Současné trendy využití integrovaných elektronických bezpečnostních systémů v PKB

Martin Pokorný

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:	**Martin POKORNÝ**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Současné trendy využití integrovaných elektronických systémů v průmyslu komerční bezpečnosti**

Zásady pro vypracování:

1. Ze současné nabídky poplachových systémů vyberte a zhodnoťte ty systémy, které by měli do této kategorie patřit.
2. Z pohledu komplexní systémové ochrany objektů posuďte jestli integrace je záležitost pouze poplachových systémů nebo by se měla zahrnout i další životně důležité technologie (vytápění, klimatizace atd.).
3. Práci konkretizujte návrhem integrovaného systému pro zvolený objekt.

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

Security Magazín
Firemní materiály fy HoneyWell
Norma ČSN CLC/TS 50398

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

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

V této bakalářské práci jsem se snažil pojmout hlavní aspekty existující legislativy integrovaných elektronických bezpečnostních systémů. Dále jsem ze současné nabídky těchto systémů na trhu vybral některé často používané systémy a s jejich pomocí jsem docílil jednoho možného způsobu aplikace. Posuzoval jsem také kritéria, která předcházejí rozhodnutí, zda zvolit integraci bezpečnostních systémů.

Klíčová slova: integrovaný, elektronický, systém, centralizace, struktura, propojení, legislativa, spolupráce

ABSTRACT

The aim of this bachelor's thesis is to contain the main aspects of existing legislative for integrated electronic security systems. Furthermore, I chose some of the more deployed systems on the market and with by using them, I designed one of the possible solutions. I have also weighted the criteria which precede the resolution whether to choose to deploy an integrated security system.

Keywords: integrated, electronic, system, centralization, structure, connection, legislature, cooperation

Tímto děkuji svému vedoucímu bakalářské práce Ing. Jiřímu Kindlovi za odborné vedení při zpracování této práce.

Dále bych chtěl poděkovat Ing. Richardu Sobotkovi z firmy Honeywell za poskytnuté materiály a odbornou konzultaci tématu.

Prohlašuji, že jsem na celé bakalářské práci pracoval samostatně a použitou literaturu jsem citoval.

Ve Zlíně, 2. června 2006 .

……

Martin Pokorný

OBSAH

ÚVOD

Potřeba kvalitnějšího zabezpečení v současné době vede k rozvoji oblasti průmyslu komerční bezpečnosti, za současného neustálého zvyšování nároků na tento obor. Otázku zabezpečení již nelze řešit zavedením jednoduchého systému. Chceme-li mít kvalitní zabezpečení, musíme vzít v potaz a vhodně zkombinovat tyto následující kategorie:

- elektronické zabezpečovací systémy,
- mechanické zabezpečovací systémy,
- režimová opatření.

Integrace bezpečnostních systémů pomáhá k efektivnější ochraně osob a majetku ve střežených budovách. Je to však široký pojem zahrnující několik možných variant řešení. První úroveň integrace systémů je na hardwarové úrovni, kdy většinou jeden druh systému (např. elektronická zabezpečovací signalizace) umožňuje připojit vstupní prvky jiného systému (např. jednotku kontroly přístupu). Na druhém stupni integrace systémů integrujeme pomocí nadstavbového softwaru několik autonomních subsystémů (elektronická požární signalizace, elektronická zabezpečovací signalizace, zabezpečovací a přístupové systémy a uzavřený okruh televizních kamer).

Můžeme rozlišit tři způsoby uplatnění integrovaného systému, které se vyvíjely na základě požadavků v daném období jejich vzniku. První způsob vychází z požadavku na centralizaci událostí ve střežených objektech, kdy má operátor možnost sledovat zprávy o stavu jednotlivých subsystémů umístěných na různých místech. Dalším způsobem je vizualizace stavu jednotlivých zařízení. Třetí způsob je založen na propojení subsystémů tak, aby mezi sebou mohly spolupracovat a aby operátor měl možnost tyto systémy ovládat a nastavovat. Tyto tři uvedené termíny se do jisté míry překrývají a dnešní integrované systémy využívají obvykle všechny nebo nějakou jejich kombinaci.

Na současném trhu je k dispozici množství různých systémů umožňujících integraci, ale je na posouzení zadavatele, které z těchto systémů zvolí, vzhledem k tomu, že neexistují jednoznačně nejlepší řešení obecného problému ochrany osob a majetku.

1 NORMA ČSN CLC/TS 50398

Do nedávné doby chyběla legislativa pro kombinované a integrované poplachové systémy. Existovala pouze technická specifikace, která byla podkladem pro normu vydanou v roce 2005 pod názvem ČSN CLC/TS 50398. Tato norma stanovuje všeobecné požadavky na kombinované a integrované poplachové systémy. Dále uvádí jednotlivé typy struktur těchto systémů a poskytuje informace pro prvotní návrh systému.

1.1 Definice pojmů pro účely této normy

Speciální vybavení - vybavení, které není popsáno v aplikační normě a které není nutné ke splnění funkcí požadovaných touto aplikační normou. Speciální vybavení může být společné pro dvě nebo více aplikací. V tomto případě může být toto vybavení speciálním vybavením v jedné aplikaci, ale v jiné aplikaci požadovaným jako normalizované. V aplikaci, pro kterou neexistuje žádná norma, každé vybavení této aplikace je považováno jako speciální vybavení.

poplach - výstraha o přítomnosti nebezpečí pro život, majetek nebo okolní prostředí,

poplachová aplikace - aplikace určená na ochranu života, majetku, prostředí jako jsou:

- zabezpečovací a tísňová signalizace,
- přivolání pomoci,
- uzavřené televizní okruhy použité pro zabezpečení a dohled,
- kontrola přístupu,
- elektrická požární signalizace,

poplachové přijímací centrum (ARC) / pult centralizované ochrany (zkratka PPC/PCO) - trvale obsluhované vzdálené středisko, do kterého se předávají informace týkající se stavů jednoho nebo více zařízení

montážní firma EZS - subjekt poskytující služby související s EZS,

poplachový stav - stav EZS nebo jeho komponentů, který je výsledkem odezvy systému na přítomnost nebezpečí,

poplachový systém - elektrická instalace, která reaguje na manuální podnět nebo automatickou detekci přítomnosti nebezpečí,

poplachové přenosové zařízení - zařízení, které je použito hlavně k přenosu poplachu z rozhraní poplachového systému v hlídaných prostorách do rozhraní signálního panelu PPC/PCO. Může přenášet informace nebo povely z PPC/PCO do jednoho nebo více poplachových systémů,

poplachový přenosový systém (ATS) - zařízení a síť používané pro přenos informací mezi jedním nebo více poplachovými systémy a jedním nebo více přijímacími centry (PPC/PCO),

aplikace (použití) - všechny uváděné funkce použité pro specifické účely, jako jsou detekce a výstraha v případě požáru, ovládání osvětlení atd.,

aplikační norma - norma, týkající se specifických aplikací,

ústřední řídící zařízení (CCF) - zařízení používané k řízení a nebo signalizaci ve struktuře (konfiguraci) typu 1, která je připojena k jednomu nebo více jednoúčelových systémů a která je normálně řízena provozní obsluhou, například počítač v dozorovém pracovišti; ústřední řídící zařízení je speciální vybavení (a není to běžná poplachová ústředna) pro alespoň jednu z aplikací,

kombinovaný a integrovaný poplachový systém - výraz v této normě „kombinovaný a integrovaný poplachový systém“ jsou synonyma a v této normě budou většinou používána jako integrovaný poplachový systém,

společné zařízení - zařízení sdílené jednou nebo více aplikací,

společné vybavení - vybavení sdílené jednou nebo více aplikací. Společné vybavení může být speciálním pro dvě nebo více aplikací a může být normalizovaným pro dvě nebo více aplikací nebo může být speciální pro jednu nebo více aplikací a normalizovaným pro ostatní aplikace,

společná přenosová trasa - přenosová trasa použitá pro několik aplikací,

jednoúčelové zařízení - zařízení používané výhradně jednou aplikací,

jednoúčelový systém - systém použitý pouze pro jednu typickou aplikaci a splňující všechny požadavky aplikovatelné tomuto použití,

jednoúčelová přenosová trasa - přenosová trasa použitá výhradně pro jednu aplikaci,

vybavení (zařízení) - hardware nebo software, který umožňuje systému plnit jednu nebo více funkcí, například přenosovou trasu, vyhodnocovací prvky, displeje,

poruchový stav - stav systému, který brání systému nebo jeho části v normální funkci,

poruchový signál - zpráva generovaná vlivem poruchy,

integrovaný poplachový systém - systém se společným vybavením použitým k různým aplikacím a alespoň s jednou poplachovou aplikací. Poplachový přenosový systém se nepovažuje za součást poplachového integrovaného systému. Jednoúčelové systémy připojené pouze přes jednosměrný výstup zařízení bez jakýchkoli komunikačních dat, např. relé, nejsou považovány za vlastní součást integrovaného systému,

integrita (kompletnost) - způsobilost aplikace fungovat dle projektu a míře odolnosti vůči vlivům, které by mohly ovlivnit správnou funkci,

provozní kniha - kniha (sešit) pro záznamy nebo jeho elektronický ekvivalent, do kterého jsou ukládány relativně bezpečným způsobem příslušné podrobnosti o systému, jeho funkčnosti a údržby pro následnou inspekci pověřenou organizací,

nepoplachové aplikace - určité aplikace k ovládání (řízení), které nejsou uvažovány především k ochraně života, majetku a prostředí, například: topení a větrání (ventilace), správa energetiky, správa budovy, osvětlení,

vyhodnocovací element - vybavení, které vykonává dle programových instrukcí matematické nebo logické datové operace k dosažení požadovaných funkcí,

normalizované vybavení - vybavení, které je popsáno v aplikační normě a které zcela splňuje tuto aplikační normu. Normalizované vybavení může být společné pro dvě nebo více aplikací. V tomto případě může být toto vybavení normalizovaným pro jednu aplikaci, ale speciálním vybavením pro další aplikace,

sabotážní stav - stav poplachového systému, ve kterém byla detekována sabotáž,

detekce sabotáže - detekce úmyslného zasahování do poplachového systému nebo do jeho části,

přenosová trasa - komunikační cesta používaná k přenosu informace v integrovaném poplachovém systému.

1.2 Všeobecný popis a základní principy

Jsou specifikovány tři typy struktur (konfigurace):

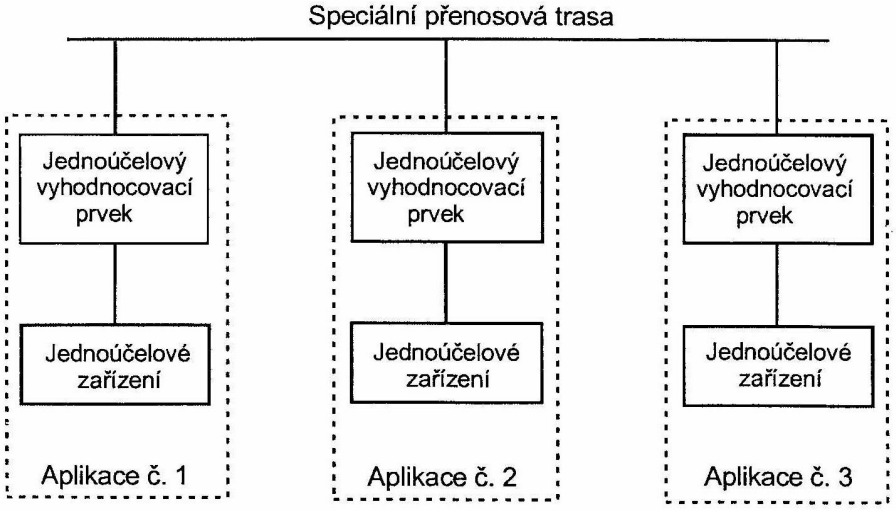
Typ 1: Struktura je vhodná pro kombinaci a integraci jednoúčelových normalizovaných poplachových systémů a jednoúčelových nepoplachových systémů.

Typ 2A: Struktura je vhodná pro kombinaci a integraci normalizovaných poplachových systémů a nepoplachových systémů používajících společných přenosových tras, společných zařízení a společných vybavení. Jediná porucha v jedné aplikaci nemá žádný nepříznivý vliv na další poplachovou aplikaci. K dosažení tohoto stavu je potřebné zdvojení (redundance).

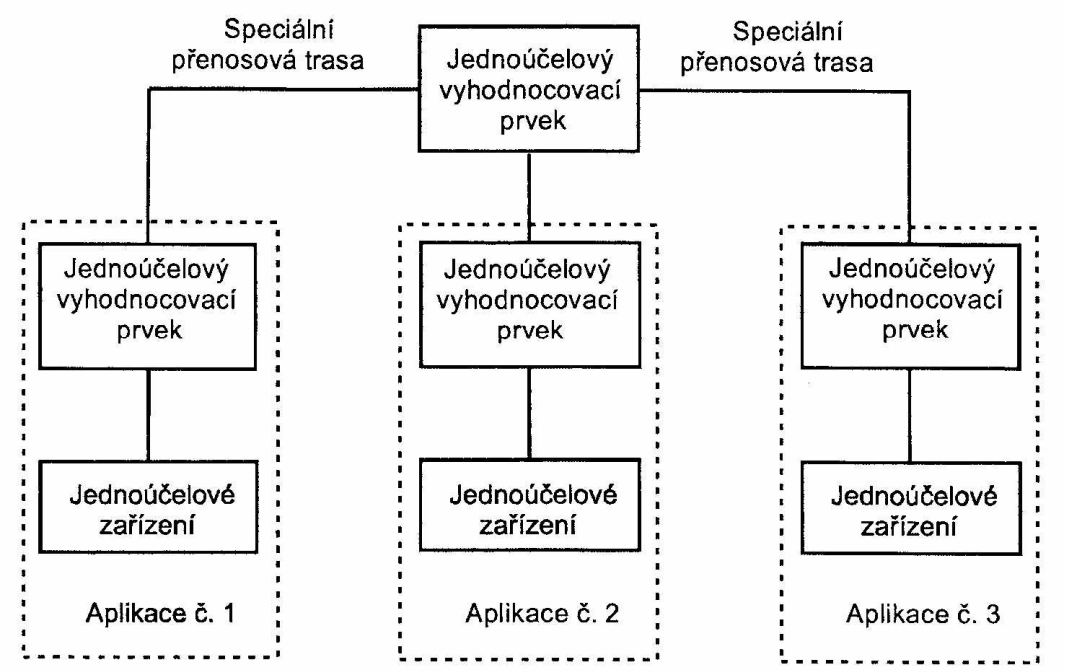
Typ 2B: Struktura je vhodná pro kombinaci a integraci normalizovaných poplachových systémů a nepoplachových systémů používajících společných přenosových tras, společných zařízení a společných vybavení. Jediná porucha v jedné aplikaci může mít nepříznivý vliv na další poplachovou aplikaci.

