházkových terminálů je rada SingleCon určena pro malé aplikace. Řídící kontrolér KSC/E může opět fungovat na sběrnici systému Aktion nebo autonomně s přímým připojením do Ethernetu. Kontrolér umožňuje ovládání jedněch dveří oboustranně nebo dvou dveří jednostranně a dalších zařízení pomocí 3 volně programovatelných relé. Obsahuje dva vstupy pro připojení čteček formátu Wiegand 26b nebo Wiegand 42b, 2 vstupy pro odchodové tlačítko, 2 vstupy pro dveřní kontakt a samotný kontrolér je vybaven tamperem.

Obr. 55 Kontrolér KSC/E

6.3.2 MultiCon

Řada MultiCon je již určena pro rozsáhlé aplikace. Řídící kontrolér KMC/E v kombinaci s dveřními moduly umožňuje ovládat až 32 dveří na jedné lince RS 485. Jsou podporovány funkce Antipassback a Messenger (vazby mezi vstupy a výstupy na fyzicky jiných modulech). Maximální kapacita paměti této sestavy je 65 535 událostí nebo 51 000 osob. Jednotka KMC/E je připojena do Ethernetu a na sekundární linku RS 485 lze připojit až 15 modulů MMC nebo terminálů TMC. Kontrolér KMC/E stejně jako moduly MMC opět umožňují připojení dvou bezkontaktních snímačů (Wiegand 26b nebo Wiegand 42b), 2 tlačítek a 2 snímačů stavů dveří. K ovládání zařízení slouží 3 volně programovatelná relé. Adresa modulu na lince RS 485 se nastavuje pomocí DIP přepínačů.

Obr. 56 Kontrolér KMC/E

6.4 Snímače

Přestože lze k terminálům, kontrolérům a modulům Aktion připojit libovolné čtečky s výstupem Wieagand 26b nebo Wieagand 42b, vyrábí firma EFG CZ spol. s r.o. také vlastní bezkontaktní snímače v širokém sortimentu. Jak již bylo zmíněno výše, jsou podporovány formáty identifikačních médií H4102 (Unique, EM Marin), High Security a Mifare. Z hlediska provedení snímačů jsou dostupné klasické modely, provedení s integrovanou PIN klávesnicí a biometrické modely s integrovaným snímačem otisku prstů. Designové provedení je dostupné ve více variantách od základního OEM provedení v lištové krabici, přes nejrozšířenější podobu APR až po novou designovou řadu .NEXT s výměnnými barevnými kryty. Ze speciálních aplikací lze zmínit bezkontaktní snímače jiskrově bezpečně, tedy do prostředí s nebezpečím výbuchu, snímače pro PDA do CF slotu nebo sní mače připojitelné do portu USB.

Obr. 57 Bezkontaktní snímače APR-P20/FP a AXR-100

6.5 Softwarová řešení

Společnost EFG CZ spol. s r.o. nabízí modulární softwarové balíky pro efektivní využití funkcí vlastního HW. Patří mezi ně:

6.5.1 Software Aktion.ONE

Aktion.ONE je ekonomické řešení docházkového systému malého rozsahu. Zákazník si pořizuje pouze HW a SW je provozován na serveru společnosti EFG CZ spol. s r.o. formou placené služby. SW je uživateli zpřístupněn pomocí webového rozhraní na adrese www.dochazkaonline.cz. Pro přihlášení do profilu zákazníka je nezbytná autorizace. Software není omezen počtem zaměstnanců (identifikátorů) ani modulů v systému.

6.5.2 Software Aktion.LITE

Aktion.LITE je ekonomickou verzí SW Aktion (OEM licence), která není omezena počtem identifikátorů, ale nabízí pouze základní systémové funkce pro řízení pohybu osobu a vjezdu vozidel

6.5.3 Software Aktion Complete

Aktion Complete je profesionální přístupový systém umožňující plné využití HW Aktion. Modulářní řešení nabízí softwarové moduly, které přizpůsobí systém kontroly vstupu a evidence docházky potřebám uživatele. Mezi nejběžnější patří:

- Základní modul Aktion administrace a kontrola vstupů (ACL)

- Evidence docházky (MDO)
- Modul evidence výrobních operací (EVO)
- Messenger, správa událostí (AMM)
- Intranetová nadstavba AktionWEB (AWB)
- Komunikační software (Aktion Device Manager – ADM)
- a další.

SW Aktion běží na databázovém serveru ACS v prostředí MS SQL 2000 s operačním systémem MS Windows XP Professional.

6.5.4 Stravovací software Astris

Stravovací systém automatizuje objednávky a kontrolu výdeje stravy v různých způsobech stravovacích zařízení. Umožňuje propojení se skladovou evidencí, účtování plateb do mzdového systému či komunikaci přes intranet a Internet. Možnost sestavování jídelníčku včetně sledování nutričních hodnot lze s výhodou využívat nejen ve variantě pro nemocniční stravování.

