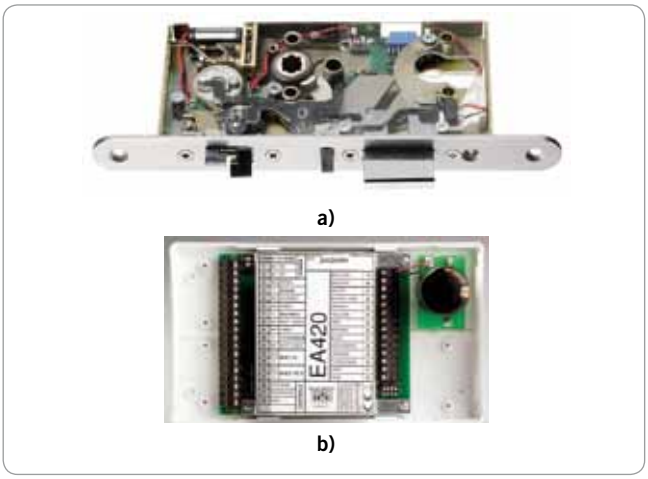
Přístupové systémy (4)

Elektromechanické a elektromotorické zámky a otvírače mohou být podle stavu, v jakém se nacházejí při přivedení napětí, rozděleny do dvou provedení:

- Běžné (tzv. fail-secure, pod napětím jsou uvolněny, po odpojení napájení se zablokují)
- Reverzní (tzv. fail-safe, pod napětím zablokovány, po odpojení napájení se uvolní)

Použití konkrétního provedení zámku pro daný prostup úzce souvisí se zálohováním přístupového systému a s požárními požadavky na tento prostup. Při návrhu bychom měli zajistit, aby v případě výpadku napájení nedošlo k samovolné změně stavu dveří, turniketů apod. Z požárního hlediska je však nezbytné zajistit za každých podmínek, aby se prostup, který je nadefinován jako únikový, vždy uvolnil a ostatní požární prostupy zůstaly zajištěny (z důvodu zamezení přívodu vzduchu, rozšíření požáru). Pokud je přístupovým systémem řízena i funkce výtahu, pak bývá při požáru vyžadováno sjetí výtahu do výchozí pozice. Konkrétní požadavky jsou předepsány požární zprávou projektové dokumentace. Je na zvážení projektanta, zda provede taková opatření, aby při požáru došlo k bezpečnému odblokování únikových prostupů tak, že bude přístupový systém zálohován (akumulátory, UPS…) a zároveň navrhne v požárních úsecích kabeláž funkčně odolnou požáru, nebo použije kombinaci běžných a reverzních typů zámků.



a)

b)

Obr. 31 Elektromotorický zámek Abloy EL520: a) zámková vložka, b) řídicí jednotka EA420

Téměř všechna uvedená výstupní zařízení se nabízejí v celé řadě variant, jednostranné, oboustranné, běžné nebo požární, se zvýšenou robustností, s integrovaným zjišťovacím kontaktem otevření, signalizací činnosti apod. Některé zámky umožňují konfiguraci fail-safe nebo fail-secure funkce zvlášť pro vnitřní a venkovní stranu. Zajímavostí je cylindrická motorická vložka se zabudovanou čtečkou, bezdrátovou konektivitou a vlastním napájením (Assa Abloy Aperio).

Legislativa

Vlastnosti kladené na systémy kontroly vstupu v bezpečnostních aplikacích jsou stanoveny v souboru norem ČSN EN 50133, ze kterých je v současné chvíli (06/2011) vypracována pouze „Část 1: Systémové požadavky“, „Část 2-1: Všeobecné požadavky na komponenty“ a „Část 7: Pokyny pro aplikace“. Tyto normy nemají závazný charakter, slouží především jako odkazové pro potřeby certifikace výrobků. V těchto národních normách jsou především stanoveny definice názvosloví a termínů, všeobecné funkční požadavky na systémy a komponenty, klasifikace stupně zabezpečení pomocí stanovení tříd identifikace a tříd přístupu. Dále jsou uvedeny definice a požadavky na třídy prostředí a třídy zařízení dle umístění, mechanické, atmosférické a elektrické zkoušky zařízení, požadavky na EMC, pokyny pro projektování, zřizování a provozování a požadavky na dokumentaci (prováděcí, provozní, pro údržbu, revize) - Tab. 3, Tab. 4.

