

Perspektiva PCO

Perspective of the CES

Bc. Pavel Zapletal

Diplomová práce
2009



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav elektrotechniky a měření

akademický rok: 2008/2009

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: Bc. Pavel ZAPLETAL

Studijní program: N 3902 Inženýrská informatika

Studijní obor: Bezpečnostní technologie, systémy a management

Téma práce: Perspektiva PCO

Zásady pro vypracování:

- 1. Specifikujte PCO jako nástroj k zajištění fyzické bezpečnosti objektu.**
- 2. Analyzujte určení a složení PCO.**
- 3. Zhodnoťte uživatelské možnosti PCO software.**
- 4. Analyzujte technické možnosti zvolených PCO.**
- 5. Vymezte možnosti využití IT použitelné pro rozvoj PCO.**
- 6. Specifikujte trendy vývoje PCO.**

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. Uhlář, J.: Technická ochrana objektů, II. díl – Elektrické zabezpečovací systémy. Praha: PA ČR 2001.
2. Kindl, J.: Projektování bezpečnostních systému I. 1. vyd. UTB Zlín 2004.
3. Křeček, S.: Příručka zabezpečovací techniky, Praha, 2006
4. Čandík, M.: Objektová bezpečnost II. UTB-Academia centrum Zlín, 2004.
5. Vyorálek, R.: Pulty centralizované ochrany. Bakalářská práce. 1. vydání. UTB Zlín 2005.

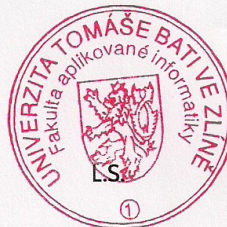
Vedoucí diplomové práce: **doc. Ing. Luděk Lukáš, CSc.**
Ústav elektrotechniky a měření

Datum zadání diplomové práce: **20. února 2009**

Termín odevzdání diplomové práce: **22. května 2009**

Ve Zlíně dne 20. února 2009


prof. Ing. Vladimír Vašek, CSc.
děkan




doc. RNDr. Vojtěch Křesálek, CSc.
veditel ústavu

ABSTRAKT

Cílem práce je specifikace současného stavu v oblasti pultů centralizované ochrany. Analýze je podrobena technické řešení, softwarové řešení i uživatelské možnosti. Závěr práce tvoří specifikace trendů, které se v předmětné oblasti očekávají, což umožní na kvalitativně vyšší úrovni řešit využití těchto systémů k zajištění bezpečnosti.

Klíčová slova: Pult centralizované ochrany (PCO), Průmysl komerční bezpečnosti (PKB)

ABSTRACT

The task objective of this research paper is the current status specification in the field of centralized electronic (desk) security (CES = PCO). Subjected to an analysis is technical solution, software solution even user possibilities. The research paper conclusion includes trends specification that is expected in this field which will enable implementation of these systems to a much higher degree to fulfill its usage as security ensurance.

Keywords: Centralized electronic (desk) security (CES), Industry of business security

Touto cestou bych chtěl poděkovat svému vedoucímu diplomové práce, doc. Ing. Ludškovi Lukášovi, CSc., za odborné vedení, ochotně poskytnuté rady a čas, který mi věnoval při vypracování mé diplomové práce.

Prohlašuji, že

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

Prohlašuji,

že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.

Ve Zlíně

.....

Podpis diplomanta

OBSAH

ÚVOD	10
1 CHARAKTERISTIKA PULŤCENTRALIZOVANÉ OCHRANY ..	11
2 VZNIK PCO	12
2.1 SOUKROMÉ BEZPEČNOSTNÍ SLUŽBY.....	12
2.2 MĚSTSKÉ POLICIE.....	12
2.3 HISTORIE TECHNICKÉHO VÝVOJE PCO.....	13
2.4 OBECNÉ POŽADAVKY NA PROVOZ PCO.....	14
2.5 INTEGRACE V PROVOZOVÁNÍ PCO.....	16
2.6 SLUŽBY NA PCO.....	17
2.7 PODMÍNKY PROVOZU DLE CI ČAP.....	20
2.7.1 PCO – Názvosloví a pojmy.....	20
2.7.1.1 Názvosloví dle ČSN EN 50136 [1] a [2].....	21
2.7.1.2 Pojmy týkající se PCO.....	21
3 SLOŽENÍ PCO	24
3.1 SAMOSTATNÉ AUTONOMNÍ ZAŘÍZENÍ.....	24
3.2 PC.....	24
3.3 KOMBINACE.....	25
3.4 TYPY PŘENOSŮ.....	25
3.4.1 Telefonní linka (JTS).....	26
3.4.2 Telefonní linka v nad-hovorovém pásmu.....	27
3.4.3 ISDN – digital.....	27
3.4.4 Sítě mobilních operátorů GSM.....	27
3.4.5 Rádiový přenos.....	28
3.4.6 Datový spoj přes internet.....	29
3.4.7 Kombinovaný přenos.....	30
3.5 ZPRÁVY NA PCO.....	31
3.6 PŘENOSOVÉ FORMÁTY.....	31
3.7 ANALÝZA SOUČASNÉHO STAVU PCO.....	32
4 SOFTWARE A UŽIVATELSKÉ MOŽNOSTI	34
VLASTNOSTI, KTERÉ BY MĚL UŽIVATELSKÝ SOFTWARE NABÍDNOUT.....	35
4.1 OKNO UDÁLOSTÍ.....	35
4.2 SEZNAM OBJEKTŮ.....	36
4.3 MAPOVÉ PODKLADY.....	38
4.4 HISTORIE DNE A HISTORIE OBJEKTU.....	39
4.5 SHRNUÍ.....	39
5 PCO RADOM	41

5.1	PŘENOS INFORMACÍ V PRIVÁTNÍ RÁDIOVÉ SÍTI.....	41
5.2	PŘENOS INFORMACÍ PO PEVNÝCH TELEFONNÍCH LINKÁCH.....	43
5.3	PŘENOS INFORMACÍ POMOCÍ SÍTĚ GSM/GPRS.....	44
5.4	ZAŘÍZENÍ PITBUL.....	45
5.5	PŘENOS INFORMACÍ POMOCÍ SÍTĚ ETHERNET.....	45
5.6	UŽIVATELSKÝ SOFTWARE RADOM SECURITY WRS32.....	46
5.7	SHRnutí SYSTÉMU RADOM.....	47
6	PCO NAM.....	49
6.1	STRUKTURA RÁDIOVÉ SÍTĚ GLOBAL.....	49
6.2	RÁDIOVÁ SÍŤ GLOBAL 2.....	50
6.3	PŘENOS ZPRÁV NA PCO RÁDIOVOU SÍŤÍ V PÁSMU 400 AŽ 470 MHZ.....	51
6.4	PŘENOS ZPRÁV NA PCO POMOCÍ SÍTĚ MOBILNÍCH OPERÁTORŮ.....	53
6.5	PŘENOS ZPRÁV NA PCO VYUŽITÍM TELEFONNÍCH LINEK.....	54
6.6	PŘENOS ZPRÁV NA PCO POMOCÍ SÍTĚ INTERNET.....	54
6.7	SOFTWARE NET- G.....	55
6.8	SHRnutí SYSTÉMU NAM.....	56
7	SPOLEČNOST TRADE FIDES.....	57
7.1	LATIS SQL.....	58
7.2	SLOŽENÍ LATIS SQL.....	58
7.3	STRUKTURA LATIS SQL.....	58
7.4	SYSTÉM ŘÍZENÍ LATIS SQL.....	60
7.5	PROGRAM LOW.....	61
7.6	SHRnutí SYSTÉMU SPOLEČNOSTI FIDES.....	61
8	TRENDY V OBLASTI INFORMAČNÍCH TECHNOLOGIÍ VYUŽITELNÉ PRO PCO.....	63
8.1	VZDÁLENÁ SPRÁVA A MONITOROVÁNÍ.....	63
8.1.1	Využití pro PCO.....	63
8.2	TRENDY V OBLASTI ZPRACOVÁNÍ OBRAZOVÉ INFORMACE.....	64
8.2.1	Využití pro PCO.....	64
8.3	ŘEŠENÍ GEOVISION.....	65
8.3.1	Využití pro PCO.....	65
8.4	NAVIGAČNÍ TECHNOLOGIE GPS.....	66
8.4.1	Funkce systému GPS.....	66
8.4.2	Využití pro PCO.....	67
8.5	GEOGRAFICKÉ INFORMAČNÍ SYSTÉMY (GIS).....	67
8.5.1	Využití pro PCO.....	68

8.6	DATABÁZE.....	68
8.7	DATABÁZE A PCO.....	69
8.8	CLOUD COMPUTING.....	70
8.8.1	Využití pro PCO.....	70
8.9	3D VIRTUÁLNÍ REALITA.....	71
8.9.1	Využití pro PCO.....	71
8.10	PROGRAM NEWTON.....	71
8.10.1	Využití pro PCO.....	72
8.11	MALÉ SOFTWAREVÉ APLIKACE POUŽITELNÉ PRO PROVOZ PCO.....	72
8.12	SHRNUTÍ IT.....	72
9	TRENDY V OBLASTI PCO.....	74
9.1	INTEGRACE BEZPEČNOSTNÍCH TECHNOLOGIÍ.....	74
9.2	DALŠÍ MOŽNOSTI UŽIVATELSKÉHO SOFTWARE.....	75
9.3	VYTĚŽOVÁNÍ INFORMACÍ Z TECHNICKÝCH ZAŘÍZENÍ.....	76
9.4	BEZPEČNÝ DŮM FIRMY BETA CONTROL, VÝTAHOVÉ SYSTÉMY.....	77
9.5	TRENDY V OBLASTI PŘENOSU.....	77
9.6	VZÁJEMNÉ PROPOJENÍ PCO.....	78
	9.7 SHRNUTÍ	78
	ZÁVĚR.....	80
	ZÁVĚR V ANGLIČTINĚ.....	81
	SEZNAM POUŽITÉ LITERATURY.....	82
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....	84
	SEZNAM OBRÁZKŮ.....	85

ÚVOD

Úroveň kriminality i vlivem hospodářské krize roste a je třeba jí čelit všemi dostupnými prostředky. Nejruznější krádeže, vloupání a jiné trestné činnosti se staly běžnou záležitostí a potřeba chránit sebe a svůj majetek se neustále zvyšuje. Ochrana mechanickými a technickými prostředky může být sebevíc účinná, ale pokud nedojde k zásahu lidskou rukou, ztrácí potřebnou efektivitu. Stálá fyzická ostraha objektů je využívána zejména v rozsáhlých firemních závodech, areálech a obchodních centrech. Pro menší objekty, provozovny, byty a rodinné domy je nejefektivnější řešení bezpečnosti připojením na pult centralizované ochrany (PCO). Pulty centralizované ochrany slouží jako prostředek ochrany majetku a osob, kdy je pomocí zvoleného přenosového kanálu operátor vyrozuměn o způsobeném poplachu v objektu zákazníka. Žádný střežený objekt není možné ochránit na 100%, jelikož zde vždy figuruje určitý časový interval od napadení objektu do příjezdu zásahové skupiny. Tuto dobu se snaží výrobci i provozovatelé PCO zkrátit na minimum.

Je třeba si také uvědomit, že zaměstnanci bezpečnostních agentur nemají žádné speciální pravomoci a veškerou svoji činnost bez výjimky provádějí v rámci platných zákonů ČR.