7 NÁVRH SYSTÉMU KONTROLY VSTUPU

Jako příklad pro praktický návrh systému kontroly vstupu jsem si vybral administrativní budovu fiktivní společnosti MYŠ, s.r.o. Přístupové body budou na všech vstupech do budovy a na všech kancelářích, kontrola vstupu spojená s evidencí docházky bude aplikována na turniketech u hlavních vchodu a vyšší stupeň zabezpečení bude použit u přístupových bodů v hlavní serverovně a jednotlivých patrových serverovnách. Řešení je postaveno na prvcích systému Aktion představených v předchozí kapitole. Návrh je zpracován s souladu s předpisy, normami ČSN a katalogy platnými v době zpracování

7.1 Rozsah projektu

V rámci instalace ACS bude provedena instalace dvou kontrolérů KMC/E, dveřních modulů, docházkových terminálů a vlastních čteček. Součástí dodávky budou i zámky, dveřní otvírače a dvojice tripodových turniketů. Centrální částí systému ACS bude aktivní prvek (switch) a server, na kterém poběží SW aplikace Aktion.

Umístění prvků systémů ACS je zřejmé z půdorysných výkresů podlaží, uspořádání sběrnice a napájení systému z blokového schématu.

7.2 Podklady pro zpracování projektu

Pro zpracování této projektové dokumentace bylo použito následujících podkladů:

- výkresová dokumentace stavební části
- projednání s investorem
- technické specifikace jednotlivých zařízení
- konzultace s dodavateli techniky

7.3 Předpisy a normy

Použitá zařízení, tj. instalované prvky el. systému kontroly vstupu, vyhovují ustanovením norem řady ČSN EN 50 133.

7.4 Základní technické údaje

7.4.1 Rozvodné soustavy

- provozní 1-NPE, 230V, 50 Hz, TN-S
- prvky systému ACS 12V DC, SELV
- napájení turniketů 230V AC

7.4.2 Vnější vlivy

Ve vnitřních prostorách vybavených prvky ACS je prostředí normální dle ČSN 33 2000-3. Vně objektu, kde je prostředí dle ČSN 33 2000-3 klasifikováno jako zvlášť nebezpečné, nejsou žádné prvky systému ACS umístěny.

7.4.3 Ochrana před úrazem el. proudem a druh uzemnění

Ochrana před úrazem el. proudem a druh uzemnění je provedena podle ČSN 33 2000-4-41 takto:

- ochrana před nebezpečným dotykem živých částí
    - izolací živých částí a kryty
    - minimální krytí vnitřní elektrické instalace musí být IP20.
- ochrana před nebezpečným dotykem neživých částí:
    - ZÁKLADNÍ (v prostorech normálních i nebezpečných):
        - síť TN: ochrana je provedena samočinným odpojením od zdroje nadproudovými jisticími prvky. Skříň všech zdrojů systému ACS musí být uzemněny.
        - napájení ACS 12 V DC: ochrana před nebezpečným dotykem živých i neživých částí malým napětím SELV.
    - ZVÝŠENÁ (v prostorech zvlášť nebezpečných):
        - zde nejsou instalovány prvky ACS - tato ochrana zde není použita
    - DOPLŇKOVÁ (v prostorech zvlášť nebezpečných):

- Zde nejsou instalovány prvky ACS - tato ochrana zde není použita.

7.5 Technická část

Zařízení systému kontroly vstupu (dále jen ACS) slouží pro zamezení přístupu osob bez patřičného oprávnění do zabezpečených prostor.

7.5.1 Systém ACS a docházka

Systém ACS je navržen dle požadavků investora. Pro ovládání systému ACS budou na všech přístupových bodech instalovány bezkontaktní snímače (čtečky) typu APR-P20 (bez zadání PIN), pouze u dveří pro vstup do serverovém a pokladny budou použity čtečky APR-PK20 (s možností zadání PIN). K evidenci docházky a současně ovládání turniketů budou instalovány docházkové terminály TMC/L.

Systémem ACS budou ovládány dveřní otvírače BeFo 211211, elektromechanické samozamykací zámky BERA-W a triodové turnikety ATR 900 dodané v rámci systému ACS. Dále budou ovládány automatické posuvné dveře dodané v rámci stavby.

Dveřní moduly MMC a docházkové terminály TMC/L budou po sběrnici RS 485 připojeny k celkem dvěma řídícím kontrolérům MultiCon typu KMC/E. Tyto kontroléry budou pomocí síťového rozhraní připojeny k řídícímu serveru ACS instalovanému v datovém rozvaděči v serverovně v 1. NP. Na serveru poběží SW aplikace Aktion.

Součástí dodávky bude také 150 identifikačních médii – klíčenek typu Keyfob.

Přesné rozmístění techniky a její schématické zapojení je zřejmé z výkresové části. Naprogramování systému ACS bylo provedeno dle pokynů uživatele v etapě zkušebního provozu včetně přiřazení přístupových práv konkrétním osobám. Vlastní zapojení techniky – jednotek, čtecích hlav, otvíračů, zámků a turniketů musí být provedeno v souladu s montážními a instalačními návody a s doporučeními jednotlivých výrobců.

