Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Kritéria výběru přístupových systémů

Criterions of the Selection of Access Systems

Bc. Daniela Skýpalová

Diplomová práce
2014

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2013/2014

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

Jméno a příjmení:	**Bc. Daniela SKÝPALOVÁ**
Osobní číslo:	**A11382**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Kriteria výběru přístupových systémů**
Téma anglicky:	**Access Systems' Selection Criterions**

Zásady pro vypracování:

1. **Zpracujte analýzu požadavků na přístupové systémy.**
2. **Popište funkční požadavky na prvky přístupových systémů.**
3. **Zhodnoťte kriteria architektury sítě, nastavení práv, definice stavů,integrace.**
4. **Zvolte přístupový systém u modelového objektu.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **LUKÁŠ, Luděk a kolektiv. Bezpečnostní technologie systémy a management I. 1. vyd. Zlín: VeRBuM, 2011, 133 s. ISBN 978-80-87500-5-7.**
2. **RAK, Roman a kolektiv. Biometrie a identita člověka. Praha: Grada, 2008, 664 s. ISBN 978-80-247-6392-7.**
3. **PÍSEK, Slavoj. Access 2013. Praha: Grada, 2013, 160 s. ISBN 978-80-247-4746-0.**
4. **BITTO, Ondřej. Šifrování a biometrika aneb tajemné bity a dotyky. 1. vyd. Kralice na Hané: Computer Media, 2005, 168 s. ISBN 80-86686-48-5; 9788086686486.**
5. **KŘEČEK, Stanislav. Příručka zabezpečovací techniky. Praha: Critetus, 2006, 315 s. ISBN 80-902938-2-4.**

Vedoucí diplomové práce: **JUDr. Vladislav Štefka**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **7. února 2014**

Termín odevzdání diplomové práce: **27. května 2014**

Ve Zlíně dne 7. února 2014

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Práce se zabývá analýzou požadavků na přístupové systémy, rozebírá kritéria, dle kterých je posuzován výběr vhodného systému, použité prvky, jejich vlastnost a možnost začlenění. Také se zaměřuje na další využití systému, zejména zaznamenaných údajů, pro potřeby firmy, pro přehled přítomných osob, nebo pro podporu případného pátrání. Cílem je získat měřítko, posuzování přístupového systému jako efektivní ochrany majetku malých a středních firem. Součástí práce je i návrh přístupového systému modelového objektu menší firmy.

Klíčová slova: přístupový bod, identifikace, snímač, přístupová práva, evidence, systém.

ABSTRACT

The work deals with the analysis of the requirements for access systems, discusses the criteria according to which the selection of a suitable system is assessed, the elements, their property and the possibility of inclusion. It also focuses on the use of the system, in particular of the recorded data, for the needs of the company for an overview of the present persons, or for the support of any search. The aim is to obtain a scale of assessment, access the system as an effective asset protection of small and medium-sized companies. Part of the work is the design of the access object model system to smaller companies.

Keywords: access point, identification, sensor, access rights, registration, system.

Ráda bych zde poděkovala svým přátelům a rodině za pomoc a podporu v mém studiu, dále firmě cominfo za poskytnuté informace, a vedoucímu práce JUDr. Vladislavovi Štefkovi za cenné rady a připomínky.

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, 10. května 2014 …….…….

podpis diplomanta

OBSAH

ÚVOD

Mít kontrolu nad stavem věcí je odedávna cílem každé společnosti či uskupení. Již ve starověku byly snahy o absolutní kontrolu vstupů a vjezdů do měst z důvodů ochránit majetek, obyvatele i zásoby.

Cíle přístupového systému nebo také systému kontroly vstupu jsou i dnes vlastně totožné. Každá firma se ochranou svého majetku a dat zabývá. Většina dobře chrání své informace zálohování a šifrováním, avšak ochrana majetku, vybavení kanceláří a strojů často zaostává, přitom nabídka ochranných prvků i celých systémů je velmi široká a nabízených funkcí a možností je nepřeberná řada. Možná právě proto není pro firmy zcela snadné se v nich zorientovat. Požadavky na přístupové systémy jsou z hlediska chráněných hodnot odlišné a potřeby firem různorodé. Přestože většina dodavatelů nabízí návrh na míru dle konkrétního zadání, je dobré uvědomit si základní funkci systému a mít předem představu o jeho možnostech.

Snahou práce, je seznámit zájemce s přístupovým systém jako celkem, s jeho funkcí i funkcí jednotlivých prvků a vhodnosti jejich použití. S možnostmi identifikace, nabídky identifikačních prvků a snímacích zařízení, popisem topologie systémů, určení vhodnosti architektury sítě a možností integrace systému, tedy s limity a variabilitou propojení a nastavení.

Vhodným výběrem přístupového systému získá firma dokonalý přehled o přítomnosti osob v objektu a jejich činnosti ve sledovaných prostorách. Zvýší bezpečnost zaměstnanců, majetku a dalších hodnot. V neposlední řadě také sníží náklady mzdové a režijní, zvýší komfort pracovního prostředí a posílí firemní prestiž.

I. TEORETICKÁ ČÁST

1 PŘÍSTUPOVÉ SYSTÉMY OBECNĚ

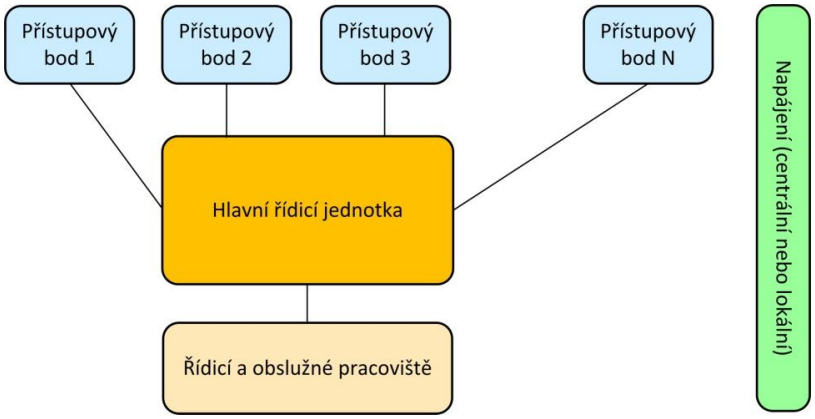
Systém kontroly vstupů tvoří soubor opatření k zajištění řízení a evidence přístupů do zabezpečeného objektu nebo prostor na základě jednoznačně přidělených přístupových práv. Je kombinací opatření systémových, fyzických, mechanických a elektronických. Snahou je omezit, nebo zcela vyloučit fyzickou ochranu, kterou obvykle vykonává strážní služba či ostraha objektu a je v systému nejrizikovější a nejnákladnější. Primární funkcí kontroly vstupu je monitorování času a důvodu průchodu přístupovým místem. Monitoring je prováděn na základě identifikace vstupujícího. Čas a důvod průchodu je zaznamenáván a dále zpracováván pro možné využití dalšími systémy. [1]

Předdefinované chování systému je možné vztáhnout na jednotlivé osoby či skupiny osob. Tedy vytvořit šablony uživatelů s určitým rozsahem přístupových práv, jako je dělník, návštěva, vedoucí pracovník a jednotlivé osoby zahrnovat do těchto skupin, přičemž jedna osoba může být zahrnuta do více skupin. Předdefinovaným chováním systému je myšleno nastavení vazeb akcí a reakcí na prostup identifikované osoby přístupovým bodem ve vztahu k prvkům systému, nebo jiným systémům (například ovládání topení, osvětlení, podmínění funkce zařízení, násobné vstupy). Definované chování může být nastaveno také dle časového filtru.

Získaná data jsou ukládána a archivována. Slouží k přehledu přítomnosti a pohybu osob v reálném čase i jako přehled historie událostí. Může být využita jako podpůrný prostředek při vzniku incidentu k odhalení pachatele. Další možností využití získaných dat, je použití pro evidenci docházky, která je zákonnou povinností zaměstnavatele, tj. evidence pracovní doby zaměstnance, přestávek, přesčasů apod. [11]

2 PŘÍSTUPOVÝ BOD

Struktura celého přístupového systému se skládá z jednoho či více přístupových bodů, hlavní řídící jednotky (pakliže je v systému nutná), napájení ať už centrálního či lokálního, komunikační sítě a řídícího a obslužného pracoviště.



Obr. 1. Struktura přístupového systému

Přístupový bod je místo, kde dochází k ověření přístupu. Obsahuje všechny prvky umožňující kontrolovaný přístup do prostor v daném místě. Často bývá stavebnicový a je tvořen identifikačním zařízením - čtečkou, řídicí jednotkou a k ní připojeného výkonového prvku. Výkonový prvek např. elektrický dveřní zámek nebo turniket, mechanicky umožní nebo zamítne přístup do vymezené zóny, na základě vyhodnocení řídící jednotky. Vyhodnocení je prováděno na základě identifikace osoby. [3]

2.1 IDENTIFIKACE

2.1.1 Identifikace heslem

Je nejstarší a nejrizikovější metodou. Je vázána na paměť nositele. Jedná se o posloupnost znaků, kterou je nutno zadat do přístupové jednotky. U vstupů a zámků většinou číselná kombinace pevně dané délky. Porovnává se shoda zadaného s databází povolených přístupů. Zadaná data, jsou srovnávána s databází oprávnění v nezašifrované či zašifrované, podobě. Pokud se používá kombinace loginu a hesla, což bývá většinou u přístupu do PC aplikací, vytvoří se z těchto údajů pomocí hash kódu otisk, který je pak porovnáván. Shoda musí být 100%. U této metody není potřeba vlastnit klíč, nebo předmět, riziko je v možnosti vyzrazení či zapomenutí číselné kombinace.

Obr. 2 Kódová klávesnice kovová ECK-02N [9]

2.1.2 Identifikace předmětem

Je založená na vlastnictví předmětu – tokenu – klíče. Ten obsahuje informaci k autentizaci. Jako tokenu se využívá karet nebo čipů, kontaktních či bezkontaktních, pracujících na různých fyzikálních principech. Načtená informace je porovnávána s databází oprávněných. Shoda musí být opět 100%. U této metody si není třeba nic pamatovat, předmět funguje jako klíč, právo přístupu lze přenášet na jinou osobu poskytnutím předmětu, rizikem je ztráta nebo zcizení předmětu.

2.1.3 Identifikace biometrií

U této identifikace je klíčem osoba samotná, respektive její behaviorální charakteristiky. Snímány jsou nejčastěji papilární linie prstů, oční duhovka, krevní řečiště rukou, rozpoznání obličeje a další. Tyto charakteristiky jsou naprosto jedinečné a neměnné, nepočítáme-li změny provedené plastickým chirurgem či devastujícím zraněním. Porovnává se binární informace, převedená pomocí nejrůznějších algoritmů z obrazce nasnímaného metodami pracujícími na různých fyzikálních principech (optika, kapacita, IR snímání). Vzhledem ke skutečnosti, že nasnímaný obrazec je při každém snímání trochu odlišný, porovnává se míra shody binární informace. Biometrická metoda je jedinou metodou identifikace, kde není vyžadována 100% shoda. Z důvodů, že biometrická informace není tajná, je součástí snímání i test živosti, jako zabezpečení proti podvrhu neživou náhražkou či fotografií. Toto bezpečnostní hledisko omezuje použití

metod biometrického snímání v bezpečnostních aplikacích. U této identifikace si není třeba nic pamatovat, ani opatrovat svazek klíčů či karet. Právo přístupu nelze předat na jinou osobu. Rizikem je skutečnost, že biometrický údaj je veřejným údajem. Dále vyskytující se problém, chybných přijetí a chybných zamítnutí (povolení neoprávněné osobě, zamítnutí oprávněné osobě). [2]

Obr. 3. Snímač otisků prstů [8]

2.1.4 Kombinace metod

Umožňuje využit výhod jednotlivých autentizací s cílem získat maximální bezpečnost chráněného majetku a maximální komfort pro uživatele. Přihlédnout je nutno i na prostředí, kde je metody užíváno v kontextu s použitým fyzikálním principem snímání (vnitřní, venkovní, prašné, výbušné apod.). Nejčastěji, se setkáváme s identifikací za pomocí kombinace předmětu a hesla, nebo předmětu a biometriky. Při kombinaci metod je důležité rozlišovat, zda hodláme mít přístup svázaný s vlastnictvím předmětem, nebo s oprávněnou osobou.

2.2 IDENTIFIKAČNÍ PRVKY - MÉDIA

2.2.1 Magnetická karta

Plastová karta, na které je nanesen proužek magnetického nosiče, obdoba magnetofonového pásku, který obsahuje všechny údaje včetně oprávnění. Informace se zapisuje pomocí nahrávací hlavy a zápis na kartě je kódován. Ke čtení dochází protažením karty štěrbinou, ve které je čtecí hlava. Kódovaná sejmutá informace je porovnána s databází oprávněných.

2.2.2 Kontaktní čipová karta a čip

Plastová karta s integrovaným obvodem (čipem), který je schopen zpracovávat data. Zařízení data přijme, zpracuje a vrátí požadované informace. Čipové karty je možné rozdělit na paměťové a mikroprocesorové. Funkce čipu a umístění na čipové kartě je standardizováno normou ISO/IEC 7816-2. Stejně pracuje i kontaktní čip. Vyznačuje se rychlostí a odolností.

Obr. 4. Kontaktní čip Dallas [10]

2.2.3 Bezkontaktní čipová karta a jiná bezkontaktní média

Proces identifikace je totožný jako i kontaktní karty. Využívá technologii RFID nebo NCF. Radiofrekvenční metoda identifikace. Jde o zařízení komunikující na dálku, skládající se z čipu a antény umístěné uvnitř těla karty. Liší se dosahovou vzdáleností a množstvím uchovávaných dat. Napájení je řešeno pomocí bezdrátové indukce z čtečky. Čtečka tedy vyšle indukční impuls, karta se nabije a pošle kódovanou informaci ke zpracování. Identifikační médium může mít i vlastní napájení, pak vysílá sám své údaje do okolí na vzdálenost až 100m. Identifikační médium může mít podobu přívěšku, hodinek, pásku či náramku. Využívá se i mobilního telefonu. Ten je opatřen NCF rozhraním, metoda identifikace je shodná. [4]

Obr. 5. RFID identifikační náramky [15]

http://www.combitrading.cz/nabizime/produkty/rfid-identifikacni-naramky.html

2.2.4 Optické karty a jiná optická média

Jedinečná informace je reprezentována černotiskem s vytištěnými pruhy - čárový kód, nebo mozaikou - QR kód a Data Matrix jako dvojrozměrné kódy, ty jsou zapisovány do čtverce. Známě i kruhový kód, který je ale variantou jednorozměrného kódu, ne jako sled čar, ale spojení těchto čar do soustředných kružnic. Informace je získávána převedením odraženého IR paprsku na elektrický signál a ten na binární hodnotu. Typ použitého čárového kódu je vybírán dle potřebného množství přenášených informací.

Obr. 6. REA::Ticket multifunkční terminál pro vstupenkové a odbavovací systémy [8]

2.2.5 Biometrie a manuální zadávání

Při identifikaci biometrií i u manuálního zadávání není třeba žádného předmětu. Snímání biometrie může probíhat snímání kontaktně či bezkontaktně, nebo automatickým rozpoznáním. Biometrie je oblast identifikace velmi rozsáhlá a více se o ni rozšiřovat nebudeme. Mohli bychom zde uvést ještě metodu automatického rozpoznávání – čtení

registračních značek vozidel, která vzešla z metody automatického rozpoznávání biometrických údajů. Využita bývá pro vjezd do rozsáhlých areálů.

2.2.6 Integrovaná a hybridní média

Jako identifikačního média můžeme využít jakéhokoli předmětu, což je velmi pohodlné pro uživatele. Vhodnější je ale využití identifikačního předmětu k více operacím, než jen k prostupu přístupovým bodem. Plastová karta má dnes v sobě implementováno více identifikačních prvků, například údaje o majiteli (fotografie, jména a příjmení, funkce nebo oddělení) pro kontrolu fyzickou ostrahou, čárový kód, nebo čip pro přístup do zón s nižším stupněm zabezpečení, i data k porovnání při snímání biometrie pro vstup do přísně střežených úseků. Identifikační médium může zároveň sloužit jako úložiště dat. Jednoho předmětu je tedy možno užívat na zařízení pracujících s různými metodami identifikace, na různých fyzikálních principech. Takové médium musí být zároveň chráněno před padělaním a zneužitím.

Identifikační média jsou opatřena bezpečnostními prvky ztěžujícím padělání, jako jsou hologramy, embossing, (vyražené či vystupující údaje o kartě a jejím majiteli), sériovým číslem apod. Data uložená na kartě či jiném médiu jsou pak uložena v šifrované podobě a proces identifikace probíhá v několika krocích, vylučujících podvrh, či hrubé překonání. Čtečka tedy ověřuje informace nejprve o pravosti média a poté o oprávnění přístupu.