1.3 Typy integrovaných poplachových systémů

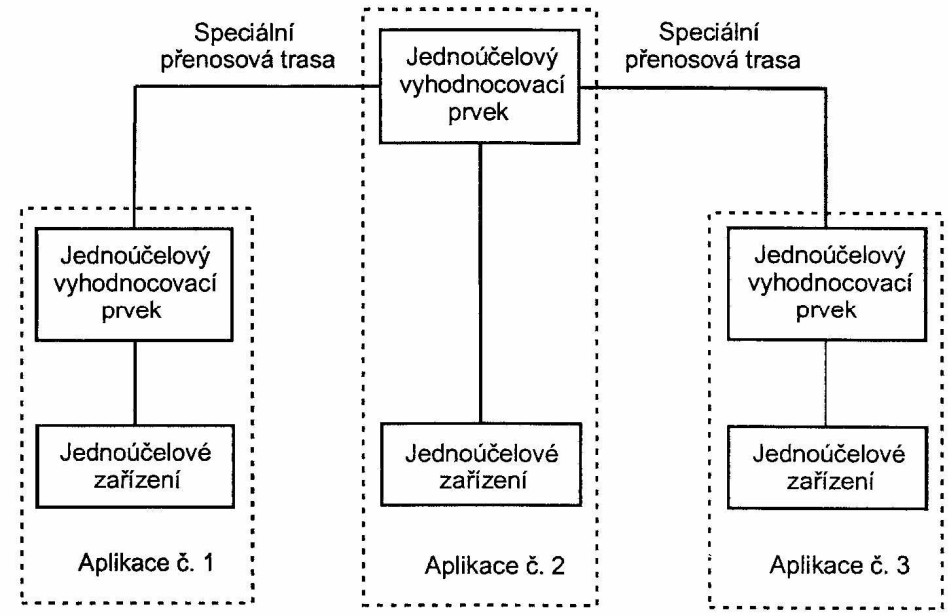
Struktura typu 1 je kombinace dvou nebo více jednoúčelových systémů. Tyto systémy jsou připojeny ke společným dalším zařízením, například propojených přes speciální přenosovou trasu. U normalizovaných vybavení typu 1 v poplachové aplikaci nesmí být tato vybavení v žádném stavu nepříznivě ovlivněna žádným dalším jednoúčelovým systémem nebo žádným zvláštním vybavením.



Obr. 1. První případ struktury typu 1

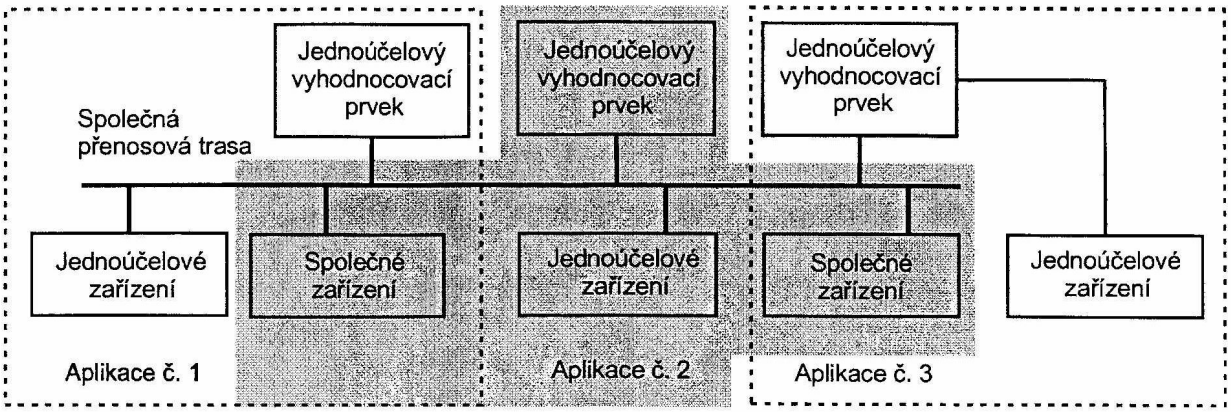


Obr. 2. Druhý případ struktury typu 1, ústřední řídící zařízení třídy 1

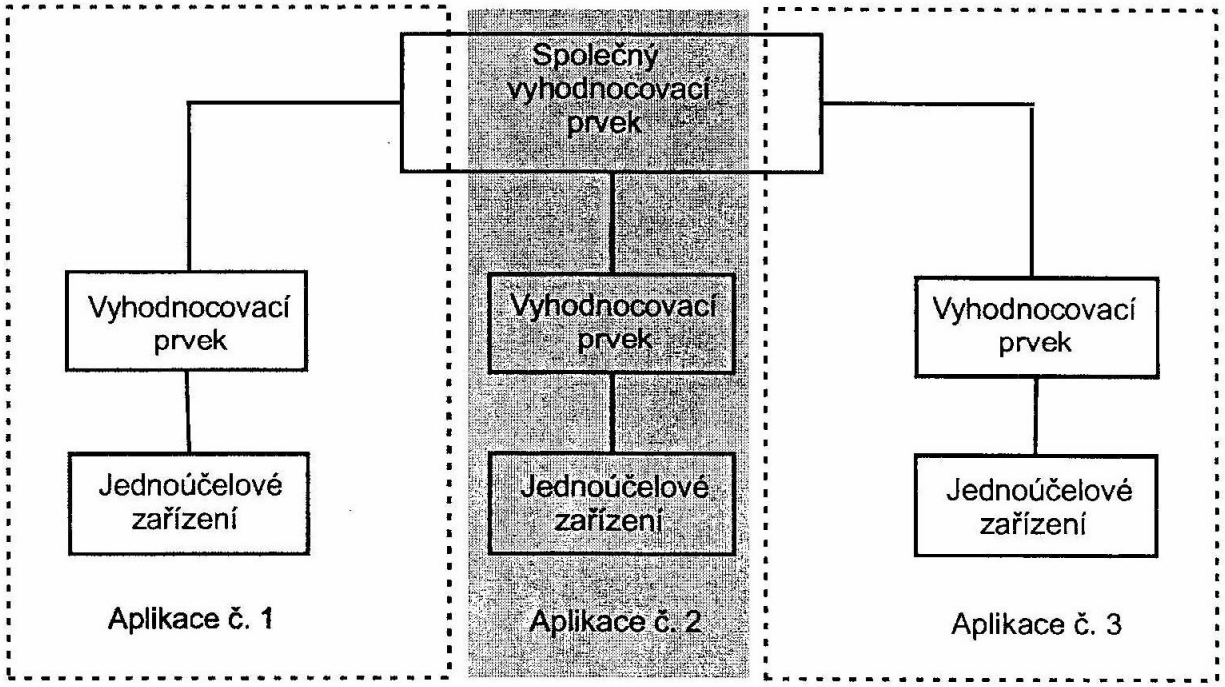


Obr. 3. Třetí případ struktury typu 1, ústřední řídící zařízení třídy 2

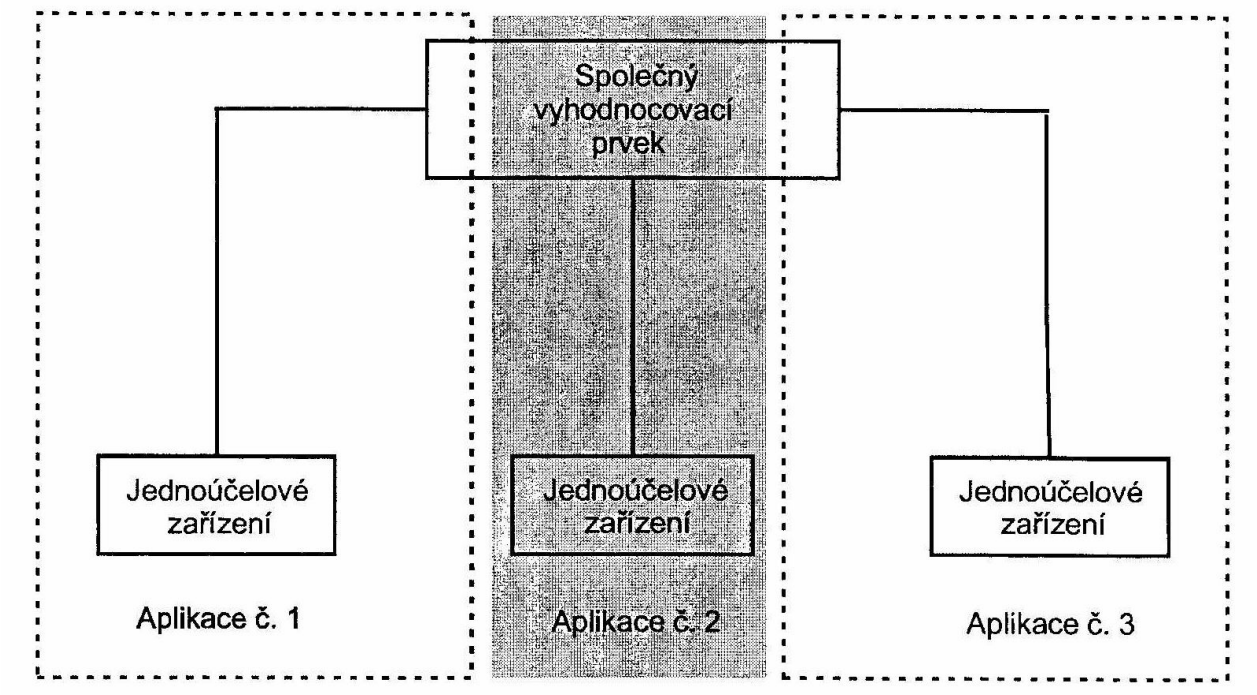
Struktura typu 2 je kombinace dvou nebo více jednoúčelových systémů, které všechny využívají normalizované společné vybavení alespoň pro jednu aplikaci. Struktury typu 2 jsou dále rozděleny na Typ 2A a Typ 2B.



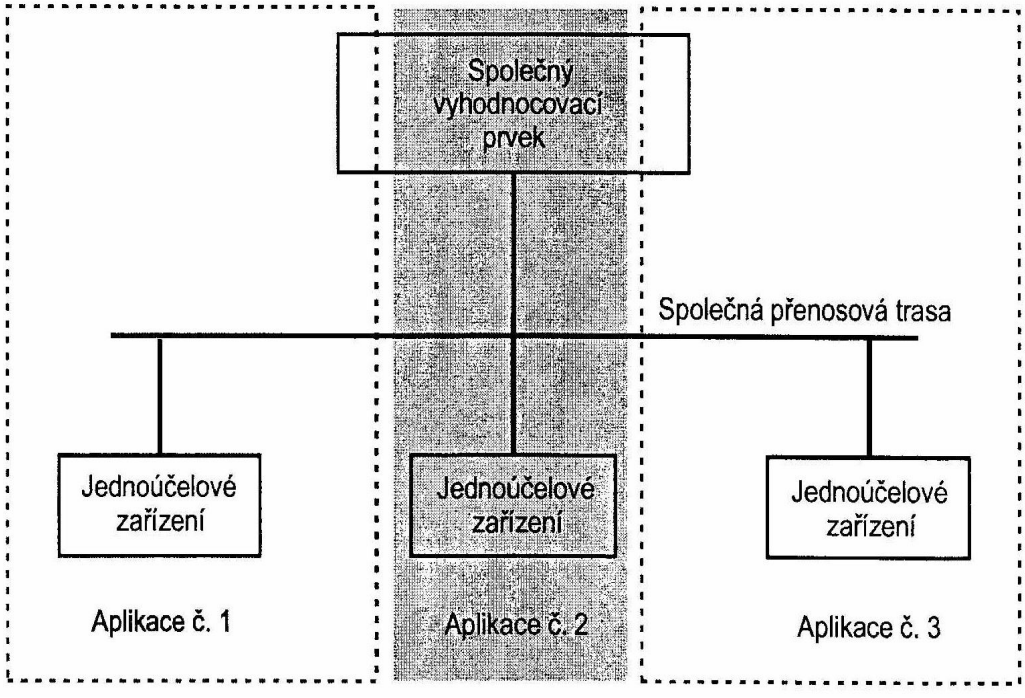
Obr. 4. První případ struktury typu 2



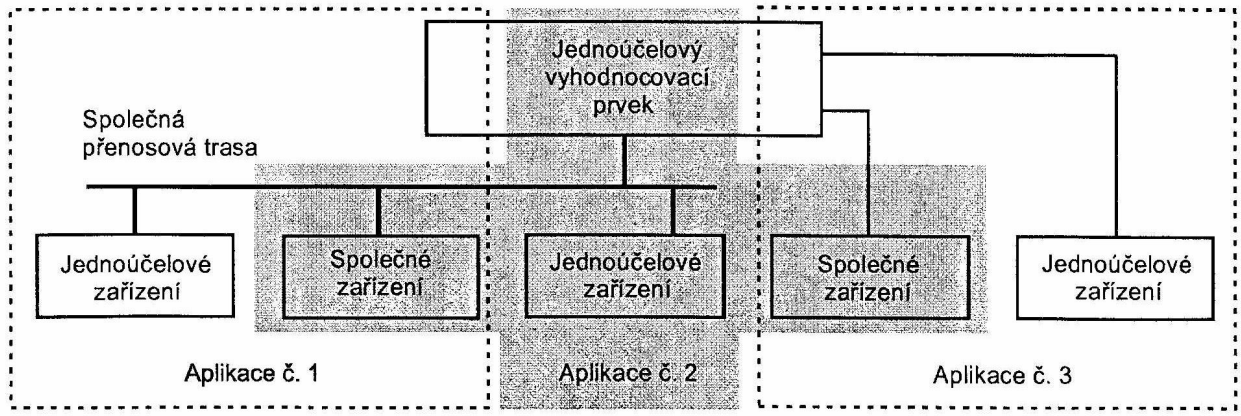
Obr. 5. Druhý případ struktury typu 2



Obr. 6. Třetí případ struktury typu 2



Obr. 7. Čtvrtý případ struktury typu 2



Obr. 8. Pátý případ struktury typu 2

U struktury typu 2A kompletnost každého normalizovaného poplachového vybavení v každé jednotlivé aplikaci nesmí být nepříznivě ovlivněna jedinou poruchou v jiné aplikaci.

U struktury typu 2B kompletnost každého normalizovaného poplachového vybavení v každé jednotlivé aplikaci může být nepříznivě ovlivněna jedinou poruchou v jiné aplikaci. Na uvedených příkladech čárkované čáry a šedá pole ukazují ty části každé aplikace, které splňují své aplikační normy, pokud existují.

1.4 Systémové požadavky a stanovení slučitelnosti

Integrovaný poplachový systém musí být navržen (projektován) tak, aby žádná aplikace nebyla v normálním stavu (včetně poplachového stavu) nepříznivě ovlivňována žádnou jinou aplikací.