Cílem práce je z různých hledisek zhodnotit pulty centralizované ochrany, popsat jejich funkci, perspektivu a vliv na rozvoj PKB. Jsou zde uvedeny tři, v ČR nejúspěšnější výrobci, jejich specifické vlastnosti včetně trendů a předpokládaného vývoje. Úroveň technické vyspělosti těchto zařízení je na vysoké hodnotě a neustále se zdokonaluje. Podobně je na tom i přenos informací na PCO s ohledem na bezpečnost.

V otázce budoucnosti je již téměř jisté, že dojde k jejich aplikaci na tzv. inteligentní budovy. Zde dojde k nárůstu dalších požadavků na nové funkce zpracovávání velkého množství příchozích dat.

1 CHARAKTERISTIKA PULTŮCENTRALIZOVANÉ OCHRANY

Pult centralizované ochrany (PCO) je dispečerské zařízení, vybavené výpočetní technikou, která vyhodnocuje poplachové a informační stavy z EZS instalovaného ve střeženém objektu. Zprávy jsou na toto zařízení přenášeny různými způsoby (telefonní linkou, mobilní sítí, radiovou sítí atd.). PCO tedy slouží k vyhodnocování údajů přenášených z EZS střeženého objektu. Výstupy ze systému jsou zpracovány speciálním uživatelským programem, který umožňuje podrobný přehled o stavu střeženého objektu a nabízí i nejrůznější doplňkové služby pro snadnější práci a efektivní reakci na vznik dané události. Po vyhodnocení poplachového signálu se vyrozumí - dle smluvních podmínek: zákazník, oprávněná osoba, policie či havarijní služba, nebo se vydá pokyn zásahové jednotce k provedení předepsaných činností. Pokud dojde k narušení objektu, je tento prověřen výjezdovou skupinou. Elektronická forma ostrahy objektů je klienty preferována vzhledem ke snadné dostupnosti a relativně nízkým pořizovacím nákladům elektronických zabezpečovacích systémů (EZS).

2 VZNIK PCO

S využíváním PCO se začalo v roce 1976. Policie byla nucena řešit zvýšený nárůst trestné činnosti. Bylo potřeba vyřešit otázku ekonomicky výhodného a efektivního zabezpečení objektů v rámci prevence kriminality, zaměřit se na rizikové oblasti s cílem minimalizace následných škod, minimalizovat rizika vloupání a zvyšovat zabezpečení i v rámci požadavků pojišťoven. Hledal se také vhodný způsob zabezpečení, který by byl stejně efektivní a ekonomicky výhodnější než zajišťování fyzické ostrahy. Elektronická zabezpečovací signalizace, která v místě poplachu pouze aktivuje zvukovou signalizaci, již není dostatečně efektivní a rozhoukaná siréna v objektu spíše budí pocit rozčilení, zejména v nočních hodinách. Četnost incidentů byla v porovnání s počtem hlídaných relativně nízká, a proto vznikla určitá možnost integrace, tedy zajištění ochrany více objektů z jednoho pracoviště. To mělo za následek vznik tzv. koncentrátorů poplachových hlášení, tedy pultů centralizované ochrany, jako dálkovým dohledem nad střeženými objekty. V dnešní době má však PCO daleko širší význam a zahrnuje také širší okruh činností, než tomu bylo v minulosti.

2.1 Soukromé bezpečnostní služby

Se změnou politického systému byl na počátku 90. let velký rozmach podnikání. Zvýšený počet provozoven, zvýšená kriminalita a zvýšená potřeba chránit svůj majetek otevřely trh pro soukromé bezpečnostní služby. Ty brzy pochopily, že okolí se stává lhostejným k akustickým signalizacím na objektech a policie nestačí technicky ani lidsky připojovat všechny žadatele na své pulty centralizované ochrany. Právě v této době začínají soukromé bezpečnostní služby používat pulty centralizované ochrany. Z počátku byly PCO linkové s přenosem po telefonní lince.

2.2 Městské policie

Policie ČR nestačila na začátku 90. let řešit nárůst trestné činnosti. Na základě zákonných ustanovení začaly obce a města zřizovat městské a obecní policie. Vzhledem k tomu, že ne ve všech městech či obcích byly soukromé bezpečnostní agentury ekonomicky silné na to, aby zbudovaly PCO, ujaly se této problematiky také městské policie. Co se týká technického vybavení, vlastně kopírovaly soukromý sektor a dnešní typy PCO se neliší od těch používaných soukromými bezpečnostními službami. V počátečním rozvoji této služby

byla myšlenka chránit městský či obecní majetek (školy, divadla, radnice atd.). Časem však některé pulty městské policie začaly komerčně využívat PCO a konkurovat tak soukromým bezpečnostním službám. [9]

2.3 Historie technického vývoje PCO

Původní PCO byly linkové s přenosem signálu po jednotné telefonní síti. Komunikace mezi střeženým objektem a PCO se zdokonalovala s rozvojem polovodičové techniky. První jednoduché tranzistorové spínací obvody dokázaly přenášet pouze informaci, zda v objektu poplach je a nebo není. Zařízení PCO byla navíc příliš velká a těžká. Další nevýhodou bylo, že objekt nebo jeho části se nedaly střežit za provozu, protože zvednutí sluchátka telefonu způsobilo přerušování přenosové trasy a vyhlášení poplachu. Poplach ve střeženém objektu byl na PCO signalizován rozsvícením žárovky. S příchodem mikroprocesorové techniky se zdokonalila efektivita elektrické zabezpečovací signalizace i komunikace mezi střeženými objekty a přijímacím dispečerským pracovištěm. První PCO, využívající telefonní linky, pocházely ze zemí východního bloku a to ze SSR nebo Bulharska. Teprve v roce 1988 byl zaveden PCO typového označení TVRZ, jehož výrobcem byl podnik METRA Blansko. Spojení mezi hlídaným objektem a pultem centralizované ochrany probíhalo pomocí telefonních linek, ale v tzv. nadhovorovém pásmu. Šlo o frekvenci 20 kHz. Nevýhodou zařízení byla nutnost požádat tehdejšího poskytovatele telekomunikačních služeb o instalaci speciálního prvku, výkonového dílu do telefonní ústředny. Výkonový díl byl koncentrátorem nadhovorových přenosů po telefonních linkách. Objekt se mohl střežit i za provozu a v případě poruchy či přestřížení telefonního vedení byla tato událost zaznamenána. [9]

Linkové PCO byly na začátku 90 let značně závislé na telefonní síti. Ta byla v té době analogová, značně nespolehlivá, riziková a kapacitně nevýkonná. Vždyť na přidělení telefonní linky do objektu, a tím i vytvoření přenosové trasy pro poplachové zprávy se čekalo i měsíce. Poskytovatelé PCO se tedy snažili přejít na jiný a technicky spolehlivější způsob komunikace a tímto směrem byl směřován i výzkum a vývoj. Situaci zlepšila až nabídka radiových PCO našich výrobců. Pro používání u Policie ČR byl v roce 1992 schválen rádiolinkový obousměrný systém PCO FAUTOR od firmy Fides. V roce 1993 se

z TESLY vyčlenila společnost Radom s.r.o., nabízející pulty centralizované ochrany pod označením RADOM SECURITY.

Přenos zpráv na PCO rádiovou cestou byl podmíněn vytvořením vlastní rádiové sítě. Potom bylo možné pomocí rádiového vysílače v objektu a přijímače na straně PCO přenášet zprávy z EZS. [10]

Rádiové spojení bylo a je s velmi dobrou spolehlivostí používáno dodnes a to zejména v rovinných nebo klimaticky příhodných oblastech. Dá se říci, že používáním radiových PCO jsme v Evropě takovou raritou. Pramení to ale z toho, že v jiných západních zemích při rozvoji PCO měli velmi kvalitní telefonní sítě, a tak nemuseli zavádět alternativní přenosové trasy.

2.4 Obecné požadavky na provoz PCO

Základní funkcí PCO je vyhodnocovat zprávy z bezpečnostních i jiných zařízení zákazníka, které tyto informace odešlou na tento pult. Operátoři PCO pak provádí, dle typu události kroky, vedoucí k vyřešení přijaté zprávy dle smlouvy a směrnic dané služby.

Dálková ochrana přes pult centralizované ochrany je v dnešní době jedním z nejspolehlivějších způsobů, jak ochránit majetek.

Kvalita poskytovaných služeb je závislá na rychlosti zásahu, profesionalitě zaměstnanců a technice přenosu dat. Správně provedený zásah je veden tak, aby byly na nejnížší možnou míru sníženy škody na napadeném objektu ze strany pachatele i ze strany zasahujících pracovníků. Velmi důležitý je důraz na ochranu života a zdraví všech účastníků zásahu.

Rychlost zásahu je nejvíce ovlivněna dojezdovým časem, tedy dobou, kterou potřebuje vozidlo zásahové skupiny k přesunu z místa svého stálého stanoviště do místa napadeného objektu. Tuto dobu ovlivňuje řada faktorů, kdy většinu z nich nelze ovlivnit (hustota provozu, kvalita a charakter provozu, počasí atd.). Mimo tyto vlivy je důležitá také vzdálenost nejbližšího stanoviště zásahové skupiny. Právě zde se projevuje výhoda vlastních vozidel – stanoviště jsou rozmístována tak, aby byla zákazníkům vždy co nejbliže.

Kvalita služeb také závisí na dobře definovaných a provedených postupech. Je důležité co nejvíce minimalizovat čas od vyhlášení poplachu do kontroly objektu, mít zpracovány velmi podrobné postupy, které musí každý pracovník dokonale znát a dodržovat. Má-li být zásah rychlý a hladký, nelze se spoléhat na improvizaci pracovníků. Jsou vytvářeny obecné a specifické scénáře (modelové situace), které jsou neustále zdokonalovány. Zaměstnanci jsou pravidelně přezkušováni nejen ze znalostí těchto postupů.

Bezúhonní a profesionální pracovníci jsou tedy další komponentou, jež je pro úspěšnou ochranu majetku naprosto nezbytná. Každý uchazeč o práci v zásahových skupinách musí splnit řadu kritérií (věk 21 let, trestní bezúhonnost, vlastnictví zbrojního průkazu a řidičského oprávnění, minimálně dvouletá praxe atp.). Mimo to je přísně zkoumána fyzická a psychická způsobilost k vykonávání činnosti. Pracovníci jsou pravidelně ze svých znalostí a dovedností zkoušeni a dále proškoleni k rozšíření potřebných profesních parametrů.

Volba správného způsobu přenosu dat z objektu na pult centralizované ochrany je podstatným rozhodnutím. Přenos dat musí splňovat základní požadavky: musí být kontrolovaný (přenosová cesta musí být odolná proti napadení pachatelem) a zprávu o poplachu je třeba co nejrychleji přenést na pult centralizované ochrany. Zařízení pro přenos dat musí být schopno předávat zprávy o všech stavech v objektu. [8]

K základnímu vybavení operačního střediska patří:

- homologovaný pult centralizované ochrany včetně záložního zdroje,
- speciální samostatné linky pro přenos signálů z EZS objektů do PCO,
- archivační počítač PCO s provozní databází všech střežených objektů,
- zařízení pro komunikaci (základnová vysílačka, pevný a mobilní telefon),
- aktuální archiv protokolů všech výjezdů zásahové jednotky,
- aktuální archiv strážních listů fyzické ostrahy,
- dokumentace (manuály, objektové směrnice, metodické pokyny, atd.).

