Integrované zabezpečení firmy

Michal Mičulka

Bakalářská práce
2006

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

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

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Michal MIČULKA**
Studijní program: **B 3902 Inženýrská informatika**
Studijní obor: **Bezpečnostní technologie, systémy a management**

Téma práce: **Integrované zabezpečení firmy**

Zásady pro vypracování:

1. Podle příslušné ČSN normy zvolte typ integrovaného systému, který použijete pro bakalářskou práci
2. Ze současné nabídky vyberte min. dva produkty, umožňující integraci.
3. Posuďte vhodnost vybraného produktu, jak z pohledu monitorování, vzdálené správy a ovládání použitých bezpečnostních systémů (EPS, EZS, CCTV, ACCESS), tak i z pohledu správy budov a řešení krizových stavů (požár, napadení aj.)
4. Práci konkretizujte návrhem integrovaného zabezpečení zvoleného objektu.

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. ČSN CLC ITS 50 398 Kombinované a integrované systémy – všeobecné požadavky (8/2005)
2. Materiály firem ADI international, Sieza, Alimex (k danému tématu)
3. Časopisy SECURITY magazin, Automatizace

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

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

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

Ve Zlíně dne 14. února 2006

prof. Ing. Vladimír Vašek, CSc.
pověřený děkan

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Tématem bakalářské práce je integrované zabezpečení firmy. Cílem je seznámit čtenáře s možnostmi využití zabezpečovacích technologií, a to z teoretického i praktického hlediska. Teoretická část má přiblížit především funkce a možnosti elektrické zabezpečovací signalizace, elektrické požární signalizace, kamerového systému a přístupového systému. V praktické části je uveden návrh na integrované zabezpečení firmy.

Klíčová slova: elektrická zabezpečovací signalizace, elektrická požární signalizace, kamerové systémy, přístupové systémy, detektor, čidlo, hlásič.

ABSTRACT

The subject of this bachelor's thesis is integrated security of a company. The aim is to familiarize readers with the possibilities of safety technologies usage from theoretical and practical point of view. The theoretical part should, first of all, zoom in functions and possibilities of electric safety signalling, electric fire alarm, camera system and access system. The practical part includes a project of integrated security of a company.

Keywords: electric safety signalling, electric fire signalling, camera systems, access systems, detector, sensor, call box.

Děkuji tímto svému vedoucímu bakalářské práce Ing. Jiřímu Kindlovi, za odborné vedení, rady a věcné připomínky, které mi poskytoval během práce. Dále chci poděkovat svým rodičům a blízkým za podporu, které se mi dostávalo během mého studia.

Ve Zlíně, 12.06.2006 .....

Mičulka Michal

OBSAH

ÚVOD

Na soukromí a bezpečí má nárok každý z nás. Ať už je to zabezpečení domu, bytu nebo své firmy.

Velké úsilí a finance stojí zajistit naše bezpečí a klid. Velmi často v České republice dochází k vloupání do firem a prodejen. Narušitelům velmi usnadňují práci naše nedbalost a lehkomyslnost. Měli bychom se těmto vlastnostem vyvarovat a předcházet takovým situacím dobrou prevencí.

Dnes je již bezpečnostní technika cenově dostupná a na velmi dobré úrovni. S její instalací si snadno poradí odborníci specializovaných firem. Vyškolení pracovníci řádně certifikované a prověřené bezpečnostní firmy umí zasáhnou jak proti případnému vloupání, tak při požáru, uniku plynu, přepětí či výpadku proudu, vyplavení vodou apod. Pokud si nejsme jisti zabezpečením, prokonzultujeme se zástupcem takové firmy technické a fyzické možnosti, vybavení pro možný zásah a zda naše podmínky zabezpečení vyhovují přísným podmínkám pojišťoven. Celkový návrh a technickou studii nám kvalitní firmy rychle zpracují. Pak už záleží na nás, na našich potřebách, místních podmínkách a zvycích zaměstnanců firmy, pro jaké zabezpečení se rozhodneme.

I přes jakékoliv zabezpečení by jsme neměli nic podceňovat. Před opuštěním firmy například uchovat cenné věci a doklady do bezpečnostní schránky nebo do trezorku, nejlépe pevně zabudovaného ve zdi, zkontrolovat pečlivě okna a dveře, zda jsou zavřené, atd.

V minulosti se nevěnovala velká pozornost zabezpečení objektů ale v dnešní době je tomu zcela jinak. Je to díky velké zkušenosti občanů s kriminalitou, ale i to že není v silách Policie ČR zabezpečit všechny prostory a objekty fyzických nebo právnických osob, firem a státních veřejných prostorů.

Policie ČR má pravdu, když tvrdí,že převážnému počtu vloupání by se dalo zabránit. K tomu sloužím například EZS poplašná zařízení, ohlašující se sirénou nebo světelnými signály, které vysílají signál o narušení na PCO.

Existuje celá řada možností, jak se proti vloupání bránit. Prevence je nesrovnatelně výhodnější než dodatečně odstraňovat většinou nemalé následky případných škod.

Na zabezpečení těchto všech vyjmenovaných věcí se nemalou částí podílí i prvky, zařízení a technologie využívané v elektrických zabezpečovacích signalizacích. A to celé společně

s mechanickými zabezpečovacími systémy, elektrickou požární signalizací a přístupovým systémem tvoří takzvané integrované zabezpečení firmy. Je velmi důležité, aby jednotlivé systémy pracovali společně. Nikoliv však, aby jeden závisel na druhém. Je třeba navrhnout takové řešení, aby se předešlo jak násilnému vniknutí, tak i sabotáži a bylo možné například rozpoznat falešný poplach.

Jelikož jsou dnes zabezpečovací systémy tak dostupné je třeba v případě zabezpečení dbát i na cenovou stránku. Aby řešení nebylo tzv. přeplácané a nebylo zaplaceno více než je třeba. Zvážit opravdová hrozící rizika a neopomenout také ochranné prostředky, jakými jsou například požární čidla.

I. TEORETICKÁ ČÁST

1 BEZPEČNOSTNÍ PRŮMYSL

Bezpečnostní průmysl zahrnuje fyzickou ostrahu majetku a osob, přepravu peněz a cenností, zpracování peněžní hotovosti, detektivní a kompletní technické bezpečnostní služby a ochranu informací a dat.

Při ochraně majetku a osob, při předcházení kriminalitě či zamezování škod vzniklých trestnou činností hrají významnou roli soukromé bezpečnostní služby. Často jsou soukromé bezpečnostní služby společností vnímány jako „soukromá policie". Toto srovnání se státní policií není ve skutečnosti přesné, protože soukromé bezpečnostní služby nemohou policii nikdy nahradit a ani nemají potřebné, rozšířené a legislativně určené a schválené pravomoci a kompetence. Služby poskytované bezpečnostními agenturami zvyšují bezpečnostní standard zákazníka a vedle toho zákazníkovi umožňují přesně si stanovit v jakém rozsahu a jakými prostředky bude ostraha objektu uskutečňována.

Rozvoj soukromých bezpečnostních služeb nastal v důsledku vysokého počtu trestných činů, zvyšování objemu soukromého majetku, rozvoje elektroniky a elektronických zabezpečovacích systémů, vyšší poptávky po ochraně majetku a ochoty připlatit si za tento nadstandard. Rozsah služeb poskytovaných bezpečnostními agenturami je průběžně doplňován a měněn podle potřeb zákazníka a může zahrnovat např. strážní službu, techniku, událost, hardware nebo speciální služby.

Sektor soukromých bezpečnostních služeb při potřebě chránit objekty před narušením vypracoval různé formy ochrany objektů. Mezi tyto formy ochrany objektů můžeme zahrnout klasickou ochranu, která je založena na zajištění objektu pomocí mechanických zábran a zařízení, které znemožňují odcizení nebo poškození objektů, jejich částí nebo cenných předmětů uvnitř objektu a režimovou ochranu, která je založena na zavedení uplatňování účinných bezpečnostních směrnic (tzv. režimových opatření) v chráněném objektu. Dále sem můžeme zařadit fyzickou ochranu prováděnou fyzickou ostrahou objektu a v neposlední řadě technickou ochranu založenou na automatickém monitorování objektu pomocí technických prostředků objektové bezpečnosti.

Soukromá bezpečnost se už stala součástí moderní společnosti, a to díky pokrokům ve všech oblastech oboru.

2 FUNKCE INTEGROVANÉHO SYSTÉMU

Typickým znakem integrace (tedy tím, co odlišuje systém neintegrovaný od systému integrovaného) je to, že prvky dosud izolovaných subsystémů jsou alespoň ve svých základních parametrech sjednoceny a prolnuty.Vznikají tímto sdružené informace o mnoha parametrech. Integrovaný systém vytvořený z těchto prvků má tedy obvykle složitější, komplexnější, ale i přesnější vazby, přičemž počet prvků při integraci má klesat. Integrovaný systém je proti neintegrovanému ucelenější, zhutněnější, komplexnější. Ideálem je úplná integrace.

Funkce integrovaného zabezpečovacího systému spočívá ve sjednocení zabezpečovacích systému jako jsou EZS, EPS, CCTV a ACCES. Tyto systémy mají pak tu výhodu, že se mohou navzájem doplňovat. V případě tedy, že dojde k narušení objektu, začnou systémy spolupracovat. Čidlo vyšle poplach na PCO a kamery začnou nahrávat záznam. Nebo při vzniku požáru se automaticky spustí hasící systémy, rozsvítí se výstražná světla na chodbách značící únikový východ. A dveře určené k nouzovému opuštění objektu jsou odblokovány. Funkcí a variací jak systém integrovat je mnoho a důležité je dbát na celou funkčnost systému. Pouze takový systém je efektivní a spolehlivý. Usnadňuje nám práci při řešení krizových situací a lépe zabezpečuje náš objekt.

2.1 Základní normy pro poplachové a integrované systémy

Technické normy jsou předpokladem pro technický pořádek v daném oboru na příslušné úrovni. V oboru poplachových systémů začaly v posledním desetiletí 20. století vznikat na území evropských (CENELEC - Evropský výbor pro normalizaci v elektrotechnice) a světových (IEC - Mezinárodní výbor pro elektrotechniku) normalizačních organizací oborové standardy nabízející pro jednotlivé skupiny zařízení z oboru poplachových systémů řešení funkčních požadavků, uvádějící metody zkoušení prokazující splnění těchto funkčních požadavků, požadavky na vlastnosti vztahující se k vlivům prostředí, metody zkoušení prokazující splnění klimatické odolnosti, systémové požadavky vztahující se k podmínkám nasazení těchto systémů nebo návody a doporučení na aplikaci poplachových systémů.

Tab. 1. Normy poplachových systémů

POPLACHOVÉ SYSTÉMY		
Všeobecně EN 50130+	**Elektronické zabezpečovací systémy (EZS)** EN 50131+	**Systém uzavřených televizních okruhů (CCTV)** EN 50132+
Systémy kontroly a řízení vstupu (ACS) EN 50133+	**Systém přivolání pomoci (SAS)** EN 50134+	**Systémy tísňové (HUAS)** EN 50135+
Přenosové zařízení (ATS) EN 50136+	**Systémy kombinovaně nebo integrované (IAS)** EN 50137+	**Elektronické požární signalizace (EPS)** EN 54+

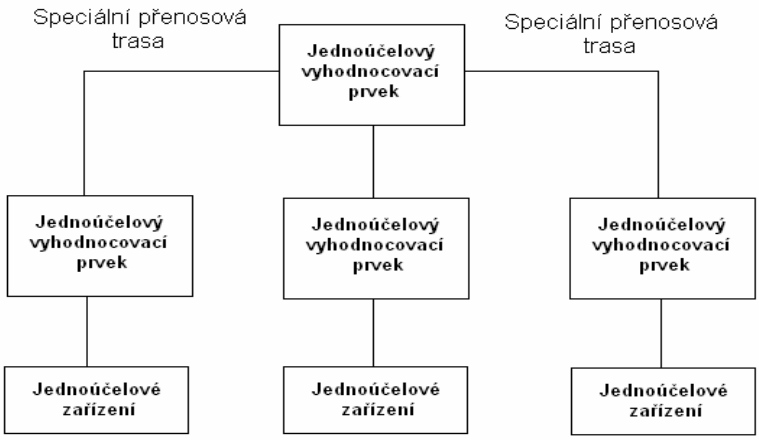
Evropské normy (EN) jsou produktem evropských normalizačních organizací. V případě poplachových systémů je to konkrétně technická komise CLC/TC79 a její pracovní skupiny. TC79 je technická komise - poplachové systémy (Alarm Systems) při Evropském výboru pro normalizaci v elektrotechnice (CENELEC). Svou působností pokrývají nejen klasickou EZS, ale komplexně celou oblast zabezpečení jako je CCTV, přenosové systémy pro hlášení poplachu, kontrola vstupů, systémy přivolání pomoci a integrované systémy. Za ČR zabezpečuje mezinárodní spolupráci s CENELEC TC79 Asociace bezpečnostních služeb Grémium Alarm, jejíž zástupce se pravidelně zúčastňuje zasedání TC79.

Česká technická norma pro poplachové systémy a integrované systémy je ČSN CLC/TS 50398

2.2 Typ integrovaného poplachového systému

Pro integrované zabezpečení firmy jsem vybral Typ 1. Struktura typu 1 je kombinace dvou nebo více jednoúčelových systémů. Tyto systémy jsou připojeny ke společným dalším zařízením , například propojených přes speciální přenosovou trasu.

U normalizovaných vybavení typu 1 v poplachové aplikaci nesmí být tato vybavení v žádném stavu nepříznivě ovlivněna v žádném provozním stavu žádným dalších jednoúčelovým systémem nebo žádným zvláštním vybavením.



