

Současné trendy využití integrovaných elektronických systémů v průmyslu komerční bezpečnosti.

Petr Skřebský

Bakalářská práce
2005



Univerzita Tomáše Bati ve Zlíně
Fakulta ...

Vložit oficiální zadání diplomové/bakalářské práce

Originál list

Děkuji tímto svému vedoucímu bakalářské práce Ing.Jiřímu Kindlovi za odborné připomínky, které mi poskytl z jeho dlouholeté praxe ve vývoji systémů.

Dále bych chtěl poděkovat všem zástupcům firem, kteří se podíleli na mém rozvoji v tomto oboru. / Ing. Procházka, p.Schwarz (Novar), Ing. Bojanovský (Johnson Controls), Ing. Konečný (Honeywell), Ing. Panáček (Trade Fiedes), Ing Merhaut (TT-systém), Ing. Pastyřík (CGC) a další./

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

Ve Zlíně, 30. 05. 2005

Petr Skřebský

Abstrakt

Předmětem této bakalářské práce je ukázat současný směr integrace elektronických systémů v průmyslu komerční bezpečnosti. Základní kámen integrace musí být položen na samém počátku výstavby systému a není rozhodně dílem jednoho člověka nýbrž týmu odborníků. Výběr a popis uvedených systémů je rozhodně důkazem snahy výrobců nalézt cestu k integraci a vzájemné kompatibilitě. Integrace uplatňovaná v průmyslu komerční bezpečnosti zahrnuje nejenom poplachové systémy, ale také i životně důležité technologie.

Abstract

The aim of this bachelor's thesis is to show the current tendency of integration of electronic systems in commercial security industry. Integration should be one of the first steps when planning the conception of the system and it shouldn't be considered by just one person but rather by the team of specialists. The sample and description of presented systems gives evidence of the effort of the producers to find the way to integration and mutual compatibility. The integration used in commercial security includes not only alarm systems but also vital technologies.

OBSAH

ÚVOD	7
1 CÍL PRÁCE A METODIKA	8
2 KONCEPCE INTEGROVANÉHO ELEKTRONICKÉHO SYSTÉMU	9
2.1 VŠEOBECNÉ POŽADAVKY DLE ČSN EN 50 398	9
2.1.1 Definice pojmů	9
2.1.2 Normativní odkazy.....	11
2.1.3 Poplachové normy po našem vstupu do EU	13
2.1.4 Základní typy struktur.....	14
2.1.5 Obecný návrh (projekt)	16
2.1.6 Zásady propojení	16
2.1.7 Současný výskyt událostí a její priority.....	17
2.1.8 Centrální řídicí zařízení	18
2.1.9 Pokyny pro použití, montáž a servis	18
3 SOUČASNÉ POPLACHOVÉ SYSTÉMY UMOŽŇUJÍCÍ INTEGRACI V PKB 21	
3.1 ROZDĚLENÍ SYSTÉMŮ A TROCHA HISTORIE	21
3.2 NOVAR.....	22
3.2.1 EZS.....	22
3.2.2 EPS	27
3.2.3 ACCES	30
3.2.4 CCTV	32
3.2.5 Centrální řídicí zařízení Winmag	32
3.3 HONEYWELL	34
3.3.1 Integrace EZS a ACCES.....	34
3.3.2 Centrální řídicí zařízení ALViS	36
3.4 SIEMENS	37
3.4.1 Integrace EZS a ACCES.....	37
3.4.2 Centrální řídicí zařízení MM 8000	39
3.5 SPELZA.....	40
3.5.1 Integrace EZS a ACCES.....	40
3.5.2 Domi Net.....	42
3.6 POSTECH	43

3.6.1	Integrace EZS, ACCES a správa budov	43
3.7	INNER RANGE	44
3.7.1	Integrace EZS, ACCES, správa a řízení budov	44
3.8	CGC SECURITY	47
3.8.1	Centrální řídicí zařízení SBI	47
4	KOMPLETNÍ SYSTÉMOVÁ OCHRANA V PKB	52
4.1	VZNIK A HISTORIE - INTELIGENTNÍ BUDOVA.....	52
4.2	PROPOJENÍ JEDNOTLIVÝCH SYSTÉMŮ, INTEGRACE	52
5	NÁVRH INTEGROVANÉHO SYSTÉMU V TECHNOLOGII SBI	55
5.1	TECHNOLOGICKÉ POŽADAVKY NA INSTALACI A PROVOZ SYSTÉMU....	55
5.1.1	Jednouúčelové systémy	55
5.1.2	Přenosová trasa.....	55
5.1.3	Serverová část	55
5.1.4	Pracovní stanice.....	56
5.1.5	Sítové rozhraní.....	56
5.1.6	Popis implementace.....	57
5.2	BLOKOVÉ SCHÉMA NÁVRHU ŘEŠENÍ	59
5.2.1	Licenční politika	59
ZÁVĚR		60
SEZNAM POUŽITÉ LITERATURY.....		61
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK		62
SEZNAM OBRÁZKŮ.....		63
SEZNAM TABULEK		64
SEZNAM PŘÍLOH.....		65

ÚVOD

Skutečná hodnota průmyslu komerční bezpečnosti je založena na znalostech a schopnostech jejich pracovníků a na inovačním spektru produktů. Průmysl komerční bezpečnosti vychází:

- z faktoru růstu potřeb v sektoru bezpečnosti
- z vysokého počtu oznámených trestních činů
- z pocitu veřejnosti a vyššího ohrožení kriminálními živly
- z rozvoje elektroniky a s tím spojené produkce
- z větší poptávky po ochraně majetku technickými prostředky.

Průmysl komerční bezpečnosti se nemůže obejít bez nasazení technických prostředků, pokud ochrana má být účinná. Integrací poplachových elektronických systémů zvyšujeme účinnost ochrany za minimálního zásahu lidského faktoru. Integrací nepoplachových elektronických systémů snižujeme rizika, která mohou nastat na zařízeních sloužících k běžnému provozu. Integrace poplachové i nepoplachové informace nepopíratelně zvyšuje pravděpodobnost adekvátního chování na vzniklou situaci vzhledem k psychofyzilogickým vlastnostem člověka. Integrace musí být založena na přesné lokalizaci technologického celku, podlaží, místnosti, jednotlivého prvku.

Navržený systém pro průmysl komerční bezpečnosti musí být řešen jako důsledně integrovaný bezpečnostní systém s jednotlivými samostatně pracujícími podsystémy. Tyto podsystémy jsou propojeny do řídicího a monitorovacího centra systému. Musí se jednat o systém událostního typu. Činnost obsluhy a podněty od jednotlivých prvků systému jsou uloženy s časovou, datumovou a popisnou značkou, která jednoznačně lokalizuje událost. Na tyto události reaguje podsystém automaticky nebo předává informaci na vyšší stupeň řízení. Pro obsluhu řídicího centra jsou prvotně zobrazovány události s prioritou ohrožující život, zdraví a majetek. Ostatní události jsou potlačeny, dle priority zobrazeny nebo jen uloženy do deníku událostí..

Závěrem lze konstatovat, že za zdravý vývoj integrovaných elektronických systémů v průmyslu komerční bezpečnosti lze považovat řešení složitých technologických celků s rozptýlenou inteligencí, v jednotlivých podsystémech propojenou za pomoci komunikačních prostředků do monitorovacího a řídicího centra.

1 CÍL PRÁCE A METODIKA

Cílem této práce bude v první řadě popsat všeobecné požadavky integrovaných elektronických systémů. V této části se zaměřuji na popis a charakteristiku všeobecných částí a na celkovou orientaci systému vzhledem k technickým možnostem dnešní doby. Poukázáním na dnešní neúplnou normalizaci a rozebráním jednotlivých struktur chci ukázat směr pro výrobce těchto systémů. V závěru této části popisuji všeobecné zásady, které mohou být výhodou při návrhu systému, projektu, montáži a následném servisu včetně modernizace, pro koncového uživatele.

V druhé části se zabývám současnými poplachovými systémy, které umožňují integraci. Rozeberu vlastnosti a vhodnost použití ve struktuře integrace. V úvodu této části se vrátím ke snaze výrobců prosadit se za každou cenu na trhu, aniž by upozornili na případné negativní vlivy jejich počínání. Dále v popisu jednotlivých systémů se snažím najít to nejzajímavější a přitom skutečné, pro vytvoření náhledu na systém jako celek. Jednotlivé unikáty, které v této pasáži uvádím, jako jsou například systém snímání hoření detektor O²T nebo systém proměnného kódu karty, poukazují na další vývoj těchto systémů.

Třetí část ukazuje, jak složitý pojem je „inteligentní budova“ v dnešním světě jednotlivých profesí. Dále se zaměřuji na vzájemnou komunikaci a kompatibilitu jednotlivých částí integrovaného systému na prahu komunikačního formátu. Poukazuji, že systémová integrace není rozhodně dílem jednoho člověka, ale týmu odborníků v čele se systémovým integrátorem. V závěru nahlížím do okénka budoucnosti, které řeší plnou integraci tj. spojení poplachových i nepoplachových systémů, vzájemnou kompatibilitu a jednoduchost uživatelského rozhraní.

Čtvrtá část je věnovaná skutečnému návrhu integrovaného elektronického systému v průmyslu komerční bezpečnosti.

Závěrem nesmí chybět seznam použité literatury se slovníčkem použitých zkratk.

2 KONCEPCE INTEGROVANÉHO ELEKTRONICKÉHO SYSTÉMU

2.1 VŠEOBECNÉ POŽADAVKY DLE ČSN EN 50 398

Podání informací o všeobecných požadavcích jsem pojal formou, která je v souladu s realitou připravované normy pro kombinované a integrované systémy. Informace jsem získal od člena technické komise TC 79 AGA. Norma je daleko obsáhlejší, vybral jsem pouze pasáže pro získání povědomí o všeobecných požadavcích kombinovaných a integrovaných systémů.

2.1.1 Definice pojmů

Speciální vybavení - vybavení, které není popsáno v aplikační normě a které není nutné ke splnění funkcí požadovaných touto aplikační normou.

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

Poplachová aplikace - aplikace určená na ochranu života, majetku nebo prostředí

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

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

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 prostorech 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 řídicí zařízení (CCF) - zařízení používané k řízení anebo signalizaci ve struktuře (konfiguraci) typu 1, které je připojeno k jednomu nebo více jednoúčelovým systémům a které je normálně řízeno provozní obsluhou, například počítač v dozorovém pracovišti; ústřední řídicí zařízení je speciální vybavení (a není to běžná poplachová ústředna) pro alespoň jednu z aplikací.

Společné zařízení - zařízení sdílené jednou nebo více aplikací.

Společné vybavení - vybavení sdílené jednou nebo více aplikací.

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.

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 určeny především k ochraně života, majetku a prostředí:

- 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.

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).

2.1.2 Normativní odkazy

Skupina norem pro zabezpečovací signalizaci (EZS)

ČSN EN 50 130 – Poplachové systémy, všeobecné požadavky.

Předmět normy : Řeší požadavky na odolnost pro komponenty poplachových systémů, určených pro použití uvnitř a v okolí budov v prostředích obytných, obchodních a průmyslových. Tato norma nespecifikuje požadavky na základní bezpečnost, jako je ochrana před úrazy el. proudem, provoz v nebezpečném prostředí, izolační pevnost a související zkoušky na elektrickou pevnost.

ČSN EN 50131 – Elektrická zabezpečovací signalizace

Předmět normy : Konkrétně popisuje čtyři stupně zabezpečení a čtyři třídy vlivu prostředí. Popisuje sestavování zabezpečovacích systémů. Norma je určena jako vodítko pro pojišťovací společnosti, dodavatele EZS, uživatele a policii při stanovování kompletní a přesné specifikace ochrany pro konkrétní objekty. Neurčuje však druh zabezpečovacího systému, rozsah nebo míru zabezpečení.

Skupina norem a vyhlášek pro požární signalizaci (EPS)

ČSN 73 08 02 – Požární bezpečnost staveb.

ČSN 730875 – Navrhování elektrické požární signalizace.

Vyhláška 246/2001 Sb. – Stanovení podmínek požární bezpečnosti u výkonu státního požárního dozoru.

ČSN EN 54 – část 1 - 7, 10 – 15 Elektrická požární signalizace.

Předmět normy : Stanovuje základní předpisy a technické požadavky pro zařízení EPS. Lze ji také použít jako základ hodnocení komponentů systémů pro jiné určení. Určuje požadavky, zkušební metody a kritéria provedení, na jejichž základě je možno hodnotit účinnost a spolehlivost komponentů systémů EPS. Norma nepokrývá možné požadavky na autonomní požární signalizaci.

Skupina norem pro uzavřené televizní okruhy (CCTV)

ČSN EN 50 132 – Sledovací systémy.

Předmět normy : Obsahuje základní předpisy a požadavky pro uzavřené televizní okruhy. Rozebírá jednotlivé části a spojení těchto částí do uzavřeného celku. V aplikační části 7 návrh, způsob a montáž instalace v aplikacích.

Skupina norem pro kontrolu vstupů (ACCES)

ČSN EN 50 133 – Systémy kontroly vstupů.

Předmět normy : Definuje požadavky na automatizované systémy kontroly vstupů a komponenty uvnitř a vně budov. Zahrnuje systémovou architekturu, funkční požadavky, požadavky na komunikaci kontroly vstupů s ostatními systémy, definice podmínek okolního prostředí a elektromagnetické kompatibility. Tato norma se nezabývá ovládacími prvky a senzory.

Skupina norem pro systém přivolání pomoci (SAS)

ČSN EN 50 134 – Systémy přivolání pomoci.

Předmět normy : Norma obsahuje doporučení poskytovatelům služeb (a jejich subdodavatelům) pro efektivní a účinnou řídicí politiku a postupy při instalaci, testování, obsluze a údržbě systémů přivolání pomoci, včetně technického vybavení a organizování pomoci.

Skupina norem pro poplachové přenosové systémy (ATS)

ČSN EN 50 136 – Poplachové přenosové systémy a zařízení.

Předmět normy : Účelem této normy je stanovit znaky provedení přenosových poplachových systémů, které používají poplachové přenosové cesty nebo vyhrazené poplachové cesty k zabezpečení jejich použitelnosti a kompatibility s různými druhy poplachových systémů (2).

Skupina norem pro kombinované a integrované systémy /dosud nevydána/

ČSN EN 50 398 – kombinované a integrované systémy.

Předmět normy : Norma uvádí požadavky na poplachové systémy, které jsou kombinované nebo integrované s jinými systémy, které mohou a nemusí být poplachovými systémy. Dále definuje požadavky týkající se pravidel integrace s cílem zdůraznit význam jednotlivých aplikačních poplachových norem a objasnit případné rozpory. Poplachové přenosové systémy nejsou zahrnuty do této normy (1).

2.1.3 Poplachové normy po našem vstupu do EU

Normy ČSN jsou z principu nezávazné. Závaznými se pro daný případ stávají na základě smluvního vztahu, například pojistné smlouvy uzavřené mezi pojistitelem a pojistníkem, případně smlouvy mezi dodavatelem (montážní firmou) a odběratelem. Česká republika jako členský stát EU postupně zavádí do národní legislativy evropské normy. Je možné zvolit různé formy zavedení (oznámením o vydání normy, vydáním normy v originále nebo vydáním překladem).

V EU je v oblasti norem pro poplachové systémy normotvorným orgánem CENELEC, technická komise TC 79. České zájmy v této technické komisi hájí AGA jako člen komise. Na půdě CENELEC vznikají evropské normy (EN), které pak jednotlivé státy začleňují do své legislativy. Není-li možné dosáhnout shody na obsahu EN, byl zvolen mezistupeň, nazvaný technická specifikace (TS). Evropské normy jsou pro členské státy EU závazné, národní normy nesmějí být s EN v rozporu. Technická specifikace není pro členské státy závazná, je však v zájmu členských států se jí řídit.

Technické normalizační informace (TNI) slouží k podrobnějšímu popisu jednotlivých fází zřizování poplachového systému. Například k normě ČSN CLC/TS 50131-7 budou v průběhu tohoto roku vydány tři TNI: - návrh a projekt, instalace a revize.

Postupně vydávané produktové normy budou zaváděny jako ČSN. V okamžiku jejich vydání budou zpravidla zrušeny příslušné kapitoly národní přílohy Z1. Je také možné ponechat v platnosti i odpovídající kapitolu národní přílohy, je-li to účelné. V takovém případě je nutné na to v úvodu ČSN/CLC TS xxxx upozornit.

Vydáním normy ČSN CLC/TS 50131-7 dojde ke zrušení kapitoly NS národní přílohy Z1. Řada článků této normy však neposkytuje dostatečně podrobný návod na postup činností v rámci jednotlivých etap. Rovněž neobsahuje odkazy na národní legislativu spojenou s projektováním v investiční výstavbě, projektováním elektrických zařízení a s revizemi elektrických zařízení. Tyto doplňující informace jsou vydány formou Technických normalizačních informací k ČSN CLC/TS 50131-7 vydaných spolu s touto normou pod označením TNI 334590-1 Návrh systémů EZS, TNI 334590-2 Montáž systémů EZS a TNI 334590-3 Zkoušky po montáži a revize systémů EZS (3).