Personální podmínky

Z hlediska personálního obsazení pracovišť PCO je trvalý požadavek na obsazení odborně

vyškoleným personálem. Obsluha PCO by měla splňovat tyto podmínky:

- umět řešit mimořádné situace,
- umět pracovat ve stresu a v časové tísní,
- znát PCO po technické a provozní stránce,
- umět komunikovat,

Požadavky na členy zásahových jednotek:

- disciplinovanost.
- fyzická zdatnost,
- perfektní znalost metodiky zásahu,
- znalost místopisu střežených objektů,
- zručnost a zkušenost při používání zbraně a ostatních donucovacích prostředků.

2.5 Integrace v provozování PCO

Poskytovatelé služeb PCO musí řešit otázku, zda PCO centralizovat (integrovat) na minimum pracovišť, řešit přenos dat centrálně a zásahové jednotky pracovišť PCO mít rozmístěné po celé ČR. Jde o diskutabilní otázku, vyhovující převážně ekonomicky i personálně silným firmám. Poplachovou informaci lze přenášet na velké vzdálenosti a to bleskově. Centralizací lze ušetřit náklady na personál dispečinku i technické náklady na zbudování PCO. Zásahová jednotka pak musí být co nejbližší objektu, ve kterém je zaznamenáván poplach. Problém spočívá v ekonomické efektivitě nebo-li vytíženosti. Velké firmy průmyslu komerční bezpečnosti jsou často v mylném domnění, že když vybudovaly nákladný technicky moderní PCO, musí mít větší inkaso poplatků, než zásahová firma v místě poplachu, což může být i firma čítající jen dvě desítky pracovníků. Každopádně pro centralizaci svědčí zlepšující se přenosové cesty, čemuž vyhovují jak sítě pevných telefonních linek, tak sítě mobilních operátorů. [8]

2.6 Služby na PCO

Služby na PCO u soukromých agentur jsou postaveny na komerčním základě. Provozovatelé nabízejí různé nabídky služeb, které se liší postupem dispečera po příjmu poplachové informace a samozřejmě také cenou. Konkurence je velká, a proto je třeba nabízet zákazníkům služby tzv. na míru.

Zde jsou uvedeny některé z příkladů služeb nabízených bezpečnostními agenturami. Pochopitelně se služby mohou prolínat nebo doplňovat.

- **Monitoring**

Základní nabídka služeb obsahuje vždy monitoring stavu bezpečnostního systému. Tato služba zaručuje sběr, vyhodnocení a archivaci příchozích zpráv. Pokud je přijata poplachová nebo jiná zájmová zpráva, operátor PCO předá tuto informaci na předem domluvené telefonní čísla zákazníka v daném pořadí. Je potom na zákazníkovi, zda situaci na objektu prověří sám a nebo vydá příkaz k výjezdu zásahové skupiny PCO. Při telefonních hovorech lze po domluvě ze strany zákazníka využívat i předem domluvených hesel pro identifikaci osoby, která rozhoduje o způsobu prověření poplachu.

- **Zásah**

Zásah znamená, že výjezdová skupina na základě poplachové zprávy jede na místo ověřit situaci, případně provést preventivní či represivní opatření v rámci zákona. Zásah je téměř vždy službou spojenou s monitoringem, protože lze těžko reagovat na něco, o čem nevíme. Zásahová skupina je vedena k cíli operátorem PCO a ten jim také předává aktuální informace o stavu v objektu.

Provozovatelé PCO mají dva přístupy k této službě. První z nich je, že v měsíčním paušálu jsou zahrnuty i případné všechny výjezdy k objektu. Ve druhém případě zákazník platí za každý výjezd.

Druhý případ je vhodnějším prostředkem jak zákazníka naučit být pozorným při obsluze bezpečnostního systému protože 90 % výjezdů je na základě poplachu způsobeného pracovníky zákazníka.

Postupy reakce dispečera můžou být různé dle smlouvy. Reakcí může být volání kontaktních osob, čekání na zrušení poplachu platným kódem či heslem, vyslání výjezdové skupiny po uplynutí intervalu pro zrušení, nebo okamžitý výjezd.

- **Patrol**

Patrol systém je preventivní nástroj ochrany objektů, je to v podstatě namátková fyzická ostraha. Provádí ho výjezdová skupina PCO. Jde vlastně o využití zásahové jednotky v době, kdy neprovádí zákrok na základě poplachové informace. Je to nástroj jak lépe využít času pracovníků zásahové jednotky v době jejich pohotovosti a zároveň zlepšit ekonomické výsledky.

Služba funguje tak, že výjezdová skupina v době své služby provádí dle harmonogramu preventivní kontroly stavu objektů a jejich okolí. Celá tato služba má preventivní charakter a působí na okolí podvědomím, že objekt není úplně bez kontroly. V případě přijaté poplachové zprávy je Patrol systém přerušen a prioritu má výjezd k napadenému objektu.

V činnosti Patrol systému potom hlídka pokračuje, pokud není vytížená kontrolou poplachů na hlídaných objektech.

- **Doplňkové služby**

Doplňkovými službami provozovatel PCO v podstatě vylepšuje komfort placených služeb. Jedná se například o vyrozumění odpovědné osoby, pokud není objekt v určitou dobu zastřežen. Je možné také zasílat SMS zprávy o stavu objektu. Například informace o tom, kdo a v kolik odemkl a zamkl objekt. Umožňuje-li to technické zařízení na objektu klienta, je možné provádět z dispečinku PCO vzdálenou správu elektronických zařízení (topení, klimatizace, osvětlení atd.), taktéž je možné informovat klienta o výpadku elektrické energie nebo poruchy telefonní linky.

Velmi rozšířenou službou jsou pravidelné měsíční nebo týdenní výpisy z historie objektu, zasílané poštou nebo v elektronické podobě. Ve výpisu jsou obsaženy všechny informace, které z daného objektu na PCO přišly. Je možné sledovat docházku do objektu, otevírací dobu mimo pracovní přístup zaměstnanců atd.

Jednou z nejrozšířenějších služeb je kontrola odkódování a zakódování objektu. Jde o službu, která klientovi umožní pomocí PCO kontrolu svého objektu, zda došlo k aktivaci či deaktivaci EZS v danou chvíli. V praxi to znamená, že v případě nezakódování objektu do stanoveného času je klient telefonicky informován, popř. SMS. U objektů, kde je vyšší riziko, či na přání klienta je možné okamžitě vysílat zásahovou skupinu.

Mezi další služby patří písemná zpráva o provedeném zásahu, kontrola automatických testů, funkční zkoušky EZS, prověření objektu v případě výpadku spojení při použití radiové sítě, rady a nabídky z praxe.

Na PCO lze také provozovat dálkový dohled pomocí kamerového systému CCTV, pokud jím střežený objekt disponuje. Dohled lze provádět v případě přijatého poplachu přímo v dané místnosti, a nebo v pravidelných intervalech.

- **Servis**

Pokud je provozovatel PCO zároveň i dodavatelem bezpečnostních systémů, může zákazníkovi nabídnout v rámci zvýšeného měsíčního paušálu služby za PCO také non-stop servis bezpečnostního zařízení. V praxi to znamená, že v případě servisních hlášek na PCO operátor PCO vyrozumí technika, který sám zákazníkovi nahlásí poruchu a domluví termín opravy. Zákazníkovi tak odpadá starost o kontrolu funkčnosti systému. Technik by měl být v pohotovosti 24 hodin tak, aby bylo možno provést okamžité opravy i v mimopracovní dobu.

- **Ostraha**

Ostraha se využívá v případě reálného napadení objektu. Výjezdová skupina provede zásah a v případě skutečného napadení objektu informuje zákazníka a Policii ČR. Provozovatel PCO by měl mít v záloze i pracovníky fyzické ostrahy, kterou je potřeba na místě zajistit do příjezdu zákazníka, popřípadě do začátku pracovní doby zaměstnanců v objektu. Fyzická ostraha je nutná, pokud po pachateli zůstaly škody na majetku např. rozbité dveře či okna. Nebo v případě zajištění stop popř. pokud není systém EZS plně funkční. I tato služba by měla být sjednána v rámci smlouvy.

Většina provozovatelů PCO v průmyslu komerční bezpečnosti nabízí služby od zajišťování fyzické ostrahy, montáže EZS, CCTV, EPS až po převozy hotovostí a cenin. Zákazník se pouze rozhoduje, kterou ze široké škály služeb využije pro ochranu svého majetku. [9]

2.7 Podmínky provozu dle CI ČAP

Vzhledem k prováděné činnosti by měl existovat požadavek na kvalitu provozu služby PCO a jejich produktů. V současné době neexistuje v ČR zákonná úprava, která by danou problematiku řešila. Z tohoto důvodu panuje v dané oblasti relativně velká benevolence a i kvalita je na různých úrovních. První, kdo se ujal tohoto úkolu a zpracoval podmínky provozu PCO je CI ČAP. Směrnice ČAP P 103 (1) Pulty centralizované ochrany, aplikační směrnice, požadavky [3], je první koncepčně zpracovaný materiál pro tato zařízení a služby. Norma udává veškeré technické, stavební i personální podmínky PCO včetně napájení, archivaci a podmínky pro komunikaci. Jedním ze základních požadavků je, že PCO musí fungovat nepřetržitě, s archivací poplachových zpráv minimálně a 1x za 24 hodin na dvě nezávislá místa. PCO musí být také stavebně upravené tak, aby bylo zabráněno přepadení dispečinku, tzn., že žádný z otvorů na plášti nevede do nestřeženého prostoru.

Dispečer má povinnost vlastnit zbrojní průkaz skupiny min. D, výsledek absolvovaných zkoušek nesmí mít horší než 2 a starší než 3 roky a musí předložit potvrzení o absolvování cvičných střeleb. Podobné požadavky platí i pro členy zásahových jednotek. Je-li například pro přenos na PCO používána telefonní linka, musí být její stav trvale hlídán a výpadek musí být signalizován jako poruchový stav nejdéle do 2 minut.

Norma obsahuje tyto a mnoho dalších náročných podmínek, které musí provozovatel splnit pro získání příslušného certifikátu.

Kromě požadavků normy ČSN EN 50 131-1 a její národní přílohy je přenos signálů na PCO a provoz PCO upraven normami řady ČSN EN 50 136. [1, 2]

2.7.1 PCO – Názvosloví a pojmy

Pro správné pochopení problematiky pultů centralizované ochrany je nutné objasnění si některých pojmů, obsažených v normě ČSN EN 50136-1-x a ČSN EN 50136-2-x – „Poplachové systémy a Poplachové přenosové systémy a zařízení“. Znalost a dodržování norem je pro provozovatele PCO nezbytná především pro uplatnění pojistných podmínek. V následujícím textu je uvedeno několik základních pojmů, bez kterých se nelze v problematice PCO správně orientovat.