7.5.2 Napájení a zálohování systému ACS

Systém je v normálním provozním režimu napájen ze síťového rozvodu 230V/50 Hz. K zajištění napájení zařízení jsou využity vlastní zdroje ACS a to 3 ks zdroje typu KPN–18-30LAW, 1 ks zdroje KPN-12-18LA a 2 ks zdroje AXSP K40/5A. Zdroje budou vždy

v příslušné serverovně, jeden zdroj bude napájet výhradně zámky a otvírače, druhý bude použit pro jednotky ACS.

Zdroje budou napájeny ze samostatně jištěného okruhu 230 V z příslušného patrového rozvaděče NN. Přívod bude proveden kabelem CYKY – J 3x1,5 a před samotnými zdroji bude instalována přepěťová ochrana 3. stupně. Příslušný jistič musí být v rozvaděči označen nápisem *„ACS NEVYPÍNAT“*.

Pro zajištění časově omezeného provozu v případě výpadku sítě bude každý zdroj ACS vybaven vlastním náhradním zdrojem 12V DC (olověný bezúdržbový akumulátor s kapacitou 12 nebo 18 Ah).

Přechod napájení na záložní napájení z akumulátoru je zajištěn automaticky, bez rušivého vlivu na funkci zařízení.

7.5.3 Použité kabely a nosné trasy

Datové propojení mezi kontroléry a síťovými prvky bude provedeno kabelem UTP cat. 5e. Sběrnice systému ACS bude realizována datovým kabelem Belden 9501. Pro rozvody napájení 12V DC od zdrojů ACS bude použit flexibilní kabel HO5VV-F 2x1 nebo HO5VV-F 2x2,5.

Bezkontaktní snímače (čtečky) budou ke dveřním jednotkám připojeny sdělovacími kabely typu FI-HX08/02.

Otvírače a zámky budou ke dveřním jednotkám připojeny kabelem LAM 6X (2x0,8 napájení + 4x0,4 přenos informace o stavu dveří).

Hlavní kabelovou trasou, společnou pro slaboproudé systémy, bude kabelový žlab instalovaný ve zdvojené podlaze. Jeho dodávka není součástí ACS. Hlavní trasa bude doplněna elektroinstalačními PVC ohebnými trubkami uloženými samostatně v konstrukci podlahy, v konstrukci příček nebo v konstrukci podhledu.

7.6 Ostatní požadavky

7.6.1 Provedení rozvodů vedení

Při montáži musí být dodrženy předpisy o bezpečnosti a ochraně zdraví při práci. Instalace kabelových tras musí být provedena dle příslušných ČSN a předpisů na ně navazujících.

Dle ČSN 34 2300 a ČSN 33 2000-5-52 je nutné dodržet odstup kabelových tras od silnoproudých rozvodů do 1 kV - 20 cm. Při souběhu kratším jak 5m lze snížit odstup až na 6 cm a při křižování až na 1 cm. Veškeré průchody a průrazy mezi požárními úseky musí být po montáži protipožárně utěsněny.

7.6.2 Revize

Požadavky na provádění výchozí a pravidelných revizí elektrických instalací vyplývají z obecně závazných právních předpisů platných v České republice. Každé elektrické zařízení musí být během výstavby a (nebo) po dokončení, před tím, než je uživateli uvedeno do provozu, revidováno.

7.6.3 Pravidelná údržba

Aby byla trvale zaručena správná funkce systému, je nutné provádět pravidelnou údržbu (provádět pravidelné prohlídky, funkční zkoušky a servisní úkony).

- pod pojmem pravidelné prohlídky se rozumí provedení takových činností a prací, které jsou nezbytné pro vystavení posudku o stavu zařízení v provozu
- funkční zkoušky se uskutečňují po provedení revize elektrické instalace systému, následně pak ve lhůtách stanovených servisní smlouvou