2.1.4 Základní typy struktur

Jsou specifikovány tři typy struktur (konfigurace):

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

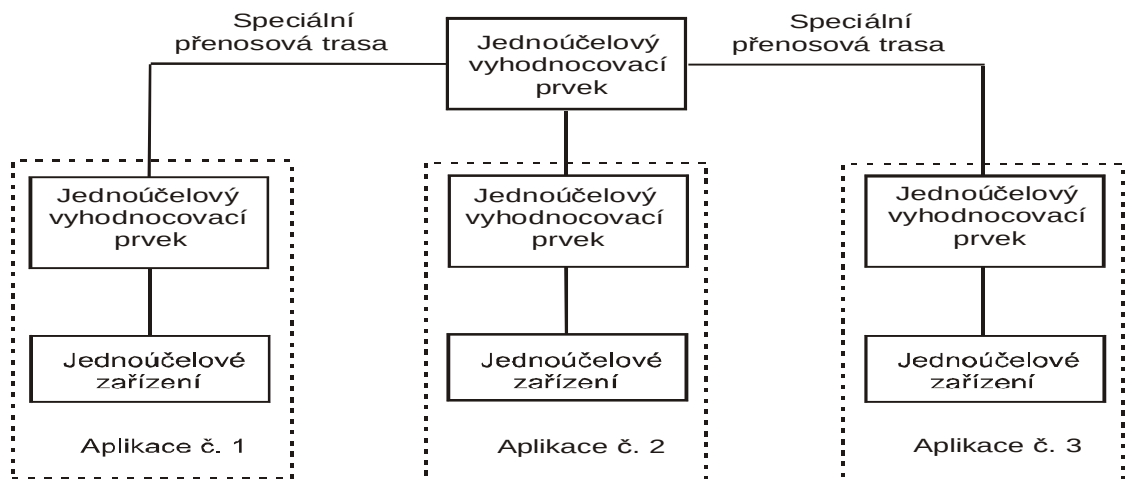
Typ 2A: Struktura je vhodná pro kombinaci a integraci normalizovaných poplachových systémů a nepoplachových systémů používajících společných přenosových tras, společných zařízení a společných vybavení. Jediná porucha v jedné aplikaci nemá žádný nepříznivý vliv na další poplachovou aplikaci.

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.

Ad Typ 1

Struktura typu 1 je kombinace dvou nebo více jednoúčelových systémů. Tyto systémy jsou připojeny ke společným dalším zařízením, například propojením 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 dalším jednoúčelovým systémem nebo žádným zvláštním vybavením.



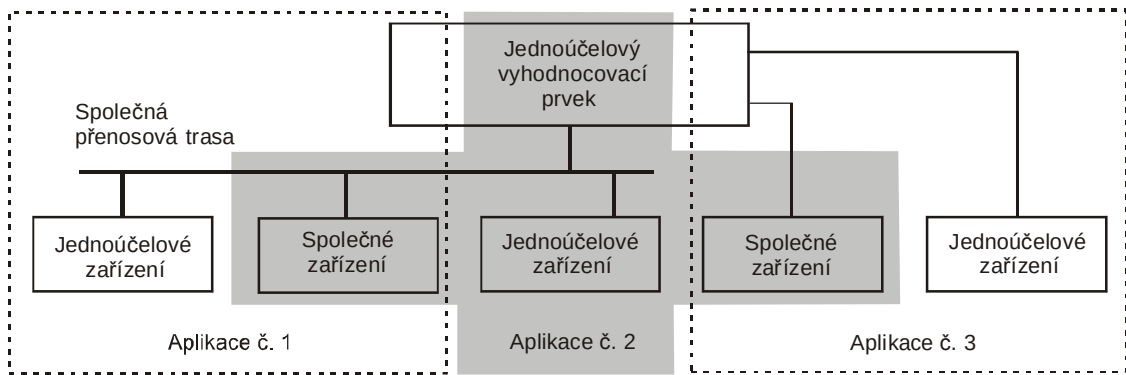
Obr. 1. Příklad struktury typu 1

Ad Typ 2

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

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.



Obr. 2. Příklad struktury typu 2

2.1.5 Obecný návrh (projekt)

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 řídicího zařízení do dalších částí aplikace. Příkladem je použití systému EZS k zapnutí záznamu vybraných kamer systému CCTV při vstupu do prostoru oprávněnou osobou.

Ve snaze zabránit povelovému vybavení a uvedení do činnosti, které by se mohlo škodlivě projevit účinností na bezpečnost správy v chráněných objektů a jejich osazenstva se doporučuje následující plán a postup realizace:

- V průběhu projektu systému by měly zainteresované strany definovat provozní podmínky pro celý integrovaný systém a zvláště povelové vybavení, které by pravděpodobně bylo požadováno.
- Vliv (dopad) nesprávného provozu povelového vybavení by měl být posouzen během projektu systému, jestliže možný nesprávný provoz by mohl mít vážný dopad na bezpečnost nebo zabezpečení, kdy by vybavení bylo jednak nefunkční nebo jeho funkce byla předdefinována k překonání této možnosti.

2.1.6 Zásady propojení

Pokud zařízení, které nemusí splňovat jednu nebo více aplikačních norem, jsou připojena k zařízením splňující požadavky norem, musí být použity následující zásady.

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.

2.1.7 Současný výskyt událostí a její priority

Systém musí být navržen tak, aby současný výskyt událostí každého typu v případě více než jedné aplikace neohrozil kompletnost žádné z aplikací. Požadavky na časování musí být v souladu s těmito podmínkami.

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 z 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.

V některých případech může být dříve uvedený postup nevhodný a současná přítomnost více zpráv než jednoho typu může vést k zobrazení jiné priority.

Všeobecné požadavky na signalizaci priorit jsou následující:

- musí být signalizovány všechny existující poplachy a postupně mohou být zobrazovány
- kromě aktuálně zobrazovaných informací 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

- žádná funkce jakékoliv aplikace nesmí bránit signalizaci poplachu.

2.1.8 Centrální řídicí zařízení

Povelové signály v integrovaném systému mohou být přenášeny z jedné aplikace do jiné nebo z ústředního (centrálního) řídicího zařízení do jiných částí aplikace. Jako příklad lze uvést dálkové vypínání senzorů v aplikacích. Použití povelových signálů může být užitečné ke správě velkých budov a komplexu budov, ale pokud je takové vybavení nesprávně aplikováno, tak může snižovat účinnost zabezpečení a bezpečnost osob.

Klasifikační třída 1

Centrální řídicí zařízení je použito pouze k zobrazování informací v prostorách, kde provozní obsluha dohlíží nad systémem. Normalizované signalizační zařízení (ústředny EZS nebo signalizační panely atd.) jsou také umístěny ve stejných prostorách.

Klasifikační třída 2

Tato třída musí být aplikována tam, kde centrální řídicí zařízení je použito pouze k zobrazování informací a je to jediný informační displej v prostoru, kde provozní obsluha dohlíží nad systémem.

Centrální řídicí zařízení :

- musí být jednoznačně rozlišeno (identifikováno) dle předcházející klasifikace
- musí být umístěno v prostředí dle specifikace výrobce zařízení
- musí být vyhrazeno jedině integrovanému systému.

2.1.9 Pokyny pro použití, montáž a servis

Specifikace

V prvé řadě by měl být vypracován výklad specifických požadavků návrhu (projektu) integrovaného systému. Podrobnosti uvedené ve specifikaci musí brát v úvahu komplexnost systému a mohou obsahovat informace alespoň o následujících aspektech:

- jednotlivé aplikace a požadavky na jejich vhodné provedení
- cíle k dosažení kombinace nebo integrace
- charakteristiky budovy, do které má být integrovaný systém namontován.

Smluvní závazky (odpovědnost)

Integrovaný systém dle definice obsahuje více než jedno zařízení a je pravděpodobné, že se některá zařízení mohou určitým stupněm vzájemně ovlivňovat. Pro usnadnění a k odstranění nepříznivých vzájemných vlivů dílčích zařízení se doporučuje vybrat jednoho hlavního dodavatele. Tento hlavní dodavatel by měl být schopný předat integrovaný systém zákazníkovi a vypracovat „Prohlášení o provedení předávacích zkoušek“ dle specifikace systému.

Hlavní dodavatel spoluodpovědný za návrh (projekt) by měl zajistit, že organizace odpovědná za návrh (projekt) má příslušné odborníky k uskutečnění zakázky. Při předávání systému by měl být hlavním dodavatelem zpracován plán zkoušek.

Montáž a propojení

Kde integrovaný systém sdílí společné vedení s více než jedním subsystémem, toto vedení by mělo splňovat odpovídající normy příslušné aplikace v nejvyšší kompletnosti a provedení

Ověření

Hlavní dodavatel by měl zákazníkovi poskytnout a seznámit ho s prohlášením o provedení předávacích zkoušek systému s tím, že montáž vyhovuje požadavkům specifikace a komponenty splňují příslušné výrobní normy.

Vedení provozní knihy

Měl by být zaveden systém záznamu a ukládání dat každé aplikace dle aplikačních norem. Zahájení systému záznamů by mělo začít od data, kdy je každá část integrovaného systému uvedena do provozu. Záznamy o všech preventivních zkouškách, revizích a opravách by měly být zaznamenány v provozní knize.

Modernizace a obměna systému

Před provedením změn nebo rozšíření systému by se měl vzít v úvahu jejich vliv na provedení stávajícího systému. Tyto změny, které byly provedeny, by měly být zapracovány do záznamů systému společně s podrobnými výsledky přezkoušení systému.

Bez předchozí dohody s organizací odpovědné za systém by dodavatelé nebo servisní organizace neměly provádět na systému žádné změny. Kde jsou provedeny změny komponentů nebo rozsah aplikací integrovaného systému po jeho schválení, organizace odpovědná za systém by měla zajistit zkoušky systému a ověření, že provedené změny jsou v souladu s danou specifikací.

Zkoušky systému

Dle plánu zkoušek by měly být hlavním dodavatelem provedeny pravidelné zkoušky a výsledky zaznamenány v provozní knize.

Systém údržby

Organizace odpovědná za integrovaný systém by měla zajistit, že příslušná údržba systému bude prováděna kvalifikovanými osobami. Při údržbě těchto aplikací by měla být prosazována vzájemná spolupráce a koordinovaný přístup. Všechny osoby provádějící servisní práce na systému by měly být plně obeznámeny s funkcí a provozem systému, na kterém pracují a jejich vliv na provedení a kompletnost ostatních aplikací. Hlavní dodavatel by měl uvést, jestli je každý speciální servisní postup nezbytný k zajištění pokračování uspokojivého provozu integrovaného systému.

Dokumentace a školení

Dokumentace kombinovaného a integrovaného poplachového systému musí být stručná, úplná a jednoznačná. Poskytované informace musí být dostatečné pro montáž, zahájení provozu, vlastní provoz a servis systému. Požadavky na dokumentaci specifikované v každé příslušné normě každé aplikace musí být v souladu s touto aplikací. K dispozici by měly být školící manuály, které jasně stanovují vlastní postupy operátorů systému. Operátoři systému by měly být na systém odpovídajícím způsobem vyškoleni a jejich znalosti by měly být pravidelně přezkušovány (1).

3 SOUČASNÉ POPLACHOVÉ SYSTÉMY UMOŽŇUJÍCÍ INTEGRACI V PKB

V této pasáži čerpám zejména ze svých zkušeností, servisního a později revizního technika poplachových systémů, protože veškeré instalační manuály popisující problematiku zapojení a programování tedy funkčních částí integrace poplachových systémů, jsou vždy mozem technika a know - how výrobního závodu.

Rozdělení systémů dle poplachových norem určující řadou ČSN EN 50 13x a souborem EN 54 je pro členění přehledné, ale pro tuto práci jsem zvolil členění dle výrobce a typu.

3.1 Rozdělení systémů a trocha historie

Dnešní doba přináší velkou konkurenci v nabízených systémech a výrobci často integrují přímo v ústředně jednotlivé systémy. Příkladem je velmi častá kombinace poplachových systémů a to EZS a ACCES, EZS a ATS.

V průběhu své praxe jsem se setkal s vývojovou řadou uváděnou na trh s integrací EZS a ACCES, která byla v době uvedení na trh naprostým průlomem v technologiích poplachových systémů, ale později se ukázalo, že tato kombinace u daného typu zařízení je při osazení max. počtu prvků spíše nevýhodou. Systém ztrácel na akceschopnosti a pružnosti vzhledem k uživateli. Tyto systémy byly navrženy se sběrníci RS 485 pro prvky EZS a procesor byl optimalizován na data z koncentrátorů pro jednotlivé smyčky v úrovních viz. tabulka 1. Ovšem data z čtecích zařízení byla několikanásobně vyšší a na zpracování časově náročnější.

Tabulka 1. Vyhodnocení odporu smyčky ústředny

Odpor smyčky (Ω)	Stav
0 - 800	Sabotáž - zkrat
800 - 900	Nízký odpor
900 – 1200	Normální stav (zavřeno)
1200 – 1900	Vysoký odpor
1900 – 12000	Poplach (otevřeno)
12000 - ∞	Sabotáž – přerušení

Docházelo k velkým odezvám na ovládacím panelu i na všech výstupech systému zejména výstupech určeného pro ATS. V počátcích poplachových systémů využívajících k řízení ústředny procesor, se na trhu objevovalo velmi malé množství pultů centralizovaných ochran (PCO). PCO přijímaly velmi malou přenosovou rychlostí (10BPS /10 bitů za sec./ max. 20 BPS) a k přenosu informace z objektu využívaly analogovou telefonní linku. Tato komunikace se ukázala vhodná pouze pro zařízení instalované v objektech s nižším stupněm zabezpečení a malým počtem prvků. Dalším vývojem se zejména u objektů s vyšším stupněm zabezpečení / muzea, banky, pošty atd. / musely volit ústředny bez vestavěné integrace se samostatným ATS zařízením. Osazovaly se výstupními moduly, které převáděly systémový formát dat na otevřený komunikační formát (RS 232, 485) vhodný pro další zpracování. Začaly se objevovat bezdrátové přenosy ATS (RADOM, FAUTOR, NAM), ovšem ne všechny měly stejné parametry. Svými přednostmi a vhodnou strategií managementu se nejvíce rozšířil přenos pro objekty s vyšším stupněm zabezpečení typ FAUTOR. Jeho předností je oboustranná komunikace od PCO až po koncový hlídáný objekt. Tato technologie přetrvává až dodnes.

3.2 NOVAR

Novar GmbH je společnost zabývající se vývojem, výrobou a prodejem velmi kvalitních poplachových systémů. Vyznačuje se velmi širokou produktovou řadou. Prakticky všechny nabízené systémy jsou vhodné pro integraci.

3.2.1 EZS

Ústředna

Pro ochranu života a zdraví osob a majetku byl navržen systém elektronické zabezpečovací signalizace ESSER 561 MB/HB. Jedná se o modulární mikroprocesorové řídicí a vyhodnocovací zařízení, které svojí konstrukcí a možností připojení rozličných prvků zaručuje efektivní ochranu.

Velikost skříně určená konfigurací ústředny v návaznosti na kapacitě použitých náhradních zdrojů je navržena podle požadavků zákazníka. Pro zobrazování stavu a ovládání systému jsou použity LCD klávesnice s displejem 2x40 znaků, grafické displeje ¼ VGA nebo barevný dotykový displej. Pro ovládání systému se preferuje používání

spínacích zařízení IK2 nebo IK3, což je moderní bezkontaktní systém používající dynamické přepisovatelné bezkontaktní médium. Ústředny lze vybavit také interní nebo externí tiskárnou, na kterou lze podle nastavení a potřeby zapisovat požadované informace.

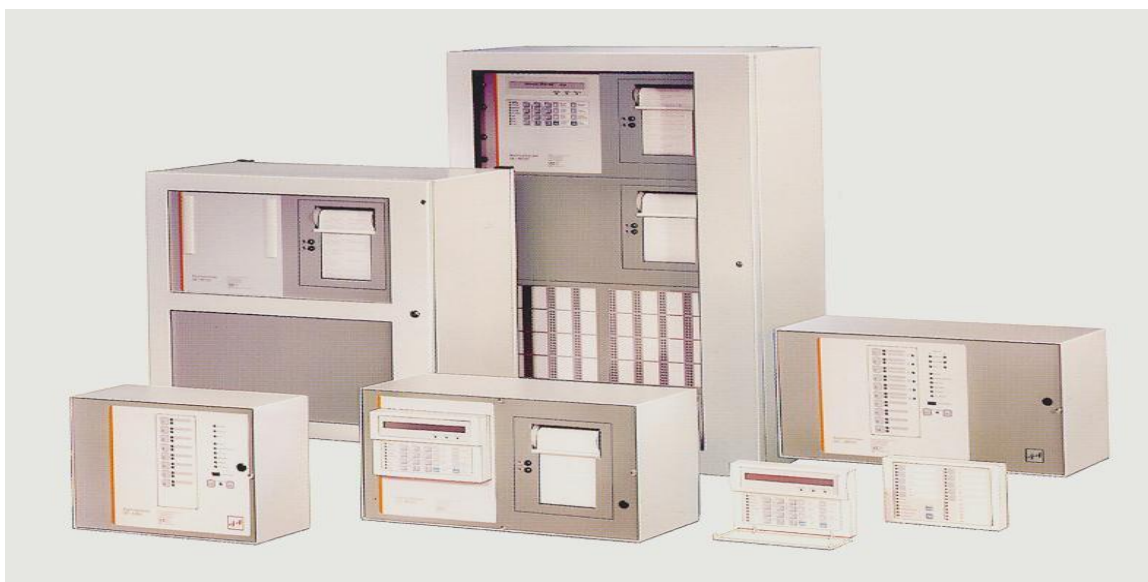
MB100

Modulární zabezpečovací ústředna nové generace pro střední a větší objekty, disponující podle konfigurace až 9 sběrnicemi BUS1 o celkové kapacitě 567 adres a 8 sběrnicemi BUS 2 o celkové kapacitě 512 adres. Adresné prvky a jednotlivé vstupy těchto prvků je možné rozdělit do 512 skupin a ty je možné přiřadit do 16 hlavních a 48 podřízených oblastí. Tento model ústředny umožňuje připojení do sítě IGIS LOOP.

