Využití přístupových systémů v průmyslu komerční bezpečnosti

Martin Kolaja

Bakalářská práce
2006

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektrotechniky a měření
akademický rok: 2005/2006

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Martin KOLAJA**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Využití přístupových systémů v průmyslu komerční bezpečnosti**

Zásady pro vypracování:

1)Přehlednou formou zpracujte a popište strukturu přístupových systémů.
2)Rozveďte problematiku využití identifikačních systémů při elektronické kontrole vstupu.
3)Popište biometrické identifikační systémy v přístupových systémech.
4)Vysvětlete požadavky na systémy elektronické kontroly vstupu pro použití v zabezpečovacích aplikacích.
5)Zhodnocení problematiky přístupových systémů a nové trendy.

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

[1]Laucký V.,Technologie komerční bezpečnosti I.,Univerzita Tomáše Bati ve Zlíně 2003
[2]Laucký V.,Technologie komerční bezpečnosti II.,Univerzita Tomáše Bati ve Zlíně 2003
[3]Přístupové systémy,Magazin SECURITY,roč.VII,č.6/2000,s.3-14,ISSN 1210-8723
[4]Čandík M.,Objektová bezpečnost II.,Univerzita Tomáše Bati ve Zlíně 2004
[5]Krejčí J.,Požadavky na systémy kontroly vstupů pro použití v zabezpečovacích aplikacích,Magazin SECURITY,roč.VII,č.6/2000,s.24-25,ISSN 1210-8723
[6]Šiška V.,Identifikační systémy,Magazin SECURITY,roč.XII,č.2/2005,s.5-10,ISSN 1210-8723
[7]Vach M.,Biometrické systémy,Magazin Zabezpečovací systémy, roč.II, č.1/2005, s.9-10

Vedoucí bakalářské práce: **Ing. Jiří Kindl**

Datum zadání bakalářské práce: **14. února 2006**

Termín odevzdání bakalářské práce: **13. června 2006**

Ve Zlíně dne 14. února 2006

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

prof. Ing. Vladimír Vašek, CSc.
pověřený děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Předmětem této bakalářské práce je ukázat současné využití přístupových systémů v průmyslu komerční bezpečnosti. Systémy kontroly vstupu tvoří celá řada komponentů, které musí vytvořit kompatibilní přístupový systém, schopný zabezpečit vstup do požadovaného prostoru. Výstavba tohoto systému není rozhodně dílem jednoho člověka, nýbrž týmu odborníků, kteří se danou problematikou zabývají. Nejdůležitějším aspektem pro vytvoření spolehlivého přístupového systému je integrace s jinými systémy a spolupráce s mechanickými prostředky, což zvyšuje efektivnost zabezpečení, které uplatňuje průmysl komerční bezpečnosti.

Klíčová slova: průmysl komerční bezpečnosti, systémy kontroly vstupu, integrace, zabezpečení, mechanické prostředky

ABSTRACT

The subject of this bachelor work is depicting the contemporary usage of access systems in the commercial security industry. Access control systems consist of a number of components that must make a compatible access system which is able to secure the access into the required room. The construction of such a system is by no means the work of a single person, but of a team of specialists who concern themselves with the issue. The most important aspect for creating a reliable access system is the integration with other systems and the cooperation with mechanical means which heightens the effectivity of the safeguard applied in the commercial security industry.

Keywords: commercial security industry, access control systems, integration, safeguard, mechanical means

V úvodu této bakalářské práce bych rád poděkoval Ing. Jiřímu Kindlovi nejen za odborné připomínky a metodickou pomoc při psaní mé bakalářské práce, ale i za ochotný a vstřícný přístup, s nímž jsem se u něho při řešení vzniklých problémů vždy setkal.

Ve Zlíně 1. června 2006 …….

Jméno diplomanta

OBSAH

ÚVOD

V současné době se v naší společnosti čím dál více setkáváme s trestnou činností a stupeň ohrožení se doposud rok od roku zvyšuje. Tato skutečnost zapříčinila to, že se klade stále větší důraz na zabezpečení a ochrana vlastního majetku se stává prioritou. Pojem zabezpečení je úzce spjat s průmyslem komerční bezpečnosti, který se touto problematikou zabývá. Průmysl komerční bezpečnosti je obor, který je den co den vyspělejší a neustále vyvíjí nové technologie, které mají sloužit ještě k dokonalejšímu zabezpečení, než tomu bylo do této chvíle.

Tento obor zahrnuje velké množství produktů a systémů, které se snaží řešit veškeré problémy týkající se zabezpečení. Jeden ze systémů, kterým se tento obor zabývá, jsou také přístupové systémy.

Přístupové systémy se stávají nedílnou součástí zabezpečení objektů, zejména pak slouží k zpřehlednění pohybu vlastního i externího personálu v zájmových prostorech. Tyto systémy obsahují všechna konstrukční a organizační opatření, která se týkají zařízení nutných pro řízení vstupů. Hlídané objekty, kde je třeba monitorovat, evidovat a případně řídit přístup osob v souladu s jejich oprávněním bývají obvykle rozděleny do přístupových zón, v nichž jsou instalovány speciální elektronické snímače. Dle přístupových práv přidělených jednotlivým osobám je pak přístup do určitého prostoru povolen a nebo odepřen. Tedy abychom vše shrnuli, tak přehled o pohybu osob v objektu vzhledem k jejich povinnostem a oprávněním jsou stále významnějšími faktory, které firmy upřednostňují v rámci svých rozvojových cílů. Jedním z nástrojů, který pomáhá řešit tuto oblast, jsou modulární integrované přístupové systémy, které představují řešení s řadou standardních i nadstandardních služeb.

Neodmyslitelnou součástí přístupových systémů se staly identifikační systémy, které zasahují do nejrozmanitějších oborů lidské činnosti. Identifikace předmětů, identifikace činností a zejména osob se staly naprostou samozřejmostí. Můžeme tedy říci, že bez identifikačních systémů by přístupové systémy nesplňovaly dokonale svoji funkci.

Tato práce provede čtenáře celou strukturou přístupového systému a poté na jednom vybraném předvede způsob praktického využití. Cílem je seznámit čtenáře se systémem kontroly vstupu, zejména popsat jakým způsobem pracuje a jaké možnosti v současnosti nabízí.

1 OCHRANA OBJEKTŮ

Abychom dovedli chránit objekty před narušením, tak se musíme seznámit s různými formami ochrany objektů. Rozlišují se:

a) Klasická ochrana

Tato ochrana je založena na zajištění objektu pomocí mechanických zábran a zařízení, které znemožňují odcizení nebo poškození objektů, jejich částí, nebo cenných předmětů uvnitř objektů. I když patří mezi nejstarší způsob ochrany objektů, je hodně rozšířená a používaná jako základní forma ochrany objektu. V současnosti bývá kombinována s ostatními druhy ochrany, se kterými se vzájemně doplňuje.

b) Režimová ochrana

Představuje organizačně administrativní opatření a postupy, které vedou k zabezpečení správných funkcí ochranných systémů a jejich sladění s provozem chráněného objektu. Režimová ochrana je založena na zavedení uplatňování účinných směrnic – tzv. režimových opatření v chráněném objektu. Režimová opatření můžeme rozlišit:

- Vnější režimová opatření
  Týkají se vstupních a výstupních podmínek u chráněných objektů (prostorů), zejména kontroly vozidel a osob při vstupu a výstupu z chráněných prostorů.

- Vnitřní režimová opatření
  Týkají se pohybu uvnitř chráněného objektu, jako např. omezení pohybu vozidel a osob na určitém úseku chráněných prostor, monitoring pohybu materiálu a výrobků v objektu, zajištění osvětlení vybraných částí objektu apod.

c) Fyzická ochrana

Tato ochrana je prováděná fyzickou ostrahou objektu (hlídací služba).

d) Technická ochrana

Je založená na automatickém monitorování objektu pomocí technických prostředků objektové bezpečnosti. Technická ochrana představuje detekční systém zabezpečující předávání informací ve chráněném prostoru. Cílem použití technické ochrany je zvýšení efektivity (účinnosti) jiných forem ochrany objektu. Technická ochrana využívá k zabezpečení objektu:

- **Mechanické prvky**

Využívají mechanických prvků, respektive mechanických zábranných prostředků a systémů, které zamezují nebo znesnadňují proniknutí do chráněného objektu. Mezi mechanické prvky bezpečnosti patří:

  - mechanické zábranné systémy obvodové ochrany (např. bezpečnostní oplocení, brány, branky, závory, atd.),
  - mechanické zábranné systémy plášťové ochrany (např. okna a balkónové dveře, mříže, rolety, bezpečnostní a ochranné fólie, bezpečnostní skla, atd.),
  - mechanické zábranné systémy předmětové ochrany (např. trezory, komerční úschovné objekty, příruční pokladničky, manipulační schránky, atd.).

- **Elektronické (elektrické) prvky**

Využívají pro ochranu majetku a osob elektrických (elektronických) prvků, zejména:

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

- **Kombinované (mechatronické) prvky**

Využívají kombinaci mechanických zábranných systémů a elektronickou ochranu jako jeden funkční blok (např. elektronické blokování dveří, závor, atd.).

- **Speciální prvky**

Využívají specifické (speciální) prostředky k zabezpečení ochrany objektů (např. chemická ochrana předmětů, atd.).

Uvedené formy ochrany objektů jsou důležité zejména pro správné „zasystemizování“ jednotlivých prostředků či prvků objektové bezpečnosti, tudíž i přístupových systémů.

2 VŠEOBECNÝ POPIS PŘÍSTUPOVÝCH SYSTÉMŮ

2.1 Definice EKV a jeho úkoly z hlediska zabezpečení

Systémy kontroly vstupu zařazujeme do technické ochrany objektů, konkrétně pak do elektronických (elektrických) prvků bezpečnosti. EKV řídí přístup osob, respektive vozidel do chráněných prostorů nebo ke chráněným zařízením, na základě přidělených přístupových práv.

Přístupová práva

Podstatnou částí přístupových systémů jsou přidělovaná přístupová práva, která se nastavují pomocí stupňů oprávnění podle prostorových, časových a personálních dispozic ve vztahu ke zcela konkrétním osobám, jež jsou vybaveny identifikačním mediem. Systém tak umožňuje sledovat pohyb osob v definovaných zónách, vyhledávání osob, kontrolu následnosti průchodu a celé spektrum dalších aplikací. Od nejjednoduššího snímače bez evidence až po ucelený on-line systém s centrální evidencí, vyhodnocením, analýzou a napojením na další bezpečnostní systémy.

Jaké úkoly plní systémy EKV (ACCESS)?

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

1. Řídí pohyb osob v objektu v denním režimu, tj. v době, kdy je systém EZS zpravidla odblokován, nebo jeho část je odblokována a nestřeží.
2. Poskytují informace o pohybu osob v objektu, trvale tyto informace zaznamenávají a sledují a zaznamenávají místo pohybu a čas. Tím přispívají k ochraně objektu i režimovým opatřením.

Další úkoly EKV:

- omezení přístupu nepovolaných osob do určitých prostor objektu (sklady, kanceláře, nebezpečné provozovny, utajované provozovny, ochrana know-how aj.),
- omezení přístupu mimo určité časové úseky (zaměstnanci, návštěvníci, noční, denní, úklid, zásobování aj.),

- registrace délky pobytu, doby pobytu, místa a účelu, čítání doby pobytu na pracovišti,
- sledování a dokumentování pohybu, monitorování stavu v objektu, měření návštěvnosti, vytíženosti pracovníků, využívání zdrojů, materiálu, vytížení dalších kapacit, zvýšení bezpečnosti technologických objektů a provozů, dohled, využívání pracovní doby, zamezení zbytečného a nepovoleného pohybu po objektu, sledování odběru stravy, dodržování technologických přestávek a činnost provozu atd.

2.2 Identifikace jako součást přístupových systémů

Přístupové systémy jsou bezpečnostní systémy, které z velké části využívají ověření identity osob. V této souvislosti je významným parametrem identifikace, tj. ověření, že daná osoba je skutečně tou osobou, za kterou se vydává. Abychom byli konkrétní, tak každá osoba, která chce vstoupit do chráněné oblasti objektu, musí být nositelem tzv. „identifikátoru“. Proto musíme rozdělit identifikační přístupy podle toho, na jaké formě identifikace jsou založeny.

Rozdělení identifikačních přístupů je založeno na:

- tom, co člověk ví – nejčastějším případem této identifikace je znalost hesla (identifikace heslem),
- tom, co člověk má – nejčastějším případem této identifikace je použití identifikačních karet (identifikace předmětem),
- tom, jaké jsou charakteristické znaky člověka – nejčastějšími případy této identifikace je použití otisků prstů, dynamika podpisu, atd. Uvedený přístup je označován jako biometrická identifikace, resp. identifikace pomocí biometrických parametrů.

Ve shodě s uvedenou klasifikací rozlišujeme:

- **identifikaci heslem**

  Tato identifikace je založená na znalosti hesla, které je utajené a známé jen uživateli. Toto heslo musí uživatel zadat přístupovému systému, když žádá o povolení vstupu do prostředí s řízeným přístupem. Výhoda tohoto identifikačního přístupu spočívá v jednoduché technické a programové realizaci, v nízké ceně a možnosti snadno měnit

a přidělovat hesla telefonicky. K nevýhodám patří relativně jednoduchá možnost odchycení hesla, obtížné zapamatování a ruční zadávání hesla. Pro identifikaci heslem je nejtypičtější kódová klávesnice, sloužící pro zadávání PIN, jejíž budoucnost je pravděpodobně zajištěna díky požadavkům většiny bezpečnostních norem na dvouprvkovou identifikaci u všech aplikací vyžadujících vyšší stupeň zabezpečení. Pro zvýšení stupně zabezpečení proti odpozorování PIN je možno použít typ klávesnice s proměnlivým rozložením číslic na tlačítkách, popřípadě náhodně generovanými a potvrzovanými číslicemi na displeji klávesnice. Díky pokroku současné elektroniky jsou pak k dispozici i klávesnice pro extrémně náročná prostředí s nebezpečím poškození vandalizmem, které jsou vybaveny dotykovými (nezdvihovými) číslicemi, které nelze tradičními způsoby bez použití nástrojů poškodit.