2.7.1.1 *Názvosloví dle ČSN EN 50136 [1] a [2]*

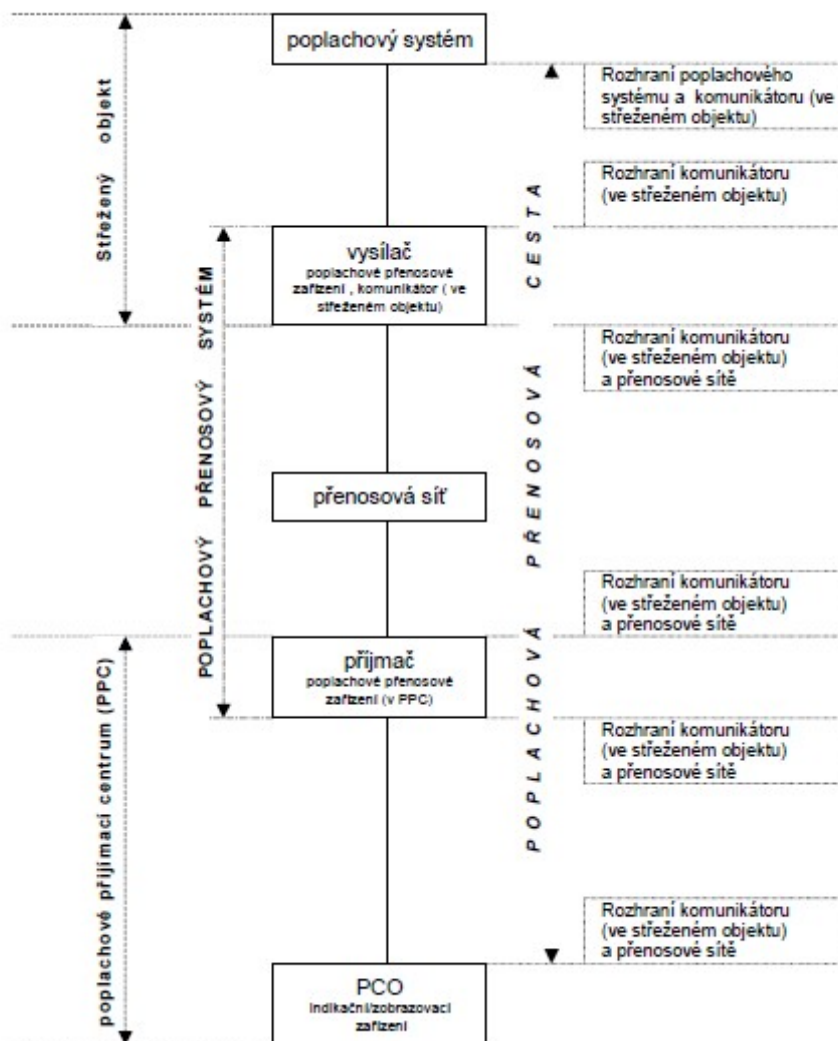
- STAV POPLACHU – Poplach – stav EZS nebo jeho komponentů, který je výsledkem odezvy nebo jeho části na přítomnost nebezpečí
- PCO (POPLACHOVÉ PŘIJÍMACÍ CENTRUM / PULT CENTRALIZOVANÉ OCHRANY) – trvale obsluhované vzdálené středisko, do kterého jsou předávány informace týkající se stavů objektů jednoho nebo více EZS
- POPLACHOVÝ SYSTÉM – elektrická instalace, která reaguje na ruční nebo automatickou detekci přítomnosti nebezpečí
- KOMUNIKÁTOR POPLACHOVÉHO SYSTÉMU – přenosové poplachové zařízení, které je umístěno ve střežených prostorách nebo satelitní stanici
- POPLACHOVÉ PŘENOSOVÉ ZAŘÍZENÍ – zařízení, které je především určené k přenosu poplachového hlášení na rozhraní poplachového systému ve střežených prostorech k rozhraní poplachového přenosového zařízení v poplachovém přijímacím centru a dále k ovládacímu a identifikačnímu/zobrazovacímu zařízení v poplachovém přijímacím centru
- POPLACHOVÝ PŘENOSOVÝ SYSTÉM – zařízení a síť, používané pro přenos informací, týkající se stavů jednoho nebo více EZS do jednoho nebo více PCO
- ZPRÁVA – řada signálů směřovaných sítí, která zahrnuje identifikaci, funkční data a různé prostředky pro zajištění její vlastní integrity, imunity a správného příjmu.

2.7.1.2 *Pojmy týkající se PCO*

V průmyslu komerční bezpečnosti je využíváno různých pojmů, pro jednodušší porozumění některých slovních obrátů a zkratk jsou zde vysvětleny některé základní pojmy, týkající se PCO.

- EZS – Elektrický zabezpečovací systém – je systém schopný zaregistrovat, vyhodnotit a oznámit vznik poplachového stavu objektu, ve kterém je nainstalován
- Poplach – výstraha při existenci nebezpečí pro život, majetek nebo okolní prostředí
- Dispečink PCO – je trvale obsazené pracoviště, na kterém jsou přenášeny informace o stavu objektů vybavených EZS. Obsluha pracoviště v případě potřeby iniciuje opatření čelící nebezpečí (řídí zásah)

- Zásahová jednotka – útvar soukromé bezpečnostní služby, provádějící po obdržení poplachového hlášení specifické úkoly potřebné pro ochranu ohroženého místa
- Přenosová cesta – funkční spojení mezi EZS a PCO
- Spojení s volbou – fyzické nebo logické spojení, které se musí pro přenos hlášení nebo kontrolu spojení teprve zřídit a po skončení přenosu opět zrušit
- Pevné spojení – fyzické nebo logické spojení, které je pro přenos hlášení nebo kontrolu spojení trvale k dispozici
- Rádiové spojení – bezdrátový způsob přenosu hlášení (simplexní či duplexní), využívající zajištěných rádiových frekvencí
- Záložní zdroj energie – soustava akumulátorů schopných opětovného dobití a disponující potřebnou kapacitou
- Náhradní zdroj energie – samostatný generátor elektrické energie
- Pracovník PCO – obsluha dispečinku PCO



Obr. 1 Blokové schéma poplachového přenosového systému [1]

Blokové schéma zobrazuje cestu poplachových zpráv na PCO. Ve střeženém objektu se nachází poplachový systém (EZS). Pokud systém detekuje narušení objektu nebo poruchu zařízení předá tuto informaci vysílači. Vysílač, neboli kodér, poplachovou informaci upravuje tak, aby jí bylo možné přenést skrz přenosovou síť, která je zvolena v závislosti na typu přenosu (tel. linka, GSM síť atd.). Na straně PCO je zpráva zpracována přijímačem (dekodérem) a předána softwarovému vybavení PCO.

3 SLOŽENÍ PCO

Pulty centralizované ochrany jsou zpravidla provozovány ve dvou variantách. Jako samostatný (autonomní systém), který je schopen samostatného provozu, nebo je provozován pomocí počítače.

3.1 Samostatné autonomní zařízení

Jde o samostatné, hardwarově realizované PCO zařízení, složené z elektronických obvodů. Zařízení většinou obsahuje sloty pro různé moduly např. telefonní linková karta, ISDN karta, radiokarta, karta pro tiskárnu. Jednotlivé karty mají svoji vnitřní paměť. Tím, že nevyužívají žádný operační systém, jsou velmi spolehlivé a málo náchylné k „padání“ systému. Na čelní straně takového systému většinou najdeme ovládací a programovací klávesnici a display. Zprávy jsou zobrazovány na displeji a při příchodu rovněž tisknuty na tiskárnu, protože displeje jsou max. dvouřádkové a zprávy by se ztrácely. Nevýhodou je, že zobrazují zprávy v číselném formátu. Chybí jim textový překlad, proto jsou méně adresné a rozklíčování číselného kódu zabere čas. Obsluha při příchodu zprávy musí za pomoci příslušné dokumentace zjistit, o jaký objekt se jedná, jaký typ zprávy je signalizován, případně ze které zóny je hlášen poplach.

Samostatná autonomní zařízení se v dnešní době již nepoužívají z důvodu malých uživatelských i technických možností. [9]

3.2 PC

PCO bývá realizováno osobními počítači využívající běžný operační systém. Bývají doplněny o telefonní, radiovou, GSM nebo ISDN kartu, zasunutou přímo po základní desky počítače nebo do zařízení mimo počítač. Toto zařízení pak komunikuje s PC přes USB či sériové rozhraní.

Jednotlivé karty mohou mít svoji vnitřní paměť až na tisíce událostí, pro případ výpadku nebo servisního zásahu na PC. Takovéto zařízení se občas nazývá Hardware PCO. Další nezbytnou součástí PCO v PC je Software. Je to vyhodnocovací a řídicí program, který zajišťuje komunikaci hardwaru PCO se softwarem počítače.

PCO provozované na PC musí mít funkční obě části SW i HW. Nevýhodou takovýchto zařízení je náročná záloha napájení v případě výpadku proudu. Běžné UPS záložní zdroje

vydrží cca ½ hodiny, což je velmi málo. Dále je zde zvýšený požadavek na stabilitu systému, jelikož zařízení musí vydržet nepřetržitý provoz.

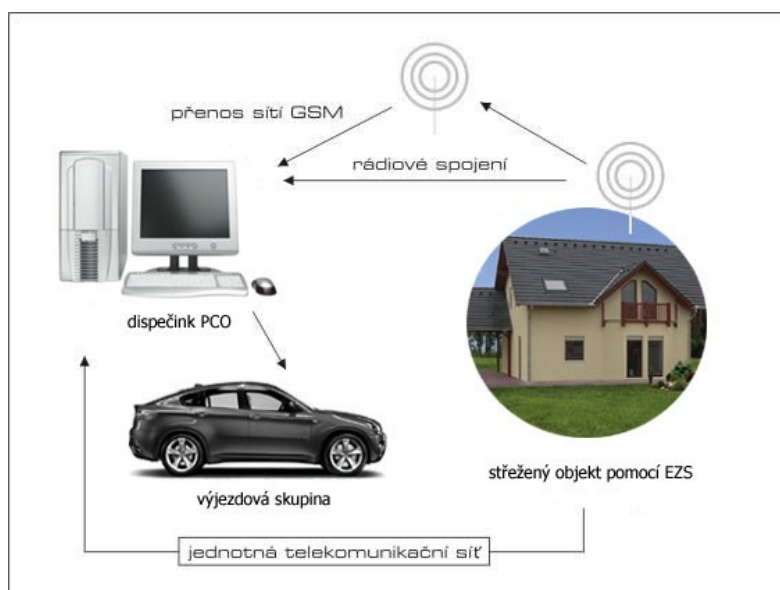
3.3 Kombinace

Uvedené dva druhy složení PCO lze kombinovat. Dříve než se začaly realizovat pulty ovládané výhradně počítačem, někteří provozovatelé používali kombinaci samostatného zařízení připojeného na monitor pro lepší obsluhu. Zařízení bylo lehce zálohovatelné v případě výpadku napájení avšak závislé na omezených funkcích používaného zařízení.

3.4 Typy přenosů

Přenos poplachových signálů z místa střežení na PCO je jednou z nejdůležitějších funkcí správně navrhnutého zabezpečení. Typy přenosů se liší náročností instalace, spolehlivostí a také pořizovacími a provozními náklady. Dnešní doba vyžaduje stále se zvyšující rychlost přenosových tras. Zde je výčet nejpoužívanějších komunikačních přenosových tras.