Obr. 7. Identifikační karta [18]

2.3 ČTEČKY

Identifikační snímací zařízení, nebo také čtečky, terminály, tabla, přístupové jednotky, jak jsou často nazývány, zajišťují proces autentizace, tedy proces rozpoznávání, při kterém je výsledkem určitý statut. Statut oprávněný nebo neoprávněný. Čtecí zařízení přijímají informace z identifikačního média nebo od identifikované osoby dle různých identifikačních metod tyto informace porovná a vykonává další funkce, dle kterých je možné dělit snímací zařízení na:

Základní – zajistí pouze zadání kódu či sejmutí otisku, tyto údaje pak postoupí nadřazené jednotce. Při snímání biometrického údaje je vzorek porovnán v čtečce. Nadřazené jednotce je poskytován pouze údaj o čísle uživatele. Těchto jednotek je nejvíc užíváno v rozsáhlých aplikacích. Ostatní kroky prostupu provádí řídící jednotka.

Polointeligentní – neprování vlastní porovnání a povolení přístupu, ale mají veškeré potřebné vstupy a výstupy pro ovládání přístupového bodu. Porovnání a povolení prování řídící jednotka.

Inteligentní – mají všechny vstupy a výstupy a provádějí i porovnání údajů, rozhodují o autentizaci samostatně a nezávisle. Hlavní řídící jednotka provádí pouze aktualizaci přístupových práv a přijímá historii událostí. [1]

2.4 ŘÍDÍCÍ JEDNOTKA

Je výkonným prvkem systému kontroly vstupů. Ovlivňuje konfiguraci (nastavení) systému, prověřuje oprávněnost vstupů, aktivuje ovládací prvky, sleduje narušení systému, zaznamenává veškeré identifikace apod. Jsou k ní připojeny vlastní identifikační jednotky a přes dané rozhraní s ní komunikují.

V některých případech není nutné stálé připojení k PC, to je potřeba, když chceme uložit nashromážděná data. Pak se vyprázdní i vnitřní paměť řídicí jednotky a je opět připravena k ukládání dalších identifikací. Vyhodnocování nashromážděných dat a vytváření přehledů o průchodech podle zvolených parametrů, je realizováno prostřednictví PC aplikace. To je případ off-line připojení.

Mnohé přístupové systémy pracují v síťovém prostředí a tedy on-line, což umožňuje řídícím pracovníkům sledovat nové průchody v systému v reálném čase. Součástí řídící

jednotky je tedy i ethernet převodník, potřebný k připojení přes ethernet. Zajišťuje převod datové komunikace z procesoru na sběrnici.

Dalšími prvky, které jsou obvyklou součástí instalace, jsou přepěťová ochrana k ochraně vstupu řídící jednotky a sériového portu PC před přepětím na sběrnici, statickou elektřinou, zemními smyčkami a naindukovanými napěťovými špičkami ze síťového rozvodu a záložní zdroj sloužící k pokrytí výpadků síťového napájení.

Obr. 8. Řídící jednotka [17]

2.5 VÝKONOVÉ PRVKY

Výkonovými prvky jsou ovládaná zařízení, které po sepnutí či rozepnutí obvodu uvolní nebo zablokují prostup. Z celého systému jsou nejvíce namáhány a jejich funkční vlastnosti a spolehlivost, jsou jejich nejdůležitějšími vlastnostmi. Výkonové prvky mohou být samostatným prvkem (brána, závora) nebo mohou být součástí mechanické zábrany (zámky, magnety).

Výběr konkrétního výkonového prvku závisí na požadavku zákazníka, požadavku napájení a na požadavcích požárních předpisů. V případě výpadku napájení nesmí dojít k samovolné změně stavu prostupu, avšak z požárního hlediska musí být systém navržen tak, aby v případě požáru umožňoval únik osobám a zároveň zamezil šíření požáru. Konkrétní požadavky jsou předepsány požárním zprávou projektové dokumentace.

2.5.1 Dveřní zámky a otvírače

Těmito prvky jsou osazeny nejčastěji dveře. Často je zaměňován pojem otvírač a zavírač, stejně jako zámek a vložka zámku. Obecně je vnímáno, že zámek zamyká dveře na závoru, otvírač odblokovává střelku zámku, a zavírač jen zpomaluje dovření dveří. Mnohé zdroje užívají název zámek i pro otvírač, zámek zamykající na závoru je pak nazýván

samozamykací. Podstatné, je, že jsou tyto prvky součástí mechanické zábrany a volný prostup učiní až na základě a elektrického impulzu. Vyráběny jsou ve variantách dle typu a konstrukce dveří, protipožární voděodolné, pro únikové cesty, apod. Eletromechanické a elekromotorické zámky a otvírače mohou být podle stavu, v jakém se nacházejí při přivedení napětí, rozděleny do dvou provedení:

- běžné fail-secure, pod napětím jsou uvolněny, po odpojení napájení se zablokují
- reverzní fail-safe, pod napětím zablokovány, po odpojení napájení e uvolní

Elektrické/eletromagnetické zámky/otvírače - jsou známé jako „bzučák“ slouží pro blokování dveřních vstupů, otvírače se instalují dle provedení přímo do zárubně nebo do křídla dveří. Ovládání může být realizováno libovolnou elektronickou jednotkou (přístupová čtečka, telefonní vrátník) nebo jednoduchým ovládacím tlačítkem (odchodová tlačítka). K odblokování či zablokování západky otvírače dochází v závislosti na přivedení napětí, střelka zámku není tedy ničím blokována a dveře umožňují průchod.

Obr. 9. Elektrický otvírač FAB [19]

Elektromechanické zámky - **z**ařízení sloužící k vlastnímu elektro-mechanickému odblokování dveří a jejich následnému otevření. Obvykle se jedná o samozamykací zámky, kde zjišťovací střelka pozná dovření dveří a následně mechanicky vysune západku (závoru). Elektromagnet pod proudem aretuje pohyblivý mechanizmus v zámku a klika je plně funkční pro otevření dveří, je však nutné ji stisknout, aby došlo k zatažení závory. Bez napětí dochází k blokování funkce kliky.

Elektromotorické zámky - zámek pracuje tak že po příchodu aktivačního signálu je motoricky zatažena závora dovnitř zámku a následně odblokována střelka. Zámek je odemčen a dveře je možné otevřít pouhým zatlačením. Po uzavření dveří je zajišťovací střelka společně s hlavní střelkou zatlačena o protiplech do těla zámku a po vyskočení hlavní střelky do zárubně dojde k automatickému vysunutí závory a následnému zablokování střelky. Zámek je uzamčen ve dvou bodech a je elektromotoricky chráněn proti vysunutí závory mimo zárubeň. V případě výpadku napájení zůstává zámek v uzamčeném stavu. Zámek je vždy možné odemknout cylindrickou vložkou z obou stran dveří nebo stiskem kliky z vnitřní strany dveří, tzv. antipanic funkce.

Elektromotorické/elektrohydraulické otvírače – slouží k automatizovanému otevírání a zavírání různých typů dveří, může pracovat jak v tlačné, tak i v tažné funkci při vnitřní i vnější montáži. Používají se zejména pro bezbariérové vstupy v nemocnicích, poliklinikách, ambulancích, do administrativních budov. Obvyklá je kombinace se zámkem. Otevírání dveří zajišťuje elektromotor, zavírání dveří zajišťuje integrovaný dveřní zavírač.

Elektromagnety – udržují prostup (dveře) v uzavřeném stavu, v případě potřeby je možno kombinovat se zámky. Jejich základní předností je vysoká spolehlivost.

Přídržné elektromagnety – po otevření udržují dveře v otevřené m stavu, bez napětí dojde díky samozavírači k uzavření prostupu. Častěji jsou řešeny v rámci EPS.

Panikové hrazdy – v podstatě jde o variantu kliky v podobě hrazdy nebo lišty, montovanou na dveře únikových cest.

2.5.2 Brány, branky, závory

Tyto zábranné systémy blokují průchod či průjezd. Důraz je kladen na ochranu a bezpečnost provozu automatických dveřních a vratových systémů.

Brány – jsou skutečnou mechanickou překážkou zabraňující průjezdu. Dle způsobu otevírání je lze dělit na křídlová a posuvná. A ty pak na jednokřídlová a dvoukřídlová symetrická nebo nesymetrická.

Závory – jsou součástí parkovacího systému jako zajištění vjezdů, případně výjezdů z objektů podnikových parkovišť, domovních dvorů, výrobních závodů a dalších prostor, kde je požadavek na uzavření objektu před vjezdem nežádoucích vozidel

Pohony závor a bran – k ovládání turniketů, automatických dveří, vjezdových vrat a závor. Druh motoru je dán typem a konstrukcí brány či závory, výkon hmotností. Pro posuvné brány a závory motory elektromechanické, pro křídlové brány a dveře elektrohydraulická zařízení Ty mohou otevírat/zavírat bránu bez omezení počtu cyklů. Zařízení má obvykle mají vlastní řídící jednotku, které kontrolérem nebo vstupně výstupním modulem předáme impuls určité délky.

Obr. 10. Elektromechanický pohon pro posuvné brány

2.5.3 Turnikety

Turnikety můžeme nelézt všude tam, kde je potřebný dohled nad prostorem bez přítomnosti specializovaného personálu, jeho úkolem je usměrňování pohybu lidí, zaměstnanců nebo návštěvníků sledovaných prostor. Jsou nedílnou součástí komplexních systémů řízení. Turnikety jsou běžně osazena RFID čtečkami karet nebo čárového kódu, nebo UHF zařízeními, která jsou schopna monitorovat uživatele v zájmových zónách na dlouhé vzdálenosti a tím umožnit průchod turniketem i bez samotného přiložení identifikačního média.

Turnikety jsou zabezpečeny proti neautorizovaným průchodům, dále funkcí Anti-Panic automatického padajícího ramene a proti výpadku proudu záložním akumulátorem.

Ramena turniketu jsou mechanická, trvale otevřená v jednom směru, nebo je řízen elektronikou a zajištěn elektromagnety. Po identifikaci osoby je uvolněn elektromagnet v daném směru. Po průchodu osoby se směr opět uzavře.

Vertikální turnikety – turniket s vertikální osou otáčení, průchozí oběma směry s možností zablokování v obou směrech, často jako vstupní turniket prodejen, podobný brance.

Horizontální (tripodové) turnikety - turniket s horizontální osou otáčení, s trojitou vidlicí, průchozí oběma směry s možnosti zablokování v obou směrech.

Brankové turnikety – uživateli umožňují průchod s větší rychlostí a pohodlím, řešené jako jednoduchá motorová branka pro monitoring průchodu, nebo jako plnohodnotná náhrada turniketu, s nůžkovým nebo otočným rozevíráním.

Obr. 11. Turniket EASYGATE [8]

Turnikety plnoprůchodové /plnorozměrové - turniket s vertikální osou otáčení, průchozí oběma směry s možnosti zablokování v obou směrech, vyznačují se robustní konstrukcí, výškou většinou 2 – 2,5 m. Jsou konstruovány tak, aby sloužili jako plnohodnotná mechanická zábrana proti neoprávněnému vstupu. Jsou součástí oplocení, do prostor bez obsluhy, často doplněny o další zábrany, které budou eliminovat možnost přelezení turniketu. [8]

Obr. 12. Plnorozměrový turniket [8]

2.5.4 Bezpečnostní kabiny

Automatický vstupní portál v podobě kabiny, vybavené dvojicí skleněných posuvných dveří. Je určen do prostor, vyžadující vyšší třídu bezpečnosti. Vstup je umožněn pouze jedné osobě. Uvnitř kabiny je provedena identifikace a poté je přístup povolen, nebo vyžadován výstup z kabiny. Kabina je vybavena ultrazvukovým detektorem pro identifikaci dvou osob v portálu, detektorem kovu, přístupovým systémem a možné je i ruční vzdálené ovládání ostrahou.

2.5.5 Doplňkové prvky

Každá firma nabízející přístupové systémy, nebo jejich komponenty nabízí také celou řadu doplňků zvyšujících bezpečnost a komfort celého systému. Patří sem například pohlcovače karet, zábrany, zábradlí, stěny, majáky, retardéry atd.

Obr. 13. Sběrací snímač – pohlcovač karet [8]

2.6 NAPÁJECÍ ZDROJE

Napájecí zdroje zajišťují napájení všech prvků, a to většinou napětím 12V stejnosměrných. Jejich součástí je i záložní bezúdržbový akumulátor, který zajistí řádnou funkci systému i při výpadku síťového napětí standardně tak, aby udržel systém v provozu po dobu cca 12 hodin výpadku síťového napětí. Napájení jednotlivých zařízení může být prováděno také přes sběrnici určenou pro komunikaci mezi zařízeními.

Obr. 14. Napájecí zdroj [8]

2.7 ROZVODY

Zajišťují přenášení dat a komunikaci jednotlivých zařízení. Mají většinou formu sběrnice, propojující řídicí jednotky, dále propojení každé řídicí jednotky s její čtečkou a výkonovým prvkem (zámkem, závorou apod.). Vedení může být kabelové, které se instaluje pod omítku, nebo na omítku a to do vkládacích plastových lišt. Možné je i využití

bezdrátové instalace, která jen náročná na údržbu a snižuje variabilitu instalace. Běžně se pro komunikaci mezi zařízeními využívá rozhraní RS-232, RS-422, RS-485, Wiegand, sériové rozhraní Ethernet (jako lokální počítačová síť) a USB vedení. Standard RS-232 pouze definuje, jak přenést určitou sekvenci bitů, Ethernet umožňuje i vyšší vrstvy komunikace. Pravidlo pro komunikaci pak zajišťují komunikační protokoly. Specifikují mnoho vlastností (např. jak začít a ukončit zprávu). Nejznámějším protokolem je TCP/IP.

3 TOPOLOGIE SYSTÉMŮ KONTROLY VSTUPU

3.1 Autonomní systémy

Za autonomní systém je považován ten, který má maximálně dvě snímací zařízení, např. oboustranný prostup, má zároveň funkci kontroléru, nebo je řídící jednotka oddělena. Systém je vhodný pro jeden nebo několik samostatných přístupových bodů, kde je četnost pohybu osob menší a nároky na bezpečnost nižší. Příkladem mohou být autonomní dveřní zámky s integrovanou čtečkou. Přístupová práva se programují pomocí specifického postupu, jsou uložena v paměti samotného kontroléru. Identifikační zařízení je propojeno s řídící jednotkou pomocí proudové smyčky, jednoduché sériové linky nebo pomocí sběrnice RS-485. Bezpečnější možností je oddělená řídící jednotka. Paměť umožňuje uložení několik desítek uživatelů, záznam událostí není, nebo jen velmi omezeně, řídící PC se připojuje jen k servisním zásahům.

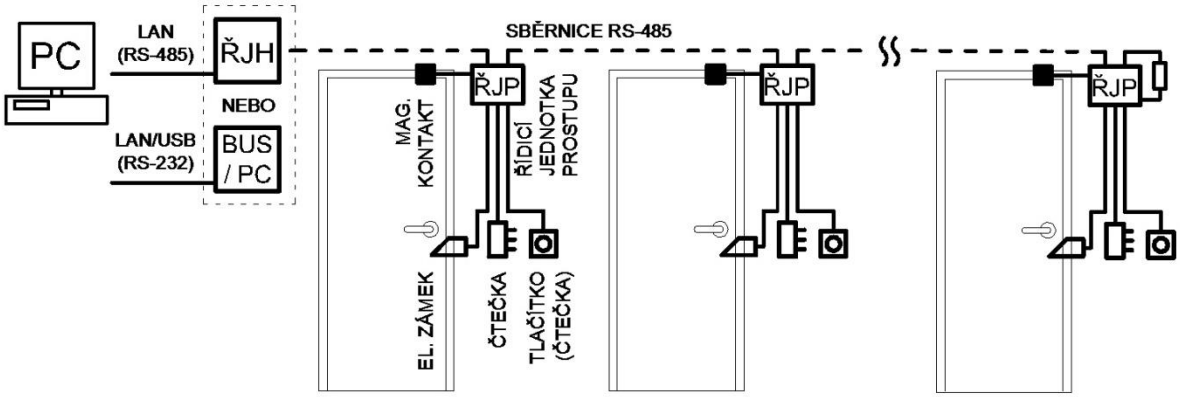
3.2 Modulární systémy

Koncepce pro rozsáhlejší systémy s řídícím pracovištěm, více přístupovými body a řídícími jednotkami. Využívá se hvězdicová nebo sběrnicová topologie, centrálním prvkem je ústředna nebo PC, tam probíhá samotná autentizace. U topologie typu sběrnice jsou všechna přístupová místa propojena pomocí RS -485 a připojena k ústředně nebo přes převodník sběrnice přímo k PC. U topologie typu hvězdice jsou přístupová místa propojena sítí Ethernet.