- **identifikace předmětem**

  Identifikace je založená na vlastnictví identifikačního předmětu. Pro obecné označení identifikačního předmětu, který potvrzuje identitu svého vlastníka, se užívá termín *token*. Tokeny by měly plnit především požadavky jedinečnosti (unikátnosti) a těžké padělatelnosti (respektive nemožnosti tvorby duplikátů). Z bezpečnostního hlediska poskytuje identifikace předmětem vyšší úroveň zabezpečení, ale nevýhodou je skutečnost, že identifikační předmět může být odcizen nebo poškozen. Používání identifikačního předmětu je jednoduché a komfortní, cena je nízká, disponuje možností bezdotykové i kontaktní verze a může nést doplňkovou informaci jako PIN, fotografii, biometrický vzor aj. Z hlediska používaných identifikačních předmětů je možné klasifikovat tokeny na:

  - tokeny paměťové – jedná se o magnetické, elektronické, resp. optické karty, které přestavují analogii mechanickým klíčům, jejich paměť obsahuje jednoznačný identifikační řetězec.
  - tokeny udržující heslo – jedná se o tokeny, které využívají jednoduchého uživatelského hesla, které je zároveň i přístupový klíč.
  - tokeny s logikou – tokeny, které umožňují zpracovávat jednoduché podněty typu vydej následující klíč, vydej cyklickou sekvenci klíčů atd.
  - inteligentní tokeny – tokeny mohou obsahovat vlastní vstupní zařízení pro komunikaci s uživatelem, mohou obsahovat vlastní časovou základnu, šifrovat, generovat náhodné čísla atd.

- **biometrickou identifikaci**

  Tato identifikace je založená na biometrických charakteristikách osoby a využívá jedinečné fyziologické znaky člověka. Patří hlavně díky ceně mezi méně rozšířené způsoby, avšak díky vysoké spolehlivosti a nízkým nárokům kladeným na uživatele ji řadíme mezi technologie stále více používané v aplikacích s vysokými nároky na bezpečnost.

2.3 Struktura přístupových systémů

1. Identifikační média

Tvoří základní pilíř identifikací při kontrole vstupu. Identifikační medium je nosičem informace (např. kód), kterou zpracovává snímač. Podle použité technologie mají nosiče informace různé podoby. Lze je dělit například z hlediska styku média se snímačem na kontaktní, bezkontaktní, magnetické, čipové, rádiové, infračervené, čárové kódy. Nejčastějším tvarem nosičů informací je karta, přívěšek, etiketa, štítek nebo visačka. Nosičem informace jsou i obyčejné klíče, nebo dokonce samo lidské tělo – biometrie.

2. Snímače

Tvoří jakýsi protipól identifikačních médií. Mají za úkol je bezpečně přečíst a dekódovat. Snímače vždy odpovídají typu nosiče informace – čtečky, klávesnice, terminály, průchozí konzoly. Výběr snímače je podmíněn použitou technologií, prostředím, požadovanou čtecí vzdáleností a formou zpracování sejmutých dat. Je třeba si uvědomit, že právě snímač je předsunutým hlídacím a kontrolním stanovištěm systému, a jako takový musí splňovat dva do značné míry protichůdné požadavky. Na jedné straně otevřenost pro potřeby uživatelů, což je jednoduchá manipulace a jednoznačná signalizace stavu. A na straně druhé odolnost proti vnějším vlivům, čímž rozumíme stupeň krytí či sabotážní bezpečnost. Většina snímačů se používá ve formě stacionární, to znamená, že u přístupů jsou instalovány na zdi u vchodu do střeženého objektu.

3. Zpracování dat

Je nedílnou součástí přístupových systémů, neboť zde dochází k rozhodovací fázi. Snímač identifikačního média čte informaci o každé osobě, která prostřednictvím svého „identifikátoru“ požaduje vstup do hlídaného prostoru. Informace, kterou snímač snímá je odesílána ke zpracování do řídicí jednotky.

Řídicí jednotka je vybavena pamětí, v níž je uložena kopie informace o identifikaci uživatele a jeho přístupových právech. Řídící jednotka přebírá elektronické signály generované snímači identifikace a na základě informací uložených v paměti rozhoduje o uvolnění, nebo naopak zablokování hlídaného vstupu. Moderní řídicí jednotky jsou řízeny mikroprocesorem a díky paměťové výstavbě disponují schopností zcela samostatně rozhodovat o vstupu nebo vyhodnocovat příslušné reálné podněty (stav dveří, poplachové vstupy). Tato schopnost plně autonomního provozu je pro vstupní systém velice důležitá. Ovládání vchodu není totiž závislé na stavu centrální jednotky nebo komunikačních linek mezi centrální a řídící jednotkou. To znamená, že v případě poruchy komunikace mezi řídící a centrální jednotkou nedojde k celkovému výpadku systému, ale pouze k dočasnému přerušení toku dat mezi těmito jednotkami. Informace o průchodech se uloží do řídící jednotky a budou do centrální jednotky přeneseny dodatečně ihned po obnovení komunikace.

Centrální jednotka monitoruje a řídí celý přístupový systém. Odtud se provádí jeho programování a obsluha. Jestliže systém obsahuje více řídících jednotek, tak ty jsou propojeny do sítě a napojeny na centrální jednotku. Centrální jednotka je počítač (PC) se specializovaným softwarem, který zajišťuje centrální správu personálních (základní personální údaje, údaje o kontrole vstupu apod.), řídících (časoprostorové zóny, parametry nastavení jednotlivých řídících jednotek) a rozličných systémových dat a jejich přenos mezi PC a řídícími jednotkami. Hlavním úkolem centrální jednotky je sběr událostí z řídících jednotek, jejich vyhodnocení a adekvátní reakce na ně v reálném čase. Sběr dat může být prováděn buď permanentně, s možností okamžité reakce systému či jeho obsluhy (on-line) nebo naopak dávkovaně (off-line).

Vyhodnocení získaných údajů bývá velice variabilní s možností filtrování (tzn. možnost odlišit určitý vstup, osobu či událost), třídění a výpisů (tisku). Řídící software by měl navíc splňovat i všechny relevantní požadavky zákazníků jako „uživatelskou přítulnost“, pohodlné ovládání a lokalizaci do národního prostředí.

Renomovaní výrobci vstupních systémů však díky široké nabídce vlastních převodníků nabízejí dále možnost volně přizpůsobit typ komunikačních linek přenosovým podmínkám, popřípadě již existujícím datovým strukturám jako jsou proudová smyčka, veřejné či soukromé telefonní linky, optická vlákna, DATEX-P, LAN apod.

4. Ovládaná zařízení

Jsou poslední důležitou součástí vstupních systémů. Ovládaná zařízení jsou koncové prvky, které jsou aktivovány po procesu zpracování dat. Pod těmito zařízeními si můžeme představit různé elektrické zámky odblokování vstupů, uvolnění turniketů při vstupu do objektů, otevření závory při vjezdu do areálu atd. Ačkoliv jsou tato zařízení v nabídkách vstupních systémů často opomíjena, jedná se prakticky o nejexponovanější a nejvíce namáhanou součást celého systému.

Důležitým faktorem při volbě adekvátního ovládacího zařízení musí být proto nejen jeho funkční vlastnosti a spolehlivost, ale i možnost výběru dle umístění a způsobu montáže.

2.4 Integrace EKV s jinými systémy

Systémy kontroly vstupu (ACCESS) mohou být používány buď samostatně, nebo v kombinaci s dalším poplachovým systémem, kdy tvoří společně jednu bezpečnostní aplikaci. V současné době se většinou používají tyto kombinace systémů kontroly vstupu:

a) kombinace přístupového systému a docházkového systému

Tato kombinace umožňuje vstup do objektu a zároveň zaznamenává datové údaje pro potřeby zaměstnavatele, které slouží k evidenci docházky. Docházkový systém zaznamenává příchod a odchod do zaměstnání, odchod na svačinu, oběd, k lékaři, služební odchody, přerušení práce, ranní, odpolední, noční práce, práce o svátcích a dnech pracovního volna a podobně. Používání docházkového systému přispívá k omezení chybovosti při zpracování dat o docházce, efektivnějšímu využívání pracovní doby a zvýšení pracovní morálky.

b) kombinace přístupového systému a systému pro výdej stravy či pracovních pomůcek

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

c) kombinace systému kontroly vstupu se zařízením EZS

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

d) kombinace systému kontroly vstupu se zařízením CCTV

Používá se tam, kde je nutno kontrolovat nejen pohyb po objektu, ale i sledovat celkovou činnost osoby nebo osob v objektu. Hlavní úkolem je mít permanentní kontrolu veškerého pohybu v objektu s možností včasné reakce na nežádoucí situaci, která může vzniknout. Využívá se zejména ve věženích, vojenských skladech, letištích, jaderných elektrárnách apod.

e) kombinace systému kontroly vstupu s zařízením EPS

Tato kombinace je jednou z nejčastějších a nejjednodušších aplikací. Používá se k zajištění automatického otevření únikových východů v případě detekce požáru systémem EPS. Z důvodů rychlosti reakce spolehlivosti a univerzálnosti je integrace prováděna zapojením napájení elektrických zámků přes kontakt signalizačního relé systému EPS.

f) kombinace systému kontroly vstupu do informačních technologií

Rostoucí využití informačních technologií vyžaduje přístup k nim. Ne všechny informace je však možno sdělovat každému a kdykoliv. Tím vznikl požadavek na integraci přístupového systému s informačními technologiemi. Vzhledem k omezeným možnostem zapamatovat si kódy a hesla se požaduje, aby byl přístup umožněn po schválení vstupu a vydání přístupového média (přihlašování k PC, do sítí, elektronický podpis atd.). Vazební-

mi prvky mezi systémem EKV pro fyzickou kontrolu přístupu a prvky řízení přístupu k informacím jsou:

- identifikační karty

  Bývají většinou ve formě kombinovaných karet, to znamená bezkontaktní karta obsahující bezkontaktní identifikační část, která současně obsahuje výkonný bezpečnostní procesor s normalizovaným kontaktním polem dle ISO 7816. Informace uživatele jména a hesla je v tomto případě převážně uschována na identifikační kartě.

- biometrické prvky

  Jsou založeny na otiscích prstu, charakteristiky duhovky oka zpracovávané pomocí programového modulu umožňujícího začlenění biometrické čtečky do existujících softwarových aplikací. U tohoto způsobu je zabezpečená informace v informačním systému chráněna na prostředky operačního systému a šifrováním. K jejímu zpřístupnění dochází po ověření shody mezi uloženým vzorem a nově sejmutým vzorkem biometrického údaje.

Cílem integrace EKV s informačními technologiemi je snížení nákladů na správu hesel (především zde hrají roli zapomenutá a špatně zadaná hesla) do různých systémů a podpora udržení bezpečnosti správy hesel zajištěním vysokého komfortu uživatelů při přístupu k prostředkům informačních technologií, čímž bráníme obcházení bezpečnostních postupů různými méně zodpovědnými uživateli.

3 VYUŽITÍ IDENTIFIKAČNÍCH SYSTÉMŮ V EKV

Identifikační systémy jsou důležitou součástí přístupových systémů z hlediska přístupu do zabezpečeného prostoru. Pokud chce osoba oprávněně vstoupit do chráněného prostoru či objektu, musí použít identifikační médium, které přísluší konkrétnímu vstupu a je nositelem určité informace potřebné k průchodu. Identifikační systémy rozlišují celou řadu prostředků identifikace osob, mezi něž patří optický identifikační systém, magnetický identifikační systém, kontaktní a bezkontaktní identifikační systém.

Optický identifikační systém

Je jedním z nejdéle používaných identifikačních systémů. Jedná se většinou o kartu sestávající se z čar a mezer různé tloušťky na bílém podkladu. Čárový kód může mít samozřejmě více podob dle použití některého ze standardů. Ke čtení dochází odrazem vysílaných paprsků. Čárový kód neobsahuje žádná osobní data nebo údaje o jménu a rodném čísle. Data jsou pouze referenční čísla, podle kterých počítač vyhledá odpovídající záznam v databázi.

Čárový kód je řada vertikálních čar různé tloušťky s mezerami. Pruhy a mezery se dohromady označují jako prvky. První a poslední pruhy slouží k synchronizaci. Čtečku čárových kódů představuje optoelektrický snímač. Když se čtečkou přejede nad čárovým kódem, je vysílaný paprsek černými pruhy absorbován, zatímco od světlých mezer se odrazí. Fotosenzor čtečky přijímá odražené světlo a převádí je na elektrický signál. Čtečka přejíždí přes čárový kód a skener vytvoří slabý elektrický signál pro mezery a silnější signál pro pruhy. Délka elektrického signálu určuje, jak široké nebo úzké prvky jsou. Signál se dekodérem čtečky rozepíše do jednotlivých znaků čárového kódu. Dekódovaná data se ve standardním formátu přenesou do počítače.

Velkou výhodou těchto médií je bezkonkurenčně nízká cena a jednoduchost. Pro snadné zkopírování se již nepoužívají v bezpečnostních systémech, ale např. v knihovnách, obchodech, supermarketech atd.