- telefonní linka
- sítě mobilních operátorů GSM
- rádiové sítě
- datový spoj přes internet



Obr. 2 Typy přenosů na PCO

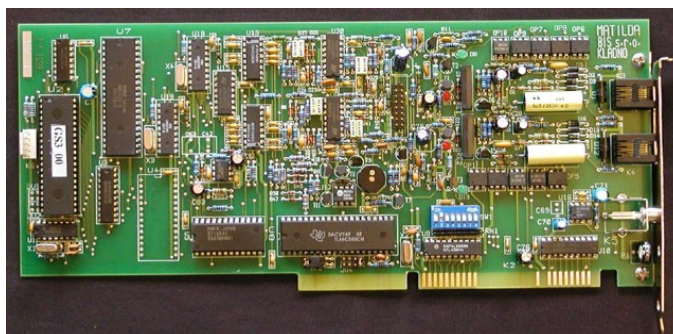
3.4.1 Telefonní linka (JTS)

Telefonní analogová linka byla dříve označována JTS – jednotná telefonní síť. Po této lince je i dnes přenášeno velké množství zpráv na PCO. Rozšíření těchto druhů přenosů sebou přinesla hlavně dostupnost a cena tohoto spoje. V objektech, kde je instalována EZS je ve většině případů rovněž telefonní linka. Tato se první připojí do ústředny EZS a následně se z ústředny EZS vytvoří připojení pro koncové zařízení. Takovéto připojení je vždy nutno dodržet, aby byla splněna podmínka priority vysílání informací ústřednou na PCO.

Další důvod rozšíření přenosu po telefonní lince je to, že každá ústředna EZS má v sobě zabudovaný telefonní komunikátor nutný pro přenos na PCO. Proto odpadají dodatečné náklady na pořízení dalších zařízení, jako je rádiový vysílač nebo GSM brána. Běžně se využívá testu spojení 1x za 24 hodin. Je třeba brát na vědomí, že předání zpráv dochází na základě sestaveného telefonního spojení. To znamená, že událost nebo soubor událostí představuje vlastně telefonní hovor. Každý tento hovor je tedy zpoplatněn dle tarifkace poskytovatele.

Na straně PCO jsou telefonní linky zapojené do telefonní karty. Karta je určena pro příjem zpráv z ústředny EZS a telefonních komunikátorů, jejich zpracování a předání vyhodnocovacímu softwaru. Bývá využíváno více linek a nastavení je takové, že když je jedna telefonní linka obsazena příjmem informací z jednoho objektu a na stejné číslo se pokouší předat informaci jiný objekt, telefon je přesměrován na volné telefonní číslo PCO. Vstupy telefonní karty se zapojí přímo do telefonních zásuvek.

Provozovatelé PCO by měli zajistit utajení telefonního čísla zapojeného PCO (nezveřejnění v telefonním seznamu), aby zamezili nechtěnému volání a tím blokování linek PCO. [9]



Obr. 3 Telefonní karta GS51 od firmy Matylida [19]

3.4.2 Telefonní linka v nad-hovorovém pásmu

Využití tohoto pásma přineslo možnost přenést poplachovou informaci z objektu na PCO pomocí telefonní linky bez přerušení pevné telefonní linky. Systém pracoval na frekvenci 20kHz, po které byla vyslána informace na PCO, kde se mohly zobrazit pouze 2 informace (signál buď byl, nebo nebyl). Výhodou přenosu byla nepřetržitá kontrola spojení. Využívání tohoto pásma je dnes spíše historií. Nevýhodou bylo omezené množství přenášených zpráv a nutnost vložení výkonového dílu do telefonní ústředny.

3.4.3 ISDN – digital

Tak jako u JTS je využíváno přenosové trasy používané pro hlasový přenos. Přenos po ISDN lince má tu výhodu, že se pro přenos poplachových zpráv používá datový kanál. Na jednom spojení tedy mohou bez omezení probíhat hlasové hovory a datové přenosy. Další výhodou je, že spojení mezi objektem a PCO je vlastně trvale hlídáno, při přerušení je ihned oznámena ztráta komunikace. Nevýhoda ISDN přenosu spočívá v tom, že na straně příjmu, tedy na PCO je potřeba mít ISDN kartu pro takový typ přenosů a na straně objektu mít záložní napájení takové linky. Tyto přenosy se v ČR příliš neujaly, zejména díky vyšší pořizovací ceně ISDN karty pro PCO a také proto, že s rozvojem ISDN v ČR byla větší priorita dána rozvoji mobilních sítí, které ISDN plně předběhly.

3.4.4 Síť mobilních operátorů GSM

Pro přenos poplachových informací z objektu na PCO lze využít síť mobilních operátorů GSM (Global System for Mobile Communications). Toto připojení je využíváno zejména v objektech bez telefonní linky a tam, kde není možno využít rádiový přenos. Systém přenosu zpráv je vyvinut pro provoz sítí GSM. Jedná se o mobilní síť druhé generace, kterou tvoří soustava tzv. BTS stanic pracujících na frekvenci 900/1800 MHz.

Přenos na PCO síť GSM v hovorovém pásmu je relativně nákladný vzhledem k tarifům mobilních operátorů. Z toho důvodu se neprovádí častá kontrola spojení a zprávy zastřežení se vůbec nepřenášejí. Finančně méně nákladnější je přenos s využitím GPRS, kde je možné za měsíční paušál přenést libovolný počet zpráv.

GPRS je mobilní datová služba přístupná pro uživatele GSM sítě. GSM komunikátor odesílá na PCO změny stavu na vstupu a také pravidelné kontrolní (testovací) zprávy. Tento typ přenosu informací má velkou perspektivu a to zejména z důvodu kvality pokrytí a nízkými provozními náklady v porovnání s cenami za hlasový přenos. Další výhodou je obousměrná komunikace mezi pracovištěm pultu centralizované ochrany a systémem instalovaným v objektu a téměř 99% pokrytí na území ČR. Navíc je možno provádět neustále test přenosové trasy a to v intervalu od 1 minuty výše.

V případě poruchy přenosové trasy, tj. ztrátě komunikace GPRS se zařízení automaticky přepne na náhradní přenosovou trasu a předá zprávu o výpadku GPRS přenosu. Po dobu poruchy tohoto spojení jsou veškeré zprávy přenášeny náhradní trasou. V případě potřeby obsluha může přenosovou trasu přepnout a zajistit si tak navázání spojení pro servisní zásah technika systému EZS.

Na straně příjemce zpráv, tedy PCO, je umístěn GSM přijímač, který umí přijímat zprávy ze sítě GPRS (např. přijímač SRX10G od firmy Radom). Přijímače můžou okamžitě po přijetí SMS zprávy z objektu odeslat tuto informaci na libovolné telefonní číslo např. zákazníka nebo člena zásahové jednotky. To umožňuje aktuální přehled o stavu bezpečnostního systému v objektu.

Další možností využití sítě GSM je přenos založený na přijímání SMS zpráv. SMS zprávy jsou odesílány z objektu prostřednictvím GSM brány. Na straně PCO je každý objekt identifikován na základě telefonního čísla, příchozí SMS zprávy jsou filtrovány pro příjem pouze od známých objektů.

3.4.5 Rádiový přenos

Jedná se o přenosovou cestu, kterou provozovatel PCO musí vytvořit. Stává se tudíž jejím správcem. Pro zřízení tohoto přenosu je nutné povolení a přidělení pracovních frekvencí od ČTÚ (Český telekomunikační úřad). Zřízení a vybudování vlastní rádiové sítě obnáší časovou a finanční náročnost. Před připojením objektu prostřednictvím rádiové sítě se v objektech provádí měření radiového signálu, aby byl zajištěn spolehlivý přenos zpráv. Velmi dobré uplatnění nachází v nížinách a příznivých klimatických oblastech, je možno zbudovat síť s velkým dosahem (např. 70 km). S náročnějším terénem a horšími klimatickými podmínkami rostou i náklady na zřízení kvalitních sítí (nutné retranslační stanice). Na straně zákazníka se instaluje vysílač naladěný na frekvenci provozovanou

poskytovatelem PCO. Výhodou pro zákazníka je beznákladový provoz za přenos informací na PCO. Další z výhod je kontrola spojení s objektem, prováděná 1 krát za minutu. Připojení je vhodné pro objekty, které nemají vlastní telefonní linku nebo je tato velmi poruchová. Někteří provozovatelé PCO vysílače do objektu s EZS zákazníkovi pronajímají za měsíční paušál, aby ho zbavili nutnosti do vysílače investovat. Rádiové sítě využívají duplexní, tedy obousměrný přenos a vysílače v objektech jsou využívány jako retranslační stanice (delší dosah pokrytí od základny). [9]

Nevýhodou je, že existuje určitá možnost rušení radiového signálu za použití silného vysílače, aniž by bylo nutno provádět další násilné akce (vstup na dispečink PCO, mechanické narušení autonomního systému apod.). Obsluha PCO sice má signalizován okamžitou ztrátu radiového spojení vysílače s dispečinkem, nemá však tušení, který objekt chce pachatel napadnout. Při velkém množství napojených objektů pak není naděje pokusit se o fyzickou ostrahu u těch, kde došlo ke ztrátě spojení.

3.4.6 Datový spoj přes internet

Internet přinesl do zabezpečovacích systémů a celkově do společnosti nové možnosti komunikace včetně obrazové a hlasové verifikace stavu objektu. V rámci PCO vznikla možnost vzdálené kontroly objektu a tím i úspory spojené se zbytečnými výjezdy zásahové jednotky.

Internet využívá dva základní typy transportních protokolů:

TCP - doručí zprávu vždy, ale může to být za velmi dlouho, až budou splněny podmínky pro navázání spojení.

UDP - doručí zprávu okamžitě, bez navázání spojení, pokud je teď cesta k příjemci volná. Pokud volná není, zpráva po určité době zanikne.

Cesta však často volná není, protože velké TCP pakety (fotografie, IP kamery, video-servery) přenos brzdí a nedovolí příjem malých UDP paketů. Jedna z hlavních úloh PCO je tedy zajistit příjem paketů UDP v každém okamžiku a zpomalit příjem TCP paketů.

Další hrozbou této přenosové trasy je možnost napadnutí zvenčí. Internetové sítě také často vypadávají a poskytovatelé jsou většinou malé soukromé firmy. Nelze se tedy spolehnout na okamžitou odbornou opravu.

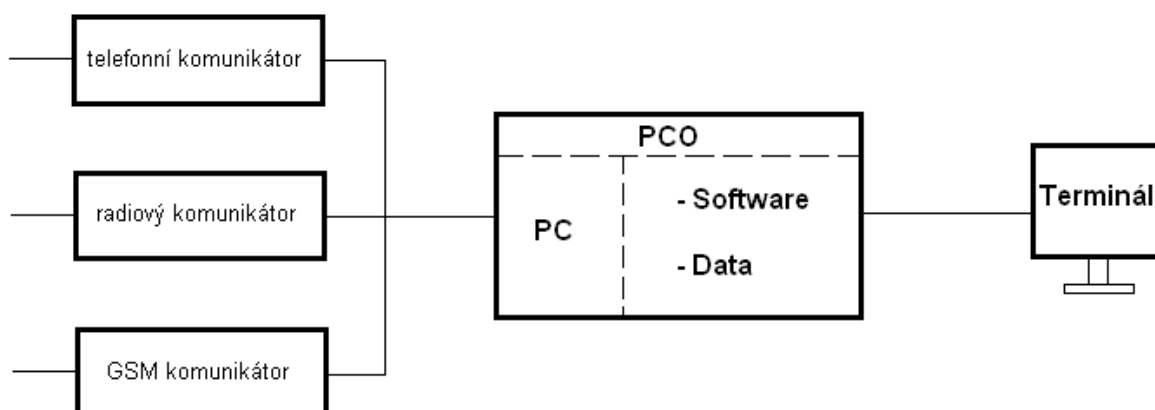
3.4.7 Kombinovaný přenos

Pro bezpečnější přenos informací se využívá kombinace dvou výše uvedených druhů přenosů. Nejčastěji se volí varianta JTS a RADIO nebo JTS a GSM. Prioritně je například přenos zpráv zajištěn po radiu a paralelně nebo záložně po JTS. V případě, že PCO nedostane kontrolní zprávu z objektu například v intervalu pěti minut, nebo když ústředna EZS v objektu nedostane potvrzení o příjmu vyslané zprávy, je využita náhradní (záložní) přenosová trasa např. po JTS. Tímto opatřením se má zabránit, že případný pachatel vyřadí přenosovou cestu a na PCO nepříjde žádná zpráva. Narušení obou přenosových cest v jediném okamžiku je prakticky neproveditelné. Pokud pachatel přestřihne nebo zruší telefonické vedení, ústředna EZS toto vyhodnotí a zašle poplachovou zprávu na PCO.