3.2.1 Sběrnicově propojené řídící jednotky přístupů

všechny terminály přístupů jsou propojeny sběrnicí RS-485 s hlavní řídící jednotkou nebo prostřednictvím převodníku k PC. Výhodou je vysoká spolehlivost sběrnice, relativně velké dosahované vzdálenosti až 1200m. Nevýhodou je nemožnost konfigurace „hvězda“, omezená rychlost komunikace a odezvy u rozsáhlejších systémů a problémy s impedančním zakončením sběrnice. Počet čteček na jedné lince RS- 485 je omezen na 32. Výhodou použití systémů s hlavní řídící jednotkou je větší spolehlivost a menší zátěž PC. Některé hlavní terminály mají integrovanou paměť, s PC komunikují pouze v případě konfigurace, aktualizace dat, varovných situací apod. Velmi často jsou hlavní terminály vybaveny LAN rozhraním, takže již není nutný žádný převodník a přístup je možný v rámci běžné Ethernet sítě. Navíc může být porucha PC detekována a komunikace nahrazena z jiného PC. Použitím řídících kontrolérů prostupů poskytuje největší

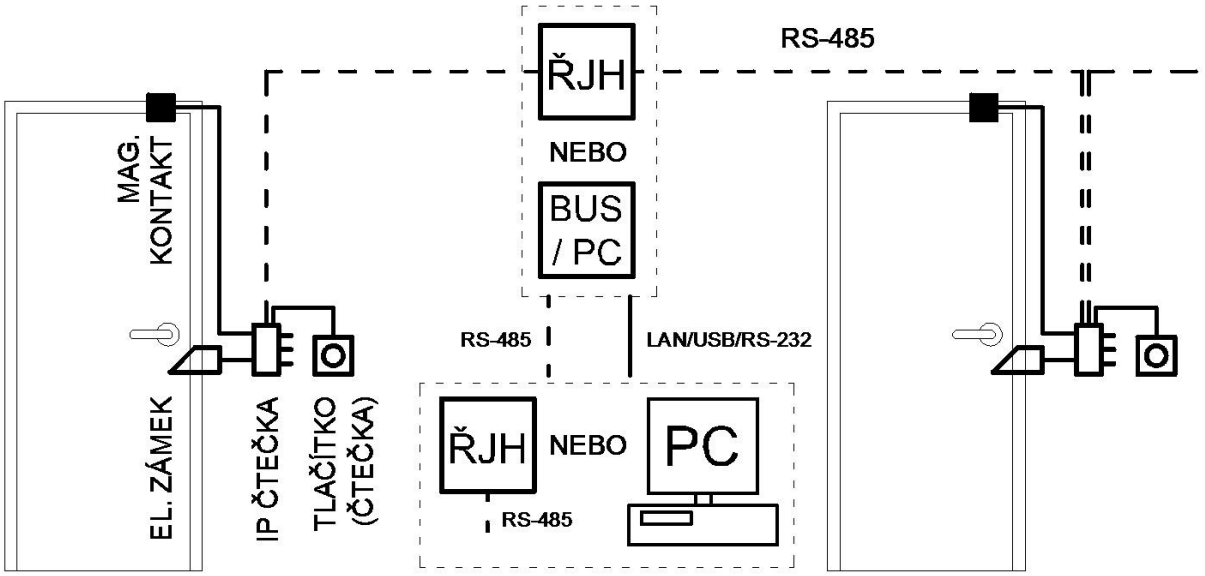
variabilitu, co se týče možností a typů použitých čteček, které jsou připojovány k řídící jednotce obvykle standardizovaným Wiegand rozhraním. [1, 5]



Obr. 15. Konfigurace sběrnicově propojených kontrolérů [1]

3.2.2 Sběrnicové propojené inteligentní čtečky

Sběrnice propojuje přímo polointeligentní nebo inteligentní čtečky bez potřeby řídících jednotek prostupů. Inteligence rozhodování se nachází v hlavní řídící jednotce, nebo v PC připojeném pomocí převodníku sběrnice. Více hlavních řídících jednotek je možné zesíťovat na stejnou sběrnici. Výhodou je jednoduchost kabeláže, nevýhodou omezený výběr inteligentních čteček. [1]



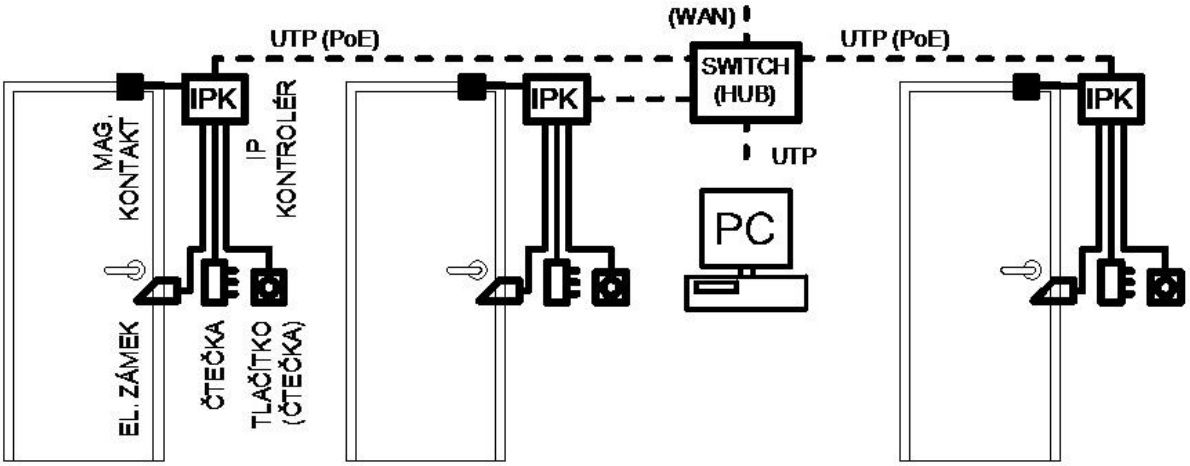
Obr. 16. Konfigurace sériově propojených inteligentních čteček [1]

3.2.3 Sběrnicově propojené systémy s převodníky LAN

Všechny topologie, využívající RS-485 sběrnici, mohou být doplněny převodníky RS-485/LAN. K distribuci signálu se následně využije stávající ethernetová struktura, na PC se nainstaluje vnitřní sériový port, jako přímé připojení. Využije se stávající sítě, výhodou je pak variabilita místa obsluhy. Zůstávají nevýhody, kterými jsou nízká komunikační rychlost a nižší spolehlivost z důvodů většího počtu prvků systému. [1]

3.2.4 IP řídící jednotky

Terminály jsou připojeny k řídícímu PC prostřednictvím LAN nebo WAN sítě. Využívá se stávající síť, odpadá omezení rychlosti a počtu prvků na RS-485. Terminál může sám vyvolat spojení s řídícím PC v případě události, nezahlcuje se tak zbytečně síť. Široké možnosti u optické sítě, wi-fi apod. Výhodné u velmi rozsáhlých systémů s velkým počtem uživatelů, v případě připojení LAN k WAN existuje riziko napadení. Zpomalení toků informací v případě přetížení LAN, Při potřebě doplňkových funkcí, kde je potřeba spolupráce více terminálů, musejí být použity terminály schopné komunikovat peer-to-peer (mezi sebou), jinak je funkce závislá na řídícím PC a při výpadku přestane fungovat.

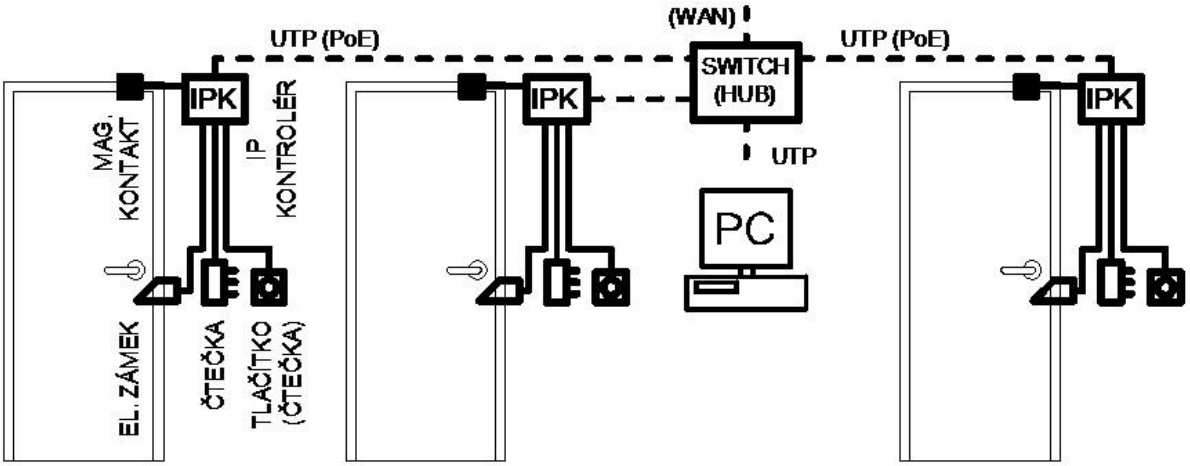


Obr. 17. Konfigurace s IP kontroléry [1]

3.2.5 IP čtečky

Inteligentní čtečky vybavení ethernet rozhraním jsou propojeny prostřednictvím stávající LAN nebo WAN k řídícímu PC. Většina IP čteček umožňuje napájení PoE (napájení po síti), což více zjednodušuje instalaci záložní napájení systému. Navíc se nabízí velmi jednoduché rozšíření stávajícího systému. Porucha jedné čtečky neovlivní zbytek systému. Technicky se ale jedná vlastně o integraci kontroléru a čtečky do jednoho celku

umístěného na přístupném místě, takže je jednodušší napadení přístupem ke kabeláži. IP čtečky jsou dražší a nenabízejí takovou variabilitu identifikačních formátů.



Obr. 18. Konfigurace s IP čtečkami [1]

4 ARCHITEKTURA SÍTĚ SYSTÉMŮ KONTROLY VSTUPU

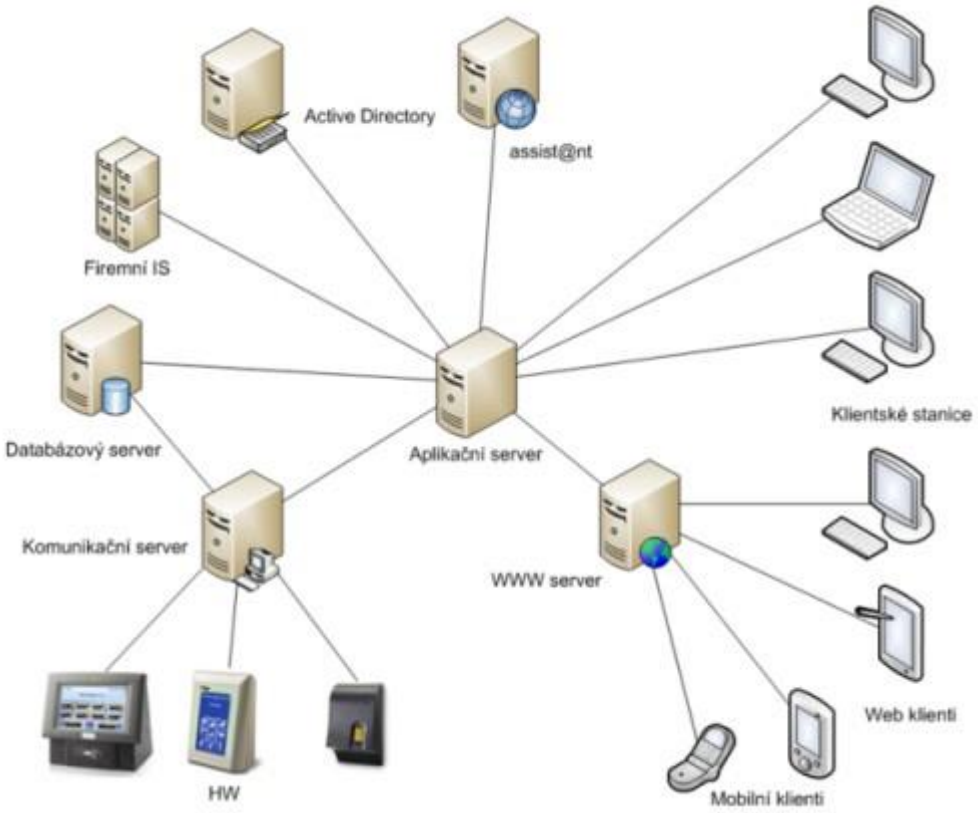
Rozsáhlejší systémy kontroly vstupů jsou prostřednictvím hlavní řídící jednotky, inteligentních snímacích zařízení spojeny s aplikačním a databázovým serverem, většinou prostřednictvím třívrstvé architektury s uspořádáním, kde:

1. vrstvou je uživatelské prostředí, jako jsou terminály, čtečky, hardware

2. vrstvou je vlastní aplikace, tedy program aplikačního serveru

3. vrstvou je databáze uživatelů a přístupových práv, tedy SQL server.

Jednovrstvá architektura soustřeďuje veškerou inteligenci do jediného centrálního počítače, u dvojvrstvé existuje databázový server a klient, a výkon je soustředěn buď na straně serveru, nebo klienta. Třívrstvá architektura je vhodná pro dosažení optimálního výkonu a stability. Klienti pracují pouze s uživatelským rozhraním, aplikační a databázové služby jsou odděleny. Komunikace probíhá prostřednictvím sítě ethernet pomocí TCP/IP protokolu.



Obr. 19. Znázornění třívrstvé architektury [1]

5 INTERGACE SYSTÉMŮ KONTROLY VSTUPU

Každá firma se chová ekonomicky a je tedy nasnadě využít jeden systém pro druhý, než instalovat dva samostatné systémy. Integraci můžeme rozdělit na hardwarovou, kde využíváme prvky jednotlivých instalací, celé moduly, nebo jen vedení a softwarovou, kde k integraci dochází programovým propojením, přesněji řečeno přes nadstavbovou programovou aplikaci. Při integraci je vždy nutné dodržet bezpečnostní požadavky, normy a předpisy na jednotlivé systémy, a nastavit priority komunikace, signalizace, vzájemné vazby a reakce na definované události.

5.1 Integrace hardwarová

Je kombinací slaboproudých systémů, tedy provázání prvků SKV s prvky jiných systémů, začlenění nebo rozšíření funkcí. V praxi se setkáme především s kombinací s těmito systémy:

Docházkový – určené prvky přístupového systému jsou využívány pro sledování docházky.

Stravovací – využívá se především shodných identifikačních médií a databáze, jinak se jedná o samostatný systém.

Poplachový zabezpečovací systém (PZS) – sofistikovanější sběrnicové systémy PZS často podporují základní funkce přístupových systémů, výhodou je zde možnost ovládat systém PZS prostřednictvím přístupových identifikátorů, monitorovat stav PZS za dveřmi na čtečce apod.

Elektrická požární signalizace (EPS) - je vždy samostatným systémem, při evakuaci nebo požáru je však nutné zajistit správnou funkci všech přístupových bodů, odblokovat únikové cesty, zablokovat požární prostupy apod. EPS poskytuje tyto signály prostřednictvím vstupně-výstupních modulů.

Kamerový systém (CCTV) - systém může při časové synchronizaci s SKV poskytnout doplňkové obrazové informace k prostupovým událostem.

IT systémy – samostatnými čtečkami identifikačních médií, připojenými k PC, se může řídit přístup k PC, k síti apod.

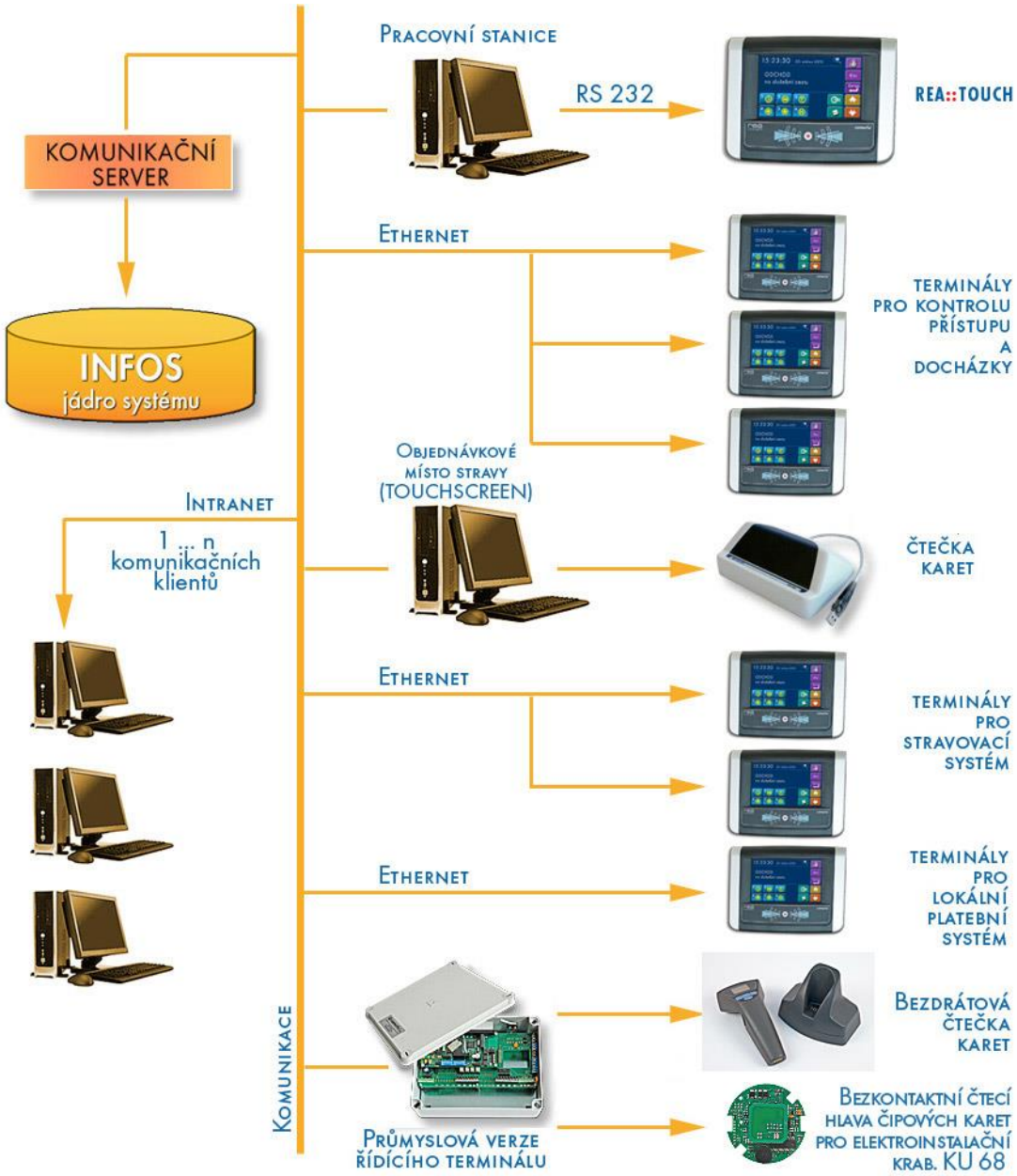
Mření a regulace – systémy měření a regulace mohou reagovat na přítomnost osob (nastavení osvětlení, vytápění, klimatizace apod.) [7]

5.2 Integrace softwarová

Softwarovou integraci je možné doporučit v případech, kde není možné bez počítačové nadstavby dosáhnout přehledného monitorování a řízení objektu. Důvodem mohou být požadavky na obsluhu nebo složitost objektu, vybaveného velkým množstvím různých slaboproudých zařízení. Jednotlivé prvky, systémy a aplikace jsou připojeny prostřednictvím sběrnice nebo síti Ethernet ke společnému serveru či klientskému PC, na kterém je nainstalován nadstavbový software. Ten vzájemně integruje systémy kontroly vstupu, docházky, elektrickou požární signalizaci, elektronické zabezpečovací systémy, kamerové systémy a systémy měření a regulace. Ovládání je možné i přes mobilní zařízení nebo v případě připojení na síť internet z kteréhokoli místa, připojeného k internetové síti.