Obr.1. Případ struktury typu 1, ústřední řídící zařízení (CFF) třídy 1

3 ELEKTRICKÁ ZABEZPEČOVACÍ SIGNALIZACE

Mozkem každého zabezpečovací systému je ústředna. Ta vyhodnocuje veškeré signály ze snímačů a ovládacích zařízení a na základě jejich analýzy a v souladu s naprogramováním rozhoduje o vyhlášení poplachu. Ústředny se vyrábějí jak pro malé aplikace, tak i takové, které mohou vyhodnocovat a zpracovávat stovky detektorů, událostí, uživatelů, aj. Ústředny po zpracovaní informací jsou dále schopny všechny své stavy signalizovat prostřednictvím svých reléových a nebo elektronických výstupů a to místně a nebo dálkově (poplach, poruchy, aj.).

Moderní EZS se zpravidla ovládá buď pomocí klávesnice nebo pomocí čipové karty pomocí níž se verifikuje identita jejího nositele prostřednictvím porovnání skutečných fyzických charakteristik nositele karty s daty uloženými na kartě. Tyto systémy jsou naprosto bezpečné. U ovládacích klíčenek bývá použit tak zvaný plovoucí přenosový kód, který zcela znemožňuje jeho zkopírování.

Videotelefony jsou určeny pro obousměrnou komunikaci s osobami nacházejícími se vně objektu. Přenos zvuku i s obrazem výrazně přispívá ke zvýšení bezpečnosti. Širokoúhlá kamera na straně zvonkových tlačítek může být vybavena infrapřisvícením, což umožní sledování i v naprosté tmě. Tato část která je většinou instalována vně objektu, může být doplněna o tzv. antivandal kryt, který ji chrání proti úmyslnému poškození. Vzhledem k tomu, že systémy používají pro přenos videosignálu metalické kroucené kabely, odpadá kabeláž pomocí koaxiálního kabelu.

Pro kvalitní ochranu vnitřních prostor před narušiteli se používají na prvním místě infrapasivní detektory (tzv. PIR detektory). Tyto detektory j sou schopny na základě analýzy teplot v místnosti spolehlivě detekovat pohyb člověka v prostoru. Pro různé aplikace se používají PIR detektory s odlišnou charakteristikou, například vhodné pro standardní prostory, pro dlouhé úzké chodby, nebo imunní proti menším domácím zvířatům, aj.

Standardem u systémů EZS je také ochrana objektů před nebezpečím požáru nebo výbuchu. Ke včasné detekci požáru se používají požární snímače. Nejpoužívanější snímače jsou opticko-kouřové.

Pokud se k topení nebo vaření používá plyn, může být do takového prostoru nainstalován

detektor úniku plynů. Nejmodernější typy umožňují detekci všech druhů. výbušných plynů a v případě zvýšení koncentrace plynu nad nastavenou bezpečnou mez aktivují po dobu celých 24 hodin zabezpečovací systém.

Elektrické zabezpečovací systémy (ústředny, pomocné zdroje) se napájí ze samostatných jištěných přívodů sítě 230V/50 Hz, 6A. Jistič v elektrorozvaděči musí být označen štítkem „EZS nevypínat". Ústředny, expandery, ovládací klávesnice a čidla jsou napájeny z vestavěného 12 V zdroje ústředny nebo pomocných zdrojů. Jejich zálohování pro případ výpadku elektrického proudu záložním akumulátorem se navrhuje v projektové dokumentaci v souladu s platnými předpisy upravující záložní napájení ČSN EN 50131-1, ČSN EN 50131-6 a české asociace pojišťoven předpis ČAP P131-6.

3.1 Ústředny elektronické zabezpečovací signalizace

Vlastní ústředna je srdcem celého zařízení. Vyhodnocuje a zpracovává příkazy od svých periferií jako jsou infradetektory, duální detektory, magnetické kontakty, detektory tříštění skla atd. a aktivuje zařízení, která jsou určena k signalizaci a předávání zpráv. Na našem trhu je poměrně široká nabídka v přibližně stejné srovnatelné kvalitě. Všechny nabízené typy pro střední a malé objekty mají srovnatelné uživatelské funkce a technické parametry. Samozřejmostí ústředny by již měl být vestavěný komunikátor, přes který lze systém připojit na bezpečnostní agenturu nebo na privátní telefon, abyste v případě poplachu dostali zprávu. Dále by mělo být možno k systému připojit více ovládacích externích klávesnic. Vzhledem k tomu, že ústředna by měla být umístěna v místě, kde je pod dozorem detektoru tzv.okamžitá zóna není vhodné, aby se systém zapínal z klávesnice umístěné přímo na ústředně bohužel některé typy jsou tímto z důvodu ceny vybaveny.

Součástí ústředny je také záložní akumulátor, který by měl systém udržet v činnosti min. 24 hod. po výpadku napájecího napětí.

3.1.1 Vyhlášení poplachu

Poplach je standardně vyhlašován venkovní a vnitřní sirénou. Vzhledem k tomu, že tyto prvky jsou snadněji napadnutelné, je nutno jak již bylo zmíněno systém napojit na bezpečnostní službu nebo alespoň na svůj privátní telefon.

U převážné většiny objektů však nastává další velký problém a to dostupnost telefonní lin-

ky pro pachatele, který před vstupem do objektu tel. linku přeruší a pak se pro něj venkovní a vnitřní siréna stává pouze formální překážkou a objekt je v tuto chvíli nezajištěn.

Bránit se proti tomuto lze celkem úspěšně připojením systému přes vysílač nebo GSM bránu na bezpečnostní službu nebo na svoje privátní telefony.Toto řešení je však poměrně finančně náročné a u malého systému může dosáhnout i ceny celé instalace vlastního zabezpečení.

Jednodušší a podstatně levnější varianta je využití komunikátoru v ústředně a připojení přes tel. linku a zakoupení jednoduchého a levného zařízení, do kterého se vloží jakýkoli mobilní telefon a toto zařízení dokáže zavolat na jedno tel. číslo přes GSM síť. Tím je zvýšena jistota, že když selže pevné telefonické připojení, tak jako záloha zůstane předání poplachové zprávy přes GSM síť.

Vnitřní interiérové sirény

Mají vysoký pronikavý zvuk. Používají se s výkonem 90 - 115 dB bez zálohování a slouží k signalizaci lokálního poplachového stavu. Instalují se do společných komunikačních prostor objektu. Jejich hlavním cílem je překvapit pachatele, znepříjemnit mu pobyt ve střeženém domě, stresovat ho a přispět k tomu, aby utekl. Důležitým cílem je taktéž informování majitele že se v daném objektu něco děje ale také využití u poplachových signalizací kde lze sirénu nemodifikovat jinak jak pro požár tak pro vloupání.

Je nutno vzít v úvahu následující faktory:

- zařízení nemají být v blízkosti ústředny ani ovládací klávesnice;
- umisťovat uvnitř střeženého prostoru na nesnadno přístupných místech, aniž by však to bylo na úkor slyšitelnosti nebo viditelnosti.

Venkovní sirény

Používají se k akustické a optické signalizaci globálního poplachového stavu na objektu s výkonem 115-130 dB. Měly by být opatřeny integrovaným majákem, který slouží pro optickou orientaci a signalizaci dalších technických stavů systému. Výstupem elektronické signalizace může být také zadýmovací zařízení, které vyplní prostor neškodným kouřem snižujícím viditelnost na deset centimetrů.

Je nutno vzít v úvahu následující faktory:

- umístit zařízení na dobře viditelném místě;
- zařízení musí být v nesnadno přístupném místě, aniž by však byla narušena všeobecná viditelnost nebo slyšitelnost;
- zařízení musí být umístěno tak, aby byla minimalizována možnost jeho neúmyslného nebo úmyslného poškození;
- zařízení musí být umístěno tak, aby bylo umožněno provádění servisu, při respektování předchozích bodů;
- veškeré přívodní kabely musí být skryté nebo vedeny v pancéřových trubkách;
- zařízení musí být upevněno na pevné části budovy.

Narozdíl od vnitřních sirén, které jsou v době poplachu napájeny přímo z řídící ústředny, by měla být venkovní sirény tzv. zálohovaná. To znamená, že siréna má vlastní bez údržbovou baterii, která jev klidovém stavu dobíjena z řídící ústředny a siréna jev klidu. Jakmile ústředna vyhlásí poplach, nebo když někdo přeruší vedení k siréně, baterie se dobíjet přestane a siréna, napájená vestavěnou baterií, se rozhouká.

V konstrukci venkovní sirény jsou použity dva kryty pro vyšší mechanickou odolnost ale také proti možnému vypěnění akustického měniče. Venkovní sirény by měly mít nejenom ochranný kontakt, který vyhlásí poplach při sejmutí krytu, ale i druhý, který vyhlásí poplach při odtržení sirény od zdi, obsahují taktéž záložní akumulátor pro nepřetržitý provoz.

Venkovní sirénu je vhodné instalovat co nejvýše na zdi, ale i zde platí "všeho s mírou". I venkovní siréna potřebuje čas od času údržbu a je pro nás jako pro uživatele poměrně nákladné, když si servisní firma musí pokaždé přivézt vysokozdvižnou plošinu, aby se k zařízení dostala.

Předpokladem pro funkční místní akustickou signalizaci je, že máme dobré vztahy se svými sousedy a že okolí na houkání sirény bude reagovat. To se samozřejmě nestane, pokud náš bezpečnostní systém bez jakýchkoliv důvodů zbytečně houká třikrát do týdne. Takový systém je nejenom k ničemu, ale navíc snižuje účinnost alarmů v okolních domech.

Když naše sousedské vztahy nejsou ideální, sousedi nebývají doma, máme-li samostatně

stojící dům nebo pokud chceme posílit svou bezpečnost, můžeme svůj bezpečnostní systém napojit na pult centralizované ochrany, nebo alespoň instalovat automatický telefonní komunikátor.

Telefonní komunikátory

Aby se informace o poplachu dostala okamžitě i k majiteli střeženého objektu používají se telefonní komunikátory, které v případě poplachu odpojí telefonní přístroj a ten začne vytáčet navolená telefonní čísla a na ně hlásí předem namluvenou zprávu, kterou si uživatel sám nahrál do paměti.

Výstup signálu "poplach" je vyveden mimo sirény ještě na telefonní komunikátor, který při aktivaci začne automaticky vytáčet předem stanovená telefonní čísla, na která v případě přítomnosti obsluhy předá krátkou zprávu o napadení objektu. Příslušná osoba musí být poučena o tom, co při převzetí zprávy má dále udělat (volat policii, zajistit střežení nebo prohlídku objektu apod.) - řešení je však závislé na přítomnosti poučené osoby u příslušného telefonu, rychlosti a kvalitě způsobu provedení zásahu v ohroženém objektu.

Digitální a hlasové komunikátory rozšiřují možnosti systémů EZS o vzdálenou signalizaci poplachového nebo poruchového stavu na občanský telefon za použití telefonní linky přivedené do objektu. Dle typu umožňuje přenést namluvenou hlasovou zprávu v délce 10-20 s na 4 až 8 telefonních čísel zadaných do paměti přístroje.

GSM moduly

Takovýto přenos není závislý na telefonních linkách. Současně vysílá i další informace z objektu (výpadek proudu, zvýšená teplota, aj.) Komunikuje až na 16 tel. čísel, včetně rozesílání poplachových zpráv SMS.

Zařízení GSM komunikátoru se skládá ze speciálního komunikačního modulu a mobilního telefonu požadovaného typu, připojuje se na výstupy ústředny EZS a činným způsobem zabezpečuje přenosy informací z mobilních objektů nebo objektů bez tel. linky.

GSM komunikátor má 4 - 8 vstupů a ke každému je možno nadefinovat zprávu s jiným textem. Aktivací vstupu se odešle odpovídající zpráva na dvě různá čísla mobilních telefonů a provede se telefonní volání s varovným signálem na předem zadané číslo. Umožňuje i průběžnou kontrolu hlídaného prostoru a nelze ho jednoduše zneškodnit odstřihnutím telefonní linky vedoucím do objektu. Většina GSM komunikátorů umožňuje i odposlech za-

bezpečeného prostoru a dálkové ovládání spotřebičů mobilním telefonem nebo elektronickou poštou. Díky vysoké spolehlivosti přenosu informace a nízkým nákladům na pořízení i provoz lze GSM komunikátor využít i pro přenos technologických informací jako například stavy hladin vodojemů, překročení teplot a podobně.

3.1.2 Připojení na pulty centralizované ochrany

Mnohem účinnější je připojení na pulty centralizované ochrany, které provozují bezpečnostní agentury nebo v některých městech i Městská policie. Jednak máte v případě poplachu zajištěný kvalifikovaný zásah odbornými pracovníky, jednak se na pult centralizované ochrany dostávají i informace o poruchách ve vašem bezpečnostním systému, o tom v jaké části domu k poplachu došlo a jaký detektor ho vyhlásil atd. Podstatnou výhodou je i to, že datový komunikátor pro připojení k pultu bývá součástí dodávané bezpečnostní ústředny, zatímco komunikátor hlasový je většinou nutné dokoupit zvlášť.

4 ELEKTRICKÁ POŽÁRNÍ SIGNALIZACE (EPS)

Zkratka EPS označuje počáteční písmena slov "Elektrická požární signalizace", jejímž úkolem je detekce nebezpečí požáru v nejčasnějším stádiu jeho vzniku. Ve většině případů bývá prvním příznakem nebezpečí kouř, který se objevuje dříve než zvýšená teplota, a který rovněž v největší míře způsobuje ohrožení osob. Detekci vzniku požáru zajišťují detektory založené na různých principech. Ionizační detektory reagují na rychle se rozhořívající požáry charakteristické hořícími částicemi určitých rozměrů. Opticko-kouřové reagují na požáry s pomalu doutnajícím ohněm, obdobně jako laserové detektory, které jsou cca 50x citlivější. Termické detektory reagují na zvýšení teploty. Existují také kombinované detektory, které v sobě spojují funkce výše popsaných detektorů. Některé z detektorů umožňují sledování naměřených veličin v čase a tak minimalizují riziko falešných poplachů.