V případě narušení radiové cesty je PCO vygenerována zpráva o nepřijetí kontrolního telegramu a v případě napadení objektu může být zpráva předána po náhradním kanále (JTS).

U všech objektů je důležité posouzení přenosu přímo na místě a rozhodnout se podle situace technické i finanční. Instalaci a provozu včetně zvolení druhu přenosu poplachových zpráv je třeba věnovat mimořádnou pozornost. Zákazník si dnes již může vybrat, který způsob přenosu poplachových informací využije pro svůj objekt. Důležitá je také vzdálenost objektu od PCO. Pro lepší spolehlivost a splnění pojistných podmínek se instalují dva typy přenosů v případě přerušení trasy jednoho z nich.

Systémy se budují tak, aby informace o poplachu byla v co nejkratším čase přenesena, zpracována a správně vyhodnocena.



Obr. 4 Blokové schéma PCO

Zařízení PCO je zobrazeno na obr. č. 4. Poplachové zprávy přicházejí z komunikátorů do PCO, kde jsou zpracovány a zobrazeny na terminálu pro obsluhu.

3.5 Zprávy na PCO

Jedná se o zprávy, které jsou vysílány bezpečnostním systémem, instalovaným ve vzdáleném objektu. Vhodným programováním se definují typy a adresy zpráv, které budou vysílány z objektu a následně přijímány na PCO.

1. Poplachové zprávy: jsou nejdůležitější informace přenášené z bezpečnostního systému a jsou z hlediska přenosu prioritní. Uživatelský software na PCO okamžitě zobrazí napadené místo a umístění detektoru, který hlásí poplach. Součástí poplachových zpráv je tzv. panik poplach (ohrožení zdraví nebo života). Dalšími typy jsou poplachu: sabotážní, požární, pohybový, otřesový.
2. Poruchové zprávy: jsou druhé nejdůležitější přenášené informace. Informují pracovníka PCO o poruchách bezpečnostního systému. Jedná se zejména o tyto poruchy: porucha napájení, záložního zdroje, porucha sirény, výpadek telefonní linky. Operátor po přijetí těchto zpráv informuje obsluhu bezpečnostního systému případně servisního technika.
3. Testovací zprávy: bezpečnostní systém informuje v předem určených časových intervalech PCO zprávou „Automatický test“, která oznamuje, že přenosová trasa je funkční.
4. Ostatní zprávy: Mají informační charakter, některé SBS je nepoužívají. Jedná se zejména o tyto zprávy: aktivace/deaktivace bezpečnostního systému, odemčení/uzamčení dveří, práce technika atd.

Uživatelský software odděluje typy zpráv barevným zobrazením a akustickou signalizací. Navíc ukládá a hlídá zprávy, kterými dispečer na přijetí poplachu reaguje. Tyto zprávy se nazývají „operátorské“ a jsou to například: voláno do objektu, vyslána zásahová jednotka, volána PČR, prohlídka objektu bez závad, příčina poplachu nezjištěna atd.

3.6 Přenosové formáty

Přenosové formáty jsou programovány v ústřednách či komunikátorech EZS. Jedná se vlastně o „kódovanou,“ zprávu (informaci), kterou bezpečnostní systém předává po

přenosové trase do PCO. Na straně PCO je zpráva přeložena (dekódována) a následně zobrazena na monitoru operátora. PCO potvrdí bezpečnostnímu systému přijetí této informace.

V České republice je jedním z nejrozšířenějších formátů 4+2 (první čtyři čísla znamenají číslo objektu + další dvě čísla jsou kód zprávy). Jde tzv. pulsní formát vysílaný po analogové lince. Mezi analogové formáty patří např. 4+2,4+3,4+1 Ademco expres, Radionics. Všechny tyto formáty využívají přenosové rychlosti 1200,2400, 4600 ... dB/s a záleží jen na typu PCO se kterým formátem a rychlostí dokáže pracovat. Dalším druhem formátů jsou tzv. tónové (DTMF), mezi které patří např. Contact ID. Je využíván u ústředn vyší generace a tzv. velkokapacitních bezpečnostních ústředn. Doporučuje se u systémů, které mají až 99 podsystémů a více než 999 poplachových zón. Tento formát má 15 čísel.

PCO odpovídá ústředně dvěma signály, které jsou nazvány Handshake a Kissoff

Handshake

Handshake generuje PCO po zvednutí linky a potvrzuje ústředně připravenost přijmout data a průchodnost přenosové cesty. Handshake musí přesně časově a frekvenčně odpovídat následujícímu předpisu, jinak ústředna nezačne posílat data.

Kissoff

Signál Kissoff oznamuje ústředně, že PCO přijal zprávu bez chyb. Kissoff je tón v Hz (např. 1400 Hz) $\pm 3\%$ s dobou trvání minimálně 750 msec – max 1 sec. Ústředna musí detekovat minimálně 400 msec signálu Kissoff, aby byl signál vyhodnocen jako „platný“.

Ústředna akceptuje odchylku frekvence $\pm 5\%$ pro zpětnou kompatibilitu.

Pokud ústředna nevyhodnotí Kissoff musí zprávu poslat minimálně 4x a teprve potom může telefonní linku položit a vytáčet znovu. Čítač posílání zpráv je pro každou zprávu samostatný a je resetován vždy po zachycení signálu Kissoff.

Bezpečnostní ústředny využívají hexadecimálního (šestnáctkového) kódování. [9]

3.7 Analýza současného stavu PCO

Dnešní pulty centralizované ochrany v průmyslu komerční bezpečnosti nabízejí velké množství služeb pro lepší komfort zákazníka. Tyto agentury SBS se většinou nezabývají

pouze provozováním PCO, ale poskytují služby od zajišťování fyzické ostrahy, převozy cenin a hotovostí, návrhy a instalace EZS, přístupové systémy atd. Podobně také funguje využívání výjezdových skupin, pokud není zásahová jednotka právě na cestě k ověření poplachové zprávy. Tito pracovníci provádějí většinou patrol kontroly, převozy poštovních zásilek nebo jiné činnosti pro klienta či poskytovatele.

Pro přenos poplachových signálů na PCO se stále využívá telefonní, GSM i radiový přenos neboť každý má své nesporné výhody a možnost použití na daném objektu. Největší poptávka je však po radiové síti.

Z hlediska technického vybavení je výhradně používána výpočetní technika s dokonalou a přehlednou softwarovou nadstavbou. Uživatelský software PCO dokáže rozlišit druhy poplachů příslušným zvukovým znamením a barvou, umožňuje časové filtry např. pro uzamčení objektu, databázi poplachů a mnoho dalších užitečných funkcí. Samostatné autonomní systémy se již nepoužívají z důvodu omezených funkcí a uživatelských možností. Počítače je zcela vyřadily. Složení PC se liší v závislosti na zvoleném druhu přenosu.

Nejpoužívanějším druhem spojení s EZS je rádiové pásmo z důvodu nízkých provozních nákladů.

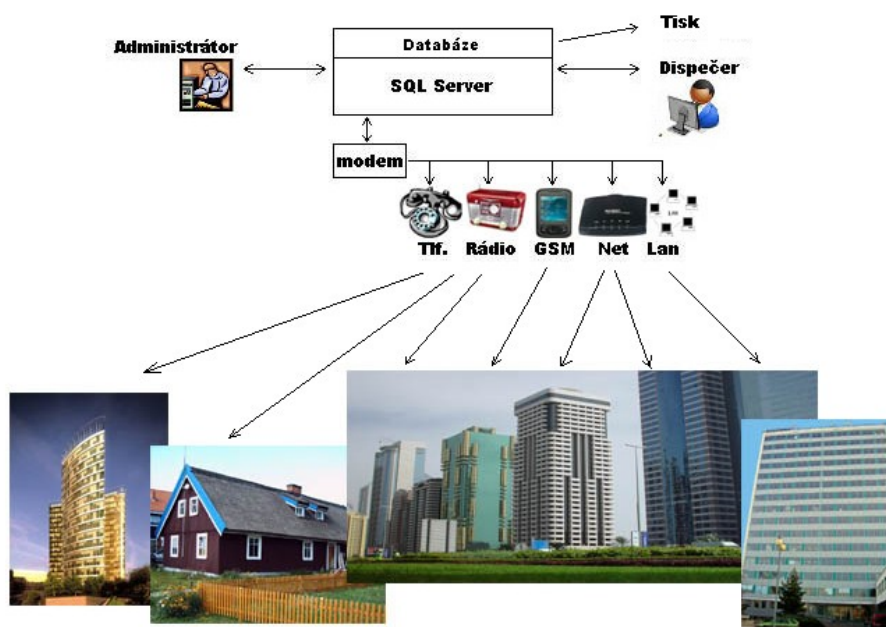
Přenosy po telefonních linkách se dají stále uplatnit. Například výrobce Genova se zabývá výrobou PCO s komunikací výhradně po telefonních linkách. Internet přináší možnost přenosu obrazu a zvuku ze střeženého objektu a tím lze minimalizovat náklady se zbytečnými výjezdy zásahové skupiny.

Pokud nechce zákazník budovat rádiovou síť, je vhodným řešením přenos pomocí sítě GSM prostřednictvím GPRS, jelikož mobilní operátoři mají pokrytí téměř 99% území ČR a přenos GPRS je relativně levný.

4 SOFTWARE A UŽIVATELSKÉ MOŽNOSTI

Uživatelský software vznikl s potřebou rychle a bezpečně zpracovávat větší množství přijatých informací na PCO. Jeho úkolem je jasně a přehledně zobrazovat přijaté zprávy tak, aby byl operátor schopen co nejrychleji reagovat na vzniklou událost. Důležitou vlastností je přehlednost a názornost zobrazované zprávy, zvukový doprovod, barevné odlišení dle důležitosti atd. Bývá doplněn o celou škálu dalších užitečných funkcí pro efektivnější práci. V současné době se do těchto aplikací promítá velké množství grafických prvků, jako jsou schémata, mapy, modely a fotografie pro přehlednější práci.

