Přístupové systémy (1)

Jedná se o relativně velkou oblast zabezpečovacích systémů s úkolem kontroly pohybu osob a zboží, event. i dalších subjektů, jako např. mobilní techniky. Systémy jsou navrhovány pro ochranu před vnikem nepovolaných subjektů, kontrole pohybu uvnitř systému a samozřejmě i ochraně proti úniku informací a dat.

Přístupový systém (ACS) neboli systém kontroly vstupů (SKV) můžeme chápat jako soubor opatření k zajištění řízení a evidence přístupu do zabezpečeného objektu nebo prostor na základě jednoznačně přidělených přístupových práv. Tato opatření mohou být systémová, fyzická (ostraha), mechanická (zámky, mříže, závory) nebo elektronická, v praxi se používá jejich kombinace. Přístupová práva jsou každému uživateli přidělena na základě personální politiky, stupně oprávnění, časového harmonogramu apod. Na základě jednoznačné identifikace uživatele je po ověření přístupových práv povolen nebo zamítnut přístup. Sofistikovanější systémy umožňují zajištění mnoha funkcí, např. sledovat pohyb a přítomnost osob v jednotlivých úsecích, definovat návaznost průchodů nebo měnit přístupová práva podle okamžité potřeby a nároků na strukturu přístupu.

Přístupový systém z hlediska svého určení zajišťuje především následující funkce [1]:

- Identifikace subjektu
- Zpracování dat
- Ovládání přístupového místa
- Programovatelnost
- Stavová hlášení
- Komunikace (s ostatními systémy nebo bloky přístupového systému)
- Styk s uživatelem (optické zobrazování, akustické signály)
- Napájení (systému nebo jednoho přístupového místa)
- Samoochrana (ochrana proti sabotáži, neoprávněné manipulaci, zjištění dat apod.)

Docházkový systém je pojem často zaměňovaný za pojem přístupový systém. U docházkových systémů je také nezbytné prokázání identity uživatele, ale hlavním cílem je především monitorování času a průchodu daným místem (příchod a odchod z pracoviště, monitorování povinných přestávek apod.). Docházkové systémy mohou být integrovány s přístupovými do jednoho celku s tím, že přístupových bodů je v objektu rozmístěno mnoho, zatímco docházkových bodů je obvykle mnohem menší počet (např. pouze u hlavního vstupu do objektu).

V článku jsou používané zkratky uvedené v Tab.1

ACS	access control system (přístupový systém)
SKV	systém kontroly vstupu
EZS	elektrická zabezpečovací signalizace
EPS	elektrická požární signalizace
APAS	ovládací prvky a senzory místa přístup
CCTV	closed circuit television (průmyslová televize, kamerové systémy)
LAN	local area network
WAN	wide area network
TCP/IP	transmission control protocol/internet protocol (nejpoužívanější protokoly internetu)
ESD	electrostatic discharge (elektrostatický výboj)
EMC	electromagnetic compatibility (elektromagnetická odolnost)
FAR	false acceptance ratio (míra chybného povolení přístupu)
RFID	Radio-Frequency Identification

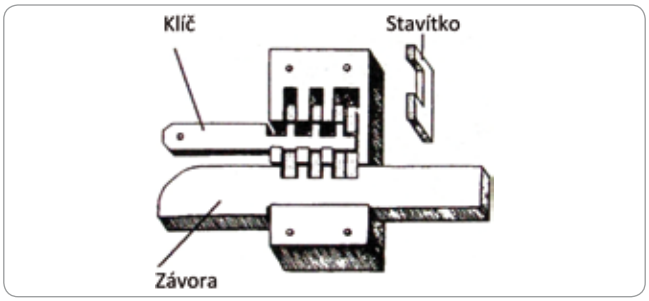
Tab. 1 Používané zkratky

Historie přístupových systémů

O ochranu majetku, osob a dalších hodnot se zajímají lidé od nepaměti. Kdysi v pravěku lidé schovávaly zbraně, jídlo a další vzácné předměty v proutěných koších do hlubokých děr, aby byly schovány před nepřátelskými kmeny. S vývojem způsobu a podmínek života lidí a především se změnou životního stylu se vyvíjely způsoby zabezpečení majetku.