V krytu ústředny jsou také umístěny dva akumulátory s kapacitou maximálně 2x 65Ah s impulsním napájecím zdrojem 230V AC/13,8V DC. Napájecí zdroje je možné typově zvolit v řadě 17-130Ah podle zvolených typů akumulátorů.

MB256

Modulární zabezpečovací ústředna pro větší a největší objekty, disponující podle konfigurace až 40 sběrnicemi BUS1 o celkové kapacitě 2520 adres a 10 sběrnicemi BUS 2 o celkové kapacitě 640 adres. Adresné prvky a jednotlivé vstupy těchto prvků je možné rozdělit do 2048 skupin a ty je možné přiřadit do 256 hlavních oblastí. Tento model umožňuje připojení do sítě IGIS LOOP.



Obr. 3. Ústředny EZS Novar

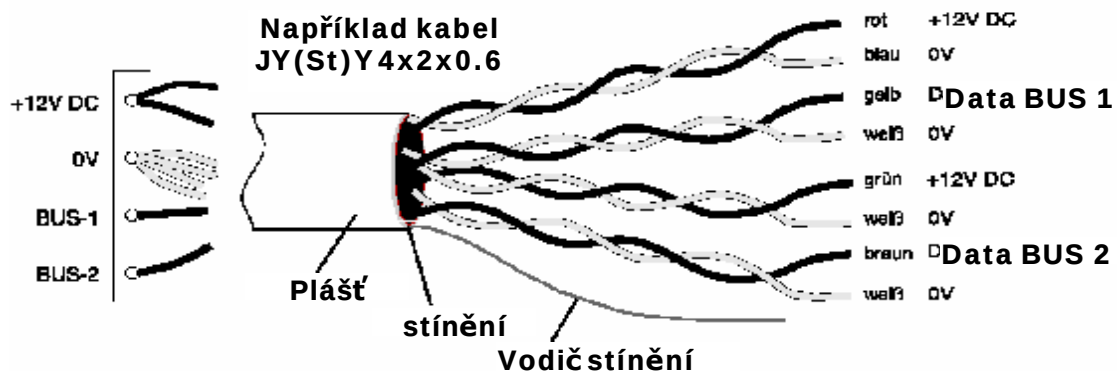
IGIS LOOP a Winmag

Propojení jednotlivých ústředn systémů EZS v objektu nebo objektech pomocí speciální kruhové integrující datové linky nazvané IGIS LOOP umožňuje zobrazovat stav a ovládat celý systém pomocí centrální řídicí jednotky Winmag, který slouží k zobrazení a ovládání i ostatních systémů např. EPS, KVS, CCTV, MAR..., a umožňuje vytvářet mezi těmito systémy vazby.

Konfigurace centrální řídicí jednotky probíhá pomocí importu dat získaných přímo z konfiguračních programů pro jednotlivé systémy (Winfem, TOOLS 8000, MultiAccess pro Windows atd.), tímto je velice usnadněna práce při umisťování symbolů pro jednotlivé prvky na plochu obrazovky.

Sběrnice

Připojení jednotlivých komponentů je realizováno 3-drátovými sběrnicemi BUS1 a BUS2. Sběrnice s možností libovolného větvení umožňuje připojení až 64 individuálně adresných inteligentních prvků do vzdálenosti 1000m. Vzhledem k nízkému odběru lze všechny prvky připojené ke sběrnici ze sběrnice také napájet, což přináší velké zjednodušení montáže i kabeláže. Z těchto vlastností vyplývají také další možnosti snadného rozšíření. Pro zvýšení bezpečnosti vedení lze použít kruhovou topologii sběrnice BUS2, která vylučuje možnost ztráty komunikace s prvky při přerušení nebo zkratu na sběrnici.



Obr. 4. Zapojení kabelu sběrnice BUS 1, BUS 2

Prvky sběrnice BUS1

Inteligentní prostorová čidla se zrcadlovou optikou SCM 2000 nebo SCM 3000 rozšířená o systém antimasking, který monitoruje zakrytí hlásiče v době, kdy je systém v denním režimu. Citlivost a dosah hlásiče se dá nastavit pomocí konfiguračního SW ústředěn Winfem.

Systém IDENTLOC slouží jako moderní náhrada magnetických kontaktů využívající bezdrátového přenosu kódovaných informací na krátkou vzdálenost. Do řídicí jednotky připojené na sběrnici lze připojit až 4 čidla IDENTLOC různých provedení. Kromě základní varianty kontroly otevření dveří, oken atd. lze použít kombinované varianty, kdy je pohyblivá část vybavena detektorem hlídajícím jak otevření tak rozbití okna nebo dveří. Lze použít také variantu velice tenkého čidla (5mm) určeného pro skrytou montáž a monitorování zavření a zamčení oken a dveří (mechanické zajištění klikou).

Pro připojení bezdrátových prvků lze použít multifunkční komunikační modul umožňující připojení až 5 bezdrátových prvků, klávesnic, prostorových čidel, připojovacích modulů a tísňových tlačítek.

Na sběrnici BUS1 je možné připojit i další prvky jako jsou tísňová tlačítka, detektory tříštění skla, vnitřní sirény, vnitřní optické signalizace, připojovací moduly, spínací reléové moduly a patice pro požární hlásiče.

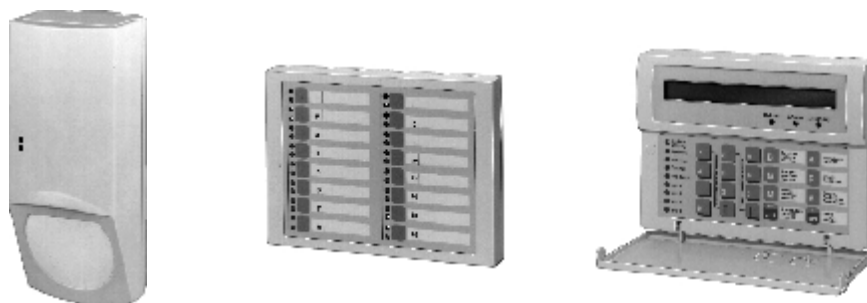


Obr. 5. Prvky pro sběrnici BUS 1

Prvky sběrnice BUS2

Zobrazení a ovládání je zajištěno pomocí 2x40 znaků LCD klávesnice, ¼ VGA displeje nebo barevného dotykového displeje. Pro ovládání jednotlivých oblastí a podoblastí systému je optimální použití externích spínacích zařízení IK2 nebo IK3 popsaných níže. Na sběrnici BUS2 lze také připojit prostorová čidla SCM 3000 s antimaskingem, panel

zobrazující stav až 64 skupin, moduly 5 vstupů, moduly 5 výstupů a 3vstupy/3výstupy mini-moduly charakteristické svými malými rozměry (40x18x13mm).



Obr. 6. Prvky pro sběrnici BUS 2

IK 2,3

Ovládání jednotlivých částí systému je realizováno pomocí externích spínacích zařízení IK 2,3. Jedná se o bezkontaktní snímače karet připojené pomocí modulů ke sběrnici BUS2. S těmito zařízeními je také možné ovládat uvolňovače dveří a zastoupit tak systém kontroly vstupu. Vyšší bezpečnosti lze dosáhnout použitím snímačů s klávesnicí, což umožní ovládání nejen kartou, ale také kódem.

Snímače IK3 používají v tomto oboru jedinečnou technologii proměnného kódu karty tak že při každém přiložení karty ke snímači dochází ke změně proměnného kódu, čímž je vyloučena možnost vyrobit funkční duplicitní kartu.



Obr. 7. Ovládací bezkontaktní místa IK 2,3

Prostorová čidla SCM

Inteligentní PIR hlásiče řady SCM se zrcadlovou optikou nabízejí možnost přímého připojení na sběrnici BUS1 nebo Bus2 podle typu. Hlásiče SCM 3000 jsou navíc vybaveny systémem antimasking, který monitoruje zakrytí hlásiče v době, kdy je systém v denním režimu. Citlivost a dosah hlásiče se dají nastavit pomocí konfiguračního SW ústředny Winfem.

3.2.2 EPS

Systém EPS 8000 obsahuje jednotnou rodinu ústředny 8000C (max. 254 hlásičů a OPPO), 8000M (max. 635 hlásičů a OPPO nebo 889 hlásičů bez OPPO), 8007 (max. 508 hlásičů a OPPO) a 8008 (max. 5.080 hlásičů a OPPO). Každá ústředna má možnost volby 9.999 SW virtuálních skupin (zón) pro hlásiče a 9.999 SW virtuálních skupin (zón) pro výstupní relé. Jednotlivé fyzické prvky (hlásiče, technické moduly, vstupní moduly, relé apod.) je možno do těchto skupin volně sdružovat a realizovat různé akční vazby mezi nimi. Všechny ústředny mají jednotný obslužný díl buď s LCD displejem 8x40 znaků, nebo ¼ VGA grafickým displejem s českým prostředím, který také obsahuje normální a soft-key klávesy pro ovládání systému. Vedle displeje je možné integrovat přímo do obslužného dílu stavový LED ukazatel až pro 192 SW skupin hlásičů a relé.

Dále ústředny obsahují pozice pro tzv. mikromoduly. Jsou to karty s elektronikou jednotných mechanických rozměrů, které určují HW výstavbu a kapacitu ústředny směrem k externímu prostředí (počet hlásičů, typ topologie vedení pro hlásiče, síťování ústředny, počet externích PC nebo jiných přístrojů s datovou komunikací apod.). Ústředny 8000C a 8000M obsahují navíc standardně bez nutnosti použití mikromodulu jedno obousměrné datové rozhraní, které se většinou využívá pro integraci. Ústředny jsou vybaveny nouzovou redundancí pro případ defektu některé části, typ 8008 navíc kompletním HW zdvojením centrální řídicí jednotky CPU.

Pomocí mikromodulu essernet je možné ústředny řady 8000 spojit do sítě essernet s rychlostí buď 62,5 Kbaud nebo 512 Kbaud. Síť essernet používá z bezpečnostních důvodů kruhovou topologii s možností integrace ústředny EZS Novar. Je možné pro každou ústřednu SW určit, zda se bude chovat jako ústředna EPS, jako externí ovládací a zobrazovací terminál této sítě, popř. jako jejich kombinace. Dále je možno SW určit, se kterými ostatními ústřednami v této síti bude komunikovat, a v jakém postavení (ústředna

Essernet panel, ústředna master, ústředna slave). Tak je možno zabezpečit rozsáhlé komplexy, kde jednotlivé akční a funkční vazby mezi prvky (hlásiče, technické moduly, vstupní moduly, relé apod.) nejsou vázány na to, ke které ústředně je daný prvek připojen. Naopak v rámci jednoho komplexu, kde sídlí několik uživatelů, je možno tvořit na společné HW síti essernet SW oddělené množiny ústředěn, které komunikují jednak uvnitř dané subsítě, a pokud je to žádoucí tak i s ústřednami, které jsou nadřazeny těmto subsítím. Počet ústředěn sítě essernet může dosáhnout několika desítek.

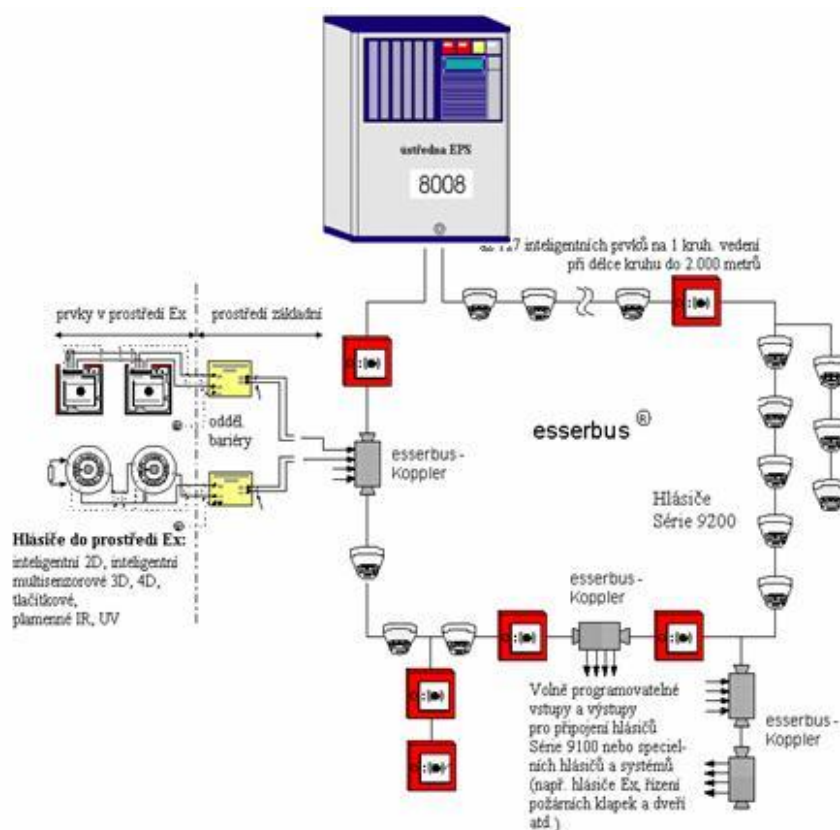


Obr. 8. Ústředny EPS Novar

Pro programování systémové řady 8000 je SW prvek TOOLS 8000. Je vytvořen na platformě Windows XP. Lze s ním provádět kompletní nastavení systému, které výrobce uvolnil pro instalační firmy. Je obrovským pomocníkem při uvádění systémů do provozu a počátečního programování. Má v sobě funkci PLAG and PLAY /samonačítání a rozpoznání/ pro prvky umístěné na kruhových vedení esserbus.

Pomocí mikromodulu esserbus se k ústředně připojují hlásiče a další inteligentní prvky. Topologie dvou vodičového vedení esserbus je kruhová s možností odboček bez použití dodatečné elektroniky. Vedení esserbus je odolné na zkrat či přerušení s celkovou délkou 2.000 metrů. Počet účastníků na tomto vedení je omezen normou VdS, popř. návrhem normy EN-54 a činí 127 individuálně adresných prvků. Jednotlivým prvkem může být automatický hlásič (optický, ionizační, tepelný, multisenzorový 3D, multisenzorový 4D, multisenzorový O2T), nasávací systém ARS 70, tlačítkový hlásič, technický modul (obsahuje 1 vstup a 1 výstup), koppler (existuje v provedení: 4 vstupy + 2 hlídaná relé, 12 relé, 32 proudových LED výstupů, 1 vstup), přičemž všechny tyto vstupní a výstupní elementy jsou volně SW programovatelné z TOOLS 8000. Základní filozofie celého

systému je postavena na technice necentrální inteligence. To znamená, že každý prvek tohoto vedení obsahuje svou vlastní inteligenci ve formě kompletního mikropočítače a navíc má velmi nízký proudový odběr (např. odběr každého hlásiče činí pouze ca. 0,04 mA). Jednotlivé prvky činí svá vlastní rozhodnutí samostatně, bez nutnosti spojení se s procesorem ústředny, jak je tomu u většiny dnešních systémů.



Obr. 9. ESSER BUS

Naprostou průlomovou technologií je multisenzorový hlásič O²T obsahuje dva optické senzory s rozdílnou geometrií detekce a tepelný senzor. Díky tomu jsou částice, které vznikají při požáru, popř. látky, které požárem nejsou, skenovány a změřeny prostorově, a to na základě dvou fyzikálně různých způsobů odrazu světla na částicích. Na základě těchto informací je hlásič O²T schopen zjistit, jaké částice se v měřicí komoře nacházejí, a pomocí sofistikovaného SW určit, z čeho tyto částice pocházejí (jaký materiál hoří). Hlásič je schopen selektivně vytrdit látky, na které běžný hlásič reaguje jako na požár, ale které požárem nejsou (vodní pára, prach z dřevovýroby apod.), a naopak reaguje se stejně správnou konstantní citlivostí na všechny typy požárů (na tmavé i světlé kouře).