7.7 Závěr

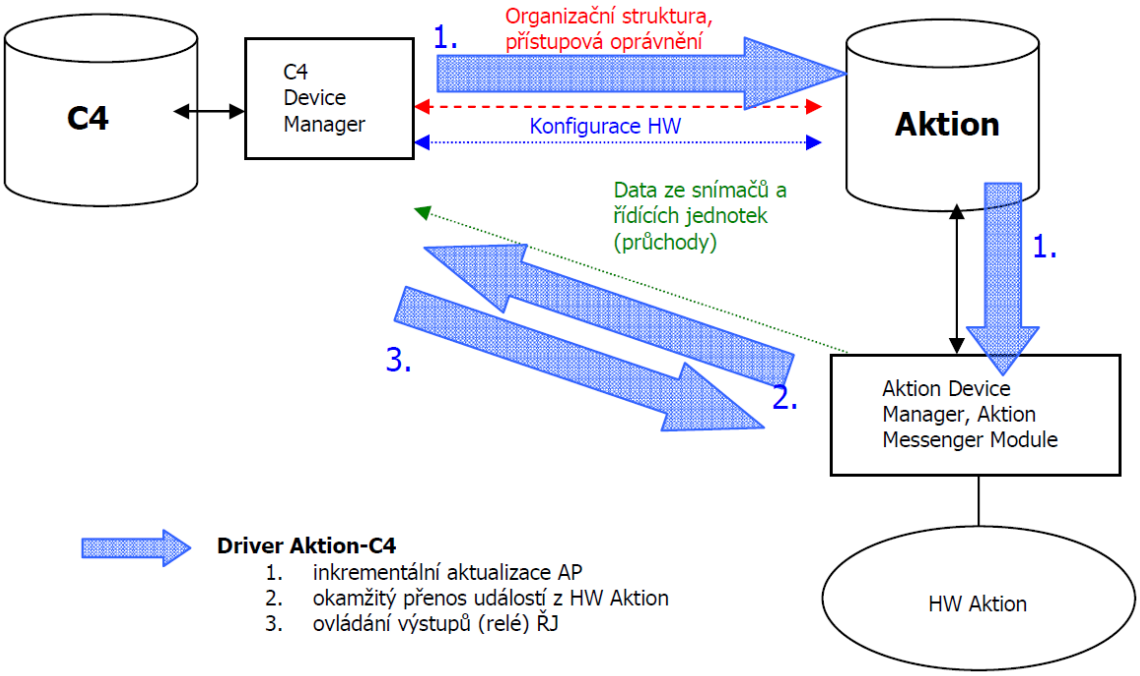
Projekt je zpracován v souladu s platnými předpisy ČSN, EN a s předpisy výrobce zařízení.

Výrobky (zařízení), které budou nainstalovány v rámci této instalace, vyhovují zákonu č. 22/97 Sb. ve znění pozdějších předpisů (Zákon o technických požadavcích na výrobky) a prováděcím předpisům (nařízením vlády).

8 PROPOJENÍ SYSTÉMU AKTION A INTEGRAČNÍHO SW C4

Na závěr uvádím příklad integrace systému Aktion do vizualizační nadstavby C4. Systém Aktion provádí samotnou funkci kontroly přístupu, evidence docházky a výrobních operací a C4 zajišťuje správu osob včetně přístupových oprávnění a vizualizaci systému. Propojení je realizováno na více úrovních. Informace o osobách, jejich profily a přístupová oprávnění jsou předávána (replikována) na úrovni databází. On-line komunikaci s hardwarovými moduly Aktion zajišťuje komunikační modul ADM.

8.1 Úrovně propojení



Obr. 58 Propojení systému Aktion a systému C4

8.1.1 Synchronizace údajů

Primárním zdrojem dat je SW C4 a jejich import do Aktionu řeší procedura. Synchronizují se údaje o osobách, přístupová oprávnění a identifikátory.

8.1.2 Nastavení oprávnění

Primárním zdrojem je opět SW C4. Aktualizace probíhá inkrementálním způsobem, kdy je provedena aktualizace databáze (dále jen DB) Aktion z databáze C4 nejdéle do 60 s od uložení záznamu do DB C4.

8.1.3 Uživatelské role

Uživatelské role jsou v obou systémech nezávislé, vlastní pro každý systém

8.1.4 Nastavení hardwaru

Zde je primárním zdrojem Aktion. Nastavení je importováno do C4 pomocí exportního souboru, jehož obsahem jsou data o struktuře HW a jeho umístění (adresa)

8.1.5 Transfer událostí

Události vyčtené ze systému ACS jako průchody osob a stavy vstupů a výstupů jsou okamžitě předávány do SW C4 softwarovým modulem ADM pomocí funkce Messenger.

8.1.6 Ovládání HW Aktion

Přímé ovládání hardwaru Aktion ze SW C4 je rovněž umožněno využitím komunikačních kanálů modulu Messenger. Lze tak např. spínat relé pro ovládání dveřních zámků, atd. Stavové informace jsou ukládány do DB Aktion, odkud jsou okamžitě předávány do DB C4 – viz předchozí bod.

ZÁVĚR

Na ochranu majetku je díky stále novým bezpečnostním prvkům a systémům kladen čím dál tím vyšší důraz nejen právnickými, ale i fyzickými osobami. Proto bychom si měli uvědomit, že tento tlak, který je vyvíjený na bezpečnostní systémy, ať už se jedná o PZTS, MZS, CCTV nebo ACS nejen v průmyslu komerční bezpečnosti, velkých firmách, podnicích, ale v dnešní přemodernizované době i domácnostech je naprosto na místě.