Třída identifikace	Identifikace na základě	Příklad identifikačního média/kombinační bezpečnost
0	není přímá identifikace	tlačítko, kontakt, detektor pohybu (prostý požadavek na průchod)
		Pro vstup se předpokládá namátková kontrola nějakého dokladu nebo pověření fyzickou osobou (ostraha, vrátný).
1	dat uložených v paměti	heslo, číslo zaměstnance
		Poměr počtu uživatelů k počtu všech kombinací kódů musí být alespoň 1:1000. Minimální počet kombinací 10000.
2	identifikačních prvků nebo biometrie	identifikačních karta/přívěšek (token), čip, otisk prstu, oční duhovka, 3D model obličeje…
		Min. 1 mil. kombinací, jednoznačná identita uživatele, chybovost max. 0,01%. Identifikační číslo prvku nesmí být přímo zobrazeno.
3	kombinace třídy 1 a 2	jednoznačný token/otisk prstu + heslo
		Alespoň kombinace tříd 1 a 2.

Tab. 3 Třídy identifikace

Třída přístupu	Kritérium dělení
A	Pro přístupové místo není vyžadován časový filtr ani ukládání přístupových transakcí.
B	Přístupové místo má funkci časových filtrů (minimální požadavek na třídu B1) a ukládání dat.

Tab. 4 Třídy přístupu

Všechny prvky přístupových systémů však musejí splňovat požadavky na elektrickou bezpečnost (ČSN EN 60950, ČSN EN 60065), elektromagnetickou kompatibilitu (EMC) a odolnost (ČSN EN 61000, ČSN EN 55022, ČSN EN 50082, ČNS EN 50130), případně požadavky telekomunikačních norem (např. ČSN EN 50529), v případě integrace s jinými systémy také ČSN CLC/TS 50398. U prvků přístupových systémů musí být také samozřejmě prokázána shoda dle zákona 22/97 Sb. a nařízení vlády 17/2003 Sb. o technických požadavcích na výrobky NN a 616/2006Sb. o EMC kompatibilitě. Požadavky na mechanické prvky přístupových systémů (otvírače, dveře, brány, turnikety…) jsou uvedeny ve standardu Evropské komise CEN/TS 33. Národní bezpečnostní úřad (NBÚ) vydal pro potřeby přístupových systémů a objektové bezpečnosti vyhlášku č. 339/99 Sb. Souhrn zde uvedených norem, zákonů a vyhlášek není zdaleka vyčerpávající, není předmětem tohoto materiálu.

Integrace SKV s jinými systémy

Kombinace se slaboproudými systémy

Systémy kontroly vstupů mohou být provázány s jinými slaboproudými systémy, jejich funkce integrovány nebo rozšířeny. V praxi existují převážně kombinace s těmito systémy:

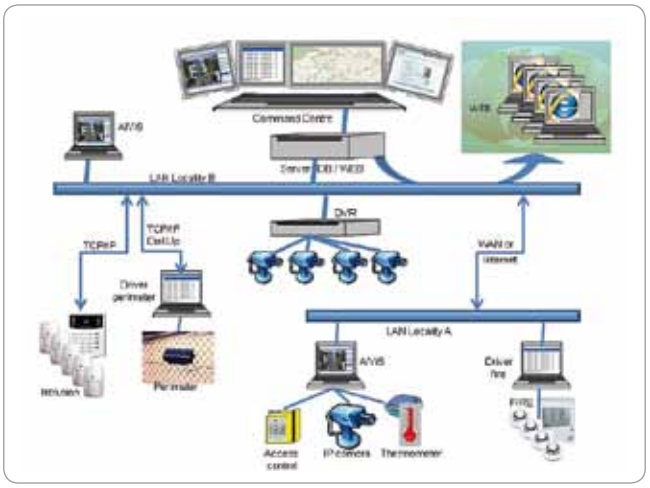
- Docházkový systém – v jednom systému jsou použity docházkové i přístupové funkce
- Stravovací systém – využívá se především shodných identifikačních médií, jinak samostatný systém
- Elektrická zabezpečovací signalizace (EZS) – sofistikovanější sběrnicové systémy EZS často podporují základní funkce přístupových systémů, výhodou je zde možnost ovládat systém EZS prostřednictvím přístupových identifikátorů, monitorovat stav EZS za dveřmi na čtečce apod. (např. otevření dveří a zároveň

odjištění EZS subsystému / delší podržení zajistí EZS subsystém apod.)