Obr. 1. Karta s čárovým kódem.

Obr. 2. Snímač karet Intermec MagScan 1354A.

Magnetický identifikační systém

Používá se prakticky pouze ve spojení s identifikačními kartami velikosti kreditních karet, použití jiného provedení je prakticky nemožné. Základem je klasický magnetický proužek, na kterém je informace zapsána pomocí nahrávací hlavy. Ke čtení dochází protažením karty štěrbinou se čtecí hlavou. Zápis informace na magnetický proužek má různé kódování podle použitého systému. Data na magnetickém proužku jsou dynamická, což znamená, že uložený záznam lze později kdykoliv přepsat nebo aktualizovat.

Systém magnetických karet neumožňuje bezkontaktní identifikaci, protože musí dojít k fyzickému protažení karty štěrbinou. Cena karty je velmi nízká, což vedlo k masivnímu rozšíření. I cena čtečky se pohybuje v průměrné výši. Toto jsou největší klady a mezi negativa patří malá bezpečnost a velká náchylnost k opotřebování. Ta je zapříčiněna protahováním karty štěrbinou, kde dochází k mechanickému opotřebení magnetického proužku. Dalším faktorem otěru je už jenom pouhé uložení karty do obalu nebo peněženky.

K poškození dat uložených na magnetické stopě může dojít, i pokud kartu vystavíme vědomě či nevědomě účinku silného magnetického pole.

Bezpečnost magnetických karet není velká, neboť lze celkem bez problémů kartu přečíst a vyrobit duplikát. I přes toto nebezpečí se používají, ale jsou doplněny ještě o druhou identifikaci, a to zadání většinou čtyřmístného čísla – PIN. Magnetické karty jsou rozšířené v oblasti bankovnictví, sledování docházky či v přístupových systémech. V přístupových a docházkových systémech se v současnosti již přechází na modernější systémy, jako jsou bezkontaktní karty či biometrie.

Obr. 3. Zámek se čtečkou magnetických karet Typ M700.

Kontaktní identifikační systém

Kontaktní systémy patří mezi identifikační systémy celkem rozšířené. Dochází u nich k předání informací na základě kontaktu média s čtecím zařízením a následné komunikaci. Média mají podobu kovového pouzdra nebo kreditní karty s kontaktní plochou. Zabezpečení kontaktních systémů je podstatně vyšší než u výše popsaných systémů. Nevýhodou je omezená životnost mechanických částí čtečky, která dost závisí na počtu uživatelů a jejich přístupu k zařízení.

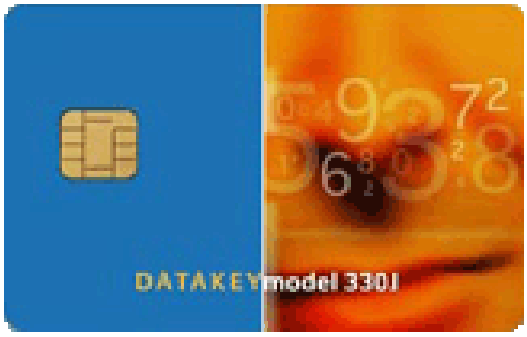
Mezi identifikační média, kterých využívají kontaktní identifikační systémy, patří:

- kontaktní čipová karta,
- kontaktní čip Dallas.

Kontaktní čipová karta

Společným faktorem těchto karet je relativně vysoká bezpečnost specializované čipové technologie a použití standardní kontaktní plošky k propojení karty se čtecím zařízením, čímž je čip zapojen do obvodu a dochází ke komunikaci mezi čtečkou a čipem. Může probíhat i oboustranná komunikace. Přenášené informace jsou pak dále zpracovávány a slouží k identifikaci uživatele.

Kontaktní ploška obsahuje osm kontaktů, jejichž funkce a umístění na čipové kartě je standardizováno normou ISO/EC 7816–2. Jednotlivé kontakty slouží pro napájení čipu, sériovou komunikaci, přivedení externího taktovacího signálu a programovacího napětí. Důležité jsou dva kontakty rezervované pro budoucí využití, které se již v současnosti používají u některých karet pro alternativní USB rozhraní.



Obr. 4. Kontaktní čipová karta.

Obr. 5. Čtečka kontaktních čipových karet V4DF.

Kontaktní čip Dallas

Osobní identifikační čip Dallas je médium nahrazující klasický klíč. Přiložením čipu ke snímací hlavě dojde k přečtení kódu a tím k jednoznačné identifikaci osoby, které byl tento čip přidělen. Jeden čip může být použit pro více činností, například docházka, otevírání dveří, objednávka stravy. Identifikační čipy Dallas jsou produktem firmy Dallas semiconductor. Obsahují jedinečný 64bitový kód a výrobce garantuje, že nikdy nevyrobí dva identické čipy, což zaručuje nezaměnitelnost identifikace.

V poslední době jsou čipy Dallas stále více oblíbené hlavně díky své spolehlivosti a jednoduché manipulaci. Každý čip je zasazen v plastovém pouzdru, které je uzpůsobeno k připnutí, čímž se omezuje ztrátovost na minimum na rozdíl od karet, které se nosí různě po kapsách. K přečtení čipu stačí jen velmi krátký dotek (řádově 150 ms) a není nutno nijak přesně volit způsob přiložení. U čipů Dallas během dlouhodobého používaní dochází k minimálnímu opotřebení. K nevýhodám patří malá mechanická odolnost spodní plošky čipu, kterou mohou poničit např. klíče na společném svazku.

Každý jednotlivý čip je naprosto nezávislý na svém majiteli. Pokud zaměstnanec ukončí pracovní poměr, může být jeho čip přidělen jeho nástupci a není tedy nutno dokupovat nové čipy.

Obr. 6. Kontaktní čipy Dallas.

Obr. 7. Externí snímač EDK 2.

Bezkontaktní identifikační systém

Stává se v poslední době nejrozšířenějším systémem v oblasti personálních i průmyslových identifikací. Bezkontaktní identifikační systém spočívá v radiofrekvenční identifikaci (RFID), která je založena na principu radiového přenosu dat mezi snímačem (čtečkou) a objektem.

Každý identifikovaný objekt musí být vybaven datovým médiem, které se u bezkontaktních identifikačních systémů nazývá většinou souhrně jako transpondér, což je elektronický obvod složený z přijímací/vysílací antény, nabíjecího kondenzátoru a paměti. K činnosti nepotřebuje napájení z vlastní baterie, a proto ho označujeme jako pasivní. V zásadě celý systém RFID pracuje jako dvouanténní, kdy jedna anténa je v transpondéru a druhá ve snímači.

Transpondéry existují v různých provedeních lišících se jak tvarem, tak i funkcí. Mohou mít podobu jako plastové karty, plastové disky, přívěsky na klíče, skleněné tyčinky, válcové provedení a mnohé další. Konkrétní výběr transpondéru závisí na aplikaci. Mezi pozitivní vlastnosti patří skutečnost, že transpondéry u bezkontaktního systému jsou neopotřebovatelné a prakticky nezničitelné. Jejich kopírovatelnost je téměř nemožná.

Princip činnosti bezkontaktního systému spočívá v tom, že snímač periodicky vysílá výkonové impulsy prostřednictvím antény do svého okolí. Jakmile se v dosahu antény objeví transpondér, tak přijme impuls přes svoji anténu, která je naladěna na stejnou frekvenci. Tato přijatá energie je usměrněna a vzniklým napětím je nabit interní kondenzátor transpondéru. Po ukončení vysílaného pulsu transpondér okamžitě vyšle svá data zpět ke snímači. K napájení transpondéru během jeho vysílání slouží právě toto napětí nastřádané na vnitřním kondenzátoru. Délka přenášených dat je různá, např. 128 bitů a více, včetně zabezpečovacího kódu a přenos trvá zhruba desítky milisekund. Přenášená data jsou zachycena anténou snímače, dekódována a mohou být předána ihned počítači ke zpracování, nebo mohou být uložena v paměti řídící jednotky příslušného snímače a později nahrána do počítače. Po odeslání všech dat do snímače je nabíjecí kondenzátor transpondéru vybit a očekává se další nabití a čtení. Perioda mezi dvěma cykly je řádu desítek milisekund a je závislá na nastavení systému.

Umístění snímače transpondéru může být libovolné, třeba za stěnou nebo i v ní. Může být umístěn dokonce i zcela mimo identifikační místo, kde bude namontována pouze anténa. Takto lze snímač bezpečně ochránit před vandaly. Při průchodu osob pak při vhodně umístěné anténě a tranpsodéru není třeba vůbec kartu vytahovat, a přesto k identifikaci dojde (tzv. FREEHAND systém). Velkou výhodou je možnost automatické identifikace – transpondéry mohou být na snímaném objektu umístěny skoro kdekoliv, snímač je dovede identifikovat (podle provedení) i na několik metrů.

Výměna a přenos dat se provádí u různých systémů RFID na různé frekvenci. Každá frekvence má jiné přednosti a je vhodná pro jiné aplikace. Komerčně nejčastěji využívaná frekvenční pásma jsou LF, HF, UHF a MW.

Základní frekvence pro RFID:

- nízké frekvence 125 – 134 kHz (LF)
- vysoké frekvence 13,56 MHz (HF)
- ultravysoké frekvence 860 – 930 MHz (UHF)
- mikrovlnné frekvence 2,45 a 5,8 GHz (MW)

V personálních identifikacích kontroly vstupu je používána radiofrekvenční identifikace (RFID) osob. Pro radiofrekvenční identifikaci osob jsou nejběžnější frekvence nízkofrekvenční pracující na 125 – 134 kHz nebo vysokofrekvenční s frekvencí 13,56 MHz. V současné době je rozšířenější technologie 125 kHz, avšak díky mnoha přednostem se začíná stále více prosazovat oblast 13,56 MHz. Oproti 125 kHz sice disponuje obecně kratším dosahem, ale hovoří pro ni rychlejší přenos dat, schopnost čtení i zápisu dat na kartu, šifrování přenášených dat, současné čtení více karet v dosahu a možnost využití jedné karty pro více různých aplikací.

Obr. 8. Bezkontaktní karta Mocard.

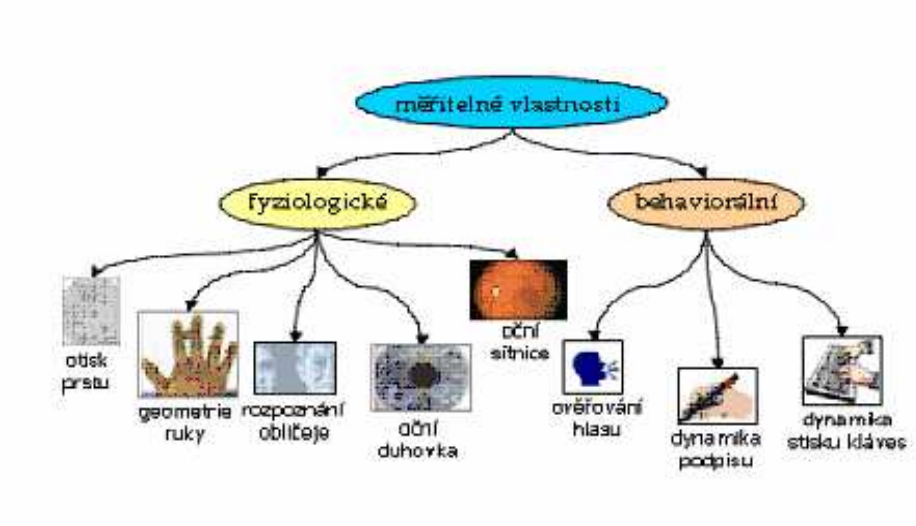
Obr. 9. Bezkontaktní čtečky Indala Mifare.

4 BIOMETRICKÉ IDENTIFIKAČNÍ SYSTÉMY

Biometrické identifikační systémy jsou speciálním odvětvím elektronické ochrany v průmyslu komerční bezpečnosti pracující na bázi možnosti měření určitých biologických veličin u člověka. Zpřesňuje se zde možnost identifikace na bázi biometrických vlastností.

Co jsou to biometriky?

Biometrikami se nazývají jedinečné měřitelné fyziologické a behaviorální (tj. týkající se chování) charakteristiky člověka, které lze použít k identifikaci nebo ověření identity osob. Příkladem fyziologických charakteristik jsou otisk prstu, geometrie tvaru ruky, oční duhovka, oční sítnice, DNA apod. Naproti tomu vlastnosti chování, kterých mohou biometrické systémy využívat, jsou například dynamika podpisu, dynamika stisku kláves nebo ověření hlasem.



Obr. 10. Základní rozdělení biometrik.

Kde lze biometrik využít?

Spektrum použití biometrických technologií je značně široké. Uplatnění mohou nalézt zejména jako náhrada za klasické klíče a sloužit tak k otevření dveří domů, bytů či kanceláří. Mohou být používány k autorizaci přístupu do počítačových sítí, pracovních stanic nebo pro zpřístupnění klientského učtu v bankomatech. Biometriky lze využít i

v souvislosti s elektronickým podpisem, kde mohou sloužit k omezení přístupu k soukromému klíči uživatele, avšak samotný soukromý klíč z nich vytvořit nelze!

Ve státní správě nacházejí biometriky uplatnění v soudnictví a soudním vyšetřování při identifikaci pachatelů, v imigračních zařízeních, při zabezpečení věznic nebo na letištních terminálech. Evropská unie připravuje návrh nových cestovních pasů, které budou obsahovat počítačový čip, v němž bude v zašifrované digitální podobě uložen otisk prstu a fotografie obličeje jeho držitele. Proti přepsání či smazání budou tato citlivá data zajištěna elektronickým podpisem.