Jádrem systému je databázová aplikace, která dokáže zpracovávat a bezpečně uchovat velké množství informací. Díky své spolehlivosti je často využíván Microsoft SQL Server. Uživatelský software je stejně jako většina aplikací složen z několika modulů, které představují určité ovládací a funkční vlastnosti. Jednotlivé moduly lze do programu doinstalovat a rozšířit funkce celého systému. Každý tento modul zastává danou operaci (např. modul pro příjem zpráv, modul zastávající automatické funkce, modul dálkové komunikace, modul pro hromadné zpracování výpisů atd.).



Obr. 5 Jednoduché schéma funkce střežení

Zprávy ze střeženého objektu jsou daným komunikačním kanálem přijaty ke zpracování příslušným modulem systému (modemem) a pomocí SQL Serveru uloženy do databáze. Zde jsou pod přihlášením uloženy tak, aby nedošlo k jejich neoprávněnému užívání.

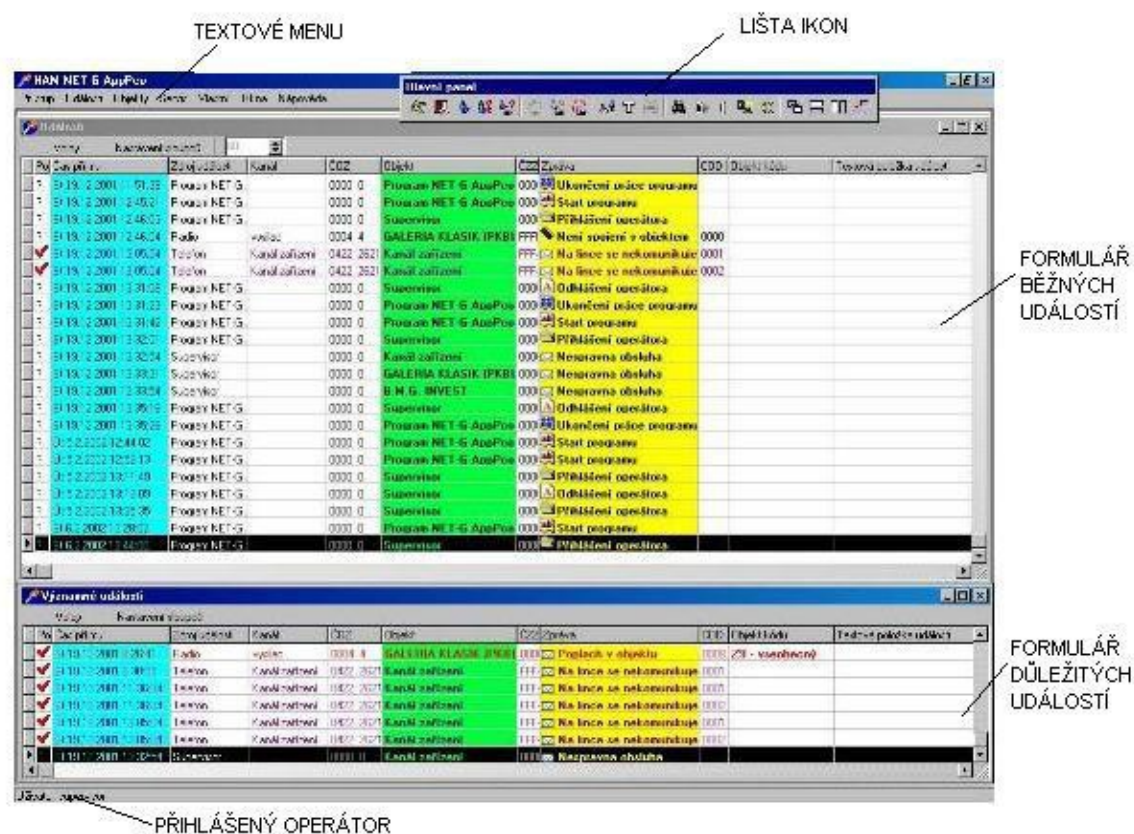
Uživatelský software se v pravidelném časovém intervalu dotazuje databáze na aktuální stav. Jestliže je v databázi nový údaj, zobrazí se na monitoru obsluhujícího pracovníka.

Vlastnosti, které by měl uživatelský software nabídnout:

- **Přihlášení** – dispečer se do systému pomocí jména a hesla přihlásí, aby se dalo bezpečně ukládat a případně zpětně zjistit, kdo a ve který den na PCO pracoval. Operátoři mohou mít také rozdílné úrovně přístupu, které jsou předem definovány správcem systému (administrátorem). Ten je po přihlášení schopen veškerého nastavení systému.
- **Okno událostí** – nejdůležitější část aplikace, zde dochází k zobrazování zpráv z objektů.
- **Karta objektu** – Zde jsou definovány veškeré vlastnosti každého z připojených objektů. Dispečer si může kdykoliv kartu otevřít a podívat se na vlastnosti daného objektu, adresu, kontakt na majitele, včetně grafického zobrazení a fotografií.
- **Vyhodnocování a zobrazování** síly rádiového signálu (kontrola spojení)
- **Modul automatických činností** – stará se všechny automatické operace, které musí systém kontrolovat a vykonávat (hlídání doby střežení, odesílání automatických povelů, informování zákazníka atd.)
- **Historie dne** – umožňuje nahlédnout na seznam příchozích zpráv zvoleného dne.
- **Historie objektu** – zpětné zjištění všech příchozích zpráv z daného objektu v určitém časovém období. Tento seznam je většinou měsíčně zasílán zákazníkovi poštou nebo mailem dle jeho přání.
- **Grafické zobrazení** (mapové podklady)
- **Servisní funkce** – upozornění obsluhy v případě výpadku spojení, napájení či jiné poruchy.

4.1 Okno událostí

V tomto okně jsou zobrazovány příchozí události, které mají být na daném pracovišti PCO řádně vyhodnoceny. Většinou se používá řádkové zobrazení zpráv, které postupně plní obrazovku. Zprávy se posunují do historie a nově příchozí se řadí na první pozici. Pro lepší přehlednost jsou příchozí zprávy barevně rozlišeny.



Obr. 6 Monitorovací software NET-G [12]

Na obr. 6 je znázorněn příklad okna událostí, tedy základní obrazovky softwaru NET-G společnosti NAM. Kliknutím na jednotlivé části se zobrazí příslušné informace.

Barevné rozlišení napomáhá k efektivnímu rozlišení dle důležitosti přijatých zpráv, software NET-G disponuje následujícím barevným rozlišením:

- **černá barva** – běžné události (odchody, příchody, pravidelné testy apod.)
- **červená barva** – poplarchy, aktivují i akustickou signalizaci (např. zvuk sirény) a vyžadují odbavení operátorem (potvrzení, že operátor zprávu přijal)
- **fialová barva** – důležité události (výpadek sítě, porucha AKU apod.), aktivují akustickou signalizaci a vyžadují odbavení operátorem

4.2 Seznam objektů

Důležitou funkcí každého takového programu je určitý seznam střežených objektů, v němž jsou ke každému uloženy jejich vlastnosti a důležité informace, které si může operátor

kdykoli zobrazit a nastudovat. Každý objekt má tzv. sloupec vlastností nebo také kartu objektu obsahující informace jako jsou:

- adresa, popis, ukázka na mapě
- fotografie, půdorys, 3D Model, rozmístění prvků EZS
- druh přenosu
- majitel (bydliště, adresa, telefon, fax, email atd.)
- kontaktní osoby (zástupce majitele či odpovědný pracovník v mimopracovní době, technik EZS)
- aktuální stav (EZS)
- pokyny pro zásahovou jednotku při zásahu
- provozní dobu

Obr. 7 Karta objektu SW Radom [9]

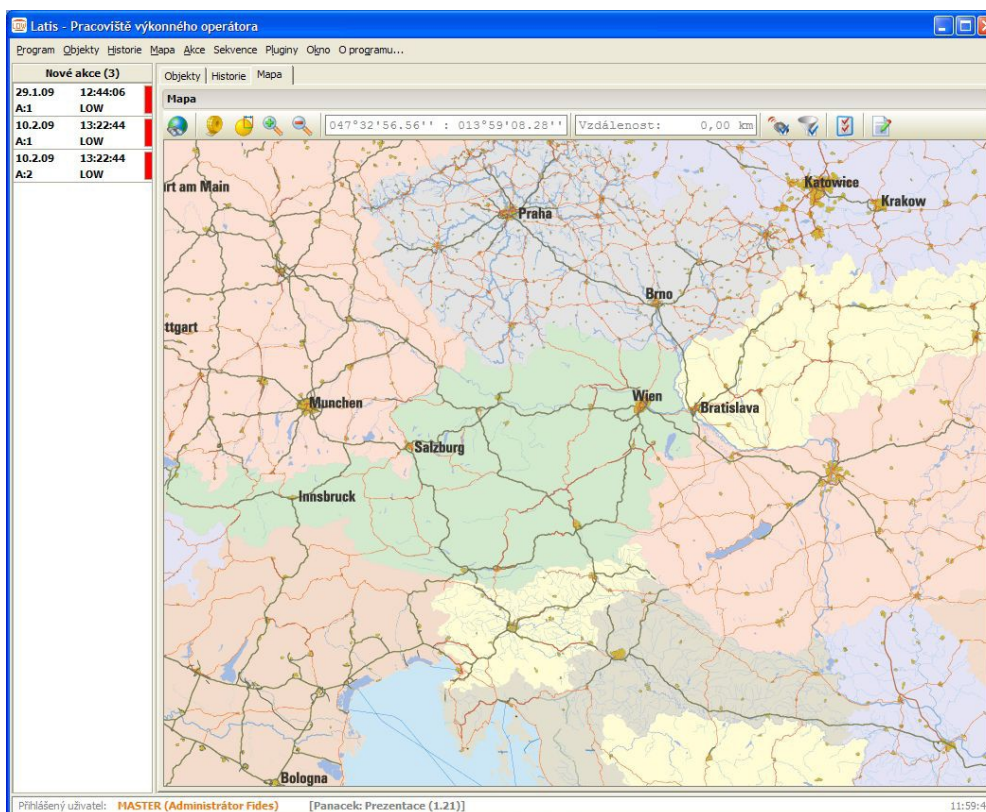
Informace o střeženém objektu slouží jednak pro operátora a také jsou součástí dokumentace zásahové jednotky. Pro posádku je nezbytná jejich znalost, neboť jsou

rozhodující při navádění na místo vzniku poplachové události a správně provedenému zásahu.

U každého objektu lze nastavit některé automatické funkce, které například hlídají dobu zastřežení či odstřežení objektu a v případě překročení nastaveného času je automaticky vygenerována upozorňující zpráva.

4.3 Mapové podklady

Jedná se o další funkci monitorovacího programu, která umožňuje operátorovi prohlížení mapových podkladů zájmového území. Na mapách mají být vyznačeny střežené objekty včetně příjezdových tras.



Obr. 8 Příklad zobrazení mapových podkladů operátora LATIS SQL [20]

Mapové podklady jsou doplňkovou částí každého ze střežených objektů. Důležité je zobrazení příjezdové trasy či schéma s příjezdovou cestou k objektu, půdorys se situačním rozmístěním místností a bezpečnostních prvků, fotografie objektu atd.

4.4 Historie dne a historie objektu

Pomocí filtrů programu lze jednoduše zobrazit zájmový den a všechny tento den přijaté zprávy na PCO.