Nachází-li se v ohroženém prostoru lidé, je pravděpodobné, že si tito všimnou vznikajícího požáru dříve než jej zaznamenají detektory. Pro případy hlášení vyvolaného lidským zásahem jsou v objektu instalovány tísňové tlačítkové hlásiče požáru.

Detektory a hlásiče jsou v závislosti na typu individuálně adresovatelné, což umožňuje přesnou lokalizaci místa, kde došlo ke hlášení z čidla. Pro zpracování takovéhoto hlášení se používají ústředny. V případě vyhodnocení požáru ústřednou může systém požární signalizace v součinnosti s ostatními systémy zajistit následující činnosti :

- spuštění optické a akustické signalizace v ohrožených prostorech objektu a řídícím centru
- sdělení poplachového hlášení na pult centralizované ochrany (PCO) veřejného hasičského sboru
- ve spolupráci se systémem místního rozhlasu spustit evakuační hlášení
- zapnout světla na únikových cestách, označení únikových východů
- vyřadit z činnosti technologická zařízení a spustit odsávání kouře z ohrožených oblastí
- aktivovat kamery umístěné v ohrožené oblasti (zjištění, zda se v oblasti ještě někdo nachází)

Je možné zajistit také sledování stavu na monitoru řídícího pracoviště, kde se dle konfigurace systému zobrazuje třeba půdorys objektu s vyznačením ohrožených místností. Je zde možnost zobrazovat také ostatní důležité údaje jako stav požárních klapek, požárních dveří, pozice výtahů. Přehled činností operátora a hlášení ústředny je možné vytisknout pro pozdější účely.

4.1 Základní charakteristika EPS

Elektrická požární signalizace slouží ke včasné detekci a signalizaci vznikajícího požáru. Musí být instalována tam, kde je to vyžadováno na základě posouzení požární bezpečnosti stavby nebo se instaluje na přání vlastníka objektu. Základní funkcí elektrické požární signalizace je včasná detekce požáru v jeho počátečním stádiu, kdy je jeho likvidace snazší a nedochází k velkým škodám na majetku a ohrožení života a zdraví osob.

4.1.1 Používané systémy

Konvenční systémy

Automatické hlásiče mají pevně nastavenou indikační úroveň, při jejímž dosažení indikují poplach. Na lince může být instalováno více hlásičů (maximálně 32), ústředna je však vyhodnocuje pod společnou adresou. Tyto systémy jsou levné a hodí se pro zajištění menších objektů.

Adresné systémy

Jsou systémy s konvenčními hlásiči, tyto jsou však doplněny elektronikou tak, aby ústředna vyhodnocovala jejich adresu a tím i jejich umístění

Analogové adresné systémy

Ústředna komunikuje s hlásiči a zná aktuální hodnotu stavu hlásiče. Na základě této informace může individuálně nastavovat citlivost hlásiče, detekovat potřebu servisního zásahu, popřípadě eliminovat falešné poplachy.

Systémy EPS v dnešní době tvoří důležitou součást systémů protipožární ochrany v různých typech objektů. Jedná se zpravidla o výrobní provozy, sklady, hotely, ubytovny, kancelářské budovy atd. Elektrická požární signalizace zajišťuje včasnou a rychlou identifikaci a lokalizaci vzniku požáru. V praxi je z prevenčního hlediska EPS doporučována i do ob-

jektů, kde není přímo předepsána požárními předpisy. Nasazením systému EPS je možné včas předejít rozšíření požáru (např. i úmyslně založeného), zabránit tak vzniku velkých materiálových ztrát a v horších případech i ohrožení životů.

Rozsah systému EPS je dán projektovou dokumentací, která vychází z požární zprávy objektu. Návrh systému, projekt i realizaci provádí naši odborníci dle platných evropských a našich norem ve spolupráci s příslušnými hasičskými orgány.

Technologie systémů EPS

Při řešení nových systémů EPS se upřednostňuje použití digitálních analogových adresných systémů, které umožňují rychlou a přehlednou orientaci v systému a jednoduchou montáž. Pro instalace malého rozsahu se doporučují z hlediska malé technické náročnosti a nižší cenové hladiny konvenční smyčkové systémy. V obou případech jsou na trhu systémy předních světových výrobců protipožární techniky ZETTLER, LITES, ES SER, ALARMCOM a ARITECH.

Digitální adresovatelné systémy již umožňují připojení hlásičů po dvoulinkovém vedení, tudíž odpadá složitá kabeláž jako u velkých konvečních systémů. Linková vedení jsou navíc řešena LOOP technologií tzn., že začátek i konec vedení je zapojen do ústředny EPS. Tímto způsobem je celé vedení ústřednou plně kontrolováno.

V praxi to znamená, že pokud dojde k poruše linky v určitém místě (porucha hlásiče, přerušení vedení) linka zůstane v provozu, protože je napájena z obou stran. K zajištění provozu ostatních hlásičů na lince při poruše jednoho hlásiče slouží tzv. izolátory. Tyto prvky zajistí odpojení jen té části smyčky, pro kterou je izolátor použit. Ostatní hlásiče zůstávají v provozu. U nejnovějších systémů ZETTLER je již izolátor zabudován do každého hlásiče, takže v případě poruchy je odpojen pouze jeden hlásič. Vše je ihned signalizováno na displeji ústředny. Ústředny jsou dodávány dle velikosti systému a max. verze dovoluje připojit až 3000 hlásičů.

Nové systémy EPS již pracují na bázi digitálního přenosu analogové informace mezi hlásičem a ústřednou. Tento princip umožňuje provádět ústředně automatickou kontrolu zaprášenosti snímače, kdy dle nasnímaných hodnot ústředna nastavuje (vyrovnává) jeho citlivost. Po překročení určité hodnoty je nahlášena porucha na snímači a ten musí být vyčištěn.

Ovládání ústředen je prováděno pomocí číselných klávesnic a LCD displejů. Konfiguraci systémů je možné provádět přímo z těchto klávesnic nebo z nadřazeného konfiguračního

počítače. Další možností je připojení ústředen na centrální monitorovací pracoviště na bázi počítače PC. Využití grafického programového vybavení potom umožňuje velmi rychlou orientaci v systému a tím max. zkrácení doby zásahu od vzniku požáru. Programovatelnými výstupy ústředny je možné ovládat další zařízení související s protipožární ochranou (požární dveře, hasící zařízení, klíčový trezor, apod.)

4.2 Charakteristické vlastnosti vzniku požáru

Charakteristickými vlastnostmi při vzniku požáru jsou:

- nárůst teploty
- přítomnost viditelných či neviditelných zplodin kouře
- infračervené či ultrafialové spektrální složky světla při hoření plamenem

Úspěšný boj proti požáru probíhá ve čtyřech hlavních fázích - přesné rozpoznání

příznaků požáru již v jeho zárodku, spolehlivé rozlišení zda se jedná o skutečný požár, či jen o planý podnět, přehledná signalizace přítomným osobám a zasahujícímu personálu a účinná organizace efektivního zásahu. Všechny čtyři tyto fáze by měly proběhnout během prvních cca 4-5 ti minut od vzniku požáru, jinak již bývá pozdě na odvrácení nenahraditelných škod. Systémy EPS nabízejí soubor řešení, která pomáhají tento závod s časem vyhrát!

Rozpoznání požáru je u moderních hlásičů EPS provedeno vysoce přesnými detekčními metodami, které jsou založeny na principu analogové detekce fyzikálních projevů hoření. Senzor v hlásiči nepřetržitě monitoruje prostředí a snímá okamžité hodnoty jednotlivých veličin, jako jsou množství kouřových částic v ovzduší, nebo teplota prostředí. Ty převádí na elektrický signál. Tento spojitý (analogový) signál je následně upraven do digitální podoby na sérii binárních čísel a dále vyhodnocován mikroprocesorem. Kromě standardní poplachové úrovně, se kterou pracují prahové hlásiče, lze proto u analogového hlásiče vyhodnocovat více stavů, představujících různé události. Tak lze například získat výstrahu o nestandardních podmínkách prostředí již ve chvíli, kdy ještě nejsou jisté příznaky opravdového požáru. V kombinaci s časovým průběhem, tzn. jakou rychlostí dochází k dosažení příslušné úrovně, lze zároveň eliminovat nevýznamné události. Pokud například dochází k nárůstu teploty během dne vlivem vytápění, rozezná hlásič tento stav od prudkého oteplení

při vznikajícím požáru. To je také důvod, proč lze tento typ hlásičů nastavit na daleko vyšší citlivost bez rizika planých poplachů. Lze také velmi přesně sledovat postupné pomalé zvyšování přítomnosti prachových částic uvnitř detekční komory a při dosažení kritické úrovně předat ústředně zprávu o zaprášení hlásiče.

Aby byla spolehlivost detekce zaručena po celou dobu provozu, je nutno ošetřit některé nežádoucí provozní vlivy. Nejvážnějším vlivem, který detekci ovlivňuje, je usazování prachu v měřící komoře. Většina opticko-kouřových hlásičů obecně pracuje na principu rozptýlení a odrazu vysílaného světelného paprsku od částic kouře na přijímací senzor. Prach, usazený na stěně měřící komory, působí jako parazitní odrazná plocha, což může být příčinou planých hlášení. Soustava labyrintů uvnitř optické měřící komory u hlásičů systému EPS zamezuje odrazům od částic usazených na vnitřním povrchu měřící komory tím, že vysílaný paprsek po průchodu komorou, případně světlo dopadající do komory zvenčí, beze zbytku utlumí. Navíc je přijímací i vysílací část dostatečně zapouzdřena a spolu s kónickým tvarem komory zajišťuje hlásičům EPS velmi vysokou odolnost proti zaprášení.

Samotná ústředna systému EPS je inteligentní vstupně-výstupní jednotkou, která po přijetí informace z hlásiče organizuje výstupní zařízení. Jednotlivé vstupní a výstupní prvky systému lze téměř libovolně softwarově sdružovat do skupin se stejnými vlastnostmi. Aktivace různých skupin hlásičů mohou být provázány s aktivacemi různých skupin výstupů. Navíc je možno tyto vazby podmínit akcí obsluhy, jako je potvrzení hlášení, zpětné nastavení systému apod., dále délkou času do potvrzení, časem na průzkum lokality hlášení, nastaveným režimem den/noc atd.

Velmi důležitou podmínkou rychlého zasahuje signalizace poplachu. Každý hlásič v adresném systému EPS disponuje vlastní jedinečnou, softwarově přidělenou adresou. Jen tak lze docílit přesné identifikace místa požáru. Kromě LCD displeje a možnosti vytvoření světelných informačních tabulí s plány objektu je v rámci koncepčního řešení s přihlédnutím k dalším budoucím požadavkům na integraci do vyšších celků umožněno napojení systémů do řídícího a monitorovacího software na počítači Během okamžiku je pak obsluha vyrozuměna o přesném místě požáru, včetně podrobného půdorysného zobrazení. Informace může být libovolně doplněna např. vyobrazením hasební techniky, čísly přístupových klíčů, telefonními čísly kanceláří, po doplnění zvukovou kartou a reproduktorem také o nezaměnitelné hlášení o požáru apod. Pomocí software lze také ovládat jednotlivé funkce systému, chronologicky archivovat a tisknout události atd. Odpadá chaotické a dlouho trvající vy-

hledávání informací v papírové dokumentaci, které degraduje vysokou rychlost

detekce systému. Počítač lze mimoto používat pro běžné kancelářské aplikace strážní služby - tvorbu pracovních výkazů, rozpisů služeb, hlášení apod. Při příchodu události má tato vždy prioritu.

4.3 Ústředna EPS

Ústředna EPS je centrální jednotkou, kde se sbíhají signály od připojených hlásičů. Pro lepší orientaci obsluhy lze většinou jednotlivé hlásiče slučovat do společných skupin (zón) se stejným názvem. V ústředně dochází ke zpracování příchozích signálů a organizaci dalších opatření, zejména zobrazení příchozích událostí, ovládání systému a aktivaci navázaných zařízení. Součástí ústředny je i vnitřní paměť pro uchování hlášení, které mohou být zpětně k dispozici při analýze poplachu. Ústřednu je rovněž možné doplnit tiskárnou pro výpis těchto událostí. Moderní ústředny jsou založeny na bázi mikropočítače, ve kterém je možno definovat funkční parametry pomocí software, a to buď přímo pomocí instalačního menu nebo na displeji ústředny, nebo pomocí připojeného počítače [1].

Ústředna dále napájí celý systém energií a to i případě výpadku sítě. Většina systémů může poskytovat toto záložní napájení v souladu s evropskou normou po dobu 72 hodin. V České republice je požadovaná záloha na dobu alespoň 24 hodin. Ústředna se umisťuje zpravidla v prostoru bez požárního rizika, nejčastěji na velínech ostrahy, vrátnicích, služebnách apod.

Detekční část zajišťuje :

- přijímá signály z připojených hlásičů.
- určuje zda tyto signály odpovídají poplachovému stavu.
- indikuje místa nebezpečí.
- případně zaznamenává každou takovou informaci.

Ovládací část zajišťuje :

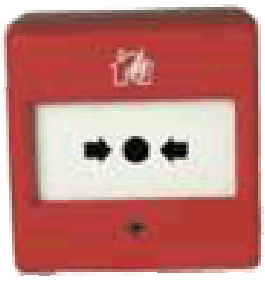
- poplachový signál předá - na akustická či vizuální zařízení. Na zařízení pro dálkový přenos poplachu. Do místa trvalé obsluhy. Pomocí řídící jednotky samočinného hasícího zařízení na automatické stabilní zařízení nebo na jakékoli jiné zařízení spolupracující se systémem EPS.