Proč zvolit biometriky?

Největší předností biometrik oproti jiným metodám je jejich jednoznačnost. Charakteristické rysy každého člověka jsou unikátní. Žádní dva lidé nemají například shodné otisky prstů a to ani v případě, že se jedná o jednovaječná dvojčata. Magnetické nebo čipové karty, identifikační karty i klasické domovní klíče mohou být ztraceny, odcizeny či okopírovány. Hesla nebo kódy PIN mohou být zapomenuty, odpozorovány nebo sdíleny více uživateli. Nic z výše uvedeného však u biometrik nastat nemůže. Navíc u všech biometrických technik je nutné, aby procesu identifikace nebo ověření identity byla daná osoba fyzicky přítomna. Z toho vyplývá, že biometriky nelze nikomu ani půjčit ani prozradit. V případě, že je vyžadována vysoká úroveň zabezpečení systému, lze biometriky s výhodou použít v kombinaci s jinými metodami identifikace, jako je heslo/PIN nebo čipová karta.

Omezení biometrik

Vždy je potřeba mít na mysli, že biometriky nejsou tajné. Prakticky kdokoliv může poměrně snadno získat váš otisk prstu (např. z obyčejné sklenice) nebo snímek duhovky. Proto nelze biometriky použít k vytvoření soukromého klíče pro digitální podpis – kdokoliv by mohl jednoduše vytvořit váš soukromý klíč.

Někteří lidé postrádají nebo mají poškozené určité tělesné orgány a mohou být vyloučeni z použití některých biometrických systémů. U biometrických technologií, jako je dynamika podpisu nebo tvar obličeje, může činit problémy proměnlivost vzorku v delším časovém období anebo v důsledku nemoci (hlas). Snímání charakteristik také může u uživatelů vyvolávat nepříjemné pocity a odmítání (oční sítnice, DNA).

Žádný biometrický systém není stoprocentně bezchybný a vždy existuje určitá pravděpodobnost výskytu chybného odmítnutí autorizovaného uživatele a chybného přijetí neoprávněné osoby. Každý kvalitní biometrický systém by však měl disponovat funkcí testování „živosti“ snímané charakteristiky, aby tak zabránil akceptování podvrhů (umělých prstů či vytisknutých fotografií oka, tváře).

Proces použití biometrik

Přestože se jednotlivé biometrické techniky vzájemně liší, postup jejich používání je velmi podobný a lze ho shrnout do čtyř základních kroků:

- získání biometrických dat,
- extrakce charakteristických znaků,
- porovnání charakteristiky s referenční šablonou,
- rozhodnutí o shodě či neshodě.

Registrace

Předtím, než může kdokoliv používat určitý biometrický systém, musí být do tohoto systému nejprve zaveden. Registrace spočívá ve vytvoření referenční šablony uživatele, vůči které se budou při dalších přístupech k systému porovnávat aktuálně získané vzorky. Právě z důvodu dalšího srovnávání je důležité, aby kvalita referenční šablony byla co možná nejvyšší. Šablona je ve své podstatě matematický kód, který vznikne extrahováním jedinečných znaků ze sejmutých biometrických dat uživatele a daného člověka jednoznačně identifikuje. Pro získání co nejlepší šablony se zpravidla sejme několik biometrických vzorků uživatele, ověří se jejich kvalita a na šablonu se poté převede pouze ten nejlepší z nich. V případě nedostatečné kvality vzorků se proces snímání opakuje, dokud se nezíská alespoň jeden uspokojivý. Referenční šablona může být uložena buď na čipové kartě, v samotném biometrickém zařízení, na pracovní stanici nebo na serveru v centrální databázi. Protože se však jedná o vysoce citlivá data, měla by být šablona vždy uložena v zašifrované podobě.

Verifikace versus identifikace

Jakmile je proces zavedení uživatele do biometrického systému dokončen (tj. byla pro něho vytvořena šablona), může se takový systém používat dvěma různými způsoby nazývanými verifikace a identifikace.

Při verifikaci uživatel nejprve zadá svoji totožnost (např. pomocí identifikační karty), poté se sejmou jeho biometrická data, ze kterých se extrahují charakteristické rysy a ty se následně porovnají s referenční šablonou uloženou v systému pro daného uživatele.

Při identifikaci uživatel nepředkládá svoji totožnost, ale rovnou se sejmou a zpracují jeho biometrické charakteristiky. Nyní je na systému, aby prohledal svoji databázi, každou uloženou šablonu porovnal s aktuálně získaným vzorkem a pokusil se nalézt shodující se záznamy. Pokud byla shoda nalezena, je identita daného člověka známa a je systémem přijat. Je zřejmé, že identifikace je časově i výpočetně mnohem náročnější proces než verifikace.

Určení shody a prahová hodnota

Při určování shody mezi referenční šablonou a aktuálně získaným vzorkem nelze v případě biometrik postupovat stejně jako u jiných metod identifikace. PIN nebo heslo jsou vždy zadány správně anebo ne, avšak biometrická data nejsou nikdy stoprocentně stejná. Například při opakovaném snímání otisku jednoho prstu je prst pokaždé přiložen na senzor nepatrně jinak (pootočen, posunut, s jiným přítlakem atd.). Z tohoto důvodu je nutné povolit určitou variabilitu mezi referenční šablonou a sejmutými biometrickými daty. Stanovuje se prahová hodnota vyjadřující hranici, kdy je ještě možné obě charakteristiky považovat za shodné a kdy již nikoliv. V případě, že je prahová hodnota nastavena příliš nízko, vyvstává nebezpečí akceptování případného útočníka jako autorizovaného uživatele. Naopak příliš vysoká prahová hodnota může vést k nepřijetí oprávněného uživatele z důvodu nedostatečně průkazných sejmutých biometrických dat.

Základní biometrické identifikační přístupy

Identifikace podle otisku prstu

Automatický systém identifikace otisku prstu je v současné době nejrozšířenější a nejpoužívanější metodou biometrických identifikačních přístupů. Systém využívá elektro-

nickou identifikaci papilárních linií na vnitřních stranách článků prstů, jejichž totožnost u dvou lidí je vyloučena. V současné době tuto starou kriminalistickou metodu rozpracovaly přední firmy do fungujících standardních hardwarových systémů s využitím v praxi.

Systém identifikace otisku prstu dnes začíná nahrazovat klíčové hospodářství, identifikační karty, kódy EZS. Pouhým přiložením prstu ke snímači je provedena identifikace a elektronické srovnání s referenčním otiskem. Podle toho, jestli otisk souhlasí s referenčním otiskem, je umožněn nebo neumožněn vstup.

Obr. 11. Snímač otisku prstu V-Station.

Obr. 12. Snímač otisku prstu FingerScan V20 UA.

Identifikace podle geometrie ruky

Tato identifikace je založena na skutečnosti, že každý člověk má specifický tvar (morfologii) ruky, který se od určitého věku nemění. Identifikace podle tvaru ruky prakticky využívá staré kriminalistické metody (bertillonáže) lidských údů, které se elektronicky

vyhodnocují. Přístroj nejprve sejme identifikační veličiny geometrie ruky a zaznamenává je do paměti. Následně umožní vstup, výstup eventuálně jinou činnost.

Obr. 13. Snímač geometrie ruky HandKey II.

Identifikace podle obličeje

Patří mezi nejpřirozenější metody identifikace osob. Pro rozpoznávání se používají víceúrovňové, tzv. šedé obrazy. Jako znaky pro rozpoznávání se používají pozice očí, nosu, úst, a vzájemné vzdálenosti mezi nimi. Problémy takové identifikace mohou nastat v případě dvojčat, velkou výhodou je to, že rozpoznávání nevyžaduje žádný kontakt s identifikovanou osobou.

Obr. 14. Snímač obličeje A4 Vision.

Identifikace podle geometrie oka

Je založena na biometrické identifikaci sítnice a duhovky oka využívající biologickou jedinečnost. Tento identifikační systém snímá speciální kamerou nasvícené oko člověka a pracuje prakticky na bázi matematické statistiky zkoumání proměnlivosti živých organismů. Tento způsob je naprosto nezaměnitelný a je využíván v přístupových systémech na nejvyšší úrovni řízení a velení ve světě a v přístupech na vysoce utajovaná a ochraňovaná pracoviště.

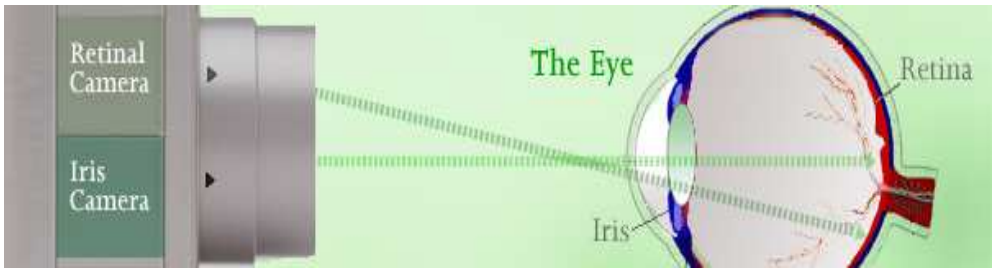
- **Identifikace podle oční duhovky**

  Každá duhovka má jedinečnou strukturu, která je dána kombinací specifických anatomických charakteristik. U každého člověka se duhovky liší, také se liší u každého jedince pravá a levá duhovka. Dvojčata mají také odlišné duhovky. Rozpoznávání podle oční duhovky je rychlejší, přesnější a bezpečnější než jakákoliv jiná metoda. Vzorec duhovky je mnohem individuálnější, než otisk prstu, takže je to pro identifikaci perfektní kritériu. Používání je pohodné, rychlé a je prováděné bezkontaktními metodami, tudíž není vyžadován žádný fyzický kontakt mezi duhovkou a kamerou. Uživatel se jen dívá do kamerové čočky ze vzdálenosti 10 až 15 cm než je jeho duhovka neskenována a následně porovnána s databází.

Obr. 15. Snímač oční duhovky Panasonic BM-ET300.

- **Identifikace podle oční sítnice**

  Oční sítnice není viditelným lidským zrakovým orgánem, proto pro její transformaci do viditelné polohy se užívají koherentní infračervené světelné zdroje. Infračervená energie je cévami sítnice rychleji absorbována, než v okolních tkanivech, což způsobuje, že cévy v oční sítnici jsou na snímaném obraze tmavší. Získaný obraz překrvení sítnice oka je pak analyzován. Metodika identifikace podle sítnice oka je z hlediska časového vývoje starší, než identifikace podle duhovky. Z hlediska podmínek přijatelnosti může být tato identifikační metoda v některých případech dosti problémová.



Obr. 16. Princip snímání oční sítnice a duhovky.

Identifikace podle hlasu

Je používána zejména pro různé vstupní systémy. Systémy jsou schopné identifikace hlasu jeho elektronickou analýzou a to i přes telefon. Pokud je příslušný hlas v databázi zařízení, po promluvení do mikrofonu je analyzován a umožněn nebo neumožněn přístup.

Obr. 17. Hlasové snímače Nuance Verifier 3.0.

Identifikace podle dynamiky podpisu

Každý člověk má specifickou dynamiku při psaní. Mírami dynamických charakteristik při identifikaci podle dynamiky podpisu jsou napětí, tlak pera na podložku při psaní, směr písma jednotlivých znaků podpisu, rychlost psaní jednotlivých tvarů, počet, délka a trvání tahů při psaní. Pro zjištění dynamiky jsou potřebná speciální pera a pomocná zařízení, jejichž úkolem je registrace a zkouška identifikačních podpisů, které jsou vyhodnocovány elektronickou cestou.

Obr. 18. Snímač dynamiky podpisu Cyber-SIGN.

Identifikace podle žil na rukách

Tato identifikace využívá skutečnost, že tvar žilového řečiště je charakteristický pro každou osobu. Princip identifikace podle žil na rukách je podobný identifikaci podle sítnice oka. Snímání se realizuje kamerou v infračervené oblasti elektromagnetického spektra.

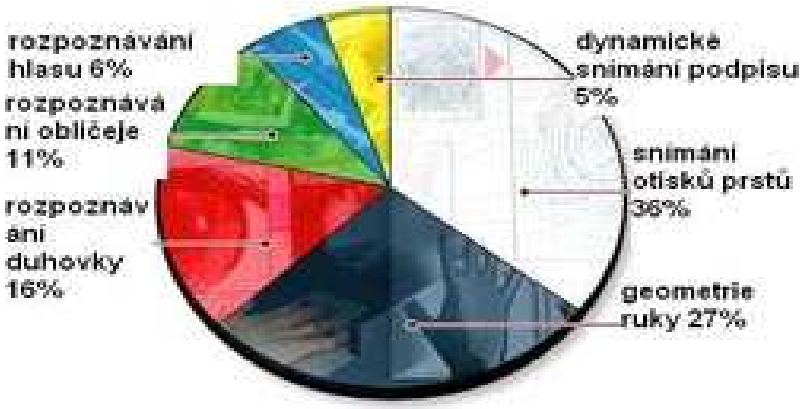
Obr. 19. Snímač žilového řečiště na rukou VP-II.

Identifikace podle specifického pachu

Tato identifikace spočívá na zcela nezaměnitelném lidském pachu, kterého využívají k identifikaci např. psi. Lidský pach je využit pro identifikaci biologicko-chemickou cestou a k umožnění nebo znemožnění přístupu nebo další činnosti. Osoba vejde do jakéhosi rámce, kde je na několik sekund uzamčena. Analýza je okamžitá. Po nasání pachu detektorem přístroj odfiltruje i různé deodoranty. Používá se pro speciální účely zpravidla tam, kde je identifikovaný ustrojen do speciálních obleků a nelze provést jinou podrobnější identifikaci.