Jednotlivé systémy mohou pracovat na odlišných softwarových platformách, integrovat je pak možné jen ty systémy, mající podporu integračního softwaru. V případě nesouladu, je nutný zásah programátora. Nadstavbové softwary jsou schopny zajistit správu systému, správu uživatelů, monitoring, vizualizaci, integraci technologií, automatizaci vazeb, evidenci návštěv a vjezdů, správu docházky, ovládání a programování, vyhodnocování a sledování událostí.

Použitím integračního softwaru lze získat zjednodušení řízení a ovládání systémů, zpřehlednění aktuálního stavu a zároveň snížení nákladů v porovnání cenou pořízení jednotlivých systémových softwarů.



Obr. 20. Schéma softwarově integrovaného komplexního identifikačního systému [8].

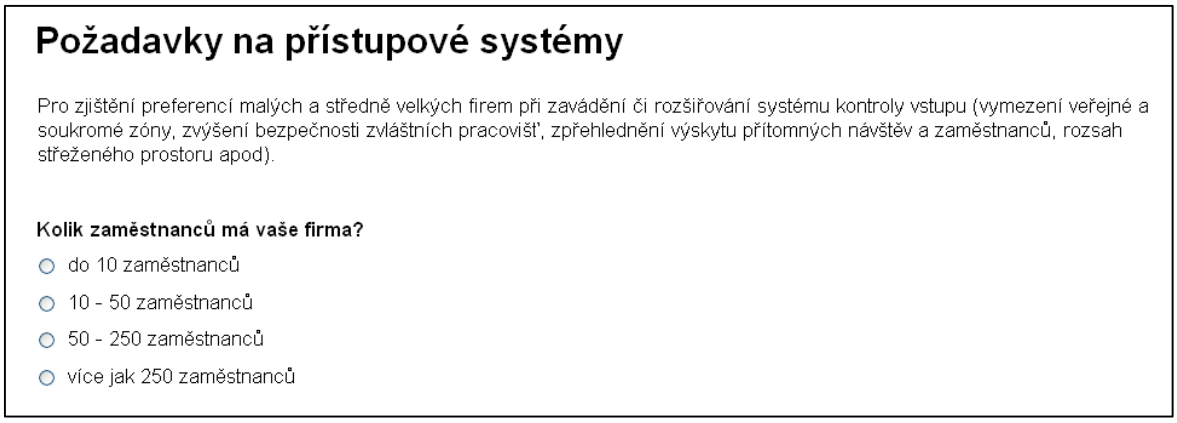
II. PRAKTICKÁ ČÁST

6 ANALÝZA POŽADAVKŮ NA SKV

Za účelem zjištění současných požadavků na přístupové systémy pro potřeby malých a středních firem, jsem vytvořila jednoduchý dotazníkový formulář, který jsem rozeslala firmám ve Zlínském kraji. Firmy jsem vybrala z rejstříku firem a databáze Inform podle počtu zaměstnanců. Osloveno bylo celkem 536 firem, dotazník vyplnilo 162 firem.

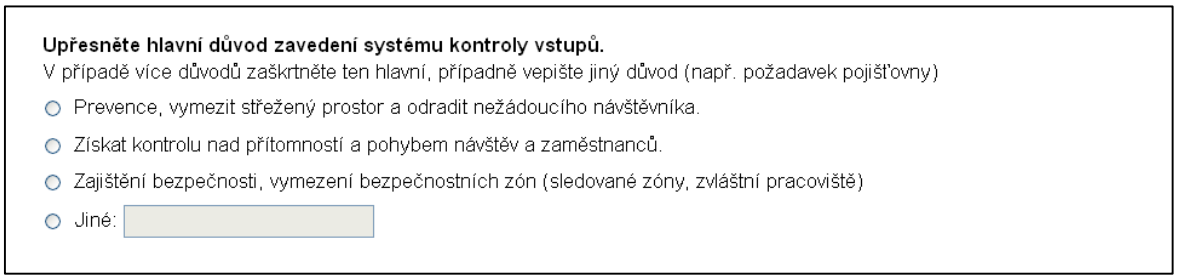
6.1 DOTAZNÍKOVÝ FORMULÁŘ

Dotazované firmy byly obeslány mailem s vysvětlením účelu dotazníku a odkazem na něj a požádány o vyplnění. Jako první krok bylo nutno vytřídit firmy, které nejsou zájmovou skupinou. Jejich odpovědi pak nejsou ve vyhodnocení zahrnuty.



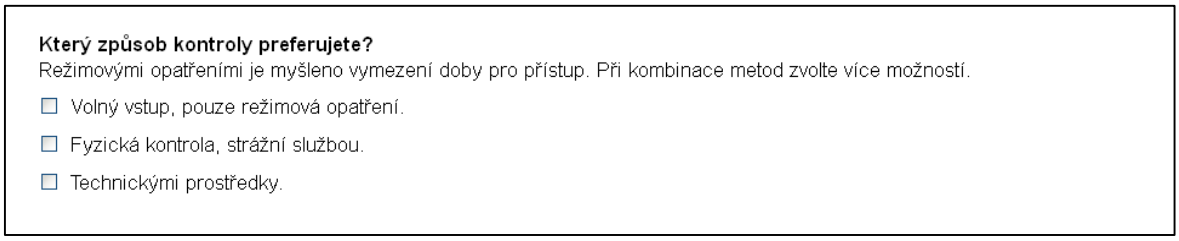
For. 1. Zjištění velikosti firmy podle počtu zaměstnanců

Dále byl zkoumán hlavní důvod zavádění přístupových systému. Co firma vnímá jako prioritu, nebo kde vidí hrozby. Zda má význam do hloubky rozebírat všechny oblasti systémů a kterým věnovat větší pozornost.



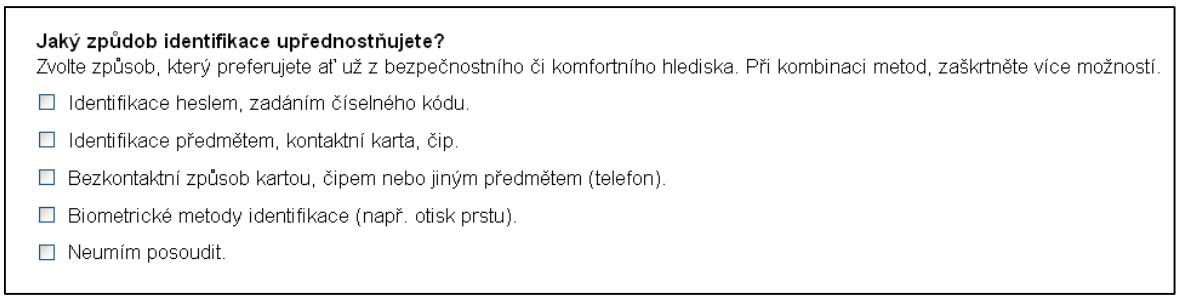
For. 2. Důvod zavádění systému kontroly vstupů

Další otázka zjišťuje, kterému způsobu ochrany firmy věří nejvíce. Lze z ní také vyvozovat, jak moc je firma tolerantní k osobám pohybujícím se v prostorách jejich podniku a do jaké míry chrání své hodnoty. Dotazovaní mohli zvolit více možností.



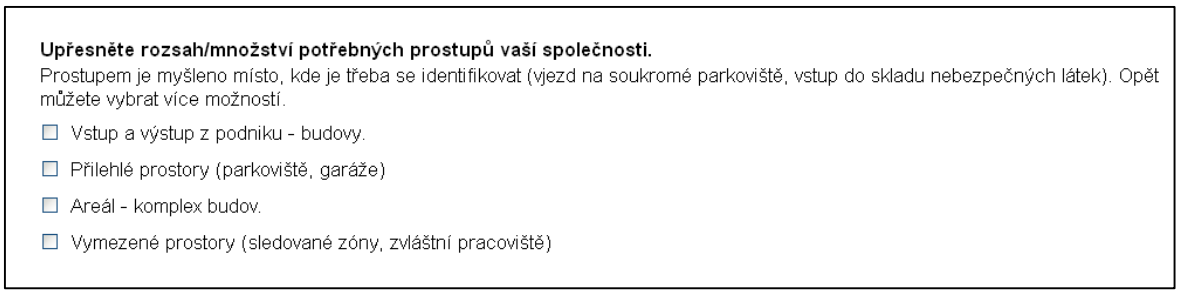
For. 3. Preference způsobu kontroly

Přístupové systémy nabízí velkou škálu identifikačních prvků, mým cílem bylo zjistit, ke kterému systému se ve firmách více přiklánějí.



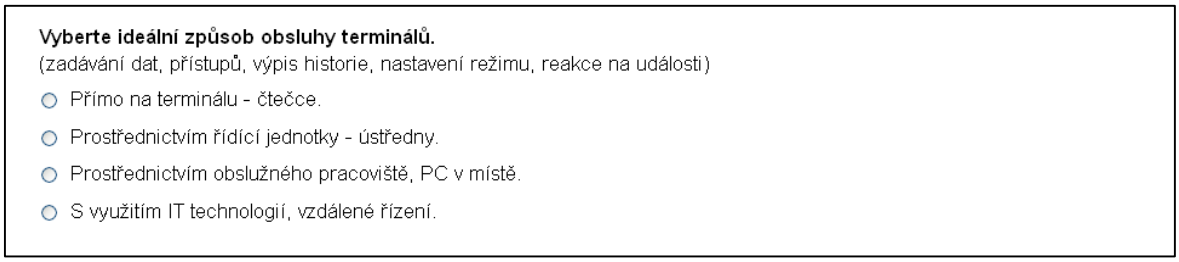
For. 4. Způsob identifikace

Množství, výběr a umístění prvků SKV je vždy individuální a záleží na konkrétních potřebách podniku. Potřeby malé obchodní firmy budou zcela odlišné od potřeb středně velkého výrobního podniku s velkou četností pohybu osob a zboží. Také pro zjištění velikosti přilehlých prostor, garáží a velikosti areálu bychom museli dotazník rozšířit. Výsledkem by bylo zpřesnění, jak rozsáhlý je potřebný systém. To pak určuje vhodnost použité topologie a architekturu sítě.



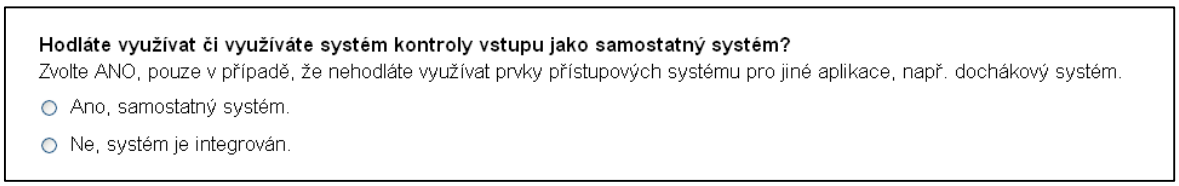
For. 5. Rozsah prostupů

Požadavek na způsob obsluhy terminálů jednoznačně určuje architekturu sítě, sofistikovanost a složitost systému. Je také měřítkem váhy, kterou dává podnikatel komfortu obsluhy.



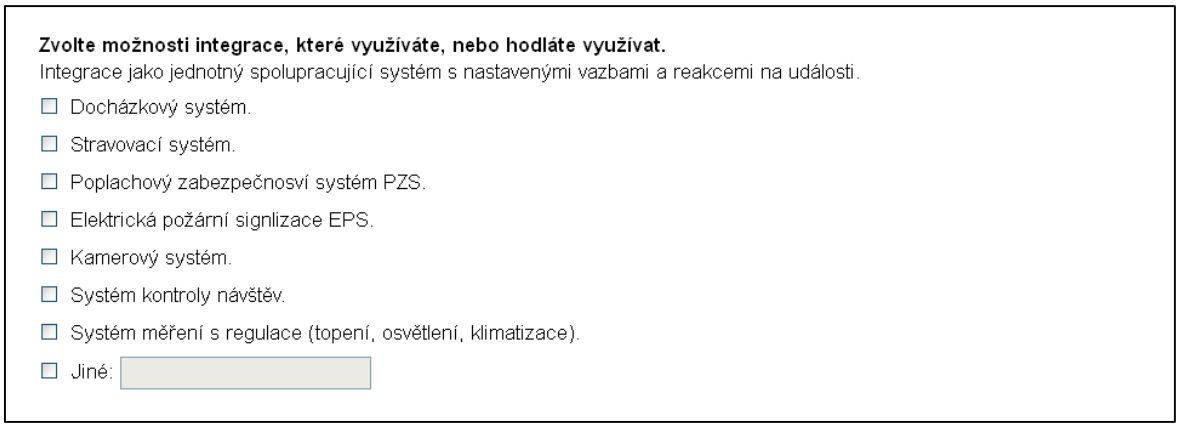
For. 6. Obsluha terminálu

Integrace systémů snižuje náklady na zavádění systémů, zvyšuje přehled a kontrolu nad systémem a tím i ochranu majetku, bezpečnost přítomných osob a zefektivňuje využívání existujících databází. Zvolená možnost sice vymezuje výběr použitých prvků, ale také odpovídá na otázku, je-li si podnik vědom výhod plynoucích z provázání systémů.



For. 7. Požadavek na integraci systému

Poslední otázka sledovala zájem o rozsah integrace. Propojení více systémů do jednoho sice zvyšuje míru efektivity, na druhé straně však klade zvýšené nároky na obsluhu, programové vybavení i použité komponenty, což systém opět prodražuje. Záleží i na tom, v jakém časovém měřítku jsou náklady posuzovány. Z odpovědí lze také odhadnout, kolik je firma ochotna do systému investovat nebo již investovala.



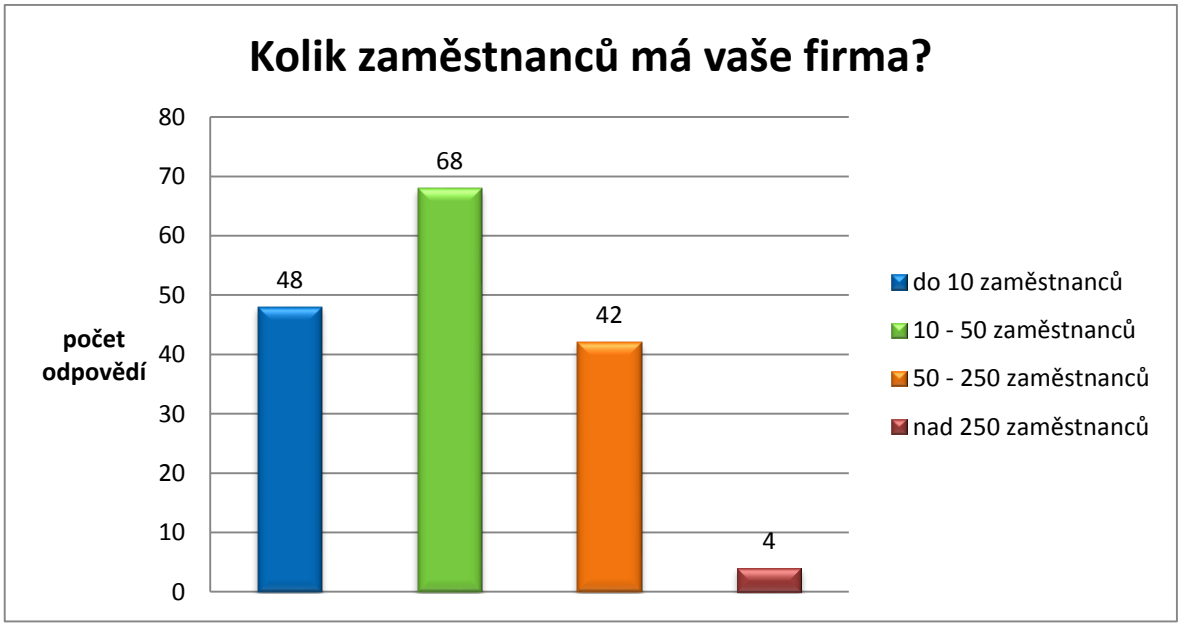
For. 8. Možnosti integrace systému

6.2 VÝSLEDKY DOTAZNÍKU

Na dotazník reagovalo celkem 162 podniků, což je z celkově oslovených 536 uspokojivé číslo. Bohužel 46, tedy celá čtvrtina dotazníků, byla vyplněna firmami spadajícími mimo cílovou skupinu dotazovaných.