Nejlépe se hodí pro nasazení do objektu se střední a vysokou koncentrací hodnot. Především tam, kde je třeba počítat s intenzivními rušivými vlivy, jako např. pára ve velkokapacitních kuchyních a skladech papíru, prach ve výrobních závodech apod. Vyhrává vlastní inteligence hlásiče O²T proti falešným poplachům na celé čáře. Tím také ušetří provozovatel zbytečné a drahé zásahy hasičů.

Detektor O²T obsahuje dva kompletní optické hlásiče s rozdílnou geometrií detekce, jeden teplotní hlásič a vlastní inteligenci.



Obr. 10. Hlásič O²T

3.2.3 ACCES

Hlavním úkolem jednotky kontroly přístupu je přebírat elektronické signály získané snímači identifikačního média (čtečkami karet) a na základě informací uložených o médiu v paměti rozhodovat o uvolnění nebo naopak o zablokování ovládaného vstupu.

Terminál ACS8 je novým základním stavebním kamenem přístupových systémů Novar, který spolupracuje se všemi typy čteček karet tohoto výrobce, včetně bezdotykových. Jedná se o plně inteligentní řídicí jednotku pro kontrolu přístupu pro malé, střední a velké systémy až do tisíce dveří.

Řídicí jednotka ACS8 je řízena mikroprocesorem a díky dostatečné paměťové výstavbě disponuje schopností zcela samostatně rozhodovat o vstupu nebo vyhodnocovat příslušné reálné podněty (stav dveří, poplachové vstupy). Tato schopnost plně autonomního provozu je pro vstupní systém velice důležitá - ovládání vchodu není totiž závislé na stavu

centrální jednotky (počítače) nebo komunikačních linek mezi centrální a řídicí jednotkou (havárie, přetížení), navíc tato zmíněná technologie distribuované inteligence zvyšuje pružnost celého systému a snižuje riziko ztráty dat.

Jednotka ACS 8 může rozlišit následující způsoby identifikace:

- jen kartou - sejmutím údajů na průkazovém médiu
- jen kód - vložení personálního kódu nebo dveřního kódu
- karta a kód - před vložení karty je třeba zadat personální či dveřní kód
- karta nebo kód - vložení karty nebo zadání příslušného číselného kódu.

Software systému ACS8 lze ze serveru modernizovat.

Jednotku ACS8 lze připojit k nadřazenému počítači pomocí inteligentního řadiče několika způsoby, běžně RS 485 nebo Ethernet, typ rozhraní je volitelný.

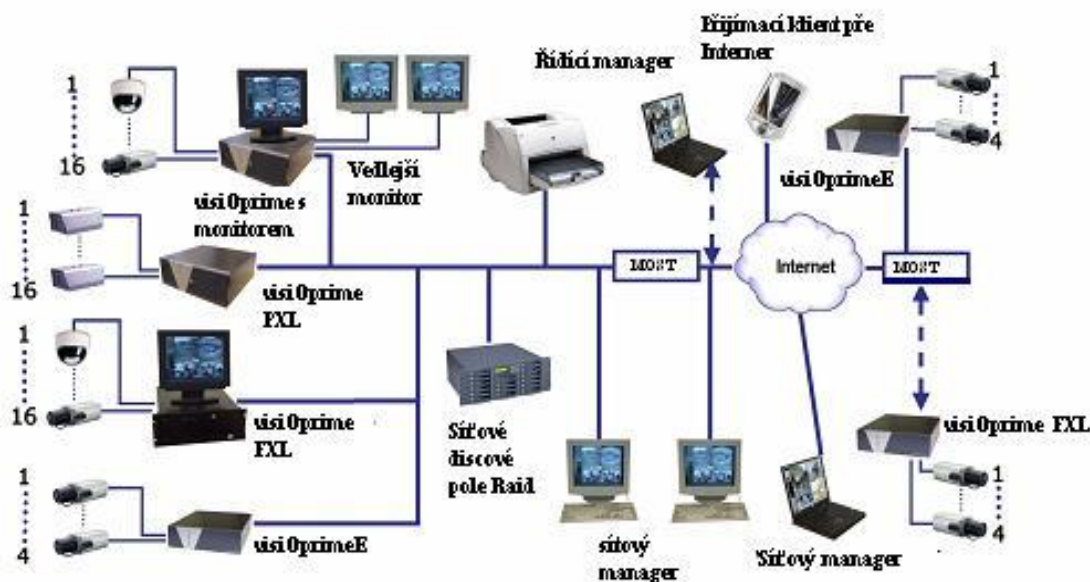


Obr. 11 ACCES Novar ACS 8

3.2.4 CCTV

Systém VisiOprime je kompletní produktový článek v CCTV. Nabízí kompletní řadu výrobků pro výstavbu rozsáhlého síťového video systému. Systém VisiOprime slouží k vytvoření, zaznamenání a dodání obrazu a zvuku. Tyto systémy používají software IVMS k vytvoření a přehrávání záznamů. Nahrávky lze sledovat s pomocí programu Repote Manager nebo sPlayer.

Pro integraci je zaručena naprostá kompatibilita s produktem řady WINMAG.



Obr. 12 CCTV Novar visiOprime

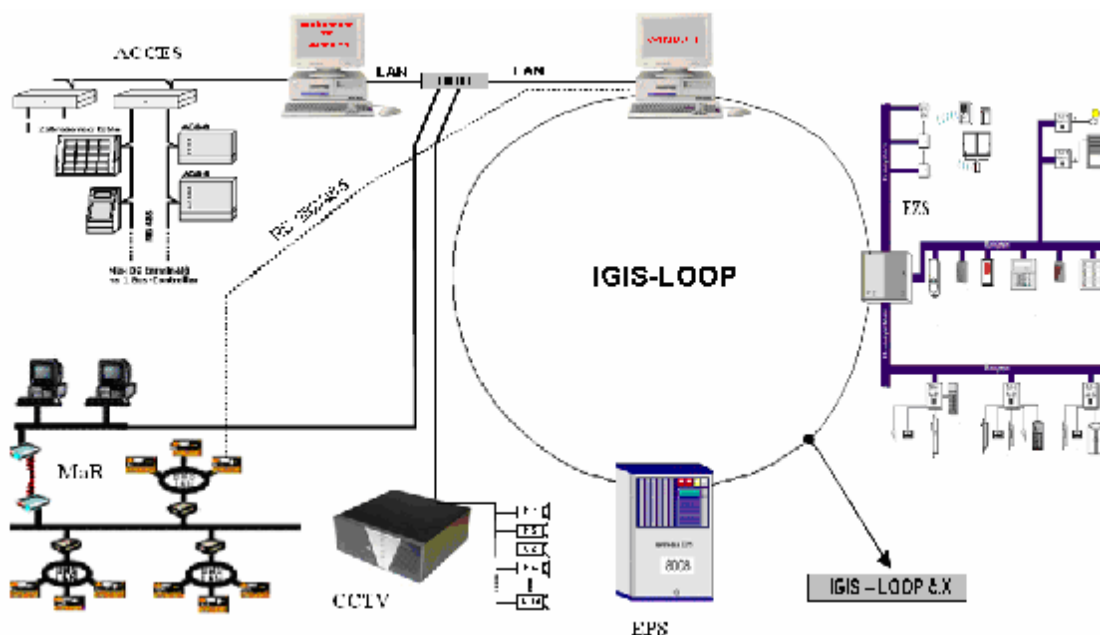
3.2.5 Centrální řídicí zařízení Winmag

Centrální řídicí jednotkou byl v koncernu Novar zvolen WINMAG. Svou koncepcí splňuje požadavky na monitorování a řízení objektů všech velikostí a nároků. Grafické znázornění umožňuje vytváření objektů, vnoření do různých úrovní a podúrovní zobrazení. Je umožněno vkládání digitalizovaných fotografií s označením aktivních a činných zón ovládání. Pomocí řídicího SW WINMAG lze realizovat komplexní správu poplachových i nepoplachových systémů budovy, je možno zobrazovat události, detekované pomocí textových zpráv a současně zobrazit stav a polohu prvků (čidel) v grafickém plánu budovy. Jednotlivé grafiky se přepínají automaticky dle přicházejících zpráv, nebo také ručně.

Z nadstavby je možné také celý komplex systémů ovládat, popřípadě simulovat stavy při revizní činnosti. Systém je naprosto otevřený pro programování v úrovni Supervisor. K programování slouží podpůrný prostředek Siasedit, který je součástí základního balíku. Monitorovací prostor je v systému WINMAG znázorněn půdorysnými plány a vloženými objekty. Na plánech a v objektech jsou rozmístěny symboly označující jednotlivé typy komponentů. Systém umožňuje definovat prakticky libovolné množství plánů, objektů a prvků.

Veškerá zařízení v systému WINMAG (hlásiče, izolátory, tlačítka, kopplery, detektory apod.) jsou reprezentována symboly. Tyto se rozmístí na mapách a v objektech dle skutečného stavu. Každý symbol umožňuje definovat a zobrazuje „chybová hlášení“ a ostatní požadované stavy díky plovoucímu atributu. Nastavitelné atributy mohou být: zvukový signál, priority poplachu, barva pozadí, flash atd.

Lze nastavit uživatelská práva k jednotlivým prvkům systému. Zprávy lze nastavit s nutností potvrzení, odsouhlasení, vložení komentáře. Systém umožňuje zobrazení krátkých informativních a přehledových zpráv. Veškeré nadefinované činnosti jsou průběžně ukládány na disk. Lze přesměrovat on-line tisk na výstupní zařízení dle výběru. Vše je chráněno systémem hesel proti neoprávněné manipulaci v úrovni technik a systémem hesel a přístupových práv v úrovni uživatel (4).



Obr. 13 Integrace s WINMAGEM

3.3 HONEYWELL

3.3.1 Integrace EZS a ACCES

Firma Honeywel přišla na trh s naprostou novinkou na letošní výstavě zabezpečovací techniky Pragoalarm 2005, s novou verzí ústředny GALAXY G3 v platformě G3 144 a G3 520. V tabulce 2 níže jsou uvedeny rozdíly v jednotlivých verzích.

Tabulka 2. Rozdíly Galaxy G3 144 a 520

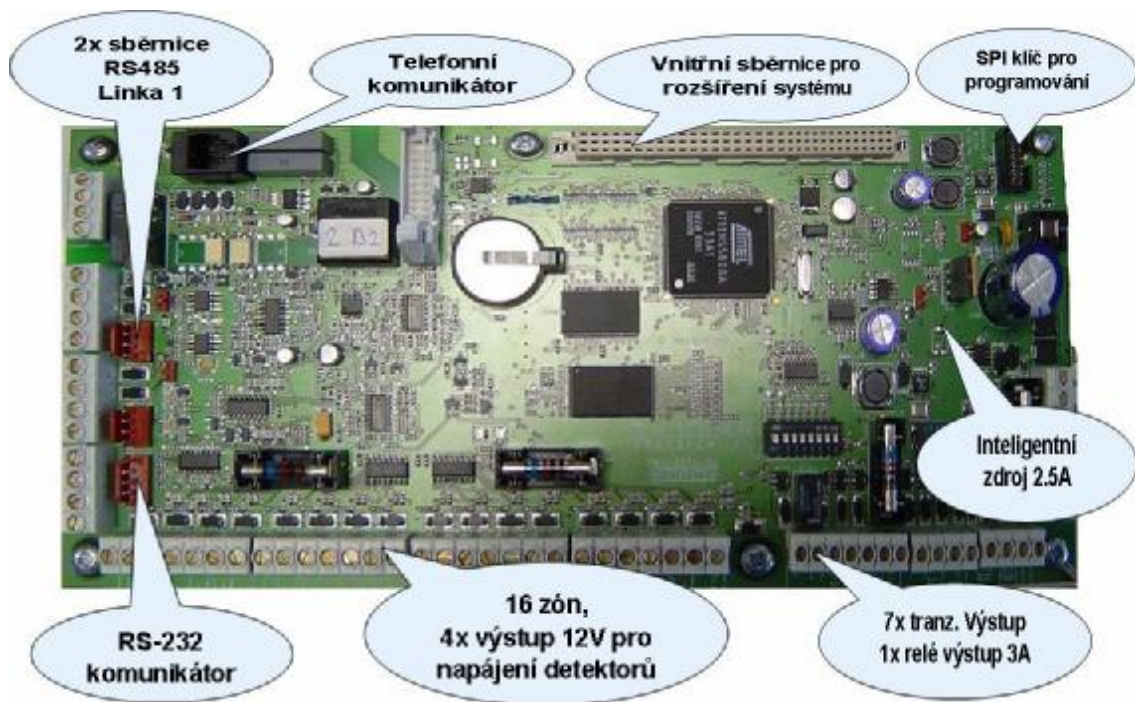
Hlavní části programu	Galaxy 3-144	Galaxy 3-520
Zóny	16 až 144	16 až 520
Výstupy	8 až 68	8 až 256
Uživatelé	250	999
Historie událostí	500	1.000
Grupy	8	32
Klávesnice	16	32
KeyProx	7	24
MAX	8	32
Typy zón	41	41
Typy výstupů	60	60
Spoje	128	255
Současná obsluha	8	16
Automat. zapnutí	20 časů zap/vyp (pro každou grupu)	20 časů zap/vyp (pro každou grupu)

Oproti dřívějším verzím je nový produkt postaven na zcela nové platformě, s integrací přímo na hlavní desce. Firmware již splňuje veškeré požadavky připravované revize normy ČSN EN 50131-1. SPY klíč zaručuje funkce přenosného paměťového média, kopírování a přepis konfigurace přímo v místě instalace bez možnosti použití PC, upgrade firmware.

Novou funkcí přibýlo sledování antimaskingu všech smyček čidel s touto vlastností, ukládání do historie, filtrování s možností upozornění obsluhy přímo na ovládacím panelu. Mezi další funkce, které se objevily s novou G3 je automatické záloha konfigurace, která je řízena vnitřním nastaveným režimem např. 1x měsíčně mezi 22.00 – 23.00, nebo vždy po

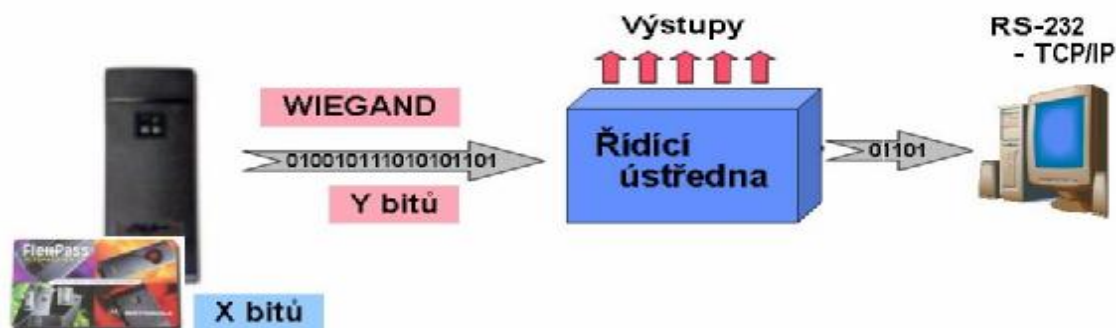
ukončení instalačního režimu, kde zálohuje pouze bloky ve kterých bylo provedeny změny nebo s dotazem ANO/NE při ukončení menu technika.

Výrobce tentokrát myslí i na budoucnost, pro kterou integroval do desky ústředny vnitřní sběrnici pro rozšíření systému, která mu umožní otevřenost komunikace přímo s procesorem.



Obr. 14 Nová podoba Galaxy G3

Systém ACCES je integrován přímo do ústředny. Výrobce se omezil na komunikační formát VIEGAND pro čtecí zařízení např. INDALA, HID, MIFARE, EM atd. Výhodou je použití jednotné databáze pro EZS a ACCES, společné přístupové body ovšem za cenu využití jednotné sběrnice. Nevýhodou je omezený počet přístupových kódů a omezený počet uživatelů.



Obr. 15 EKV GALAXY G3

3.3.2 Centrální řídicí zařízení ALViS

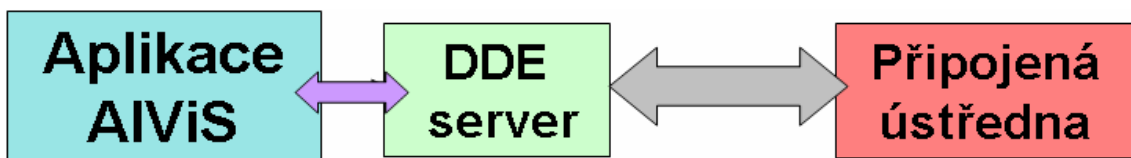
ALViS je určen pro monitorování a řízení poplachových a nepoplachových systémů. Je výsledkem dlouholetého vývoje, který se úročí velkým množstvím skutečných instalací. Použitím systému se zvyšuje rychlost a kvalita reakce obsluhy v mimořádných situacích, dále sjednocuje uživatelské rozhraní všech připojených autonomních systémů, přehledně zobrazuje stav i u velké a rozsáhlé instalace.

