Integrace systémů kontroly a řízení vstupu

Integration of access control systems

Bc. Petr Švejčara

Diplomová práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2010/2011

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

Jméno a příjmení:	**Bc. Petr ŠVEJČARA**
Osobní číslo:	**A09406**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Integrace systémů kontroly a řízení vstupu**

Zásady pro vypracování:

1. **Pojednejte o významu, použití a možnostech přístupových systémů (ACS).**
2. **Analyzujte požadavky technických předpisů na ACS.**
3. **Pojednejte o použití a systémových požadavcích na integrované poplachové systémy.**
4. **Specifikujte možnosti integrace ACS v zabezpečovacích systémech.**
5. **Vypracujte ideový návrh ACS ve struktuře integrovaného zabezpečovacího systému na modelovém objektu.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **KŘEČEK Stanislav. Příručka zabezpečovací techniky. 3. vyd. Praha: Critetus, 2006. 315 s. ISBN 80-902938-2-4.**
2. **UHLÁŘ, J. Technická ochrana objektů II. [učební text]. 1. vyd. Praha: Policejní akademie České republiky, 2005. 230 s. ISBN 80-7251-189-0.**
3. **Software pro ústředny EZS [online]. Brno: ADI Global Distribution, 2011 [citováno 2011-01-24]. Dostupné z URL [http://www.adiglobal.cz].**
4. **ČSN CLC/TS 50398 Poplachové systémy- Kombinované a integrované systémy- Všeobecné požadavky. Praha: ÚNMZ.**
5. **ČSN EN 50133-1 ed. 2. Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích - Část 1: Systémové požadavky. Praha: ÚNMZ, 2001.**

Vedoucí diplomové práce: **Ing. Jan Valouch, Ph.D.**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **25. února 2011**

Termín odevzdání diplomové práce: **27. května 2011**

Ve Zlíně dne 25. února 2011

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Diplomová práce pojednává o významu, použití a možnostech přístupových systémů (Acces control systems- ACS). Analyzuje požadavky technických předpisů na ACS. Práce se rovněž zabývá použitím a systémovými požadavky na integrované poplachové systémy a specifikací možnosti integrace ACS v zabezpečovacích systémech. Stěžejní výstup práce představuje návrh ACS ve struktuře integrovaného zabezpečovacího systému na modelovém objektu.

Klíčová slova: přístupové systémy, ACS, integrované poplachové systémy, zabezpečovací systémy, integrace.

ABSTRACT

The topic of the diploma thesis is the significance, use and potential of the access control systems (ACS). The thesis analyses the requirements imposed on the ACS by technical regulations. Furthermore, it covers the use and the system requirements of integrated intruder alarm systems, and carries out a specification of the possibility to integrate the ACS in alarm systems. The principal output of the thesis is a project of the ACS incorporated in the structure of integrated intruder alarm systems, shown in a model building.

Key words: access control systems, ACS, integrated intruder alarm systems, alarm systems, integration.

Poděkování, motto

Děkuji mému vedoucímu, Ing. Janu Valouchovi, Ph.D., za odborné vedení, cenné rady a připomínky, které mi velmi pomohly při psaní mé práce.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně ……

podpis diplomanta

OBSAH

ÚVOD

Pro svou diplomovou práci jsem si zvolil téma, které se týká přístupových systémů a jejich integrace do zabezpečovacích systémů. Toto téma mě zaujalo, protože jsem se chtěl dozvědět více o přístupových systémech a jejich vzájemných kombinacích v zabezpečovacích systémech.

Přístupové systémy nám umožňují kontrolu pohybu osob, jejich přístupových práv do objektů, budov, místností, a přístupů k zařízením (tiskárny, PC). Po předložení identifikačního média nebo ověření platnosti přístupového kódu je umožněn vstup do místnosti nebo objektu. To umožňují systémy, jako jsou automatické závory, turnikety, kódové klávesnice, čipové karty a jiné. Přístup uživatele se zjišťuje podle toho, jestli zná heslo, vlastní identifikační médium (čipová karta) nebo se identifikuje biometrickou charakteristikou. Na základě uvedené autentizace je vstup do objektu povolen nebo ne.

V dnešní době se klade velký důraz na zabezpečení objektu a na monitorování pohybu osob v areálech. To však zahrnuje spojení více systémů do jednoho celku, který takovouto integraci umožňuje. Dnešní technicky vyspělá doba však vyžaduje, aby integrované systémy byly co nejefektivnější, nejjednodušší a aby zajišťovaly vysokou bezpečnost. Zejména u poplachových aplikací, které chrání osoby a majetek se vyžaduje vysoká míra zabezpečení a ochrany. Také se zvyšují nároky jednoduchého ovládání a komfortu u nepoplachových aplikací při řízení technologických procesů budov. Integrovat se mohou různé systémy, avšak platí, že některé systémy přináší v integraci více výhod než jiné. Přístupové systémy můžeme nejčastěji integrovat se zabezpečovacími a docházkovými systémy, také se jejich vlastností využívá v mzdovém účetnictví, především v podnikatelské sféře. V mé diplomové práci se budu zabývat integrací ACS (Acces control systems), a to jak kombinacemi různých typů technologií, druhů přístupových zařízení, tak i integrací se systémy MZS (Mechanické zábranné systémy), PZS (poplachové zabezpečovací systémy) a CCTV (systémy uzavřených televizních okruhů), docházkovými systémy a s řízením technologických procesů budov, kde navrhnu možné způsoby integrace přístupových systémů s ostatními systémy. Práce analyzuje požadavky technických předpisů na ACS. Výstup diplomové práce tvoří ideový návrh ACS v modelovém objektu.

I. TEORETICKÁ ČÁST

1 SYSTÉMY KONTROLY VSTUPU

Systémy kontroly vstupu jsou systémy, které se používají pro kontrolu pohybu osob v objektech, jejich evidenci a určení práv přístupu.

Systémy kontroly vstupu

Slouží pro řízení přístupu k chráněným zařízením, informacím na základě jednoznačně přidělených přístupových práv.

Docházkové systémy

Slouží ke sběru informací o čase a důvodu průchodu místem kontroly a jejich dalším zpracování.

Tyto dva systémy spolu vytvářejí integrovaný identifikační systém kontroly vstupu.[1]

Obr. 1 Ukázka přístupového systému [1]

1.1 Význam a použití systémů kontroly vstupu

Systém kontroly vstupu nám určuje oprávněnost vstupu do jednotlivých objektů nebo jejich částí, tyto vstupy následně eviduje a ukládá. Zabraňuje tak přístupu neoprávněných osob do vyhrazených prostor, k utajovaným informacím, nebezpečných prostorů aj. Umožňuje sledování pohybu osob, jejich vyhledávání, kontrolu průchodu a pokusů o neoprávněný přístup.[2]

Součástí systémů kontroly vstupu jsou tyto části:

- Systém snímání průchodů – je tvořen elektronickými snímači- terminály, které jsou umístněny na místech, kde je potřeba monitorovat průchody a též řídit přístup.
- Přístupový terminál – je specializované zařízení, které zajišťuje veškeré přístupové funkce. Tvoří ho základní jednotka, která je umístněná v nepřístupné oblasti uvnitř chráněné zóny.
- Sledování stavu – přístupových terminálů, které se provádí na určených monitorech.
- Definování přístupových modelů – při konfigurování systému se vytvářejí přístupové modely pro skupiny či jednotlivce, přiřazované konkrétním osobám a terminálům.
- Sledování průchodu přes zámky – umožňuje trasovat průchody a kontrolovat přítomnost vybraných osob v zadaném časovém intervalu pro konkrétní terminál.
- Systém antipassback – (systém antipassback) tento systém umožňuje hlídání opakovaných vstupů v jedné zóně, tzn. pro každý vstup jeden výstup.[3]

Typy vstupních oprávnění:

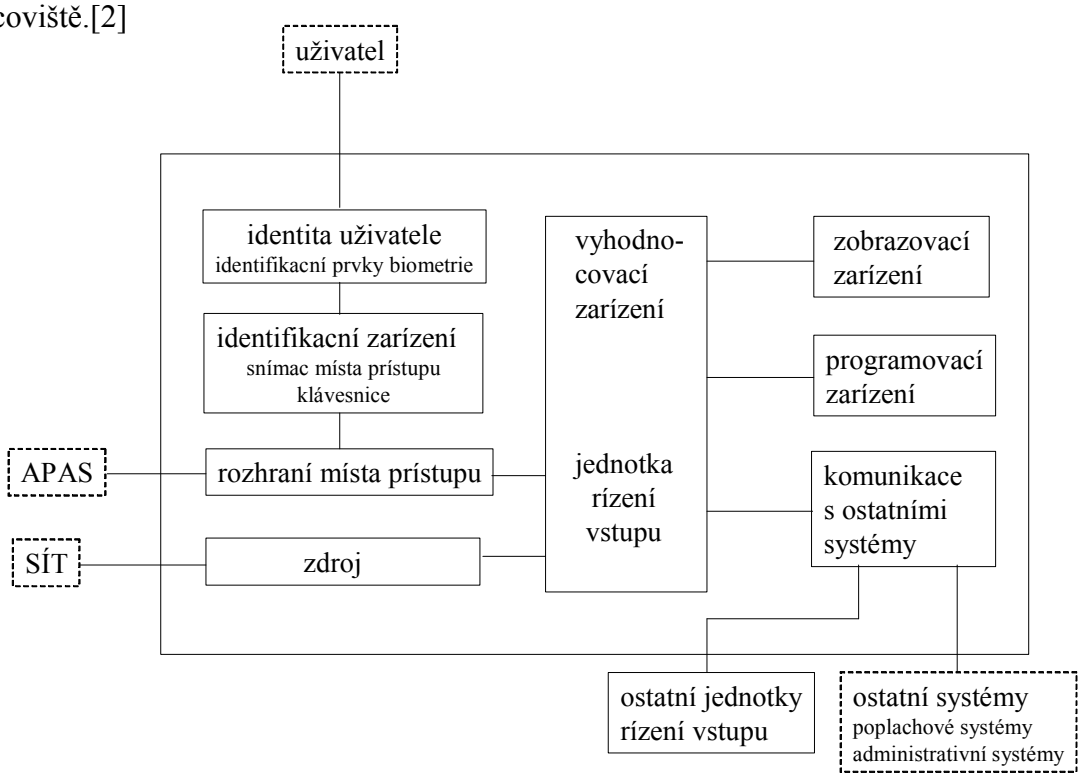
- generální oprávnění ke vstupu – uživatel má povolen vstup kdykoliv a kamkoliv,
- omezení generálního oprávnění – uživatel má povolen vstup kdykoliv a kamkoliv, ale jen s pověřenou další osobou,
- časově omezené oprávnění – uživatel má povolen vstup kamkoliv, ale jen v určité době,
- prostorové omezení oprávnění – uživatel má povolen vstup do určitých prostor kdykoliv,
- prostorově a časově omezené oprávnění – uživatel má povolen vstup v určité době do určitých prostor,
- oprávnění vstupu s omezením – umožněn vstup pokud je v prostoru méně než X osob, nebo více než X osob.[2]

Typy zón:

- časová zóna – představuje časové intervaly, ve kterých je povolen nebo zakázán vstup do prostoru.
- prostorová zóna – představuje vymezení oblasti, pro kterou je povolen nebo zakázán vstup.

Struktura systému kontroly vstupu

Systém se skládá z čtecího a snímacího zařízení, vyhodnocovací jednotky, výstupního prvku (zámek, indikátor = APAS), napájecího zdroje a dohledového a správního pracoviště.[2]



Obr. 2 Schéma struktury systému kontroly vstupu [2]

1.2 Typy autentifikace

K ověření přístupu do místnosti je potřeba autentizace uživatele. Uživatel se autentizuje znalostí hesla, vlastněním identifikačního média nebo biometrickou charakteristikou.

Autentizaci rozdělujeme na:

Autentizace heslem

Je založena na znalosti hesla uživatelem. Heslo je utajené a známé jen uživateli. Toto heslo uživatel zadá přístupovému systému. Výhodou této autentizace je jednoduchá, technická a programová realizace a relativně nízká cena. Nevýhodou je nutnost zapamatování hesla, přičemž se dá heslo snadno zneužít /zjistit/.

Autentizace předmětem

Je založena na vlastnictví tokenu. Jedná se o obecné označení autentizačního předmětu, který potvrzuje identifikaci nositele. Výhodou této autentizace je vyšší úroveň zabezpečení. Nevýhodou je možnost ztráty, odcizení identifikačního předmětu.

Tokeny:

- Tokeny paměťové – paměť karet obsahuje jednoznačný identifikační řetězec.
- Tokeny udržující heslo – po zadání jednoduchého uživatelského hesla je výstupem přístupový klíč.
- Tokeny s logikou – zpracovávají jednoduché podněty (vydej následující klíč, vydej cyklickou sekvenci klíčů, apod.).
- Inteligentní tokeny – obsahují vlastní vstupní zařízení pro komunikaci s uživatelem, časovou základnu, mohou šifrovat, generovat náhodná čísla, apod.

Biometrická autentizace

Autentizace založená na biometrických charakteristikách uživatele. Výhodou biometrických autentizací je, že uživatel na prokázání své identity nepotřebuje znát žádné heslo nebo vlastnit token, např: kartu. Další výhodou je rychlost systému a jednoduché ovládání. Nevýhodou snímání biometrické charakteristiky je přesnost měření, které může mít za následek povolení vstupu nepovolené osoby do objektu a naopak zabránění vstupu povolené osoby do objektu.

Typy autentifikací

Podle počtu použitých metod k autentifikaci rozlišujeme:

- *Jednofaktorová autentifikace – použití jedné metody.*
- *Dvoufaktorová autentifikace – použití kombinace dvou metod, např. token + heslo.*
- *Třífaktorová autentifikace – použití tří metod autentifikace[3]*

1.2.1 Magnetická média

Jedná se o identifikační karty o velikosti kreditní karty. Jsou opatřeny magnetickým páskem z jedné strany, který nese uloženou informaci. Tato informace se přečte pomocí čtecího zařízení. Zápisem dat na magnetický proužek pomocí magnetické indukce se vytvoří množství malých permanentních magnetů.

Obr. 3 Ukázka magnetické karty [3]

Tyto magnety nabývají dvou stavů a to:

- Logická 1 – zmagnetizovaný
- Logická 0 – nezmagnetizovaný

Páska na magnetických kartách obsahuje tři stopy, které jsou dány normou ISO 7811. Každá ze stop má svůj specifický význam a umožňuje uložení určitého množství informací.

- 1. stopa – má velikost 78 B a ukládá numerické a alfanumerické znaky.
- 2. stopa – má velikost 40 B a ukládá numerické znaky 0-9 a rovnítko.
- 3. stopa – má velikost 107 B a ukládá numerické znaky 0-9, rovnítko a dvojtečku[3, 4].

Podle hustoty záznamu informací karty dělíme na:

- **LoCo** (Low Coercivity) s nízkou hustotou záznamu. Tyto karty vyžadují menší množství magnetické energie k záznamu a zapisovací zařízení LoCo, jsou mnohem levnější než čtecí zařízení HiCo.
- **HiCo** (High Coercivity) s vysokou hustotou záznamu. Tyto karty jde těžce vymazat, mají velkou životnost a jsou vhodné pro časté používání.

Čtečky magnetických karet

Jedná se o záznamové zařízení, které čte informace z magnetické karty. Při čtení z pásky přejíždí čtecí hlava po zmagnetizovaném povrchu a malý permanentní magnet umístěný ve čtecí hlavě je páskou přitahován nebo odtahován, čímž dochází k indukci kladného nebo záporného napětí.

Čtecí zařízení mohou číst až 3 stopy záznamu. Podle toho, kolik stop záznamu dané čtecí zařízení přečte, se rozdělují na:

- Jednostopé
- Dvoustopé
- Třístopé

Podle stopy, kterou zaznamenávají dělíme čtecí zařízení:

- Pro první stopu
- Pro druhou stopu
- Pro třetí stopu

Obr. 4 Čtečka magnetických karet [4]

Výhody magnetických karet:

- Vysoká životnost karet je 5-6 let.
- Spolehlivé uložení dat.
- Ekonomicky nenáročné.
- Dynamická paměť – schopnost přepisování záznamu.

Nevýhody magnetických karet:

- Možnost poškození dat při vystavení silnému magnetickému poli.
- Snadné zkopírování záznamu na kartě.
- Karta podléhá opotřebení používáním a vnějšími vlivy (koroze)[3,5].

1.2.2 Čipová média

Jsou to média v podobě karet nebo kapesních přívěšků, které obsahují integrovaný obvod. Integrovaný obvod zpracovává informace v digitální podobě. Obsahuje také paměť s větší paměťovou kapacitou a uložená data jsou chráněna bezpečnostní logikou.