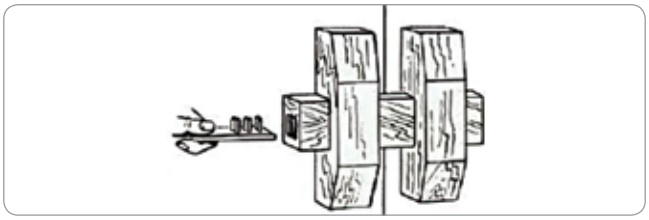
V Indii si majetní obchodníci stavěli domy obklopené vodními nádržemi, kde se volně pohybovali krokodýli. Pro volný průchod znali majitelé způsoby, jak krokodýli ovládat, např. pomocí opiátů. V antickém Řecku používali k zabezpečení svazování dveří domů speciálními uzly, které bylo obtížné pro neznalé rozvázat v krátkém čase. Bohužel tento způsob měl nedostatek v tom, že nezabránil zlodějům spleť uzlů rozřezat noži.

První mechanický zabezpečovací přístupový systém pochází ze starověkého Egypta. Byly to předchůdci dnešních zámků, tzv. egyptské dřevěné závory. Na obr. 1 je dřevěný zámek egyptského typu z roku cca 1500 B.C., jehož mechanismus se stal základem pro různé typy zámků a závor, pro otevírání se používá zásuvný klíč.



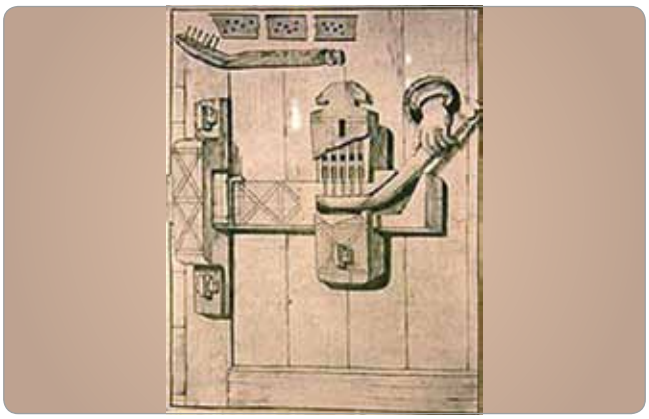
Obr. 1 Zámek egyptského typu z roku cca 1500 B.C.

Závory byly opatřeny systémem západek. Klíč představovala destička s kolíky, která se vsouvala do závory a nadzvedávala západky. Téměř všechny známé civilizace využívaly tento systém různě modifikovaný, do dnešní doby se zachoval v podobě cylindrické vložky – obr. 2.



Obr. 2 Egyptská dřevěná závora [2]

Princip egyptského zámku se stal známý po celém světě, varianty jsou známé z různých období. Zřejmě princip nevznikl jenom v Egyptě, ale zrodil se na více místech světa (Čína, Izrael nebo Persie). Na obr. 3 je uveden perský zámek, kde vnitřní závora šla odsunout, když byla dovnitř prostrčena ruka s klíčem a nadzdviženy příslušné kolíky [2].



Obr. 3 Perský zámek [2]

Římané znali kovové zámky umístěné na vnitřní straně dveří, které byly odemykány klíčem zvenku, klíče nosili jako ozdoby a šperky na krku nebo na oděvu. Po pádu Říma zámky zaznamenaly neobvyklý rozvoj, šířily se po celé Evropě i Orientu. Postupně se ustálily standardy a pozornost byla věnována vzhledu, technika stagnovala. Další vývoj zámků pokročil až v 18. století. Velké množství typů zámků zmizelo v propadlišti dějin, řada s historickými základy je používána i dnes, např. cylindrický zámek, v principu velmi podobný nejstarším zámkům známým z Egypta, Izraele nebo Persie.

Skutečný převrat ale nastal až s příchodem moderních, elektronicky řízených systémů, jež umožňují lepší zabezpečení vstupu do střeženého objektu. Odpadá též nutnost měnit zámek při ztrátě či odcizení klíče. I podoba samotného klíče se s postupem času měnila a dnes takto mohou sloužit magnetické karty, kontaktní i bezkontaktní čipy, číselné kombinace, radiové či IR vysílače a dokonce i části lidského těla, jako například oční duhovka či prst. Často také bývá vhodné kombinovat přístupový systém se systémem docházkovým, který umožňuje evidenci osob, jež se v objektu nacházejí.