Firmy s počtem pod 10 zaměstnanců jsou mikro firmou, kde zná každý každého. V takových firmách mají dobrý přehled o pohybujících se osobách, mohou velmi pružně reagovat na vzniklé situace. Hodnoty podniku jsou chráněny samostatnými prvky. Investovat finanční prostředky do systémů kontroly nevidí jako prioritu. Oproti tomu velké firmy s počtem zaměstnanců nad 250, řeší jednotlivé systémy jako spolupráci celých úseků odborně vyškolených pracovníků, jejich pohled a přístup je odlišný.

Z těchto důvodů byly tyto odpovědi mikro a velkých firem z výsledků vyloučeny. S ohledem na účelu dotazníku je však i zbylé číslo dostačující, a dává reálnou představu o potřebách firem v oblasti přístupových systémů.



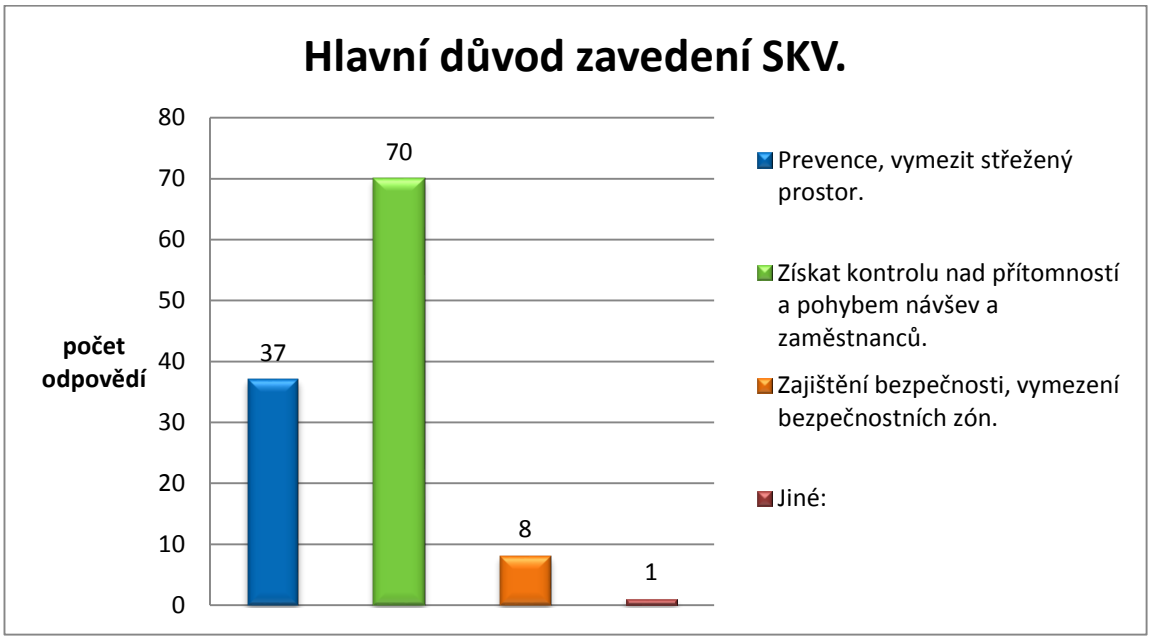
Graf 1. Zjištění velikosti firmy podle počtu zaměstnanců

Hlavním důvodem zavedení systému kontroly vstupů je získání kontroly nad přítomností a pohybem osob. Je pozitivní zjištění, že více jak polovina firem chce mít přehled, kdo se

v jejich podniku nachází, případně kde, a čím se zabývají jejich zaměstnanci. Je jim jasné, že prostým zavedení systému kontroly zvýší pracovní výkon svých zaměstnanců.

Další třetina ani tak nepotřebuje kontrolovat své zaměstnance a vidí v zavedení kontroly prevenci před nechtěnými návštěvníky.

Zajímavý je také údaj, že 5% dotazovaných vidí hlavní důvod pro zavedení systému bezpečnostní hledisko. Jsou to firmy, které jsou si vědomi svých hodnot a na zajišťování a zvyšování bezpečnosti firemního prostředí mají vyčleněny finanční prostředky. Pro instalační firmy jsou nejlepšími obchodními partnery.



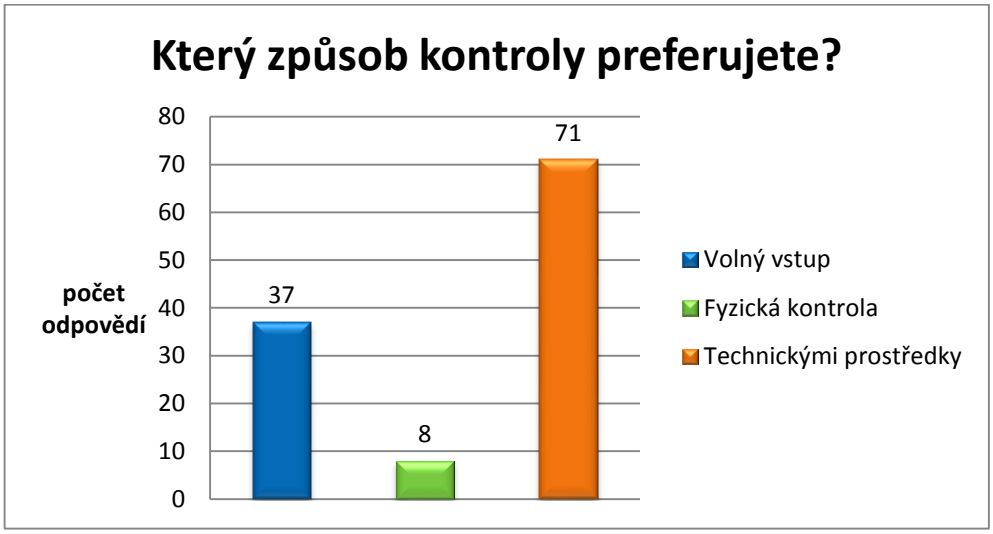
Graf 2. Důvod zavádění systému kontroly vstupů

Co se týče způsobu kontroly vstupu, využívá nebo hodlá využívat valná většina dotazovaných technických prostředků. Je to přirozené, technické prostředky jsou běžnou součástí našeho každodenního života, jejich obsluha je jednoduchá a pohodlná.

V kombinaci s fyzickou kontrolou nebo režimovými opatřeními by kontrolu vstupu řešila celá třetina dotazovaných. Z odpovědí vyplývá, že celá třetina se nespoléhá jen na technické prvky. Fyzickou kontrolu jako jediného způsobu kontroly přístupu neuvedl žádný dotazovaný.

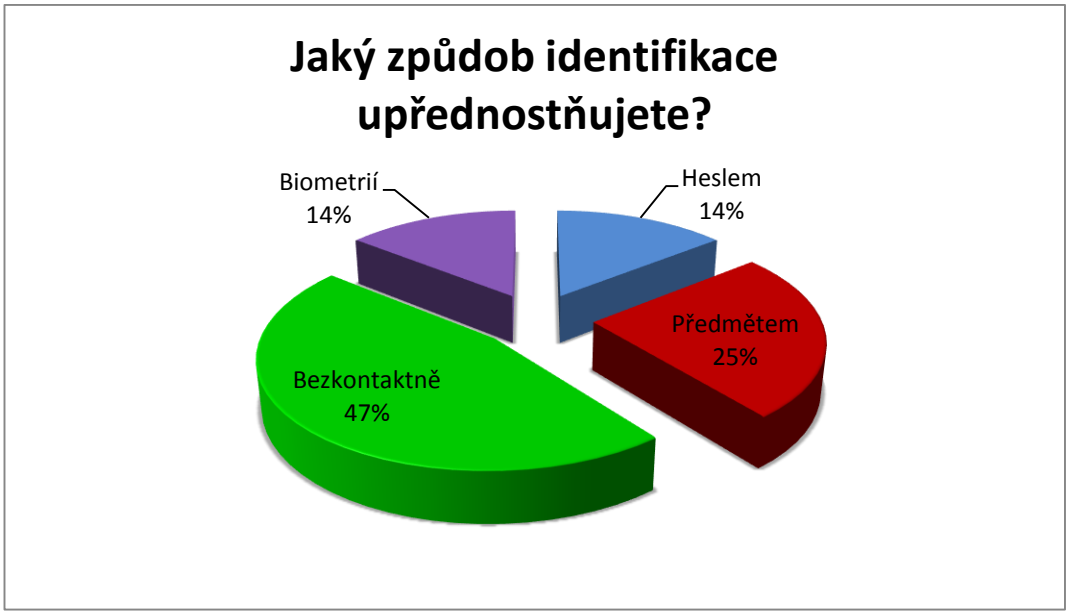
Zarážející je, počet odpovědí s volným vstupem. Osobně jsem očekávala použití režimových opatření jen v kombinaci s technickými prvky, jako u fyzické ostrahy, ale polovina odpovědí tohoto způsobu kontroly, tedy 15% z celkově dotázaných, by nechala

kontrolu vstupu pouze na režimových opatření. Jednalo se vždy o firmy do 50 zaměstnanců. Znamenalo by to, že tyto firmy kontrolu vstupu a pohyb návštěv a zaměstnanců neřeší, nebo jsou přesvědčeni, že ji nepotřebují a ochranu majetku řeší zřejmě tím, že poslední kóduje a zamyká. Jsou to ideální noví zákazníci. Dalším vysvětlením je prostě, nevhodně položená otázka, kdy mohla být uvedena možnost žádná opatření. Nebo neznalost terminologie, kdy může každý respektovat, že do pokladny může jen pokladní a jen ve vymezeném čase, jinak tomu brání speciální prvky, ale jako technické a režimové opatření to vnímáno není.



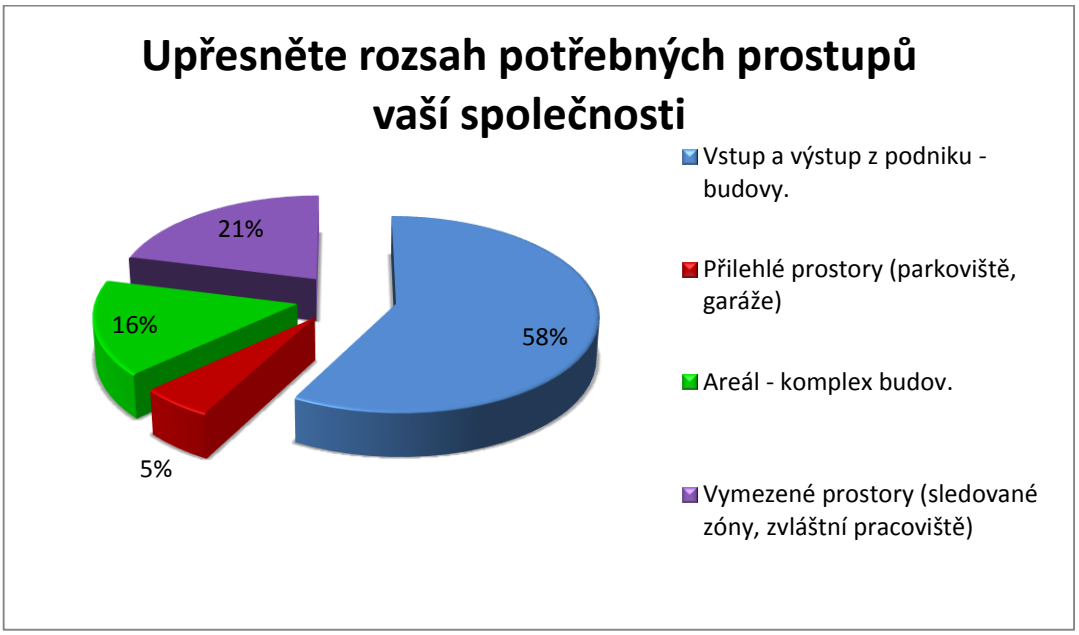
Graf 3. Preference způsobu kontroly

Z odpovědí bylo patrné, že ne všichni dotazovaní jsou si vědomi výhod a nevýhod jednotlivých metod identifikace, možnostech snímačů a využití identifikačních prvků. O tom svědčí i výsledek, že téměř polovina firem hodlá využívat bezkontaktní technologie, snad proto, že kontaktní způsob považuje za překonaný. Metody by zkombinovala necelá třetina, stejně jako v předchozím případě.



Graf 4. Způsob identifikace

Další otázky měla zjistit, jak velký prostor hodlá mít firma pod kontrolou. Necelých 60% se nemusí pouštět do rozsáhlejších instalací a složitých systémů, využije jen vstupy a výstupy budovy, dalších 20% zostří ještě kontrolu určených zón či prostor a zbylých 20% venkovní prostory.

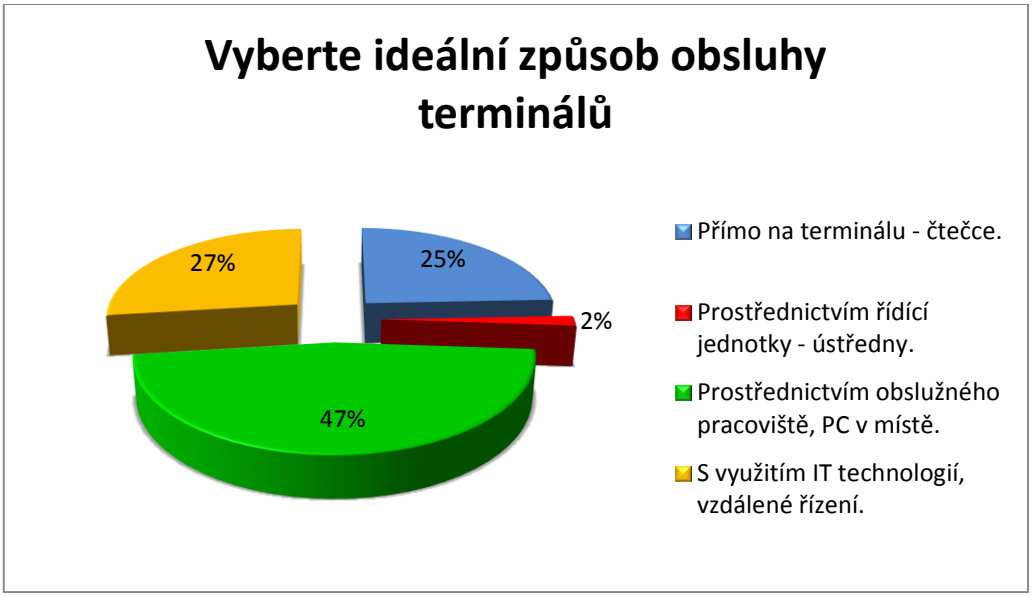


Graf 5. Rozsah prostupů

V návaznosti na předchozí odpovědi je třeba konstatovat, že i firmy s nižším stupněm ochrany nebo menším kontrolovaným prostorem s nižším počtem prvků v systému,

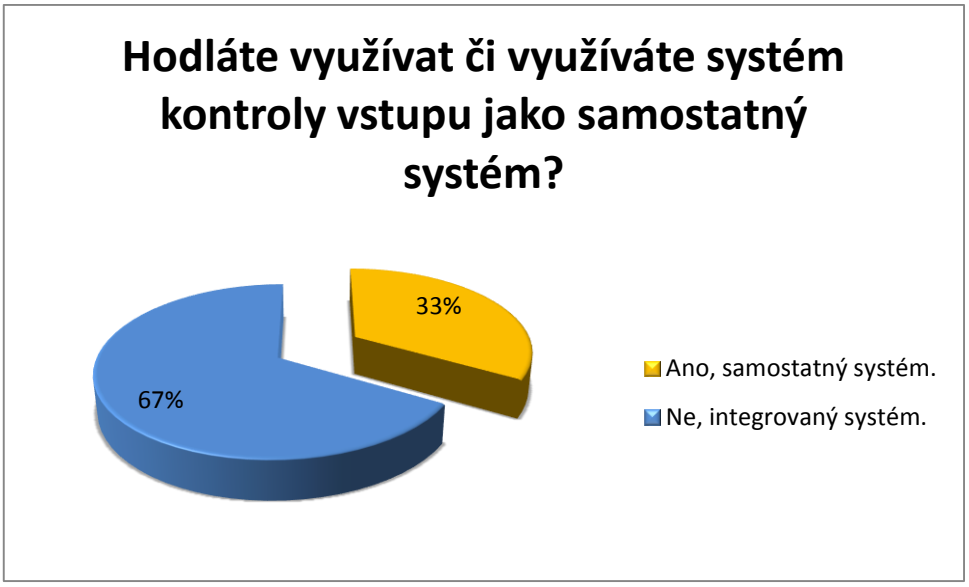
upřednostňují komfort obsluhy z jednoho centrálního místa, kde obsluha a kontrola zůstává uvnitř firmy bez možnosti nahlížet a obsluhovat vzdáleně.