Čipové karty jsou dvojího druhu a to:

- Paměťové karty, které obsahují energeticky nezávislou paměť.
- Mikroprocesorové karty, které obsahují energeticky závislou paměť a mikroprocesorové komponenty.[6]

Čipová média se rozdělují na:

- Kontaktní média
- Bezkontaktní média

1.2.2.1 Kontaktní média

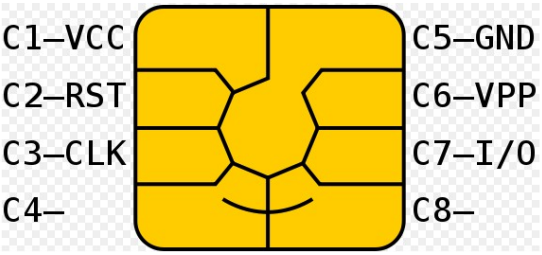
Tyto média obsahují kontaktní pole. Zapojením čipu do obvodu dojde k propojení kontaktního pole. Výhodou je, že může probíhat obousměrná komunikace, nevýhodou je omezená životnost mechanických částí čtečky. [3]

Čipové karty

Jedná se o plastové kapesní karty, které jsou vyrobeny z PVC(Polyvinylchlorid) nebo ABS (Akrylonitrilbutadienstyren). Na kartách je umístněn čip, který má kontaktní plochu o velikosti přibližně 1cm^2, složenou z osmi pozlacených kontaktních destiček. Tyto destičky poskytují elektrické propojení mezi kontakty čtečky a čipové karty. Díky tomuto propojení karta nepotřebuje vlastní elektrické napájení. Propojením kontaktů dojde ke komunikaci mezi čtecím zařízením a čipovou kartou.

Velikost karty udává standart ISO / IEC 7810 a definuje velikost na 85.60x53.98x0.76 mm.

Vlastnosti čipu udává standart ISO/IEC 781, který definuje: fyzický tvar a vlastnosti, pozici konektorů, jejich tvar, elektrickou charakteristiku, základní funkce a komunikační protokoly.



Obr. 5 Popis čipu. [5]

VCC – napájení čipu

RST – Reset, který se používá pro reset komunikací

CLK – poskytuje hodinový signál, ze kterého je odvozeno časování datové komunikace.

GND – Uzemnění

VPP – Vstup programovacího napětí

I/O – vstup nebo výstup pro sériová data

C4, C8 – dva volné kontakty, používané pro rozhraní USB, a další využití.[6]

Kontaktní čtecí zařízení čipových karet.

Čtecí zařízení se používá jako kontaktní médium při komunikaci s čipovou kartou. Může být propojené s počítačem nebo mobilním telefonem.

Obr. 6 Čtečka čipových karet .[6]

Kontaktní čipové přívěsky

Kontaktní čipové přívěšky jsou tvořeny kovovými čipy umístněnými v plastové klíčence. Přiložením kovové části ke snímací hlavě čtečky, dojde k vodivému spojení kovových částí (stačí velmi krátký kontakt cca 200 ms). Přiložením čipu na čtecí hlavu dojde k přečtení kódu a identifikaci nositele.

Kontaktní čipové přívěsky vynikají svou vysokou mechanickou odolností, díky čemuž se málo opotřebovávají. Jsou vhodné pro více činností např. docházku, otevírání dveří, výdej stravy, apod. Jsou velmi lehké a vhodné k připnutí ke klíčence.[7]

1.2.2.2 Bezkontaktní média

Bezkontaktní čipové médium je čipová karta, ve které je zabudovaný logický obvod s vnitřní pamětí a malou anténou. Komunikace mezi čtecím zařízením a bezkontaktním médiem se provádí prostřednictvím radiofrekvenční identifikace (RFID). Bezkontaktní čipové karty mají schopnost bezpečně řídit, ukládat a poskytovat přístup k datům na kartě. Mohou provádět šifrování, ověřování a komunikovat s bezkontaktním čtecím zařízením.

Bezkontaktní čipové médium obsahuje anténu vestavěnou do těla karty (přívěšku na klíče, hodinek, aj). Přiblížením karty do magnetického pole čtecího zařízení se čip v kartě zapne a je zahájen přenos dat mezi čtečkou a čipovým médiem.

Čtecí zařízení používají tyto frekvence:

Nízké frekvence (LF) – 125/134 kHz

Vysoké frekvence (HF) – 13,56 MHz

Ultravysoké frekvence (UHF) – 900 MHz

Bezkontaktní čipové technologie mohou být ve formách: plastové karty, hodinky, přívěsky na klíče, doklady, aj.[8]

1.2.3 Elektronické zámky

Jsou blokovací zařízení, která pro svou funkci potřebují elektrický proud. Mohou být jak samostatné s elektrickým ovládáním přímo na zámku, tak napojené na systém kontroly vstupu. Svou funkci elektronické zámky vykonávají pomocí magnetů, elektromagnetů nebo motorů.

1.2.3.1 Typy zámků

Magnetické zámky

Jsou tvořeny velkým elektromagnetem, který se skládá ze dvou částí. Jedna část je namontována na rámu dveří, druhá je na dveřích. Pokud je magnet napájen, jsou dveře uzamčené. Po odemknutí dveří se přeruší napájení a dveře se otevřou. Výhodou magnetických zámků je jejich jednoduchá instalace a mechanická pevnost.

Elektromotorické zámky

Obsahují vestavěný elektromotor, který se využívá pro odjištění nebo zajištění závory zámku. Zámek bývá propojený s externí ústřednou, která řídí jeho činnost.[9]

Elektromechanické zámky

Dveře se otevírají pomocí elektrického impulsu přivedeného na elektromagnetickou cívku, který zaaretuje (zajistí) pohyblivý mechanizmus v zámku a vnější klika je plně funkční pro otevření dveří.[10]

1.2.3.2 *Metody ověřování přístupu*

- Číselné kódy, hesla a přístupová hesla

  Nejrozšířenější forma elektronických zámků. Obsahují klávesnici pro zadávání číselných kódů. Pro odemknutí zámku musí uživatel zadat správné heslo na klávesnici (obvykle kombinace 4-6 čísel).

- Bezpečnostní žetony, karty

  K otevření dveří se používají bezpečnostní žetony, které se vhazují do zámku a karty, které se vkládají do zámku.

- Biometrické

  Moderní forma elektronických zámků představuje identifikaci uživatele pomocí biometrických charakteristik, nejčastěji se používají zámky se snímáním otisků prstů.

Obr. 7 Zámek na otisk prstu.[7]

- RFID

  Zahrnuje elektronické zámky s radiofrekvenční identifikací. K povolení vstupu je zapotřebí vlastnit autorizovaný RFID čip.[10]

1.2.4 Biometrická identifikace

Biometrická identifikace je identifikace, založená na biometrické charakteristice člověka, která je pro každého člověka jedinečná. Biometrické charakteristiky se rozdělují na:

Anatomicko-fyziologické

Identifikace je založena na základě vědeckých poznatků. Tyto biometrické rysy jsou unikátní a časově stálé. Zahrnuje otisky prstů, dlaní a chodidel, geometrii prstů a ruky, topografii žil zápěstí, oční duhovku, oční sítnici, tvář, stavbu vnějšího ucha, lidském

tělesném pachu, obsahu solí v lidském těle, rozměrech a vahách lidského těla a skladbě DNA (deoxyribonukleová kyselina) apod.

Behaviorální

Tato identifikace je založena na seriózních poznatcích o lidském hlase, pohybu těla, o znalostech a dovednostech psaní (psaní souvislého textu, podpis osoby, psaní na klávesnici). Behaviorální charakteristiky jsou unikátní a časově nestálé.[11]

Biometrická identifikace zahrnuje tyto úkony:

- **Rekognice (rozpoznávání)** – rozpoznání člověka podle použití vhodné tělesné vlastnosti.
- **Verifikace (ověření)** – je proces porovnání totožnosti jedince biometrickým systémem, který porovnává sejmutý vzorek jedince se vzorkem již zapsaným.
- **Identifikace** – je proces identifikace neznámého jedince, kdy biometrický systém porovnává sejmutý vzorek se všemi vzorky v databázi.
- **Autentifikace (autentizace)** – tento pojem lze sloučit s termínem rozpoznání, kdy na konci procesu uživatel získá určitý status, např. oprávněný, neoprávněný atd.[12]

U biometrických systémů se sledují tyto charakteristiky:

Univerzálnost (universality) – každá osoba vlastní biometrickou charakteristiku.

Jedinečnost (uniqueness) – neexistují dvě osoby, které by měly stejné biometrické charakteristiky.

Permanence (permanence) – biometrické charakteristiky se nemění s časem.

Jednoduchost (simplicity) – biometrické charakteristiky jsou jednoduché, přesné a kvantitativně měřitelné.

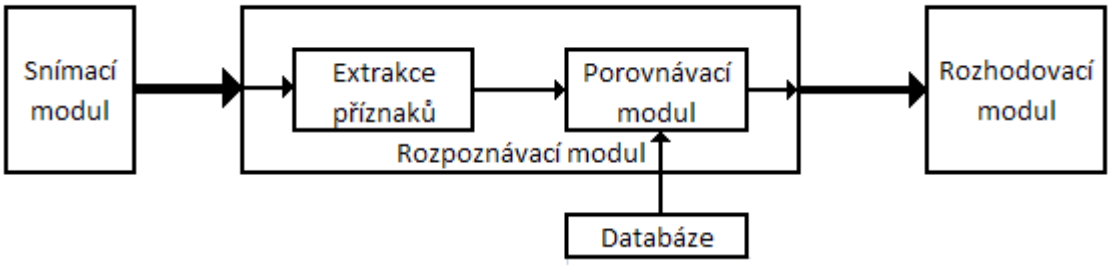
Přijatelnost (acceptability) – snímání biometrických charakteristik je nenáročné.[3]

U biometrických systémů nelze zajistit 100% shody při porovnávání vzorků a musí se počítat s odchylkami. Tyto odchylky vyjadřují přesnost dané biometrické metody:

False rejection rate (FRR) – popisuje, kolik osob bylo odmítnuto identifikačním přístrojem, ačkoli odmítnuti být neměli. Jedná se o chybu přístroje a udává pravděpodobnost, s jakou bude oprávněná osoba odmítnuta.

False acceptance rate (FAR) – popisuje, kolik osob bylo přijato identifikačním přístrojem, ačkoli přijati být neměli. Tato chyba přístroje vyjadřuje pravděpodobnost, s jakou bude neoprávněná osoba přijata. [1]

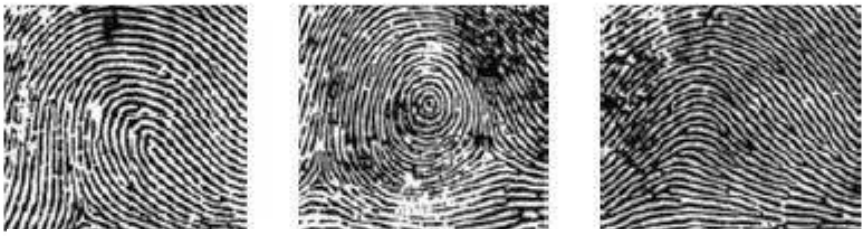
Biometrický systém se skládá z několika logických bloků, první blok tvoří snímací modul, který získává biometrické data osob. Druhý blok tvoří rozpoznávací modul, který v sobě zahrnuje modul pro extrakci příznaku a porovnávací modul. Modul extrakce příznaků zpracovává jen část nasnímaných informací (tzv. příznaky) a provádí matematické operace, díky kterým se realizuje identifikace osoby. Porovnávací modul dále zpracovává příznaky a porovnává je s daty uloženými v databázi. Poslední blok tvoří rozhodovací modul, který provádí závěrečné rozhodnutí, v závislosti jsou-li snímané údaje shodné s údaji v databázi.



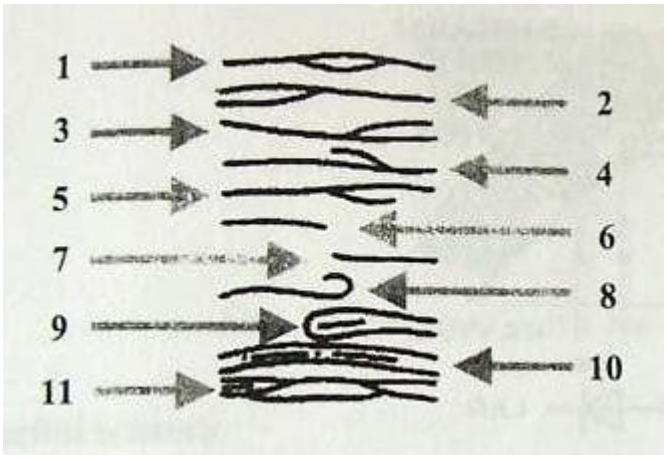
Obr. 8 Princip činnosti biometrického systému [8]

1.2.4.1 Otisk prstu

Otisk prstu je historicky nejstarším vyhodnocovacím biometrickým systémem a v dnešní době také nejvíce rozšířeným. Patří do skupiny daktyloskopických identifikací. Přičemž daktyloskopie představuje nauku o obrazech papilárních linií na vnitřních stranách prstů, dlaní člověka a chodidlech lidských jedinců. Na vnitřních stranách prstů se nacházejí papilární linie, které mají různé tvary. Ty jsou definovány ve třech základních skupinách tzv. klasifikačních vzorech. Jedná se o smyčku, vír a oblouk. Smyčka zaujímá 60 až 70 % všech otisků prstů, vír 25 až 35 % a oblouk pouze 5 % otisků prstů. K identifikaci to však nestačí a k rozeznávání otisků se využívají ještě charakteristické znaky. Ty tvoří např. oko, vidlice, hák, vložená linie.[3,13]



Obr. 9 Základní klasifikační vzory. Zleva: smyčka, vír, oblouk [9]

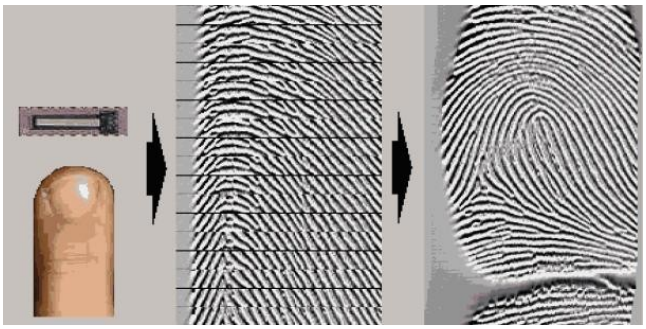


Obr. 10 Charakteristické znaky papilárních linií [10]

Popis obrázku 10 : 1. Oko, 2. Vidlice, 3. Protividlice, 4. Hák, 5. Protihák, 6. Končící linie, 7. Začínající linie, 8. Nedokončená smyčka, 9. Vložená linie, 10. Přerušovaná linie, 11. Ostrov a spojená vidlice.

Existují tři metody zachycení otisku prstu:

- **Otisk získaný pomocí inkoustu a papíru** – metoda používající se ve forenzní sféře. Prst se namočí do inkoustu a poté se s ním roluje na papíře, aby se získal co nejkvalitnější otisk prstu.
- **Statické snímání –** je nejběžnější metodou zachycení otisku prstu. Uživatel přitiskne prst na snímací senzor, který sejme celý otisk.
- **Snímání šablonováním** – V této metodě uživatel přejíždí prstem po senzoru, který snímá a opětovně skládá obraz pomocí pásů.



Obr. 11 Snímání šablonováním [11]

Snímače otisků prstů.

U snímání otisků prstů se používá mnoho technologických postupů a stále se vyvíjejí nové. Zde je přehled současných metod snímání otisků prstů:

- Optické snímače - na základě odrazu (reflexní), reflexní se skládáním obrazu, bezdotykový odraz, transmisní.
- Elektroluminiscenční snímače.
- Kapacitní snímače - křemíkové čipy a kapacitní snímač, kapacitní snímač a TFT, TFT optické.
- Tlakové snímače - vodivá membrána na silikonu, vodivá membrána na TFT, dotekové mikro-elektromechanické spínače.
- Rádiové snímače.
- Teplotní senzory.
- Ultrazvukové snímače.
- Fotonové krystaly.
- Snímače povrchové impedance.[12]

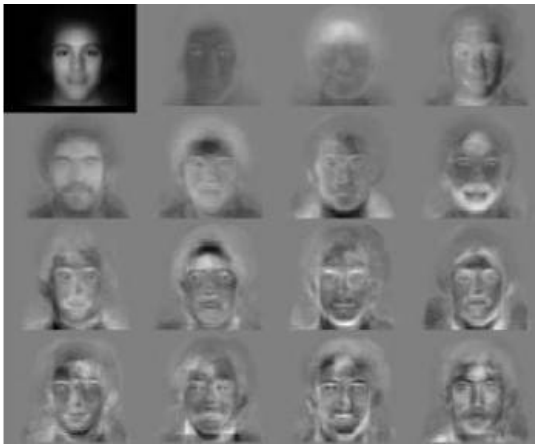
Obr. 12 Snímač otisku prstu [12]

1.2.4.2 Geometrie tváře

Identifikace osoby podle obličeje je nejvíce zkoumanou metodou. Rozpoznání obličeje je založené na srovnávání obrazu sejmutého kamerou s obrazem, který je uložen v centrální databázi. K identifikaci osoby slouží tvar obličeje a poloha opticky významných míst na tváři, jako jsou oči, nos, ústa, obočí, atd.