Uvnitř kombinovaných a integrovaných systémů mohou být povelové signály přenášeny z jedné aplikace do jiné nebo z ústředního řídícího zařízení (CCF) do dalších částí aplikace. Příkladem je dálkové vypínání senzorů z CCF nebo zablokování CO2 hasícího systému systémem kontroly vstupů, když osoba vstoupí do chráněného prostoru.

Použití povelových signálů může být užitečné k ukáznění osazenstva velkých budov (objektů) nebo míst, která se skládají z počtu budov, ale mohou však také snížit zabezpečení a bezpečnost, když je takové vybavení nesprávně použito. Příkladem může být dálkové odemykání přístupových dveří systémem elektrické požární signalizace bez patřičných hledisek důsledků na zabezpečení objektů.

1.5 Zvláštní požadavky návrhu na typy struktur

U struktury typu 1 nesmí normalizované vybavení při použití ve všech stavech nepříznivě působit v žádném provozním stavu na žádný jiný jednoúčelový systém nebo další zařízení.

U struktury typu 2 použití sdílející společné vybavení s jinými aplikacemi nesmí být v normálním provozu ovlivňováno jinými aplikacemi, které jsou také v normálním provozu.

U struktury typu 2A a 2B kompletnost každého normalizovaného poplachového vybavení v každé jednotlivé aplikaci nesmí být nepříznivě ovlivněna jedinou poruchou v jiné aplikaci.

1.6 Priority signalizování

Informace musí být signalizovány v prioritním pořádku jasným a jednoznačným způsobem. Důvody zpětného nastavení priorit musí být vždy vyhodnoceny. Všeobecně by měly být použity následující priority:

- Priorita 1 Poplachové signály týkající se např. požárního poplachu k ochraně života nebo napadení osob.
- Priorita 2 Poplachové signály týkající se ochrany majetku nebo ochrany proti nedovolenému vniknutí do objektu.
- Priorita 3 Poplachové signály ostatních poplachových systémů.
- Priorita 4 Poruchové signály ze systémů ochrany života a majetku.
- Priorita 5 Poruchové signály z ostatních poplachových systémů.
- Priorita 6 Informace z nepoplachových systémů.

Musí být signalizovány všechny existující poplachy a postupně mohou být zobrazovány kromě aktuálně zobrazovaných informací. Také musí být na vyžádání k dispozici dostatečné informace, ale viditelnost prioritních informací musí mít přednost. Opakovaný poplachový signál, který byl již zobrazen, nesmí být znovu zobrazován. Musí být signalizována existence poplachů z více než jedné aplikace.

1.7 Zpracování dat z normalizovaných vyhodnocovacích prvků

Pro ty aplikace, pro které je požadováno monitorování dle aplikační normy, provozní program společné vyhodnocovací jednotky musí být monitorován tak, že chyba monitorovací sekvence zahrnující všechny takové aplikace je detekována a signalizována.

V integrovaném systému, který používá společný vyhodnocovací prvek, výpadek (ztráta) tohoto prvku může pravděpodobně ohrozit efektivní správu (řízení) událostí. Proto se doporučuje pro takové systémy zařadit záložní vyhodnocovací prvek, zvláště (zpravidla) ve velkých nebo rozsáhlých lokalitách a tyto záložní vyhodnocovací prvky musí umožnit aplikace, které vykonají standardně požadované funkce.

1.8 Připojení k poplachovému přenosovému systému

Pokud jsou poplachové systémy připojeny k poplachovému přenosovému systému, potom tento systém musí splňovat příslušné normy pro poplachové přenosové systémy. Pokud poplachový přenosový systém slouží k přenosu poplachových signálů z jedné nebo více aplikací, musí být tento poplachový systém připojen na ty části integrovaného poplachového systému, které plně splňují příslušné aplikační normy.

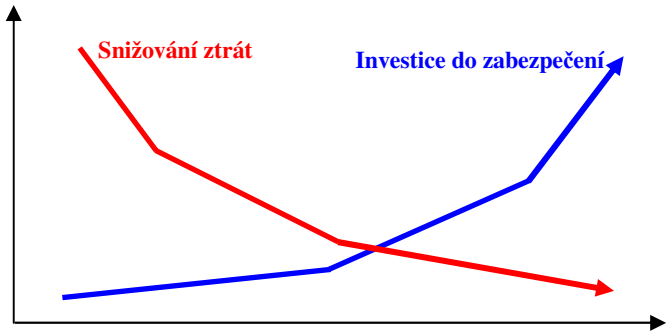
Kupříkladu poplachový přenosový systém projektovaný (navržený) k přenosu signálů ze zabezpečovacích systémů musí být připojen tak, aby splňoval požadavky evropských norem na zabezpečovací systémy.

1.9 Zásady propojení

Pokud zařízení, které nemusí splňovat jednu nebo více aplikačních norem, jsou připojena k zařízením splňující požadavky norem, musí být použity některé zásady propojení. Zařízení musí být propojena takovým způsobem, že pouze takové řízení poplachového systému bude akceptováno a provozováno, které povolují aplikační normy, neidentifikované signály nemají nepříznivý vliv, má navíc promyšlený interface, nemá žádný nepříznivý vliv na zabezpečovací aplikace, kontroly vstupů a CCTV, nebo tato zařízení musí splňovat požadavky monitorování a sabotáže dle aplikačních norem.

2 INTEGROVANÉ SYSTÉMY NA NAŠEM TRHU

K jakémukoliv zabezpečení je nejlepším začátkem vhodně zpracovaná analýza bezpečnostních rizik, která nám umožní přesnější pohled na to, jaký druh zabezpečení zvolit. Existuje několik kritérií, podle kterých je možné vhodný druh zabezpečení vybírat – cena chráněného majetku musí být alespoň zhruba odpovídající ceně vynaložené na jeho zabezpečení.



Obr. 9. Vzájemná závislost investic do zabezpečení a velikost ztrát

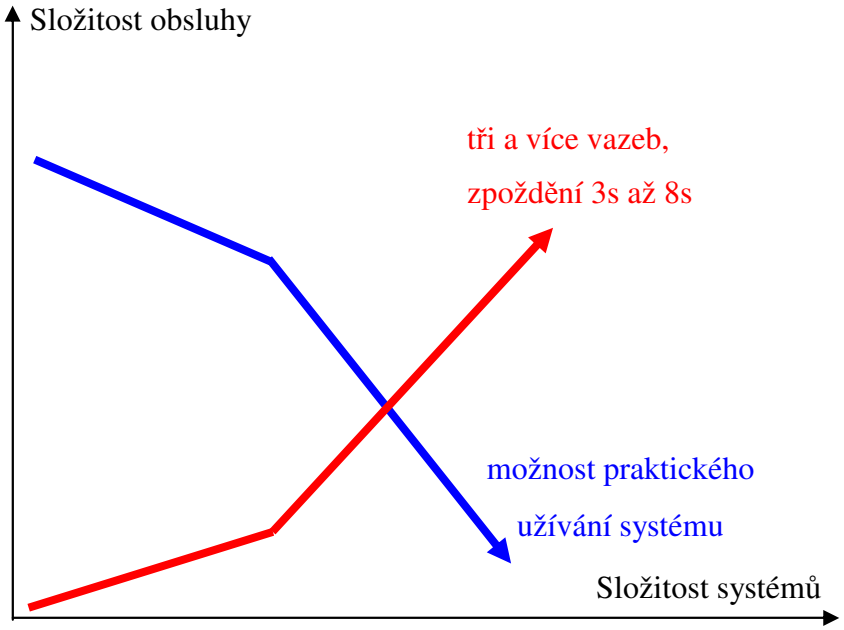
Nejdříve si musíme stanovit důvody, proč chceme zabezpečení daného objektu realizovat integrovaným systémem a co nám tento způsob přinese. Pokud se jedná o větší technologické komplexy, případně o požadavek na centralizaci informací z různých vstupů umístěných na vzdálených místech, je integrace subsystémů nevyhnutelná, neboť lidská obsluha by neměla šanci takové množství informací zpracovat a vyhodnotit. Zde již samozřejmě mluvíme o integraci veškerých technologických systémů, které se ve chráněném objektu nacházejí.

Integrace nám může přinést za prvé úspory, a to přímé (dojde ke snížení výdajů) a také nepřímé (odrazení pachatelů). Za druhé nám integrování systémů přinese nové funkce, které nám umožní efektivnější zabezpečení objektů. Funkce těchto systémů jsou vizualizace, centralizace a integrace. Využívat tyto funkce lze z operátorských pracovišť, které mohou být umístěny buď ve spravované budově nebo téměř na jakémkoli jiném místě, kde je možné se k systému připojit většinou pomocí WAN. Operátoři mohou vzdáleně provádět konfiguraci a ovládání zařízení, jejich monitoring a také správu uživatelů. Tyto činnosti ale většinou vykonávají jiná operátorská pracoviště. Monitoring a přijímání poplachových

zpráv bude mít na starosti jedno pracoviště a správu uživatelů druhé, které může být součástí personálního oddělení podniku.

Prvotní myšlenkou integrace bylo však využití spolupráce systémů tak, abychom mohli vyloučit fyzickou obsluhu. Například vhodným propojením přístupového systému a systému EZS, který nám bude detekovat veškeré nestandardní pokusy průchodu přes vstupy, ošetřenými přístupovým systémem.

Na druhé straně je také třeba vzít v úvahu, že integrace systémů může přinést některé problémy, které jsme doposud řešit nemuseli. Jednotlivé subsystémy většinou nekomunikují stejným protokolem, který je potom použitý pro přenos signálů po LAN/WAN, a proto je třeba tyto protokoly převádět. Je také rozdíl, chceme-li integrovat systémy obsažené v jedné budově a můžeme k tomu využít lokální síť, a nebo integrujeme systémy z různě rozmístěných budov, kdy musíme počítat s použitím světové sítě a tak i se změnami v rychlosti přenášených dat. A pokud bychom chtěli integrovat celky rozmístěné mezi různými časovými pásmy, musíme vzít v úvahu, zda software, který chceme použít, se umí vypořádat z odlišnými časy v těchto pásmech. Také je dobré posoudit celkovou složitost systému a složitost jeho obsluhy, aby výsledný navrhnutý systém nebyl provozně neefektivní.



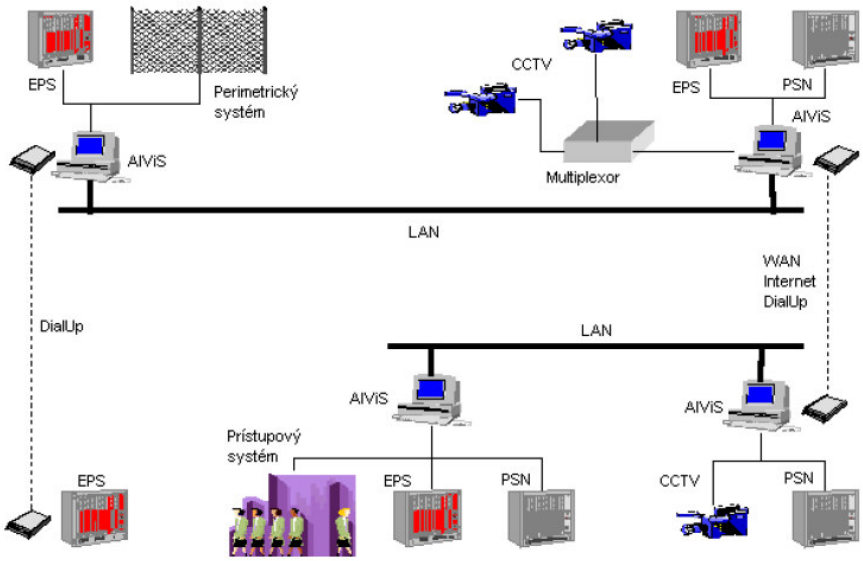
Obr. 10. Závislost složitosti obsluhy na složitosti systému

Dá se říct, že neexistuje jediný systém, který by se hodil pouze na konkrétní aplikaci nejlépe příp., že by jiný systém u této aplikace neobstál. Současná nabídka integrovaných systémů je na našem trhu poměrně rozsáhlá, i když existuje několik systémů od renomovaných firem, které zaujímají v oblibě používání přední místa. Vybral jsem několik systémů, které umožňují hardwarovou integraci nebo jsou nadstavbovými systémy integrující veškeré subsystémy, které se v budově nacházení a zařadil jsem také dva nadstavbové softwary, které zlepšují především možnosti vizualizace stavu jednotlivých zařízení integrovaných systémů.

2.1 Grafické vývojové prostředí AlViS

Programové řešení pro řízení a monitorování elektrické zabezpečovací signalizace, elektrické požární signalizace, přístupových systémů, kamerových systémů, výrobních procesů a jiných integrovaných zařízení.

AlViS je univerzální grafické vývojové prostředí určené na tvorbu aplikací řídících a monitorovacích systémů. Jeho použití je vhodné všude tam, kde vzhledem k požadavkům obsluhy, složitosti sledovaného objektu, množstvím různých zařízení a prioritních úrovní není možné bez použití počítačového systému dosáhnout přehledný a flexibilní a lehce adaptovatelný monitorovací a řídící poplachový systém.



Obr. 11. Schéma propojení systému AlViS

Systém je založený na architektuře klient/server, což umožňuje distribuované rozdělení monitorovacího a poplachového systému na více počítačů, vzájemně propojených pomocí počítačové sítě (LAN, WAN, INTERNET).

Samotný program AlViS je klientem určeným na vizualizaci stavu monitorovaného prostoru. Pro svoji činnost využívá služby programových serverů, které komunikují s připojenými zařízeními a poskytují potřebné údaje.

Na komunikaci mezi servery a klienty se využívá standardní protokol „DDE“ (v případě síťové komunikace NEJDDE). Každý klient může zobrazovat libovolnou podmnožinu údajů poskytovaných dostupnými servery.