- Elektrická požární signalizace (EPS) – EPS je vždy samostatný, při evakuaci nebo požáru je však nutné zajistit správnou funkci všech přístupových bodů, odblokovat únikové cesty, zablokovat požární prostupy apod. EPS poskytuje tyto signály prostřednictvím vstupně/výstupních modulů (relé)
- Kamerový systém (CCTV) – CCTV systém může při časové synchronizaci s SKV poskytnou doplňkové obrazové informace ke každé prostupové události
- IT systémy – samostatnými čtečkami identifikačních médií připojenými k PC se může řídit přístup k PC, k síti apod.
- Měření a regulace – přítomnost osob může např. automaticky přizpůsobit osvětlení, vytápění apod.

Softwarová integrace

Softwarová integrace je vhodná všude tam, kde vzhledem na požadavky obsluhy nebo složitost objektu, vybaveného množstvím různých slaboproudých zařízení, není možné bez počítačové nadstavby dosáhnout přehledného monitorování a řízení objektu. Z důvodu zjednodušení, zpřehlednění, a zároveň snížení nákladů za jednotlivé systémové softwary, je možné použít tzv. „integrační softwary“ (grafické, vizualizační nadstavby) – obr. 32. Ty vzájemně integrují systémy kontrolu vstupu, docházky, elektrickou požární signalizaci, elektronické zabezpečovací systémy, kamerové systémy a systémy měření a regulace. Nabízejí funkce vizualizace, centrálního managementu, analýzy událostí, automatizaci bezpečnostních procesů, správu identit, řešení krizových situací apod. Pracují na různých softwarových platformách (obvykle Windows), spolupracují s SQL databázemi. Je zřejmé, že integrovat je možné pouze systémy, které mají podporu integračního softwaru. Obecně platí, že produkty solidních výrobců velkých bezpečnostních systémů jsou podporovány alespoň v nějakém nadstavbovém integračním softwaru, bohužel nemusí vždy dojít ke sladění všech technologií tak, aby byly pokryty jedním integračním softwarem. Dopracování technologií je často možné pomocí uvolněného SDK individuálně na zakázku.



Obr. 32 Příklad architektury integračního softwaru AIViS [17]

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
[7] Karty s magnetickým proužkem http://pandatron.cz/?535&karty_s_magnetickym_pruhem
[8] (www.st.com)
[9] Teplý,T., Přístupové systémy, přednáška, ČVUT, 2008
[10] http://www.cl.cam.ac.uk
[11] http://www.bundesregierung.de/Content/EN/Artikel/2007/11/Bilder/hightech-serie-sicherheit-3d-objekterfassung,layoutVariant=Poster.html
[12] http://www.3dface.org/media/images.html
[13] Husák,M., Mikrosenzory a mikroaktuátory, Academia 2008
[14] Meghdadi, Majid; Jalilzadeh, Saeed (29 October 2005). „Validity and Acceptability of Results in Fingerprint Scanners“. Proceedings of the 7th WSEAS International Conference on Mathematical Methods and Computational Techniques In Electrical Engineering. Retrieved 4 November 2010.
[15] http://www.sandiacontrolsystems.com/page3.html
[16] Informace o přístupových systémech, firma Aktion [online]: http://www.aktion.cz - 06/2011
[17] Informace o integračním software AIViS [online]: http://www.alvis.sk - 06/2011

Koniec seriálu.

Prof. Ing. Miroslav Husák, CSc.

Ing. Tomáš Vítek

Ing. Tomáš Teplý

České vysoké učení technické v Praze
Elektrotechnická fakulta, Katedra mikroelektroniky