Mezi nejlepší algoritmy rozpoznání tváře patří:

- Analýza hlavních částí (PCA – Principal components analysis) – využívá vektorů tváře. Každá tvář se rozdělí na vzory tváří s rozdílnou maticí jasových úrovní a poté se opět složí.

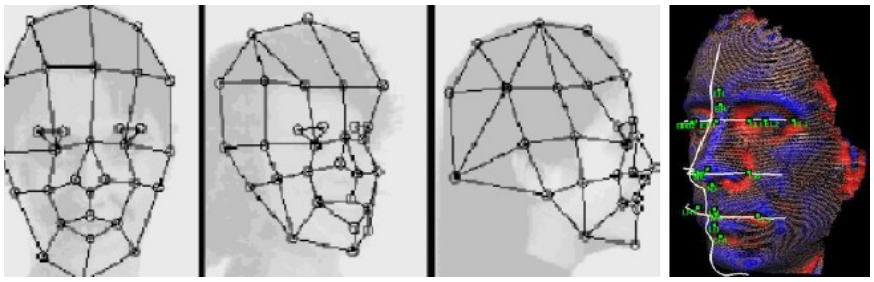


Obr. 13 PCA – rozložení obrazu [13]

- Lineární diskriminační analýza (LDA – Linear diskriminant analysis) – Jedná se o metodu, která třídí pořízené obrazy tváří do skupin za cílem maximalizování rozdílů mezi jednotlivými skupinami a minimalizování rozdílů v každé skupině, kde každý blok reprezentuje jednu třídu.

Obr. 14 Příklad šesti tříd užitím LDA [14]

- Elastický srovnávací diagram (EBGM – Elastic bunch graph matching) – tato metoda definuje na obličeji uzlové body, které se propojí a tím definují linie tváře v prostoru. Vznikne tak souřadnicová síť obličeje.



Obr. 15 Souřadnicová síť obličeje [15]

Identifikace osob podle geometrie tváře je v dnešním světě moderní. Používá se především na letištích, nádražích, rušných ulicích a všude tam, kde by se mohly pohybovat pohřešované a hledané osoby.[12]

1.2.4.3 Oko – duhovka

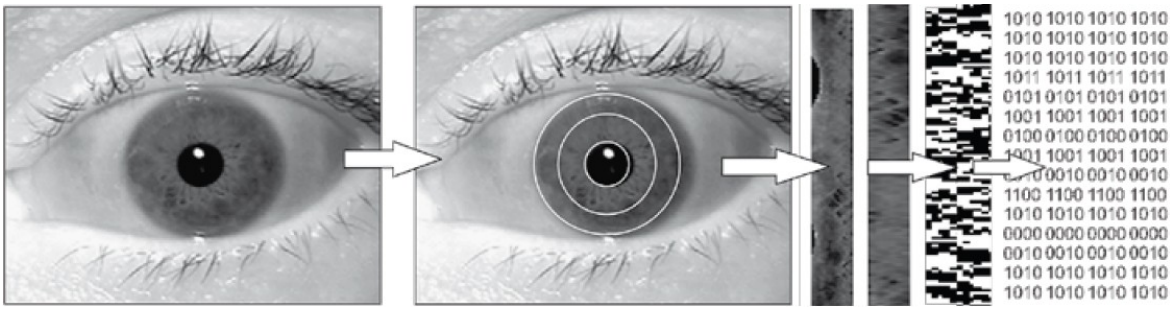
Tato metoda je nejpřesnější identifikační biometrickou metodou. Duhovka je barevná část oka. I když zbarvení a struktura duhovky je geneticky daná, její vzorkování nikoli. Vzorkování duhovky je naprosto jedinečné a člověk má u každé duhovky různé vzorkování.

Lidská duhovka obsahuje enormní množství informací a počet charakteristických vzorků dosahuje 400 (pro srovnání otisk prstu má zhruba 60 – 70 charakteristických vzorků).

Snímání duhovky

U snímání duhovky je zapotřebí velice kvalitní digitální kamery a infračervené osvětlení oka. Při snímání se duhovka mapuje do fázorových diagramů, ty obsahují informaci o orientaci, četnosti a pozici speciálních plošek. Poté se vytvoří duhová mapa a šablona pro identifikaci.

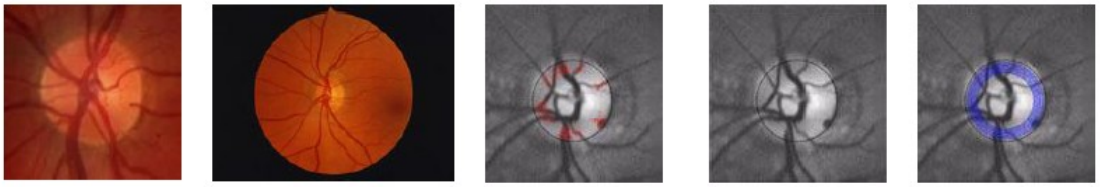
Výhodou snímání duhovky je nejenom přesnost identifikace, ale i uživatelsky přívětivé snímání oční duhovky, a to až ze vzdálenosti 1 metru. Také dokáže velmi rychle prohledávat databázi očních duhovek, a to rychlostí 10^6 datových snímků za sekundu. Mezi nevýhody patří nutnost polohování oka pro snímání a převážně cena.[12,14]



Obr. 16 Princip snímání oční duhovky [16]

1.2.4.4 Oko – sítnice

Při skenování oční sítnice se používají koherentní infračervené světelné zdroje. Jelikož je infračervená energie pohlcována cévami sítnice rychleji, nežli v okolních tkanivech, jsou cévy ve výsledném obrazu tmavší. Následný obraz oka je analyzován a porovnán s databází. Tato metoda není příliš uživatelsky přívětivá, jelikož je zapotřebí oproti snímání duhovky zásah uživatele.[3]



Obr. 17 Ukázka lokalizace sítnice a znázornění charakteristických parametrů [17]

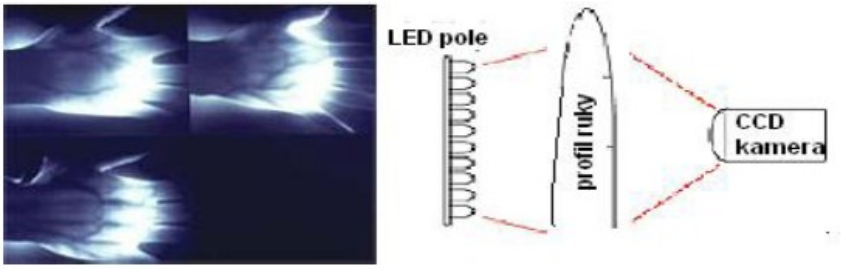
1.2.4.5 Geometrie ruky

Tato metoda je založená na specifickém tvaru ruky každého člověka, který se od určitého věku nemění. Při snímání se porovnává výška, šířka a délka prstů. Výhodou této metody je její rychlost porovnávání výsledků, nevýhodou je přesnost.[3]

Obr. 18 Snímač geometrie ruky [18]

1.2.4.6 Struktura žil na zápěstí

Biometrická metoda, která je založená na snímání hřbetu ruky pomocí speciální infračervené kamery. Snímání probíhá tak, že hřbet ruky se prosvítí zdroj a na základě různé absorpce záření krevních cév a ostatních tkání se pomocí snímání CCD kamery vytvoří obraz. Ten se nadále zpracovává a vyextrahuje se z něj síť cév, která se následně porovná s databází. Výhodou této metody je bezkontaktní princip a nemožnost jakéhokoliv napodobení sítě cév.[12]



Obr. 19 Obraz světelné prostupnosti ruky a ukázka principu snímání [19]

Další biometrické metody například:

- Psaní na klávesnici
- Dynamika podpisu
- Dynamika chůze
- Akustická charakteristika hlasu
- Verifikace a identifikace podle pachu
- Verifikace podle DNA
- Biometrické pole
- Spektroskopie kůže

1.3 Poplachové systémy – Systémy kontroly vstupů pro použití v bezpečnostních aplikacích. (ČSN EN 50133)

České technické normy jsou obecné pravidla, směrnice nebo charakteristiky činností, které stanovují kritéria bezpečnosti, chrání spotřebitele i výrobce, chrání životní prostředí a představují tzv. „společnou řeč obchodu“.

Problematiku ACS řeší řada norem ČSN EN 50133. Doposud byly vydány následující části:

- Část 1: Systémové požadavky. Rok vydání: 2001.
- Část 2-1: Všeobecné požadavky na komponenty. Rok vydání: 2001.
- Část 7: Pokyny pro aplikace. Rok vydání: 2000.

1.3.1 Systémové požadavky (ČSN EN 50133-1)

Tato norma obsahuje popis všeobecných požadavků na funkčnosti systému kontroly vstupu pro použití v zabezpečovacích systémech. Dále popisuje všeobecné požadavky na komponenty z hlediska prostředí. Zabývá se zabezpečovacími aplikacemi pro každé přístupové místo, kde se systém kontroly vstupů může skládat z libovolného počtu přístupových míst. Dále definuje třídy rozpoznání a systémy kontroly vstupů, které mají nebo nemají záznam času.

Norma obsahuje definice, které slouží k lepšímu pochopení dané problematiky, zjednodušení popisu a vysvětlení pojmů.

Všeobecné požadavky

U systémů kontroly vstupu se zabezpečení skládá z klasifikace přístupu a klasifikace identifikace.

Tab. 1 Klasifikace přístupu [1]

Třída přístupu A	Nevyžaduje pro místo přístupu časový filtr ani uložení dat o přístupových transakcí.
Třída přístupu B	Vyžaduje pro místo přístupu časový filtr a uložení dat o přístupových transakcí, dále zahrnuje podtřídu B, která se vztahuje na místo přístupu zahrnující časové filtry, ale bez funkcí ukládání dat.

Tab. 2 Klasifikace identifikace [2]

Třída identifikace 0	žádná přímá identifikace	přístup bez potřeby identity uživatele
Třída identifikace 1	informace uložená v paměti	hesla, pin kódy, osobních identifikačních čísel
Třída identifikace 2	identifikační prvky nebo biometrie	Skládá se z identifikačních prvků, karet, otisků prstů, hlasu
Třída identifikace 3	identifikační prvky nebo biometrie spolu s informací uloženou v paměti	Skládá se z kombinace biometrického prvku, identifikačního prvku a informace uložené v paměti

Společné funkční požadavky pro třídy přístupu A a B

V této části norma definuje časový filtr, počet nesprávně zadaných hesel do zablokování systému a čas, po který budou moci být znovu zadávána u různých tříd identifikace. Dále obsahuje ochranu programovatelnosti, kde uvádí počet různých kombinací kódů k počtu

oprávněných osob, minimální počet kombinací a správce musí mít možnost změnit přístupový kód. Také jsou v normě pokyny pro ovládání míst přístupu, kde popisuje ovládání apas a monitorování stavu zabezpečení apas. Norma definuje počet kombinací kódů, četnost chybných povolení a chybných odmítnutí pro různé třídy identifikace. Dále musí mít systém kontroly vstupů prostředky pro hlášení ve formě výstrahy, zobrazení detekce sabotáže, aj. Také obsahuje požadavky pro komunikaci systému kontroly vstupů s ostatními systémy.

Doplňkové funkční požadavky pro třídu přístupu B

Rozdělení této části normy je shodné se společnými funkčními požadavky pro třídy přístupu A a B, přičemž obsahuje doplňující požadavky pro třídu přístupu B.

Požadavky na komponenty kontroly vstupů

Tato část normy se zabývá požadavky na zkoušky vlivu prostředí pro komponenty kontroly vstupů. Zkoušky se provádějí při standardních atmosférických podmínkách a při jmenovitém napájecím napětí konektoru.

Atmosférické podmínky:

Teplota: 15°C až 35°C

Relativní vlhkost: 25% až 75%

Tlak vzduchu: 86 kPa až 106 kPa

Při zkouškách se používají stupně přísnosti, které jsou definovány takto:

Tab. 3 Stupně přísnosti [3]

I Vnitřní	omezené na obytné/kancelářské prostředí (např. obytné pokoje a kancelářské místnosti).
II Vnitřní všeobecně	např. prodejny, obchody restaurace, schodiště, výrobní a montážní haly, vestibuly a skladové prostory
III Vnější	chráněné proti přímému dešti a slunečnímu záření nebo vnitřní s extrémními podmínkami okolního prostředí (např. garáže, půdy, stodoly a nákladové prostory)
IV Vnější	všeobecně

V každé zkoušce norma definuje účel zkoušky, její princip a postup, jakým se má daný komponent kontroly vstupu zkoušet.

Zkoušky se provádí pro prostředí:

- Suché teplo (provozní)
- Chlad (provozní)
- Vnik vody (provozní)
- Ráz (provozní)
- Vibrace, sinusové (odolnostní)
- Změny síťového napájecího napětí (provozní)
- Poklesy a krátkodobá přerušení síťového napájecího napětí (provozní)

Požadavky EMC

Zde norma uvádí požadavky na EMC.

Zkušební metody pro funkční požadavky

V této části norma definuje požadavky a postupy pro zkoušení komponentů systému kontroly vstupu.

Značení a identifikace

Důležité je označení všech komponentů systému kontroly vstupů, přičemž toto označení musí být snadno čitelné, pevně uchycené a trvanlivé.[15]

1.3.2 Všeobecné požadavky na komponenty (ČSN EN 50133-2-1)

Tato norma odkazuje na certifikaci výrobků patřících do systému kontroly vstupů a vypracovaná v souladu s EN 50133-1. Obsahuje doplňující informace k části všeobecné požadavky. Dále jsou v normě uvedeny požadavky na:

napájení – vstupy a výstupy napájení každého komponentu systému kontroly vstupů musí být chráněny proti zkratu.

kryty – norma obsahuje pokyny pro otevření, nastavení, kabelové průchodky, dokumentaci a značení/identifikaci.

Norma definuje specifické zvláštní požadavky pro:

Rozhraní místa přístupu – musí splňovat alespoň IP 3X podle EN 60529

V závislosti na třídě prostředí:

- Třída prostředí I, II IP 30;
- Třída prostředí III IP 32;
- Třída prostředí IV IP 34;

Identifikační zařízení – musí splňovat alespoň IP 3X podle EN 60529

V závislosti na třídě prostředí:

- Třída prostředí I, II IP 30;
- Třída prostředí III IP 32;
- Třída prostředí IV IP 34;

V závislosti na třídě prostředí, kde kryty identifikačního zařízení musí splňovat alespoň následující hodnoty IK podle EN 50102:

- Třída prostředí I, II, III IK 04;
- Třída prostředí IV IK 06;

Zkoušky

V této části norma uvádí doplňující informace pro:

- kontrolu dokumentace, kontrolu a funkční zkoušky
- zkoušky vlivu prostředí[16]

1.3.3 Pokyny pro aplikace (ČSN EN 50133-7)

Tato norma obsahuje pokyny k použití automatizovaných systémů kontroly vstupů a komponentů uvnitř a vně budov. Pokyny zahrnují návrh systému, instalaci, předávání, provoz a údržbu systémů kontroly vstupů. Jsou určeny pro systém kontroly vstupů a zahrnují oblasti od jednoduchých systémů pro řízení jednoho přístupového místa až po složité systémy s mnohonásobnými přístupovými místy.

Norma všeobecně definuje systém kontroly vstupů a zahrnuje všechny konstrukční a organizační náležitosti společně se zařízením požadovaným k ovládání vstupů.

Posláním systému kontroly vstupů je:

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

b) minimalizovat riziko nepovoleného vstupu

Zavedení systému kontroly vstupů se řídí následujícím pořadím:

a) projekt (návrh) systému

b) instalace systému

c) předání systému

d) provoz systému

e) údržba systému

Proces realizace se řídí národními předpisy. Prováděcí návrh schvaluje kupující.

Návrh systému

Návrh systému se skládá z:

konzultace:

- kde požadavky na návrh systému se konzultují mezi kupujícím a jinými zainteresovanými stranami.

rozvahy:

- pro každé přístupové místo – obsahuje výčet rizik získaných analýzou rizik a informací od zákazníků
- pro systém s více místy přístupu – obsahuje doplňující rizika pro systém s více místy přístupu
- doplňující údaje – obsahuje další rizika v návaznosti na výše uvedené.

Instalace systému

V této části norma uvádí pokyny pro instalaci zařízení, napájecího zdroje, kabeláže a provedení revize.

Předávání

Předmětem předávání je převedení odpovědnosti z projektové a instalační firmy na nakupujícího.

Provoz

Dále norma uvádí odpovědnost správce při provozu a ovládání systému kontroly vstupu.

Údržba

Pro správnou funkci systémů je zapotřebí provádět v dohodnutých intervalech údržbu, prověrku, prohlídku a servis.