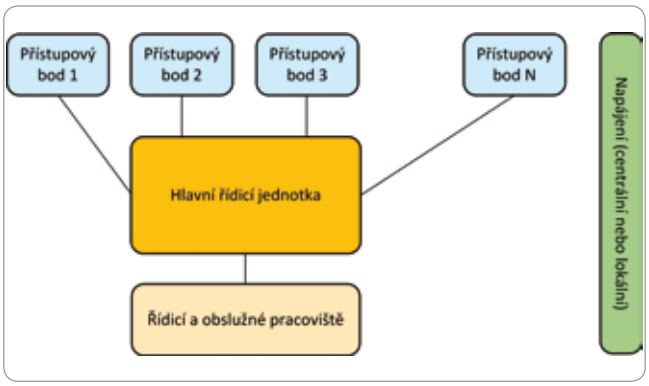
Faktem nicméně zůstává, že nejzranitelnější částí jakéhokoliv systému stále bývá lidský faktor. Při ztrátě přístupového klíče může být bez obtíží překonán i ten nejlepší zámek. Nejlepších výsledků tedy bývá dosaženo za použití kombinace elektronického a mechanického zabezpečení s několika různými klíči.

Struktura přístupového systému

Struktura přístupového systému se může odlišovat v závislosti na požadované aplikaci, obecně lze strukturu zobrazit na obr. 4, jako systém složený z následujících bloků:

- Přístupové body (jeden a více)
- Hlavní řídicí jednotka (pokud je v systému nutná)
- Napájení (centrální nebo lokální)
- Komunikační sítě (RS-485, LAN, proudová smyčka, bezdrátová komunikace)
- Řídicí a obslužné pracoviště (PC)

Uvedená topologie SKV a potřeba konkrétních prvků se může značně lišit v závislosti na potřebné aplikaci.

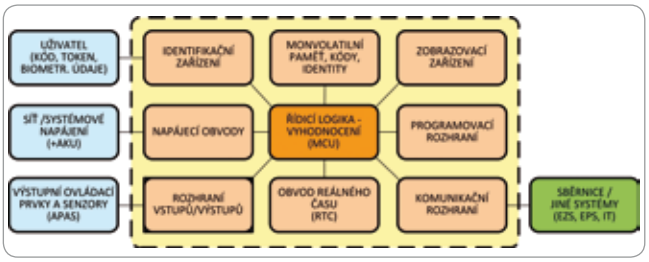


Obr. 4 Přístupový systém

Přístupový bod

Přístupový bod v SKV označuje uspořádání všech prvků, které umožňují kontrolovaný přístup do prostor nebo k informacím v daném místě. Přístupový bod se obecně skládá z několika součástí [1] – obr. 5:

- místa přístupu – zařízení, které může být ovládáno k poskytnutí přístupu, dveře, turnikety, brány apod.
- rozhraní místa přístupu – zařízení, které ovládá otevření a zabezpečení místa přístupu
  - řídicí jednotka/kontrolér – obsahuje řídicí logiku, vstupy/výstupy potřebné k ovládání APAS, zajišťuje převod dat z identifikačního zařízení, komunikaci apod.
- snímače místa přístupu – „identifikační zařízení“, čtečka, klávesnice, biometrie
- APAS – výstupní ovládací prvky a senzory přístupového místa
  - vstupní prvky – magnetické kontakty, spínače, optické závory (určeny k signalizaci a zabezpečení místa přístupu)
  - výstupní prvky – otvírač, zámek, motor turniketu apod.

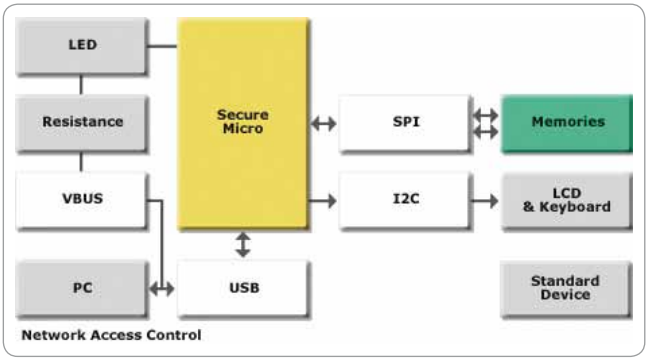


Obr. 5 Typický přístupový bod

Velké a složité přístupové systémy určené pro kontrolu pohybu uvnitř systému se realizují s využitím optických médií – obr. 6. [3].