Systémy kontroly vstupu umožňují jednoduchou a pohodlnou kontrolu přístupu do vybraných prostor. Kde na základě přístupových práv je přístup umožněn, nebo zamítnut. Dále evidují a monitorují pohyb osob, která osoba kde byla, v jakém čase a brání přístupu nepovolaných osob do daných prostor. Tyto systémy nacházejí čím dál tím větší uplatnění nejen u velkých firem s větším pohybem zaměstnanců, ale i u menších podniků, popřípadě fyzických osob, které si uvědomují hodnotu svého majetku, dat a hlavně Know-how.

V dnešní době je hodně kladen důraz na integraci systémů a kombinaci s dalšími. Toto nám umožňuje dosáhnout vysokého stupně zabezpečení, jednoduchou obsluhu a přehledný monitoring. Základním předpisem, kterým se máme řídit při instalaci kombinovaných a integrovaných systémů je ČSN CLC/TS 50398, která nám udává všeobecné požadavky a typy konfigurací kombinovaných a integrovaných poplachových systémů, které musí být respektovány, když se do poplachového systému integruje jedna nebo více aplikací.

Na trhu s bezpečnostními systémy je k dispozici spousta zabezpečovacích systémů, prostředků. Je tedy velmi důležité vybrat si ten pro nás nejvhodnější výrobek, který bude uspokojovat naše nároky na potřebné zajištění, kontrolu vstupu. Nejlepším možným řešením je obrátit se na specializované firmy, které se zabývají zabezpečovacími systémy. Ty nejen pomůžou s výběrem toho nejvhodnějšího systému, produktu, ale i s jejich návrhem, instalací a uvedení do provozu včetně případných revizí a oprav.

K zajištění objektu systémy kontroly vstupu je nutné přistupovat individuálně, dle různých kritérií. Mezi tyhle kritéria může patřit o jaký objekt, prostory se jedná, co se v něm nachází, jak moc chceme, aby byl omezen, chráněn, evidován či monitorován přístup do něj.

ZÁVĚR V ANGLIČTINĚ

Protection of property is still due to new security features and systems put an increasing emphasis not only legal, but also individuals. Therefore, we should recognize that the pressure that is exerted on the safety systems, whether on PZTS, MZS, CCTV and ACS both in the commercial security industry, large companies, enterprises, but today modernized time is perfectly at home place.

Access control systems allow for easy and convenient control access to selected areas. Where access rights on the basis of access is granted or rejected. Furthermore, record and monitor the movement of a person she was, what time and prevents unauthorized access to the premises. These systems are increasingly used not only for large companies with more movement of employees, but also for smaller companies or individuals that realize the value of its assets, mainly data and know-how.

Nowadays a lot of emphasis on systems integration and combination with others. This allows us to achieve a high degree of security, simple operation and easy monitoring. The core provisions, which we manage the installation of combined and integrated systems is ISO CLC / TS 50398, which gives us the general requirements and types of configurations, combined and integrated alarm systems, which must be respected when the alarm system integrates one or more applications.

On the market for safety systems is available a lot of security systems, devices. It is therefore very important to choose the best product for us, which will meet our demands required to ensure access control. The best possible solution is to turn to specialized companies that deal with security systems. They not only help you choose the most suitable system, the product, but also their design, installation and commissioning, including any revisions and corrections.

To ensure the building, room access control systems must be treated individually, according to various criteria. Among these criteria may include what the object space is what it is, how much we want to be restricted, protected, registered and monitored access to it.

SEZNAM POUŽITÉ LITERATURY

[1] KINDL, Ing. Jiří. Projektování bezpečnostních systému I. druhé. Zlín : Univerzita Tomáše Bati, 2007. 134 s. ISBN 978-80-7318-554-1.

[2] ČANDÍK, Ph.D., Ing. Marek. Objektová bezpečnost II. první. Zlín : Univerzita Tomáše Bati, 2004. 100 s. ISBN 80-7318-217-3.

[3] Doc. LUKÁŠ, Ing. Luděk. *Nadstandartní prvky objektové bezpečnosti*. Zlín : Zlín, 2007. Systémy kontroly vstupu jako zdroj informací o pohybu zaměstnanců I, s. 82-193.

[4] *Kompet : identifikační a bezpečnostní systémy* [online]. 2004 [cit. 2010-04-2]. Dostupné z WWW: <http://www.kompet.cz/str12.htm>.

[5] KOLAJA, Martin. *Využití prístupových systému v prumyslu komercní bezpecnosti*. Zlín, 2006. 67 s. Bakalářská práce. Univerzita Tomáše Bati.

[6] Electronic lock. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 20.4.2010, last modified on 20.4.2010 [cit. 2010-05-29]. Dostupné z WWW: <http://en.wikipedia.org/wiki/Electronic_lock>.

[7] Čárový kód. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 14.4.2008, last modified on 12.5.2010 [cit. 2010-05-29]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Čárový_kód>.

[8] *Čárový kód* [online]. 2009 [cit. 2010-05-5]. Dostupné z WWW: <http://www.carovykod.com/index.php?id=2&lang=cz>.