Dokumentace

V poslední části se norma zabývá dokumentací, která je nezbytná pro instalaci, provoz, schvalování, údržbu systému kontroly vstupu a je přizpůsobena rozsahu a složitosti instalovaného systému.[17]

Dílčí závěr

Kapitola se zabývá popisem významu, struktury a použití systému kontroly vstupu a technickými požadavky. K autentifikaci uživatele slouží velké množství identifikačních metod, v komerční sféře jsou však omezeny cenou. Nejoblíbenější jsou bezkontaktní čipové tokeny, pro své jednoduché ovládání, cenu a univerzálnost. Co se týče bezpečnosti, patří mezi nejpřesnější a nejbezpečnější identifikace biometrické systémy, a to identifikace oční duhovky nebo sítnice. Neustále se také zdokonaluje metoda rozpoznání obličeje, zejména na letištích, kde je velká frekvence pohybu osob. Kamery jsou schopné rychle rozpoznat hledané a pohřešované osoby. Výrobci přístupových systémů by však měli využívat pokynů Českých státních norem, které popisují a definují charakteristiky a kritéria bezpečnosti přístupových systémů, aby jejich výrobky byly srozumitelné, bezpečné, chránily jak výrobce, tak i spotřebitele.

2 INTEGROVANÉ POPLACHOVÉ SYSTÉMY

Integrovaný poplachový systém představuje systém mající jedno nebo více společných zařízení, kde alespoň jedním z nich je poplachová aplikace. Je to systém, který umožňuje propojení elektronických zabezpečovacích systémů, elektronických požárních signalizací, systémů kontroly vstupu, kamerových systémů a technologických procesů budov. Příkladem takové integrace může být propojení přístupového systému s docházkovým systémem, kdy nejenom zajistíme, aby nám do objektu nevstoupila nepovolená osoba, ale zároveň budeme vědět čas příchodu a čas odchodu zaměstnance.

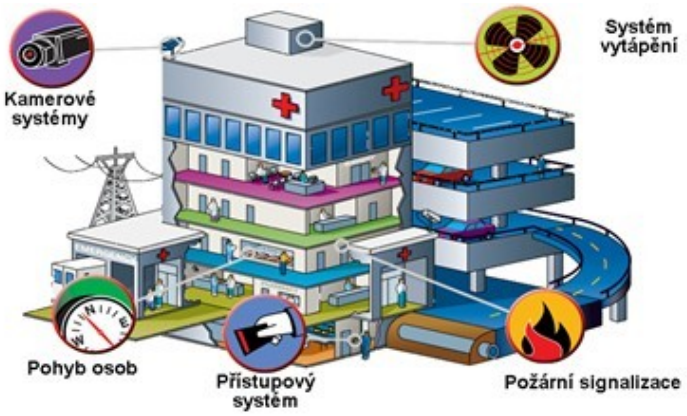
Poplachový systém – je systém, který je určený na ochranu života, majetku nebo prostředí. Mezi poplachové systémy patří:

- systém kontroly vstupu (ACS)
- zabezpečovací aplikace (EZS), PZS ,IAS
- tísňové systémy IAS (PTS)
- SAS – Systémy přivolání pomoci
- CCTV
- EPS

Přičemž CCTV a ACS můžeme v určitých případech považovat za poplachový systém a naopak. V případě ACS např. při detekci požáru se odblokují dveře. Nebo v případě CCTV se jedná o poplachovou aplikaci pokud umožňuje automatickou detekci pohybu v obraze.

Nepoplachový systém – je tvořen systémy určenými k ovládání a jejich primární funkcí není ochrana života, majetku nebo prostředí. Nepoplachové systémy tvoří např:

- topení a větrání (ventilace),
- správa energetiky,
- správa budovy,
- osvětlení,
- zavlažování,
- řízení výtahů [18],



Obr. 20 Integrované systémy v budově [20]

Systémy kontroly vstupu představují především poplachové systémy, vhodným příkladem je integrace přístupových systémů s elektrickou požární signalizací. V případě požáru EPS předá informaci přístupovým systémům a ty pak odblokují zámky na dveřích. Avšak mohou být systémy kontroly vstupu chápány také jako nepoplachové aplikace, a to především při integraci se systémy řízení technologických procesů budov. Kde například po přiložení přístupové karty zaměstnance předá přístupový systém infromaci ke spuštění topení, větrání v budově, místnosti.

2.1 Způsoby integrace poplachových systémů

Integrovat poplachové systémy můžeme dvěma způsoby a to hardwarově nebo softwarově, přičemž každý má své výhody a nevýhody. Při integrování je nejdůležitější komunikace mezi jednotlivými zařízeními. Ta je prováděna pomocí komunikačních protokolů, jako jsou: EIB/KNX, Modbus, EcheLON, Mbus, BACnet, OPC a SNMP.

Obr. 21 Komunikační protokoly [21]

Propojení protokolů je možné provést dvěma způsoby:

- **Pomocí adaptérů nebo výsuvných karet** – k integraci systémů je zapotřebí připojení zásuvných karet (obsahující převodníky) nebo adaptérů k řídícímu PC. Řídící PC pak obsahuje systém zprávy budov, jehož součástí jsou příslušné ovladače. Vytváří tak grafickou vizualizaci nad integrovanými technologiemi.
- **Pomocí regulátoru –** Regulátor obsahuje fyzické vstupy a výstupy (převodníky a adaptéry jsou součástí systému), zajišťuje integraci připojených technologií, které využívají různé komunikační protokoly. V podstatě nahrazuje PC, kde umožňuje vytváření řídící logiky a grafické vizualizace celého systému. Dané regulátory mohou obsahovat konektory pro připojení LAN (TCP/IP a BACnet) a konektory pro připojení sériové linky RS232 a RS485.[19]

Obr. 22 Propojení komunikačních protokolů [22]

2.1.1 Hardwarová integrace

U hardwarové integrace jde především o multisystém, kde je kombinováno několik bezpečnostních systémů od jednoho výrobce. V tomto případě mají bezpečnostní systémy předem vyřešenou komunikaci, systém propojení a programování jednotlivých aplikací. Toto je hlavní výhoda hardwarové integrace. Nevýhodou však je, že takový systém může být složen jen z výrobků jedné firmy, aby byl kompatibilní a fungoval správně. Tady však může nastat problém, protože některý výrobek od výrobce nesplňuje námi požadované vlastnosti a my bychom chtěli k integraci použít jiný výrobek od jiné firmy. V tomto případě se můžeme dostat do potíží, protože systémy nemusí být kompatibilní a taky výrobce není ochoten integrovat cizí výrobek.

Příkladem pro hardwarovou integraci je systém Johnson Controls Cardkey P2000

Představuje modulární systém, který používá komunikační protokol BACnet pro integraci systémů řízení vstupu. Systém je vhodný pro střední a velké aplikace s vysokými nároky na bezpečnost. Jedná se především o systém zaměřený na přístupové systémy a volitelnou integraci CCTV a DVR (Digital Video Recorder).[20]

Obr. 23 Cardkey P2000 [23]

2.1.2 Softwarová integrace

Softwarová integrace nám umožňuje propojení více druhů výrobků od různých výrobců. Výhodou softwarové integrace je, že si můžeme vybrat bezpečnostní systémy, které nejlépe splňují naše požadavky. Nevýhodou je komunikace mezi jednotlivými systémy, která se provádí pomocí softwarových převodníků. Softwarové převodníky jsou vlastně systémové utility, které jsou nainstalované na komunikačních serverech a zajišťují přenos dat mezi jednotlivými aplikacemi. K provedení softwarové integrace tedy potřebujeme znát komunikační protokoly jednotlivých bezpečnostních systémů. Tady však nastává problém, že někteří výrobci nechtějí poskytnout komunikační protokoly. Důvod proč tak činí je konkurenční boj, kdy chtějí, aby byly integrovány jen jejich výrobky. Dalším problémem mohou být také softwarové převodníky, které mohou vykazovat chybovost kvůli špatným algoritmům.[21]

Příkladem pro softwarovou intergraci je program ALViS

Program ALViS představuje grafický systém pro integraci, řízení a monitorování technologických zařízení budov. Podporuje připojení přístupových systémů, poplachových systémů, systémů požární ochrany, obvodové ochrany, video ochrany, měření a regulace výtahů, ventilací, osvětlení, aj. Tento program umožňuje zapojení výrobků od různých výrobců, které mají podporu pro univerzální komunikační protokoly (OPC, Modbus, Espa, DDE, Ascii), nebo obsahují ovladače zařízení pro systém ALViS. Jedná se o modulární systém s možností kombinování architektury klient/server resp. WEB server. [22]

2.2 Kombinované a integrované systémy

Problematiku integrovaných systémů upravuje norma ČSN CLC/TS 50398. Tato norma uvádí všeobecné požadavky a typy struktur kombinovaných a integrovaných poplachových systémů. Norma zajišťuje integraci jedné nebo více aplikací do jednoho integrovaného systému. Dále norma poskytuje informace týkající se prvotního návrhu (projektu) systému, plánování, instalace, předávání, provozu a údržby (servisu) kombinovaného a integrovaného systému. Specifikuje požadavky na poplachové systémy, které jsou kombinovány nebo integrovány s jinými systémy, které mohou a nemusí být poplachovými systémy. Také definuje požadavky týkající se pravidel integrace s cílem zdůraznit význam jednotlivých aplikačních poplachových norem a objasnit případné rozpory.[23]

Všeobecný popis a základní principy

Integrování poplachových systémů lze rozdělit dle jejich konfigurace na typy:

- Typ 1 aplikovatelný pro kombinaci a integraci jednoúčelových poplachových systémů a jednoúčelových nepoplachových systémů.
- Typ 2A aplikovatelný pro kombinaci a integraci poplachových systémů a nepoplachových systémů, používajících společné přenosové trasy, společná zařízení a společné vybavení. Porucha v kterékoli části nemá žádný negativní účinek na jakoukoli další poplachovou aplikaci. K dosažení tohoto stavu je potřebné znásobení (nadbytečnost).

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

Pro každou aplikaci systému u integrovaných poplachových systémů musí být použity příslušné normy a společné zařízení musí vyhovovat všem aplikačním normám, jejichž splnění je vyžadováno.

Typy konfigurace integrovaných poplachových systémů

V této části norma obsahuje příklady konfigurace integrovaných poplachových systémů

Typ 1 – Konfigurace je kombinací dvou nebo více jednoúčelových systémů a tyto jednoúčelové systémy jsou připojeny ke společnému doplňkovému zařízení. Přičemž zařízení nesmí být nepříznivě ovlivněno jakýmkoli dalším jednoúčelovým systémem nebo doplňkovým zařízením.

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

Systémové požadavky a stanovení kompatibility:

- Obecný návrh (projekt) – Zde norma definuje, jak má být integrovaný poplachový systém navržen a realizován. V normě jsou také popsány speciální požadavky návrhu (projektu) pro konfigurace typu 1 a 2.
- Společné ovládací zařízení – manuální ovládání musí být jasné a jednoznačné.
- Společné signalizační zařízení – Tato část normy se zabývá signalizačními zařízeními a uvádí, jak mají být signalizační zařízení používána (jako doplňkové zařízení nebo normou vyžadované). Specifikuje signalizaci informace a priority, u kterých musí být informace signalizovány v pořadí priorit jasným a jednoznačným způsobem.
- Integrita normou požadovaných prvků pro zpracování poplachů – Tato část se zabývá monitorovacím programem a softwarem pro společné vyhodnocovací prvky.

- Připojení k poplachovému přenosovému systému – norma zde určuje, jaké normy musí splňovat poplachový přenosový systém, ke kterému jsou připojeny poplachové systémy a uvádí, že může být použit k přenosu několika druhů poplachů a dalších informací.
- Propojení – Dále definuje požadavky pro připojení zařízení, které nesplňuje jednu, nebo více aplikačních norem připojeném na zařízení splňujícím požadavky norem.
- Napájecí zdroje – požadavky pro speciální, nebo společná zařízení.
- Požadavky na načasování – pro každou aplikaci musí být splněny všechny požadavky načasování, specifikované ve všech příslušných normách.
- Současný výskyt událostí – nesmí ohrozit integritu žádné z aplikací.
- Prověření provozuschopnosti – prověření provozuschopnosti integrovaného systému musí být v souladu s příslušnými normami, použitými pro příslušnou aplikaci.
- Centrální ovládací zařízení (CCF) – V této části norma definuje použití a požadavky pro centrální ovládací zařízení.

Dokumentace a školení

Norma zde uvádí požadavky na dokumentaci kombinovaného a integrovaného poplachového systému.[18]

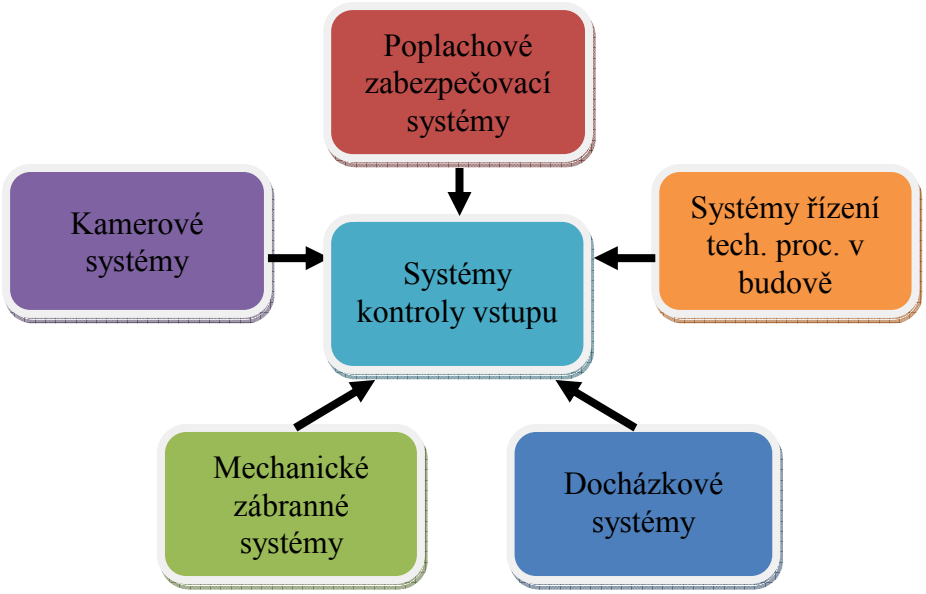
Dílčí závěr

Kapitola se zabývá popisem integrovaných poplachových systémů a technickými požadavky. Integrované poplachové systémy tvoří nedílnou součást ochrany majetku a zabezpečení objektu. Firmy, které se zabývají vývojem a výrobou bezpečnostních komponentů si uvědomují, že budoucnost v bezpečnostní sféře se bude ubírat cestou integrace jednotlivých komponentů, proto se snaží vytvářet systémy tak, aby se daly kombinovat navzájem a aby dokázaly mezi sebou komunikovat. Bohužel kvůli konkurenčním bojům mezi jednotlivými výrobci nedochází k sjednocení kompatibility všech systémů. Naštěstí se integrace výrobků od jednotlivých výrobců dá řešit buď softwarovým programem, nebo hardwarovým regulátorem. K podpoře fungování integrovaných systémů byla vydána norma CLC/TS50398, která obsahuje všeobecné požadavky a typy struktur kombinovaných a integrovaných poplachových systémů.

II. PRAKTICKÁ ČÁST

3 MOŽNOSTI INTEGRACE SYSTÉMŮ KONTROLY VSTUPU

Přístupové systémy kontroly vstupu je možné kombinovat s různými systémy, jako jsou PZS, CCTV, MZS, docházkový systém a systémy řízení technologických procesů budov. Integrace se provádí buď softwarově, především speciálním programem, který umožňuje komunikaci mezi dvěma různými systémy. Druhou možností je hardwarově, kde je integrace provedena hlavně přes ústřednu PZS, která podporuje dané systémy.



Obr. 24 Možnosti integrace ACS s jinými systémy

3.1 Integrace systému kontroly vstupu s poplachovými zabezpečovacími systémy

Mezi nejvýznamnější možnosti integrace přístupových systémů je integrace s poplachovými zabezpečovacími systémy, které zajišťují bezpečí osob a majetku. Umožňuje poplachovým aplikacím odblokovat vstupy při požáru nebo při jiných nestandardních situacích. Také odblokuje střežení místnosti při vstupu osoby do objektu a naopak zapne střežení při odchodu osoby. Také v situacích, kdy zjistíme pomocí PZS narušení objektu neznámou osobou může integrovaný systém například uzavřít dveře a zabránit tak narušiteli v úniku.