Identifikace podle dlaní

Patří do skupiny daktyloskopických identifikací, využívá podobných přístupů a technologií, jako identifikace podle otisku prstů. Vyžaduje snímání podstatně větších rozměrů, než při snímání otisků prstů, což představuje limitní faktor z techniko-realizačního pohledu a z hlediska rychlosti zpracování snímaných dat.



Obr. 20. Podíl jednotlivých technologií biometrických systémů na trhu.

5 MECHANICKÉ ZÁBRANNÉ PROSTŘEDKY VE SPOJENÍ S ELEKTRONIKOU V EKV

Dveře, vložka zámku a zámek sám patří k citlivým místům stavebního otvoru objektu. Především z tohoto důvodu u nich dochází k zvyšování bezpečnostní úrovně. Je patrný trend integrace elektronických funkcí do klasické mechaniky (zadlabací zámky, cylindrické vložky) a zvyšování bezpečnostních možností u cylindrických vložek.

Razantní vývoj elektronických identifikačních systémů v oblasti hardware i software a jejich rozšiřování nabízí stále větší možnosti v zabezpečení jednotlivých dveří, a tím i celého objektu. Jedná se o kombinaci mechaniky vysoké úrovně a inteligentní elektroniky.

Propojením mechaniky s elektronikou umožňuje splnění všech požadavků, které od komplexního zabezpečení uživatel očekává. Je to zejména odolnost proti mechanickému překonání, kontrola průchodů, časové údaje, organizační požadavky, kontrola uzamčení, automatika uzavírání a propojení s EZS. Všechny tyto uvedené požadavky lze aplikovat v zadlabacím zámku, v cylindrické vložce, nebo propojením obou podsystémů.

Zadlabací zámek

Nejjednodušší propojení elektroniky se zadlabacím zámkem je případ blokovacích zámků. Termín blokovací zámek se používá ve spojení s ovládáním systémů EZS. Tyto zámky splňují funkci únikových dveří, kde z vnitřní strany lze dveře kdykoliv otevřít zmáčknutím kliky (funkce „antipanik“). Po zabouchnutí dveří se automaticky vysune závora zámku ovládaná elektronicky (motorový pohon nebo elektromagnet). Z venkovní strany lze zámek otevřít klíčem nebo pomocí impulsu libovolného identifikačního prvku jako je klávesnice, čtečka magnetických karet, bezdotyková identifikace apod. Možnosti doplnění těchto zámků dalšími prvky a programovým vybavením umožňují následné rozšíření oblastí použití jako je neustálá kontrola stavu uzavření dveří, dveřní kontakt, vyhodnocování průchodu jednotlivých osob a mnoho dalších možností.

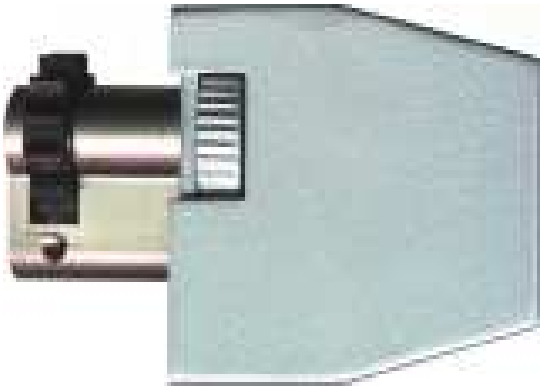
Obr. 21. Standardní blokovací zámek SBS, VdS A/B.

Cylindrické vložky

Ještě větší pokrok v propojení s elektronikou lze pozorovat v oblasti cylindrických vložek. Zde jsou na podstatně menším prostoru koncentrovány nejmodernější prvky používané v oblasti zabezpečení, kontroly prostupu, evidence průchodu a identifikačních médií se zachováním mechanických funkcí cylindrické vložky.

Nejjednodušším systém propojení mechanického a elektronického systému u cylindrické vložky, stejně jako u zadlabacích zámků, představují systémy blokovacích vložek, které jednoduchým elektromagnetickým blokováním rozhodují o oprávnění přístupu. Zde dochází na základě vyhodnocení identifikačního zařízení (čtečka apod.) k zablokování nebo uvolnění válce vložky nebo spojky uzamykacího zubu vložky.

Na vyšší technické úrovni jsou motorické cylindrické vložky, kde je skloubena funkce bezpečnostní vložky nejvyšší mechanické odolnosti s vlastním motorem a ovládáním elektronikou. Softwarové vybavení těchto vložek splňuje nejvyšší kritéria pro speciální systémy kontroly prostupu, evidenci docházky, propojení na EZS. Díky možnostem řídící jednotky lze naprogramovat přesně specifikované časové zóny, kdy bude cylindrická vložka odemčená nebo uzamčená, a mnoho dalších možností.

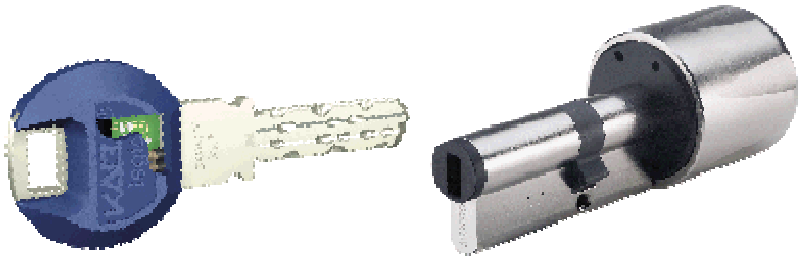


Obr. 22. Cylindrická motorická vložka Fa.Ba.

Obr. 23. Cylindrická motorická vložka Keso.

Známá je i cylindrická vložka, u níž je dominantním prvkem systému zvláštní klíč opatřený integrovaným speciálně vyvinutým čipem, a ve vložce zabudovaným identifikačním čtecím zařízením. Čip má přepisovatelnou paměť, do níž je naprogramována oprávněnost použití klíče k příslušné vložce opatřené miniaturní elektronickou čtecí jednotkou (typu Read-Write).

Díky programovému vybavení může systém sloužit nejen ke kontrole vstupu osob do objektu, ale např. i k evidenci neoprávněných pokusů o vstup, pokusu o sabotáž apod.



Obr. 24. Programovatelný klíč a vložka KABA elologic.

Velmi propracovaný je i další systém, kdy je nejmodernější elektronika obsažena jak v řídicí jednotce, tak v klíči samém. Mezi oběma počítači probíhá vzájemná výměna informací o přístupu, dochází k rozhodování o přístupu a zaznamenávají se veškeré aktivity. Inteligentní klíč je srdcem systému řízení přístupu. Klíč nese údaje o řízení přístupu a osobní identitě svého majitele. Každý klíč v popisovaném systému může být mnohosetkrát přeprogramován a sloužit tak postupně mnoha majitelům a mnoha funkcím. Nikdo nepovolaný s výjimkou pověřených pracovníků pro dané pracoviště tak nezíská přístup k potřebným údajům, ani si nemůže opatřit kopii.

Obr. 25. Inteligentní klíč.

Obr. 26. Kontrolní program. jednotka.

Od kvality cylindrické vložky závisí často i kvalita a úroveň zabezpečení celého objektu. Podle evropských norem se zvyšují požadavky na cylindrické vložky hlavně z pohledu jejich odolnosti proti běžným metodám „napadnutí“, ale také z pohledu kombinačních možností a právní ochrany uživatele. Proto cylindrická vložka zařazená do nejvyšší třídy bezpečnosti musí představovat výrobek, který je dlouhodobě odolný v nejnáročnějších podmínkách provozu a výrobce musí uživateli garantovat právní ochranu výroby klíčů.

Elektrické zámky

Elektrické zámky doplňují mezeru v přístupových systémech všech typů, neboť přinášejí kromě vysoce bezpečnostního ovládání zámku elektrickým signálem i širokou škálu zpětné signalizace detailně monitorující stav dveří (např. pohyb kliky, otevření dveří, odemknutí dveří, uzamknutí dveří apod.). Tato signalizace je bezpodmínečně nutná pro správné vyhodnocení poplachových stavů obsluhou EZS a pro případnou eliminaci falešného poplachu.

Elektrické zámky jsou vyráběny v nejrůznějším provedení funkcí tak, aby pokryly veškeré požadavky zákazníků. K dispozici je ucelená škála všech typů zámků, a to jak pro plné dřevěné nebo kovové dveře, tak pro dveře s úzkým profilem rámu (např. plastové). Je nutné si uvědomit, že součástí instalace musí být vestavěná ovládací jednotka a připojení na napájecí zdroj většinou 12V nebo 24V.

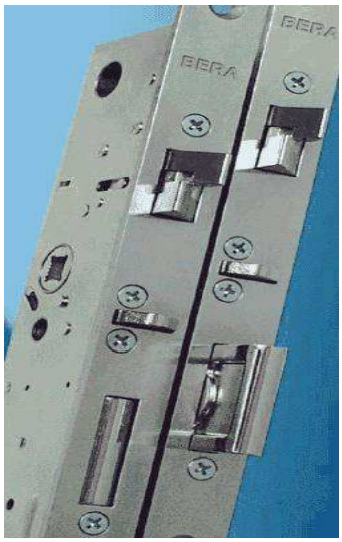
Zámky se principem odemykání dělí na zámky elektromechanické, tedy na zámky, které jsou po příchodu aktivačního signálu elektricky odblokovány a otevírány stiskem kliky, a na zámky elektromotorické, u kterých dochází plně k motorickému odemčení.

Obr. 27. Elektromechanický zámek Abloy EL 440.

Obr. 28. Elektromotorický zámek Abloy 8120.

Elektromechanické zámky jsou navíc vyráběny ve dvou provedeních. Buď při výpadku napájení zůstává zámek v uzamčeném stavu, nebo při výpadku napájení zůstává v odemčeném stavu, umožňujícím nouzově opustit prostory v případě požáru, výbuchu apod.

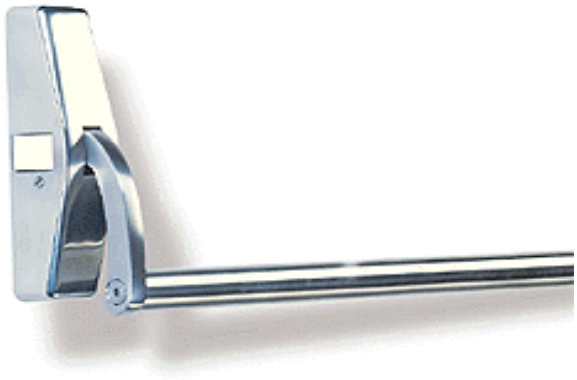
Dále se elektromotorické a elektromechanické zámky rozlišují podle toho, zda jsou elektricky ovládány z venkovní i vnitřní strany dveří, nebo pouze ze strany venkovní. V tomto případě je z vnitřní strany použita funkce antipanik, která umožňuje otevření dveří pouhým stiskem kliky.



Obr. 29. Samozamykací zámek BERA s funkcí antipanik.

Jinou možností jsou elektromechanická paniková kování. Je to nový bezpečnostní koncept zajišťující jak ochranu objektu proti násilnému vniknutí, tak možnost úniku při nouzové situaci. Systém splňuje požadavky na inteligentnější řešení únikových cest pomocí doplňkových funkcí jako blokování madla nebo elektromotorické ovládání madla a závor pro umožnění stálého vstupu po určitou dobu, například během otvíracích hodin nákupního centra. Použití je opět velmi široké – únikové cesty v objektech s kontrolou vstupu a úniku, které využívají muzea, nemocnice, supermarkety, banky a průmyslové objekty.

Systém může být napojen na další technická zařízení jako EPS, EZS, terminál pro kontrolu únikového východu, kartová čtečka, kódová klávesnice apod.



Obr. 30. Panikové kování Řada 89.

Celý sortiment zámků zajišťuje vysokou pasivní bezpečnost, neboť po dovření dveří se zámky automaticky uzamknou, a zároveň i zablokují střelku (dvojité jištění a blokace zámku).

Všechny elektromechanické a elektromotorické zámky je možné ovládat libovolným zařízením s výstupním kontaktem, např. kartovou čtecí jednotkou, ústřednou přístupových systémů, tlačítkem apod.

Jako doplňky k zámkům existují kabelové průchodky, protiplechy a bezpečnostní cylindrické vložky, které zaručují odolnost proti odvrtání, otevření planžetou a vysokou odolnost proti klimatickým vlivům.

Obr. 31. Bezpečnostní cylindrická vložka Fab NZS 3a.

Navíc je možné každý typ zámku vylepšit i odpovídajícím vysoce kvalitním bezpečnostním kováním, a to k elektromotorickým zámkům v provedení madlo – klika a k elektromechanickým zámkům v provedení klika – klika. Pro maximální komfort zákazníků je možné elektromotorické zámky kombinovat s automatickými dveřními ovládači.

Obr. 32. Bezpečnostní kování Komas 785.

Vzhledem k neustálému vývoji v oblasti cylindrických vložek a elektronických systémů a postupné miniaturizaci jednotlivých prvků lze i v dalších letech očekávat novinky v oblasti propojení mechanických zámků, cylindrických vložek a elektroniky. Přesto lze ale s potěšením konstatovat, že čistě mechanická funkce těchto zámků zůstává u všech známých výrobců zachována. To jenom potvrzuje známé rčení, že mechanické zabezpečení je základem správné strategie celkového zabezpečení každého objektu.