4.4 Hlásič požáru

Je komponent EPS, obsahující alespoň jeden senzor, monitorující trvale nebo v daných časových intervalech určitý fyzikální či chemický jev spojený s požárem, který poskytne nejméně jeden odpovídající signál ústředně EPS. V systémech EPS se používají dva zkladní druhy hlásičů - automatické a tlačítkové.

Tlačítkové hlásiče

Tlačítkový hlásič je určen k vyhlášení požárního poplachu přítomnou osobou, která požár zjistila a nedokáže jej zlikvidovat vlastními silami. Umisťuje se tam, kde se předpokládá výskyt osob (chodby, schodiště, přístupové cesty). Funkčně se tlačítkové hlásiče dělí na dvě skupiny - s přímým a nepřímým ovládáním. V případě přímého ovládání stačí pro aktivaci poplachu pouze rozbít sklíčko tlačítkového hlásiče. Při nepřímé aktivaci je nutné pro spuštění požárního poplachu rozbít sklíčko a stisknout tlačítko.



Obr. 2.Tlačítkový hlásič

Automatické hlásiče

Detekují požár na základě průvodních fyzikálních jevů a mohou být buď bodové nebo lineární. Bodové zjišťují průvodní jevy požáru v bodě umístění a jejich účinnost se určuje podle způsobu šíření této veličiny. Lineární hlásiče zjišťují průvodní jevy požárů v celé délce jejich nasazení.

4.4.1 Komponenty systému EPS

Požární poplachové zařízení

Používá se pro vyhlášení požáru, jedná se o zdroj zvuku nebo optickou signalizaci, (pozn. : v praxi se nejčastěji setkáme s poplachovou sirénou).

Zařízení pro přenos požárního poplachu

Zprostředkovává přenos požárního poplach z ústředny EPS do ohlašovny požáru.

Řídící jednotka samočinného zařízení požární ochrany

Aktivuje samočinné zařízení požární ochrany po obdržení signálu od ústředny.

Zařízení pro přenos hlášení poruchových stavů

Zprostředkovává přenos poruchového signálu z ústředny do přijímací stanice hlášení poruchových stavů.

Napájecí zařízení

Dodává napájení pro ústřednu a pro komponenty, které jsou napájeny z ústředny. Napájecí zařízení se může skládat z několika zdrojů (např. síťové napájení a náhradní zdroje). Napájecí zařízení musí při výpadku základního zdroje napájení zůstat v časově omezeném provozu na vlastní náhradní zdroj. Časově omezeným provozem se rozumí min. 24 hodin v pohotovostním stavu, z toho 15 minut ve stavu signalizace požáru.

Propojovací elementy

Jsou všechny elementy, které tvoří propojení mezi různými komponenty systému EPS (pozn. : kabeláž, svorkovací krabice, patice atd.)

5 KAMEROVÉ SYSTÉMY (CCTV)

Kamerové systémy zaznamenávají v současné době veliký rozvoj, a zvyšující se zájem ze strany investorů. Tyto systémy jsou nasazovány všude tam, kde je potřeba mít přehled a provádět nepřetržité monitorování pohybu osob, automobilů, nebo materiálu. Jedná se zejména o skladové prostory, výrobní procesy, benzinové čerpací stanice, haly s nekontrolovatelným pohybem většího množství osob, ale i ke střežení soukromých pozemků a objektů, garáží, nebo veřejného prostranství (kina, nádraží aj.).

Kamerový systém má za úkol pořizovat obrazové záznamy z vybraných prostor jako důkaz. U EZS se pouze dozvíme, že někdo byl uvnitř objektu a případně, kde se pohyboval. U přístupových systémů máme naprostou jistotu, kde se pohyboval, a víme, že se dotyčná osoba prokázala vstupníkem např. pana Nováka, ale nemáme jistotu, že to byl opravdu pan Novák. U dobře navrženého kamerového systému získáme snímek dotyčné osoby, která se po objektu pohybovala.

Obecně lze říci, že kamerové systémy nabírají v celosvětovém měřítku nových rozměrů a progresivně tlačí na všechna odvětví průmyslu, obchodu a všude tam, kde jsou kladeny požadavky na monitoring osob apod. S kamerovými systémy se setkáváme doslova na každém kroku a tato technologie donutila většinu firem alespoň se zamyslet nad náklady investovanými do zabezpečení nebo ostrahy objektů. Kamerové systémy nacházejí uplatnění při hlídání parkovišť, objektů, monitorování technologických procesů nebo třeba kontrole pracovníků při práci. Propojením na docházkové, přístupové nebo elektronické zabezpečovací systémy se z nich stávají aktivní prvky v boji proti kriminalitě a zabraňují škodám na majetku.

Technologie kamerových systémů spočívá ve snímání daného prostoru kamerou se standardním nebo vysokým rozlišením a přenášení obrazu po optických, datových nebo koaxiálních kabelech do místa zpracování. S úspěchem se pro přenos obrazu využívá i mikrovlnné spojení, ISDN nebo telefonní linka, což umožňuje monitorovat objekty vzdálené i několik kilometrů. Zpracování obrazu se provádí pomocí např. multiplexeru, což je zařízení zobrazující signály z jednotlivých kamer na monitoru, ovládající pohyb kamer a připravující obraz pro záznam. Záznamová zařízení dělíme do dvou základních kategorií -jako digitální nebo analogová.Analogový záznam má své místo všude tam, kde nejsou vysoké

požadavky na chod bez obsluhy a dálkovou správu.

V současné době jsou již na ústupu pomaloběžné páskové videorekordéry, které umožňovaly záznam v řádu desítek až stovek hodin a u nichž byla editace záznamu poněkud časově náročná.

Dnešní digitální rekordéry využívají jako záznamové médium většinou pevné disky, stejné, které se používají ve stolních počítačích. Mají vynikající poměr cena / záznamová kapacita a doba záznamu se zde pohybuje řádově v desítkách dnů v závislosti na počtu kamer a kvalitě obrazu. Umožňují za dostupné finanční prostředky záznam i přenos obrazu po síti při velmi slušném rozlišení detailu a obnovovací frekvenci snímků.

Při použití standardní techniky je nutné instalovat kamery, propojit je kabely s nějakým kvadrátorem, sekvenčním přepínačem nebo multiplexerem a případně s videodetektorem pohybu a dále s pomaloběžným videorekordérem, který dokáže na běžnou tříhodinovou kazetu nahrát třeba i týden záznamu.

I do oblasti kamerových systémů ovšem již vtrhla digitalizace a za poměrně přijatelnou cenu část problémů velice elegantně vyřešila.

Pro záznam poplachových situací, můžeme použít skrytou černobílou kameru, umístěnou ve funkčním detektoru pohybu. Obrázky z této kamery jsou komprimovány a nahrávány spolu s datem a časem pořízení do paměťové FLASH karty, známé například z digitálních fotoaparátů.

Kamera snímá sledovaný prostor a obrázky ukládá do vyrovnávací mezipaměti, což umožňuje využití záběrů pořízených i před vznikem poplachové události. Nahrávání snímané scény na FLASH kartu může být aktivováno jak detektorem pohybu, ve kterém je kamera umístěna, tak i nějakým vnějším signálem. Počítačem nastavená kamera pak v případě poplachu zaznamená určený počet fotografií nebo celou videosekvenci. Detektor s kamerou je programovatelný a lze například určit, že po naplnění kapacity FLASH karty se začnou nejstarší záznamy přepisovat novými a podobně.

Ke kameře se dodává dálkový ovladač, který umožňuje aktivovat a deaktivovat funkci automatického nahrávání a také ručně zapnout zaznamenávání sledované scény. Vypnutí nahrávání je přitom chráněno bezpečnostním číselným kódem.

Při prohlížení nahrávek se paměťová karta jednoduše vyjme z detektoru a vloží se do čteč-

ky, připojené k počítači. FLASH karty se dodávají v několika velikostech a na jednu kartuje možné nahrát až 6000 černobílých obrázků.

Uvedený systém tak nahradí kameru, videodetektor pohybu a pomaloběžný videorekordér, eliminuje nahrávání "hluchých" míst a zároveň omezí kabelovou instalaci pouze na napájení detektoru s kamerou.

Kamerové systémy mají široké spektrum použití vzhledem k jejich možnému stavebnicovému rozšiřování, tyto systémy lze libovolně rozšiřovat dle požadavků. Výstup systému lze sledovat přímo na monitoru obsluhy, nebo lze tento signál přenášet na vzdálené stanoviště pomocí web serverů a také je možno celý záznam archivovat na záznamové zařízení pro zpětnou kontrolu střežení [6].

Aplikace CCTV v oblasti zabezpečovací techniky lze shrnout do těchto úloh :

- sledování plotů v kombinaci s EZS
- sledování pozemků a objektů
- sledování vjezdů a vstupů do objektu
- kontrola oprávněnosti dokladů u vstupních propustí
- sledování exponátů v muzeích a galeriích
- sledování bankovních provozů a provozů v obchodních domech
- sledování odpadních plynů a vod
- sledování parkovišť
- sledování provozu zdymadel
- sledování provozu letišť a přistávacích ploch
- monitorování požárního nebezpečí objektů
- diskrétní sledování v infraspektru

Výhody systému CCTV :

- monitoruje non-stop střežený prostor
- umožňuje dokonalou historii události (archivuje záběry z chráněného prostoru před, v průběhu i po mimořádné události)
- kompatibilita s ostatními bezpečnostními systémy
- přesná lokalizace míst narušení s identifikací narušitele
- prevence
- pomocí skrytých kamer zajištění ochrany majetku i proti profesionálním narušitelům
- napomáhá k odhalení případné neloajálnosti vlastního personálu

5.1 Kamery

Základním konstrukčním prvkem kamery je snímací čip. V kamerách pro bezpečnostní systémy se používají snímací čipy CMOS a CCD (zkratka z anglického názvu Charge Coupled Divice - česky nábojově vázaná struktura). Čipy CMOS jsou levnější, ale jejich cena je vykoupena horšími parametry. Mají výrazně horší citlivost a většinou i menší rozlišení a menší spolehlivost.

Prvním předpokladem je určení typu kamer - černobílé nebo barevné a jejich provedení - vnitřní nebo venkovní. Dále je nutné určit, mají-li být kamery skryté, nenápadné (malé rozměry) nebo naopak výrazné (odstrašující efekt). Dalším důležitým faktorem jsou světelné podmínky ve kterých budou kamery pracovat - běžné světelné podmínky, kdy lze použít kamery se standardní citlivostí, špatné osvětlení (šero, pouliční osvětlení), kdy se používají kamery ultracitlivé nebo den/noc popř. úplná tma, kdy se použijí kamery s IR přisvícením nebo přídavné osvětlení a v neposlední řadě rozlišení kamer. Pro výběr vhodného objektivu je důležitý údaj o sledovaném prostoru (vzdálenost snímaného objektu od kamery a požadovaná šířka záběru), případně nutnost použití proměnného ohniska - zoomu. Dále jsou kamery statické (pevné) nebo pohyblivé (s možností natáčení) a umístění (stěna, strop, podhled ...).

6 PŘÍSTUPOVÝ SYSTÉM (ACS)

Systém řízení přístupu (často nazývaný přístupový systém) umožní osobě na základě prokázání oprávněnosti vstup nebo vjezd do objektu, případně do střežené části objektu.

Systémy kontroly vstupu řídí přístup osob, resp. vozidel do chráněných prostorů nebo ke chráněným zařízením, případně informacím, na základě přidělených přístupových práv. Tato zařízení umožňují sledovat pohyb osob v definovaných prostorových zónách. Jako nositel přístupového oprávnění jsou využívána různá média,např.magnetické a čipové karty,čipové přívěšky různých tvarů a nejnověji se využívá biometrických informací, např.otisky prstů,zobrazení oční duhovky nebo sítnice nebo obraz obličeje.

Přístupový systém bývá označován zkratkou "PS", případně "ACS" (dle anglického názvu access control system).

Systém sestává z čtečky (používá se rovněž název terminál) identifikačního média, vyhodnocovací (používá se rovněž název řídící) jednotky, a výstupních obvodů. Vyhodnocovací jednotky bývají zpravidla spojeny datovou sběrnicí (nejběžněji RS 485) pro vzájemnou komunikaci. Tato sběrnice bývá přes příslušný převodník (nejčastěji na komunikační rozhraní RS 232) přizpůsobena k propojení s PC, odkud je možné systém centrálně monitorovat, nastavovat oprávnění a vstup/výstupní vazby systému.

Identifikačním médiem nejčastěji bývá karta, nebo přívěsek na klíče, ve kterém je zakódována datová informace. Uložení datové informace může být řešeno magneticky, opticky, nebo elektronicky. O způsobech uložení datového kódu na média podrobně pojednává tento článek.

Čtečka snímá uložený kód z identifikačního média, který převede na elektronický datový tok daného formátu a tento předá po komunikačním rozhraní nejčastěji se používá rozhraní WIEGAND) k dalšímu zpracování vyhodnocovací jednotce.

Vyhodnocovací jednotka zpracovává vstupní informace od čtečky (nebo několika čteček), komunikuje z řídícím PC a ostatními jednotkami (jsou-li zapojeny do sběrnice) a na základě kombinace vstupních informací dle předem definovaného programu řídí přes výstupní obvody další zařízení (el. zámky, ovládání elektromotorů, pohonů vrat atd.). O způsobech ovládání ostatních zařízení přes výstupní obvody podrobně informuje tento článek.

V některých případech, zejména u systému sledování docházky je čtečka a vyhodnocovací jednotka zaintegrována v jednom komponentu.