Výhody:

- Vyšší míra zabezpečení
- Při požárech odblokování zámků u dveří
- Odstřežení místnosti při vstupu, zastřežení při odchodu
- Minimalizování poruchových stavů

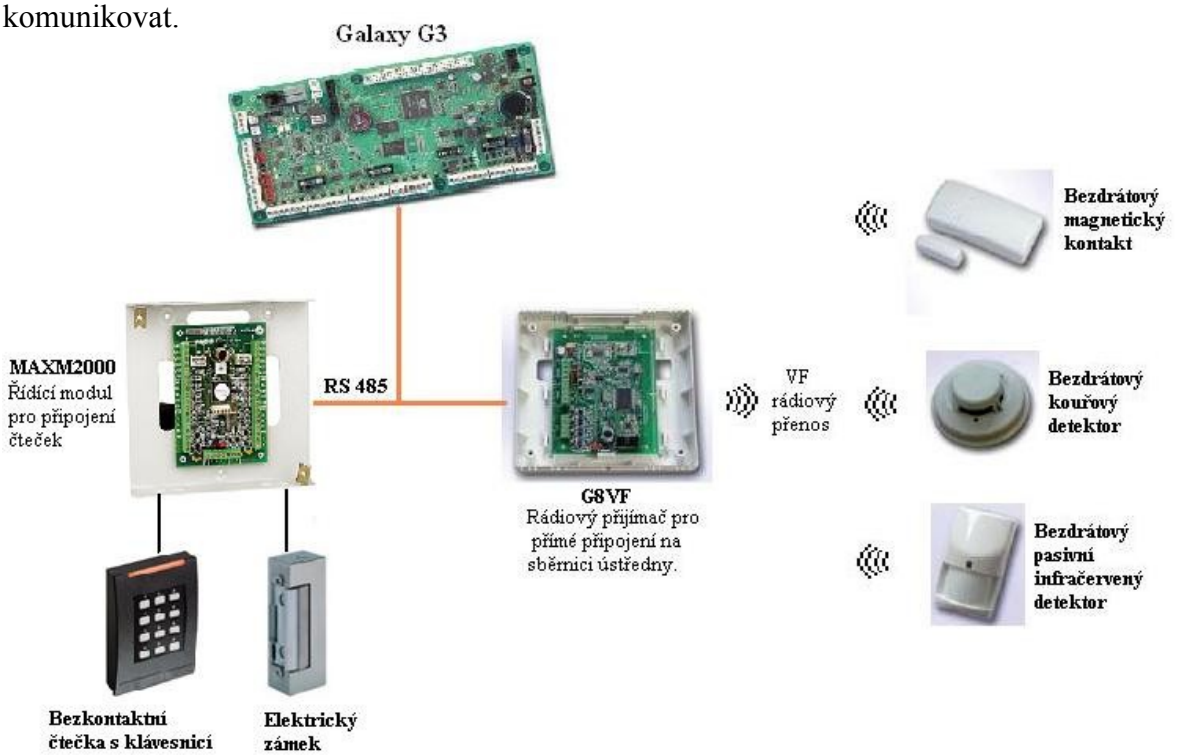
Nevýhody:

- Při špatném nakonfigurování vykazuje systém chyby

Způsoby integrace:

Hardwarová

Hardwarová integrace se řeší propojením přístupového systému s poplachovým zabezpečovacím systémem přímo na ústředně PZS. V tomto případě je potřeba, aby ústředna podporovala komunikační protokol přístupového systému a byla schopna s ním komunikovat.



Obr. 25 Příklad hardwarové integrace ACS a PZS produktů od firmy Honeywell

Softwarová

U softwarové integrace se vychází z toho, že komponenty poplachových zabezpečovacích systémů jsou spojeny v ústředně a ta je propojená s PC. K PC je také připojený přístupový systém a pomocí speciálního programu oba dva systémy lze sjednotit do jednoho.

3.2 Integrace systému kontroly vstupu s kamerovými systémy

Kamerové systémy jsou vhodné k integraci, pokud chceme mít vizuální přehled o osobách při vstupu do objektu nebo o jejich pohybu v objektu. Umožňuje nám sledovat činnost osob v objektu a permanentní kontrolu veškerého pohybu osob v objektu s možností včasné reakce na nežádoucí situaci, která může vzniknout. Také umožňuje natočení kamery a přiblížení horní části těla vstupující osoby, která prošla přes přístupový systém.[24]

Výhody:

- Přehled o činnostech osob v objektu
- Sledování osob při vstupu do objektu
- Možnost včasné reakce na nestandardní situaci
- Vyšší míra zabezpečení

Nevýhody:

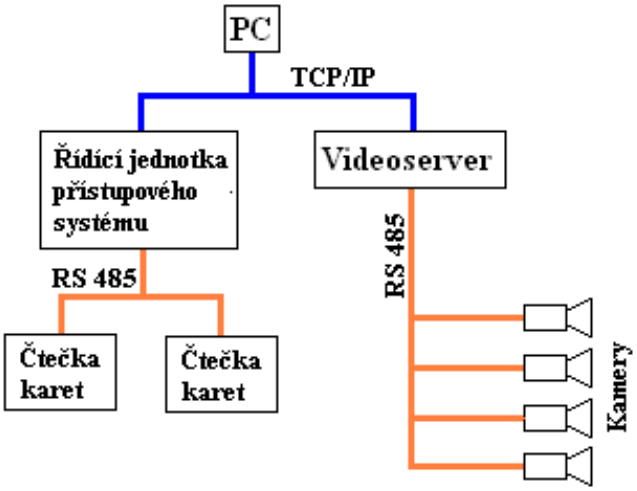
- Finanční náročnost
- Systém je náročný na obsluhu – nutnost osoby, která sleduje monitor.

Možnosti integrace:

Integraci kamerového systému s přístupovým lze provést softwarovou integrací. Kdy pomocí speciálního programu provedeme integraci přístupového systému s kamerovým systémem.

Softwarová integrace:

U softwarové integrace propojíme kamery a přístupový systém k PC pomocí RS 485, RS 232, TCP/IP. Pro integraci je zapotřebí softwarový převodník tvořený speciálním programem, který umožní komunikaci kamerového systému s přístupovým systémem. Jednoduchý příklad integrace je na obrázku č. 28.

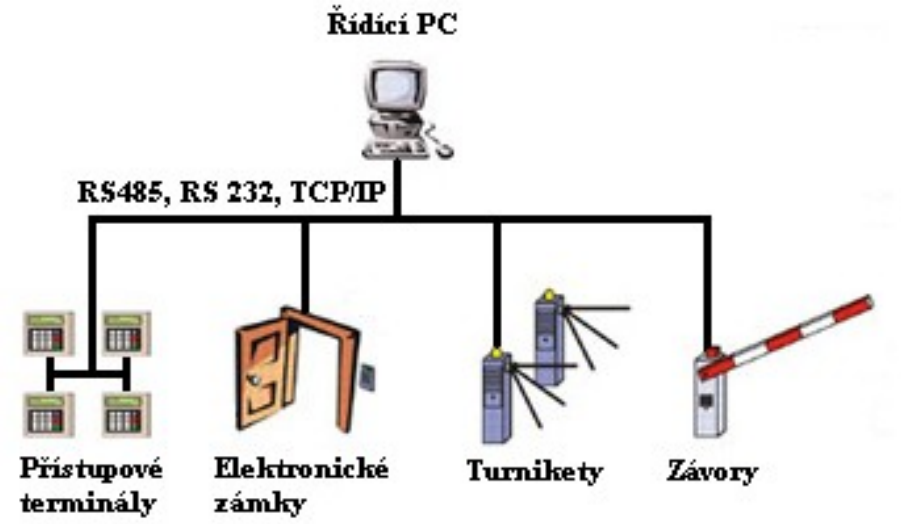


Obr. 26 Integrace ACS s CCTV

Obr. 27 Střežení vstupu kamerou CCTV [24]

3.3 Integrace systému kontroly vstupu s mechanickými zábrannými systémy

Mezi mechanické zábranné systémy patří turnikety, brány, elektrické zámky. Ty je možné integrovat se systémem kontroly vstupu. Integrace je prováděna buď přímo u výrobce, který poskytuje celkový systém, např. turnikety s vestavěnou čtečkou otisků prstů a řídící jednotkou, elektrické zámky s kódovou klávesnicí anebo mohou být turnikety, závory, elektrické zámky a přístupový systém propojeny přes řídící počítač. Propojení může být vedeno přes RS485, RS 232, TCP/IP, jak je vidět na obrázku:



Obr. 28 Integrace ACS s MZS

Obr. 29 Praktický příklad integrace [25]

3.4 Integrace přístupového systému se systémy řízení technologických procesů v budově

Kombinace přístupového systému se systémy řízení technologických procesů budov představuje elegantní a efektivní řešení pro inteligentní budovy. Pokud se osoba identifikuje pomocí přístupového systému při vstupu do objektu, může například předat povel ke spuštění větrání, topení nebo rozsvítí v místnosti světla.

Výhody integrace:

Úspora energie – například při vstupu do místnosti se rozsvítí světla, zapne klimatizace, topení a při opuštění místnosti se světla, topení nebo klimatizace vypnou.

Efektivní řízení procesů – například pomocí přístupových systémů můžeme sledovat počet osob v místnosti a nastavit tak klimatizaci nebo osvětlení v místnosti.

Nevýhody integrace:

Technická náročnost provedení integrace v již postavených budovách.

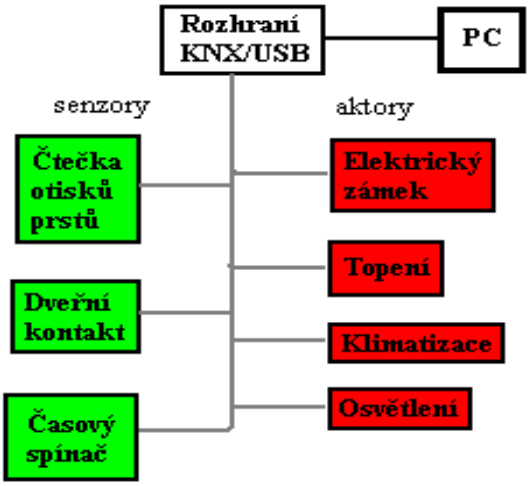
Způsob Integrace:

Jedním ze způsobů integrace přístupového systému se systémy řízení technologických procesů budov je integrace pomocí sběrnice jako je například KNX. Komunikace jednotlivých prvků probíhá přes sběrnici KNX/EIB, ke které jsou připojeny prvky a ty dělíme na SENZORY a AKTORY. Přičemž SENZORY jsou zařízení, které obsahují vstupní informace do systému (čtečka bezkontaktních karet, nebo jiný přístupový systém, teplotní Detektor, termoregulátor) a AKTORY jsou zařízení, které provádí nějakou akci nebo povel (elektromechanický zámek, turniket, řídící jednotky pro ovládání motorů ventilačních oken). Jednotlivé senzory propojíme se sběrnicí. Způsoby propojení mohou být provedeny s využitím:

- Kroucených párů (Twisted pair)
- Napájecích (síťových) vedení (Power line)
- Radiových přenosů (RF = Radio Frequency)
- Infračervených přenosů (Infra)
- Ethernetu, Bluetooth, WiFi /Wireless LAN nebo FireWire

Topologie propojení senzorů a aktorů může být provedeno v případě twisted pair hvězdicovou, stromovou nebo sběrnicovou strukturou.

SENZOR se skládá ze sběrnicové spojky, aplikačního rozhraní a aplikačního modulu. Sběrnicová spojka obsahuje svorky pro připojení k dvou-žilkové sběrnici KNX, aplikační rozhraní propojuje sběrnicovou spojku s aplikačním modulem a aplikační modul představuje druh zařízení (hardware) například čtečku otisku prstů. Sběrnicová spojka převádí signál na sběrnici a ze sběrnice jde pak signál do sběrnicové spojky a aplikačního modulu AKTORU jako je například osvětlení, ventilace. Programování jednotlivých zařízení se pak provádí v programu ETS 4.[25]



Obr. 30 Integrace ACS se systémem KNX/EIB

Obr. 31 Praktický obrázek technologických procesů v budově [26]

3.5 Integrace přístupového systému s docházkovým a mzdovým systémem

Kombinace přístupového systému s docházkovým systémem patří mezi nejčastější integrace přístupových systémů. Umožňuje vstup do objektu a zároveň zaznamenává datové údaje pro potřeby zaměstnavatele, které slouží k evidenci docházky. Zprostředkovává informace o příchodu a odchodu zaměstnance do/z objektu, odchodu na svačinu, k lékaři nebo na služební cestu. Tato kombinace se používá k přesnějšímu a

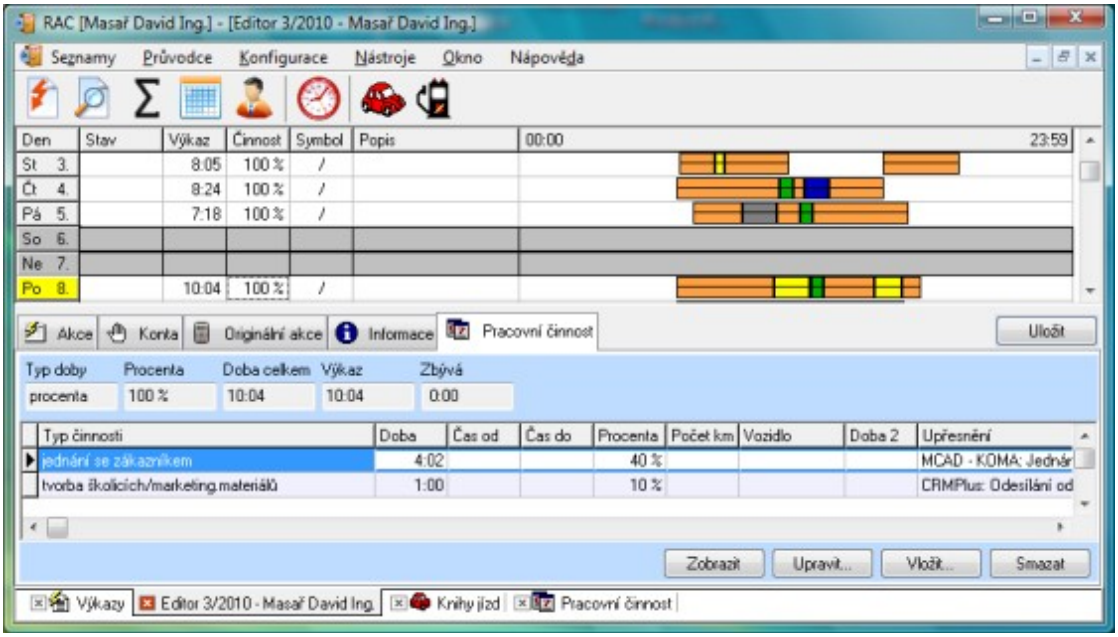
jednoduššímu zpracování dat o docházce, efektivnějšímu využívání pracovní doby a zvýšení pracovní morálky.

Výhody integrace:

- Docházka – možnost sledování příchodu a odchodu zaměstnanců.
- Mzdový systém – export dat do mzdových programů.
- Personalistika – získávání údajů o zaměstnancích o začátku a konci jejich pracovněprávního vztahu, úvazku, dovolených, přeřazení na jinou pozici nebo lokalitu.
- Šetří čas a peníze – automatické zpracovávání docházky a mezd.
- Efektivní kontrola – sledování údajů o docházce, kdo je ze zaměstnanců právě přítomen v práci a kde se nachází.

Nevýhody integrace:

- Chyba v softwarovém programu – při špatně naprogramovaném algoritmu může program vykazovat chyby.
- Nutnost kompetentního pracovníka pro správu systému
- Docházka – pokud pracovník odejde z objektu, nemusí to znamenat, že ukončil pracovní dobu, avšak by měl mít možnost danou skutečnost do systému zaznamenat.



Obr. 32 Ukázka docházkového systému [27]

Způsob integrace

Integrace přístupového systému s docházkovým a mzdovým systémem se provádí softwarovým způsobem pomocí programu, který zpracovává údaje ze čtecích zařízení. Program by měl umět zpracovávat pevnou i pružnou pracovní dobu s rovnoměrným i nerovnoměrným rozdělením, různé typy směn, přerušení pracovní doby, dovolené, evidovat noční a přesčasovou práci, pohotovost a pracovní cesty. Také je důležitá podpora procesů žádostí, povolování a schvalování (například dovolených, přesčasů a pracovních cest).

Dílčí závěr

Kapitola se zabývá problematikou integrace systémů kontroly vstupu s ostatními systémy. Integrace přístupového systému s ostatními systémy se v dnešní době stává téměř samozřejmostí. Integrace může být prováděna hardwarově pomocí rozhraní RS485, RS 232, TCP/IP nebo softwarově pomocí univerzálních programů jako je například AlViS, atd. Integrací přístupového systému s ostatními systémy se zvyšuje bezpečí v případě integrace PZS, komfort v případě integrace se systémy řízení technologických procesů budov nebo správa mzdového účetnictví v případě integrace s docházkovým systémem. Integrace různých systémů s přístupovým systémem přináší mnoho výhod, kdy pomocí ostatních systémů můžeme zastřežit oblasti, ve kterých se nikdo nenachází, sledovat pohyby osob pomocí kamer, při vstupech do místností, zapínat osvětlení, topení, atd. Nevýhody integrace vznikají při nekvalitní montáži systému nebo špatně zvolených komponentů při integraci s ACS.

4 NÁVRH PŘÍSTUPOVÉHO SYSTÉMU NA MODELOVÉM OBJEKTU

Pro svůj návrh integrovaného přístupového systému jsem si zvolil modelový objekt typu hotel. Vybral jsem si ho proto, že v hotelu jde zavést přístupový systém, který je flexibilní a umožňuje jednoduchou zprávu přístupu do objektu a do jednotlivých pokojů hotelu. Přístupový systém bude integrován se systémy řízení technologických procesů budov, poplachovým zabezpečovacím systémem, kamerovým systémem a docházkovým systémem.