6 POŽADAVKY NA SYSTÉMY EKV PRO POUŽITÍ V ZABEZPEČOVACÍCH APLIKACÍCH

Systémy kontroly vstupů tvoří nezanedbatelnou část sytému celkové ochrany objektů. Zpravidla navazují některou částí na systémy elektronického zabezpečení objektu (např. rozhraní přístupového místa apod.), a tato část musí kromě jiného splňovat také požadavky ostatních norem na zabezpečovací systémy.

Systémové požadavky a funkční vlastnosti systému kontroly vstupů stanoví norma ČSN EN 50133-1. Přesný název této normy zní: Systémy kontroly vstupů pro použití v zabezpečovacích aplikacích – Část 1: Systémové požadavky. Tato norma se zabývá požadavky pro bezpečnostní aplikace v každém přístupovém místě, přitom v systému jich může být libovolný počet. Uvedená norma neobsahuje požadavky na prvky přístupu (turnikety, závory apod.), tyto jsou předmětem norem CEN/TC 33. Současně stanovuje i požadavky na odolnost proti působení okolních vlivů zejména z hlediska požadavků na EMC uvedených v ČSN EN 50130-4.

Stupeň zabezpečení přístupového systému dle ČSN EN 50133-1

Různé úrovně ochrany vedly k definování tříd rozpoznání při identifikaci uživatelů uplatňujících vstup příslušným přístupovým místem. Stupeň ochrany kontroly vstupů je založen na:

- klasifikaci identifikace uživatelů,
- třídě přístupu uživatelů.

Klasifikaci zabezpečení je možné definovat pro každé místo přístupu, a to odděleně pro vstup i výstup z chráněné zóny. Výsledná klasifikace zabezpečení je kombinací třídy identifikace a třídy přístupu.

Klasifikace identifikace

Klasifikace identifikace pro systémy kontroly vstupů odráží úroveň důvěrnosti ve vztahu k identifikaci oprávněných osob. Současně zohledňuje i riziko prozrazení oprávnění vlastního uživatele bez ztráty práva zachovat si výsadu vlastního přístupu. K identifikaci práva přístupu dochází na vstupních místech při použití identifikačního media. Norma

ČSN EN 50133-1, řadí identifikační prvky celkem do čtyř tříd pod označením 0 až 3 od nejnižšího stupně až po nejvyšší stupeň zabezpečení.

Třída 0 nevyžaduje žádnou přímou identifikaci a umožňuje přístup při použití jednoduchých ovládacích prvků jako např. tlačítek, kontaktů, čidel pohybu apod. Tento způsob bez identifikace může být použit pouze při opuštění chráněného místa.

Třída 1 je založena na informaci uložené v paměti, tj. informaci, která je známá uživateli, jako jsou např. hesla, osobní identifikační čísla (kódy) a podobně.

Třída 2 vyžaduje použití identifikačního prvku nebo biometrie, jako např. data ve formě přístupových karet, klíčů, geometrie ruky, otisku prstu a podobně.

Třída 3 je založena na kombinaci tříd 1 a 2, tedy na využití identifikačního prvku nebo biometrie spolu s informací uloženou v paměti. Přitom kombinace identifikačního prvku a biometrie je rovněž považována za třídu identifikace 3.

Klasifikace přístupů

Klasifikace přístupů zahrnuje požadavky systému kontroly vstupů na časový filtr a na ukládání přístupových transakcí. Systémy jsou děleny do dvou tříd přístupů:

- třída přístupu A,
- třída přístupu B.

Třída přístupu A platí pro místo přístupu, ve kterém požadovaný stupeň zabezpečení nevyžaduje ani časový filtr ani ukládání přístupové transakce.

Třída přístupu B platí pro místo přístupu, které zahrnuje časové filtry a funkce ukládání. Zahrnuje také podtřídu B1, která se vztahuje na místo přístupu zahrnující časové filtry, ale bez funkcí ukládání dat.

Společné funkční požadavky pro třídy A a B

Každému uživateli v systémech kontroly vstupů třídy přístupu B musí být umožněno přiřadit časový filtr (jedna nebo více časových zón přiřazených k přístupové úrovni). Program musí minimálně umožnit definovat dva časové úseky uvolnění – jeden 5 sekund a druhý 60 sekund. Dále musí umožnit definovat dva časové úseky otevření výstupních ovládacích prvků (apas), a to jeden 10 sekund a druhý 60 sekund. U systému, který se automaticky restartuje po připojení napájení, musí uchovat naprogramované přístupové parametry

po dobu minimálně 120 hodin po výpadku napájení. Současně musí být monitorován stav, zda je apas otevřen nebo uzavřen. Při připojení nebo odpojení napájení nesmí dojít k chybnému uvolnění vstupu.

Pro přístup třídy identifikace 1, která využívá informaci uloženou v paměti, nesmí být možné po sekvenci pěti za sebou nesprávně zadaných informací umožněn přístup dříve než po pěti minutách. Při pěti nesprávně zadaných sekvencích za sebou u stejného identifikačního prvku u přístupu třídy identifikace 3, což je kombinace identifikačního prvku nebo biometrie v kombinaci s informací uloženou v paměti, musí být vyslána výstraha do místa obsluhy. Komponenty a svorkovnice rozhraní místa přístupu musí být konstruovány tak, aby je nebylo možné otevřít bez nástrojů, a pokud k neoprávněnému otevření došlo, musí být umožněna signalizace sabotáže. Pro zabránění neoprávněné změny naprogramovaných dat v systému je nutné chránit přístup k programování jedním nebo více kódy. Minimální počet kombinací musí být 10^4 a správce systému musí mít možnost tento kód změnit.

Celková úroveň zabezpečení systémů kontroly vstupů je dána řadou faktorů, avšak za prvořadý faktor je považována úroveň identifikace oprávněného uživatele. Ta je především ovlivněna počtem kombinací a snadnosti zhotovení duplikátu. Pro třídu identifikace 1 musí být poměr počtu různých kombinací kódů k počtu identifikovatelných uživatelů nejméně 1000 : 1. Minimální počet kombinací systému musí být 10^4.

Pro třídu identifikace 2 a vyšší musí být především každému uživateli přiřazena jednoznačná identita. Struktura kódování identifikace musí poskytovat minimálně 10^6 kombinací a každá informace předávaná uživatelem do systému musí být s touto strukturou porovnána. Míra chybných odmítnutí nesmí přesáhnout 1 %.

Systém kontroly vstupů musí signalizovat a zobrazit formou výstrahy především sabotáž na komponentech systému, místo otevření přístupu bez oprávnění, a otevření místa přístupu po uplynutí povolené doby pro poskytnutí přístupu. Každá výstraha musí být ohlášena v místě obsluhy maximálně s desetisekundovým zpožděním. V bezpečnostních aplikacích musí být přístupové místo/prostor střeženy prvky EZS pro případ destruktivního proniknutí, které přístupový systém nepozná.

Pro systémy třídy přístupu B jsou nutné ještě další doplňkové funkční požadavky, především zabudování hodin reálného času s minimálním cyklem jednoho týdne a maximální odchylkou 5 sekund za den. Uživateli musí být umožněno přiřadit úroveň přístupu,

časový filtr musí mít v rámci této úrovně přístupu minimální rozlišení v týdnu po dnech a ve dni po minutách. V nepřetržitém provozu je pro případ výpadku sítě vyžadováno zálohované napájení. Systém musí mít prostředky pro ukládání do paměti, a ukládá minimálně následující události:

- detekce sabotáže včetně místa sabotáže,
- vstupu do režimu nebo výstupu z režimu programování,
- otevření přístupu bez oprávnění včetně uvedení místa,
- otevření přístupu po uplynutí povolené doby včetně uvedení místa,
- transakce s odkazem na uživatele a místo,
- odmítnutý přístup pro uživatele v systému s odkazem na místo.

Každá událost musí být uložena maximálně do 60 sekund a musí obsahovat údaj o druhu události, datum a čas. Systém musí mít kapacitu pro uložení minimálně 500 událostí. Systémy kontroly vstupů pro použití v rozsáhlejších objektech však v praxi tento požadavek mnohonásobně převyšují a mají kapacitu paměti řádově až desítky tisíc událostí.

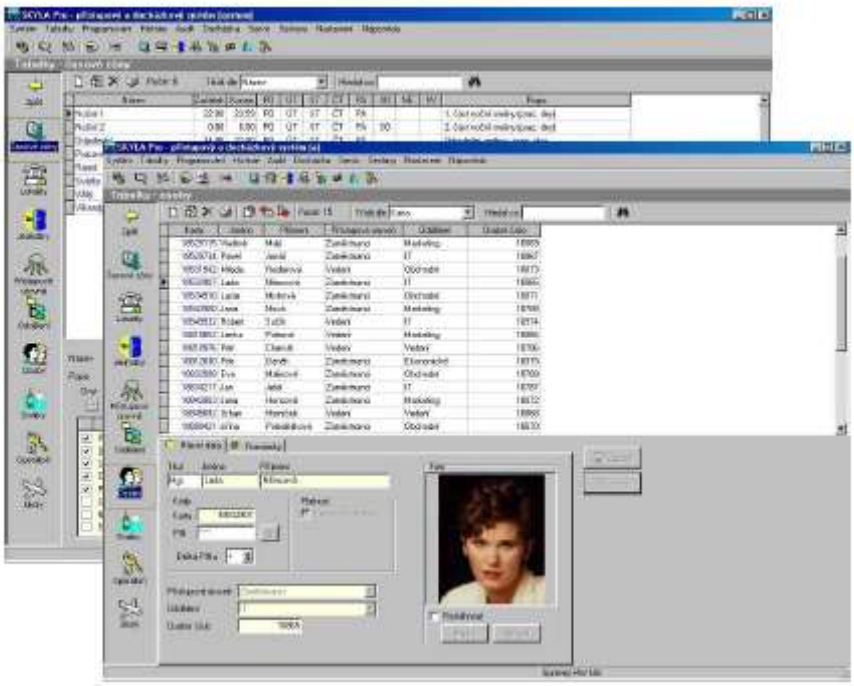
Systémy kontroly vstupu jsou obdobně jako ostatní systémy elektronické zabezpečovací signalizace vystaveny působení vlivů okolního prostředí. Jedná se především o vlivy, které nejsou ovlivnitelné obsluhou, a působí na systém nahodile v závislosti např. na klimatických podmínkách, rušení okolními zdroji elektromagnetických polí, rušením v napájecí síti a podobně. Jednotlivé komponenty systému kontroly vstupů vzhledem k jejich předpokládanému umístění mohou být určeny pro různé stupně klimatické odolnosti v rozsahu prostředí I až IV. Další oblastí ovlivňující provoz systémů kontroly vstupů jsou vlivy zahrnuté pod elektromagnetickou kompatibilitou, což je obor zabezpečující bezporuchovou činnost elektrického zařízení – v našem případě konkrétně systému kontroly vstupů tak, že dané zařízení není zdrojem rušení pro okolí, ani není jeho bezchybná funkce svým okolím nepřípustně narušena. Zde je nutné především při zkouškách odolnosti proti rušení sledovat, zda systém, vystavený těmto podmínkám, neumožní samovolný přístup, nebo zda nedochází ke změnám nastavení, případně ztrátě záznamu události apod.

Stupeň zabezpečení systému kontroly vstupů je výslednicí požadovaných technických parametrů a odolnosti vůči působení okolních vlivů spolu s provozní spolehlivostí.

7 SYSTÉM KONTROLY VSTUPU SKYLA PRO A HUB PRO

Dnešní doba přináší velkou konkurenci v nabízených systémech kontroly vstupu, záleží pouze na zákazníkovi, jaké má požadavky a který z nich bude preferovat. V této kapitole si představíme systém kontroly vstupu SKYLA Pro, s řídicí jednotkou HUB Pro. Tento přístupový systém je momentálně nabízen na trhu a je produktem firmy HONEYWELL.

7.1 SKYLA Pro



Obr. 33. Software SKYLA Pro.

SKYLA Pro je program pro konfiguraci, sběr dat a monitoring systémů kontroly vstupu malého až středně velkého rozsahu s řídicími jednotkami HUB Pro a docházkovými terminály DT2000 SA. Program umožňuje podrobné sledování jak vlastní činnosti přístupového systému (příchody, odchody, narušení režijních opatření apod.), tak i zpětné sledování operací a zásahu všech operátorů. Ze získaných dat může uživatel vytvářet filtrované přehledy, provádět základní vyhodnocení docházky nebo nechat data exportovat do programu PowerKey, ve kterém se provádí komplexní vyhodnocení docházky. Ke všem zmí-

něným funkcím poskytuje program SKYLA Pro uživateli bohatou paletu podpůrných funkcí a nástrojů.

Obr. 34. Ovládací panel programu PowerKey.

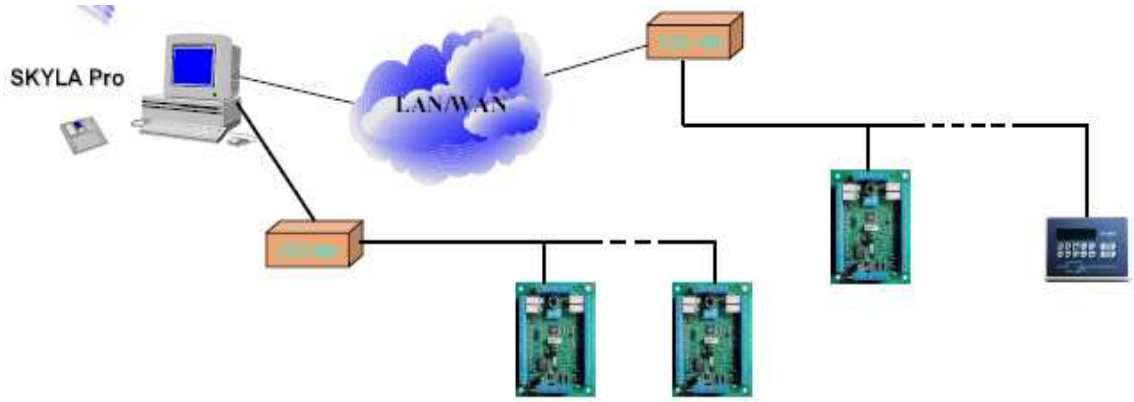
SKYLA Pro pracuje v operačních systémech Windows 9x, NT a 2000 a je koncipován jako aplikace typu klient/server. Pro uživatele tento koncept přináší především možnost souběžné činnosti více operátorů (max. 5) nad stejnými databázemi. Jednotlivé klientské aplikace komunikují se serverem prostřednictvím TCP/IP protokolů – systém tak lze spravovat prakticky odkudkoliv. Přihlášení všech operátorů je chráněno heslem, administrátor může navíc každému z nich povolit přístup jen do některých částí programu.