Převodník datového rozhraní umožní připojení vyhodnocovacích jednotek zapojených do sběrnice k monitorovacímu a konfiguračnímu PC. Vyhodnocovací jednotky nejčastěji komunikují přes rozhraní RS 485 (poměrně značný dosah po 1 páru vedení - v průměru 1.2km a pro přístupový systém přijatelný datový tok do 2Mb). Standardní PC bývá vybaveno výstupem rozhraní RS 232. Proto je nutné vzájemné přizpůsobení komunikačního rozhraní mezi čtečkami a vstupního komunikačního rozhraní na PC.

Konfigurační a monitorovací PC umožní přes uživatelské prostředí příslušného software konfigurovat oprávnění výstupních operací ve vztahu k jednotlivým kódům uloženým na identifikačních médiích a nadefinování dalších vstup/výstupních operací v závislosti na čase a dalších elektronicky sledovatelných veličinách. Dále umožní sledovat a monitorovat chronologickou historii jednotlivých událostí snímání kódů a provedených či zamítnutých výstupních operací. Z této historie pak je možné sestavit různé vztahy, grafické průběhy, přehledové schémata a možnosti předmětových roztřízení. Je-li PC, na které je připojena sběrnice začleněno do lokální (ale i rozsáhlé, nebo i do internetové) počítačové sítě je možná dálková správa,nebo monitorování systému z jiného PC (umožňuje-li to příslušný software dodávaný k přístupovému systému).

Výhody přístupového systému :

- jedna identifikační karta, nebo čip (klíčenka) nahrazuje několik klíčů
- umožňuje kontrolu pohybu osob v určitém objektu
- jednoduché omezení pohybu nepovolaných osob, případně povolení přístupu pouze určitým osobám
- časové omezení přístupu vybraným osobám
- není nutný bezprostřední kontakt se zámkem
  stanovená jedinečnost, není možnost si vytvořit duplikát identifikačního prvku tak, jako například u klasického klíče
- komunikace s PC, sledování průchodů jednotlivých zaměstnanců
- definice „KDO, KDY a KAM“

II. PRAKTICKÁ ČÁST

7 VÝBĚR SYSTÉMŮ UMOŽŇUJÍCÍCH INTEGRACI

7.1 Galaxy

Jedná se o výrobky anglické firmy MicroTech SECURITY, jsou vhodné pro nejvyšší rizika s možností kombinace s přístupovým systémem.

Systém Galaxy je označení 5 typů technologicky vysoce vyspělých mikroprocesorem řízených ústředen EZS homologovaných pro vyšší bezpečnostní rizika. Tento systém je možno konfigurovat podle konkrétní aplikace. Jeho programové, vybavení je na nejvyšší úrovni a umožňuje uživateli vytvořit zabezpečovací systém s vysokým komfortem a mnoha různými funkcemi. Bezpečnost a spolehlivost je ověřena v praxi v mnoha významných aplikacích.

Systém Galaxy tvoří následující řada ústředen

Galaxy 8 a Galaxy 18/6 - nejmenší ústředny řady, vhodné pro zabezpečení bytů, rodinných domů nebo pro malé objekty, jako například obchody, drobné provozovny, buňky s technologií apod.

Galaxy 60/6, Galaxy 128/6 - ústředny pro menší až středně velké budovy, oproti předchozím dvěma typům mají více softwarových funkcí jako například univerzální časovače, zákaznické zóny a více typů zón a výstupů. U Galaxy 128 je možné ovládat jednotlivé podsystémy pomocí časovačů.

Galaxy 500/6, Galaxy 504/6 - ústředny pro rozsáhlé objekty a areály nebo pro i středně velké a menší objekty s většími požadavky na dělitelnost do samostatně ovladatelných podsystémů. Ve srovnání s předcházejícími dvěma typy se liší hlavně počtem zón, výstupů, čteček, uživatelů, podsystémů a softwarových spojů.

Galaxy 512/6 - tyto ústředny svým určením vybočuje z řady ústředen 8-500. Je určená pro nasazení v objektech s vysokými riziky, přičemž využívá všechny výhody starších ústředen a konstrukčně je téměř shodná s ústřednou Galaxy 500. Její výjimečnost spočívá v mocném softwarovém vybavení. Navíc obsahuje některé funkce použitelné zejména v oblasti bankovních aplikací jako je časový zámek, časovače pro uzamčení grup, speciální zóny a rutiny pro monitorování bankomatů, apod. Ústředna má funkce vyžadující poměrně přísná režimová opatření (vynechat lze pouze jednu zónu, nelze ovládat systém v instalačním re-

žimu, zákaz nuceného zastřežení a automatického odstřežení).

Řada ústředen Galaxy umožňuje zabezpečit prakticky libovolný objekt. Ústředny Galaxy 8 a 18 nacházejí své místo především v menších instalacích, kde je požadován vysoký komfort obsluhy, zatímco ústředny Galaxii 60 a 500 jsou přímo předurčeny pro rozsáhlé a z hlediska dělení komplikované objekty a komplexy budov. Poslední zmíněné typy ústředen se často používají i ve středně rozsáhlých instalacích se zvýšenými nároky na dělitelnost. Protože ústředny nekladou prakticky žádná omezení z hlediska dělitelnosti a jsou velmi flexibilní jak po hardwarové tak i po softwarové stránce, lze ji nasadit i v objektech, kde se dá předpokládat rozšíření systému nebo změna jeho logické struktury.

Bohaté programové vybavení ústředny je velmi propracované a poskytuje technikovi řadu mocných nástrojů k vyřešení i velmi netypických požadavků koncového uživatele. Ústřednu lze rozdělit na několik nezávisle ovládaných podsystémů. Možnosti jejich ovládání nejsou nijak omezeny. Z libovolné klávesnice lze ovládat jeden, několik nebo všechny podsystémy, přičemž přístup k nim závislý navíc i na oprávnění uživatele. Akustická odezva klávesnice na poplachy a další události v systému se může vztahovat i na jiné části systému. O variabilitě systému vypovídá i do čtyř režimů programovatelné podsvícené displeje individuálně pro každou klávesnici a dvě "horké klávesy" na každé klávesnici, jimž je možné přiřadit některou z funkcí menu. Dělitelnost lze ještě dále zvyšovat samostatným ovládáním jednotlivých koncentrátorů.

Pro připojení čidel jek dispozici 38 typů pevně předdefinovaných zón, od základních typů až po speciální zóny. Kromě toho lze dva typy zákaznických zón sestavit podle zcela specifických požadavků. Stejná situace je i s programovatelnými výstupy, kde ústředna nabízí 47 předdefinovaných typů. Mocným nástrojem jsou tzv. programovatelné spoje, které umožňují logicky propojovat zóny, kódy a programovatelné výstupy.

Při návrhu systému bylo pamatováno i na snadný servis. Z klávesnice je možné měřit odpor ve smyčkách a napětí na koncentrátorech. Navíc je možné sledovat i kvalitu komunikace ústředny s jednotlivými moduly systému (vyjádřeno hodnotou na displeji). Komunikace je indikována také LED diodami na jednotlivých prvcích.

Tvůrci systému nezapomněli ani na uživatelský komfort při ovládání, kde se nabízí nepřeberné množství možností. Uživatelé mohou ovládat jeden nebo více podsystémů a to buď najednou nebo s možností výběru. Každý podsystém lze zapínat plně nebo částečně a to

okamžitě i s odchodovým zpožděním. Systém nabízí speciální zóny, které se chovají dvojím způsobem podle toho, zda je podsystém střežen úplně nebo částečně. Další neobvyklou funkcí je tzv. zapínací logika, která umožňuje pro každý podsystém definovat podmíněné zapnutí v závislosti na stavu ostatních podsystémů. Hloubka přístupu do menu je rozdělena do sedmi úrovní, které lze přidělit podle znalostí uživatele. Kromě plného menu lze sestavit i menu zkrácené, které má stejně jako menu plné úrovně hierarchickou strukturu. Uživatele ale není nutné pouštět do menu vůbec a lze mu povolit pouze zapínání a vypínání systému pomocí horkých kláves, které mohou mít přiřazeny některé z funkcí menu. Ústředna umožňuje současné ovládání systému několika uživateli.

7.2 Intellex

Intellex je inteligentní digitální videosystém, který v sobě kombinuje funkce multiplexeru, alarmové jednotky, detektoru pohybu, zvukového, textového a obrazového záznamu a mnoho dalších funkcí. Intellex umožňuje sledovat živý obraz nebo přehrávat obrazový záznam s nebo bez zvukového a textového záznamu a zároveň připojit vzdálené uživatele, archivovat data, vyhledávat záznamy a mnohé další funkce – to vše při současném záznamu obrazu ze všech kamer a s ovládáním sdruženým do jednoduchého a intuitivního grafického rozhraní.

Intellex je možné připojit do počítačové sítě Ethernet, což umožňuje vytvořit rozsáhlý systém pro záznam a zpracování obrazu skládající se z Intellexů a PC stanic s programem Network Client. Tento program umožňuje plnohodnotné připojení vzdálených uživatelů. Při připojení do počítačové sítě nabízí i nové bezpečnostní funkce pro zvýšení bezpečnosti.

Záznamem a přehráváním obrazových, zvukových a textových záznamů, integrací inteligentních vyhledávacích nástrojů a možnostmi správy a konfigurace nad rámec vlastností poskytovaných mnoha standardními systémy digitálního záznamu nabízí Intellex efektivní možnost komplexní analýzy událostí. Široce konfigurovatelný detektor pohybu s analýzou velikosti, směru a rychlosti pohybu objektu umožňuje pomocí záznamového filtru IntelleCord nahrávat pouze to, co je pro uživatele skutečně důležité. Rozšířený textový filtr umožňuje nahrávat pouze důležité transakce v případě splnění nadefinovaných kritérií. Velké množství dalších nadstandardních uživatelsky konfigurovatelných funkcí poskytuje uživateli možnost přizpůsobení systému přesně podle jeho požadavků a potřeb.

Pomocí vyhledávací funkce SmartSearch je možné uživatelsky definovat nejrůznější konfigurovatelná vyhledávací kritéria pro vyhledávání v obrazových i textových záznamech a nalezenou událost okamžitě přehrát v digitální kvalitě jako časově synchronizovaný obrazový, textový a zvukový záznam. Pro vyhledávání v obrazových záznamech je mimo jiné možné využít široce konfigurovatelný detektor pohybu s analýzou velikosti, směru a rychlosti pohybu objektu, pro vyhledávání v textových záznamech rozšířený textový filtr. Multikanálové přehrávání událostí analýzu záznamů dále zefektivňuje. Vyhledávání a přehrávání záznamů probíhá nezávisle na dalších funkcích a současně se záznamem obrazu ze všech kamer.

Intellex poskytuje možnosti síťového propojení a dálkové správy a je jednoduše integrovatelný s dalšími systémy.

7.3 Skyla

SKYLA Pro II je program pro konfiguraci, sběr dat a monitoring systémů kontroly vstupu malého až středně velkého rozsahu s řídicími jednotkami HUB Pro a docházkovými terminály DT2000 SA. Program umožňuje podrobné sledování jak vlastní činnosti přístupového systému (příchody, odchody, narušení režijních opatření…), tak i zpětné sledování operací a zásahů všech operátorů. Ze získaných dat může uživatel vytvářet filtrované přehledy, provádět základní vyhodnocení docházky nebo získaná data zpracovávat v docházkových programech.

SKYLA je určena pro operační systémy Windows NT / 2000 / XP a je koncipován jako aplikace typu klient/server. Pro uživatele tento koncept přináší především možnost souběžné činnosti více. Jednotlivé klientské aplikace komunikují se serverem prostřednictvím TCP/IP protokolů – systém tak lze spravovat prakticky odkudkoliv. Přístup všech operátorů je chráněn heslem, administrátor může navíc každému z nich povolit přístup jen do některých částí programu. Heslem lze rovněž chránit přístup datového serveru k SQL databázím.

Základní úlohou programu je nastavení přístupového systému. Jednoduchým a přehledným způsobem tak nadefinujete časové zóny, parametry všech jednotek HUB Pro i docházkových terminálů DT2000 SA, přístupové úrovně pro hromadné přidělování oprávnění

kdo, kdy a kam může vstoupit, personální údaje osob včetně fotografií a uživatelsky nastavitelných poznámkových polí nebo oprávnění pro všechny operátory, kteří s programem mají pracovat.

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

Monitorování systému provádí SKYLA Pro II dvěma způsoby: za prvé řádkovým způsobem vypisuje všechny události, které zaznamenávají jednotky HUB Pro nebo terminály DT2000 SA. Každá událost je doplněna o datum a čas vzniku a všechny ostatní potřebné informace (např. jméno a příjmení osoby). Tento přehled lze filtrovat, třídit a prohledávat podle různých kritérií nebo nechat program barevně odlišovat jednotlivé typy událostí ve výpisu. Druhým způsobem sledování systému je záznam veškerých akcí operátorů – editace nebo mazání údajů v tabulkách, přihlášení, odhlášení apod.