Integraci PZS, ACS a systémy řízení technologických procesů budov navrhuji realizovat pomocí ústředny Galaxy GD-520. Systémy řízení technologických procesů budov budou připojeny k ústředně Galaxy pomocí čtyřnásobných univerzálních rozhraní. Přístupový systém bude připojen na ústřednu přes sběrnici RS485. Ústředna bude propojena s řídícím PC pomocí komunikačního rozhraní, které podporuje program AlViS. Tento program podporuje kamerový systém od firmy Samsung, který bude připojen k řídícímu PC přes TCP/IP.

Údaje o objektu:

Název hotelu je Hotel Modrá hvězda. Jedná se o třípatrovou budovu se sedlovou střechou, uvnitř budovy bude 14 pokojů s celkovou kapacitou 43 osob. V přízemí se bude nacházet malá restaurace, recepce a místnost pro správu objektu s trezorem.

Stupeň zabezpečení:

Pro celý hotel navrhuji stupeň zabezpečení 2, jen pro místnost s trezorem stupeň zabezpečení 3, jak je vidět na tabulce č. 4.

Tab. 4 Stupně zabezpečení podle normy ČSN EN 50131-1 [4].

Stupeň 1	Nízké riziko	Předpokládá se, že narušitelé mají malou znalost EZS a že mají k dispozici omezený sortiment snadno dostupných nástrojů.
Stupeň 2	**Nízké až střední riziko**	**Předpokládá se, že narušitelé mají určité znalosti o EZS a že použijí základní sortiment nástrojů a přenosných přístrojů.**
Stupeň 3	**Střední až vysoké riziko**	**Předpokládá se, že narušitelé jsou obeznámeni s EZS a mají úplný sortiment nástrojů a přenosných elektronických zařízení.**
Stupeň 4	Vysoké riziko	Předpokládá se, že narušitelé jsou schopní nebo mají možnost zpracovat podrobný plán vniknutí a mají kompletní sortiment zařízení včetně prostředků pro náhradu rozhodujících prvků v EZS.

Třída okolního prostředí:

Zařízení umístněná v objektu budou splňovat třídu prostředí 2. Zařízení, která budou umístněna vně objektu budou splňovat třídu prostředí 3, jak je vidět na tabulce č.5

Tab. 5 Třídy prostředí podle normy ČSN EN 50131-1 [5].

Třída 1	Prostředí vnitřní	Komponenty EZS musí správně pracovat, jsou-li vystaveny vlivům prostředí, které se vyskytuje ve vytápěných místnostech.	Předpokládají se změny teplot v rozmezí +5 °C až +40 °C při střední relativní vlhkosti okolo 75 % bez kondenzace.
Třída 2	**Prostředí vnitřní všeobecné**	**Komponenty EZS musí správně pracovat, jsou-li vystaveny vlivům prostředí, které se vyskytuje všeobecně v objektech, kde není udržována stálá teplota.**	**Předpokládají se změny teplot v rozmezí –10 °C až +40 °C při střední relativní vlhkosti okolo 75 % bez kondenzace.**
Třída 3	**Prostředí venkovní chráněné**	**Komponenty EZS musí správně pracovat, jsou-li vystaveny vlivům prostředí, které se vyskytuje všeobecně vně budov s tím, že komponenty EZS nejsou vystaveny plně vlivům počasí.**	**Předpokládají se změny teplot v rozmezí –25 °C až +50 °C při střední relativní vlhkosti okolo 75 % bez kondenzace. V průběhu roku se po dobu 30 dnů předpokládají změny relativní vlhkosti v rozmezí 85 % až 95 % bez kondenzace.**
Třída 4	Prostředí venkovní všeobecné	Komponenty EZS musí správně pracovat, jsou-li vystaveny vlivům prostředí, které se vyskytuje všeobecně vně budov s tím, že komponenty EZS jsou vystaveny plně vlivům počasí.	Předpokládají se změny teplot v rozmezí –25 °C až +60 °C při střední relativní vlhkosti okolo 75 % bez kondenzace. V průběhu roku se po dobu 30 dnů předpokládají změny relativní vlhkosti v rozmezí 85 % až 95 % bez kondenzace.

Přehled navržených komponent:

Poplachový zabezpečovací systém:

Poplachový zabezpečovací systém bude tvořit ústředna PZS Galaxy GD-520, která bude propojená s řídícím PC pomocí rozhraní RS232. Ústředna umožňuje střežit 16 zón. K ústředně PZS bude připojen rozšiřující modul, který ji rozšíří o 8 zón. Na jednu zónu připojenou k ústředně Galaxy GD-520 lze zapojit maximálně 5 detektorů, na zónu rozšiřovacího modulu lze zapojit maximálně 10 detektorů. Detektory budou tvořeny magnetickými kontakty, čidly tříštění skla, opticko-kouřovými hlásiči, termodiferenciálními hlásiči.

Ústředna PZS

Představuje zařízení, které přijímá a vyhodnocuje výstupní elektrické signály od detektorů PZS. Také ovládá signalizační, přenosová, zapisovací a jiná zařízení, která indikují narušení. Umožňuje napájení detektorů a dalších prvků PZS elektrickou energií.

Pro svůj návrh jsem zvolil ústřednu Galaxy GD-520 od firmy Honeywell. Jedná se o multiplexní ústřednu PZS s vestavěným napájecím zdrojem, 16 zónami (v jedné zóně může být zapojeno až 5 detektorů), 8 výstupy, telefonním komunikátorem a obousměrným portem RS232 a dvěma komunikačními sběrnicemi. Ústředna umožňuje připojit až 32 řídících modulů C080.

Vzhledem k potřebě střežení více zón v objektu je zapotřebí rozšířit ústřednu o rozšiřovací moduly G8.

Obr. 33 Ústředna Galaxy GD-520 [28]

G8(RIO)

G8(RIO) je vstupně/výstupní modul pro rozšiřování systému o 8 smyček (zón) a 4 výstupy. Také bývá označován jako RIO (Remote Input Output). K ústředně se připojuje pomocí sběrnicové linky RS485. Na jedné smyčce může být zapojeno až 10 detektorů.

Obr. 34 G8 rozšiřující modul [29]

GXYSMART

Tento komunikační modul k ústředně Galaxy G3 umožňuje integraci s programy třetích stran. V našem případě se jedná o program AlViS.

Obr. 35 Komunikační modul [30]

Požární hlásiče

Požární hlásiče jsou zařízení, která reagují na průvodní jevy, které nastávají při požáru, jako je kouř, nárůst teploty, plameny, nebo jejich kombinace. [26]

Do mého návrhu jsem zvolil dva typy požárních hlásičů, a to:

- opticko-kouřový – který pracuje na principu zeslabení nebo odražení infračerveného paprsku vyzařovaného LED diodou, který zaznamenává fotodioda. Opticko-kouřový hlásič bude umístněn v každém pokoji, na chodbách a v jídelně. Navrhuji detektor opticko-kouřový od firmy System Sensor. Detektor umožňuje nastavení tří úrovní citlivosti. Pracuje o teplotách od -20 do 60°C. Poplachový výstup je NO/NC, 30 Vss / 1 A.

Obr. 36 Opticko-kouřový hlásič [31]

- teplotní hlásič – Při hoření se zvyšuje okolní teplota a teplotní hlásiče tuto teplotu sledují, pokud teplota překročí určitou hodnotu, vyhlásí hlásič poplach. Také mohou fungovat na principu sledování rychlosti změny teploty. Tento typ hlásiče je vhodný pro umístnění do kuchyně. Zvolil jsem detektor termodiferenciální od firmy System Sensor, který vyhlásí poplach při teplotě 58°C. Pracovní podmínky má od 20 do 60°C. Poplachový výstup je NO/NC, 30 Vss / 1 A.

Obr. 37 Termodiferenciální hlásič [32]

Detektory tříštění skla

Slouží ke střežení skleněných ploch oken. Tříštění skla vyvolává charakteristický zvuk, který je následně čidlem vyhodnocen a je vyhlášen poplachový stav.[26]

Detektory tříštění skla navrhuji umístnit na okna v přízemí a prvním patře. Pro střežení oken jsem zvolil Detektor tříštění skla s vestavěným magnetickým kontaktem od firmy Honeywell. Výhodou tohoto detektoru je propojení magnetického kontaktu s detektorem tříštění skla, čímž se šetří na nákladech. Dosah detektoru činí 2,4 m, jeho pracovní teplota je od -10 do 50 °C. Poplachový výstup je NC, 25 Vss / 250 mA.

Obr. 38 Duální detektor tříštění skla [33]

Magnetické kontakty

Slouží k hlídání otevření, popř. destrukce prostupů pláště budov. Magnetické kontakty se montují na okna, dveře, rolety, vrata. Skládají se z dvojice dílů, z jazýčkového kontaktu a permanentního magnetu. Pokud je kontakt jazýčkového relé sepnut magnetickým polem permanentního magnetu, je magnetický kontakt v klidovém stavu. K vyhlášení poplachu dojde při oddálení magnetu. [26]

Obr. 39 Magnetický kontakt [34]

Magnetické kontakty navrhuji umístnit na okna v přízemí a prvním patře a na dveře vedoucí do objektu. Zvolil jsem magnetický kontakt se svorkovnicí, který má pracovní vzdálenost 30mm od firmy United Security Products. Poplachový výstup je NC.

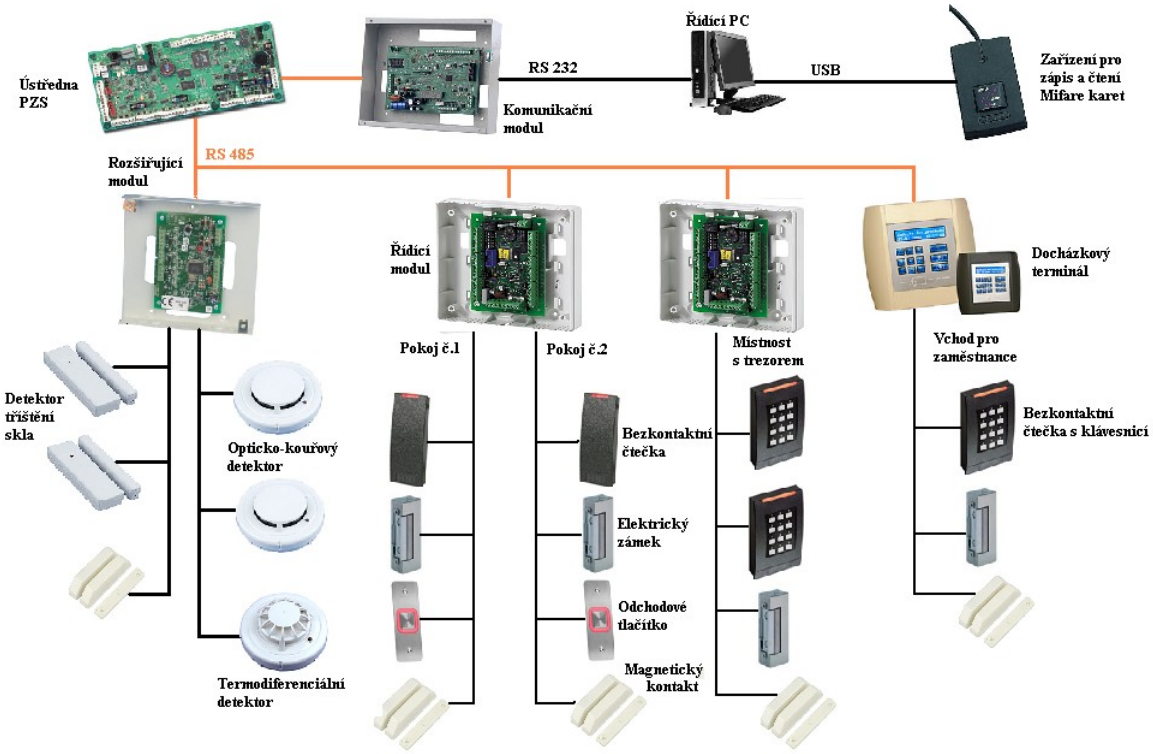
Přístupový systém:

Přístupový systém je v hotelu nainstalován pro přehlednou kontrolu pohybu osob a určení zón, kde se mohou osoby pohybovat. Zaměstnanci hotelu budou vybaveni bezkontaktní kartou a budou znát heslo, kterým se budou identifikovat v přístupovém systému. Zaměstnanci tedy budou mít přístup do hotelu přes hlavní a vedlejší dveře, také budou mít přístup do šaten. Pověřené osoby budou mít povolen přístup do místnosti s trezorem. Uklízečky budou mít přístup v době úklidu do všech pokojů, do posilovny a bazénu.

Hosté budou mít umožněn vstup přes bezkontaktní kartu do objektu přes hlavní dveře (v noci, ve dne budou hlavní dveře otevřeny) a do svého pokoje. Přístup do posilovny bude umožněn každému, přístup do bazénu jen, pokud si ho hosté zaplatí.

Přístupový systém se bude skládat z řídícího PC, ke kterému bude připojena ústředna PZS Galaxy GD-520, propojení bude provedeno přes komunikační rozhraní RS 232. K ústředně bude připojeno přes sběrnici RS485, 17 řídících modulů C080, které umožňují ovládat dvoje dveře naráz, pokud je z jedné strany čtecí zařízení a z druhé strany odchodové tlačítko, jako například pokoje hostů, šatny, posilovna, úklidová místnost. Pro potřebu umístnění dvou čteček z vnitřní a venkovní strany dveří budou zapojeny řídící moduly vždy jeden na dveře, a to u hlavních dveří, recepce, místnosti s trezorem, jídelny a kuchyně (ty jsou otevřeny přes den pro hosty, v noci jen zaměstnanci s příslušným oprávněním). U vedlejších dveří pro vstup do budovy bude umístněn docházkový terminál DT3000 SA, který bude připojen k ústředně přes sběrnici RS 485, umožňuje připojení externí čtečky, která bude umístněna z venkovní strany dveří. Na řídící moduly budou připojeny bezkontaktní čtečky Mifare karet, elektrické otvírače, dveřní kontakty a odchodové tlačítka. Jako přístupový prvek budou sloužit bezkontaktní karty Mifare, které bude možné programovat pomocí čtecího a zapisovacího zařízení, které bude připojené k řídícímu PC pomocí rozhraní USB. Na obrázku č. 40 je uveden příklad zapojení ústředny Galaxy GD-520, rozšiřujícího modulu, řídícího modulu pro dvoje dveře (např. pokoj č. 1 a č. 2), pro jedny dveře (např. místnost s trezorem) a docházkového terminálu. Ústřednu je zapotřebí

zapojit přes komunikační modul k řídícímu PC, z důvodu kompatibility s programem AlViS.



Obr. 40 Zapojení přístupového systému s ústřednou PZS

Řídící modul přístupového systému

Řídící modul jsem zvolil C080 od firmy Honeywell. Tento modul umožňuje propojení dvou čteček bezdrátových karet pro jedny nebo dvoje nezávislé dveře. Podporuje připojení dvou čteček stejného typu s výstupním formátem wiegand 26, 27, 32, 34 a 40 bitů. Modul také podporuje mnoho druhů čteček jako například čtečky typu Mifare. Modul se propojuje s ústřednou Galaxy GD-520 pomocí sběrnice RS485. Také obsahuje 2 relé pro ovládání zámků, možnost připojení dvou dveřních kontaktů typu NC, dvou odchodových tlačítek typu NO, napájení pro čtečky.

Obr. 41 Řídící modul C080 [35]

Docházkový terminál

K evidenci docházky zaměstnanců jsem zvolil docházkový terminál DT3000 SA s vestavěnou čtečkou karet iClass/Mifare/DESFire. Terminál obsahuje čtecí zařízení karet Mifare, a možnost připojení externí čtečky pro vstup do objektu. Je vybaven modrým displejem s 12 tlačítky, která umožňují nastavit 20 docházkových důvodů. Obsahuje paměť pro 6000 karet. Podporuje datové formáty wiegand. Jeden výstup pro relé na ovládání zámku dveří. Jeden vstup pro odchodové tlačítko a jeden vstup pro NC dveřní kontakt. Komunikační rozhraní má Ethernet, RS-232, RS-485. Umožňuje nastavit 8 časových zón.

Docházkový terminál bude umístněn u příchodových dveří personálu uvnitř budovy. Pro vstup do budovy bude umístněna externí čtečka s klávesnicí, která umožní vstup zaměstnanci do objektu a zároveň zaregistruje jeho příchod do zaměstnání.

Obr. 42 Docházkový terminál DT3000 SA [36]

Bezkontaktní čtečka Mifare karet

Tyto čtečky od firmy HID budou sloužit jako přístupový systém pro hosty. Umožňují čtení karet typu Mifare a to do vzdálenosti 8 cm. Mají pracovní frekvenci 13,56 MHz a výstupní formát wiegand. Obsahují LED diodu na indikaci stavu a bzučák.

Obr. 43 Bezkontaktní čtečky Mifare karet [37]

Bezkontaktní čtečka Mifare karet s klávesnicí

Umožňuje čtení karet Mifare do vzdálenosti 10 cm, výstupní formát má wiegand. Obsahují LED diodu na indikaci stavu a bzučák.