[9] *Kodys-Čárový kód* [online]. 2009 [cit. 2010-05-16]. Dostupné z WWW: <http://www.kodys.cz/carovy-kod.html>.

[10] *Karty s magnetickým pruhem* [online]. 2010 [cit. 2010-05-17]. Dostupné z WWW: <http://pandatron.cz/?535&karty_s_magnetickym_pruhem>.

[11] *Magnetické karty* [online]. 2009 [cit. 2010-05-20]. Dostupné z WWW: <http://www.inplastor.at/cz/plastikkarten/magnetkarten/index.html>.

[12] *Siemens - multifunkční čipové karty* [online]. 2007 [cit. 2010-05-20]. Dostupné z WWW: <http://www.itsolutions.siemens.cz/web/topics/main_topic7>.

[13] *Čtečka čipů - Dallas* [online]. 2006 [cit. 2010-05-20]. Dostupné z WWW: <http://www.aterm.cz/DSRS2130.htm>.

[14] *Vše o elektronice a programování : Bezkontaktní karty dobývají svět* [online]. 2009 [cit. 2010-05-21]. Dostupné z WWW: <http://hw.cz/Firemni-clanky/Elatec/ART321-Bezkontaktni-karty-dobyvaji-svet.html>.

[15] *Tesla : Bezkontaktní přístupový systém BES (RFID)* [online]. 2010 [cit. 2010-05-22]. Dostupné z WWW: <http://www.teslastropkov.cz/katalog/pristupove-systemy/pristupove-systemy-BES.htm>.

[16] ŠČUREK Ph.D., Mgr. Ing. Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi : Studijní text FBI VŠB TU Ostrava*. Ostrava : VŠB TU Ostrava, 2008. 58 s.

[17] MĚRKA, Petr. *IMA* [online]. 2006 [cit. 2010-05-22]. Biometrické technologie. Dostupné z WWW: <http://www.ima.cz/download/cz/aktuality/2infodenima/14_Merka_Bull_Biometrika_IMA.pdf>.

[18] Česká Republika. ČSN EN 50133-7 : Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích - Část 7: Pokyny pro aplikace. In *Česká technická norma*. 2000, 58303, s. 1-16.

[19] *ČSN EN 50133-7 - Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích - Část 7: Pokyny pro aplikace* [online]. 2008 [cit. 2010-05-23]. Technické normy. Dostupné z WWW: http://www.technickenormy.cz/csn-en-50133-7-poplachove-systemy-systemy-kontroly-vstupu-pro-pouziti-v-bezpecnostnich-aplikacich-cast-7-pokyny-pro-aplikace/

[20] Česká Republika. ČSN CLC/TS 50398 : Poplachové systémy - Kombinované a integrované systémy - Všeobecné požadavky. In *Česká technická norma*. 2009, 33 4597, s. 1-20.

[21] *Technické normy : ČSN CLC/TS 50398 - Poplachové systémy - Kombinované a integrované systémy - Všeobecné požadavky* [online]. 2008 [cit. 2010-05-25]. Dostupné z WWW: <http://www.technickenormy.cz/csn-clc-ts-50398-

poplachove-systemy-kombinovane-a-integrovane-systemy-vseobecne-pozadavky/>.

[22] *TZB info : Nová verze systému kontroly vstupu* [online]. 2010 [cit. 2010-05-25]. Dostupné z WWW: <http://www.tzb-info.cz/t.py?t=2&i=6487>.

[23] UHLÁŘ, Jan. Technická ochrana objektů. 1.vyd. Praha : [s.n.], 2001. 205 s. ISBN 8072510762

[24] LAUCKÝ, Vladimír. Technologie Komerční bezpečnosti I. 3.vyd. Zlín : [s.n.],2010. 81 s. ISBN 978-80-7318-889-4

[25] JUDR. ČERNÝ, Josef; Ing. IVANKA, Ján. *Systematizace bezpečnostního průmyslu : TECHNICKÉ PROSTŘEDKY A PRVKY ZABEZPEČOVACÍ TECHNIKY*. Zlín : Zlín, 2004. 38 s.

[26] *Přístupové systémy* [online]. 2006 [cit. 2010-05-20]. Dostupné z WWW: <http://www.micro.feld.cvut.cz/home/X34EZS/prednasky/08%20Pristupove%20systemy.pdf>.

[27] *EFG CZ : Katalogové listy a údaje o systémech* [online]. 2010 [cit. 2010-05-26]. Dostupné z WWW: <http://www.efg.cz/>.