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

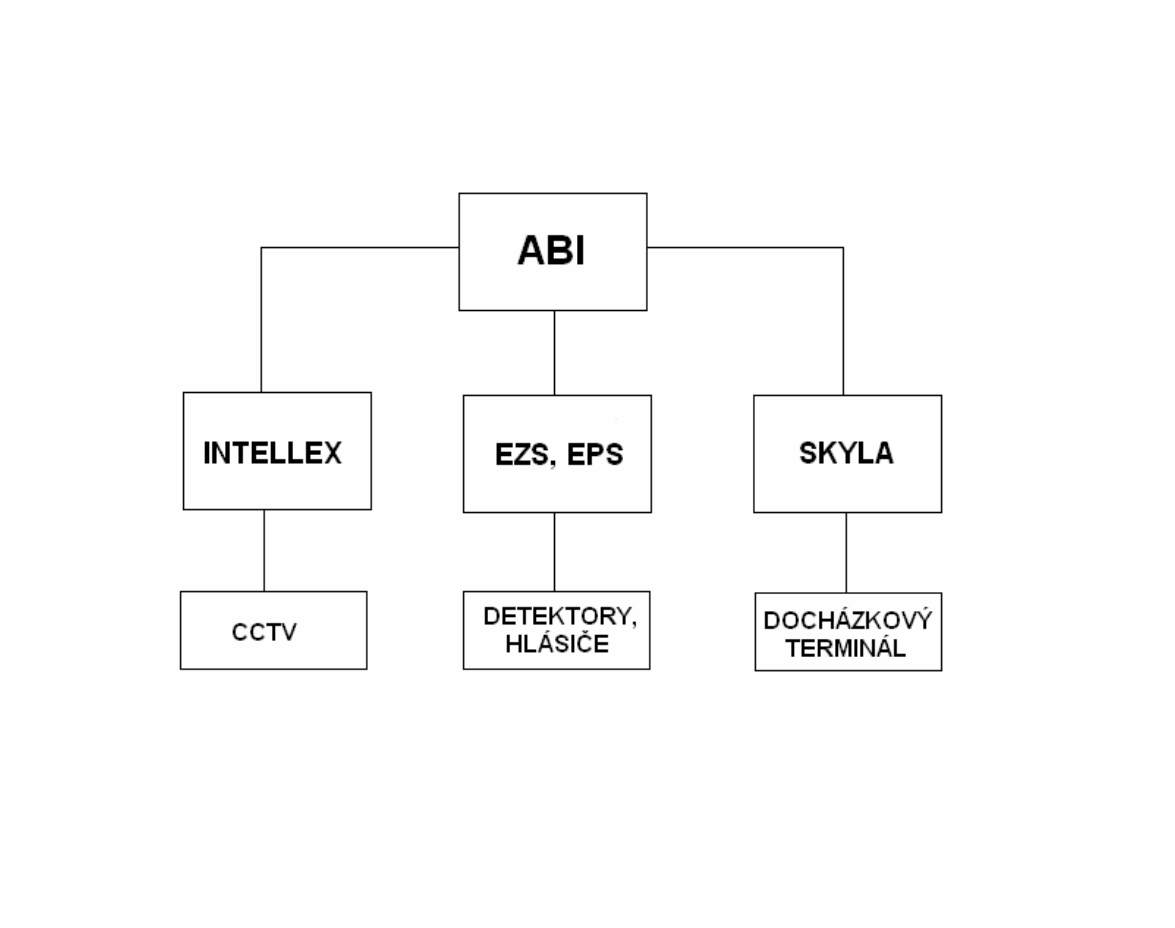
SKYLA Pro II umožňuje těsnou spolupráci s docházkovým programem DOCH. Databáze obou programů jsou provázány a záznam osoby provedený do tabulky SKYLY Pro II tak bude automaticky proveden i do databáze programu DOCH. Oba programy mohou využívat společný komunikační server - v databázi SKYLY Pro II tak je uložen přehled veškerých událostí v systému, zatímco do docházkové databáze programu DOCH se ukládají pouze události docházkového charakteru.

SKYLA Pro II nabízí celou řadu diagnostických nástrojů užitečných pro oživení systému nebo lokalizaci hardwarových problémů – od mapování sběrnic pro zjištění všech připoje-

ných a komunikujících jednotek až po podrobnou diagnostiku vybrané jednotky nebo docházkového terminálu. Tou můžete dálkově ověřovat stavy všech vstupů a výstupů, kontrolovat velikost napájecího napětí, mazat jednotlivé databáze v paměti jednotky nebo ovládat výstupy. Lze tak dálkově odemykat zámky, ovládat EZS, rušit probíhající poplachy apod.

8 NÁVRH INTEGROVANÉHO ZABEZPEČENÍ FIRMY

Pro integraci jednotlivých systémů jsem zvolil software ABI (Advanced building inteligence).



Obr. 3.Schéma integrace systémů

8.1 ABI - Advanced building inteligence

ABI je software pro dálkovou správu, řízení a monitorování integrovaných systémů v samostatných budovách i rozsáhlých komplexech. Jedná se o modulární vícevrstvou aplikaci typu klient/server, která umožňuje snadnou práci z jakéhokoli počítače připojeného do sítě Internet/intranet a vybaveného libovolným webovým prohlížečem.

Základními funkcemi ABI jsou centrální dálková správa uživatelů, ovládání a monitorování veškerých zabezpečovacích systémů a funkce pasport pro správu a údržbu budov. Díky svým unikátním funkcím Vám ABI umožní dosáhnout snížení finančních nákladů nutných na provoz obsluhovaných lokalit i snížení celkového počtu personálu potřebného pro vlastní obsluhu a provoz.

ABI nabízí plnou otevřenost vůči integrovaným systémům od libovolných výrobců. Standardní součástí instalace ABI je rozhraní ABI Web Service, které umožňuje výměnu údajů mezi ABI a aplikacemi třetích stran (personalistika, mzdy apod.).

ABI také umožňuje operativní řešení krizových stavů, jako je požár, napadení apod. V případě vzniku kritické situace, která vyžaduje nouzový únik z budovy, Vám ABI dokáže zobrazit nejkratší únikové trasy, umístění hasících přístrojů a další důležité informace.

Správa uživatelů

ABI umožňuje snadnou a přehlednou centrální dálkovou správu uživatelů odkudkoli a kdykoli. V rámci správy uživatelů je možné provádět operace přidávání a mazání uživatelů, přiřazování karet a přístupových kódů, přidělování oprávnění, vytváření skupin uživatelů i skupin oprávnění. Dále lze definovat nové zabezpečovací ústředny včetně terminálů a přístupových a zabezpečovacích oblastí.

Monitorování

ABI nabízí přehledné grafické monitorování zabezpečovacího systému, které je postaveno na standardních vektorových formátech grafiky.

Z ABI lze provádět dálkové zapínání nebo vypínání zabezpečovacího systému ze střežení. Při poplachu je zajištěna automatická lokalizace a zobrazení aktivovaného detektoru. Veškeré události se ukládají do protokolu, v němž lze vyhledávat a filtrovat.

Provázanost s kamerovými dohledovými systémy, jako je Intellex, Convision nebo IP kamery, Vám umožňuje podívat se přímo na místo, kde došlo k poplachu, a ověřit si tak, zda nešlo jen o falešný poplach.

Operátoři

Uživatelé s povoleným přístupem do ABI se nazývají operátoři. Každému typu operátora lze nastavit, které nabídky ABI bude mít dostupné, povolené skupiny uživatelů, povolené lokality a oprávnění a přístup do monitorování.

Operátorovi se v ABI zobrazují jen ti uživatelé, kteří patří do skupin, které má povolené, nebo nejsou v žádné skupině a může pracovat jen jemu povolenými lokalitami a oprávněními. Takto lze vytvořit různé přístupy pro administrátory, techniky, personalisty nebo pracovníky pultu centralizované ochrany (PCO).

Pasport

Pasport je funkce ABI určená pro správu a údržbu budov a tvoří funkční základ pro tzv. facility management. Umožňuje evidenci vybavení, inventarizaci majetku v budově a sdílení informací nad jednou společnou databází. Existují různé druhy pasportu: pasport stavebních částí (stavební), jednotlivých technologií v budově (technologický) nebo využitelný pro energetický audit (energetický).

Pasport je rovněž využitelný pro rychlé získání podkladů k zadávání požadavků na servisní práce a opravy budov, pro outsourcing služeb jako je úklid nebo malování apod.

Stavební pasport může zahrnovat vše od rozměrů a povrchů místností, plochy a materiály podlah, zdí a stropů, počty a plochy oken a dveří apod.

Technologický pasport může obsahovat trasy a prvky elektronického zabezpečení, kamerových systémů, přístupových bodů, požární signalizace, HVAC technologií atd. Energetický pasport zahrnuje koeficienty použitých materiálů, oken, dveří, výpočty zisků a ztrát apod.

9 VŠEOBECNÁ ČÁST

9.1 Rozsah projektu

Projekt řeší instalaci elektrické zabezpečovací signalizace (EZS), elektrické požární signalizace (EPS), uzavřený televizní okruh (CCTV) a přístupový systém (ACCES). Cílem projektu je dosáhnout integrace všech zmiňovaný systému.

9.2 Základní technické údaje

Budova firmy která je určená k zabezpečení se skládá ze čtyř pater.

- První patro – recepce (vrátnice), výtah a schody do druhého patra
- Druhé patro - konferenční sál, výtah a schody do třetího patra
- Třetí patro – 4 místností, které slouží jako kanceláře, výtah a schody do čtvrtého patra
- Čtvrté patro – 4 místnosti – 2 kanceláře, 1 účtárna, 1 IT- místnost kde jsou servery, a veškerá informační technologie, která budovu řídí.

10 POPIS ŘEŠENÍ INTEGRACE SYSTÉMU

10.1 Ústředna

Pro řízení a tzv. srdce celého systému jsem vybral řídící ústřednu Galaxy 60 ovládanou klávesnicí MK7. Ústředna umožňuje integraci všech součástí EZS. Je připojena po síti LAN na PC přes modul E 080 do místnosti 402, kde je také nainstalována. Součástí je digitální telefonní komunikátor E062 - 43 s integrovaným modemem pro dálkový servis a hlášení na PCO.

10.2 Elektrická zabezpečovací signalizace (EZS)

10.2.1 Duální detektory

K zabezpečení pomocí EZS jsem použil duální detektory DX60PLUSI. Duální detektor DX60PLUSI (MW + PIR) je osazen velmi kvalitním PIR detektorem s víceohniskovou optikou, kulovou čočkou a vyhodnocením "QUAD ZONE LOGIC". Prostor je pokryt velmi hustým detekčním diagramem s 82 samostatnými segmenty. Mikrovlnná jednotka má vestavěny obvody samokontroly (při poruše MW jednotky dojde k přepnutí detektoru do režimu PIR se zvýšenou spolehlivostí) a obvody pro tvarování detekčního diagramu s možností nastavení krátkého nebo dlouhého dosahu, díky kterému je maximálně eliminován průnik mikrovln mimo střežený prostor. PIR detektor je chráněn proti zamaskování s následným vyhlášením poplachu. Vylepšené utěsnění optické soustavy eliminuje falešné poplachy způsobené např. prachem nebo hmyzem nebo prouděním vzduchu.

Detektory jsou značeny (D01 – D09 pro lepší přehled. Viz. Schéma nákresů firmy 1 až 5. Detektor D01 je umístěn pod kamerou systému CCTV, ve vstupní hale v prvním patře. Snímá dveřní prostor, vrátnici. D02, který je instalován na vrátnici pokrývá výtah a schodiště. V druhém patře se nachází detektor D03 a D04. Střeží Vstup do konferenčního sálu a konferenční sál.Oba jsou umístěny pod kamerami. V patře třetím je D05, který snímá prostor mezi kancelářemi. Jé též instalován pod kamerou. Ve čtvrtém patře jsou detektory D06 – D08. D06 snímá prostor před kancelářemi a je instalována pod kamerou. D07 je instalován v IT centru, kde je největší riziko úniku informací a proto je doplněn i kamerou,

která tuto místnost snímá. D08 je v účtárně kde se nachází trezor s penězi a důležité dokumenty. Poslední detektor D09 se nachází pod kamerou ve venkovní části objektu. Střeží hlavní příjezdovou bránu a zároveň část vstupu do budovy.

Obr. 4.DX 60

PLUS I

10.2.2 Detektory tříštění skla

V prvním patře je použito k plášťové ochraně detektorů tříštění skla GLASSTREK 456. Jedná se o duální audiodetektor, který vyhodnocuje tlakový náraz při rozbití skla, porovnává zaznamenaný zvuk a frekvenci tříštěného skla s údaji uloženými v paměti a sleduje časový průběh jednotlivých událostí. Frekvence tlakové vlny a tříštěného skla je digitálně zpracovávána v mikroprocesoru. Tyto detektory jsou rozmístěny po celém obvodu prvního patra po 9m což je jeho max. dosah.

10.2.3 Magnetické kontakty

Ve třetím a čtvrtém patře jsou ve dveřích od kanceláří a v účtárně instalovány magnetické kontakty ve dveřích. Celkem 7 magnetických kontaktů typu MC 2110 AH – hliníkový magnetický kontakt. Jde o čtyř drátový hliníkový příložný magnetický kontakt. Vodiče jsou pevně zality v kontaktu a jsou chráněny armovanou hadicí. Pracovní mezera těchto kontak-

tů je 50 mm. Mg. Kontakty jsou napojeny na ústřednu z které prostřednictvím PC snadno zjistíme ve kterém místě došlo k narušení.

10.3 Hlásiče požáru

10.3.1 Automatické hlásiče

Ve všech patrech budovy jsou instalovány automatické hlásiče požáru typu SS 2351 KNL/KRL - opticko kouřový detektor řady 300. Označení P01 – P14, celkem tedy 14 instalovaných hlásičů požáru. Hlásič SS 2351 KNL/KRL je kombinovaný detektor kouře a teploty řady 300.Reaguje na kouř vznikajícího požáru anebo na rychlý nárůst okolní teploty. Pokud je přítomen naráz kouř i nárůst teploty, detektor reaguje rychleji. Skládá se z detekční hlavice a patice. Je zvolený detektor má patici NL, která provádí resetaci detektoru samostatně, tj. nevyžaduje resetaci detektoru přerušením napájení .Prostřednictvím výstupního NC/NO relé jsou detektory připojeny k ústředně Galaxy 60 systému EZS.