Systém AlViS pracuje ve dvou režimech. První režim „vývoj“ je určený pro návrh monitorovacího a výstražného systému. Umožňuje vkládat plány objektů, připravené ve formě bitových map, rozmístit v plánech smyčky hlásičů a zařízení. Má zabudované prostředky umožňující přizpůsobit aplikaci na požadavky zákazníka (má vnitřní skriptovací jazyk s množinou funkcí) a prostředky ulehčující práci při tvorbě aplikace jako:

- funkce kopírování konfiguračních údajů na různých úrovních,
- funkci skupinových úprav aplikace pomocí inteligentního příkaze „Nahradit“ s využitím regulárních výrazů,
- funkci konfigurování symbolů podle předem připravených šablon,
- tvorbu aplikace v textovém a tabulkovém editoru (MS Word, MS Excel),

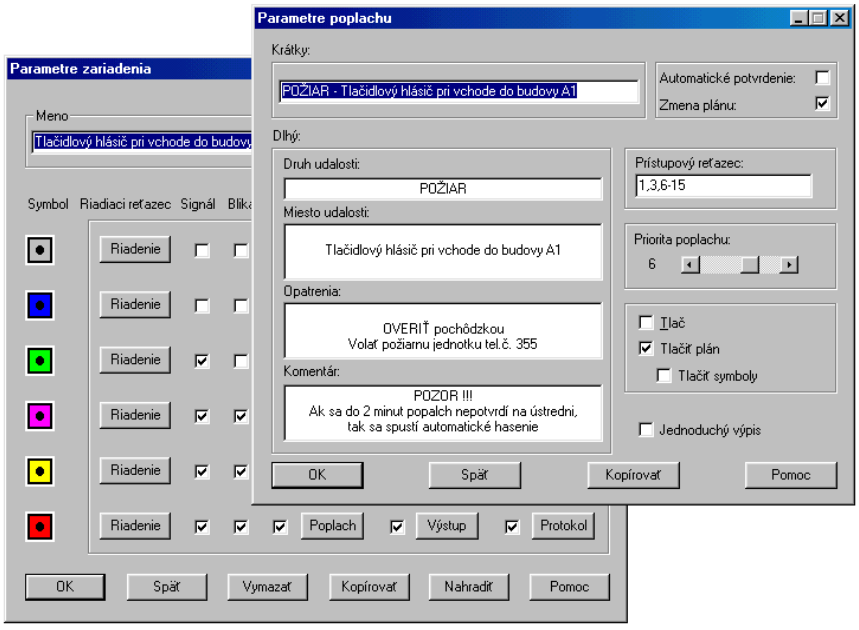
Druhý režim „monitorování“, který aktivuje vstupní a výstupní linky a zobrazuje změny stavů monitorovacích zařízení. Umožňuje sledovat všechny události na monitoru, aktivně pomocí myši přepínat plány, případně vysíláním povelů řídit připojené zařízení.

Monitorovaný prostor je v systému AlViS reprezentovaný plány. Na plánech umístěné symboly prezentují monitorované zařízení. Systém umožňuje definovat libovolné množství plánů. Plán je obrázek - bitová mapa vytvořená grafickým programem anebo scanovacím zařízením.

Všechny monitorované zařízení (kamery, detektory pohybu, otřesu, požáru) jsou v systému AlViS reprezentované symboly umístěnými na plánech. Pro každý symbol je možné definovat chybové hlášení a stavy v závislosti na skutečně naměřených hodnotách

signálů přicházejících od zařízení. Pro každé zařízení je možné definovat následující atributy:

- **chování symbolu** – zvukový signál resp. blikání symbolu v případě, že nastal daný stav zařízení,
- **poplach** – definování daného stavu jako poplachového, přičemž pro každý poplach je možné určit prioritu poplachu, oprávněnost obsluhy potvrdit poplach, automatické zobrazení plánu, na kterém nastal poplach a automatické potvrzování poplachu,
- **poplachové zprávy** – krátkou zprávu zobrazující se v přehledovém okně poplachů a dva druhy podrobných zpráv zobrazujících se ve zvláštním okně s instrukcí pro obsluhu resp.s podrobnějším popisem stavu, automatický tisk plánu a podrobných informací o poplachu
- **výstupy** - povelové řetězce, které budou automaticky vyslané na požadované zařízení v případě, že nastal daný stav resp. aktivované manuálně obsluhou (kliknutí myší na symbol zařízení). Tato vlastnost umožňuje na základě signálu zařízení řídit ostatní zařízení signálu (např. na základě změny stavu detektoru pohybu aktivovat kameru),
- **protokol** – definování zprávy, která se zapisuje do protokolu na disk počítače spolu s datem a časem, kdy stav nastal a s možností na on-line výstup tiskáren.



Obr. 12. Prostředí systému AlViS

V případě, že monitorované zařízení změní stav a nastane poplach, ALViS může automaticky zobrazit plán, na kterém je umístěný symbol daného zařízení. Symbol změní svoji barvu a tvar podle poplachu, který nastal. Zároveň může blikat a vydávat zvukový signál. V přehledovém okně poplachů se zobrazí poplachová zpráva, na obrazovce se objeví okno s instrukcemi pro obsluhu a s podrobnějším popisem zařízení. Do protokolu událostí se zapíše protokolová zpráva s datem a časem.

Poplachové stavy jsou vyhodnocovány podle priority a času vzniku. Systém AlViS vyhodnocuje poplach s nejvyšší prioritou v reálném čase. V případě, že nastane více poplachů se stejnou prioritou, systém je vyhodnocuje podle času, ve kterém nastaly. Po potvrzení poplachu obsluhou se zobrazí poplach s další nejvyšší prioritou a to pokračuje až do potvrzení všech poplachů v systému. Všechny aktuální poplachy jsou zároveň zobrazované v přehledovém okně poplachů.

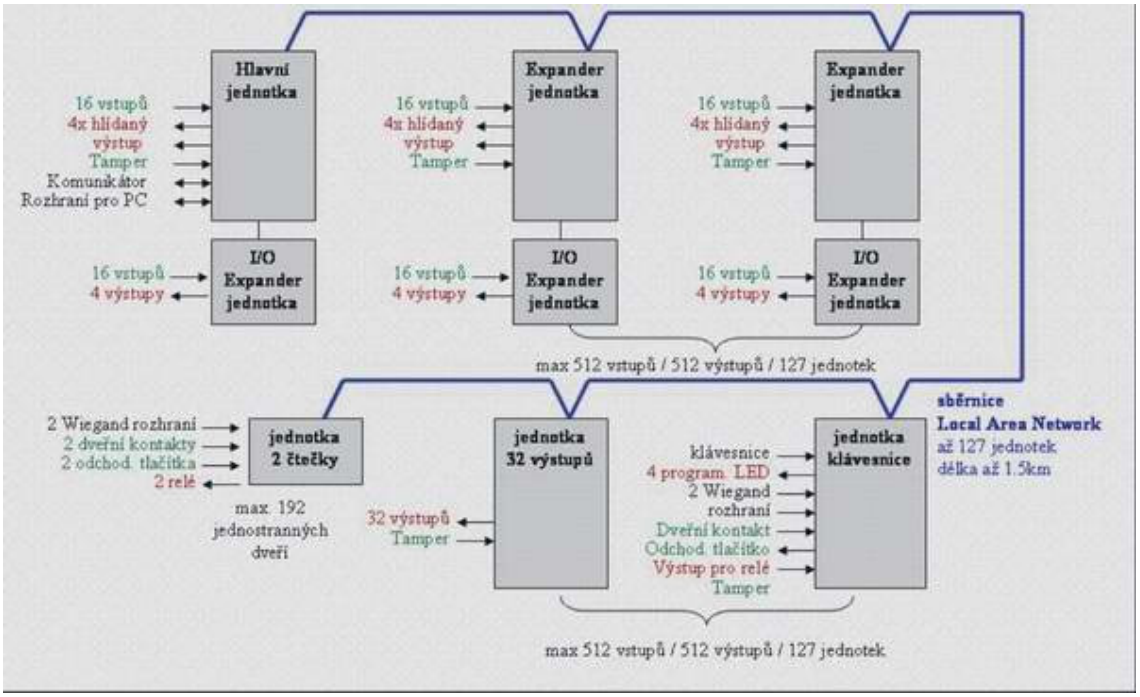
Všechny události, které nastaly v monitorovacím a poplachovém režimu jsou zaprotokolované zápisem v protokolu událostí. Protokol událostí je soubor nepřetržitě zaznamenávaný na disk počítače a na tiskárnu. Zapisuje se popis a druh události, klíčová slova, datum a čas události, datum a čas zprávy. Prohlížení, filtrování a tisk protokolů, kterých může být víc, umožňují přehledová okna protokolu.

Všechny významné zásahy do programu AlViS jsou chráněné proti neoprávněné manipulaci. Systém hesel a přístupových práv umožňuje flexibilní nastavení oprávnění na vykonávání různých funkcí nezávisle pro jednotlivé pracovníky obsluhy. Ve vývojovém režimu je možné definovat seznam operátorů, počet a druh informačních oken na obrazovce, parametry zobrazovaných oken (např. jestli obsluha může měnit jejich velikost a umístění na obrazovce). Po přepnutí do režimu monitorování je možné vykonávat jen ty operace, na které má přihlášený operátor oprávnění. Také komunikace mezi programovými moduly je v počítačové síti chráněna kryptovacím mechanizmem tak, aby nemohla být zneužita.

2.2 Systém Genesis

Systém umožňující integraci elektrické zabezpečovací signalizace, kontroly přístupu a řízení technologií. Systém má programovatelné vstupy a výstupy. Každý vstup je možné programovat ve čtyřech analogových úrovních. Je-li vstup použit jako smyčka zabezpečovacího systému, lze volně programovat hodnoty vyvažovacích a ukončovacích im-

pedancí, včetně tolerance pro vyhlášení poplachu či sabotáže. Tuto vlastnost můžeme také využít pro jednoduché snímání veličin např. teploty, tlaku, vlhkosti apod.



Obr. 13. Blokové schéma zapojení systému Genesis

Hlavní jednotka – ústředna GEN 001

Obsahuje 16 programovatelných vstupů, samostatný vstup pro tamper, 4 programovatelné tranzistorové výstupy, vestavěný zdroj 12V / 1A, rozhraní RS 232 pro programování a připojení dalších zařízení. Toto rozhraní může být použito pro přímou integraci s jinými systémy např. CCTV.

Expandér s napájecím zdrojem GEN 010

Má 16 programovatelných vstupů, samostatný vstup pro tamper, 4 programovatelné tranzistorové výstupy, vestavěný zdroj 12V/1A, vestavěný telefonní komunikátor s protokolem Contact ID, rozhraní RS 232 pro programování a připojení dalších zařízení.

Klávesnice GEN 030

Má LCD displej 2 × 16 znaků s nastavitelným kontrastem, české menu pro obsluhu a uživatelské programování, 4 programovatelné LED diody signalizující stavy a události. Klávesnice má standardně dvě rozhraní Wiegand pro připojení čteček a výstup pro relé. Z klávesnice lze řídit kontrolu přístupu pro jedny dveře s rozlišením příchodu a odchodu. Dveře lze ovládat kartou, PIN kódem nebo jejich kombinací.

Expandér GEN 025

Má 8 programovatelných vstupů pro připojení zařízení, samostatný vstup pro tamper, 2 programovatelné tranzistorové výstupy, rozhraní RS 232 pro programování a připojení dalších zařízení.

Jednotka kontroly přístupu GEN 045

Využívá rozhraní Wiegand pro připojení čteček, má 2 reléové výstupy, 2 vstupy pro odchodová tlačítka, 2 vstupy pro monitorování stavu dveří, 4 programovatelné výstupy otevřený kolektor. Z jednotky lze řídit kontrolu přístupu pro jedny dveře s rozlišením příchodu a odchodu nebo dvoje dveře s jednosměrnou kontrolou přístupu.

Expandér výstupů

Obsahuje 32 programovatelných výstupů otevřený kolektor, samostatný vstup pro tamper, rozhraní RS 232 pro připojení tiskárny, počítače s grafickým softwarem nebo se softwarem pro uživatelské programování.

Hlavní parametry systému Genesis (hodnoty platí pří rozšířené paměti na 4Mb):

- 128 jednotek – expandérů,
- 512 programovatelných vstupů,
- 512 programovatelných výstupů,
- 64 podsystémů (oblastí),
- 9 400 uživatelů (PIN kód + karta),
- 128 skupin úrovně přístupu pro EZS,
- 128 skupin úrovně přístupu pro EPS,
- 20 000 událostí v paměti,
- 192 dveří pro kontrolu vstupu (127 s oboustrannou kontrolou průchodu),
- 250 úrovní anti-passbacku,
- 254 čteček s univerzálním rozhraním Wiegand 26,
- 32 telefonních čísel na PCO.

2.3 Nadstavbový systém MM8000

Je vytvořený pro centralizaci a řízení bezpečnostních a řídících systémů. Zahrnují řešení pro řízení systémů pro elektrickou požární signalizaci, elektrickou zabezpečovací signalizaci, systémy kontroly vstupu, systémy průmyslové televize, detekci plynu, hasící a evakuační systémy. Jeho otevřená struktura vychází ze současných standardů hardwaru a softwaru. Jeho struktura je vhodná i pro aplikace, u kterých se očekává v budoucnosti rozšiřování.

2.3.1 Vyřízení události

Hlavní obrazovka části Vyřízení události obsahuje seznam událostí, jako jsou poplachy, které se vyskytly, a které vyžadují zásah. Události jsou v seznamu řazené směrem dolů podle jejich důležitosti a jsou prezentovány v různých barvách podle typu, takže lze velmi snadno rozpoznat nejkritičtější hlášení. Seznam událostí lze rovněž filtrovat; pomocí filtru jsou vybrány pouze události s určitými atributy nebo kritérii. Tato funkce umožňuje operátorům zobrazit pouze určitý typ událostí, například podle kategorie nebo podle disciplíny. Mód „V údržbě“ může také být použit pro zobrazení separátního seznamu pro události, které vznikly při servisu nebo testování systému.

2.3.2 Prohlížeč objektu

Tento nástroj vám umožní se pohybovat skrz různé úrovně objektu a řídit všechny nakonfigurované body v systému MM8000. Navigace se provádí pomocí přehledného zobrazení hierarchického stromu objektu a na volitelné grafice nebo mapách. Tato metoda poskytuje snadné vyhledání jednotlivých částí objektu pro provádění jednotlivých příkazů. Mezi ně patří:

- zapínání a vypínání sekcí nebo zón (jejich odpojení a připojení),
- přepnutí libovolného datového bodu do módu údržby,
- přepínání sekcí nebo zón do testovacího módu.

2.3.3 Prohlížení archivu událostí

Poskytuje přístup k záznamu každé události, která se vyskytla a to včetně detailů, jak byla událost vyřízena, kdy a kým. Pomocí této utility jsou snadno generovány přehledy a data snadněji vyvolána pro potřeby vyhodnocení činnost systému a jeho obsluhy.

2.3.4 Plánovač

Slouží pro definování časově závislých funkcí založených na systémovém čase a kalendáři. Také lze vytvořit několik organizačních módů za účelem definování časových bloků, v rámci kterých se systém chová požadovaným způsobem. Během spuštění aplikace se dají modifikovat předdefinované úkoly a také tvořit úkoly nové.

2.3.5 Kontrola vstupu

Integrace systému SiPass do MM8000 umožňuje obsluze dálkově zamykat a odemykat dveře a řídit (jednoduše pomocí myši) přístup do různých částí objektu.

2.3.6 Integrace videa

Vyřízení události a ovládání systému umožňuje doplnit systém MM8000 kamerovým systémem a sledovat a nahrávat vzdálené události.