K IT technologiím tíhne více jak čtvrtina dotazovaných. Což je v porovnání s průzkumem deníku.cz o využívání a investicích IT technologií malými a středními firmami, kde je hodnota na 3/4, nízké procento. Značí to o důvěře v jednoduchý stabilní snadno kontrolovatelný prověřený systém a to potvrzuje i zbylá čtvrtina, které vyhovuje obsluha na terminálu. Ukazuje na menší firmy se systémem s menším počtem prvků, pravděpodobně se stabilním prostředím, které již nesměřují k expanzi, a jednodušší systémy jsou pro ně dostačujícím řešením přístupu.



Graf 6. Obsluha terminálu

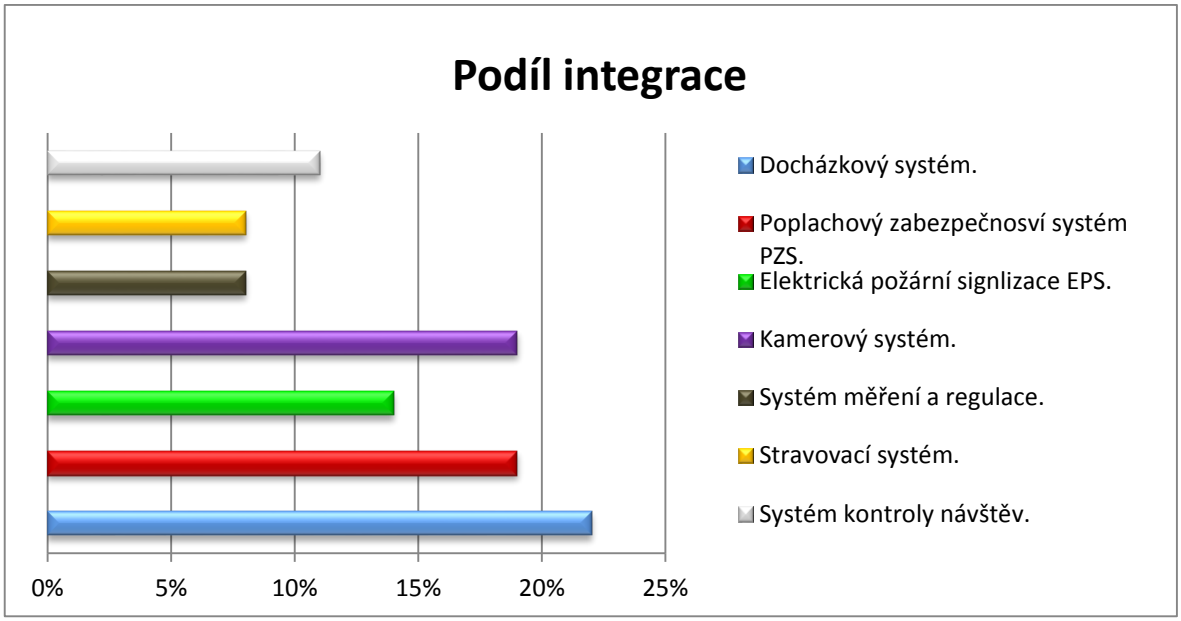
Provázaný systém kontroly vstupů s jinými by využily dvě třetiny dotazovaných. Tuto možnost zvolili všechny střední firmy. Třetina by systém kontroly vstupu řešila jako systém samostatný. To může být dáno nekompatibilností již zavedených systémů, nevědomostí výhod a možnostech instalace.



Graf 7. Požadavek na integraci systému

Graf možností integrace je vyhotoven jako podíl jednotlivých systému na integraci ve vztahu k přístupovým systémům. Systém kontroly vstupu by tedy činil 100%.

Z odpovědí je patrné, že pokud již firma využívá integraci, integruje více systému současně. Je očividné, že největší podíl integrace ve vztahu k přístupovým systémům má docházkový systém. Oba systémy mají k době blízko a často využívají shodných zařízení. Vysoké procento PZS, Kamerového systému i EPS ukazuje, na tendenci nahlížet na bezpečnostní situaci v podniku jako na soubor souvisejících činností, s komplexním řešením. Překvapením je nízké procento systémů měření a regulace, které jsou schopny velmi citelně zvýšit komfort uživatelů a snížit režijní náklady.



Graf 8. Podíl integrace

6.3 SHRNUTÍ POZNATKŮ Z DOTAZNÍKU

Z dotazníku vyplývá, že celá třetina firem bere bezpečnost a kontrolu nad systémy v podniku vážně a přistupuje k řešení problematiky systémově, efektivně a komplexně. Velký prostor zůstává pro objasnění principů, funkcí a možnosti využití identifikačních prvků. Integrace je také již běžným standardem a k ovládání systému je upřednostňováno centrálního PC v místě. Dotazník také odhalil, že existuje skupina firem, která nepřikládá systému kontroly vstupu velkou důležitost.

7 FUNKČNÍ POŽADAVKY NA PRVKY SKV

Systém kontroly vstupu je určen pro řízení, kontrolu a zpracování pohybů a přístupů osob, vozidel a zboží. Správná funkce systému je zajištěna prvky systému, kterými jsou identifikační média, čtečky, řídící jednotky, komunikační zařízení a převodníky komunikačních linek, výkonové prvky, napájecí zdroje, rozvody a je zastřešena počítači s potřebným programovým vybavením. Respektive jejich správným sestavením, propojením a nastavením. Jednotlivé prvky musí být tedy vybírány s ohledem na funkčnost celého systému. Projektanti a instalační firmy musí respektovat mimo funkční, také technické a systémové požadavky. Některé z nich předepisují či doporučují normy.

7.1 Legislativa

Vlastnosti kladené na systémy kontroly vstupu v bezpečnostních aplikacích jsou stanoveny v souboru norem ČSN EN 50133. Normy slouží zejména pro potřeby certifikace výrobků, nemají závazný charakter, stanovují především definice názvosloví a termínů, všeobecné funkční požadavky na systémy a komponenty, klasifikace stupně zabezpečení pomocí stanovení tříd identifikace a tříd přístupu. Uvádí definice a požadavky na třídy prostředí a třídy zařízení dle umístění, mechanické, atmosférické a elektrické zkoušky zařízení, požadavky na EMC, pokyny pro projektování, zřizování a provozování a požadavky na dokumentaci (prováděcí, provozní, pro údržbu, revize). [6]

7.1.1 Třídy identifikace

Třída identifikace 0 nepožaduje přímou identifikace, vstup je uskutečňován na základě prostého požadavku (tlačítko, kontakt, detektor pohybu), nebo jen namátkovou kontrolou dokladu či pověření prováděnou fyzickou ostrahou nebo vrátným.

Třída identifikace 1 je identifikace prováděná na základě dat uložených v paměti, pro přístup je požadováno heslo, nebo číslo zaměstnance, poměr počtu uživatelů k počtu všech kombinací kódu musí být alespoň 1:1000. Minimální počet kombinací 10000.

Třída identifikace 2 požaduje k identifikaci prvku či biometrie, k průchodu je potřeba identifikačního média (tokenu, čipu, karty) nebo je autentizace prováděna prostřednictvím biometrického prvku (otisk prstu, oční duhovka, 3D model obličeje.) Minimální počet

kombinací 1 mil., jednoznačná identita uživatele, chybovost max. 0,01%. Identifikační číslo prvku nesmí být přímo zobrazeno.

Třída identifikace 3 kombinuje třídu 1 a 2, požaduje jednoznačný token nebo otisk prstu spolu s heslem, alespoň kombinace tříd 1 a 2

7.1.2 Třídy přístup

Třída přístupu A - pro přístupové místo není vyžadován časový filtr ani ukládání přístupových transakcí.

Třída přístupu B - přístupové místo má funkci časových filtru a ukládání dat.

Všechny prvky přístupových systémů však musejí splňovat požadavky na elektrickou bezpečnost (ČSN EN 60950, ČSN EN 60065), elektromagnetickou kompatibilitu (EMC) a odolnost (ČSN EN 61000, ČSN EN 55022, ČSN EN 50082, ČNS EN 50130), případně požadavky telekomunikačních norem (např. ČSN EN 50529), v případě integrace s jinými systémy také ČSN CLC/TS 50398. U prvků přístupových systémů musí být také samozřejmě prokázána shoda dle zákona 2297 Sb. a nařízení vlády 17/2003 Sb. o technických požadavcích na výrobky NN a 616/2006Sb. o EMC kompatibilitě. Požadavky na mechanické prvky přístupových systémů (otvírače, dveře, brány, turnikety…) jsou uvedeny ve standardu Evropské komise CEN/TS 33. Národní bezpečnostní úřad (NBÚ) vydal pro potřeby přístupových systémů a objektové bezpečnosti vyhlášku č. 339/99 Sb. Souhrn zde uvedených norem, zákonů a vyhlášek není zdaleka vyčerpávající, není předmětem tohoto materiálu. [12]

7.2 Požadavky na prvky

Základní funkční požadavky na prvky systému jako je bezporuchovost, spolehlivost, bezpečnost jsou dány normou a uživatel je bere jako samozřejmost. Další požadavky jako je třída přístupu a třída identifikace rozlišuje ve chvíli, kdy se ho tento požadavek dotýká, většinou požaduje pojišťovna. Jsou zde ale další požadavky, na hlášení a komunikaci či zpracování dat.

Bezporuchovost - schopnost zařízení plnit požadovanou funkci po stanovenou dobu, nebo za definovaných podmínek.

Udržovatelnost – schopnost zařízení setrvat ve stavu, v němž může plnit požadovanou funkci za předpokladu pravidelné údržby.

Spolehlivost – schopnost zařízení pracovat za ztížených podmínek.

Bezpečnost – vlastnost zařízení neohrožovat lidské zdraví nebo životní prostředí při plnění své funkce.

Umístění do příslušného prostředí – každé jednotlivé zařízení je schopno správně fungovat v definovaném prostředí. (venkovní, vnitřní, prašné, výbušné)

Signalizace – schopnost signalizovat nebo zobrazovat stav, ve kterém se nachází (porucha, sabotáž, proběhlou operaci apod.)

Komunikace a připojení – schopnost zařízení komunikovat s jinými, akceptovat povely, přijímat a vysílat stavová hlášení a reagovat na ně definovaným způsobem.

Sběr dat – schopnost zařízení uchovávat data, či historii událostí.

7.3 Požadavky na systém

Funkční požadavky na systém jsou stanoveny společně pro třídu přístupu A i B. Udávají časy hlášení, dobu archivace událostí, signalizaci na stav, zásah apod.

Zpracování – v případě, že jsou postupy zpracování uloženy ve snímači místa přístupu a jsou nastavení viditelná, případně je možné vyměnit jednotku bez účasti správce systému, musí dokumentace uvádět, že tento výrobek je vhodný pro použití na hranicích přístupového pásma s nižším stupněm bezpečnosti. Musí existovat možnost přiřadit uživateli časový filtr. U postupů musí být možno definovat minimálně dva časové úseky uvolnění (jeden 5 sekund a druhý 60 sekund), a dva povolené časové úseky otevření výstupního ovládacího prvku (jeden 10 sekund a druhý 60 sekund). Dalším požadavkem je uchovávání naprogramovaných přístupových postupů nejméně po dobu 120hod. po výpadku napětí u automaticky se restartujících systémů. Pro třídu identifikace 1 platí, že u systému, který využívá informaci uloženou v paměti, nesmí být možné po sekvenci 5 za sebou nesprávně zadaných informací umožněn přístup dříve než po 5 minutách. Pro třídu identifikace 3, že systém, který používá kombinaci identifikačního prvku (tokenu) nebo biometrie a informace uložené v paměti, musí vyslat výstrahu po 5 sekvencích za sebou nesprávně zadaných informací při stejném identifikačním prvku nebo biometrii.

Napájení – požadavek na zajištění vstupu**,** při připojení nebo odpojení napájení nesmí dojít k jeho chybnému uvolnění. Napájení výstupního ovládacího prvku systémem kontroly vstupu požadováno není.

Ochrana programování – požadavek na ochranu neoprávněný změn předvolených postupů zabezpečovacími prostředky. Poměr počtu různých kombinací kódu k počtu oprávněných osob musí být nejméně 1000:1, minimální počet kombinací musí být 10000, správce systému musí mít možnost změnit tento přístupový kód.

Ovládání míst přístupu – prvky systému musí být vybaveny rozhraním ke spojení s řídící jednotkou. Rozhraní musí zahrnovat ovládání a monitorování stavu zabezpečení. Svorkovnice rozhraní místa přístupu musí být umístěna uvnitř skříňky. Ta musí při otevření normálním způsobem detekovat sabotáž. Nesmí být možno získat přistup (při dodržení pokynů výrobce), ze strany s nižších úrovní zabezpečen. Systém kontroly vstupů musí monitorovat stav výstupního ovládacího prvku, zda je nebo není prvek uzavřen. Ovládací výstup rozhraní místa přístupu musí být sepnut, pokud je přístup povolen, a musí být zrušen, pokud uběhl předvolený časový úsek uvolnění výstupního ovládacího prvku, nebo pokud monitorování výstupního ovládacího prvku indikuje, že je otevřen.

Hlášení – přístupový systém musí mít prostředky pro hlášení ve formě výstrahy a zobrazení událostí tykající se detekce sabotáže, nastane-li situace, že je místo přístupu otevřeno bez poskytnutí přístupu, nebo proběhlo otevření místa přístupu po uplynutí povolené periody pro poskytnutí přístupu. Zpoždění, každé požadované výstrahy, může být maximálně 10 sekund.

Komunikace s jinými systémy - každé místo přístupu systému kontroly vstupu musí mít výstup, který avizuje okamžik oprávněného přístupu. Pokud je tímto výstupem binární spínač, musí být galvanicky oddělen a sepnut při poskytnutí přístupu a rozepnut, když nastane jedna z následujících událostí:

- místo přístupu je otevřeno a zavřeno,
- povolená doba pro uvolnění výstupního ovládacího prvku uběhla a nedošlo k otevření místa přístupu,
- místo přístupu zůstalo otevřené i po uběhnutí povolené doby pro otevření.

Pokud jsou pro tento výstup použity alternativní prostředky, musí poskytovat stejné logické informace. Pokud připojené systémy mají vybavení pro změny postupů daného systému kontroly vstupů, potom musí splňovat požadavky ochrany programování. Připojením nebo odpojením komunikačních linek nesmí dojít k poskytnutí přístupu. [5]

Vnitřní zabezpečení - neoprávněná osoba nesmí mít možnost bez použití nástrojů si zajistit přístup, platí pro třídy identifikace 1 až 3. [6]

7.3.1 Základní funkce z pohledu zákazníka

Při prezentaci komplexního systému kontroly vstupů jsou zákazníku nabízeny základní a nadstandardní funkce systému, podle kterých se rozhoduje.

Identifikace – je základní funkcí přístupového systému, rozpoznat žadatele, porovnat vzorek s databází a vyhodnotit oprávněnost vstupu

Zpracování dat – jednak jsou zpracovávána data v samotné čtečce při autentizaci, jednak jsou shromažďována data o jednotlivých událostech a ty archivována ať už na terminálu nebo v řídící jednotce. Ty pak mohou být dále využívána.

Ovládání přístupového místa – zákazník rozlišuje způsob ovládání přístupového místa, tedy možnosti přímo na terminálu, na řídící jednotce či ústředně, nebo centrálně prostřednictví počítačové aplikace.

Programovatelnost – schopnost zařízení nastavit režim dle požadavků zákazníka. Programovat můžeme z přístupového místa. U jednotlivých prvků se rozsah možností programovatelnosti může značně lišit.

Stavová hlášení – zpráva prvku systému o jeho stavu, otevřeno, zavřeno, alarm, porucha. Toto hlášení podává prvek v pravidelných intervalech, při změně stavu, nebo na vyžádání. Dle těchto hlášení pak reagují další prvky, nebo celý systém. Hlášení stavu je doprovázeno signalizací na prvku samotném a na centrální ovládací jednotce.

Styk s uživatelem – jedná se o komunikaci s uživatelem (autentizovanou osobou), zařízení dává opticky nebo akusticky najevo svou připravenost k úkonu, nebo reakci na identifikaci.

Napájení – systému nebo jednoho přístupového místa, může se u jednotlivých zařízení lišit.

Samoochrana – ochrana proti sabotáži, neoprávněné manipulaci, zjištění dat apod.

Definování přístupových bodů a zón – pro správnou funkci musíme definovat kontrolované místo vstupu a zóny, tedy množinu snímačů definující vstupy do určité oblasti.