Monitorování aplikace je v systému reprezentováno mapami (plány) a symboly prvků. Plány zobrazují půdorysy sledovaných objektů, symboly na nich umístěné pak jednotlivé prvky poplachových i nepoplachových systémů.

Pro každý stav symbolu lze nastavit: chování (zvukový signál a flash), poplach (priorita zpracování a odbavení), výstupy (vzájemné vazby automatické i po potvrzení manuální), zápis do deníku událostí (bez možnosti zásahu z důvodu časových posloupností).

Grafická lokalizace místa události je řešena aktuálním zobrazením prvku v mapě ke které náleží, vždy s textovou zprávou v okně přehledů. Zprávu lze vybavit ještě zvukovou signalizací s podmínkou verifikace. Priorita a pořadí příchodu zprávy jsou rozhodujícími faktory pro zpracování. Poplachové zprávy jsou všechny uloženy do poplachového okna, kde dle barvy textu lze poznat zprávy potvrzené a nepotvrzené.

Architektura systému klient, server umožňuje distribuované rozdělení monitorovacího systému na více počítačů. Vzájemná komunikace je pomocí počítačové sítě (LAN, WAN, Internet.....). Server je přímá komunikační jednotka s jednotlivými systémy, klient je pouze zobrazovací a povelová jednotka. ALViS je vhodný pro použití ve větších aplikacích s několika stovkami až tisíci prvky, ale i pro aplikace menší řádově desítky prvků. Nemá žádné omezení na druh, typ ani způsob připojení monitorovacích zařízení.



Obr. 16 Struktura připojení ALViS

Systém hesel a přístupových práv poskytuje při realizaci instalace široké možnosti nastavení práv (pouze čtecí, potvrzení poplachu, ovládání zařízení, prohlížení událostí pro jednotlivé pracovníky obsluhy. Soubory s nastavením aplikace i komunikace mezi klienty a servery jsou šifrovány (5).

Tabulka 3. Vyvinuté DDE Servery k AlVisu

Typ zařízení (výrobce, ústředny)	Technologie
ARITECH , ATS CD 91/148,CD 95/150	EZS
ALARMCOM , Sintony	EZS
EUROPLEX , 3GS,Aplex 100/30, Midiplex	EZS
GENESIS , Genesis	EZS
MIKROTECH ,Galaxy	EZS
INNER RANGE , Concept	EZS
SATEL , CA - 64	EZS
SECURITON , SecuriPro	EZS, EPS
Spelza , Dominus	EZS
ZETTLER , Zetadress	EZS
ARITECH , FP 800, 900,1100,1200,1216,2000	EPS
ADEMCO , FCC 5000	EPS
ALARMCOM , Synova	EPS
CERBERUS , AlgoRex	EPS
ALTEK ,ANX 95E	EPS
NOVAR , kompletní řada 8000	EPS
KIDDE , Procyon	EPS
LITES , MHU 103,109,110,111	EPS
SCHRACK ,Compact,Maxima,Integral	EPS
ZETTLER ,Loop 500, Zetfas	EPS
ARITECH , ACS	ACCES
BIS , BIS	ACCES
LINEAR ,Linear	ACCES
COTAG ,Granta	ACCES
HONEYWELL ,Hub Pro	ACCES

3.4 SIEMENS

3.4.1 Integrace EZS a ACCES

Poplachová ústředna Sintony řady SI 4xx s dálkovým přenosem je konstruována modulárně.Veškeré komponenty jsou řízeny centrálou přes sběrnici E-BUS, která dále slouží k napájení účastníků a externích spotřebičů napětím. Ústředna se dá provozovat s min

jedním ovládacím LCD panelem s možností rozšíření až na 32. Lze také programovat kompletně celý systém přes tento panel. Kapacita smyček je 16 – 464 s kapacitou 500 uživatelů.

Ústředna je vhodná pro obchodní střediska, průmyslové komplexy a administrativní budovy. Má možnosti 16 podsystémů a 128 ovládacích skupin.

Umožňuje 3 úrovně podsystémů. Úroveň 1 jsou 4 skupiny, do kterých může být zařazen libovolný počet ze 16 podsystémů. Úroveň 2 je pro všech 16 podsystémů možnost být naprogramován jako hlavní, podřízený nebo virtuální. Úroveň 3 je 8 ovládacích skupin na podsystémy, které potom umožní až 16 nezávislých instalací. To znamená, že ústředny Sintony 4xx mohou být přizpůsobeny všem strukturám nebo všem organizačním požadavkům v chráněném objektu.



Obr. 17 Ústředna Sintony 410

Pro audio video verifikaci (dálkové ověřování poplachu) výrobce opatřil systém sběrnicí AUDIO - BUS a VIDEO – BUS. Na tyto sběrnice je možno připojit komponenty s možností záznamu obrazu a zvuku s následným přenosem na PCO pro audio a video zařízení. Funkce ověření poplachu přímo v čase.

Kombinace odposlechu a video záznamu v době poplachové informace je velmi potřebná pro pracovníky PCO, ke skutečnému zjištění události, než je uvedena do činnosti výjezdová skupina.

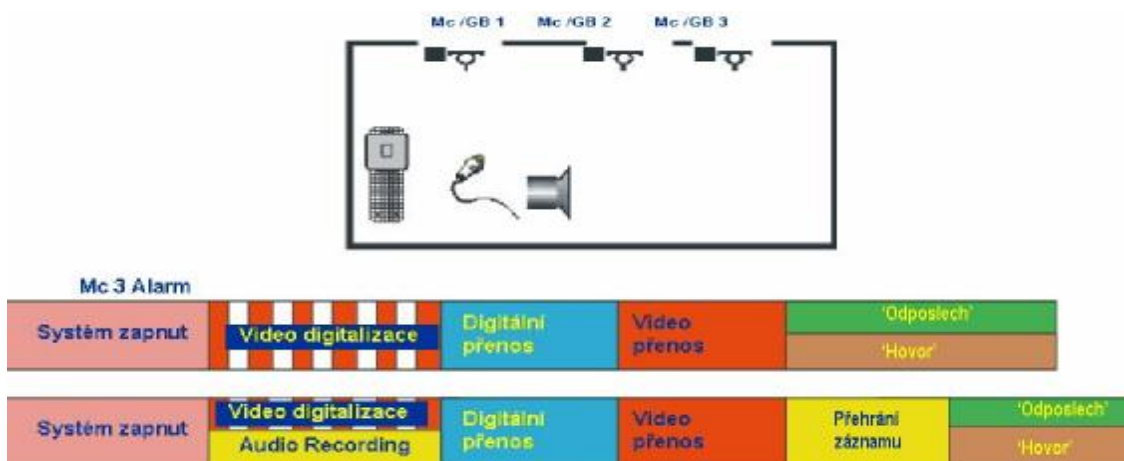
'Odposlech'



Dálková asistence



Obr. 18 Schéma audio komunikace na PCO



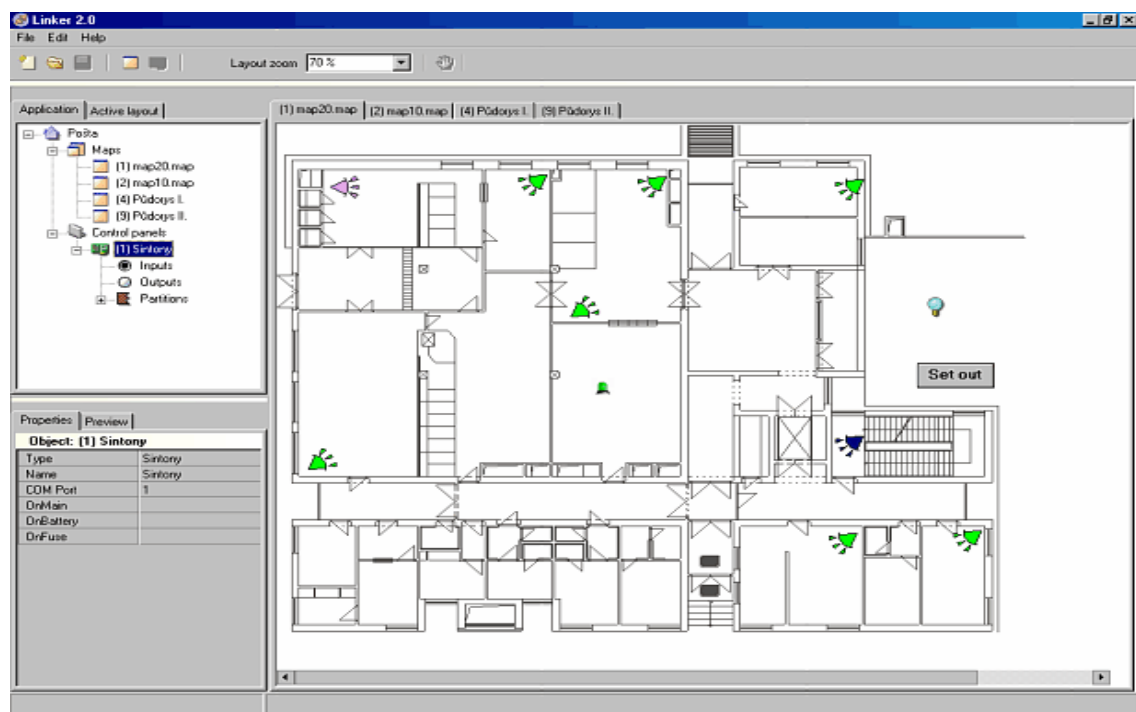
Obr. 19 Schéma video komunikace na PCO

3.4.2 Centrální řídicí zařízení MM 8000

Systém MM 8000 poskytuje bezpečné a řídicí pracoviště pro bezpečnostní aplikace, určené pro ochranu života, zdraví a majetku. Centrální dohled nad technologiemi snižuje náklady na provoz a údržbu. Ergonomická grafika uživatelského rozhraní zvyšuje bezpečnost daného objektu. MM 8000 zobrazuje jednotným a uživatelsky příjemným způsobem hlášení a informace od všech připojených systémů v pořadí bezpečnostní priority. Systém vede pomocí přednastavených postupů uživatele k nezbytným krokům, zásahovým plánům při vzniku krizové situace.

Systém využívá modulární architekturu, a proto nabízí uživateli cenově odstupňované řešení pro malé instalace až po složité komplexy tvořené jedním nebo více pracovišti. Úplná podpora všech cizích zařízení je zaručena naprostou otevřeností systému.

MM 8000 zaručuje excelentní koncepci ovládání, která prakticky vylučuje chyby operátorů. Unikátní uživatelský profil každého operátora zaručuje vstup do jasně definované oblasti s jasně definovanou zodpovědností (6),(17).



Obr. 20 Systém MM 8000

3.5 SPELZA

3.5.1 Integrace EZS a ACCES

Systém DOMINUS MILLENIUM je stavebnicový systém ústřední, linek a modulů pro stavbu zabezpečovacích systémů a integraci různých technologií v objektech o rozličné velikosti. Pro jednodušší aplikace je určena ústředna MU1, která je osazena vstupy

a výstupy přímo na základní desce systému a je rozšiřitelná pomocí nové sběrnice DN-BUS. Tento typ sběrnice umožňuje připojit na jednu linku různé typy modulů - panely, linkové moduly pro připojení čidel, snímače karet, zdroje apod., měnit přenosovou rychlost centrálně, identifikovat typy připojených modulů, programovat centrálně V/V zámky, to vše při udržení nízké ceny jednotlivých modulů. Ústředny MU2, MU3, MU4 mají rozšířené možnosti připojení spolupracujících zařízení přes sériové a paralelní porty.

Systém DOMINUS MILLENNIUM je produkt vycházející čistě z tuzemského prostředí. Vznikl na základě zkušeností v oblasti bezpečnostních systémů v předchozích letech a na základě požadavků, které souvisí s dynamickým rozvojem informačních technologií moderní doby.

Jedním ze zásadních požadavků uživatelů je plnohodnotná vazba mezi klasickou EZS a systémem ACCES, kde jsou kladeny vysoké nároky na jednoduchost obsluhy systému EZS prostřednictvím identifikačních karet. Toto DOMINUS MILLENNIUM řeší pomocí propojení modulů EZS a ACCES na společných komunikačních linkách DN-BUS a pomocí programu **ALFA** nabízí uživateli rozhraní pro konfiguraci vzájemných vazeb mezi povolením vstupu do střeženého prostoru a automatickým ovládáním podsystemů EZS. Program **ALFA** dále zajišťuje sběr dat ze systému o povolených či zakázaných průchodech a evidenci těchto informací. Doplnkovou nadstavbou tohoto programu je tzv. funkce „Recepce“, která umožňuje pro jednotlivé uživatele sledovat interaktivně přítomnost a nepřítomnost osob ve vybraných oblastech. .

Dalším nadstavbovým prvkem je pak systém pro kontrolu docházky, který lze do celého systému integrovat pomocí terminálů pro docházku tvořenými ve většině případů pomocí klávesnice s integrovanou čtečkou **MP1/PROX** sloužící pro různé typy odchodů, či průchodů a externí čtečkou **AY-X** připojenou do terminálu pro docházku. Těchto terminálů může být v systému instalováno až několik desítek a vytvořit tak nejen jednoduchý systém s jedním terminálem, ale i mohutný nástroj pro dohled pohybu osob ve střežených prostorech a evidenci docházky, kterou zpracovává program pod názvem **BETA**.



Obr. 21 Systém DOMINUS MILLENIUM

3.5.2 Domi Net

Systém umožňuje vzdálený centrální dohled objektů, osazených bezpečnostními ústřednami Dominus Millenium, které hlídají stavy jednotlivých detektorů. Monitorování je velmi flexibilní, protože pro komunikaci je využita síť Internet. Nezáleží zde na fyzické vzdálenosti jednotlivých objektů od dohledového pracoviště a dohled je možný prostřednictvím libovolného internetového prohlížeče (Internet Explorer, Netscape, ...) nebo prostřednictvím mobilního telefonu (protokolem WAP) --- připojením se k WWW serveru dohledového počítače. Systém lze využít i pro vzdálené ovládání ústředen na objektech (zastřežování / odstřežování prostor, rušení alarmů,...) a dokonce i ke vzdáleným změnám konfigurace ústředen. Obvyklý sortiment detektorů, které je možno hlídat, zahrnuje EPS (elektrická požární signalizace), EZS (elektrická zabezpečovací signalizace - soubor magnetických, prostorových a jiných detektorů), hlídání fyzikálních stavů (vlhkost, teplota, přepětí, podpětí, ...), klíčové hospodářství a další.

Dohledový software zvládne obsloužit prakticky neomezené množství připojených hlídaných objektů a stavů detektorů (nazývaných služby) na jednotlivých objektech.

Mezi vlastnosti dohledového software dále patří:

- přehledné textové zobrazení hlídaných služeb formou jednoduchých tabulek
- grafické zobrazení globální mapy s přehledem hlídaných objektů
- grafické zobrazení změn stavů jednotlivých služeb na časové ose
- procentuální vyhodnocení stavů a výpadků služeb (i ve formátu CSV)
- přístup k plné historii změn v systému
- práce se zvukovou signalizací vyhlášených alarmů a varování

Centrální dohledové pracoviště vyžaduje pouze zřízení serveru s operačním systémem Linux a jeho připojení k síti Internet. K přidání nového objektu k dohledu stačí připojit místní bezpečnostní ústřednu k sériovému portu místního počítače s operačním systémem Linux, který má trvalé připojení k síti Internet a který komunikuje s centrálním serverem. Objemy přenášených dat jsou zde zanedbatelné, což je jistě příznivé z ekonomického hlediska.

Monitorování sítě objektů může být redundantní nebo paralelní, lze provozovat několik dohledových pracovišť s různými oprávněními ke sledování jednotlivých stavů. Pro zajištění utajení a důvěryhodnosti přenášených informací jsou použity symetrické šifrovací algoritmy AES (Rijndael) a Triple DES (7).

3.6 POSTECH

3.6.1 Integrace EZS, ACCES a správa budov

URIDIUM je výkonný elektronický systém integrující systém EZS, ACCES a správu budov. Tyto tři celky řídí jedna centrála, ale také vytváří logické vazby mezi nimi. K základním funkcím lze přidat ještě ovládání EZS nejen pomocí primárně načtené karty, ale také třeba pomocí kontroly osob v daném prostoru a to vše úročit časovými okny. Tyto funkce lze podmiňovat či vázat k jiné činnosti. Na tuto konstrukci navazuje správa budov, která může být řízena na základě jakékoliv primární či výsledné akce. ACCES umí svazovat kontrolu přítomnosti osob v prostoru se dvěma vstupy, aniž by musel ten daný uživatel opustit prostor. Pokud uživatel v platném časovém okně vstoupí do povoleného prostoru, může dojít k vyvolání sekundární akce, v návaznosti na správu řízení budov atd.

Systém je vhodný pro střední objekty dle rozsahu. Při použití maximálních pamětí je systém schopen obsloužit 2500 zón, které se mohou rozdělit do 250 nezávislých

podsystemů s obsluhou 65000 uživatelů. 250 spínačů pro správu budov . Datová linka čtyř vodičová kódovaná RS485 v délce 900m pojme 250 modulů různých funkcí. Moduly výrobce doporučuje řadit sériově.