Další funkce, které systém MM8000 umožňuje:

- zabezpečení přístupu propojené s Windows,
- grafika umožňující využít soubory z programu AutoCAD,
- použít dvou monitorů (jeden na grafické zobrazování, druhý na textové zprávy),
- makro sekvence pro vykonávání naprogramovaných akcí v zabezpečeném objektu,
- programovatelné reakce pro vytvoření automatického spouštění návazností,
- přenos informace o události pomocí SMS, telefonního volače, e-mailu a pageru.

2.3.7 Seznam připojitelných systémů

Požární signalizace, detekce plynu:

- CS11 AlgoRex (EP5) systém elektrické požární signalizace,
- CS11 AlgoRex (EP7F) systém elektrické požární signalizace,
- FC700A systém elektrické požární signalizace,

- CZ10 systém elektrické požární signalizace,
- CC60 systém detekce plynu.

Zabezpečovací signalizace:

- SI410/SI420 Sintony systém elektrické zabezpečovací signalizace,
- CS6 MP3 Guarto elektrické zabezpečovací signalizace,
- CS440 elektrické zabezpečovací signalizace,
- CS4 elektrické zabezpečovací signalizace,
- CZ12 elektrické zabezpečovací signalizace.

Průmyslová televize:

- Video matice SIMATRIX.
- Video digitální záznam SISTORE AX a MXpro,
- Video Web server TELESCAN.

Kontrola vstupu:

- SiPass 2.2.

I/O jednotky:

- Digitální PLC MF7033,
- I/O systém CF9000.

2.3.8 Architektura řešení

Samostatná stanice je nejjednodušší řešení určené pro malé systémy. Má jednu pracovní stanici, která obsahuje všechny softwarové úrovně (client, server a komunikaci). Stanice komunikuje pomocí lokálních portů (EIA/TIA-232) nebo přes Ethernet port NK8000.

Bod na bod je řešení vhodné pro středně velké systémy mající více pracovních stanic, které obsahují všechny úrovně (client, server a komunikaci). Stanice také využívá komunikace přes lokální porty (EIA/TIA-232) nebo přes Ethernet port NK8000.

Architektura typu Client/Server se uplatní nejlépe u velkých systémů s různým účelem ovládacích míst. Stanice serveru zajišťuje komunikace a podpůrné funkce pro jednu nebo více pracovních stanic typu Client. Server koordinuje všechny aktivity tak, že několik operátorů může současně spolupracovat v rámci jednoho systému. Tato architektura také může obsahovat přístup k subsystémům přes síť.

2.4 Systémy Concept 3000 a Access 4000

Představují modulární sytém, který umožňuje vytvářet subsystémy jako zabezpečovací systém, přístupový systém, systém řízení a správy budov (řízení výtahů, klimatizace). Systém je dále schopen částečně integrovat docházkový systém a také další systémy např. CCTV ve spolupráci s nadřazeným PC pomocí softwaru Accept či aplikace ALViS.

Concept 3000 a Access 4000 se řadí mezi modulární systémy, protože jsou rozděleny na řadu zařízení, které mají specifické funkce a komunikují spolu vzájemně po společné LAN. Na jedné LAN jich může být maximálně 250. K rozlišení jednotlivých zařízení na LAN se používá adresa.

Systém se skládá z několika zařízení. Hlavní je ústředna, která shromažďuje všechna konfigurační data, komunikuje se všemi ostatními moduly připojenými do LAN a na základě těchto podkladů rozhoduje o činnostech, které bude systém vykonávat.

K nastavení nebo ovládání systému se používá klávesnice s poosvětleným LCD displejem a 20 klávesami. Tento modul obsahuje 2 vstupy a 2 výstupy, které se dají použít například k ovládání přístupového systému.

Dále systém obsahuje univerzální expandéry s integrovaným zdrojem využívající se na zvýšení počtu zón, výstupů či modulovaných sirén. Přístupové moduly a inteligentní přístupový modul, který umožňuje plně ovládat a monitorovat 4 přístupové body.

Analogové moduly dovolují měřit a vyhodnocovat spojitě se měnící veličiny, jako je teplota, intenzita osvětlení, vlhkost půdy a jiné. Každý analogový modul je vybaven 4 vstupy, které mohou být nezávisle nastaveny. Protože analogové moduly nemají vlastní zdroj je nutné je napájet buď z LAN nebo externího zdroje. LAN izolátor slouží pro rozšíření či rozdělení komunikační LAN. Poskytuje galvanické oddělení mezi jednotlivými segmenty LAN, eliminuje problémy se zemními smyčkami a zlepšuje přepěťovou ochranu. LAN izolátor dále zlepšuje poměr signál/šum a zesiluje signál na velmi dlouhých kabelových trasách. Dovoluje také zapojení „do smyčky“, což zvyšuje bezpečnost LAN subsystému. 2,5 A zdroj je dostupný v různých provedeních. Výstupní napětí je 13,8 V, maximální odebíraný proud je až 2,5 A. Na desce jsou dále obsaženy konektory pro připojení zálohovacího akumulátoru. Zdroj umožňuje detekovat ztrátu AC napájení či pokles napětí zálohovacího akumulátoru. Jednodušší typy zdrojů tyto událostí indikují pomocí výstupů, pokročilejší typy zdrojů tyto informace přenášejí přímo pomocí LAN.

2.4.1 Funkce systému

Základní funkcí systému Concept je zabezpečovací subsystém. Jeho základem jsou vstupy (zóny), které detekují pohyb a jiné události v chráněném objektu.

Základní vlastnosti zabezpečovacího systému:

- max. 4000 zón (vstupů),
- max. 250 nezávislých prostorů (podsystémů,
- max. 4000 uživatelů s kódem PIN a 24576 s přístupovou kartou,
- prostory mohou být ovládány buď jednotlivě či po skupinách,
- programové vlastnosti umožňují ovládání prostoru uživatelem, stavem zóny, výstupem, pomocí PC, na základě časových zón, počtu, uživatelů aj.,
- mohou být vytvořeny „společné“ prostory, které se automaticky aktivují po zabezpečení všech nadřazených oblastí,
- lze použít modulované či spínané sirény, každý prostor může aktivovat jinou sirénu (resp. sirény),
- lze nastavit různé odezvy (typy zón) na jednotlivých vstupech. V rámci typu zóny lze nastavit stavy, které má zóna zpracovávat,
- každá zóna (vstup) smí být zařazena v až 8 různých prostorech s různě definovanou odezvou,
- systémové stavy (výpadek AC, nízké napětí baterie) jsou zpracovávány jako pomyslné zóny a lze tak definovat libovolnou odezvu na vznik těchto událostí,
- uživatelé jsou sdruženi do skupin (do tzv. typů uživatele), přičemž každému typu lze určit, které prostory a dveře smí ovládat a které funkce v systému má mít povoleny,
- každému uživateli lze přiřadit PIN či přístupovou kartu, dále je nutné přidružit typ uživatele,

2.4.2 Řízení přístupu

Systém Concept umožňuje vybudovat plnohodnotný přístupový systém, který může být jednoduše provázán se systémem zabezpečovacím. Základem přístupového systému jsou přístupové body, kterými lze projít až po identifikaci a následném povolení systémem (např. dveře vybavené elektromagnetickým zámkem, turnikety, aj.). Uživatelé jsou v přístupovém systému autorizováni kartou (načítána ve snímači, který je připojen k přístupovému modulu) nebo kódem PIN, který lze zadat na LCD klávesnici. Každým dveřím je nutné přiřadit tzv. skupinu přístupu. Tato programová volba určuje, jaké prostředky (PIN / karta / odchodová / příchodová tlačítka) slouží k otevření dveří. Dále lze nastavit časové okno, kdy bude přístup platný. Mezi další funkce patří vzájemné blokování dveří či proti-dvojí přístup (antipassback).

Volby přístupového systému umožňují:

- Používat max. 250 dveří, dveře mohou být primárně ovládány pomocí čtečky a přístupového modulu či pomocí LCD klávesnice.
- Počet uživatelů vybavených pouze kartou může dosahovat 24 576.
- Dveře mohou být dále ovládány pomocí příchodových a odchodových tlačítek, na základě stavu zóny, na základě výstupu, z ovládacího PC, dle časového nastavení.
- Po připojení detektoru, který kontroluje stav dveří, je možné vyhodnotit násilné otevření dveří či překročení povolené doby pro otevření dveří.
- Přístupový systém lze provázat se zabezpečovacím, např. automatickým vypnutím prostoru, do kterého uživatel vchází skrze konkrétní dveře nebo zamezením přístupu do dveří, které předcházejí zabezpečenému prostoru.
- Proti-dvojí přístup (antipassback), kdy uživatel nesmí vícekrát vstoupit do prostoru, kde se již nachází (nesmí dvakrát vstoupit ze stejné strany dveří)
- Vzájemné blokování dveří znemožňuje otevření dveří v případě, že jsou otevřeny jiné dveře či je sepnut kvalifikační výstup.

2.4.3 Systém správy a řízení budov

Systém Concept se dá využívat i pro správu a řízení budov. Mezi tyto funkce patří zejména ovládání výtahů a ovládání klimatizace.

V systému lze nastavit tři druhy řízení výtahu :

a) jednoduché ovládání pomocí výstupů bez zpětné informace o stisku tlačítka Systém po přiložení karty sepne na určitou dobu výstupy, které „povolují“ tlačítka jednotlivých pater. Tato varianta ovládání se používá v případech, kdy není nutné mít informaci o tom, které tlačítko uživatel vybral.

b) jednoduché ovládání pomocí vstupů a výstupů se zpětnou informací o stisku tlačítka. Systém po přiložení karty snímá po určitou dobu vybrané vstupy a po narušení konkrétního vstupu sepne korespondující výstup, pokud toto dovoluje i nastavení uživatele. Tento typ ovládání výtahu se používá v případech, kdy je nutné mít informaci o výběru patra konkrétním uživatelem.

c) Vysokoúrovňové ovládání skrze linku RS 232. Systém předává informace o přistupujícím uživateli a vybraném patře pomocí sériové linky. Řídící systém výtahu musí podporovat komunikaci ve formátu OTIS/B.

Řízení klimatizace probíhá pomocí výstupů na základě stavu vstupů. Maximálně lze ovládat 4 klimatizační jednotky, každá klimatizační jednotka může řídit klimatizaci v max. 10 prostorech. Systém Concept umožňuje i řízení jednodušších elektrospotřebičů pomocí výstupů. Dále lze nastavit programové volby, které umožňují definici vlastní funkce určitého prvku systému (např. výstupu) na základě stavu jiného prvku (např. zóny). Tak lze definovat funkci, která umožní spínání osvětlení po detekci pohybu v určitém prostoru.

Systém řízení a správy budov dovoluje :

- Řídit přístup max. 32 výtahových kabin do 64 pater.
- Ovládat max. 4 klimatizační jednotky, z nichž každá může řídit klimatizaci v 10 prostorech.
- Zapínat a vypínat jednoduché elektrospotřebiče pomocí výstupů. Maximum výstupů je 3800.
- Definovat vlastní odezvu určitých prvků systému po výskytu konkrétní události.
- Analogový modul může monitorovat a vyhodnocovat spojitě se měnící veličiny.

2.4.4 Komunikační subsystém

Systém Concept je standardně vybaven integrovaným telefonním komunikátorem a jednou sériovou linkou (lze rozšířit až na 5 nezávislých RS 232 linek). Pomocí těchto rozhraní lze komunikovat v mnoha formátech se širokou škálou různých zařízení. Pomocí telefonního rozhraní lze předávat zprávy na PCO, komunikovat se vzdáleným modemem (pro změnu konfiguračních voleb) či používat DTMF ovládání systému. Sériová linka může předávat informace přímo v textovém formátu do připojeného PC či sériové tiskárny, pomocí speciálních komunikačních protokolů PC Direct nebo Accept lze obousměrně komunikovat (měnit konfigurační data, monitorovat či ovládat systém). Takto lze připojit buď PC (programy WDirect, AcceptNet, AlViS) nebo další externí zařízení (GSM modem, komunikační převodník IRC02 / COM, převodník RS232 na TCP/IP).

Komunikační vlastnosti systému :

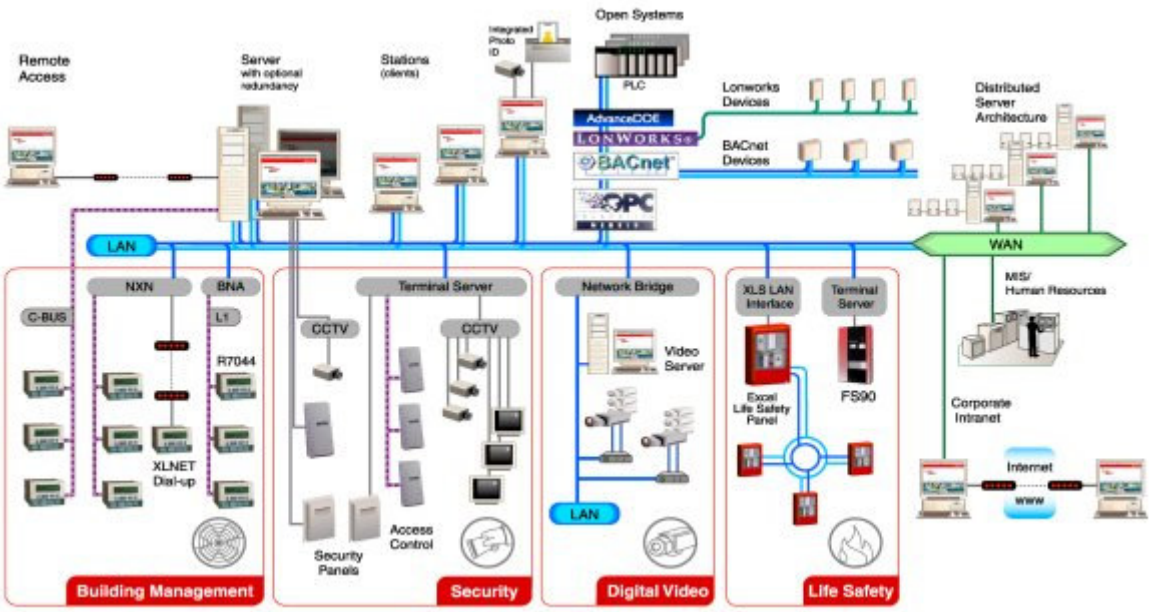
- Ústředna má integrován telefonní komunikátor a jednu sériovou linku.
- Pomocí rozšiřujících portů lze počet sériových linek zvýšit na 5.
- Telefonní komunikátor může předávat zprávy na PCO ve formátech 4+2 Pulse, Contact ID, IR Fast, Securitel.
- Pomocí telefonního rozhraní je dále možné provádět vzdálený přístup přes modem a měnit konfigurační data, monitorovat stav systému či ovládat jeho jednotlivé prvky. Další možností je DTMF ovládání.
- Telefonní rozhraní poskytuje standardní funkce pro monitorování linky, přemostění záznamníku a zpětné volání.
- Sériové linky RS 232 mohou přenášet data do externího systému (sériová tiskárna, PC, převodník RS 232 na TCP/IP, modem, GSM modem) v textovém formátu či pomocí obousměrných protokolů WDirect, Accept.