V prvním patře je instalován hlásič P01 na stropě vzdálen od recepce asi 5 pět metrů. P02 je instalován v chodbě mezi schodištěm a výtahem. P03 a P04 jsou v konferenční místnosti, všechny jsou umístěny na stropě. P05 se nachází v třetím patře v prostoru mezi kancelářemi a P06 – P09 jsou instalovány po jednom v jednotlivých kancelářích. Všechny jsou instalovány na stropě. Ve čtvrtém patře je P10 v prostoru mezi kancelářemi. P11 – P14 po jednom v kancelářích, IT místnosti a účtárně. V IT místnosti je též instalováno stabilní hasící zařízení na plyny typu HFC-227ea. Po detekci potenciálního požáru hlásiči a časovém zpoždění, určeném pro evakuaci personálu, dojde do 10 sekund k automatickému celkovému zaplavení chráněných prostor hasicím médiem. Hasicí účinek plynu spočívá především v absorpci tepla z plamenů.

V každém patře je na stěně vedle schodiště instalován požární tísňový hlásič BF 380 MR. Požární tlačítkový detektor je aktivován zatlačením plastové náhrady skla. Aktivace tlačítka je signalizována žlutým páskem nad horní vodorovnou hranou zatlačeného plastu a změnou stavu výstupního relé.

Všechny hlásiče komunikují s ústřednou EZS. Jsou umístěny na 24 hodinové smyčce. V případě detekce požáru je vyvolán poplach. Pomocí ústředny a PC je možné zjistit ve kterém místě byl poplach vyvolán. Dále se přenáší informace o poplachu na PCO prostřednictvím ústředny a jejího komunikačního modulu.

Obr. 5. Hlásič SS 2351

KNL/KRL

10.4 Uzavřený televizní okruh (CCTV)

10.4.1 Kamery

V objektu jsou použity kamery typu Samsung SHC 730. Jedná se o profesionální systémovou barevnou přepínatelnou den/noc kameru s digitálním zpracováním obrazu.Tato kamera je velmi kvalitní, spolehlivá a má perfektní podání obrazu i za nepříznivých světelných podmínek (vysoký kontrast mezi snímaným objektem a jeho pozadím, silné protisvětlo, nízká úroveň osvětlení apod.).

Kamera Samsung SHC 730 obsahuje tyto funkce :

- **Enhanced SSNR** je funkce digitálního odstranění šumu a „duchu“ v obraze. Tím také dochází ke zvýšení poměru signál/šum. Tato funkce má velký přínos zejména pro snímání scén za špatných světelných podmínek. Díky SSNR také dochází ke zmenšení velikosti snímku v DVR a to až o 70% pro MPEG a 40% pro JPEG.
- **WDR** je funkce digitální kompenzace protisvětla. Tato funkce oproti běžnému BLC dokáže plynule zpracovat nepříznivé světlé a tmavé přechody v kterékoliv části bez ztráty detailu v obraze.
- **Den/noc** je funkce kamery pro sledování scén s nízkou úrovní osvětlení. Principem této funkce je možnost mechanického odstranění IR filtru (ICR) umístěného před snímacím CCD čipem. Tento filtr před CCD čipem se používá z důvodu omezení vlivu IR složky spektra, na kterou je bohaté i bílé denní světlo. Při poklesu intenzity osvětlení je potom možné IR složku využít. Technologie ICR, právě tuto vlastnost umožňuje.
- **Double Scan CCD** je snímací prvek vyznačující se velmi vysokým rozlišením a velmi vysokou citlivostí**.** S tímto snímacím prvkem umožňuje kamera SHC-730 pracovat v barevném režimu při 0.05 luxech (resp. 0.0002 Luxu v Sens-up módu) a v černobílém režimu při 0.01 Luxu. Vynikající je také rozlišení kamery, které má v barevném režimu více jak 520 TV řádku a v černobílém režimu 570 TV řádku.

10.4.2 Instalace kamer

Kamery jsou v objektu instalovány na konzolách typu CH-609 (Plastová konzole pro kameru bez krytu pro vnitřní montáž na stěnu nebo na strop, délka 280mm) od firmy KOBI. Kamery jsou označeny C01 – C011. Celkem je tedy v objektu instalováno 11 kamer stejného typu.

Kamera C01 snímá prostor hlavního vchodu a recepci (vrátnici), C02 pak prostor před výtahem a C03 která je instalovaná zdi recepce monitoruje prostor mezi výtahem a schodištěm.C04 se nachází ve druhém patře a monitoruje chodbu před konferenčním sálem.C05 je umístěna v konferenčním sále a zabírá prostor od podia směrem ke vstupním dveřím. Ve třetím patře je kamera C06, která snímá prostor mezi kancelářemi. V patře čtvrtém kamera C07 snímá prostor mezi kancelářemi. Kamera C08 je instalována v IT místnosti a C10 v účtárně. Kamera C11 je umístěna venku na zdi a snímá prostor hlavní brány a část pro-

storu před vstupními dveřmi. Kamera C11 je opatřena vnitřním hliníkový krytem SG-50-NH a konzolí s kloubem na zeď. Kamery jsou připojeny na systém Intellex, který zprostředkovává obraz z těchto kamer.

Obr. 6.Kamera Samsung SHC 730

10.4.3 Digitální záznam obrazu

V IT místnosti a částečně i v recepci bude vybavení pro monitoring pomocí kamerového systému. Pro digitální záznam obrazu jsem použil Intellex 3.2, který nabízí technologii digitálního managementu a je kompatibilní se softwarem ABI.

Intellex DV8000/16000 v3.2 – je inteligentní digitální video systém, který sdružuje řadu funkcí. Obsahuje multiplexer, který je důležitý pro zobrazování více kamer na jednom monitoru. Dále je to digitální pohybový detektor, digitální záznam obrazu, zvuku, textu a komunikace po Lan/Wan sítích.

Intellex nabízí tyto funkce:

- **Smart Search** - je inteligentní vyhledávací algoritmus pomoci něhož obsluha jednoduše nadefinuje oblast v obraze a Intellex během několika sekund vyhledá všechny zaznamenané události s aktivitou v této oblasti. Tím šetří obsluha při vyhledávání události hodiny práce.
- **IntelleCord** - pomoci této funkce lze velmi přehledne a rychle nastavit kritéria pro poplachový záznam. Záznam každé kamery muže být aktivován každých 30 minut jiným detekčním polem, nebo poplachovým vstupem. Samozřejmostí je Pre a Post poplachový záznam.
- **Dynamická komprese** – principem této komprese je záznam jednoho celého referenčního snímku - JPEG, u následujících rozdílových 32 snímku se zaznamenávají pouze změny v obraze - DELTA. V běžné praxi je tato komprese při srovnatelné kvalitě záznamu minimálně 3x úspornější na záznamové medium, než nejčastěji používané komprese JPEG nebo Wavelet, které pracují pouze s referenčními snímky.
- **Vzdálený přístup** - je možné uskutečnit pomocí softwaru Network Client a Intellex Browser Client 1.1.6. Tento software umožňuje sledování živého videa přes standardní internetový prohlížeč Internet Explorer.

Intellex digitálně zaznamenává obraz z kamer na interní harddisk čímž odstraňuje nedostatky záznamu u analogového videorekordéru. Kvalita záznamu, jeho rozlišení, stabilita obrazu při zastavení atd. Intellex dokáže bez přerušení záznamu přehrávat záznam, exportovat záznam na CD, vyhledávat záznam pomocí unikátního algoritmu Smart Search a komunikovat se vzdálenými PC se softwarem Network Client až s deseti uživateli současně. Kvalitu záznamu lze nastavit pomocí tří úrovní komprese a dovoluje ji nastavit pro každou kameru zvlášť. Intellex umožňuje nahrát požadovanou část záznamu z libovolné kamery, nebo umí po aktivaci poplachového vstupu automaticky vyexportovat aktuální záznam. Zaznamenaný obraz je opatřen vodotiskem, který chrání záznam před případnými nežádoucími úpravami. K zobrazování jsou použity 19´´ LCD monitory HMLCD od firmy Honeywell, určené speciálně pro CCTV. Disponují zobrazovací schopností 500 TV řádků v rozlišení 1280 x 1024 XGA.

10.4.4 Systém přístupu (ACCES)

Do objektu je instalován docházkový terminál DT2000 SA. Externí čtečka karet Indala ASR-610 na zdi před hlavním vchodem, je napojena na DT2000SA. Dává impuls, který na výstupu bude otevírat zámek u dveří a umožní tak vstup do budovy. DT2000SA je umístěn uvnitř objektu u recepce. Slouží pro identifikaci osob a zaznamenání docházky při příchodu a odchodu. Osoby, které mají oprávnění vstoupit do objektu jsou vybaveny bezkontaktními kartami značky Indala typu FlexCard, které obsahují informace důležité k identifikaci a evidenci docházky a umožnění přístupu do objektu. Pokud osoba není držitelem identifikační karty, tak má možnost zazvonit. Pověřená osoba, která je na vrátnici se s osobou domlouvá prostřednictvím videotelefonu Memory 128 (od firmy CityMax). Poté mu udělí nebo naopak zamítne přístup do objektu.

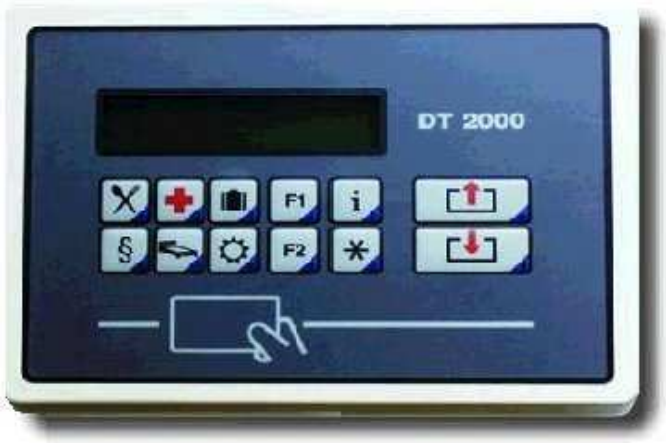
10.4.5 Docházkový terminál DT200SA

DT2000 SA – jedná se o terminál pro sledování docházky určený pro provoz v systému s ovládacím programem SKYLA Pro. Identifikace osoby se provádí prostřednictvím vestavěné bezkontaktní čtečky. Terminál je vybaven membránovou klávesnicí pro zadávání tzv. důvodů přerušení – odchod na dovolenou, k lékaři, na oběd atd. – a dvouřádkovým displejem pro zobrazování uživatelských informací. Kromě funkcí docházkového terminálu funguje jako kontrolér vstupu pro jedny dveře. DT2000 SA může komunikovat s řídícím počítačem přímo přes vestavěné rozhraní RS- 232. Má paměť pro max. 1000 karet a 10000 událostí. Kromě příchodu nebo odchodu umí DT2000 SA zpracovat až 8 dalších důvodů přerušení – odchody na služební cesty, na dovolenou apod. Rychlý výběr správné volby uživateli usnadňují piktogramy na jednotlivých tlačítcích klávesnice. Textové popisy těchto přerušení jsou uživatelsky konfigurovatelné prostřednictvím programu SKYLA Pro.Výstupem terminálu je přepínací kontakt relé pro ovládání dveřního zámku. Terminál je proti neoprávněnému otevření chráněn vestavěným tamper kontaktem na desce plošných spojů.

Stejným systémem přístupu je vybavena i IT místnost kde je důležité aby do ní měli přístup pouze pověřené osoby a v případě situace bylo možné zjistit kdo naposledy v místnosti byl.

10.4.6 Softwarové vybavení pro DT 2000SA

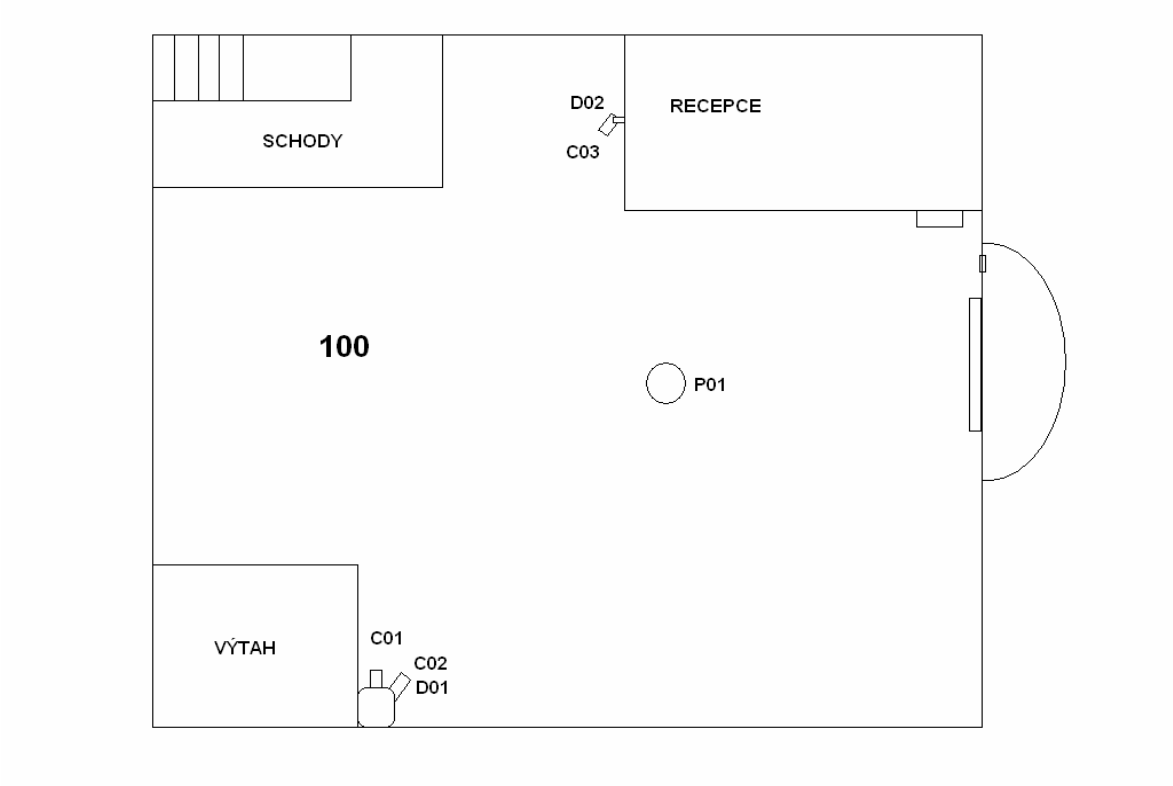
Základní úlohou programu je nastavení přístupového systému. Jednoduchým a přehledným způsobem tak nadefinujeme časové zóny, parametry všech docházkových terminálů DT2000 SA, přístupové úrovně pro hromadné přidělování oprávnění kdo, kdy a kam může vstoupit, personální údaje osob včetně fotografií a uživatelsky nastavitelných poznámkových polí nebo oprávnění pro všechny operátory, kteří s programem mají pracovat. Monitorování systému provádí SKYLA Pro II dvěma způsoby: za prvé řádkovým způsobem vypisuje všechny události, které zaznamenávají terminály DT2000 SA. Každá událost je doplněna o datum a čas vzniku a všechny ostatní potřebné informace (např. jméno a příjmení osoby). Tento přehled lze filtrovat, třídit a prohledávat podle různých kritérií nebo nechat program barevně odlišovat jednotlivé typy událostí ve výpisu. Druhým způsobem sledování systému je záznam veškerých akcí operátorů – editace nebo mazání údajů v tabulkách, přihlášení, odhlášení apod.