Definování přístupů - množin identifikačních karet i s případným organizačním rozdělením (stromová organizační struktura i s právy na jednotlivá střediska)

Definování práv - jednotlivých ID karet pro vstup do zóny (časová práva vstupu se definují v rámci dne a týdne)

Zpřístupnění aktuálních stavů systému - kde se která identifikační karta, nebo osoba nachází, stav zařízení, signalizace alarmových stavů za pomocí monitorovacích úloh
definice a vyhodnocení nátlakových kódů (tajný alarm)
Funkce sledování překročení doby nutné k zavření dveří, kontrola otevření dveří jiným způsobem než identifikační kartou
Definice různých úrovní alarmových stavů systému (zejména z hlediska jejich vyhodnocování a potvrzování)
kontrola a signalizace stavů dveří

7.3.2 Speciální funkce

Antipassback -Funkce antipassback zabezpečuje kontrolu násobných průchodů. Osoba s kartou nemůže podruhé vejít do určitého prostoru, aniž by z něj odešla a opačně – nemůže odejít, aniž by vešla. Antipassbackem kontrolované průchozí místo, musí být vždy opatřeno z obou stran - na vstupu i na výstupu snímacím zařízením (celým snímačem nebo snímací hlavou). Systém zahrnuje dvě možnosti kontroly antipassbacku:

- antipassback časový lokální pro jeden snímač
- antipassback globální pro více snímačů

Dveře mohou být osazeny z každé strany snímačem nebo tlačítkem pro evidenci průchodů. Samotný průchod použitím tlačítka lze evidovat jako „volný průchod“ (bez určení karty). Snímač při přiložení karty s příslušnými oprávněními a případného zadání PIN spíná relé pro otevření dveří. V rámci systému ACCESS je možno nastavit způsob odesílání dat o události:

- ihned po sepnutí relé – v rámci této varianty nemusí být připojen dveřní kontakt a stačí jednodušší verze turniketu (bez rozlišení směru otáčení), data jsou po sepnutí relé ihned odesílána do komunikačního klienta.
- až po skutečném průchodu (po otevření dveří nebo protočení turniketu), v tomto případě musí být zapojen a na snímači povolen dveřní kontakt nebo výstup z turniketu pro rozlišení směru otáčení. Dále se tato funkce musí povolit v rámci nastavení snímače, a pak jsou data odeslána až po skutečném průchodu.

Funkce pásmová propust (Interlock) - do prostoru interlock - pásmové, komorové propusti je možno vstoupit některými z dveří, pouze pokud se ve vnitřním prostoru interlocku nikdo nenachází. V tom případě jsou vnitřní snímače blokovány a vnější

povoleny. V případě blokování snímač kartu vůbec nečte, je jednotkou interlocku skutečně blokován. Opačně to platí také – pokud se někdo ve vnitřním prostoru interlocku nachází – jsou povoleny pouze vnitřní snímače a venkovní jsou blokovány. [8]

8 KRITÉRIA SKV

Měřítka, podle kterých se podnik rozhoduje, kterému z přístupových systému dát přednost a jakými prvky bude vybaven je celá řada. Výsledek je ale vždy kompromisem více kritérií.

Bezpečnostní hledisko – při výběru přístupového systému musí být brán vždy zřetel na konkrétní situaci. Posoudit nejen požadavky, ale zejména potřeby podniku, jaké jsou jeho vnitřní i vnější bezpečnostní situaci. Provést bezpečnostní analýzu a teprve na základě ní provádět návrh. Instalací vhodného přístupového systému získá firma zvýšený přehled o bezpečnostní situaci v objektu, o pohybu přítomných osob. Dostupnost a množství potřebných informací ať už v textové podobě, obrazové, nebo vizualizovaná podoba grafické programové nadstavby usnadňuje řešení nenadálých nebo krizových situací, rychlá odezva na tyto situace či stavy často zabraňuje ztrátám či vysokým škodám na majetku firmy, zvyšuje efektivitu zásahu či evakuace. V neposlední řadě také odradí případné narušitele nebo nechtěné návštěvníky.

Funkce a vazby – je potřeba definovat nároky na jednotlivé přístupové body a dle toho vybírat jednotlivé prvky, definovat vzájemné vazby mezi přístupovými body i chování systému jako celku. U integrovaných systémů je nutné nastavit vzájemné vazby jednotlivých systémů nebo prvků systému, reakce na události, priority hlášení, signalizace a chování systémů v definovaných stavech a respektovat požadavky a norem. Zohledňovat je třeba také případný stávající systém i budoucí výhled. Tj. definovat potřeby podniku, chování systému, nastavení práv - kdo se má dostat kam a kdy a jak má systém reagovat, když to tak není.

Ekonomická náročnost – pohled na hledisko ekonomické náročnosti je odvislý od období, ke kterému je vztaženo. Návratnost se počítá v střednědobém horizontu do 5 let. Ale ne vždy je možné veškeré ukazatele převést na finanční jednotky. Poměr investice také můžeme vztáhnout k hodnotě chráněného majetku, podobně jako u pojištění. Ziskem investovaných prostředků je především úspora mzdových nákladů ve srovnání s fyzickou ostrahou, v případě integrace se úspora rozšiřuje o snížení pořizovacích nákladů samostatného systému, snížení energetických nákladů, optimalizace využívání technologií, úspora času – pracovní doby zaměstnance, vždy ve vazbě na příslušnou integraci.

Legislativní požadavky – jedná se o požadavky technických norem, při integraci norem EPS, PZS, chování systému v krizových situacích, evakuace, požadavek při použití

osobních údajů zaměstnanců (na přistup k informacím a uchovávání citlivých dat), případně požadavek v případě, že se jedná o část kritické infrastruktury, nebo strategický objekt.

Individuální požadavky uživatele – jedná se zejména o požadavky nad rámec bezpečnostního standardu, požadavky, které nevyžaduje ani povaha podniku, ani bezpečnostní stav okolí (např. posedlost IT technologiemi).

Význam, výhody, přínos – krom výhod ekonomických, můžeme posuzovat i výhody technické jako zjednodušení činnosti obsluhy, efektivnější řešení událostí a využívání dat, zvýšená rychlost reakcí na podněty, přehled o stavu podniku a zvýšení komfortu a kultury pracovního prostředí. Držet krok s novými technologiemi také zvyšuje prestiž podniku a je odrazem filozofie jejího přístupu a může být v tomto ohledu ziskem.

Estetická kritéria – vzhled jednotlivých prvků je také kritériem výběru a souvisí s firemní kulturou a prestiží, ne nadarmo terminály navrhují přední designerské firmy.

8.1 KRITÉRIA ARCHITEKTURY SÍTĚ

Pro podniky s nízkými nároky na bezpečnost či nízkou četností pohybu osob využívajících autonomní systémy, kde je obsahem přístupového systému vstup a výstup z podniku případně pokladní místnost nemůže být o architektuře sítě ani řeč.

Taktéž tomu je u modulárních systémů, který je schopen pojmout větší množství přístupových bodů s více řídícími jednotkami, kde centrálním bodem je ústředna nebo PC, ovšem komunikace probíhá po nejčastěji po sběrnici RS-485, což je komunikační standard, kde komunikace neprobíhá ve vrstvách a jako taková má své limity. Nízká komunikační rychlost, omezená velikost přenášených dat, komunikační vzdálenost do vzdálenost 1200 metrů, při velkém počtu prvků klesá spolehlivost.

Síťová komunikace je komunikace po síti, která probíhá ve vrstvách, tyto vrstvy jsou rozděleny podle důležitosti činností, které jsou při řízení komunikace vykonávány. Každá vrstva sítě je definována službou, která je poskytována vyšší sousední vrstvě, a funkcemi, které vykonává v rámci protokolu. Řízení komunikace protokoly, ty jsou tedy tvořeny souhrnem pravidel, formátů a procedur, které určují výměnu údajů mezi dvěma či více komunikujícími prvky. Užívanou skupinou protokolů jsou protokoly TCP/IP, využívá čtyř vrstev. Z těchto čtyř vrstev protokoly TCP/IP "obsazují" jen tři nejvyšší. U nejnižší vrstvy – vrstvy síťového rozhraní se počítá s tím, že zde budou využity takové přenosové

mechanismy, jaké jsou k dispozici, a které "pochází odjinud" tj. nejsou součástí TCP/IP. Může jít třeba o Ethernet, Wi-Fi, ADSL atd. Komunikace po síti je tedy rychlá a velkoobjemová data, jako jsou například biometrické údaje, nejsou problémem.

Architekturu sítě známe jednovrstvou, dvouvrstvou a vícevrstvou. Odpovídá účelu a typu sítě, technologickým a finančním možnostem, počtu uživatelů sdílejících informace a typu zpracovávaných informací. U přístupových systémů je používá třívrstvá architektura, která odděluje vrstvu uživatelského prostředí využívanou čtečkami a dalším hardwarem, vrstvu aplikace a vrstvu databáze – SQL server.

Měřítkem výběru je tedy konkrétní situace objednatele, jeho požadavky na systém, prvky, funkce a integraci, podle které se vybírá adekvátnost topologie. Pokud je požadavkem zákazníka ovládání byť propojení slaboproudých systémů rozsáhlejšího systému s centrálního místa v podniku, s obsluhou prostřednictvím samostatných aplikací, bude spokojen s modulárním systémem na sběrnici. Je-li však jeho požadavkem ovládání prostřednictvím vizualizačního softwaru, vybudujeme systém na síťové architektuře.

8.2 NASTAVENÍ PRÁV

Systém kontroly vstupu, přebírá funkci zabezpečení objektu v době, kdy je PZS odblokován. Prostřednictvím přístupových bodů registruje a reguluje, přítomnost osob. Tedy kdo, kdy, na jak dlouho, případně co využívá. Takové definici pak říkáme přístupové právo. Jedná se o balíček oprávnění k průchodu či úkonům. Oprávnění je realizováno prostřednictvím identifikačního média. Identifikační médium je v podstatě náhražkou klíče. Nastavení je prováděno centrálně a zahrnují následující soubory definic:

Omezení přístupu - omezení přístupu nepovolaných osob do určitých prostor. V objektu jsou definované zóny ohraničené překážkou s prostupem, který je přístupovým bodem. Do tohoto prostoru zóny pak osoba má či nemá přístup. (sklady, výpočetní centra, školicí místnost, kanceláře, nebezpečné provozy, utajované provozy, ochrana know – how)

Časové omezení - vymezení přístupu mimo definované časové úseky (pokladní hodiny, směnný provoz, úklid, zásobování), časové omezení může být rozšířeno na sledování doby pobytu.

Přístupová práva se vystavují konkrétním osobám, na základě stupňů oprávnění podle prostorových, časových, personálních a jiných dispozic. Osoba je reprezentována přiděleným identifikačním médiem. Někdy je vhodné vytvořit šablonu oprávnění, kdy jsou

definována práva na celou skupinu osob. I ty lze pak individuálně upravovat. Obecně existují 3 základní šablony uživatelů:

Administrátoři – oprávněné osoby, které mohou zasahovat do systému, jejich ID je akceptovány všemi prvky systému.

Standardní uživatelé – standardní zaměstnanec, jeho práva jsou omezena na běžné pracovní prostředí, jejich ID jsou známy jen u povolených prostupů, ostatní je zamítá.

Návštěvy – jejich práva jsou omezena na veřejná prostranství či návštěvní místnost, jejich ID jsou známy jen povoleným prostupům.

8.2.1 Zásady nastavení oprávnění

Než se začnou nastavovat oprávnění, je potřeba naplánovat a ujasnit systém rolí a oprávnění ve firmě. Správně navržený systém oprávnění ušetří čas potřebný pro nastavení a budoucí správu uživatelů. Je doporučeno dodržovat následující zásady:

Preference skupin před uživatelem – jde o sestavení seznamu pracovních pozic (rolí) uživatelů. Pro každou pozici je založena skupina a jednotliví uživatelé jsou do těchto skupin zařazeni. Při nástupu nového zaměstnance je jednodušší zařadit jej do příslušné skupiny (nebo skupin) a tím mu jedním krokem přiřadit příslušná oprávnění.

Oprávnění uživatele výjimkou - oprávnění pro uživatele je vhodné používejte pouze pro řešení výjimek. Je třeba si uvědomit, že jeden uživatel může být členem více skupin. Oprávnění se v tom případě kombinují.

Co není nastaveno je povoleno – pokud je třeba omezovat přístup k některému objektu, nebo zóně, je lepší nenastavovat pro něj žádná oprávnění. Nastavovat oprávnění ke každému jednotlivému vstupu, je ztráta času. Necháme-li oprávnění nenastavené, rozumí se, že přístup je povolen v plném rozsahu.

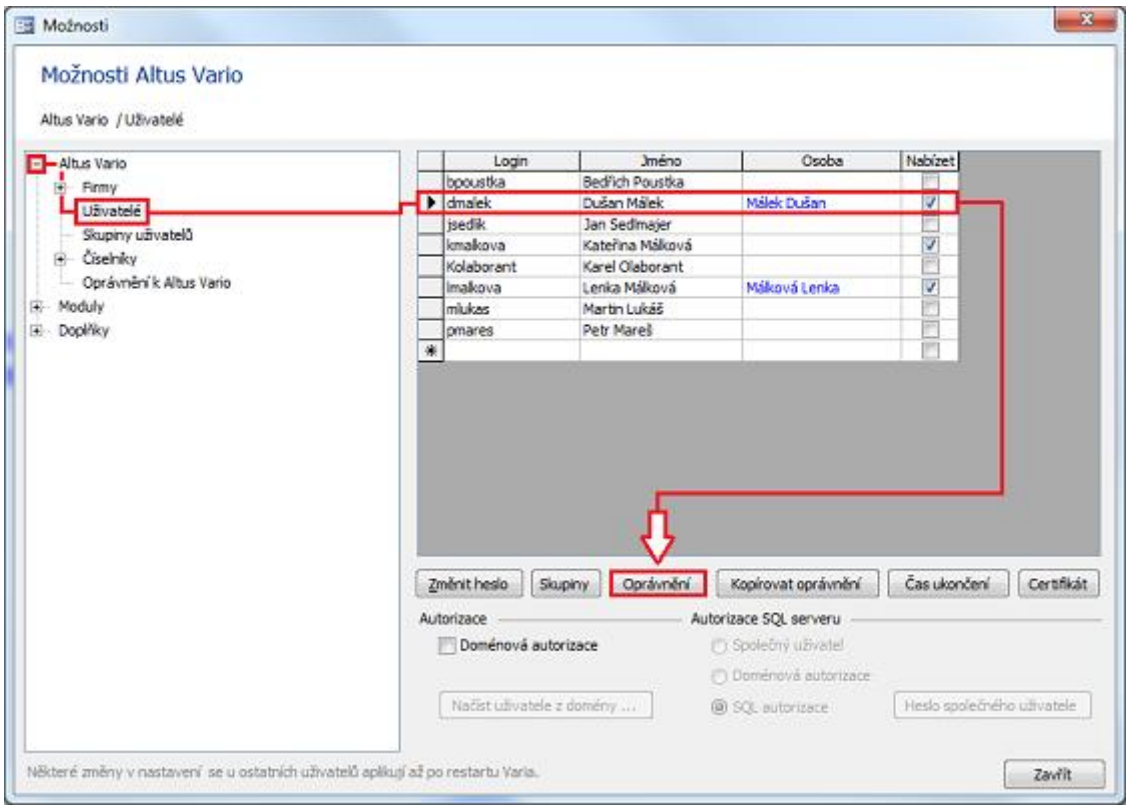
Co je povoleno není třeba zakazovat – odepření oprávnění je vhodné používat výjimečně. Jakmile u objektu nastavíte jakékoli oprávnění, mají k němu pouze přístup uživatelé s nastaveným oprávněním. Kdo nemá oprávněním explicitně povolený přístup, má jej automaticky odepřený. Definovat proto skupině právo přístupu a zároveň jiné skupině odepření, je ztrátou času.

Zásada říká „co není nastaveno, je povoleno“ a pak platí, že „co je nastaveno, je zakázáno“.

Odepření je vhodné pouze, pokud chceme individuálně odepřít některou z položek uživateli, který má tuto položku povolenou členstvím ve skupině (nový neproškolený zaměstnanec).

Oprávnění stačí nastavit na jednom místě - je jednodušší definovat přístup k celému modulu než k jednotlivým agendám. V případě, že nastavíme oprávnění k modulu nebo agendě, nemusíme již definovat oprávnění k jednotlivým knihám dané agendy – uživatel se ke knihám nedostane. [13]

Pokud potřebujete nastavit oprávnění k jednotlivým knihám agendy, nemusíte definovat oprávnění k agendě - bez oprávnění ke knize agendu uživatel neotevře.



Obr. 21. Definice oprávnění uživatele nebo skupiny systému Altu Vario [13]

8.3 DEFINICE STAVŮ

Podstatným krokem úspěšné funkce systému kontroly je definování stavů systému. Jednak reakce systému na jednotlivá stavová hlášení (otevřeno, zavřeno, porucha, sabotáž) jednotlivých prvků systému, jednak chování systému jako celku. Tedy „Co se má stát když…“.

Zásadní věcí je nastavení chování systému v krizových situacích, haváriích a při vyhlášení poplachu. Jedná se o stavy, kdy může být přímo ohrožen život a zdraví přítomných osob, pak jsou oprávnění stranou a je nutné zpřístupnit všechny únikové cesty a přístup k prostředkům potřebným pro zásah.

Centrální řídící jednotka přijímá stavová hlášení z modulů systému, nebo z konkrétních prvků systému a aktuálním stavu, nebo o proběhlé události. Těmto informacím se říká stavová hlášení, jsou reprezentovány stavovým kódem (pokud jsou přijímány v datové podobě, nebo se jedná o sekvenci napěťových poměrů na vodiči). Stavové kódy zastupují předdefinované informace o stravu jednotky (otevřené dveře). Centrální jednotka seřazuje jednotlivá hlášení podle priority, vyhodnocuje je a dává povel k akci, některé stavy nejsou následovány akcí, jsou pouze registrovány a archivovány. Priorita je přiřazována také akčním povelům. Hlášení stavu je doprovázeno signalizací na prvku samotném i na centrální ovládací jednotce.