Vestavěný sériový port RS 232 umožňuje přímé napojení PC v místě instalace. Mezi další užitečné porty patří rozhraní TCP / IP, tiskárenský LPT, externí modem JTS pro vývod dálkové signalizace na PCO. Modulární struktura dovoluje nasazení modulů dle rozsahu aplikace.

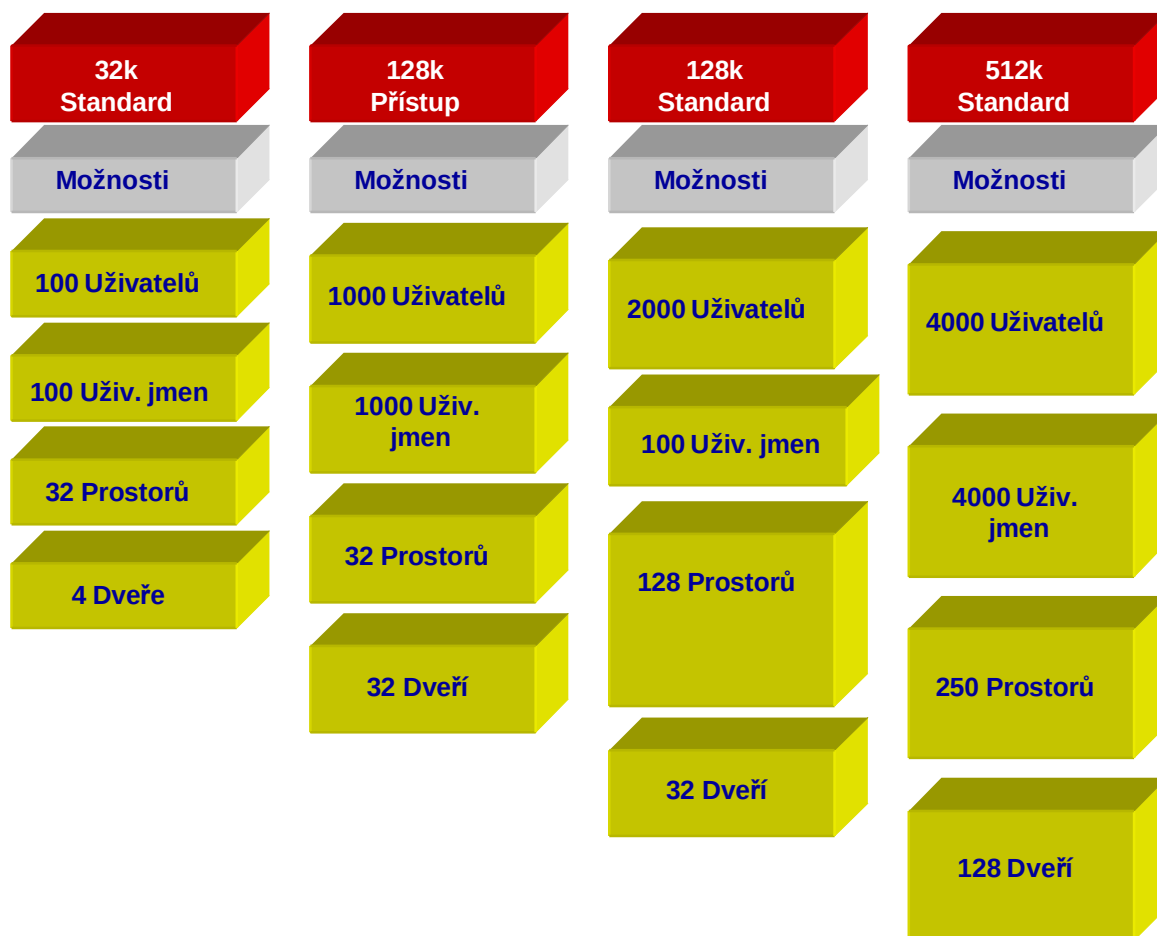
Kompletní programování a správu systému lze provádět z LCD klávesnice, ale daleko přehledněji pomocí SW produktu Xplorer Full. Pro uživatele je dostupná ještě light verze pro přehlednost. Otevřenost systému je přínosem k upgrade firmware, čímž je zjednodušeno zavádění nových verzí nebo zakázkově tvořených projektů.

Za zmínku ještě stojí modul digiplex, který vytváří sekundární datovou sběrnici pouze pro moduly digiplex. Strategie firmy směřuje k nahrazení tohoto systému, který je určen do malých aplikací systémem, který tvoří integraci více systémů pro vytvoření komfortní aplikace za minimálních finančních a provozních prostředků. Instalační firmy jistě kvitují tuto strategii (8),(16).

3.7 Inner Range

3.7.1 Integrace EZS, ACCES, správa a řízení budov

Systémy Concept 3000 / Access 4000 patří mezi novou generaci zařízení pro řízení přístupu osob, zabezpečení, správu a řízení budov. Celý systém je rozdělen do ucelené řady modulů, z nichž každý v systému vykonává určitou funkci. Všechny moduly sdílí vysoce výkonnou a zabezpečenou LAN sběrnici. Její délka může dosahovat řádově stovky a při použití prku tzv. LAN izolátoru tisíce metrů. LAN izolátor dále provádí obnovu signálu sítě, ochranu LAN min. výše 2,5 kV. Systém je plně modulární a lze ho sestavit pro danou aplikaci na míru. Pro velmi velké aplikace lze uvedené ústředny síťovat např. pomocí TCP / IP protokolu. Systém umožňuje za použití maximálních pamětí obsloužit 4000 zón, které je možno dělit do 250 nezávislých podsystemů s obsluhou 65500 uživatelů.



Obr. 22 Závislost velikosti paměti na rozsahu systému Concept

Možno využít 3800 programovacích výstupů, které splňují nejnáročnější kritéria vazeb a časových logických funkcí od všech integrovaných systémů. Historie sahá na počet 6500 událostí.

ACCES systém je ovládán klávesnicí /PIN kódem/ nebo kartou. Průchod dveřmi HI-Security může být umožněn po zadání dvou kódů časově svázaných. Mírná nebo tvrdá ochrana proti dvojitému přístupu na všech dveřích systému ukazuje variabilitu použití logiky. Volba karta + PIN nebo PIN nebo karta, kterou lze nastavit povolení průchodu u každých dveří samostatně. Možnost zapnutí či vypnutí průchodem přes zabezpečenou lokalitu považují za samozřejmost v rámci integrace. K přístupovým modulům lze připojit libovolnou čtečku s formátem Wiegand či Swipe. Plnohodnotná kontrola dveří s lokálním ovládáním v modulu umožňuje snadnou montáž s maximálním výsledkem

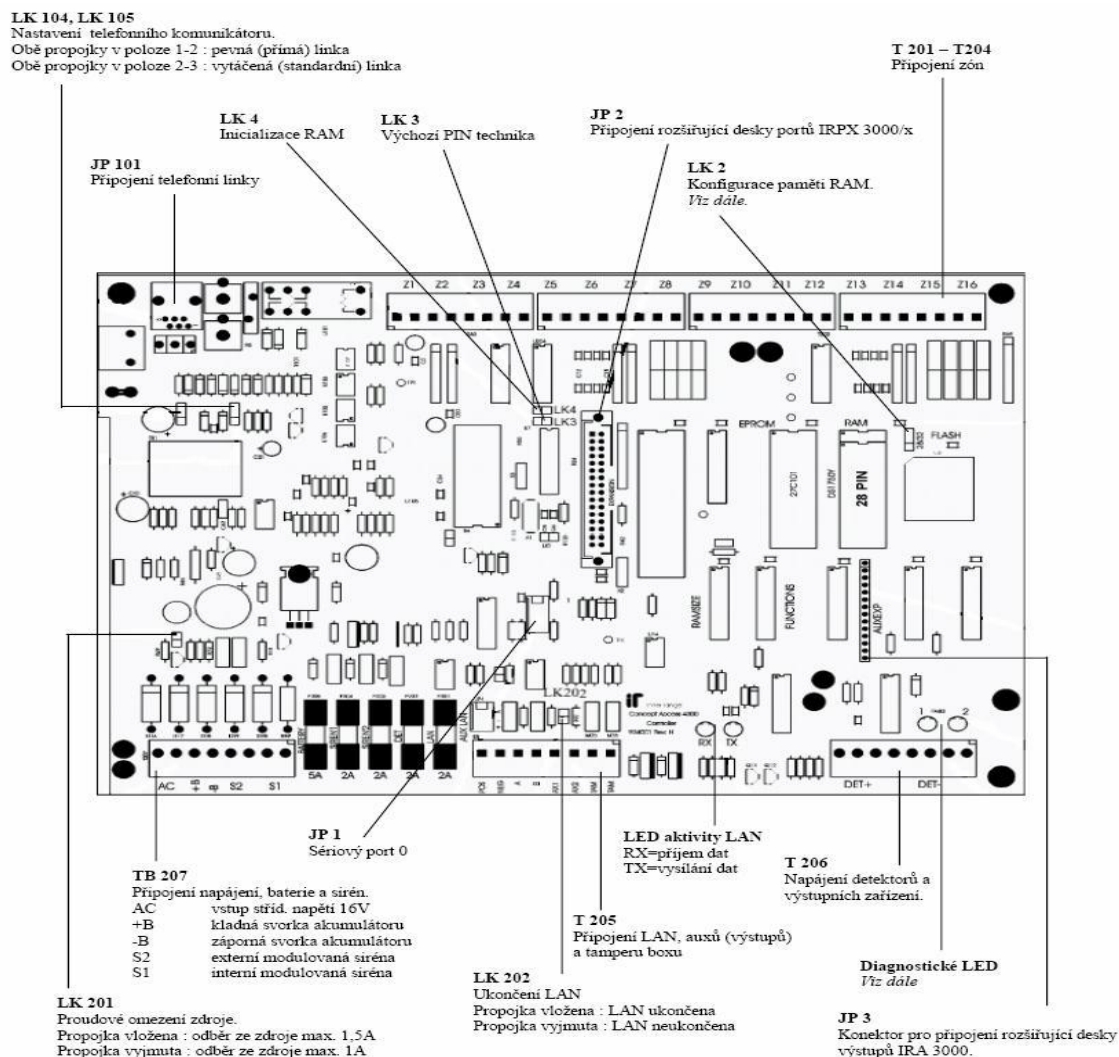
K vlastnostem systému ke správě a řízení budov lze dodat, že systém vykazuje univerzálnost použití. Lze plně ovládat a monitorovat 32 nezávislých výtahových kabin pro

64 pater. Ovládání 4 klimatizačních centrálních jednotek včetně snímání analogových veličin / intenzita osvětlení, teplota atp./ prokazuje neméně cenné informace o energetické situaci a úsporách.

Integrovaný systém Concept má ještě jednu zvláštnost a to sice v provádění několikanásobného vývodu dálkové signalizace stavu či poplachu. Je schopen v jeden okamžik aktivovat současně komunikátor na PCO po JTS, GSM modem ve formátu SMS, poslat pokyn zobrazovacímu lokálnímu tablu, předat informaci do lokální PC, aktivovat LPT výstup a přenášet po LAN s protokolem TCP / IP.

Firma Inner Range doplnila systém opravdu bohatou nabídkou různých SW produktů:

- **Wdirect**, program určený zejména technikům, slouží k plnému naprogramování ústředny. Podporuje upload/download konfigurace, on-line programování a monitorování.
- **Accept lite**, program pro programování, monitorování a ovládání ústředny Concept. Podporuje připojení jednoho PC k jedné ústředně pomocí sériové linky.
- **Accept**, programovací, monitorovací a ovládací software. Připojení pomocí jedné ústředny k jednomu PC prostřednictvím sériové linky. Dále umožňuje grafické monitorování objektu, vylepšenou práci s historií událostí (filtrování, změna textu výpisů jednotlivých událostí, ...) a nastavení individuálních přístupových práv každého uživatele.
- **Accept net**, stejné vlastnosti jako předchozí program, možnost spojení s více ústřednami pomocí sériové linky, modemu či TCP/IP sítě, možnost provozu na více PC.
- **PSD messenger**, program pro zasílání zpráv o dění v systému na pager, SMS či e-mail.
- **PSD reporter**, generování různých výstupních sestav na základě informací z přístupového systému.
- **PSD photo ID**, správa uživatelských karet, tvorba designu a potisku karet. Spolupracuje s programem Accept, v software AcceptNet je integrován.
- **Accept time**, Software pro zpracování docházky. Umožňuje generovat sestavy o odpracované době či výpisy jednotlivých příchodů-odchodů, funkce přítomní / nepřítomní pomáhá lokalizovat jednotlivé pracovníky. Možnost práce v síti (9)(12).



Obr. 23 Systém Concept

3.8 CGC Security

3.8.1 Centrální řídicí zařízení SBI

Produkt SBI (System of Building Security and Automation) je určený pro komplexní obsluhu a integraci poplachových a nepoplachových elektronických systémů. Představuje nejmodernější softwarové řešení v oblasti monitorování, řízení, správy systému EZS, EPS, měření a regulace, CCTV, EKV, včetně komfortního vyhodnocení docházky. Program využívá progresivní softwarové technologie k vytvoření aplikačního uživatelského prostředí v prostředí prohlížeče web stránek Internet Explorer. Základem prostředí je databáze MS SQL (MSDE), jež udržuje všechny databáze, tabulky a číselníky potřebné pro provoz

programu. Kompletní obsluhu a správu a údržbu programu lze provádět z jakéhokoli PC s MS Internet Explorer připojeného prostřednictvím sítě LAN, WAN k databázovému serveru. Systém podporuje sběr dat z monitorovaných technologií jak pomocí rozhraní RS 232 (lokální připojení), tak i prostřednictvím sítí LAN, WAN s využitím komunikačního protokolu TCP/IP.

Program je důsledně řešen jako modulární systém (uživatel volí, které moduly systému chce používat), včetně propracované správy připojených lokalit a technologií. Pro vizualizaci je zvoleno přehledné mapové zobrazení aktuální situace v objektu. Pro každého operátora je možné nastavit jiné aplikační prostředí, které není závislé na PC kde je aktuálně operátor přihlášen.

Operátorovi je tak na kterékoli stanici automaticky vytvořeno jeho aplikační prostředí včetně jeho práv v systému SBI. Samozřejmostí databázového prostředí je komfortní systém přihlašování všech aktivit – uživatelských i technologických. Program je určen zejména pro zákazníky, kteří mají objekty rozprostřeny v rámci velkého území a jednotlivé objekty jsou vybaveny datovou sítí. Z hlediska funkčnosti je SBI aplikační prostředí pro vývoj aplikace řešené na klíč zákazníkovi.

Mezi základní vlastnosti systému SBI patří:

- **enterprise** – možnost centrálního řízení vzdálených objektů, vysoký stupeň modularity umožňující vybavit server nebo monitorovací pracoviště konkrétními částmi aplikace, jež jsou potřebné pro správu a řízení.
- **otevřenost** - flexibilní postupné rozšiřování o nové oblasti řízení a monitorování oblastí bezpečnosti a provozu budov v reálném čase např. stravovací, parkovací, kamerové systémy, enviromentální systémy (klimatizace, UPS) atd.
- **nezávislost na provozu** a funkčnosti komunikační infrastruktury (LAN, WAN)
- **integruje technologie různých výrobců**, které mohou být společně zastřešeny jedinou nadstavbou
- **systém je parametricky** přizpůsobovaný požadavkům jednotlivých zákazníků
- **jednoduchá údržba a inovace celého systému** – díky koncepci programu je na minimum omezena údržba aplikace. Udržuje se pouze výkonné jádro, není nutné udržovat a obnovovat klientské stanice. Distribuce nových nebo modifikovaných funkcí ke klientovi probíhá automaticky. Samozřejmostí je i možnost spravovat dálkově vlastní výkonné jádro aplikace.

- **Vícejazyčnost** – možnost nastavení profilu aplikace s vytvořením vazby na jazykovou mutaci programu. Volbu jazyka je možné provádět za chodu aplikace bez nutnosti jejího ukončení. Podporovanými jazyky jsou čeština, slovenština, němčina a angličtina.

Moduly systému jsou:

Základní

Zabezpečuje řízení celého systému, komunikaci mezi jednotlivými moduly a správu osob a oprávnění. Pro každého uživatele je možné navolit množinu práv a umožnit tak kompetentní delegování pravomocí obsluhy. Činnost programu je zabezpečena proti neúmyslným chybám i pokusům o zneužití údajů. Kromě běžné ochrany přístupovými jmény a hesly společně s nastavitelnými právy je program vybaven podrobnou archivací provozu aplikace, uživatelů i reakcí technického vybavení systému. Program umožňuje ve stanovených termínech automatické zálohování kompletní databáze. Díky využití SQL databáze je možné řešit i automatizované replikace databází, jejich zrcadlení pro velmi snadnou údržbu a celkové zvýšení bezpečností aplikace. Aplikace je řešena jako vícejazyčná, s možností nastavení uživatelského profilu obsahujícího informace o jazykové verzi (anglická, německá, česká, slovenská) i za chodu aplikace bez jejího restartu. Pro běh jádra jsou nutné následující komponenty: MS W2000 server, MS IIS, MS SQL 2000, MS Internet Explorer 5.