AIR ID Writer Mifare

Jedná se o čtecí a zapisovací zařízení Mifare karet, které je možné připojit k PC přes USB. Pracuje na frekvenci 13,56kHz, čtení a zápis provádí do vzdálenosti 20mm. Pomocí tohoto zařízení se budou upravovat karty pro hosty.

Obr. 44 AIR ID Writer Mifare [38]

Kamerový systém

Kamerový systém jsem zvolil proto, abych měl vizuální záznam z kamery, která bude střežit parkoviště před hotelem, také pro střežení uvnitř objektu budou umístněny kamery na chodbách, které budou zaznamenávat veškerý pohyb na chodbách. Záznam z kamer budou sledovat zaměstnanci na recepci. Kamerový systém bude tvořen 8 kanálovým videorekordérem, 6 kamerami tvořené dvěma venkovními kamerami a čtyřmi vnitřními kamerami. Kamerový systém budu integrovat s ostatními systémy softwarově pomocí programu AlViS, který tento kamerový systém podporuje.

Osmi kanálový videorekordér

Videorekordér, na který se může připojit 8 kamer, velikost hardisku má 1 TB, formát komprese je H.264. Rychlost záznamu má 200 obr./s. Má tři připojení USB, jeden výstup pro monitor BNC / VGA / HDMI. Možnost připojení ovládací telemetrie přes rozhraní RS485. Také mám možnost připojení na místní ethernet rychlostí 15Mb/s, přes který bude propojený s řídícím PC.

Obr. 45 DVR videorekordér od firmy Samsung [39]

Vnitřní IP box kamera

Vnitřní IP box kamera, která bude umístněna na chodbách, a před místností s trezorem, která má snímací prvek CMOS 1/4". Rozlišení je 640x480 a maximální rychlost snímání je 25 sn./s. Snímá při minimálním osvětlení až 1,4 lux. Připojuje se k DVR videorekordéru pomocí koaxiálního kabelu.

Obr. 46 Vnitřní IP box kamera firmy Samsung [40]

Venkovní IP box kamera

Pro monitorování parkoviště a vstupu pro zaměstnance jsem zvolil SNB-3000 od firmy Samsung. Je to Den/Noc IP s triple kodekem H.264, MPEG-4, MJPEG. Snímací prvek má 1/3" Super HAD PS CCD. Minimální osvětlení které je schopná snímat je 0,12 lux. Pro umístnění do venkovního prostředí je zapotřebí přikoupit venkovní kryt.

Obr. 47 Venkovní IP kamera od firmy Samsung [41]

Zdroj pro kamery

Pro napájení kamer jsem zvolil napájecí lineární zálohovaný zdroj. Umožňuje připojit až 8 kamer. Každý výstup je samostatně jištěný elektronickou vratnou pojistkou. Napájí se 230 V a výstupní napětí má 12 v. Maximální celkový trvalý odběr je 3,2 A.

Obr. 48 Napájecí zálohovaný zdroj [42]

Systémy řízení technologických procesů budov:

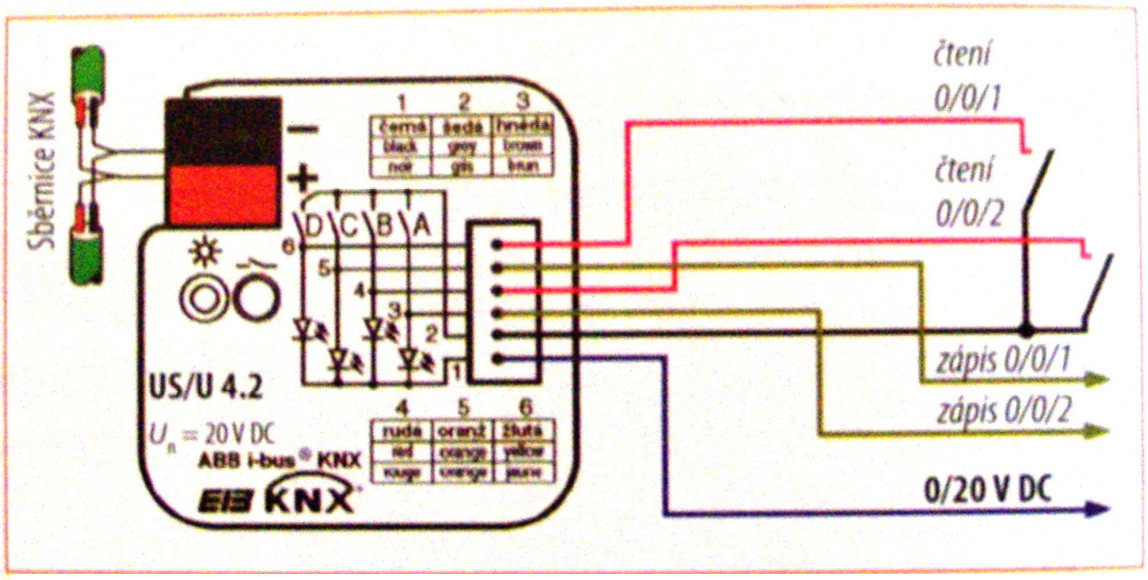
Pro větší komfort hostů jsem zvolil inteligentní ovládání osvětlení, žaluzií, ventilace, topení. Tyto funkce ovládání navrhuji realizovat pomocí sběrnice KNX/EIB a výrobků ABB i-bus® KNX. Sběrnice KNX bude připojena k ústředně PZS pomocí čtyřnásobných univerzálních rozhraní, které umožňují komunikaci PZS s KNX. Způsob zapojení je na obrázku č 49. Tyto zařízení komunikují pomocí adresných telegramů s jednobitovým příkazem, např. 0/0/1 aktivace PZS, 0/0/5 vypnutí světel, atd. Každá funkce bude mít

přiřazenou skupinovou adresu v telegramu, jak je znázorněno na tabulce č. 6. s návazností na obrázek č. 49.

Hotel navrhuji vybavit tlačítkovými spínači, akčními členy spínacími, které budou ovládat osvětlení, akčními členy topení, žaluzií, klimatizace, pohybovými detektory, termostaty a snímači intenzity osvětlení.

Tab. 6 Příklad jednobitové vazby mezi KNX a PZS [6]

Skupinová adresa	Funkce	Význam pro 0	Význam pro 1
0/0/1	Aktivace PZS	nezastřeženo	zastřeženo
0/0/2	poplach-narušení	neaktivní	aktivní



Obr. 49 Jednobitová vazba [43]

Konfigurace systému

Stav střežení bude aktivní pro neobsazené pokoje (bez hostů), pro pokoje obsazené hosty platí stav klid. Pokoj s trezorem bude stále ve stavu střežení, do stavu klidu přejde, pokud do místnosti vstoupí autorizovaná osoba.

Hlášení poplachu v rámci I&HAS

Výstup poplachové signalizace je na recepci, která provede vyhodnocení signálu a zákrok, případně přivolá pomoc. V případě zjištění požáru pomocí požárního detektoru ústředna spustí sirénu. Ústředna pak pomocí telekomunikačního modulu zašle rovněž zprávu majiteli objektu.

Legislativa

Prvky systému jsou ve shodě s požadavky národní legislativy.

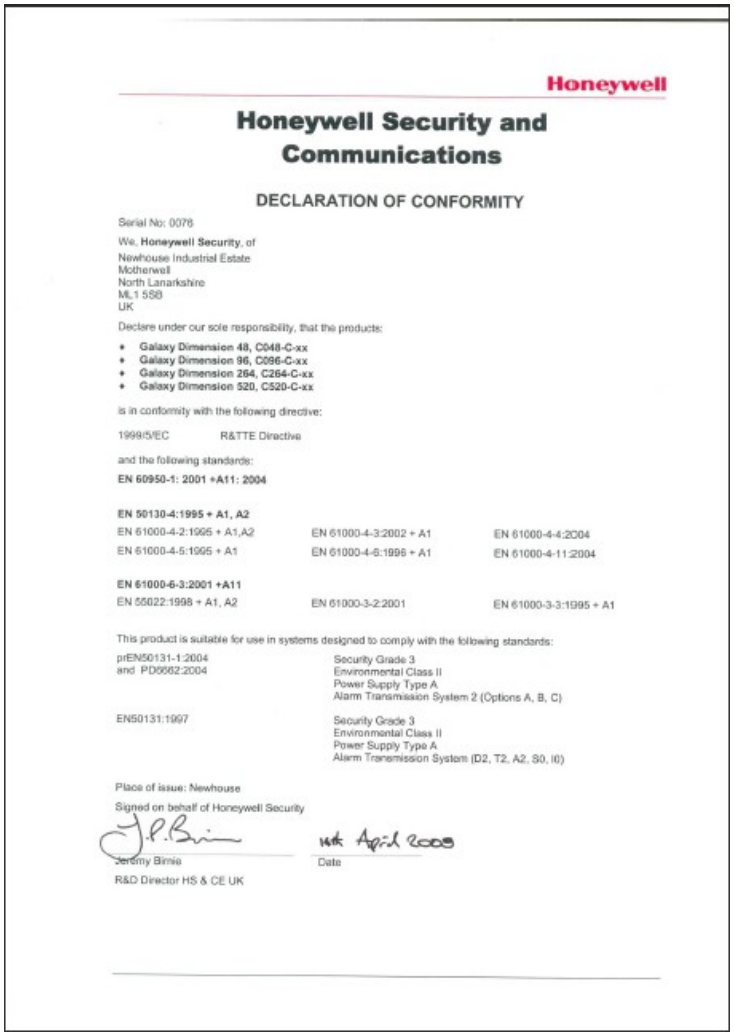
Normy

Prvky systému splňují požadavky národních a evropských norem.

Další předpisy

Prvky systému se dále řídí podle směrnic nebo kódů publikovaných pojišťovnami.

Certifikace



Honeywell

Honeywell Security and Communications

DECLARATION OF CONFORMITY

Serial No: 0076

We, **Honeywell Security**, of
Newhouse Industrial Estate
Motherwell
North Lanarkshire
ML1 5SB
UK

Declare under our sole responsibility, that the products:

- **Galaxy Dimension 48, C048-C-xx**
- **Galaxy Dimension 96, C096-C-xx**
- **Galaxy Dimension 264, C264-C-xx**
- **Galaxy Dimension 520, C520-C-xx**

is in conformity with the following directive:

1999/5/EC R&TTE Directive

and the following standards:

EN 60950-1: 2001 +A11: 2004

EN 50130-4:1995 + A1, A2

EN 61000-4-2:1995 + A1,A2 | EN 61000-4-3:2002 + A1 | EN 61000-4-4:2004
EN 61000-4-5:1995 + A1 | EN 61000-4-6:1996 + A1 | EN 61000-4-11:2004

EN 61000-6-3:2001 +A11

EN 55022:1998 + A1, A2 | EN 61000-3-2:2001 | EN 61000-3-3:1995 + A1

This product is suitable for use in systems designed to comply with the following standards:

prEN50131-1:2004 and PD6662:2004 — Security Grade 3, Environmental Class II, Power Supply Type A, Alarm Transmission System 2 (Options A, B, C)

EN50131:1997 — Security Grade 3, Environmental Class II, Power Supply Type A, Alarm Transmission System (D2, T2, A2, S0, I0)

Place of issue: Newhouse

Signed on behalf of Honeywell Security

Jeremy Birnie
R&D Director HS & CE UK

4th April 2008
Date

Obr. 50 Prohlášení o shodě Galaxy Dimension [44]

Ústředna Galaxy G3 má certifikát s evidenčním číslem (e.č.) T1109/2008, který vydává Národní bezpečnostní úřad podle § 46 zákona č. 412/2005 sb. O ochraně utajovaných informací a o bezpečnostní způsobilosti.

Detektor rozbití skla s magnetickým kontaktem FG1608AS s e.č. T1128/2010

Hlásič konvenční optický kouřový 2351E s e.č. E4009/2009

Hlásič teplot konvenční 5351E s e.č. T4011/2009

Komunikační interface pro ústředny Galaxy Dimension GD bylo uděleno posouzení o shodě CE v roce 2008.

Systém kontroly vstupů MAXM 2000 s e.č. T3022/2008

Bezkontaktní čtečka iClass R10 bylo uděleno prohlášení o shodě.

Bezkontaktní čtečka s klávesnicí iClass RK40 bylo uděleno prohlášení o shodě.

Zdroj pro kamery 12Z8 uděleno prohlášení o shodě v roce 2006.

Zásah

Při aktivaci poplachu je informován majitel objektu, případně zásahová služba.

Údržba

Údržba bude prováděna dle pokynů dodavatele prvků zařízení.

Opravy

Opravy zařízení budou prováděny servisní firmou.

Finanční náklady realizace

Pro lepší přehlednost uvádím ceník navržených komponentů v hotelu v tabulce č. 7. Náklady na ACS činí 248 989 Kč, náklady na PZS činí 114 318 Kč, náklady na CCTV činí 116 020 Kč. Celková cena všech komponentů je 479 327 Kč. Cena je pouze informativní, není v ní zahrnuta montáž, kabeláž, revize, atd.

Tab. 7 Ceník komponentů navržených do hotelu

	Typ	Množství	Cena za j.	Cena celkem
ACS				
Řídící modul	MAXM2000	17	4996	84932
Docházkový terminál	DT3000 SA	1	15900	15900
Bezkontaktní čtečka	iClass R10	27	2900	78300
Bezkontaktní čtečka s klávesnicí	iClass RK40	5	8900	44500
Čtecí/zapisovací zařízení	AIR ID Writer Mifare	1	5675	5675
Elektrický zámek		26	757	19682
Celková cena ACS				**248989**

PZS				
Ústředna	GALAXYGD-520	1	18200	21990
Rozšiřující modul	G8	2	3200	6400
Komunikační modul	GXYSMART	1	7900	7900
Požární hlásič opticko-kouřový	SS2351NL	35	1364	47740
Požární hlásič teplotní	SS5351RL	2	1119	2238
Detektor tříštění skla	FG1608	35	690	24150
Magnetický kontakt	SP1000	26	150	3900
Celková cena PZS				**114318**

CCTV				
Videorekordér	SRD-870	1	55990	55990
Vnitřní IP box kamera	SNB-1000	4	6590	26360
Venkovní IP box kamera	SNB-3000	2	11590	23180
Zdroj pro kamery	12Z8	1	10490	10490
Celková cena CCTV				**116020**

Celkem :	**479327**

Dílčí závěr

Kapitola se zabývá návrhem ACS na modelovém objektu a integrace PZS, CCTV, docházkového systému a systému řízení technologických procesů.

Pro svůj návrh modelového objektu jsem si zvolil objekt typu hotel. Jedná se o budovu se sedlovou střechou, ve které je 14 pokojů, jídelna, kuchyně, posilovna a bazén. Přístup do objektu, pokojů a dalších místností jsem řešil pomocí systému kontroly vstupu, který jsem navrhl integrovat s docházkovým systémem (sledování docházky zaměstnanců), poplachovým zabezpečovacím systémem (vyšší zabezpečení majetku a osob), kamerovým systémem (střežení parkoviště) a systémy řízení technologických procesů budov (vyšší komfort hostů a úspora el. energie hotelu). Integraci jsem navrhl provádět hardwarově přes ústřednu PZS a softwarově pomocí programu AlViS (umožňuje připojení kamerového systému).

ZÁVĚR

Přístupové systémy jsou v dnešní době čím dál více využívány a přikládá se jim stále větší význam v zabezpečovací technice. Tyto systémy kontrolují vstupy do objektů, anebo přístup k zařízením. Umožňují nám získat přehled nad tím, kdo, kdy a kam vešel. Díky nim je možno kontrolovat pohyb osob v objektu a definovat, do kterých míst bude mít osoba povolený vstup. Přístup do objektu je povolen tehdy, když osoba žádající o vstup vlastní heslo, identifikační předmět, nebo biometrickou charakteristiku. Mezi přístupové systémy patří magnetická média, čipová média, elektrické zámky a biometrické charakteristiky. Magnetická média bývají nejlevnější, zároveň se ale častěji opotřebují a není problém je zkopírovat. Čipová média jsou dražší, ale poskytují vyšší úroveň zabezpečení oproti magnetickým médiím. Nejvyšší úroveň zabezpečení však představují biometrické systémy, kde již nepotřebujeme vlastnit předmět, který můžeme ztratit, anebo znát heslo, které můžeme zapomenout. Mezi nejrozšířenější biometrické charakteristiky patří otisk prstu, ale nejpřesnější je skenování oční duhovky nebo sítnice.

Problematiku přístupových systémů řeší řada norem ČSN EN 50133. V současné době v rámci uvedené řady byly vydány a vstoupily v platnost tři normy, které se zabývají všeobecnými požadavky, na funkčnost systémů kontroly vstupu, požadavky na komponenty a pokyny pro aplikace.

Integrované poplachové systémy se dělí na poplachové aplikace, zahrnující zabezpečovací aplikace, tísňové systémy a v určitých případech systémy kontroly vstupu nebo kamerové systémy, a na nepoplachové aplikace, které představují např. správu energetiky, budovy, osvětlení. Poplachové systémy je možno integrovat dvěma způsoby, a to hardwarově pomocí převodníků, anebo softwarově přes speciální program. Požadavky na integrované poplachové systémy jsou uvedeny v normě ČSN CLC/TS 50398, ve které jsou také informace týkající se prvotního návrhu systému, plánování, instalace, předávání, provozu a údržby kombinovaného a integrovaného systému.