Stav klid – jedná se o stav, prvek je připraven k akci.

Stav sabotáž – prvek registruje pokus o neoprávněnou manipulaci.

Stav porucha – ji vyhodnocena nesprávná funkce prvku

Stav alarm – signalizuje pokus o neoprávněný vstup (definovat lze různé úrovně alarmových stavů)

Stav akce – prvek vykonává operaci, ke které je určen

Tajný alarm – vyhodnocení nátlakových akcí

Funkce sledování překročení doby nutné k zavření dveří,

Kontrola otevření dveří jiným způsobem než identifikační kartou

8.4 INTEGRACE

Při posuzování měřítka integrace je rozhodující zda klient již nějaký systém má a zda jej hodlá zachovat v plné šíři. Poté se zjišťují možnosti integrace, které jsou závislé na použitých prvcích, vedení a topologii. Pro rozšiřování systému není problém použít zesilovačů vedení, nebo převodníků komunikace, případně použít bezdrátové technologie. Primárním hlediskem je správná, bezpečná funkce systému s komfortní obsluhou.

Integrace je realizována prostřednictvím propojení:

Technologií - jednotlivých bezpečnostních systémů, CCTV, EPS, EZS, docházkového systému, systému měření a regulace.

Funkcí - funkcí přístupových karet (karta může být použita ke vstupu, chodu strojního zařízení i nákupu z automatu)

Uživatelského rozhraní – zastupuje sdružené ovládání aplikací, ovládacích panelů, aplikací z různých míst (mobilní telefony)

Datová – propojení s využíváním společné databáze

Metodická – nestavení metodiky registrace, evidence, blokace, časový filtr (režimová opatření).

Propojit můžeme tedy prvky, data, rozhraní, nebo také vše najednou podle aktuální potřeby zákazníka. Ideálně prvky sytému kontroly přístupu pro docházkové systémy, přístupová média pro stravovací systém, poplachový a zabezpečovací systém v rámci ovládání prostupů, elektrickou požární signalizaci v rámci evakuace, respektive EPS ovládá SKV při evakuaci, kamerový systém k zobrazení míst přístupu a měření a regulaci ke zvýšení komfortu a snížení režijních nákladů. Jak již bylo popsáno výše.

9 PŘÍSTUPOVÝ SYSTÉM U MODELOVÉHO OBJEKTU

9.1 CHARAKTERISTIKA OBJEKTU

Budova se nachází v okrajové části města v sousedství sídliště a je součástí areálu komerčních objektů a skladových hal. Areál je přístupný veřejnosti do 5 do 20hod. Přízemí není obsazeno, jeho prostory jsou určeny k pronájmu. V prvním patře zabezpečovaného objektu se nachází 12 kanceláří, účtárna s pokladnou a zasedací místnost. Kanceláře jsou vybaveny osobními počítači a další drobnou elektronikou. Zasedací místnost je přizpůsobena k poradám, prezentacím a školení zaměstnanců a je vybavena potřebnou výpočetní technikou.

Obr. 22. Zabezpečovaný objekt

Zabezpečení se provádí z důvodu omezení pohybu nepovolaných osob v objektu, v souvislosti s ochranou dat v psané i elektronické podobě, ochranou drobného hmotného majetku, výpočetní techniky před zcizením i ochraně firemního know – how. Pracovní činnost zde vykonává 36 osob. Pracovní doba je volná od 6:30 do 16:30 hodin v pracovní dyn pondělí až pátek. Do budovy je vstup volný, do prostoru obsazeného firmou je vstup vstupními dveřmi osazenými před schodištěm. Místem zabezpečení jsou vstupní dveře, serverová místnost, místnost pokladny a zasedací místnost.

9.2 POUŽITÉ KOMPONENTY

Pro zabezpečení jsem použila produkty firmy cominfo. Systém je řešen jako modulární identifikační systém s ohledem na požadavek zákazníka v krátkém časovém horizontu rozšířit použití dalších modulů (prodejní sklad).

Identifikace je řešena použitím identifikační karty v kombinaci s číselným kódem, tedy informace uložené v paměti. Jde o zabezpečení ve třídě identifikace 3. Třída přístupu je B. Použité komponenty:

Řídící jednotka

Identifikační terminál REA TOUCH

Tento přístupový bod slouží zároveň jako terminál kontroly docházky. Terminál má dotykovou obrazovku.

Obr. 23. Identifikační terminál REAL TOUCH [8]

Elektromechanický úzký zámek ABLOY EL560

Jakmile se dveře uzavřou, zámek automaticky uzamkne, vysune se závora, střelka se zablokuje. Stisknutím aktivované nebo panikové kliky je závora zatažena do těla zámku a následně odblokována střelka. Zámek je vždy možné odemknout cylindrickou vložkou z obou stran dveří nebo stiskem kliky z vnitřní strany dveří, tzv. antipanic funkce.

Čtecí hlava H-PRO a H-PRO/K

Čtecí hlav s klávesnicí je určena pro přístupový bod serverové místnosti a pokladny, čtecí hlava bez klávesnice pro přístupový bod zasedací místnosti. Funkčním prvkem k otevření je elektromagnetický zámek, připojený k čtecí hlavě.

Obr. 24. Čtecí hlava H-PRO a H-PRO/K [8]

Napájení a záložní zdroj

Slouží pro společné napájení všech komponentů systému. Vnitřní zálohovací akumulátor zajišťuje nepřerušenou funkci systému i při výpadku síťového napájení. Zdroj vždy automaticky zajišťuje dobíjení akumulátoru. Pro zařízení bude stačit zálohovaný zdroj 12V-1,2 A, akumulátor 12V/1,3Ah.

Identifikační médium

Jako identifikační médium jsem zvolil bezkontaktní kartu MIFARE, které pracují na frekvenci 13,56kHz s čipem S50 ve standardním ISO formátu. Karta je vyrobena z bílého PVC materiálu s lesklým povrchem. Provozní teplota se pohybuje v rozmezí od -20 °C do 50 °C.

9.3 ZABEZPEČENÍ

Řídící jednotka, napájecí a záložní zdroj budou umístěny uvnitř objektu v místnosti serveru. Komunikace mezi čtečkami a řídící jednotkou bude probíhat pomocí standardu RS-485. Komunikace mezi řídící jednotkou a serverem bude realizována přes Ethernetové rozhraní. Každá osoba s oprávněním ke vstupu do objektu dostane identifikační kartu a kód, který si určí. Přes libovolný webový prohlížeč se následně přiřadí tyto identifikační karty k jednotlivým osobám a nastaví se přístupová práva.

Nastavení oprávnění bude povoleno v pracovní dny všem zaměstnancům do společných prostor, vedoucím zaměstnancům do zasedací místnosti, ekonomickému úseku do prostor pokladny a administrátoru serveru a jeho zástupci do serverové místnosti. Přístup do

místnosti serveru a zasedací místnosti je omezen na pracovní dobu, ostatní přístupová místa, tj. pokladna a ostatní prostory, na pracovní dobu rozšířenou o 30 minut.

Při vstupu do objektu přiloží osoba svoji kartu ke čtečce u dveří a následně zadá přístupový kód. Přístupový systém vyhodnotí přístupová práva, otevře dveře a zaeviduje datum a čas vstupu. V případě, že přístupová práva nesouhlasí, osoba se snaží vstoupit např. mimo pracovní dobu, tak přístupový systém zaeviduje datum a čas přiložení karty, ale dveře neotevře. Pro přístup je vyžadována kombinace karty a kódu, pro přístup do zasedací místnosti není číselný kód vyžadován.

Veškerá data o přístupu a pokusech o přístup jsou ukládána na server. Server je vybaven modulem sloužícím k archivaci da, spouštění aplikací a exportní aplikací pro vazby na externí moduly (správa docházky). Ovládání a nastavování probíhá z ovládacího místa, klientského počítače. Nastavení a změny nastavení provádí pouze administrátor, nahlížení do historie je povolen u vybraných pracovišť - klientských počítačů (vedoucími pracovníky). Celý systém pracuje jako uzavřený systém bez možnosti ovládání z venku.
Prohlížení je možné přes systém INFOS (softwarový produkt prostředí Windows), pomocí něhož lze zobrazit přehled o tom, která osoba kdy v kolik hodin vstoupila. Dále je možno zobrazit pokusy o nepovolené vstupy do objektu a další události. Historii lze tedy prohlížet z pohledu přístupového bodu i z pohledu přístupového média. Dále systém monitoruje stav dveří. Jejich případné nezavření do určité doby, nebo násilné otevření vyvolá v nastaveném intervalu poplach. Doporučit lze pravidelnou změnu přístupových hesel.

ZÁVĚR

Malé a střední podniky jsou kategorií podniků, které jsou teenagery ekonomiky. Umí pružně reagovat na změny podnikatelského prostředí i změny trhu, jsou inovativní, jsou to právě oni, kdo vytváří nejvíce pracovních příležitostí, vzhledem k jejich pružnosti lépe odolávají recesi a mohou velmi rychle přijímat podnikatelská rozhodnutí. Naproti tomu mají omezené možnosti zaměstnávání odborníků ve správě a řídících činností a omezené prostředky na propagaci, reklamu a investice. Přestože podle průzkumů má 70% těchto podniků zájem o IT technologie. Investice v této oblasti reálně provede pouhé 1% firem. Z čehož lze vyvodit, že investice dobře promýšlejí a investují v oblastech, které jsou jim skutečným přínosem. O to více se instalační firmy snaží navrhnout zákazníkovi systém na míru. [14]

Malé a střední podniky většinou nezaměstnávají odborníka na bezpečnost, a při posuzování kontrolních mechanizmů takříkajíc plavou na suchu. Ve firmě posouzení svěří většinou administrátoru dat, či správci sítě. Stává se tak, že ač mají dobrou ochranu firemních dat, zálohování a ochranu sítě, ochrana know how, hmotného majetku nebo vybavení zaostává.

Hlavním kritériem je mnohdy získaná úspora, což je u počáteční investice základního modulu nad 100tisíc někdy těžké obhájit, ovšem, pokud lze takový systém rozšiřovat o další funkce, propojit s jinými systémy a tak ušetřit budoucí náklady, nemůže podnik výhodu investice popřít. Zejména v porovnání mzdových nákladů fyzické ostrahy v delším časovém úseku. Vzhledem k tomu, že firma nemusí disponovat odborně zdatnou osobou, schopnou nabídky instalací systémů posoudit, není od věci si najmout nezávislou osobu, která posouzení provede. Přeci jen je to investice do budoucna a je třeba brát ohled nejen na směr vývoje, ale i technologií komplexně.

Obecně platí, že čím bohatší firma, tím větší prostředky věnuje na investice a inovace. Vybírá si kvalitnější produkty, má větší zájem využívat celý soubor činností systémů. Má vysoké procento integrace a dobře zvažuje použití technických novinek a výstřelků. Úzkostlivěji chrání svůj majetek, neboť si je vědoma své hodnoty. Čím bude takovýchto firem více, tím častěji se budeme setkávat se systémy kontroly vstupu, které jsou nespornou výhodou při ochraně majetku podniku, nejen pro zrazení případného pachatele ale i získání přehledu nad stavem v podniku.

O tom vypovídají výsledky dotazníku. To že převážná část firem hodlá mí vše pevně ve svých rukou, vyplynulo i z procenta odpovědí upřednostňující kombinaci metod

identifikace, centrální ovládání i postoj k integraci. Postoj firem je jasný i v jednoznačné preferenci bezkontaktních technologiích a jisté procento benevolence oprávněným osobám. Vyplývá to z odpovědí, že pokud je již uděleno oprávnění vstupu, může oprávněná osoba v podstatě kamkoli. Což by bylo na místě změnit a použít pravidlo „Důvěřuj, ale prověřuj." ve formě „Důvěřuj, ale kontroluj".

SEZNAM POUŽITÉ LITERATURY

[1] LUKÁŠ, Luděk a kolektiv. *Bezpečnostní technologie systémy a management I*. 1. vyd. Zlín: VeRBuM, 2011, 133 s.ISBN 978-80-87500-5-7.

[2] RAK, Roman a kolektiv. *Biometrie a identita člověka.* Praha: Grada, 2008, 664 s.ISBN 978-80-247-6392-7.

[3] PÍSEK, Slavoj. *ACCESS 2013.* Praha: Grada, 2013, 160 s.ISBN 978-80-247-4746-0.

[4] BITTO, Ondřej. *Šifrování a biometrika, aneb, Tajemné bity a doteky.* Vyd. 1 Kralice na Hané : Computer Media, 2005. 168 s.ISBN 80-86686-48-5

[5] KŘEČEK, Stanislav. *Příručka zabezpečovací techniky.* Praha: Critetus, 2006, 315 s. ISBN 80-902938-2-4.

[6] ČSN EN 50133-1. *Poplachové systémy – Systémy kontroly vstupů pro použití v bezpečnostních aplikacích – Část1: Systémové požadavky.* Březen 2001 s.28.

[7] LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti II.* Vyd. 2 Zlín : Univerzita Tomáše Bati ve Zlíně, 2007. 124 s. ISBN 978-80-7318-631-7.

[8] Nabídka komplexního identifikačního systému INFOS. Cominfo, a.s. 2013

[9] SEGURO, *Kódová klávesnice kovová ECK-02N*. [online]. [cit. 2014-05-03]. Dostupný z WWW: http://www.seguro.cz/eshop/2162-kodova-klavesnice-kovova-eck-02n-0902-002.html

[10] GACC, *Kontaktní čip Dallas*. [online]. [cit. 2014-05-03]. Dostupný z WWW: http://www.gacc.cz/eshop/kontaktni-cip-dallas

[11] IT SYSTEMS, *Moderní docházkové a přístupové systémy*. [online]. [cit. 2014-04-22]. Dostupný z WWW: http://www.systemonline.cz/hrm-personalistika/moderni-dochazkove-a-pristupove-systemy.htm

[12] IDB JOURNAL, *Přístupové systémy (4c* Dostupný z WWW: http://www.idbjournal.sk/rubriky/prehladove-clanky/pristupove-systemy-4.html?page_id=15837&from=rss

[13] ALTUS VARIO, *Nastavení oprávnění.* [online]. [cit.2012_04_22]. Dostupný z WWW: http://www.altusvario.cz/?document=7514

[14] AMSP, *Investice malých a středních podniků do IT.* [online]. [cit.2012_04_24]. Dostupný z WWW: http://www. http://www.amsp.cz/investice-malych-a-strednich-podniku-do-it

[15] COMBITRADING, *RFIDidentifikační náramky vestice malých a středních podniků do IT.* [online]. [cit.2012_04_24]. Dostupný z WWW: http://www. http://www.amsp.cz/investice-malych-a-strednich-podniku-do-it

[16] GVRATA, *Pohony pro posuvné brány*. [online]. [cit.2012_04_24]. Dostupný z WWW: http://www.gvrata.cz/automaticke-pohony/pohony-pro-posuvne-brany/

[17] Z-WVARE, *Řídící jednotka pro posuvné brány* [online]. [cit.2012_05_02]. Dostupný z WWW: http://www.gvrata.cz/automaticke-pohony/pohony-pro-posuvne-brany/

[18] BESTAPRINT, Přístupové karty. [online]. [cit.2012_05_02]. Dostupný z WWW: http://www.bestaprint.cz/karty

[19] FAB, *FAB Befo KLASIK 211*. [online]. [cit.2012_04-24]. Dostupný z WWW: http://www.bestaprint.cz/karty

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

Ah	*Amperhodina,* jednotka elektrického náboje.
CCTV	*Closed Circuit Television*, uzavřený kamerový okruh.
EMC	Elektromagnetocká kompatibilita.
EPS	Elektrická požární signalizace.
ID	*Identifikační,* rozpoznávací.
IR	*Infrared,* infračervené záření.
IT	Informační technologie.
LAN	*Local Area Network,* lokální - místní síť.
NCF	*Near field communication,* technologie k bezdrátové komunikaci na krátkou vzdálenost.
PC	*Personal Computer,* osobní počítač.
PoE	*Poower over Ethernet,* napájení po síti.
PVC	*Polyvinilchlorid,* zkratka nejběžnější umělohmotné hmoty.
PZS	Požární zabezpečovací signalizace.
QR kód	Prostředek pro automatizovaný sběr dat
RFID	*Radio Frequency Identification*, identifikace na rádiové frekvenci.
RS-232	komunikační standartd, vedení pro připojení nízkonapěťových prvků
RS-485	komunikační standartd, vedení pro připojení nízkonapěťových prvků
SKV	Systém kontroly vstupů.
SQL	*Structured Query Language,* strukturovaný dotazovací jazyk.
UHF	*Ultra high frequency,* ultra krátké vlny
USB	*Universal Serial Bus*, univerzální sériová sběrnice.
V	*Volt,* jednotka elektrického napětí.
VA	*VoltAmper,* jednotka zdánlivého elektrického výkonu.
WAN	*Wide Area Network*, počítačová síť pokrývající rozsáhlá území.

WWW *World Wide Web*, celosvětová síť propojení počítačů.

SEZNAM OBRÁZKŮ

SEZNAM GRAFŮ

SEZNAM FORMULÁŘŮ