2.5 EBI (Enterprise Buildings Integrator)

Základem systému EBI je architektura klient-server v prostředí místních i rozprostřených sítí (LAN / WAN) procující pod systémem Windows NT. Systém EBI obsahuje aplikační programy (managery) pomocí kterých lez integrovat tyto systémy:

- kontroléry přístupu a čtečky přístupových karet,
- monitorování bezpečnostních systémů budovy,

- monitorování a řízení vytápění a klimatizace,
- monitorování protipožárních a řízení evakuačních systémů,
- monitorování a řízení spotřeby energií,
- řízení osvětlení budovy či kampusu,
- analogové kamerové systémy (CCTV),
- Digital Video Manager po LAN / WAN síti,
- průmyslové regulátory,
- systémy pro management lidských zdrojů (např. SAP, Peoplesoft),
- časové a docházkové systémy,
- systémy údržby budovy a detekce poruch,
- webové, internetové a intranetové stránky a systémy.



Obr. 14. Architektura systému EBI

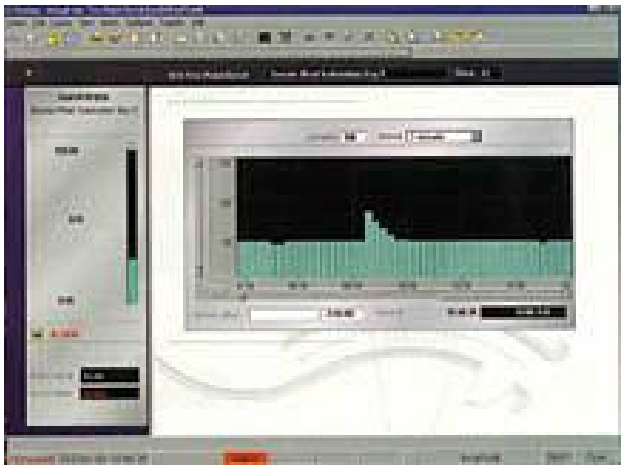
2.5.1 Systém Honeywell LifeSafety Manager

Tato aplikace zajišťuje protipožární ochranu majetku a osob v budovách. Obsahuje tyto součásti:

- Inteligentní zařízení osazená mikroprocesory, např. detektory s více čidly, které velmi brzy upozorňují na kouř nebo požár a téměř zcela odstraňují falešné poplachy.
- Síť peer-to-peer pro rychlou a spolehlivou komunikací požárních řadičů.

- Pokročilý distribuovaný komunikační systém s digitálním zvukem zajišťující bezpečnou a spořádanou evakuaci osob z budovy.
- Integrovaný telefonní komunikační systém pro hasiče.
- Ovládání vytápění, ventilace a klimatizace budovy, např. ventilátorů a klapek, s cílem zadržet kouř a vytvořit bezpečné sekce.
- Otevření požárních dveří a zajištění požárních únikových tras.
- Dohled nad požárními systémy, sprinklerovými ventily a požárními čerpadly.

Rozšiřitelnost systému Honeywell LifeSafety Manager je zajištěna jeho modulární architekturou. Instalace systému je možná na jeden server nebo na více serverů ve více lokalitách. Systém je založen na síťových technologiích firmy Microsoft a standardu TCP / IP a je schopen po sítích LAN / WAN komunikace s dalšími aplikacemi Honeywell EBI, firemními informačními systémy a dalšími obchodními systémy.

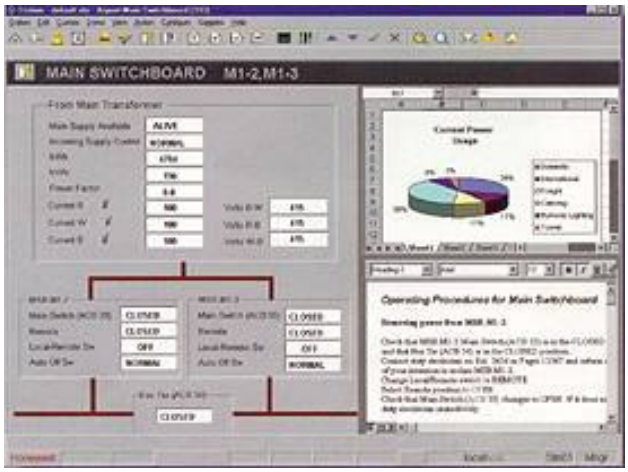


Obr. 15. Správa incidentů a krizí

Systém je vybaven nástrojem ke správě incidentů a krizí. Ten umožňuje správci zobrazit si v reálném čase stav systému. Při instalaci ve více lokalitách umožňuje systém Honeywell LifeSafety Manager poskytováním dat dalším serverům provádět vzdálený dohled v mimopracovní době. Správci tak mohou kontrolovat stav systému a ověřit, jestli byly splněny požadavky na provádění údržby, na dodržování zákonných požadavků a prohlížet si kompletní záznamy o události, nezávisle na vzdálenosti této stanice.

2.5.2 Honeywell Building Manager

Představuje platformu pro otevřenou datovou integraci tradičních systémů budov a klíčových podnikových systémů. Podporuje hlavní standardy (např. LonMark, BACnet, ODBC).



Obr. 16. Uživatelské rozhraní

2.5.3 Honeywell Security Manager

Funkce systému:

- grafické uživatelské rozhraní založené na operačním systému Microsoft Windows NT,
- distribuované sledování a řízení až 40 místních a vzdálených pracovních stanic,
- grafické obrazovky, které lze upravit tak, aby zobrazovaly podrobné mapy budovy a umožňovaly přehlednější řízení kritických informací,
- napojení na špičkové CCTV řadiče průmyslových kamer třetích stran,
- databáze údajů držitelů karet Microsoft SQL Server 7.0,
- strukturované řízení alarmů se zobrazením akčních plánů a souvisejících informací na obrazovce, což zajišťuje včasnou a správnou reakci na alarmy,
- plně integrovaný systém identifikačních karet s fotografií,
- pružně měnitelné sestavy,
- průmyslový síťový standard.

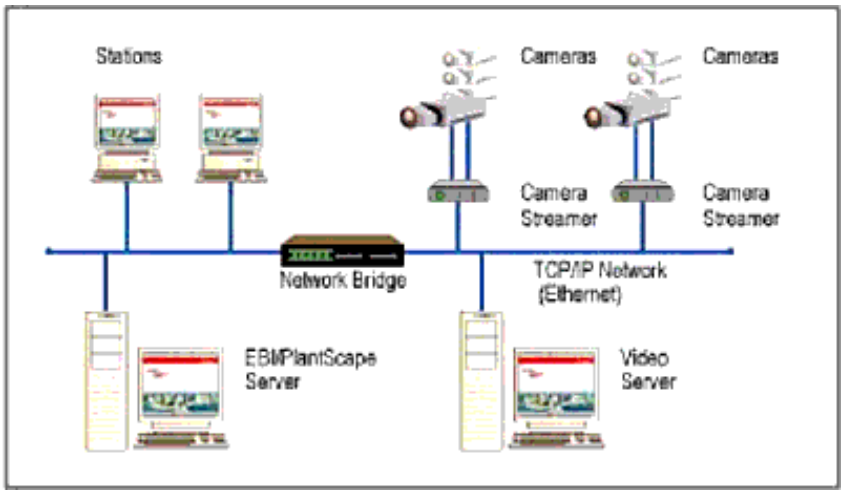
Obr. 17. Centrální řízení karet

Systém Honeywell Security Manager využívá databázi SQL 7.0 Server k usnadnění řízení přístupu zaměstnanců, dodavatelů a návštěvníků. Databáze podporuje 70 standardních konfiguračních polí na každého držitele karty. Do každého pole lze napsat 55 znaků.

2.5.4 Honeywell Digital Video Manager

Převádí do digitální platformy záznamy z videokamer, provádí transport záznamů po lokální síti a umožňuje s nimi pracovat. Všechna data jsou přenášena pomocí sítí a ukládají se na počítačích.

Nahrávání záznamu je založeno na vzniku události (alarmu), tím se šetří zdroje a snižuje zatížení sítě. Záznam se nahrává i v době před vznikem události, a tak umožňuje určit příčinu vzniku poplachu. Obrazové záznamy můžeme prohlížet on-line a současně nahrávat. Na uživatelské obrazovce se dají zobrazit 4 kamery současně. Všechny záznamy jsou dostupné z každého pracoviště EBI.



Obr. 18. Struktura systému Honeywell Digital Video Manager

2.6 Bezpečnostní systém Cardkey P2000

Bezpečnostní systém Cardkey P2000 je určen pro střední a velké aplikace s vysokými nároky na bezpečnost. Kromě základních funkcí přístupového systému je nedílnou součástí programového vybavení poplachová grafika, monitorování poplachů, integrace výtahů, podpora evakuace a správa kontrolovaných prostor a nebezpečných zón, správa návštěvnických karet, zálohování databáze a možnost integrace systému P900. Volitelnými součástmi jsou integrace CCTV a DVR, potisk a správa karet, obchůzka strážných, dělení databáze pro více uživatelů, redundance pro zajištění zálohy systému a podpora protokolu BACnet. Komunikační protokol BACnet zajišťuje jednoduchou integraci do systému řízení budov Johnson Controls Metasys. Modulární architektura systému umožňuje jeho snadné rozšiřování a přizpůsobování představám a požadavkům uživatele. Kapacita systému je až 2048 čteček, 100 000 držitelů karet a možnost připojení až 1 000 vzdálených míst. CardKey PEGASYS 2000 umožňuje připojit až 39 pracovních stanic a 1 server v síti.

P2000LE je nová verze produktu P2000. Je určen pro malé a střední aplikace a zajišťuje komfort a obsluhu jako P2000při nižších nákladech. Základní kapacita systému je 32 čteček s možností rozšíření až na 128. Programové moduly jsou shodné se systémem P2000.

2.7 Integrovaný bezpečnostní systém WIN-PAK PRO

Program WIN-PAK PRO je softwarovým nástrojem pro konfiguraci jednotek kontroly přístupu řad N-1000 a PW-5000, monitorování jejich činnosti a provádění podpůrných operací. Kombinací vyspělých bezpečnostních technologií s moderními síťovými funkcemi přináší uživateli plnohodnotné řešení otázek bezpečnosti přístupu vhodné pro instalace jakéhokoliv rozsahu.

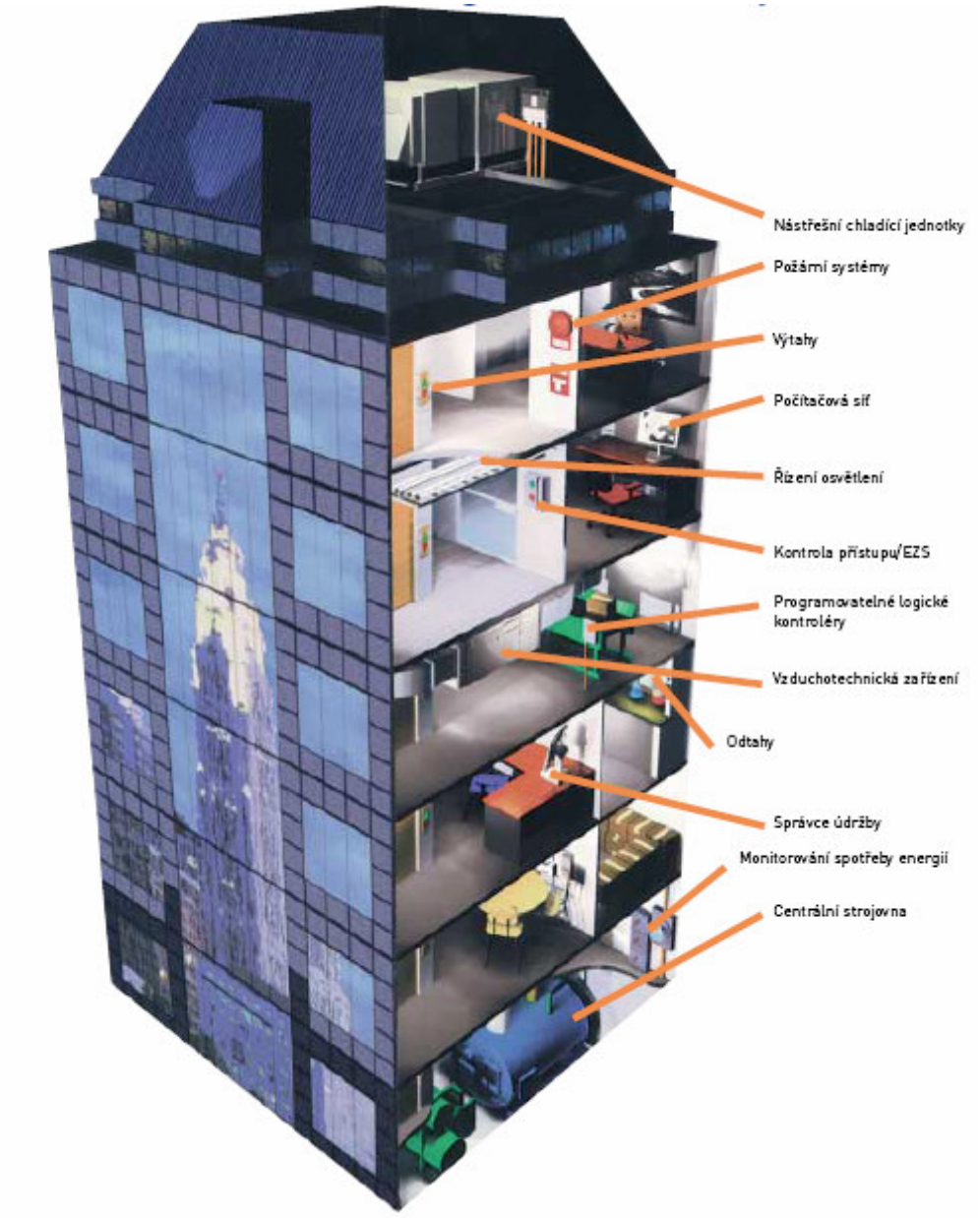
WIN-PAK PRO má implementovány funkce pro kontrolu přístupu, alarm monitoring, řízení CCTV i personifikaci identifikačních karet. Je to 32-bitová aplikace určená pro použití v prostředí Windows NT, Windows 2000 nebo Windows XP, jejichž bezpečnostních funkcí plně využívá. Model oddělených serverů v rámci LAN/WAN umožňuje distribuované zpracování, což výraznou měrou zvyšuje výkon systému. Flexibilní databázová architektura používá jako databázový stroj Microsoft SQL Server. Ten je vhodný všude tam, kde je kladen důraz na výkon, spolehlivost a rychlost zpracování. Podpora vícenásob-

ných účtů dovoluje operátorům rozdělení karet a jejich držitelů do samostatných skupin, se kterými se pracuje odděleně. Navíc mají operátoři k dispozici nástroje pro návrh potisků karet, sledování prostor pomocí kamer nebo vytváření tištěných přehledových zpráv. WIN-PAK PRO umožňuje:

- integrované řízení CCTV, snímání fotografií a potisk karet,
- oddělené servery v rámci LAN/WAN,
- vícenásobné účty pro dělení karet do skupin v rámci LAN/WAN,
- přímé propojení s řídicími jednotkami metalickou sběrnicí nebo vytáčeným spojem,
- dálkové propojení s řídicími jednotkami po LAN/WAN (TCP/IP),
- dynamické mapy podlaží pro ovládání a monitorování systému,
- podpora jazykových mutací,
- hromadné přidávání a mazání karet,
- vytváření návrhů pro potisk karet a vlastní potisk (ID Badging),
- automatické vyhledávání a zobrazování karty při jejím načtení (pro ověřování totožnosti držitele).