Základní úlohou programu SKYLA Pro je nastavení přístupového systému tak, aby v maximální možné míře vyhovoval požadavkům uživatele. K tomu používá sadu tzv. tabulek neboli databází, pomocí nichž se veškeré parametry systému kontroly vstupu nastavují. Jednoduchým a přehledným způsobem tak nadefinujete časové zóny, parametry všech jednotek HUB Pro i docházkových terminálů DT2000 SA, přístupové úrovně pro hromadné přidělování oprávnění kdo, kdy a kam může vstoupit, personální údaje osob včetně fotografií a uživatelsky nastavitelných poznámkových polí nebo oprávnění pro všechny operátory, kteří s programem mají pracovat.

SKYLA Pro pracuje s přehlednou definicí přístupových práv pro osoby prostřednictvím přístupových úrovní. V každé této úrovni můžete kromě povolení nebo zakázání přístupu navíc určit podmínku vstupu (pouze karta, pouze PIN nebo jejich kombinace) a také jejich režimy. Ten určuje, jak bude jednotka na platnou identifikaci osoby reagovat – prostým sepnutím relé na nastavenou dobu, jeho přepnutím do opačného stavu nebo rozepnutím, případně zda bude aplikován tzv. režim antipassback (kontrola směru průchodu). Přepínací režim slouží např. pro ovládání EZS nebo zásuvkových okruhů. Dveře navíc mohou být díky funkci tzv. autoodemknutí odblokovány i zcela samočinně v předem určených časových oknech.

Monitorování systému provádí SKYLA Pro dvěma způsoby. První způsob je řádkové vypisování všech událostí, které zaznamenávají jednotky HUB Pro nebo terminály DT2000 SA. Každá událost je doplněna o datum a čas vzniku a všechny ostatní potřebné informace (např. jméno a příjmení osoby). Tento přehled lze třídit a prohledávat podle různých kritérií. Druhým způsobem sledování systému je záznam veškerých akcí operátorů jako editace nebo mazání údajů v tabulkách, přihlášení, odhlášení apod. Také v tomto přehledu může správce rychle vyhledat požadované údaje.

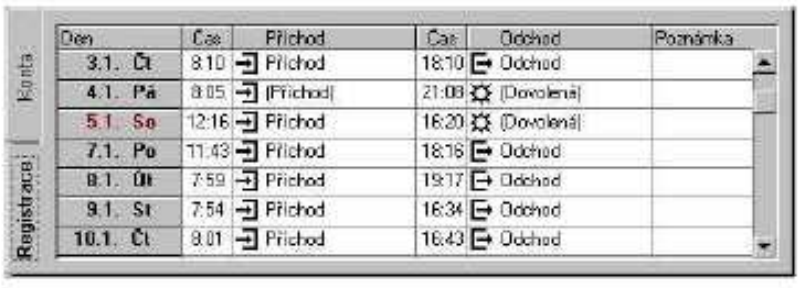
Komunikace s jednotkami HUB Pro nebo docházkovými terminály DT2000 SA může probíhat buď po metalické sběrnici RS-485 nebo dálkově přes LAN/WAN (TCP/IP) síť. Přímá podpora TCP/IP spojení umožňuje realizaci prakticky libovolně rozlehlého systému zahrnujícího např. i monitoring velmi vzdálených lokalit.



Obr. 35. Komunikace programu SKYLA Pro s HUB Pro a DT2000 SA.

SKYLA Pro je vybavena nástroji pro vytváření tzv. sestav. Jde o zpracované textové výpisy buď zaznamenaných událostí, nebo obsahu databází. Výpis hledaných událostí lze filtrovat podle řady kritérií – data, času a místa vzniku, typu události nebo třeba jména osoby. Pomocí sestavy může provádět i jednoduché vyhodnocení docházky (měsíční přehled přítomnosti, první a poslední událost za den apod.) nebo vytvořit přehled aktuální přítomnosti osob v objektu. Všechny tyto sestavy můžete kromě vytištění i exportovat do textového souboru pro další zpracování.

Na pokyn obsluhy nebo samočinně v nastavených časech se prování export docházkových dat z terminálů DT2000 SA, případně i jednotek HUB Pro do programu PowerKey, kde se docházka zpracovává komplexně. Přístupový a docházkový systém je tak téměř kompletně integrován do jediného.



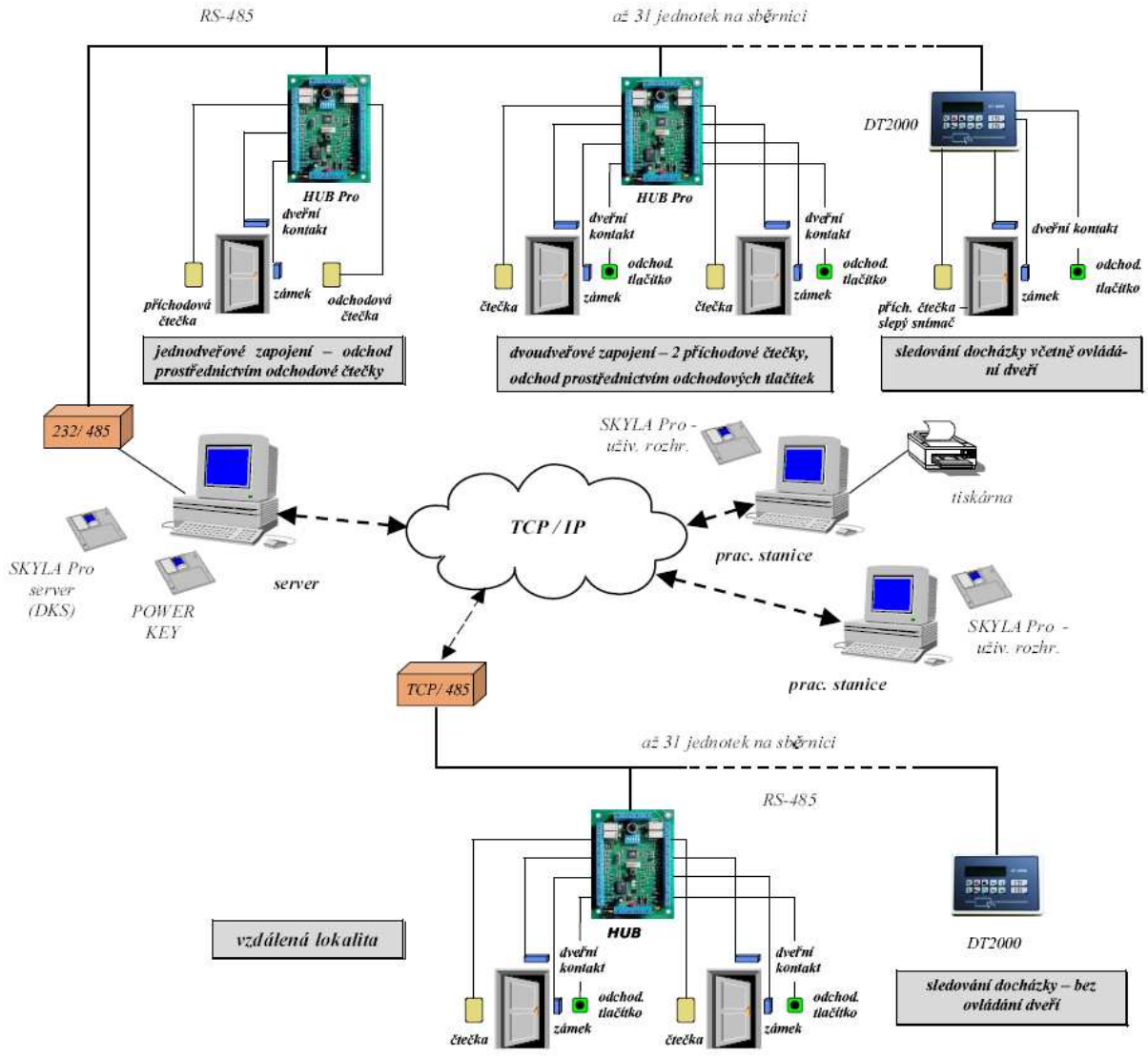
Obr. 36. Zpracování docházky v programu PowerKey.

SKYLA Pro umí ve spolupráci s jednotkami HUB Pro realizovat i tzv. anti-passback režim. Ten brání zneužívání karet k více násobným průchodům tím, že nepovolí dva příchody nebo dva odchody po sobě. Vždy pokud je anti-passback aktivní je nutné dodržet sekvenci příchod-odchod-příchod. Navíc lze nastavit i minimální časový interval, který musí mezi příchodem a odchodem uplynout – tzv. časový anti-passback. Režim anti-passbacku se nastavuje prostřednictvím přístupových úrovní u libovolné kombinace dveří, což umožňuje vyčlenit skupiny osob, pro které nebudou tato režijní omezení platit (např. management).

SKYLA Pro nabízí celou řadu diagnostických nástrojů užitečných pro oživení systému nebo lokalizaci hardwarových problémů a to od mapování sběrnic pro zjištění všech připojených a komunikujících jednotek až po podrobnou diagnostiku vybrané jednotky

nebo docházkového terminálu. Tou můžete dálkově ověřovat stavy všech stupů a výstupů, kontrolovat velikost napájecího napětí, mazat jednotlivé databáze v paměti jednotky nebo ovládat výstupy. Lze tak dálkově odemykat zámky, ovládat EZS, rušit probíhající poplachy apod.

SKYLA Pro je vybavena sadou podpůrných nástrojů pro usnadnění a zpohodlnění práce obsluhy. Mezi ně patří např. automatické zálohování všech databází v nastavených intervalech, samočinné programování karet do pamětí jednotek pro bezobslužnou aktivaci a exspiraci karet nebo posílání záznamů o probíhajících událostech na vybraný sériový port. Posledně jmenovaná funkce umožňuje tisk zaznamenaných událostí na řádkové tiskárně nebo integraci s jiným programem pro jejich další vyhodnocení.



Obr. 37. Princip funkce systému SKYLA Pro včetně integrace docházky.

7.2 HUB Pro

HUB Pro je řídicí jednotka pro systémy kontroly vstupu, určená k ovládání až dvou dveří v instalacích malého až středně velkého rozsahu. Sestává ze dvou identických polovin, tzv. podsystémů, z nichž každý řídí vstup buď do samostatných dveří (dvoudveřový režim) nebo do jedněch dveří, ale různými směry (příchod/odchod – jednodveřový režim). O konfiguraci jednotek i jejich monitoring se stará program SKYLA Pro.

Obr. 38. Řídicí jednotka HUB Pro.

Jednotky HUB Pro mohou pracovat i v síťovém provozu. V něm lze na společnou sběrnici RS-485 připojit až 31 jednotek a ovládat tak celkem 62 nezávislých dveří. Kromě jednotek HUB Pro mohou být na téže sběrnici připojeny i docházkové terminály DT2000 SA, což vytváří základní předpoklad pro plnohodnotnou integraci přístupového a docházkového systému. Díky plně distribuovaným databázím mohou jednotky pracovat i zcela autonomně, bez nutnosti komunikace s řídicím PC nebo ostatními jednotkami. Vedle sběrnice RS-485 může HUB Pro komunikovat s řídicím počítačem i přímo přes vestavěné rozhraní RS-232 nebo dálkově přes TCP/IP síť prostřednictvím terminálového serveru. HUB Pro je osazen pamětí pro 1.000 karet na každém z podsystémů a 10.000 událostí s označením data a času vzniku.

Jako vstupní snímače identifikačních údajů mohou být připojeny 2 čtečky bezkontaktních karet, čárových kódů, biometrické čtečky apod., které se svým okolím komunikují prostřednictvím Wiegand (26b, 27b, 32b, popř. 40b) nebo ABA (signály Clock a Data). HUB Pro tak podporuje většinu čteček všech hlavních světových výrobců. Čtečky lze kombinovat i s klávesnicemi pro zpřísnění podmínek vstupu (PIN + karta). Kromě rozhraní pro připojení čteček je každý z podsystémů osazen vstupy pro připojení dveřního snímače a odchodového tlačítka a jedním pomocným vstupem ovládajícím separátní relé.

Každý z obou podsystémů je vybaven jedním relé pro vládání dveřního zámku, jedním pomocným relé a jedním tranzistorovým výstupem indikujícím nestandardní stavy dveří jako násilné otevření nebo nedovření. Stavy všech reléových výstupů jsou indikovány pomocí čtveřice LED. Obě hlavní, zámková relé navíc mohou pracovat v několika režimech a to běžném, přepínacím (např. pro ovládání EZS), zavíracím nebo anti-passback režimu.

Jednotka HUB Pro se dodává buď jako deska plošného spoje nebo jako modul v kovovém krytu. Jeho neoprávněné otevření signalizuje tamper kontakt integrovaný na desku plošných spojů.