[28] *Aktion : Katalogové listy a údaje o systémech* [online]. 2010 [cit. 2010-05-28]. Dostupné z WWW: <http://www.aktion.cz/>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACCESS	ACCESS control systems – Přístupové systémy.
CCF	Centrální ovládací zařízení.
CCTV	Closed Circuit Television - uzavřený televizní okruh.
ČSN	Česká státní norma.
EAN	European article number.
EN	Evropská norma.
EPS	Elektrická požární signalizace.
EZS	Elektrické zabezpečovací systémy.
IR	Infrared nebo Infrared Radiation – infračervené záření.
IS	Informační systém.
ISO	Význam od řeckého slova ἴσος (isos), znamenající stejný a odkazující na cíl organizace – standardizaci.
LED	Light-emitting diode – elektroluminiscenční dioda.
PC	Personal computer (Osobní počítač).
PIN	Personal identification number- osobní identifikační číslo.
PZTS	Poplachové zabezpečovací a tísňové systémy.
RFID	Radio Frequency Identification - identifikace na rádiové frekvenci.
SKV	Systém kontroly vstupu.

SEZNAM OBRÁZKŮ

SEZNAM PŘÍLOH

PŘÍLOHA P I: SOUPIS TECHNIKY A MATERIÁLU

Soupis techniky a materiálu			
Odběratel:	MYŠ, s.r.o.		
Název instalace:	Systém kontroly vstupu		
Zakázka:	xxx		
Typ	***Popis***	***Množ.***	***MJ***
Řídící jednotky			
KMC/E	Řídící kontrolér MultiCon	2	ks
MMC	Dveřní modul	17	ks
Prvky přístupového systému			
TMC/L	Docházkový terminál MultiCon	4	ks
APR-P20/B42CN	Bezkontaktní snímač, H4102, černá barva, Wiegand 42 bitů, konektor	28	ks
APR-P20/B42CB	Bezkontaktní snímač, H4102, černá barva, Wiegand 42 bitů, kabel 3 m	1	ks
APR-PK20/B42CB	Bezkontaktní snímač s klávesnicí, H4102, černá barva, Wiegand 42 bitů, kabel 3 m	7	ks
APR-P20/HS/USB	Bezkontaktní snímač, H4102, pro zadávání karet, USB	1	ks
ACA001	Odchodové tlačítko	5	ks
ATR900	Obousměrný rotační tripodový turniket s integrovanou řídící jednotkou, 230 V AC	2	ks
IDB-KEY	Bezkontaktní klíčenka typu Keyfob H4102	150	ks
Zámky			
BeFo211211	Dveřní otvírač BeFo PROFI se signalizací otevřených dveří, 12V DC, 230 mA	30	ks
LR0	Lišta rovná 250x25x3 (Zn)	30	ks
BERA-W 55	Elektromechanický zámek s kontrolou funkcí a blokací obou klik, 12V DC, 0,9A	2	ks
LRS	Lišta rovná, nerez	2	ks
Pap	Průchodka vnější, délka 280 mm	2	ks
Kabel6s	Prodlužovací kabel, 6 metrů, pro typy M,W	2	ks
KPCrD	Bezpečnostní kování pro samozamykací zámky, klika-klika, rozteč 92, pravé, chrom broušený	1	ks
KLCrD	Bezpečnostní kování pro samozamykací zámky, klika-klika, rozteč 92, levé, chrom broušený	1	ks
Napájecí zdroje			
KPN-18-30LAW	Napájecí zdroj 13,8V/3A v kovovém krytu, prostor pro akumulátor 12V/18Ah	3	ks
KPN-12-18LA	Napájecí zdroj 13,8V/1,8A v kovovém krytu, prostor pro akumulátor 12V/12Ah	1	ks
AXSP K40/5A	Napájecí zdroj 13,8V/5A v kovovém krytu, prostor pro akumulátor 12V/40Ah	2	ks
AKU 12V/12Ah	Olověný bezúdržbový akumulátor 12V/12Ah	4	ks
AKU 12V/18Ah	Olověný bezúdržbový akumulátor 12V/18Ah	2	ks

Přepěťová ochrana			
DA-275 DFI 6	Přepěťová ochrana s vf filtrem, SPD typ 3, 230 V AC, 6 A, signalizace poruchy	3	ks
Centrální prvky a licence			
SD205	Switch Linksys, 5x10/100 Mbps port s autodetekcí, plně duplexní	1	ks
R210	Server Dell R210, Intel Xeon 2.4GHz, 4 GB RAM, 2x 250 SATA 7.2k 3.5 HDD	1	ks
Win Server2008	Licence Microsoft Windows Server 2008	1	ks
MS SQL 2005	Licence Microsoft SQL Server 2005	1	ks
ACL/150	Základní modul administrace a kontrola vstupů, 150 identifikátorů	1	ks
ACL/150/Lc	Uživatelská licence pro kontrolu vstupů	5	ks
ADM/23	Komunikační software (Aktion Device Manager) pro 23 adresných bodů	1	ks
MDO/150	Modul evidence docházky pro 150 identifikátorů	1	ks
MDO/150/Lc	Uživatelská licence pro docházku	5	ks
AWB/150	AktionWEB, intranetová nadstavba, návštěvy, docházka, přítomnost	1	ks
AKT	Aktualizace SW Aktion na 1 rok	1	ks
Instalační materiál			
Belden 9501	Sdělovací stíněný kabel pro sběrnici RS-232/485	60	m
FI-HX08/02	Sdělovací kabel se zesíleným párem pro napájení	870	m
LAM 6X	Nízkofrekvenční sdělovací kabel 2x0,8+4x0,4	760	m
SXKD-5E-UTP-PVC	Instalační kabel UTP cat. 5, PVC plášť	50	m
HO5VV-F 2x1,5	Flexibilní vodič 2x1,5	90	m
HO5VV-F 2x2,5	Flexibilní vodič 2x2,5	70	m
CYKY-J 3x1,5	Kabel silový, 3x1,5	50	m
1225	Ohebná trubka, střední mechanická odolnost, Φ25, včetně příchytek a příslušenství	80	m
1232	Ohebná trubka, střední mechanická odolnost, Φ32, včetně příchytek a příslušenství	220	m
8130	Propojovací krabice 85x85x40	40	ks
8135	Propojovací krabice 105x105x40	15	ks
	Drobný instalační materiál	1	kpl