Přístupový a návštěvnický

Jeho základní funkcí je řízení autorizovaných přístupů pro autorizované osoby. Slouží na omezení volného a nekontrolovatelného pohybu osob ve vyhrazených prostorech, kontrolu pohybu osob a zjišťování jejich přítomnosti v určeném prostoru a čase. V systému je možné realizovat vazby mezi jednotlivými systémy a řešit tak například možnost ovládání systému EZS prostřednictvím karet systému kontroly vstupu.

Stravovací

Modul umožňuje vytvoření aplikačního prostředí pro systém objednávek jídel s využitím dat pocházejících ze systému kontroly vstupu. Dostupná je i vazba na účetní systémy pro realizaci plateb odebraných jídel. Z jednotného prostředí je tak možné přímo objednávat, sledovat objednávky a vytvářet vazbu pro účtování.

EZS, EPS, CCTV a perimetru

Slouží na centrální monitorování, řízení bezpečnostních a požárních ústředí. Poskytují bezpečnostní službě informace o stavu jednotlivých požárních a bezpečnostních zón v reálném čase, přímé ovládání a záznam historie jednotlivých monitorovaných událostí. Při propojení s přístupovým systémem je možné na základě oprávnění automatické vypnutí střežícího režimu v dané zóně, nebo i automatické zapnutí systému do střežení v případě opuštění zóny poslední osobou. Propojení s CCTV systémy umožňuje automatické spuštění kamerového systému v kritické oblasti na základě vyhodnocení události z ústředí EZS. Jednotná databáze umožňuje stejný způsob ovládání i pro technologie různých výrobců. Pro vybrané technologie (např. EZS GALAXY) modul umožňuje řešit také správu uživatelů a karet s nastavením oprávnění.

Docházkový

Umožňuje zpracování údajů z identifikačních snímačů ve formě docházky, podle požadavku personálních, mzdových a informačních útvarů uživatele.

Real time

Modul svou funkcí nahrazuje pulty centrální ochrany (PCO). Je určený pro nepřetržité sledování stavu jednotlivých technologických subsystémů v přehledném mapovém zobrazení zájmového objektu nebo objektu. Na rozdíl od PCO umožňuje i zpětné řízení (zapínání, vypínání, rušení poplachu, přemostování) v reálném čase pomocí softwarových nástrojů. Zároveň poskytuje dispečerům potřebné informace nevyhnutelné pro kompetentní a rychlé rozhodování při vzniku mimořádných událostí. Díky členění mapových částí do pracovních vrstev je možné jednotlivým operátorům rychle a flexibilně definovat objekty a lokality, s nimiž mají pracovat a vytvářet tak hierarchickou strukturu monitoringu. Počet monitorovaných lokalit není nikterak omezen.

Environment control

Systém zabezpečuje centrální řízení obecných technologií v reálném čase a ukládá do databáze všechny informace o událostech, které na zařízeních nastaly. Modul umožňuje úplné řízení základních systému budovy, jako je klimatizace, ventilace, napájení, záložní zdroje a mnoho dalších technologií. Díky použitému konceptu systém umožňuje správcům řízení a monitorování velkého množství budov bez ohledu na vzdálenost.

Mail manager

V případě monitoringu velkého množství technologií a veličin je pro obsluhu náročné v reálném čase zpracovávat tyto informace a provádět rychlá a kompetentní rozhodnutí. Modul Mail manažer umožňuje směřovat vybrané informace z vybraných monitorovaných

technologií konkrétním kompetentním pracovníkům a to i bez nutnosti jejich přítomnosti na pracovišti. Informace je možné k uživateli zasílat ve formě SMS, E-mailu nebo SNMP zpráv. Je možné také definovat přesnější podmínky zasílání zpráv (např. výpadek síťové komunikace musí být detekován 5x během definované časové periody), zasílat zprávy přímo servisní organizaci a minimalizovat tak aktivitu lidské obsluhy a zkracovat dobu technického zásahu.

Prostory

Modul Prostory je nový nástroj umožňující bezproblémově řešit počítání lidí (automobilů, zboží...) v prostoru s možností návaznosti na další technologie. Díky systému správy tzv. softwarových prostorů je možné vytvořit prostor z libovolného počtu příchodových a odchodových čtecích míst a sledovat aktuální stav zaplnění prostoru. Tento modul řeší i požadavek na automatizované zapnutí a vypnutí EZS, skupiny kanceláří pomocí karty, kartového systému pro ty typy ústředěn EZS, které je možné zapínat a vypínat příkazem z PC. Systém „Prostory“ je možné také doplnit o funkci antipassbacku zamezujícím dvojí použití karty v rámci stejného směru pohybu – například dvojí příchod bez předchozího odchodu.

Audit

Samozřejmostí je možnost analýzy činnosti systému a jednotlivých operátorů. Program si za běhu ukládá záznam o svém provozu, data z jednotlivých monitorovaných technologií a o práci jednotlivých operátorů. Tato data jsou kdykoli dostupná ve formě uživatelsky definovaných sestav určených pro prohlížení a tisk. Informace jsou v databázi uloženy tak, aby nebylo možné záznamy neautorizovaně mazat nebo jinak modifikovat.

Modul správy parkovišť

Modul představuje nadstavbu přístupového systému umožňující sledovat aktuální stav zaplnění hlídaného parkoviště, spolupracovat s výdejními stojany, definovat blokování stání pro vybrané vozy či firmy. Je také možné pro stálé uživatele parkoviště řešit propojení údajů z Modulu správy parkovišť do účetního systému a vytvořit tak systém pro automatizované účtování použití parkoviště (10).

4 KOMPLETNÍ SYSTÉMOVÁ OCHRANA V PKB

4.1 Vznik a historie - inteligentní budova

Termín „inteligentní budova“ vznikl v 80 – tých letech v USA. Tento pojem skýtá mnoho definicí. Můžeme se na to podívat s pohledu tří základních rozdělení:

- **Koncepčního** – komplex budov adekvátně reaguje na potřeby člověka a jeho okolí.
- **Ekonomického** – soubor organizačních, finančních a technických opatření, zajišťujících minimalizaci nákladů na provoz budovy a její konkurenceschopnost na trhu nemovitostí.
- **Technického** - soubor organizačně - technických řešení uplatněných při výstavbě a směřovaných k vytvoření komfortních, ekonomických a bezpečných podmínek pro majitele i nájemce budovy.

Směr vývoje jednoznačně ukazuje inteligentní budovu jako integraci systémů, služeb a správy budov, jehož cílem je splnění současných i budoucích požadavků vlastníků a uživatelů. Mezi požadavky vlastníků patří úspora investičních prostředků, úspora provozních nákladů, minimalizovat náklady na inovace a rekonstrukce, zatímco mezi požadavky uživatelů patří kvalitní a účelné pracovní prostředí, flexibilita budovy při změně využití, jednoduchost obsluhy komplexu.

Jednoduše řečeno inteligentní budova musí zabezpečit odpovídající komfort při optimalizovaných nákladech.

4.2 Propojení jednotlivých systémů, integrace

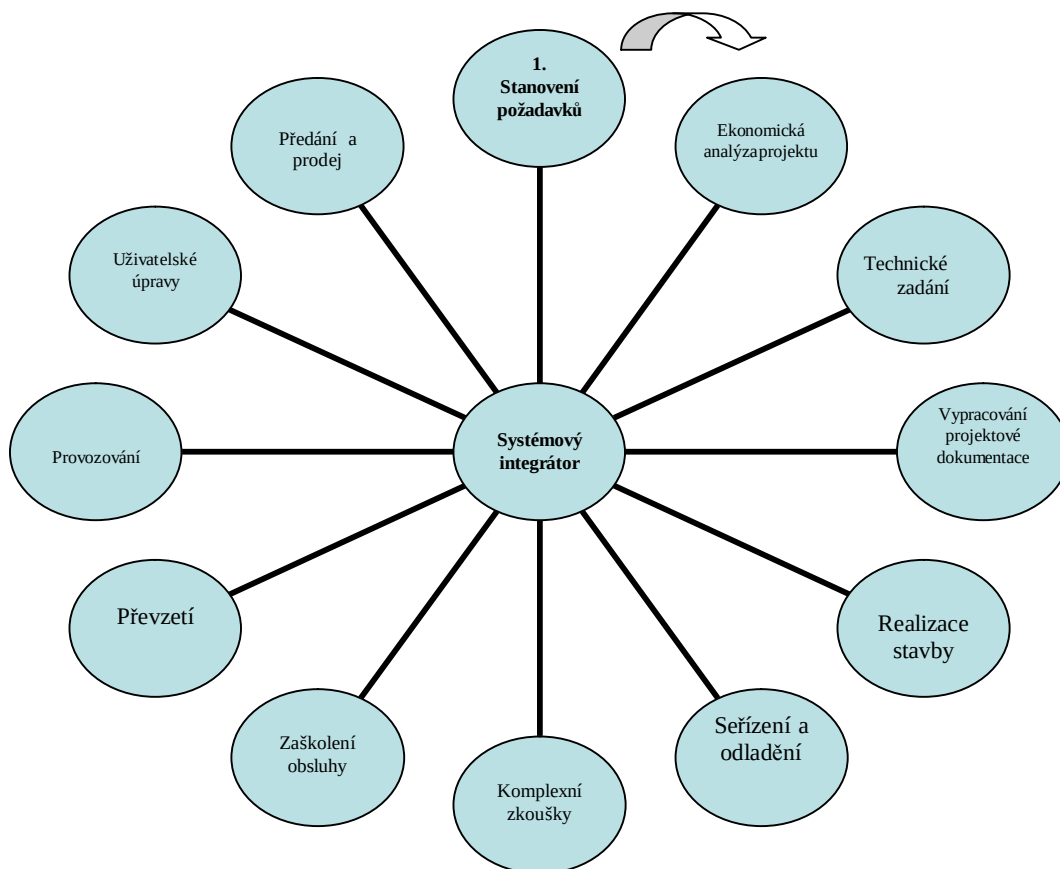
V topologii integračního systému bychom měli vidět tři úrovně, kde probíhají vazby.

- Úroveň periférií – je to nejnižší úroveň. Skládá se většinou z kontaktů, někdy analogových signálů. Je nutné provádět galvanické oddělení. Plní funkci sběru dat, logických vazeb v rozsahu maximálně desítek kontaktů.
- Úroveň automatizační – převodníky protokolů jako mikroprocesorové systémy s několika porty buď standardní nebo na zakázku. Funkčně vykonávají sběr dat, logické vazby, odečty hodnot. Rozsahově desítky až stovky datových bodů.
- Úroveň řídicí – převodníky protokolů, obvykle jako SW drivery v řídicí stanici. Funkčně vykonávají monitorování a odečty hodnot. Rozsahově desítky až tisíce datových bodů.

Provázání jednotlivých systémů – koncepce je založena na systémovém řešení, které není rozhodně dílem jednoho člověka. Na dobré koncepci se musí podílet tým lidí různých profesí. Koncepce integrovaného řešení musí vycházet již od vzniku myšlenky projektu. Na koncepci se podílí:

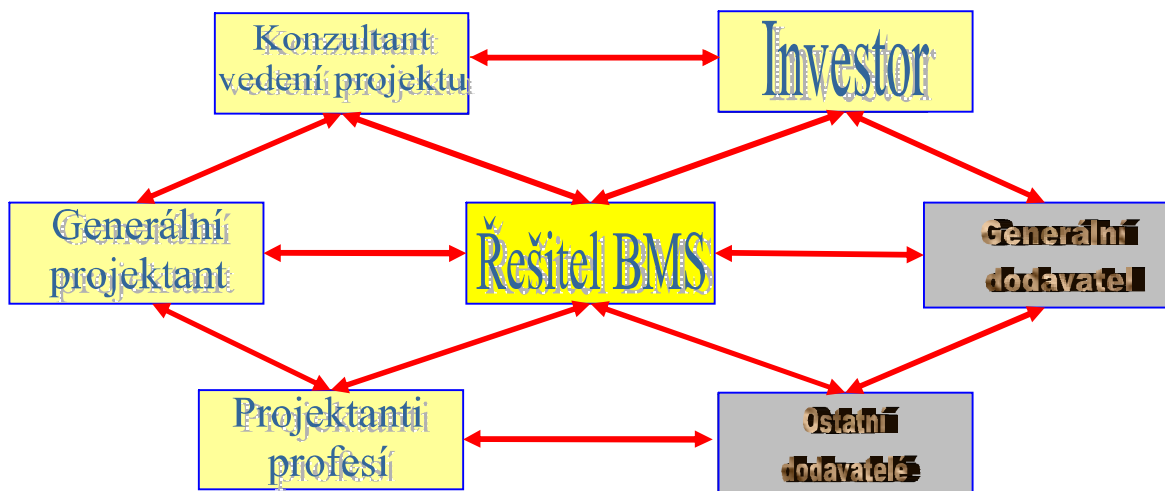
- investor
- architekt
- odborní konzultanti
- generální dodavatel
- projektanti profesí
- uživatel - nájemce

Celkovou odpovědnost za úspěšnost propojení musí nést systémový integrátor. Tento článek používá ke své činnosti prostředky a metody z oblasti IT /informačních technologií/. Řeší datové komunikace, protokoly, sítě. Stává se partnerem uživatele po celou dobu životního cyklu budovy.



Obr. 24 Systémový integrátor

Systémový integrátor ne vždy pokrývá celé spektrum činností potřebné pro komplexní řešení ve vztahu k její technologii, proto si bere řešitele řídicího systému budovy /BMS/. BMS využívá svých zkušeností při správě a údržbě budov, monitoruje a ovládá technické zařízení budovy, plánuje a organizuje údržby, vede evidenci údržby, spravuje skladové hospodářství, databáze subdodavatelů atd. Graficky je na obrázku 26 znázorněna vazba na BMS při tvorbě projektů.



Obr. 25 Vazby BMS na realizace projektů

Integrace uplatňovaná v průmyslu komerční bezpečnost zahrnuje nejenom poplachové systémy, jako jsou EPS, EZS, ACCES, CCTV ale také životně důležité systémy, jako jsou například řízení a regulace tepla, chladu a vzduchotechniky, měření spotřeby tepla, chladu a vody, řízení osvětlení, monitorování a provoz náhradních zdrojů, management energetického hospodářství, řízení a provoz výtahů. Uvedu příklady, které by se nedaly uskutečnit bez tohoto propojení.

- Využití informace o přítomnosti osob z přístupového systému pro řízení klimatizace nebo osvětlení.
- Využití informace o stavu okenních kontaktů systému EZS pro řízení místní klimatizace.
- Využití informace ze systému EPS pro řízení VZT zařízení, výtahů a pod. (11).

5 NÁVRH INTEGROVANÉHO SYSTÉMU V TECHNOLOGII SBI

Pro ukázkou nasazení technologie SBI jsem zvolil střední firmu co do velikosti tak do technického vybavení. Firma má jedno ředitelství a tři pobočky umístěné na různých místech naší republiky.

5.1 Technologické požadavky na instalaci a provoz systému

5.1.1 Jednoúčelové systémy

Kompatibilitu jednotlivých jednoúčelových systémů se systémem SBI jsem volil z výběru firmy CGC Security dle seznamu příloh. Jednotlivé pobočky jsem vybavil systémy, které v běžné praxi a svým rozsahem odpovídají navrhovanému řešení. Všechny navrhované jednoúčelové systémy poskytují otevřený komunikační formát RS 232.

5.1.2 Přenosová trasa

Jednotlivá jednoúčelová zařízení komunikují přes stávající počítačovou firemní síť. Zabezpečené informace procházejí místním serverem a přecházení do sítě Internet. SBI SQL server na ředitelství sbírá tyto informace ze sítě Internet a ukládá do svých databází. Pokud by došlo k přerušení přenosové trasy, jednotlivá jednoúčelová zařízení pracují v předdefinovaném režimu naprosto autonomně. Události a informace, které jsou požadovány na přenos jsou ponechány na jednotlivých pobočkách do navázání spojení s mateřským SQL serverem.

5.1.3 Serverová část

Na serverovou část implementace SBI je kladený důraz s ohledem na celkovou spolehlivost provozu řídicího serveru z dlouhodobého hlediska.

Software serverové části:

- WINDOWS SERVER 2000, XP
- Microsoft Internet Information Server
- Microsoft SQL Server 2000 nebo MSDE 8

Hardware serverové části, doporučená konfigurace

- CPU: Intel Pentium III FSB133 1GHz
- RAM: SDRAM, 3V, PC 133 256 MB
- HDD: 2 ks UDMA100, 7200ot/min, 8,5 ms 30 GB
- VGA: AGP 16 GB
- FDD: Teac 3.5“ 1.44MB
- CDR: ATAPI, int., 6000kB/s 40x
- ETN: PCI Fast Ethernet adapter 10/100MB
- DAT Internal IDE DAT HP Sure Store nebo obdobný 24 GB
- MODEM: External ISDN s Hub Zyxel Prestige100IH
- MONITOR: COLOR SVGA 17“
- UPS: Server bude připojený na napájení GT „no-break“.