Obr. 6 Přístupové systémy využívající optická média

Přístupové systémy jsou řízeny s využitím integrovaných elektronických obvodů, které lze jednoduše programovat a různě propojovat do sítí. Na obr. 7 je uvedeno blokové zapojení přístupového systémů [4].



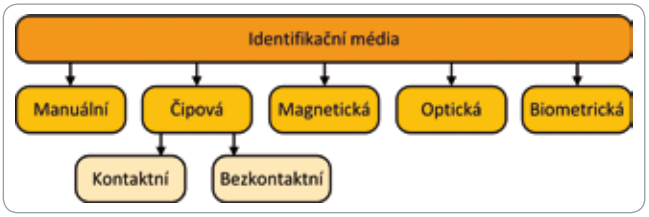
Obr. 7 Integrované obvody pro řízení přístupových systémů

Způsoby identifikace

Subjekt se může identifikovat různými způsoby, tj. s využitím různých parametrů, podle nich lze rozdělit identifikaci na jednotlivé typy. K často rozšířeným typům náleží identifikace s využitím hardware prostředků, tj. co musí subjekt mít u sebe (přívěsek, čip, karta, klíč apod.). Další typ využívá informaci uloženou v paměti subjektu (kód, heslo apod.). V současnosti jsou velmi rozšířené typy identifikace využívající typické fyziologické znaky subjektu a jeho chování (biometrické).

Pro identifikaci jsou podle typu identifikace využívány různé typy identifikačních médií, od jednoduchých a laciných až po složitá a drahá.

Identifikační média mohou být různého provedení s různými principy činnosti. Základní rozdělení identifikačních médií je uvedeno na obr. 8.



Obr. 8 Obvyklé dělení identifikačních médií

Manuálně ovládaná identifikační média

Do skupiny manuálních identifikačních médií patří například vypínače, kódové zámky, apod. Jsou pasivní a vyžadují manuální aktivitu (vstup) od subjektu (člověka). Příklad typického manuálního média – kódové klávesnice je na obr. 9.

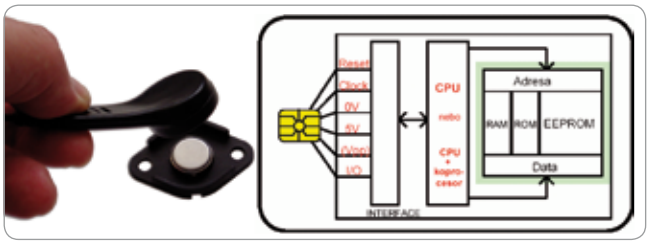
Obr. 9 Kódová klávesnice (CDVI DGA)

Identifikační čipy

Identifikátor je uložen v integrovaném obvodu (čipu, paměti), je možné čtení i zápis. Čipová média lze dále dělit podle způsobu předávání informací a napájení.

Kontaktní čipy

Identifikační médium vyžaduje přímý kontakt se čtečkou. Data se přenáší prostřednictvím vodivých spojení kontaktů čtečky s kontakty umístěnými na povrchu média. Typickým zástupcem jsou iButton čipy a kontaktní čipové karty (SmartCard) – obr. 10. Čtečky k těmto médiím jsou uvedeny na obr. 11.



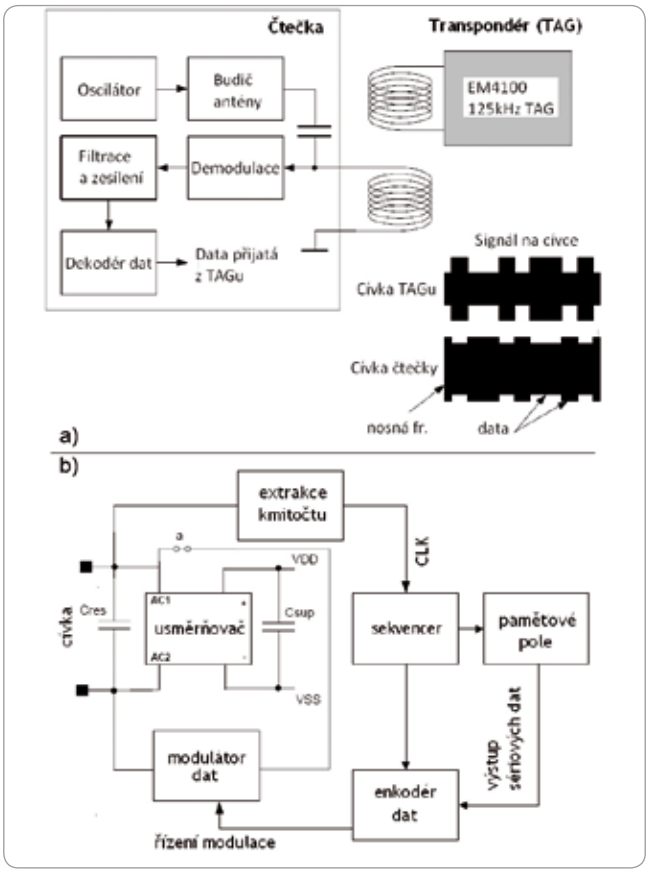
Obr. 10 Kontaktní čipové identifikační média:
a) iButton®, b) blokové schéma čipové kontaktní karty [5]