Přístupové systémy je možné integrovat s poplachovými zabezpečovacími systémy, mechanickými zábrannými systémy, kamerovými systémy, docházkovými systémy a se systémy řízených tech. procesů budov. Integrace se řeší buď hardwarovým způsobem, nebo softwarovým programem.

Pro svůj ideový návrh jsem si vybral model objektu typu hotel. Tento objekt představuje vhodný příklad integrace přístupového systému s ostatními systémy. Vytvořil jsem návrh integrace přístupového systému s poplachovým zabezpečovacím systémem, docházkovým systémem, systémem řízení tech. procesů budov a kamerovým systémem. Integraci jsem navrhl provádět hardwarově (ústředna Galaxy G3) a softwarově pomocí programu AlViS. Díky této integraci bude hotel zabezpečen před nezvanými hosty, majitel získá přehled o svých zaměstnancích a dojde k úspoře el. energie. Hosté si budou užívat komfortu hotelu a rozhodně se nestane, že se v hotelu dostanou tam, kam by neměli. I zaměstnanci ocení výhody integrace systémů, čímž budou mít práci jednodušší, budou mít přehled o své docházce a mohou si tak plánovat dovolené a jiné události. Integrace, pokud je provedena správně, přináší mnoho výhod, a to jak v přítomnosti, tak i s výhledem do budoucnosti. Proto je namístě, aby při návrhu projektu projektant zvážil do budoucna možnost integrace dalších systémů.

ZÁVĚR V ANGLIČTINĚ

Nowadays, the access systems are used in steadily larger scale and more importance is attached to them in safeguarding technique. The access systems control entries to objects and/or access to equipment. They enable us to gain an overview of who entered where and when. Owing to them, we can very easily control the movement of persons on the premises, and define the spaces into which a given person will be permitted to enter. The access to object is authorized in cases the person asking entry holds the knowledge of password, the identification item or the biometric characteristic. Magnetic media, chip media, electric locks, and biometric characteristics count among the access systems. The magnetic media are the cheapest, however, they can be copied easily and are prone to wear. The chip media are more expensive but provide higher level of safeguarding compared to magnetic ones. Biometric systems represent the highest level of safeguarding, since one does not have to hold an item that can be lost, or to remember a password that can be forgotten. The fingerprints are among the most widespread biometric characteristics, bud iris or retina scan can be considered among the most accurate ones.

The issue of access systems is covered by the standard series ČSN EN 50133. At present time, three standards have been issued and are valid. These standards deal with the general requirements on the functionality of access control systems, on the components, and on the application instructions.

Integrated alarm systems are divided into alarm applications, that include safeguarding applications, emergency systems, and in certain cases the access control systems or camera systems, and non-alarm applications that are represented, for example, by energy, building or lighting management. Alarm systems can be integrated by two methods, namely hardware by means of converters, or software through special program. The requirements imposed on integrated alarm systems are stated in the standard ČSN CLC/TS 50398 that includes also the information on primary system design, planning, installation, commission, operation, and maintenance of combined and integrated system.

The access systems can be integrated with alarm safeguarding systems, with mechanical barrier systems, closed circuit television systems, attendance systems, and technological processes in buildings. The integration is solved either by hardware, or by software program.

I have chosen a model object of the hotel type for my hypothetic project. This object represents a suitable example of the integration of access system with other ones. I created the design of the integration of access system with the alarm safeguarding system, the attendance control and camera systems and with the technological processes of the building. I have proposed the integration by hardware (Galaxy C3 exchange) and software by means of the AlViS program. Thanks to this integration, the hotel will be guarded against unwanted visitors, the owner/manager will gain the track of his/her employees, and the energy saving will be gained. The guests will enjoy the hotel comfort and there will be no way that they could get to places in the hotel where they should not. Even the employees will appreciate the advantages of integrated systems because they will have track of their work attendance and will be able to plan vacations and other events. The integration, if done properly, brings many advantages at the present time, as well as in the future prospects. Therefore it is appropriate that the project manager takes into account the possibility of future system integration during the design stage of the project.

SEZNAM POUŽITÉ LITERATURY

[1] KONÍČEK, T., KOCÁBEK, P. *Cesta k bezpečí*. Praha: BEN, 2002. 256 s. ISBN 80-7300-032-6.

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

[3] ČANDÍK M. *Objektová bezpečnost II.* Zlín: Academia centrum, 2004. 100 s. ISBN 80-7318-217-3.

[4] *SOOM.cz* [online]. 2011 [cit. 2011-03-22]. Bezpečnost magnetických karet. Dostupné z WWW: <http://www.soom.cz/index.php?name=articles/show&aid=427>.

[5] *Wikipedia* [online]. 2011 [cit. 2011-03-25]. Magnetic stripe card. Dostupné z WWW: <http://en.wikipedia.org/wiki/Magnetic_cards>.

[6] *Wikipedia* [online]. 2011 [cit. 2011-03-25]. Smart Card. Dostupné z WWW: <http://en.wikipedia.org/wiki/Smart_card>.

[7] *ACSline* [online]. 2011 [cit. 2011-03-26]. ID_KEY. Dostupné z WWW: <http://www.acsline.cz/cs/id_key-kontaktni-cip-dallas-ds1990a-f5>.

[8] *Smart card alliance* [online]. 2011 [cit. 2011-03-27]. About Smart Cards. Dostupné z WWW: <http://www.smartcardalliance.org/pages/smart-cards-faq>.

[9] *Wikipedia* [online]. 2011 [cit. 2011-03-29]. Electronic lock. Dostupné z WWW: <http://en.wikipedia.org/wiki/Electronic_lock>.

[10] *Bera* [online]. 2011 [cit. 2011-03-29]. Samozamykací zámek elektromechanický. Dostupné z WWW: <http://www.bera.cz/?page=cz,sze>.

[11] RAK, R., MATYÁŠ, V., ŘÍHA, Z. *Biometrie a identita člověka*. Praha: Grada, 2008. 664 s. ISBN 978-80-247-2365-5.

[12] ŠČUREK, R. *Biometrické metody identifikace osob v bezpečnostní praxi: Studijní text FBI VŠB TU Ostrava*. Ostrava: VŠB TU Ostrava, 2008. 58 s.

[13] *Lupa* [online]. 2011 [cit. 2011-04-02]. Biometriky nejen v pasech . Dostupné z WWW: <http://www.lupa.cz/clanky/biometriky-nejen-v-pasech-1/>.

[14] *SOUČASNÉ TRENDY BIOMETRICKÝCH IDENTIFIKACÍ* [online]. BRNO : PYROS/ISET, 2008 [cit. 2011-04-02]. Dostupné z WWW: <www.isc.utb.cz>.

[15] ČSN EN 50133-1. *Poplachové systémy: Systémy kontroly vstupů pro použití v bezpečnostních aplikacích - Část 1: Systémové požadavky.* Praha: Český normalizační institut. 2001. 28 s.

[16] ČSN EN 50133-2-1. *Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích - Část 2-1: Všeobecné požadavky na komponenty* Praha: Český normalizační institut. 2001. 12 s.

[17] ČSN EN 50133-7. *Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích - Část 7: Pokyny pro aplikace.* Praha: Český normalizační institut. 2000. 16 s.

[18] ČSN CLC/TS 50398. *Poplachové systémy - Kombinované a integrované systémy - Všeobecné požadavky.* Praha: Český normalizační institut, 2009. 20 s.

[19] *Vytapeni.tzb-info* [online]. 2011 [cit. 2011-04-14]. Systémy a komponenty používané pro automatizaci budov - integrace systémů. Dostupné z WWW: <http://vytapeni.tzb-info.cz/mereni-a-regulace/7011-systemy-a-komponenty-pouzivane-pro-automatizaci-budov-integrace-systemu>.

[20] *Ambo* [online]. 2011 [cit. 2011-04-15]. Bezpečnostní systémy Johnson Controls Cardkey P 2000. Dostupné z WWW: <http://www.ambo.cz/index.php?lang=cz&cat2_open=1&sec=catal_detail&c_cat=13&oldsec=catal_menu2&id_catal=350&title_string=OESV>.

[21] KOMÍNEK, A. *Návrh a virtuální realizace komplexního zabezpečení objektu FAI-UTB s dálkovým dohledem a ovládáním*. Zlín, 2008. 80 s. Diplomová práce. UTB.

[22] *ALViS* [online]. 2011 [cit. 2011-04-15]. ALViS. Dostupné z WWW: <http://www.alvis.sk/>.

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

[24] *Průvodce integrovanými bezpečnostními systémy. Dokument BSIA* [online]. 2010, 1, [cit. 2011-04-19]. Dostupný z WWW: <http://www.ijs-security.cz/text/903PIBS.pdf>.

[25] *KNX technické informace. Dokument Schneider electric* [online]. 2009. [cit. 2011-05-01]. Dostupný z WWW: <http://www.vypinac.cz/download/vypinac.cz_knx_tech.informace.pdf>.

[26] KŘEČEK, S. *Příručka zabezpečovací techniky. vyd. 3.* Blatná: Cricetus, 2006. 350 s. ISBN 80-902938-2-4.

Seznam použitých zdrojů obrázků

[1] *Ukázka přístupového systému.* http://www.its-sro.cz/dochazkove-systemy

[2] *Schéma struktury systému kontroly vstupu.* ČSN EN 50133-1

[3] *Ukázka magnetické karty.* http://pandatron.cz/?532&ctecka_magnetickych_karet

[4] *Čtečka magnetických karet.* http://www.levna-pokladna.cz/

[5] *Popis čipu.* http://en.wikipedia.org/wiki/Smart_card

[6] *Čtečka čipových karet.* http://www.cteckykaret.cz/OMNIKEY-5321-USB-v2.aspx

[7] *Zámek na otisk prstu.* http://www.animobohemia.cz/ostatni-sortiment/kovani/

[8] *Princip činnosti biometrického systému.* Čandík Marek, Objektová bezpečnost II

[9] *Základní klasifikační vzory.* http://www.lupa.cz/clanky/biometriky-nejen-v-pasech-1/

[10] *Charakteristické znaky papilárních linií.* Čandík Marek, Objektová bezpečnost II

[11] *Snímání šablonováním.* Ščurek Radomír, Biometrické metody identifikace osob v bezpečnostní praxi

[12] *Snímač otisku prstu.* http://www.gme.cz/cz/snimac-otisku-prstu-p763-420.html

[13] *PCA – rozložení obrazu.* Ščurek R., Biometrické metody identifikace osob v bezpečnostní praxi

[14] *Příklad šesti tříd užitím LDA.* Ščurek Radomír, Biometrické metody identifikace osob v bezpečnostní praxi

[15] *Souřadnicová síť obličeje.* Ščurek Radomír, Biometrické metody identifikace osob v bezpečnostní praxi

[16] *Princip snímání oční duhovky*. http://www.vesmir.cz/clanek/identifikace-skenem-duhovky

[17] *Ukázka lokalizace sítnice a znázornění charakteristických parametrů*. Ščurek R., Biometrické metody identifikace osob v bezpečnostní praxi

[18] *Snímač geometrie ruky.* http://strade.fit.vutbr.cz/index.php?act=51&menu1=52&menu2=83

[19] *Obraz světelné prostupnosti ruky a ukázka principu snímání.* Ščurek R., Biometrické metody identifikace osob v bezpečnostní praxi

[20] *Integrované systémy v budově.* http://vytapeni.tzb-info.cz/mereni-a-regulace/7011-systemy-a-komponenty-pouzivane-pro-automatizaci-budov-integrace-systemu

[21] *Komunikační protokoly.* http://vytapeni.tzb-info.cz/mereni-a-regulace/7011-systemy-a-komponenty-pouzivane-pro-automatizaci-budov-integrace-systemu

[22] *Propojení komunikačních protokolů.* http://vytapeni.tzb-info.cz/mereni-a-regulace/7011-systemy-a-komponenty-pouzivane-pro-automatizaci-budov-integrace-systemu

[23] *Cardkey P2000.* http://www.ambo.cz/index.php?cat2_open=1&lang=cz&sec=catal_detail&oldsec=catal_list_page&id_catal=350&title_string=Bezpe%C4%8Dnostn%C3%AD%20syst%C3%A9my%20Johnson%20Controls%20Cardkey%20P%202000

[24] *Střežení vstupu kamerou CCTV*. http://www.realworldhouses.com/rw3frontdoor_9-06.html

[25] *Praktický příklad integrace přístupového systému s turniketem.* http://www.acsline.cz/cs/turnikety

[26] *Praktický obrázek technologických procesů v budově.* http://www.merel.cz/knx.html

[27] *Ukázka docházkového systému.* http://www.tdevelop.cz/dochazkovy-system.aspx

[28] *Ústředna Galaxy GD – 520.* http://www.elektronis.cz/galaxy-g3-system-ezs-elektronicke-zabezpecovaci-systemy.html

[29] *G8 rozšiřující modul.* http://www.adiglobal.cz/iiWWW/cz/produkty110.nsf/web_category_panel2_cenik_asc/560EE4A18358175EC1257359006289FF

[30] *Komunikační modul.*

http://www.adiglobal.cz/iiWWW/cz/produkty110.nsf/w/D3C77A77503E9D2AC125738C0035CCC0?OpenDocument

[31] *Opticko-kouřový hlásič.*

http://www.adiglobal.cz/iiWWW/cz/produkty122.nsf/web_category_panel1_cenik_asc/FD884EDD66FD2BC9C12574190064B0C5

[32] *Termodiferenciální hlásič.*

http://www.adiglobal.cz/iiWWW/cz/produkty122.nsf/web_category_panel1_cenik_asc/65DCDB834EAD1173C12574190064AD21

[33] *Duální detektor tříštění skla.*

http://www.adiglobal.cz/iiWWW/cz/produkty110.nsf/web_category_panel2_cenik_asc/8814D9A97293C25FC125735900628826

[34] *Magnetický kontakt.*

http://www.adiglobal.cz/iiWWW/cz/produkty110.nsf/web_category_panel3_cenik_asc/9FD77157492D4011C125735900628C70

[35] *Řídící modul C080.*

http://www.adiglobal.cz/iiWWW/cz/produkty110.nsf/w/20AB8350DC8374BDC125735900628A3F?OpenDocument

[36] *Docházkový terminál DT3000 SA.*

http://www.adiglobal.sk/iiWWW/cz/produkty130.nsf/web_category_panel1_cenik_asc/86D4DE562998D5B5C12577880049ADF8

[37] *Bezkontaktní čtečky Mifare karet.*

http://www.adiglobal.cz/iiWWW/cz/produkty130.nsf/w?Readform&c2=13025

[38] *AIR ID Writer Mifare.*

http://www.adiglobal.cz/iiWWW/cz/produkty130.nsf/web_category_list1_cenik_asc/1FDD75420D5A32C5C12573B4005F8244

[39] *DVR videorekordér od firmy Samsung.*

http://www.adiglobal.cz/iiWWW/cz/produkty141.nsf/web_category_list1_cenik_asc/08924263B651525AC12577880049CF96

[40] *Vnitřní IP box kamera firmy Samsung.*
http://www.adiglobal.cz/iiWWW/cz/produkty141.nsf/web_category_panel2_vyrobce_asc/2C65BD3EA13CB3BEC12577880049CBE3

[41] *Venkovní IP kamera od firmy Samsung.*
http://www.adiglobal.cz/iiWWW/cz/produkty141.nsf/web_category_panel2_vyrobce_asc/59568351B9AEDA83C12577880049CBEB

[42] *Napájecí zálohovaný zdroj.*
http://www.adiglobal.cz/iiWWW/cz/produkty141.nsf/w/15F54158C63615EDC1257359003157EE?OpenDocument

[43] *Jednobitová vazba.* Elektroinstalatér, 1/2011, strana 16.

[44] *Prohlášení o shodě Galaxy Dimension.*
http://www.adiglobal.cz/iiWWW/homologace.nsf/all/5754BFA995233963C12574B3004F07E7/$FILE/GALAXYGD_NBU_2011-06.pdf

Seznam použitých zdrojů tabulek

[1] *Klasifikace přístupu.* ČSN EN 50133-1

[2] *Klasifikace identifikace.* ČSN EN 50133-1

[3] *Stupně přísnosti.* ČSN EN 50133-1

[4] *Stupně zabezpečení.* ČSN EN 50131-1

[5] *Třídy prostředí.* ČSN EN 50131-1

[6] *Příklad jednobitové vazby mezi KNX a PZS.* Elektroinstalatér, 1/2011, strana 16.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACS Access kontrol systems

MZS Mechanické zábranné systémy

PZS Poplachové zabezpečovací systémy

CCTV Systémy uzavřených televizních okruhů

PVC Polyvinylchlorid

ABS Akrylonitrilbutadienstyren

ms milisekunda

TFT Thin-Film Transistors

m metr

CCD Charge-Coupled Device

kPa kilopascal

IAS tísňové systémy

LAN local area network

DVR digital video recorder

TB terabyte

SEZNAM OBRÁZKŮ

SEZNAM TABULEK