5.1.4 Pracovní stanice

Pracovní stanice můžou být s operačním systémem Windows2000 nebo Windows XP s nainstalovaným internetovým prohlížečem Microsoft Internet Explorer verze 5.0 a vyšší. Všechny aplikace systému SBI běží prostřednictvím MS Internet Explorer.

Pro práci s modulem Real time je podmínkou, že na pracovní stanici bude instalovaný operační systém MS Windows 2000 Professional nebo Windows XP Professional.

Hardware „ Pracovní stanice“ minimální

- Procesor: INTEL P5, P6 Celeron, Klamath a AMD
- RAM: min 32 MB
- Video karta: min 8MB
- HDD: min 2 GB
- Ethernet: 10/100 MB/s
- Monitor: 15“ Color.

5.1.5 Sítové rozhraní

Uvedený software požaduje pro svoji činnost přítomnost komunikačního protokolu TCP/IP na sítích LAN, WAN. Pro správnou funkci navrhovaného vstupního a kontrolního systému je zapotřebí zabezpečit minimální rychlost na LAN, WAN 64 kb/s, přičemž

uvedený systém nezatěžuje přípustnost sítí kontinuálně, ale jen krátkodobě řádově ve stovkách ms. (10).

5.1.6 Popis implementace

Instalace serveru

- Úvodní analýza instalace serveru, volba umístění citlivých dat a konfigurace síťového rozhraní.
- Nová konfigurace PC, instalace MS IIS, vytvoření provozních a administrátorských účtů, instalace a konfigurace MS SQL.
- Instalace software SBI.
- Úvodní spuštění SBI, zavedení licenčního souboru a vytvoření operátorských účtů pro administraci a nastavování SBI.

Import a konfigurace dat pro server SBI

- Konfigurace komunikačních okruhů, nastavení hraničních oblastí pro upload dat do ústředen, nastavení časových pravidel pro upload dat do ústředen.
- Import číselníků senzorů (smyčky, výstupy, kamery, čtečky...) pro jednotlivé okruhy a technologie.
- Import číselníků podsystémů EZS a vytvoření vazeb mezi senzory EZS a podsystémy EZS
- Import a konfigurace přístupových terminálů systému EZS, EKV.
- Import karet platných v jednotlivých lokalitách.
- Vytvoření modelu organizační struktury (oddělení, střediska) a vazeb mezi nimi.
- Naplnění číselníku údajů o osobách (personální údaje, foto, přihlašovací údaje, přidělené karty, začlenění do organizační struktury, vazby na docházku..).
- Nastavení oprávnění k obsluze jednotlivých lokalit pro konkrétní definované osoby.
- Nastavení příznaků Audio varování pro vybrané prioritní typy událostí.
- Konfigurace a naplnění vědomostní databáze a vytvoření vazby mezi zpracovávanými údaji a znalostní bází.

Příprava grafických podkladů a konfigurace modulu Realtime.

- Zpracování CAD podkladů do formátu WMF a jeho optimalizace.

- Zavedení grafických podkladů do systému SBI a vytvoření stromu instalací.
- Umístění prvků senzorů (EVS, CCTV, EKV, EPS) do map a vytvoření vazeb mezi grafickými prvky a databází senzorů.

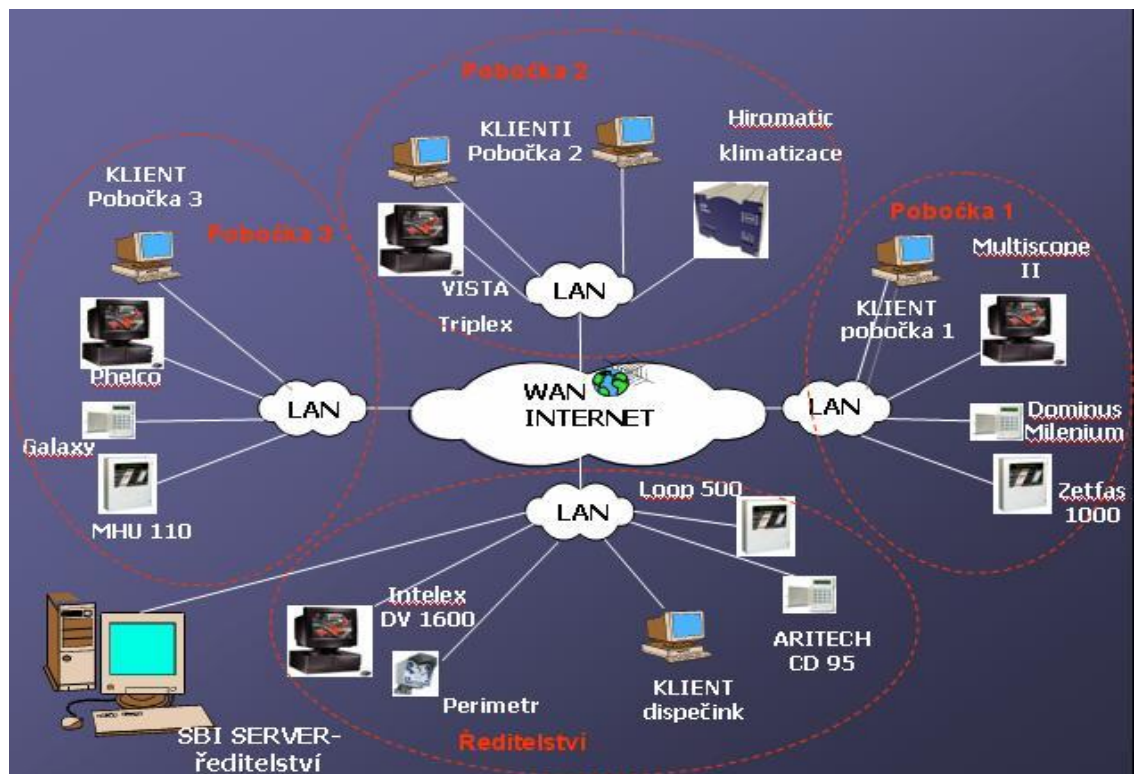
Definování uživatelů programu SBI a nastavení jejich práv

- Definice přístupových práv k jednotlivým modulům a jejich funkcím pro oddělení, střediska nebo jednotlivce.
- Nastavení přístupu uživatelů SBI k doménovému serveru organizace pro umožnění přebírání uživatelských účtů (jména, hesla) z tohoto serveru.
- Definování lokálních účtů a práv pro vybrané jednotlivce nebo skupiny nezařaditelné do doménových účtů.

Konfigurace klientských stanic určených pro provoz systému SBI a test funkčnosti spojení

- Test funkčnosti jednotlivých modulů a funkcí dostupných přihlášenému operátorovi.
- Nastavení uživatelského profilu uživatele SBI (jazyková verze, podpora práce se zvuky, nastavení způsobu zobrazování údajů)
- Úvodní zaškolení uživatele systému SBI

5.2 Blokové schéma návrhu řešení



Obr. 26 Návrh řešení SBI

5.2.1 Licenční politika

Dostupnost jednotlivých modulů je podmíněna zadáním softwarového licenčního klíče. Takto je možné doplňovat funkcionalitu systému bez nutnosti reinstalací, migrací dat mezi verzemi atd. Inovace u systému SBI jsou prováděny pouze na serveru. Na centrálním serveru jsou současně umístěny i klientské komponenty, které se automaticky stahují na klientskou stanici při prvním připojení klienta na server – tzv. nulová administrace klientské strany.

Licenční politika i technologický model serverové části komunikující s jednotlivými technologiemi umožňují maximální míru ochrany investic u klienta. Systém SBI je totiž koncepčně navržen pro snadné začleňování nových, v čase instalace nepodporovaných technologií do stávající instalace. Pro komunikaci s technologiemi je využit systém tzv. zásuvných driverů – DLL knihoven. Takto je možné doplňovat podporu nových technologií do jednotného jádra systému bez masivních úprav.

ZÁVĚR

Cílem této práce nebylo popsat veškeré možnosti integrovaného elektronického systému. Integrovaný elektronický systém obsahuje ohromné množství vlastností a možností použití, že nebylo možno do tak malého prostoru vyhrazeného pro bakalářskou práci vměstnat všechny důležité informace.

Proto jsem se věnoval jen obecným informacím o problematice nasazení v průmyslu komerční bezpečnosti. Snažil jsem se o co nejsrozumitelnější vysvětlení práce na vývoji a zrodu integrovaného elektronického systému a poukázat na všechny aspekty, které se rozhodující měrou podílejí na budování a pozdější údržbě. Věnoval jsem se praktickým vlastnostem jednotlivých vybraných systémů od jednotlivých výrobců nejen tuzemských. Přiblížením nejzajímavějších vlastností a předností tyto systémy staví do žebříčku úspěšného prodeje a nasazování do jednotlivých aplikací. Aby bylo možno posoudit kvalitu a výhody při integraci nahlédl jsem do kuchyně software i hardware přípravy jednotlivých výrobků. V širším pohledu na věc si uvědomuji složitost a pečlivost při nasazování jednotlivých systémů vzhledem k nekonceptnosti jednotlivých výrobců ve formátu výstupního datového protokolu.

Efektivitu nasazení integrovaných elektronických systémů v budoucnu spatřuji ve zvýšení produktivity práce provozních pracovníků a snížení nákladů na provoz a údržbu budov. Tedy pro optimální funkci budovy musí být zajištěna jednotlivá propojení:

- pocitu bezpečí
- komfortu prostředí
- efektivity práce.

Integrací elektronických systémů přinášíme informace, které neobtěžují běžnými provozními stavy, ale zdůrazňují stavy vyžadující pozornost. Budoucnost je nabízet nové způsoby zobrazení pomocí multimediální techniky. Všechny zobrazovací a povelové funkce zjednodušovat a uvádět do jednotného uživatelského rozhraní, abychom omezili chyby vyvolané lidským faktorem.

SEZNAM POUŽITÉ LITERATURY

- [1] Poplachové systémy- Kombinované a integrované systémy- Všeobecné požadavky, ČSN CLC/TS 50398, Březen 2005
- [2] KINDL, J. *Projektování bezpečnostních systémů I.díl*, Zlín: vyd. Universita Tomáše Bati ve Zlíně, 2004. ISBN 80-7318-165-7.
- [3] MERHAUT, J., Seminář AGA 01/2005
- [4] Instalační a uživatelské manuály firmy NOVAR
- [5] Instalační a uživatelské manuály firmy HONEYWELL
- [6] Instalační a uživatelské manuály firmy SIEMENS
- [7] Instalační a uživatelské manuály firmy SPELZA
- [8] Instalační a uživatelské manuály firmy POSTECH
- [9] Instalační a uživatelské manuály firmy INNER RANGE
- [10] Instalační a uživatelské manuály firmy CGC
- [11] BOJANOVSKÝ, J. Seminář AGA 02/2005
- [12] Concept na českém trhu, Magazín *SECURITY*, roč.XI, č.4/2004, s.21. ISSN 1210-8723
- [13] POLÁK, J. Systém EPS Aritech a integrace, Magazín *SECURITY*, roč.VII, č.3/2000, s.24-25. ISSN 1210-8723
- [14] TFAPS – přístupový systém pro integrované zabezpečení průmyslu, Magazín *SECURITY*, roč.VII, č.6/2000, s.30. ISSN 1210-8723
- [15] Nová verze ústřední Galaxy Classic, Magazín *SECURITY*, roč.X, č.1/2003, s.27-28. ISSN 1210-8723
- [16] Uridium – poslední krok integrace v EZS, Magazín *SECURITY*, roč.X, č.1/2003, s.36. ISSN 1210-8723
- [17] MORÁVEK, J., SIEMENS, Magazín *SECURITY*, roč.XI, č.5/2004, s.51. ISSN 1210-8723

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACCES	Systém kontroly vstupu
AGA	Asociace grémium alarm
ATS	Poplachové přenosové systémy
CCF	Ústřední řídicí jednotka
CCTV	Uzavřený televizní okruh
CENELEC	Normotvorný orgán v EU
ČSN	Česká státní norma
EPS	Elektrická požární signalizace
EZS	Elektrická zabezpečovací signalizace
PCO	Pult centralizované ochrany
PKB	Průmysl komerční bezpečnosti
PPC	Poplachové přijímací centrum
SAS	Systém přivolání pomoci
TNI	Technická normalizační informace
TS	Technická specifikace
RS 485	Typ komunikační sběrnice
RADOM	Typ pultu centralizované ochrany
FAUTOR	Typ pultu centralizované ochrany
NAM	Typ pultu centralizované ochrany
BUS1,2	Komunikační sběrnice
IGIS	Kruhová komunikační linka
LOOP	
VdS	Německá asociace pojišťoven

SEZNAM OBRÁZKŮ

Obr. 1. Příklad struktury typu 1	15
Obr. 2. Příklad struktury typu 2	16
Obr. 3. Ústředny EZS Novar	23
Obr. 4. Zapojení kabelu sběrnice BUS 1, BUS 2	24
Obr. 5. Prvky pro sběrnici BUS 1	25
Obr. 6. Prvky pro sběrnici BUS 2	26
Obr. 7. Ovládací bezkontaktní místa IK 2,3.....	26
Obr. 8. Ústředny EPS Novar	28
Obr. 9. ESSER BUS.....	29
Obr. 10. Hlásič O ² T	30
Obr. 11 ACCES Novar ACS 8	31
Obr. 12 CCTV Novar visiOprime	32
Obr. 13 Integrace s WINMAGEM.....	33
Obr. 14 Nová podoba Galaxy G3.....	35
Obr. 15 EKV GALAXY G3	35
Obr. 16 Struktura připojení AIViS	36
Obr. 17 Ústředna Sintony 410	38
Obr. 18 Schéma audio komunikace na PCO.....	39
Obr. 19 Schéma video komunikace na PCO.....	39
Obr. 20 Systém MM 8000	40
Obr. 21 Systém DOMINUS MILLENIUM.....	42
Obr. 22 Závislost velikosti paměti na rozsahu systému Concept	45
Obr. 23 Systém Concept.....	47
Obr. 24 Systémový integrátor	53
Obr. 25 Vazby BMS na realizace projektů	54
Obr. 26 Návrh řešení SBI	59

SEZNAM TABULEK

Tabulka 1. Vyhodnocení odporu smyčky ústředny	21
Tabulka 2. Rozdíly Galaxy G3 144 a 520.....	34
Tabulka 3. Vyvinuté DDE Servery k AlVisu.....	37

SEZNAM PŘÍLOH

Přehled technologií podporovaných SBI

 SECURITY	kontrola vstupu	Docházka	Systémy EPS	Systémy EZS	Klimatizace	UPS	CCTV	V/V – dohled	V/V – ovládání	Ostatní	Poznámka
A2B											
A2B Device Patrol						•					
A2B S94						•					
ADEMCO Microtech											
Galaxy Classic 8-512	•			•							
AISA Information Systems, SK											
Aisa MTC 2.1	•	•									
Alimex											
Alimex G2	•	•	•	•			•	•	•		
American Dynamics											
SpeedDome							•				
ASCOM											
DCI 48V 3000VA						•					
STS 2000						•					
Axis Communications											
Axis Network Cameras							•				
Baxall											
Baxall IP Codec							•				
Baxall Dome BPD2							•				
Convision											
V6xx, V7xx, V8xx							•				
Cominfo											
REI AC4/Open	•	•									
Dialoc, NL											
ZAP Series	•										
Duha Systems CZ											
NetBox series	•	•									
Goldcard CZ											
300, 400, 7800 Series	•	•									
Hiross-Liebert											
Hiromatic					•						
GE Interlogix – Aritech											
FP1100, FP2000, FP3000				•							
Aritech ATS2000, 3000, 4000, 4500	•			•							
GE Interlogix – Aritech											
Aritech CD 95				•							
DVMRe Triplex							•				
Geutebrück											
Multiscope II							•				
IMA CZ											
IMA CKP1, 2	•	•									
Impro, SA											
FlexiScan E	•										
Intellex											
DV16000							•				
KABA Benzing											
Bedanet series	•	•									
Lites											
MHU 110				•							
MHU 111				•							
Nes											
Nes Protec							•	•			Spínaný zdroj pro katodovou ochranu
Olympo (Honeywell Security Products)											
HUB PRO	•										
DT2000	•	•									
Simux 64							•				DIO karta 64 vstupů / 4 výstupy
PaPouch											
PaPouch AS1							•				Modul analogových vstupů
Quadrax									•		4x RS232 multiplexer
Logger							•				Modul záznamů analogových vstupů
Paradox											
Digiplex 48				•							
Digiplex NE	•			•							
Pelco											
Pelco Spectra Dome							•				
Spelza											
Dominus Millenium	•	•		•							
Vista											
Vista Columbus Triplex							•				Digitální záznam
Winkhaus											
Intras series	•	•									
OEM 9050		•									
Zettler											
Loop 500			•								
Zetfas 1000			•								