Tab. 1. Technické parametry řídící jednotky HUB Pro.

rozměry (V x Š x H)	133 X 70 X 35 mm
napájení (bez přip.čteček	10 ÷ 15 Vss (nom. 12 Vss) / 100 mA (max.)
počet četek / klávesnic	2, na každém podsystému 1 čtečka a 1 klávesnice
datová rozhraní pro čtečky	ABA (Clock, Data) / Wiegand (26b, 27b, 32b, 40b)
vstupy (každý podsystem)	▪ dveřní kontakt (NC) ▪ odchodové tlačítko (NO) ▪ pomocný vstup (NC) ▪ Data O, Data 1 (Wiegand) / Clock, Data (ABA)
výstupy (každý podsystem)	▪ relé pro ovládání dveřního zámku - přepínací kontakt 30V/4 A (rezist.) ▪ pomocné relé - dvojitý přepínací kontakt 3aV/2A (rezist.) ▪ tranzistorový výstup (12V/50mA)
indikace sepnutí relé	4xLED
ovládání LED a bzučáku čtečky	✓
ochrana vstupů a výstupů	(ochrana proti přepětí i přetížení)
komunikační rozhraní	▪ RS-232 (pasivní; RxD, TxD, GND) ▪ RS-485 (délka sběrnice max. 1.200 m) volitelné propojkou
indikace komunikace	2xLED
počet jednoket na sběrnici	max. 31 (RS-485)
kapacita paměti událostí	10.000 záznamů se značkou data a času
kapacita paměti karet	1.000 na každý podsystém
režimy karet	▪ normální ▪ přepínací ▪ zavírací ▪ anti-passback
obvod hodin reálného času	✓
časovač otevření zámku	1÷99 s
indikace dlouho otevř. dveří	✓
indikace násilně otevř. dveří	✓
počet časových zón / svátků	8 / 16
aut.přechod na letní / zimní čas	✓
rozsah pracovních teplot	-25÷65°C

7.3 DT2000 SA

DT2000 SA je terminál pro sledování docházky určený pro provoz v systému s ovládacím programem SKYLA Pro. Identifikace osoby se provádí prostřednictvím vestavěné bezkontaktní čtečky (standardně Motorola, Indala nebo HID). Terminál je vybaven membránovou klávesnicí pro zadávání tzv. důvodů přerušení, což je odchod na dovolenou, k lékaři, na oběd atd., a dvouřádkovým displejem pro zobrazování uživatelských informací. Kromě funkcí docházkového terminálu funguje jako kontrolér vstupu pro jedny dveře.

Obr. 39. Docházkový terminál DT2000 SA.

Podobně jako jednotky HUB Pro, i terminály DT2000 SA mohou pracovat v síťovém provozu, v němž lze na společnou sběrnici RS-485 připojit až 16 terminálů. Terminály DT2000 SA i jednotky HUB Pro mohou být zapojeny na téže sběrnici až do celkového počtu 31 zařízení a konfigurovány i monitorovány jediným programem. Z hlediska funkce kontroléru vstupu pracuje DT2000 SA jako jedna polovina jednotky HUB Pro. Díky plně distribuovaným databázím proto může terminál pracovat i zcela autonomně bez nutnosti komunikace s řídicím PC nebo ostatními prvky. Vedle sběrnice RS-485 může DT2000 SA komunikovat s řídicím počítačem i přímo přes vestavěné rozhraní RS-232 nebo dálkově přes TCP/IP síť prostřednictvím terminálového serveru. DT2000 SA je osazen pamětí pro 1.000 karet a 10.000 událostí se značkou data a času.

Kromě „prostého“ příchodu nebo odchodu umí DT2000 SA zpracovat až 8 dalších důvodů přerušení jako odchody na služební cesty, na dovolenou apod. Rychlý výběr správné volby uživateli usnadňují piktogramy na jednotlivých tlačítcích klávesnice. Textové popisy těchto přerušení jsou uživatelsky konfigurovatelné prostřednictvím programu SKYLA Pro. Displej s 2*20 znaky může uživatel využít i pro zobrazování libovolných jiných textů.

Vedle vestavěné čtečky můžete připojit k terminálu ještě jednu externí, tzv. slepý snímač, který slouží pouze pro identifikaci příchodů a může být umístěn na nechráněné straně dveří. Kromě rozhraní pro připojení čteček je DT2000 SA osazen vstupy pro připojení dveřního snímače a odchodového tlačítka. Výstupem terminálu je přepínací kontakt relé pro ovládání dveřního zámku. Terminál je proti neoprávněnému otevření chráněn vestavěným tamper kontaktem na desce plošných spojů.

Tab. 2. Technické parametry docházkového terminálu DT2000 SA

rozměry (V x Š x H)	135 X 190 X 50 mm
napájení	12 Vss /250 mA
počet četek	2 - vnitřní a vnější, tzv. slepý snímač příchodu
datová rozhraní pro čtečky	ABA (Clock, Data) / Wiegand (26b, 27b, 32b, 40b)
vstupy	▪ dveřní kontakt (NC) ▪ odchodové tlačítko (NO)
výstupy	▪ relé pro ovládání dveřního zámku -přepínací kontakt 30V/4 A (rezist.)
ovládání LED a bzučáku čtečky	✓
ochrana vstupů a výstupů	✓ (ochrana proti přepětí i přetížení)
komunikační rozhraní	▪ RS-232 (pasivní; RxD, TxD, GND) ▪ RS-485 (délka sběrnice max. 1.200 m) volitelné propojkou
indikace komunikace	2xLED
počet terminálů na sběrnici	max. 16 (RS-485)
kapacita paměti událostí	10.000 záznamů se značkou data a času
kapacita paměti karet	1.000
režimy karet	▪ normální ▪ přepínací ▪ zavírací ▪ anti-passback
obvod hodin reálného času	✓
časovač otevření zámku	1+99 s
indikace dlouho otevř. dveří	✓
indikace násilně otevř. dveří	✓
počet časových zón / svátků	8 / 16
aut.přechod na letní / zimní čas	✓
rozsah pracovních teplot	0 ÷ 40°C

8 ZHODNOCENÍ PROBLEMATIKY PŘÍSTUPOVÝCH SYSTÉMŮ A NOVÉ TRENDY

Praktické poznatky z realizace technických bezpečnostních systémů (EZS, CCTV, ACCESS) stále častěji poukazují na posuzování jejich užitné hodnoty podle stupně integrace s ostatními technologiemi. Vyhledávanou předností takovýchto systémů se stává schopnost jejich spolupráce na principu oboustranné interní komunikace.

V obecně technických požadavcích na bezpečnostní systémy vyžaduje každý uživatel nekompromisně co nejvyšší úroveň bezpečnosti, stabilní výkonnost, uživatelsky přívětivé prostředí a jednoduchý přístup k informacím. V případě integrace jednotlivých systémů se dostáváme k pojmu „inteligentní systémy“, jež pak chápeme jako systémy s integrovaným managementem, tj. se sjednoceným systémem řízení, zabezpečení a správy objektu nebo lokality.

Z hlediska problematiky systémů ACCESS musíme vzít v úvahu skutečnost, že samotný přístupový systém bez spolupráce se systémy EZS a CCTV nedokáže v řadě aplikací zabránit vstupu nežádoucích osob. Proto je v současnosti důležitým krokem při zabezpečení objektu integrace technické ochrany, tzn. najít vhodný integrující systém, který by byl schopen systémy, jako EZS, CCTV a ACCESS vhodně propojit a vytvořit tak přehledné prostředí pro práci operátorů a bezpečnostních pracovníků na všech stupních řízení.

Do oblasti nových trendů můžeme zahrnout to, že systémy ACCESS se podílí na správě tzv. „inteligentních budov“. Pokud uživatel v platném časovém okně vstoupí do povoleného prostoru, může dojít k vyvolání sekundární akce, jako je řízení technologických systémů. V praxi to znamená, že po správné identifikaci vstoupí osoba (zaměstnanec) do určitého prostoru např. kanceláře, kde se zapne klimatizace a osvětlení, včetně snímání analogových veličin, což jsou intenzita osvětlení, teplota apod. Pokud osoba tento prostor opustí, tak se klimatizace i osvětlení vypnou. Další vlastností systému ke správě a řízení budov je např. ovládání a monitoring výtahových kabin pro určitý počet pater apod.

Samozřejmě, že aplikace přístupového systému zahrnuje celou škálu možností využití. Mezi další možnosti patří systém výdeje klíčů, parkovací systém, sledování vjezdů a výjezdů vozidel, ovládání kopírek, platební a věrnostní systém, aplikace v průmyslové výrobě, sledování povinnosti pochůzkové činnosti, automatický výdej pohonných hmot, zajištění bezpečnosti na stadionech apod.

ZÁVĚR

Cílem této práce nebylo popsat veškeré možnosti přístupového systému, protože rozsah bakalářské práce zdaleka nepostačuje k tomu, abych do ní zahrnul veškeré možnosti a vlastnosti, kterými přístupový systém disponuje.

V této práci jsem se snažil objasnit, co to jsou přístupové systémy, jak pracují, jakou mají strukturu a možnost integrace s jinými systémy. Zejména jsem se zaměřil na identifikační systémy, které v systémech kontroly vstupu mají nepostradatelný význam. Dále tato práce vysvětluje, jak fungují biometrické identifikační systémy, které při identifikaci využívají charakteristických znaků člověka. Biometrické identifikační systémy jsou v současnosti z hlediska identifikace považovány za nejspolehlivější, ale patří mezi ty nejdražší. Používá se mnoho biometrických identifikací, z nichž mezi nejrozšířenější patří identifikace podle otisku prstu.

Přístupové systémy zařazujeme do elektronických zabezpečovacích prvků i přes to, že tyto systémy využívají pro svou činnost mechanických zábranných prostředků, jimiž realizují své výstupní reakce, což jsou například zamknutí či odemknutí dveří. Můžeme bezpečně říct, že mechanické zábranné prostředky ve spojení s elektronikou mají nezastupitelné místo v přístupových systémech.

V neposlední řadě jsem se zaměřil na některé skutečnosti, kterými se zabývá norma ČSN EN 50 133, což je norma, která popisuje systémy kontroly vstupu v bezpečnostních aplikacích.

Součástí práce je také aplikace přístupového systému, jenž je v současnosti nabízen na trhu firmou HONEYWELL. Tato aplikace přístupového systému je jedna z mnoha, kterou současný trh nabízí a posloužila k tomu, aby čtenář tento bezpečnostní systém pro kontrolu vstupu dokonale pochopil a seznámil se s jeho praktickým využitím v průmyslu komerční bezpečnosti. V závěru práce jsem zhodnotil problematiku přístupových systémů a popsal některé nové trendy, které systémy kontroly vstupu používají.

SEZNAM POUŽITÉ LITERATURY

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

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

[3] Čandík, M., Objektová bezpečnost II., Zlín: vyd. Univerzita Tomáše Bati ve Zlíně, 2004. ISBN 80-7318-217-3.

[4] Přístupové systémy, Magazín SECURITY, roč.VII, č.6/2000, s.3-17. ISSN 1210-8723

[5] Šiška, V., Identifikační systémy, Magazín SECURITY, roč.XII, č.2/2005, s.5-10. ISSN 1210-8723

[6] Toms, L., Mechanické a elektromechanické zábranné systémy, Magazín SECURITY, roč.XII, č.3/2005, s.8-10. ISSN 1210-8723

[7] Krejčí, J., Požadavky na systémy kontroly vstupů pro použití v zabezpečovacích aplikacích, Magazín SECURITY, roč.VII, č.6/2000, s.24-25. ISSN 1210-8723

[8] Bezpečnostní systémy s integrovaným managementem, Magazín SECURITY, roč.XI, č.6/2004, s.41. ISSN 1210-8723

[9] Vach, M., Radiofrekvenční identifikace osob, Zabezpečovací systémy, roč.II, č.1/2005, s.7.

[10] Vach, M., Biometrické identifikační systémy, Zabezpečovací systémy, roč.II, č.1/2005, s. 9-10.

[11] Instalační a uživatelské manuály firmy HONEYWELL

[12] *Kontaktní čipy DALLAS.* Dostupné z WWW: <http://www.icn-hardware.cz/produkty/pristupove_systemy/term_dallas.php>.

[13] *Kontaktní čipová karta.* Dostupné z WWW: <http://portal.oksystem.cz/pls/portal/PORTAL.wwv_media.show?p_id=580273>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

EKV	Systém kontroly vstupu
ACCESS	Systém kontroly vstupu
EZS	Elektrická zabezpečovací signalizace
EPS	Elektrická požární signalizace
CCTv	Uzavřený televizní okruh
ČSN	Česká norma
EN	Evropská norma
ISO	Mezinárodní norma
CEN/TC	Technická komise
PIN	Osobní identifikační číslo
RFID	Radiofrekvenční identifikace
EMC	Elektromagnetická kompatibilita
TCP/IP	Přenosové protokoly internetu/Internet protokol
SKYLA Pro	Typ softwaru pro systémy kontroly vstupu
HUB Pro	Typ řídící jednotky pro systémy kontroly vstupu
DT2000 SA	Typ docházkového terminálu
RS-485	Typ metalické komunikační sběrnice
RS-232	Typ metalické komunikační sběrnice
LAN	Typ komunikační sítě pro dálkový přenos dat
WAN	Typ komunikační sítě pro dálkový přenos dat
ABA	Datové rozhraní pro čtečky
WIEGAND	Datové rozhraní pro čtečky
LED	Světlo eliminující dioda

SEZNAM OBRÁZKŮ

SEZNAM TABULEK