3 INTELIGENTNÍ BUDOVY

Inteligentní budovy jsou objekty s integrovaným managementem, tzn. sjednocenými systémy měření a regulace (technika prostředí, komunikace, energetika), zabezpečení (kontrola přístupu, požární ochrana, bezpečnostní systém) a správy budov (plánování, pronájem, leasing, inventář).



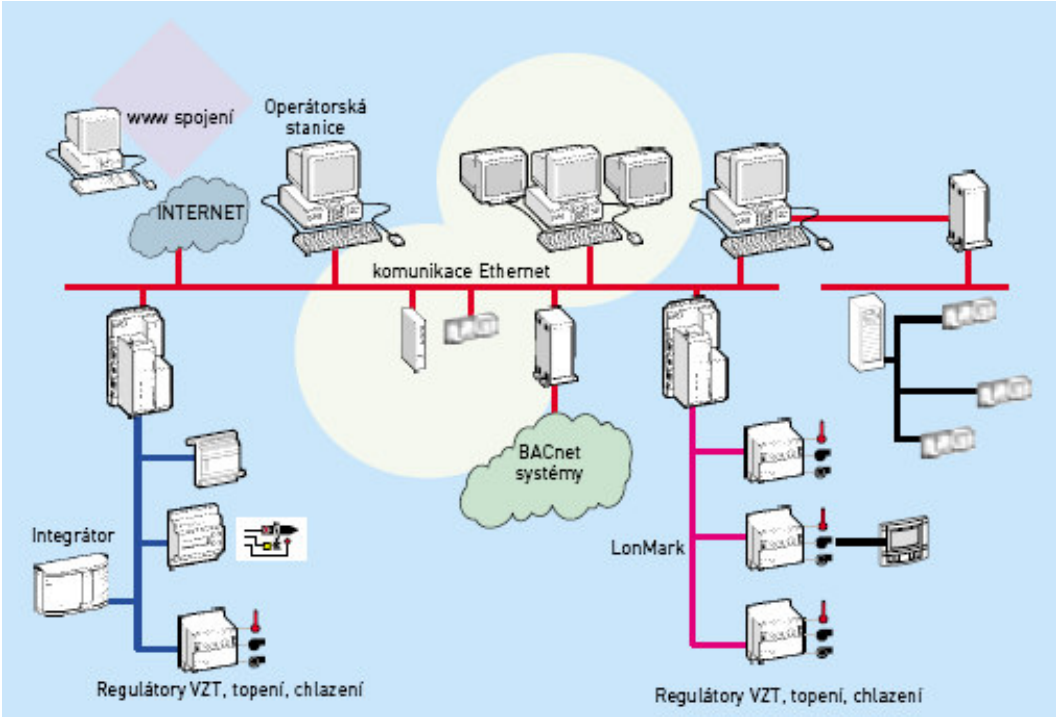
Obr. 19. Profil inteligentní budovy

Optimalizací těchto složek a vzájemnými vazbami mezi nimi je dosaženo prostředí, které je efektivní z hlediska nákladů, uspokojuje potřeby vlastníka budovy i nájemníků. K požadavkům vlastníka (investora) patří minimalizace nákladů na energii, minimalizace

provozních nákladů, minimalizace nákladů na opravy a rekonstrukce. Nájemníci mají požadavky na flexibilitu pronajatých prostorů a na to, jakým způsobem bude kvalita prostředí budovy přispívat ke zvýšení produktivity práce. Dá se říct, že termín „inteligentní budova“ znamená koncepci, která vychází z trvalých potřeb uživatelů (zatímco jednotlivé technologie jsou rychle překonávány modernějšími).

3.1 Přenos dat mezi systémy

Pro funkci budovy jako celku je však nutný přenos informace mezi jednotlivými systémy (při požárním poplachu se spustí požární ventilace, vypne ostatní vzduchotechnika, uvedou se do požárního režimu výtahy, osvětlí se evakuační trasy atd.). Přenos dat je uskutečňován elektronickou cestou, která je operativnější a hlavně méně chybová, než pokud by spolu komunikovali pracovníci.



Obr. 20. Přenosové trasy

Vazby mezi systémy mohou být realizovány diskrétními signály přenášenými mezi vstupním a výstupním zařízením jednotlivých systémů. Tento způsob je omezen počtem vstupů a výstupů a také je náročný na pozdější rozšiřování systému, protože se musí udělat zásahy do hardwaru a vytvořit nová propojení. Vhodnější metody propojení u inteligent-

ních budov se dá dosáhnout propojením systémů prostřednictvím komunikačních kanálů a to následovně:

- využitím brány (gateway) – jednotky, které překládají komunikační protokol a data jednoho dodavatele do protokolu jiného dodavatele,
- sdílenými protokoly, které jsou výsledkem spolupráce dvou nebo více dodavatelů, vyvíjející společný protokol, který umožňuje oboustrannou komunikaci jejich zařízení,
- aplikací standardních protokolů. Výrobce, který je ve shodě s daným standardem, se může připojit na jakékoliv zařízení jiného výrobce. V současné době existuje řada takovýchto standardů (BACnet – Building Automation and Control Network, LON – Local Operating Networks).

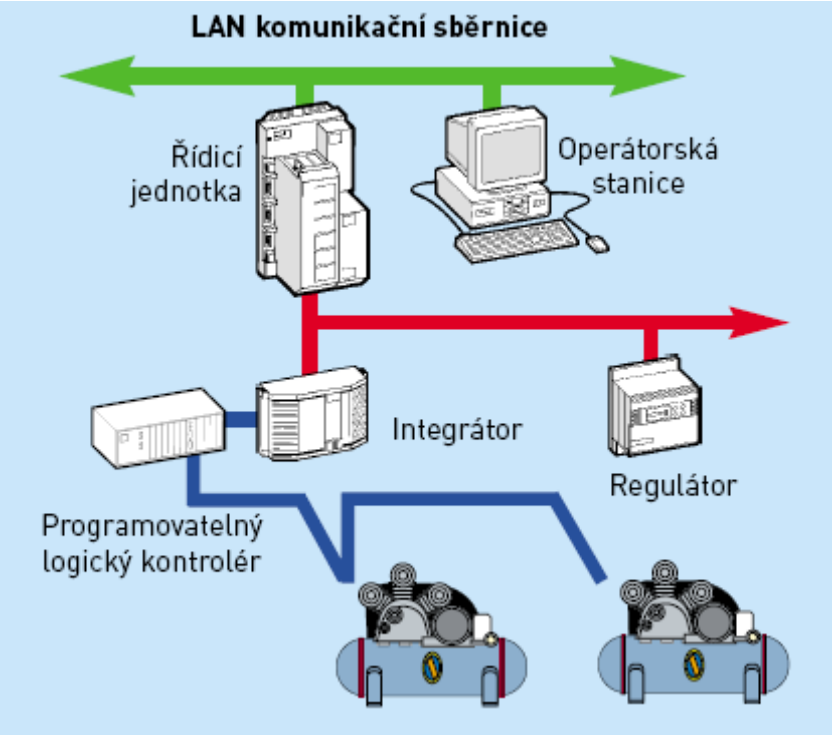
3.2 Systémy řízení, vytápění, chlazení a vzduchotechniky.

Jsou řešeny v decentralizovaném systému, jehož hlavní výhody spočívají ve větší odolnosti proti poruchám systému (to znamená, že pokud nastane porucha v některé části systému, má to vliv pouze na část systému), v lepší možnosti údržby a kontroly systému (to umožňuje umístění regulátorů poblíž řízené technologie) a také větší spolehlivosti systému (té se dosahuje zkrácením kabeláže k čidlům a tím omezení indukování rušivých signálů).

Evropská standardizační komise definuje tři automatizační úrovně. První úrovní je lokální řízení. Tato úroveň je tvořena mikroprocesorovými regulátory, ke kterým jsou připojena všechna čidla a akční členy sloužící k sledování měřených a regulovaných veličin. Regulátory podle určitého algoritmu zpracovávají vstupní signály, vyhodnocují je a na základě toho regulují jednotlivá zařízení dané technologie. Regulátory jsou vybaveny také ručním ovládáním, které je třeba zabezpečit proti neoprávněnému zásahu.

Druhá je automatizační úroveň, která je nadřazená úrovni lokálnímu řízení. Zajišťuje vzájemnou komunikaci mezi regulátory a všemi komponenty spadající do této technologické úrovně a také řeší algoritmy vyšší úrovně. To zajišťuje operační systém pracující v reálném čase. Jednotlivé síťové jednotky společně komunikující v síti LAN protokolem TCP/IP. Hlavní činnost těchto jednotek spočívá ve sběru historických dat, omezování spotřeby a přesouvání zátěží, ve spouštění a odstavování zařízení a v provádění komplexních časových programů.

Nejvyšší úrovní je správa informací, kterou provádějí operátorské pracovní stanice, které už nezajišťují žádné dohlížecí a řídící funkce. Jsou připojeny také k síti LAN a jsou vlastně zprostředkovateli informací o průběhu řízení budovy. Operátorům poskytují informace o stavu řízené technologie, a to v textové nebo grafické podobě, a upozorňují na poplachová hlášení.

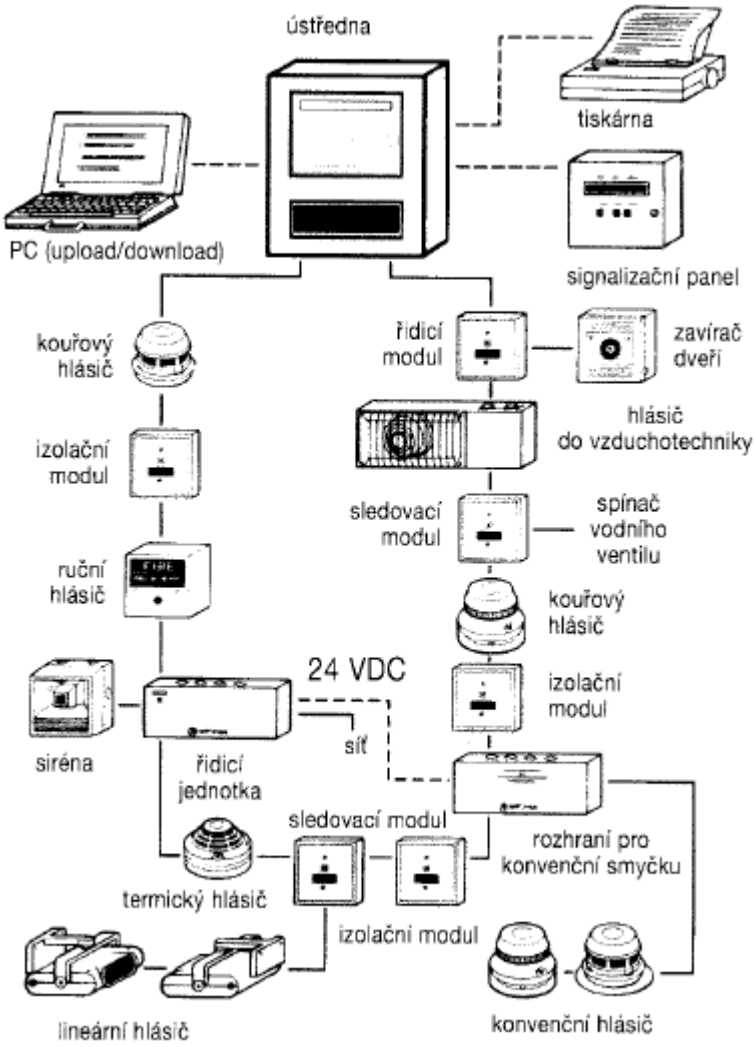


Obr. 21. Automatizační úrovně

3.3 Elektronická požární signalizace

Jejím hlavním úkolem je detekovat místo vzniku požáru, a to v co nejranějším stádiu vzniku. Využíváme na to několik druhů detektorů, které podle principu detekce dělíme na detektory kouře, teploty a plamene. Existují detektory detekující pouze jeden jev, ale i detektory kombinované. Propojení požární signalizace s ostatními subsystémy budovy umožňuje činnosti vedoucí k efektivnějšímu zvládnutí poplachové situace. Může to být aktivace kamerových systémů v ohrožené oblasti, zabezpečení požárního režimu provozu výtahů, aktivování akustické a optické signalizace, uvolnění dveří na únikových trasách a aktivace požárních klapek. Celkový průběh situace je zobrazován na operátorském pracovišti, a to např. v grafickém režimu, kdy je zobrazen půdorys budovy s přesně vymezenou lokalitou

nebo místem poplachu. To umožňuje operátorům mít dostatečný přehled o situaci, a tak předcházet panice a zbytečným ztrátám na životech a majetku.