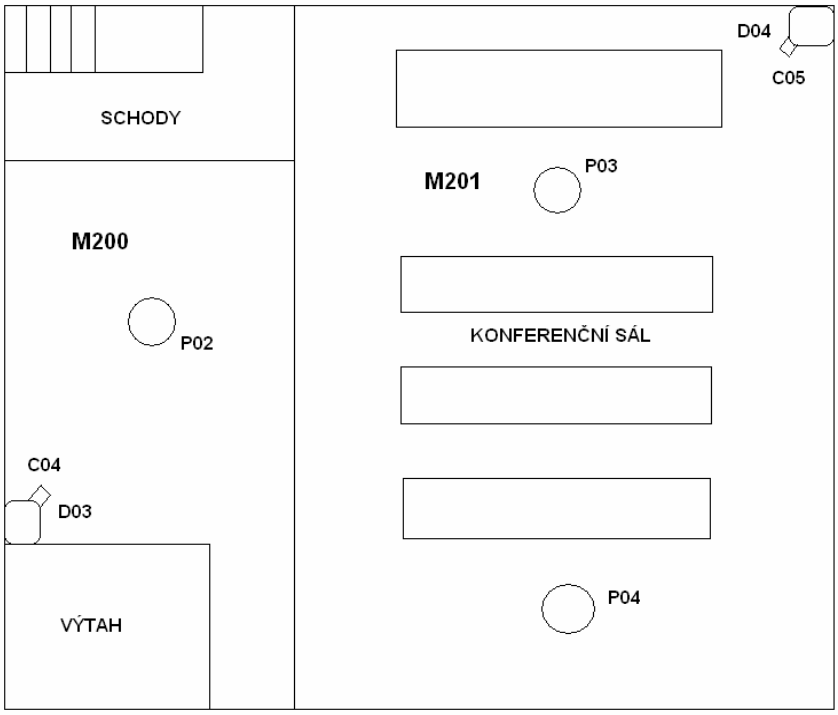
Obr. 7.DT 2000SA

11 PŮDORYSY PODLAŽÍ

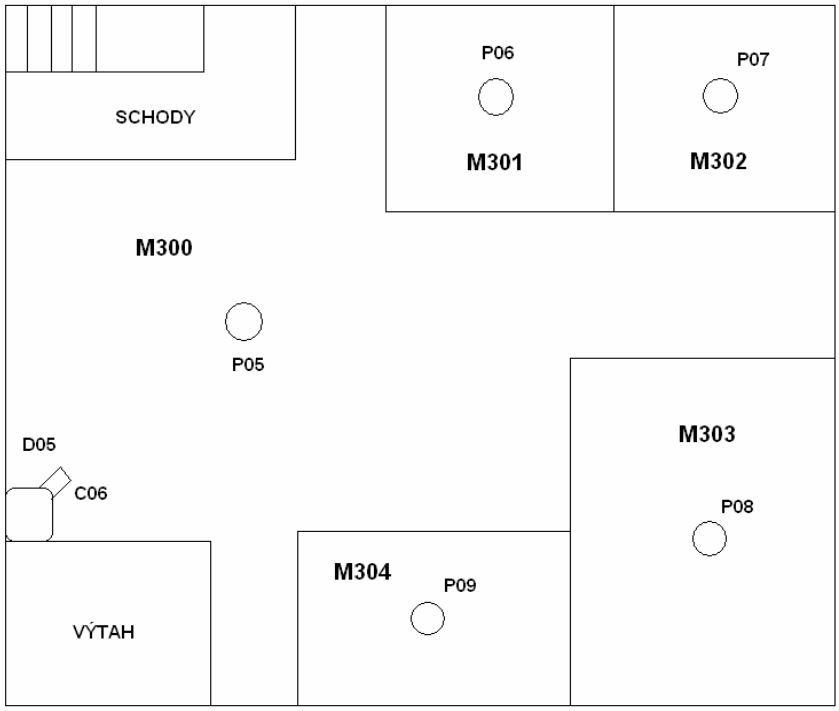
Pomocí těchto jednoduchých nákresů chci přiblížit jak asi firma vypadá a kde se nacházejí jednotlivé detektory, hlásiče a kamery instalované v objektu.



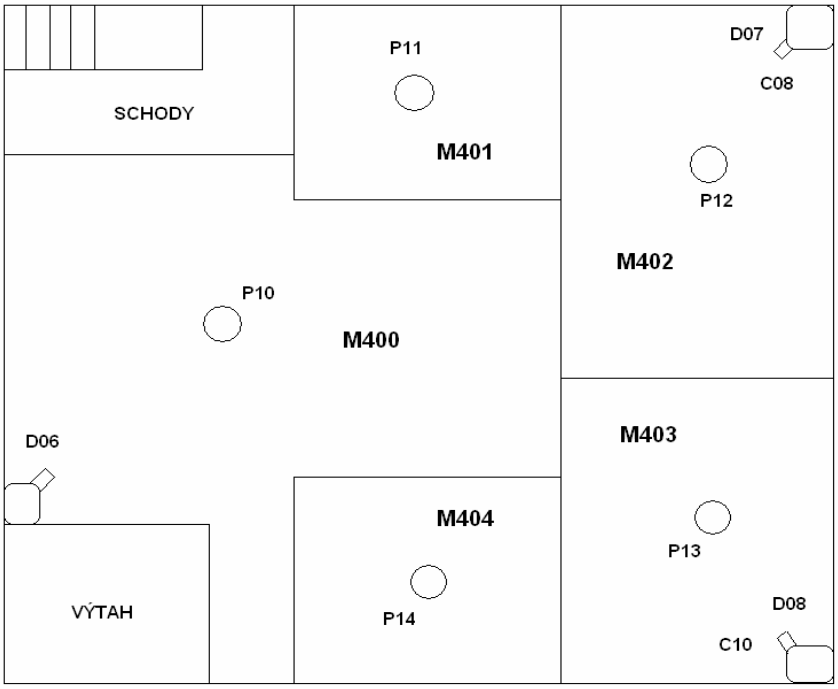
Obr. 8. První patro firmy



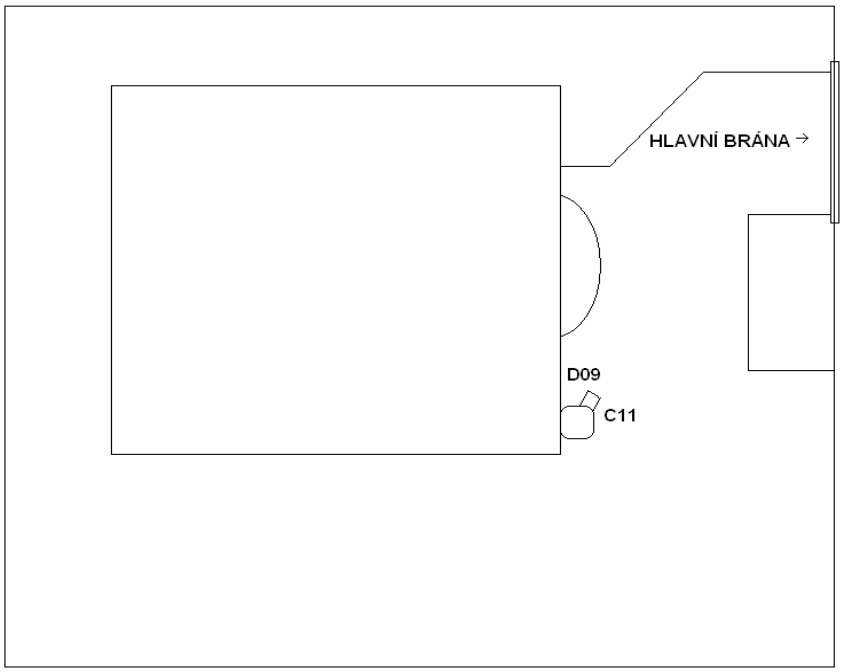
Obr. 9. Druhé patro firmy



Obr. 10. Třetí patro firmy



Obr. 11. Čtvrté patro firmy



Obr. 12. Celá firma, pohled z vrchu

ZÁVĚR

Ve své práci jsem se snažil navrhnout integrovaný zabezpečovací systém. Má za úkol zlepšit a zefektivnit zabezpečení, díky integraci nebo-li sjednocení jednotlivých zabezpečovacích systémů a prvků do jednoho celku.

V současné době je kladen velký důraz na integraci bezpečnostních systémů za účelem dosažení vysokého stupně zabezpečení, zachování jednoduchosti obsluhy a přehledné monitorování stavů bezpečnostního systému.

Na našem trhuje je k dispozici mnoho druhů zabezpečovacích systémů a prostředků. Je důležité umět si vybrat vhodný výrobek, který pokryje všechny naše potřeby, a proto je nutné obrátit se na odbornou firmu. Zákazníci často ani netuší, jaký sortiment zabezpečovacích zařízení je k dispozici. Při výběru bychom se ne vždy měli řídit pouze cenou ale zejména kvalitou a nabízenými funkcemi. Pokud do zabezpečovacího řetězce přidáváme další komponenty, jako detektory a ovladače, musíme se informovat jestli jsou kompatibilní s naším systémem.

Pro integraci zabezpečovacích prvků a systému jsem vybral software ABI (Advanced Building inteligence), který je velmi vhodný díky své kompatibilitě a příjemnému uživatelskému prostředí. Umožňuje sledovat, spravovat a řešit krizové situace z jednoho místa. Bezpečnostní agentura nebo sám majitel tak mají k dispozici ucelený přehled o tom co se v objektu děje. Nabízí také možnost nahlédnout do objektu prostřednictvím webového prohlížeče. Výhodou toho je, že pokud dojde k poplachu, tak je možnost se do objektu podívat prostřednictvím instalovaných kamer a díky softwaru ABI zjistit, kde a jakým zařízením byl poplach vyvolán. To může předcházet například falešným poplachům, které se mohou vyskytnout, nebo pomoci zásahové jednotce při lokalizaci pachatele.

V této práci nebyl brán zřetel na žádné finanční stránky. Použitá zařízení byly vybrány bez ohledu na jejich cenu. Práce pro mě byla opravdu přínosem kvalitních informací a prohloubil jsem si tak znalosti bezpečnostních technologií.

SEZNAM POUŽITÝCH PRVKŮ

- Ústředna EZS GALAXY 60
- Duální detektory DX60 PLUS I
- Detektory tříštění skla GLASSTREK 456
- Magnetické kontakty MC2110 AH
- Opticko kouřové detektory SS 2351 KNL/KRL
- Stabilní hasící zařízení na plyny HFC – 227ea
- Tísňové hlásiče požáru BF 380MR
- Kamery SAMSUNG SHC 730
- Docházkové terminály DT2000 SA
- Čtečka karet INDALA ASR – 610
- Videotelefon MEMORY 128

SEZNAM POUŽITÉ LITERATURY

[1] KINDL, Jiří: Projektování bezpečnostních systémů I. 1. vyd. UTB Zlín 2004. ISBN 80-7318-165-7

[2] ADI International [online]. 2006 [cit. 2006-05-24]. Dostupný z WWW: <http://www.olympo.cz>.

[3] Sieza spol. s.r.o. [online]. 2006 [cit. 2006-05-30]. Dostupný z WWW: <http://www.sieza.cz>.

[4] Alimex spol. s.r.o. [online]. 2006 [cit. 2006-05-30]. Dostupný z WWW: <http://www.alimex.cz>.

[6] Poznámky z výuky. UTB Zlín 2004-2006

[7] Technické materiály z výstavy Pragoalarm. Praha 2004

[8] Technické materiály fy HONEYWELL. Brno: Honeywell spol. s r.o., 2006

[9] ČSN CLC ITS 50 398 Kombinované a integrované systémy – všeobecné požadavky (8/2005)

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

EZS Elektrická zabezpečovací signalizace

EPS Elektrická požární signalizace

CCTV Closed Circuit Television (Uzavřený televizní okruh)

ACS Acces System (přístupový systém)

Dxx Označení detektoru

Cxx Označení kamery

Pxx Označení hlásiče požáru

Mxx Označení místnosti

ČSN Česká státní norma

PC Počítač

SEZNAM OBRÁZKŮ

SEZNAM TABULEK