Obr. 11 Čtečky kontaktních čipových identifikačních médií:
a) iButton® čtečka b) čtečka čipových karet

Bezkontaktní čipy

Bezkontaktní čipová média nevyžadují přímý kontakt se čtečkou. Data jsou přenášena bezdrátově a napájení se získává z elektromagnetického pole vyzařovaného čtečkou. Patří sem pedevším přívěšky a čipové karty RFID.

RFID (Radio-Frequency Identification) je technologie, která využívá k přenosu informace mezi čtečkou a čipovým identifikačním médiem (tag) radiofrekvenčních vln. V současné době se jedná v SKV o nejrozšířenější identifikační metodu a prosazuje se masivně i v ostatních odvětvích. Formát média v SKV je nejčastěji karta nebo přívěšek. V případě karet mluvíme o tzv. proximitních kartách, jsou definovány v ISO/IEC 14443 a ISO/IEC 15693 (vicinity cards), nejčastěji pracují na frekvencích 125 kHz, 13,56 MHz. V „pasivních" RFID transpondérech (nemají baterii) vybudí čtečka svým elektromagnetickým polem dostatek energie k napájení a zároveň k přenosu informace klíčováním nosné frekvence, nikoli vysíláním – obr. 12. U „aktivních" transpondérů (pracují také v pásmu 2,4 GHz) dochází k nepřetržitému vysílání datové informace, u „pasivních traspondérů s baterií" dochází k vysílání pouze v případě aktivace čtečkou. Při přenosu dat je používáno manchester, bifázové nebo PSK kódování. V praxi je využíváno velké množství technologií různých výrobců, např. Unique EM, HID Prox, Indala, Mifare, iClass, FeliCa® iDM, CEPAS apod.



Obr. 12 Princip RFID: a) princip přenosu dat, b) vnitřní uspořádání EM4100 RFID čipu [6]

Poděkování

Obsah článku vznikl v souvislosti s řešením projektu Centrum bezpečnostních technologií (CEBET II) podporovaného MŠMT ČR, částečně v souvislosti s řešením projektu MV ČR VG 2010 2015 015 „Miniaturní inteligentní analyzační systém koncentrací plynů a škodlivých látek, zejména toxických".

Literatura

[1] ČSN EN 50133-1 + změna A1: Poplachové systémy – Systémy kontroly vstupů pro použití v bezpečnostních aplikacích – Část 1: Systémové požadavky, Česká technická norma, r. 2001 a 2003
[2] Technet.cz [online]. 2008-03-08 [cit. 2012-02-29]. Pavel Kasík: Klíče zapomínáme už 4000 let. Od dřevěných zámků k čtečkám otisků prstů. Zdroj: http://technet.idnes.cz/klice-zapominame-uz-4000-let-od-drevenych-zamku-k-cteckam-otisku-prstu-1gj-/tec_technika.aspx?c=A080307_153542_tec_technika_pka
[3] http://www.tensor.co.uk/
[4] http://www.st.com/stonline/domains/applications/security/access
[5] ROSOL I., [online]. 2008-10-10 [cit. 2010-11-30]. Čipové karty. Dostupné z WWW: <http://www.systemonline.cz/it-security/cipove-karty.htm>
[6] EM4100 katalogový list [online]: http://www.emmicroelectronic.com – 06/2011

Pokračovanie v budúcom čísle.

Prof. Ing. Miroslav Husák, CSc.
Ing. Tomáš Vítek
Ing. Tomáš Teplý
Katedra mikroelektroniky, Elektrotechnická fakulta ČVUT v Prahe