PŘÍLOHA P II: SPOTŘEBA I. NADPODLAŽÍ

		Spotřeba klidová (A)		Spotřeba maximální (A)	
Počet	*Zařízení*	*1 ks*	*celkem*	*1 ks*	*celkem*
7	BeFo 211211	0,000	0,000	0,230	1,610
2	BERA-W	0,220	0,440	0,900	1,800
	Celkem zámky		0,440		3,410
1	KMC/E	0,200	0,200	0,200	0,200
6	MMC	0,090	0,540	0,090	0,540
8	APR-P20	0,055	0,440	0,055	0,440
5	APR-PK20	0,070	0,350	0,070	0,350
4	TMC/L	0,140	0,560	0,140	0,560
	Celkem moduly		1,530		1,530

Spotřeba klidová	***zámky***	***0,44 A***	***CELKEM***	***1,970***
	moduly	***1,53 A***		
Spotřeba maximální	***zámky***	***3,41 A***	***CELKEM***	***4,940***
	moduly	***1,53 A***		

Kapac. akumulátoru při záloze (hod):	**12**	**28,69 Ah**

Výpočet kapacity akumulátoru uvažuje využití 85% jeho jmenovité kapacity !!!

PŘÍLOHA P III: SPOTŘEBA II. NADPODLAŽÍ

		Spotřeba klidová (A)		Spotřeba maximální (A)	
Počet	*Zařízení*	*1 ks*	*celkem*	*1 ks*	*celkem*
13	BeFo 211211	0,000	0,000	0,230	2,990
0	BERA-W	0,220	0,000	0,900	0,000
	Celkem zámky		0,000		2,990
1	KMC/E	0,200	0,200	0,200	0,200
6	MMC	0,090	0,540	0,090	0,540
12	APR-P20	0,055	0,660	0,055	0,660
1	APR-PK20	0,070	0,070	0,070	0,070
0	TMC/L	0,140	0,000	0,140	0,000
	Celkem moduly		1,470		1,470

Spotřeba klidová	***zámky***	***0 A***	***CELKEM***	***1,470***
	moduly	***1,47 A***		
Spotřeba maximální	***zámky***	***2,99 A***	***CELKEM***	***4,460***
	moduly	***1,47 A***		

Kapac. akumulátoru při záloze (hod): **12** **21,63 Ah**

Výpočet kapacity akumulátoru uvažuje využití 85% jeho jmenovité kapacity !!!

PŘÍLOHA P IV: SPOTŘEBA III. NADPODLAŽÍ

		Spotřeba klidová (A)		Spotřeba maximální (A)	
Počet	*Zařízení*	*1 ks*	*celkem*	*1 ks*	*celkem*
10	BeFo 211211	0,000	0,000	0,230	2,300
0	BERA-W	0,220	0,000	0,900	0,000
	Celkem zámky		0,000		2,300
0	KMC/E	0,200	0,000	0,200	0,000
5	MMC	0,090	0,450	0,090	0,450
9	APR-P20	0,055	0,495	0,055	0,495
1	APR-PK20	0,070	0,070	0,070	0,070
0	TMC/L	0,140	0,000	0,140	0,000
	Celkem moduly		1,015		1,015

Spotřeba klidová	***zámky***	***0 A***	***CELKEM***	***1,015***
	moduly	***1,015 A***		
Spotřeba maximální	***zámky***	***2,3 A***	***CELKEM***	***3,315***
	moduly	***1,015 A***		

Kapac. akumulátoru při záloze (hod):	**12**	**15,01 Ah**

Výpočet kapacity akumulátoru uvažuje využití 85% jeho jmenovité kapacity !!!

PŘÍLOHA P V: VÝKRESY V AUTOCADU

Výkres č. 001 – ACS, Půdorys 1.NP

Výkres č. 002 – ACS, Půdorys 2.NP

Výkres č. 003 – ACS, Půdorys 3.NP

Výkres č. 004 – ACS, Blokové schéma