Obr. 22. Typická konfigurace systému EPS

3.4 Zabezpečovací a přístupový systém

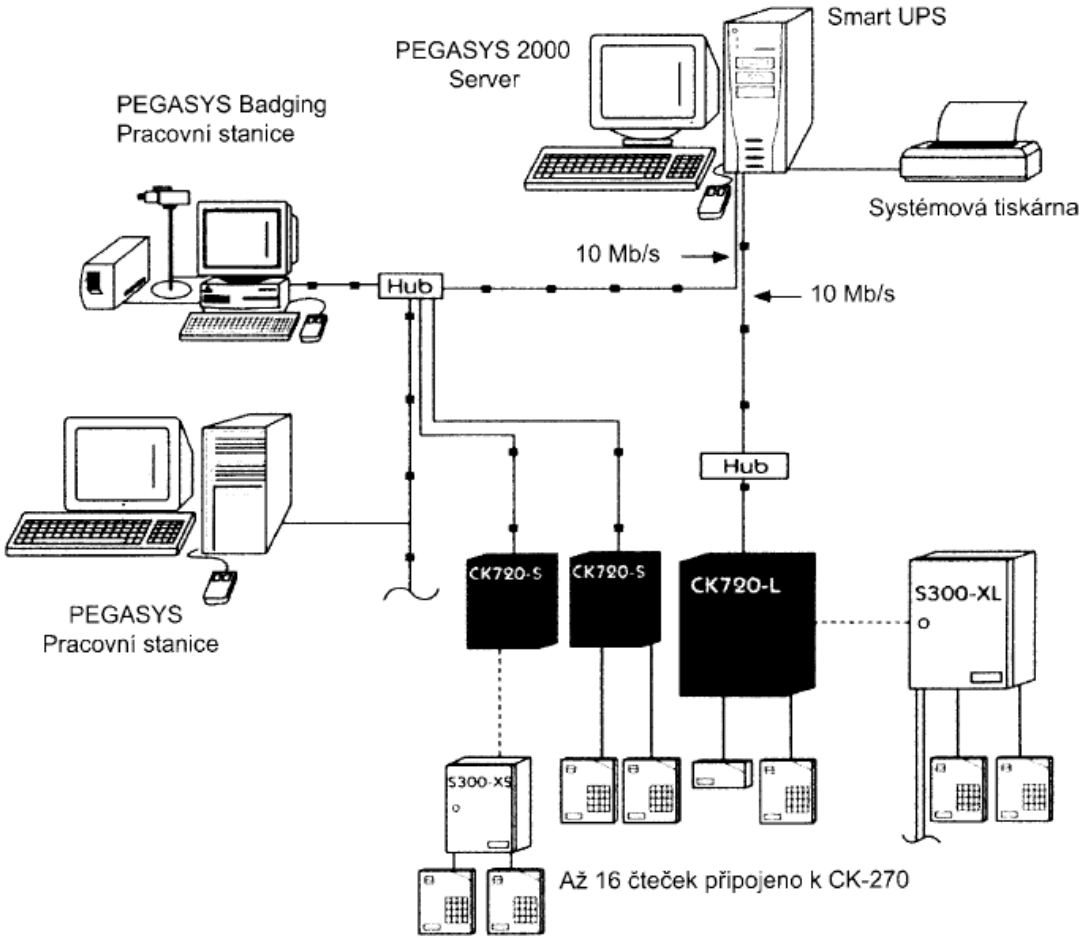
Tento systém slouží pro ochranu osob a majetku nacházejících se ve střeženém objektu. Jeho vstupními členy jsou čidla, která reagují na různé fyzikální. Jsou to zejména detektory reagující na pohyb osob, detektory tříštění skla, magnetické kontakty a tísňová tlačítka.

Stejně jako u systému EPS má operátor k dispozici informace o tom, v jakém stavu se jednotlivá čidla nacházejí, a je upozorněn, když některé vyhlásí poplach. Většinou má

k dispozici software s půdorysy budovy a přesným umístěním jednotlivých čidel. To mu umožňuje sledovat i případnou trasu narušitele a informovat členy ostrahy. Pokud je tento systém propojen i se kamerovým systémem můžeme získat detailní informace o činnosti narušitele.

Propojení s ostatními subsystémy jako je osvětlení a klimatizace se využívá k ušetření nákladů na provoz budovy.

Jedna z nejčastějších integrací systému EZS je se systémem kontroly vstupu. Tím se nám stává z přístupového systému systém poplachový, který nás upozorní na jakékoliv nestandardní situace, které nastávají při vstupu nepovolané osoby.



Obr. 23. Integrace systému EZS se systémem kontroly vstupu

3.5 Uzavřený televizní okruh

Jedná se o systém monitorování pomocí kamer jednotlivých prostorů v budově. Kamery volíme podle požadavků monitorování. Snímané scény jsou zobrazovány na pracovišti příslušného operátora na monitoru buď z jednotlivých kamer nebo pomocí multiplexerů i z více kamer najednou. V dnešní době existují inteligentní druhy softwarů umožňující „poznat“ definované nestandardní situace a upozornit na ně obsluhu (např. vnik osoby nebo vozidla do monitorovaném prostoru, počet projetých vozidel případně rozpoznání polohy monitorované osoby). U kamerového systému je užitečná provázanost se systémem elektronické zabezpečovací signalizace, kdy se můžeme podívat pomocí jednotlivých kamer na zóny, ve kterých došlo k vyhlášení poplachu, zapnout příslušný režim zaznamenávání obrazu z těchto zón a také při ztrátě signálu z některé kamery může systém EZS vyhlásit poplach.

3.6 Management energetického hospodářství

Provozní náklady u inteligentních budov jsou jedním z hlavních kritérií návrhu systému. Vhodnou organizací práce a dobou provozu jednotlivých energeticky náročných pracovišť lze výrazně provozní náklady snížit. Zde se projeví jak vhodně je nastavena schopnost jednotlivých subsystému společně komunikovat. Úspor energie můžeme dosáhnout hlavně následujícími postupy:

- spolupráce systémů vytápění, chlazení a vzduchotechniky musí být účinná a nesmí se stávat, že by např. bylo v určité oblasti pro dosažení požadované teploty aktivováno jak chlazení, tak vytápění,
- při vytváření vnitřního klimatu vzít v úvahu vnější podmínky v okolí budovy,
- snižování spotřeby krátkodobým vypínáním zařízení, např. vypínáním ventilátorů na 10 minut v každé hodině,
- využívat úspornější zdroje osvětlení,
- vytvořit regulaci intenzity osvětlení podle denního světla.

Důležitou funkcí řídícího systému je také sledování technického maxima tak, aby nebyla překročena penalizovaná hodnota. Toho systém docílí tím, že neustále monitoruje okamžitou hodnotu odebírané energie a srovnává ji s ideální hodnotou a v případě překro-

čení vypne zařízení s menší prioritou. Systém také musí počítat s jednotlivými druhy zařízení (těžké stroje nebo setrvačné spotřebiče s dlouhou časovou konstantou). Je samozřejmé, že zařízení patřící k ochraně osob a majetku má nejvyšší prioritu a tudíž je jeho vypnutí nepřípustné.

4 NÁVRH INTEGROVANÉHO SYSTÉMU

4.1 Požadavky

Pro návrh integrovaného systému jsem vybral budovu, u které je požadavek na integraci systémů elektronické zabezpečovací signalizace (vybral jsem variantu, která již sama obsahuje možnost připojení kontroly přístupu), dále plnohodnotného systému elektronické kontroly vstupu a kamerového systému.

4.2 Popis integrující části systému

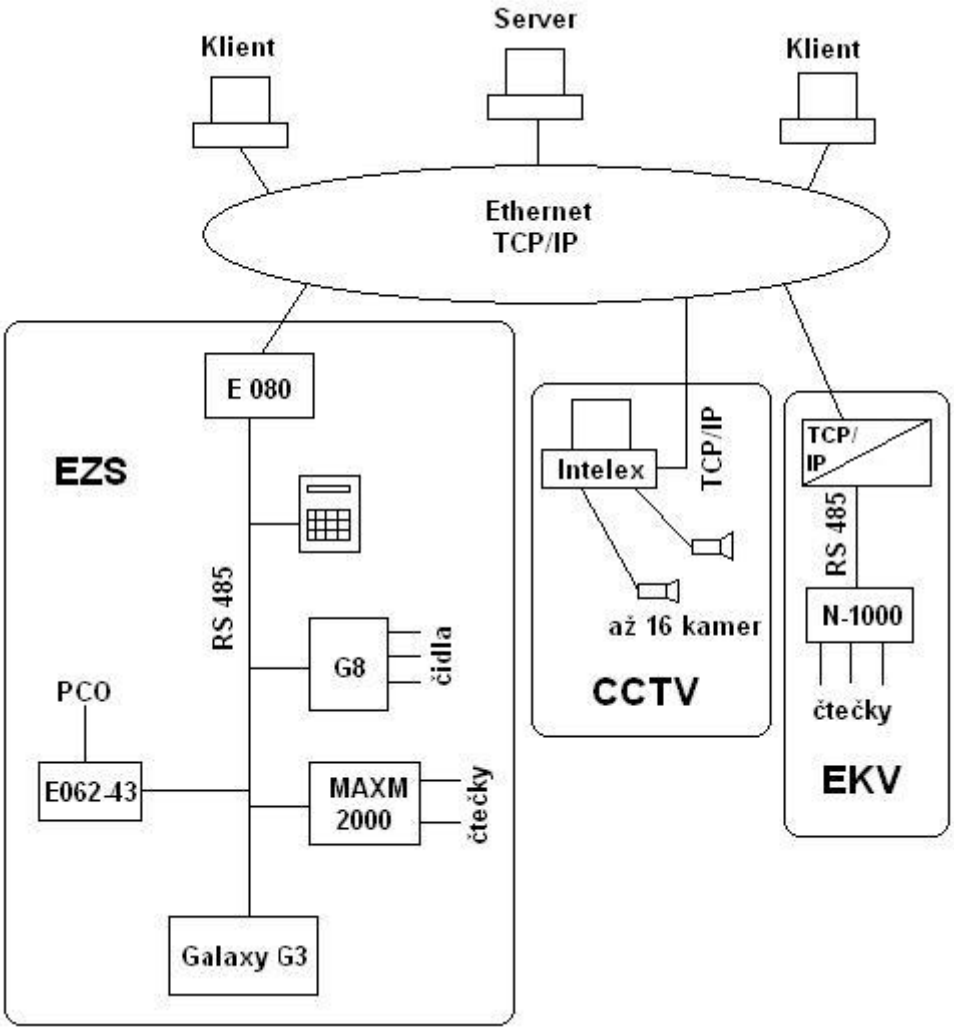
Celou aplikaci jsem se rozhodl integrovat pomocí systému ABI (Advanced Building Intelligence), který je produktem firmy Honeywell. Umožňuje vzdálenou správu, řízení a monitorování integrovaných systémů. Pro jeho využití zakoupíme licencovanou verzi (ošetřeno hardwarovým klíčem) a nainstalujeme na server. Dále budeme potřebovat softwarové překladače, tedy DDE servery a to konkrétně:

- DDE server Galaxy
- DDE server Intelex
- DDE server Northern Computers

Přenosové prostředí je tvořeno sítí LAN v rámci budovy, ve které systémy fungují, ale také sítí WAN pokud uvažujeme klienty, kteří budou chtít správu vykonávat vzdáleně. Vše přes protokol TCP/IP a připojení web klientů s rychlostí minimálně 128 kB/s.

4.3 Popis jednotlivých systémů

Pro systém EZS jsem vybral ústřednu Galaxy G3-144, která umožňuje vytvoření až 68 zón za použití vstupně výstupního modulu G8. Dále digitální komunikátor E062-43 s integrovaným modemem pro přenos událostí na PCO. Integrovanou součástí této ústředny bude systém kontroly vstupu MAXM 2000. Ústředna používá ke komunikaci datovou sběrnici RS 485 a musíme tedy pro připojení k LAN/WAN použít modul E080, který převádí tento formát na protokol TCP/IP.



Obr. 24. Blokové schéma systému

Kontrolu vstupu bude zajišťovat systém N-1000-IV, který umožňuje nastavit 63 časových zón a základní jednotka může pracovat v autonomním režimu a ovládat 4 dveře nebo ji lze rozšířit připojením na sběrnici RS 485 a tím počet jednotek zvýšit na 63.

K zabezpečení kamerovým systémem jsem použil digitální videosystém Intellex v3.2, který má výstup přímo připojitelný do počítačové sítě a tak nepotřebuje žádný převodní modul. Lze na něj připojit až 16 kamer. Umožňuje sledovat živý obraz (z jedné nebo více kamer), vytvářet a přehrávat obrazové záznamy a další funkce jako úpravu a přibližování obrazu, nahrávání před i při detekci poplachu, zaznamenávat zvuk atd.

ZÁVĚR

Integrované poplachové systémy jsou systémy, které umožňují spolupráci svých jednotlivých subsystémů, jejich ovládání a nastavování a také vizualizaci a centralizaci informací, které tyto subsystémy poskytují. Tyto funkce nám umožňují efektivnější zabezpečení chráněných zájmů a přinášejí nám i ekonomicky výhodnější řešení. Před výběrem konkrétního systému musíme posoudit řadu kritérií a podle nich zvolit vhodný typ integrovaného systému. Základním vodítkem a také legislativním celkem v této oblasti je norma ČSN CLC/TS 50398. Ta definuje jednak názvosloví související s integrovanými a kombinovanými poplachovými systémy, dále uvádí obecné typy struktur těchto systémů a rady pro prvotní návrh systému a další požadavky a pokyny na montáž a testování týkající se integrovaných systémů.

Pro obsáhnutí znalostí o integrovaných systémech je třeba znát jednak možnosti těchto systémů, ale také vlastnosti a princip jednotlivých subsystémů, které integrujeme. Výrobci integrovaných systémů v této souvislosti narážejí na problém kompatibility protokolů, pomocí kterých tyto systémy komunikují. Tento fakt je dán historickým vývojem nejen elektronických zabezpečovacích systémů, ale prakticky u všech technologických systémů, které využívají nějaký protokol. Výběr integrovaných systémů je na dnešním trhu dostatečný a při návrhu systému je třeba dobře posoudit o jak velkou aplikaci se bude jednat a jaké systémy chceme integrovat.

V případě objektů s integrovaným managementem (inteligentních budov), tedy se sjednocenými systémy měření a regulace, zabezpečení a správy budov je integrování systémů nevyhnutelné, protože zvládání řízení těchto systémů pouze lidskými zdroji je nemožné. Integrace systémů přináší mnoho viditelných výhod, kterými jsou úspory energií a tedy nákladů na provoz, efektivnější spravování a zabezpečení budovy a větší komfort pro osoby nacházející se v budově.

SEZNAM POUŽITÉ LITERATURY

[1] KINDL, J. Projektování bezpečnostních systémů I.díl, Zlín: vyd. Univerzita Tomáše Bati ve Zlíně, 2004. ISBN 80-7318-165-7.

[2] Poplachové systémy- Kombinované a integrované systémy- Všeobecné požadavky, ČSN CLC/TS 50398, Březen 2005

[3] Katalogové listy, instalační a uživatelské manuály firmy Honeywell

[4] Katalogové listy, instalační a uživatelské manuály firmy Siemens

[5] Katalogové listy, instalační a uživatelské manuály firmy Eurosat CZ

[6] Katalogové listy firmy Alarm Absolon

[7] Katalogové listy firmy Johnson Controls

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

CCF	Ústřední řídící jednotka.
CCTV	Uzavřený televizní okruh.
ČSN	Česká státní norma.
EPS	Elektrická požární signalizace.
EZS	Elektronická zabezpečovací signalizace.
LAN	Local Area Network – lokální datová síť.
PCO	Pult centralizované ochrany.
PKB	Průmysl komerční bezpečnosti.
PPC	Poplachové přijímací centrum.
RS 232	Komunikační sběrnice
RS 485	Komunikační sběrnice.
TCP/IP	Komunikační protokol.
WAN	Wide Area Network – dálková datová síť.

SEZNAM OBRÁZKŮ