Podobně je možno v daném časovém období zobrazit všechny zprávy, které z konkrétního objektu přišly a kolik z nich bylo vyhodnoceno jako porucha, falešný poplach, výpadek signálu atd. Software může tyto data také převést do statistiky nebo grafu. Zákazníkům jsou tyto informace pravidelně zasílány ve formě výpisu.

Může se stát, že v případě napadení objektu vznikne požadavek na prohlédnutí času příchodu zprávy na PCO, času reakce operátora, dojezdu zásahové jednotky atd. Při každém vloupání do objektu dochází jednak k trestné činnosti a často k poškození majetku zákazníka. Provozovatel ve vlastním zájmu zjišťuje, zda při reakci na poplachovou zprávu nikdo z pracovníků PCO nepochybil. Proto je historie dne a historie objektu důležitou funkcí každého PCO.

4.5 Shrnutí

Uživatelský software slouží k vyhodnocování přijatých zpráv ze střežených objektů, u něhož se předpokládá přehledné zobrazení a patřičný uživatelský komfort určený pro správné, rychlé a efektivní vyhodnocení přijaté události. Tyto programy se budou zřejmě dále rozšiřovat o nové funkce, ovládací a monitorovací možnosti a grafické dovednosti. Právě rozvíjející se grafické nadstavby s možností ovládání prvků objektu jsou trendem v této oblasti a začínají se postupně do programů dostávat. Operátor bude mít na obrazovce půdorys objektu s virtuálně rozmístěnými prvky EZS, EPS, ACS a v případě zaznamenání poplachové zprávy program jednoduchou vizualizací zobrazí narušené místo.

Lze předpokládat, že se tyto aplikace začnou v blízké době přizpůsobovat na již zmiňovanou oblast inteligentních budov, kde bude nutné doplnění o další ovládací, monitorovací a měřicí funkce. Na program a jeho obsluhu budou tedy kladeny mnohem vyšší nároky.

Pokud se zaměříme na shrnutí tří, v této práci popsaných uživatelských softwarů tj. SW Radom, NET-G, a Latis, tak lze říci, že programy společností Radom a NAM mají z pohledu obsluhy téměř shodné vlastnosti a funkce. Osvědčený způsob zpracování a zobrazování informací řádkovou formou je pro operátora dostatečně přehledný a informace

o objektu včetně mapových podkladů přináší potřebnou efektivitu práce. Je však možné, že se tento způsob obsluhy PCO stane brzy zastaralým. Software společnosti Fides podporuje grafické zobrazení půdorysu objektu včetně vizualizace a možnosti ovládání prvků různých technologických zařízení. Tento systém je tedy k současně rozvíjející se oblasti inteligentních budov nejbliže.

5 PCO RADOM

Společnost Radom byla založena v roce 1992 a nabízí svým zákazníkům komplexní služby v oblasti dálkové komunikace a zabezpečení. (Vývoj hardware i software, projekce, výroba, montáže atd.). Mezi hlavní oblasti činnosti patří systémy pro rádiové přenosy dat, systémy střežení objektů, satelitní komunikace, vysokofrekvenční a anténní technika. Společnost Radom patří mezi přední výrobce pultů centralizované ochrany v ČR.

Vlastní dispečerské pracoviště PCO tvoří zařízení pro příjem zpráv z objektů a počítačová sestava s uživatelským softwarem i v síťovém provedení pro zobrazení, vyhodnocení a archivaci zpráv z objektů. Přenos probíhá v rámci privátní rádiové sítě 400 MHz, po telefonních linkách či sítěmi mobilních operátorů GSM (SMS, GPRS). K dispozici jsou i datové sítě LAN/WAN a nebo kombinace uvedených způsobů přenosu. [13]

Základ vlastního PCO tvoří vždy počítač, ke kterému jsou připojena tzv. komunikační zařízení. Tyto elektronické prvky zprostředkovávají přenos dat na PCO.

5.1 Přenos informací v privátní rádiové síti

Na straně střeženého objektu se k ústředně EZS připojují vysílače s označením STR20 (předchozí generace nesla název STX13A/400). Je to vysílač nové generace, určený jako objektové zařízení pro rádiové sítě systému Radom Security.

Vysílač se vyrábí v několika variantách, které se liší použitím (EZS nebo EPS), počtem vstupů, výstupů, napájením atd.

Technické parametry:

- Napájení: 11 až 15 V/ max 2,0 A pro variantu bez vestavěného transformátoru a zálohovacího akumulátoru. S transformátorem a akumulátorem (12V, 7AH) síť ~230V ±10% / 50Hz / max. 30VA.
- Přenášené informace: U objektových vysílačů řady STR20 se přenášejí vnější a vnitřní stavové informace (SÍŤ, AKU, SAB, D/N), vnější poplachové vstupy a také kódy přicházející do vysílače prostřednictvím telefonního komunikátoru z EZS, resp. sériové linky. Všechny tyto informace se přenášejí okamžitě po jejich vzniku.

- Paralelní vstupy: Tyto vstupy jsou určeny k propojení s výstupním modulem ústředny, nebo přímo k připojení čidel. Počet vstupů je 8.
- Paralelní výstupy: Pro ovládání jiných zařízení (např. klíčový trezor)
- Sériové připojení: RS232, respektive RS485 pro komunikaci s EZS.

Vysílací a přijímací rádiový blok je tvořen radiostanicí UTR08 se simplexním datovým provozem. Stanice pracuje v pásmu 84,010 – 87,490 MHz s kanálovým odstupem 20 kHz.

Vlastní PCO je tvořeno počítačovou sestavou s uživatelským softwarem, který nese označení WRS32. Na vstupu PC je rádiový přijímač SRX10/400 s anténním systémem, případně retranslační stanice.

Rádiový přijímač SRX10/400/W:

Jde o rádiový přijímač, který se skládá z vlastního přijímače (URX40), jehož NF výstup je přiveden do modemu (SMR45). Ten data zpracovává a na dotaz je po sériovém portu předává do řídicího systému (PC). Napájení zajišťuje síťový zdroj zálohovaný akumulátorem 6,5Ah.

Retranslační stanice SRE40

Pro zkvalitnění přenosové cesty na PCO se využívá retranslační stanice, která přijímá zprávy od komunikátorů střeženého objektu a v definovaném okamžiku je předává na PCO.

Pro lepší informovanost obsluhy PCO přidává k vysílané zprávě informaci o síle signálů z jednotlivých komunikátorů.

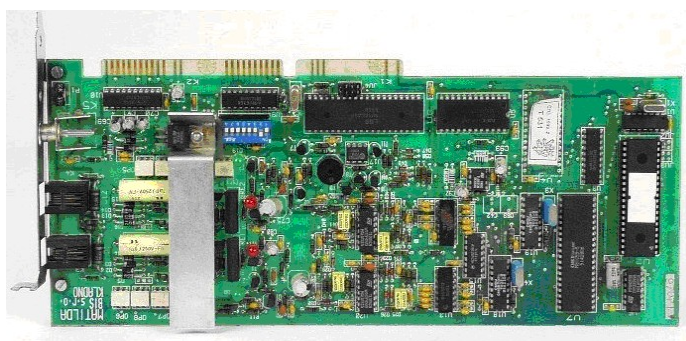
Složení retranslační stanice:

- Přijímač MAXON DM70
- Vysílač UTX40
- Modem SMR40
- Deska logiky objektového vysílače STX20

Modem slouží ke zpracování zpráv z jednotlivých vysílačů v objektech, přidává informaci o síle elektromagnetického pole v místě příjmu a odesílá tato data na PCO. Deska logiky je název pro elektronický prvek k ovládání a nastavení vlastní retranslační stanice (pomocí osmi konfigurovatelných vstupů).

5.2 Přenos informací po pevných telefonních linkách

Uvedený způsob přenosu je snadno realizovatelný, jelikož telefonní komunikátor bývá součástí téměř každé ústředny EZS. Na straně PCO se nachází telefonní karta GS51 nebo TF98 s boxem pro příjem zpráv po telefonní lince.



Obr. 9 Telefonní karta GS51 [13]

Další možností komunikace s PCO je pomocí telefonního internetového komunikátoru (INET), který je určen k přenosu zpráv ve formátu Ademco Contact ID, získaných z vestavěného přijímače telefonní komunikace nebo alternativně po sériové lince od zařízení SXS24 (GSM hlásič). Na straně zabezpečovacího systému je připojen pomocí telefonní linky nebo zařízením SXS24. S PCO probíhá komunikace prostřednictvím UDP/IP paketů na rozhraní ETHERNET. Modul umožňuje dále na povel z PCO, případně automaticky při ztrátě komunikace provést přemostění svého přijímače a umožnit komunikaci EZS přímo s veřejnou telefonní sítí. O stavu modulu může být ústředna EZS informována prostřednictvím 2 výstupů. Komunikace mezi modulem a PCO může být pro zvýšení bezpečnosti šifrována. Toto šifrování musí být ovšem podporováno i na straně PCO. Pro případ nutnosti jednosměrné komunikace modul umožňuje provoz v jednosměrném režimu s omezenou funkcí.

5.3 Přenos informací pomocí sítě GSM/GPRS

Jedná se tedy o přenos poplachových zpráv na PCO v rámci sítí mobilních operátorů. I zde Radom nabízí kompletní systém přenosu informací a jejich zpracování. Vysílací část tvoří tzv. GSM komunikátory, nebo také GSM hlásiče, připojené k výstupu zabezpečovacího systému EZS.

Základní typ GSM komunikátoru určeného pro přenos na PCO nese označení SXS21. Zařízení umožňuje přenos informací z osmice (7+1) binárních vstupů až na osm telefonních čísel a to formou hlasového volání (prozvonění) i SMS zpráv. Hlásič je možno přímo použít jako jednoduchou zabezpečovací ústřednu, nebo v kombinaci s libovolnou komerčně dodávanou ústřednou EZS.

Vstupy jsou určeny k propojení s výstupním modulem ústředny, nebo přímo k připojení čidel. Mohou být využity jako potenciálové nebo bezpotenciálové (platí vždy pro celou osmicí). Hlásič nabízí i vstup pro připojení elektretového mikrofону.

Komunikátor disponuje dvěma výstupy, které lze ovládat (např. SMS zprávami) a jeden výstup určený pro sirénu.

SXS21 je vybaven dvoupásmovým komunikačním GSM modulem Siemens nebo Wavecom. Modem komunikuje s PCO prostřednictvím sítě GSM zvoleného provozovatele a to v pásmu 900 i 1800 MHz. SIM karta se vkládá do čtečky SIM karty na desce modulu. Protože se využívá hlasové volání, musí být na SIM kartě povolena hlasová komunikace. Pro co největší spolehlivost provozu je vhodné zvolit pro SXS21 a mobilní telefon zákazníka stejného provozovatele sítě.

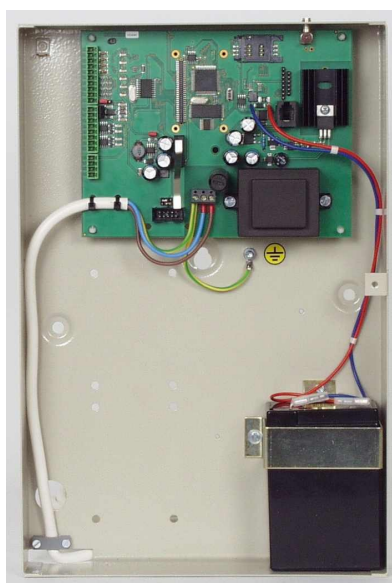
Další z řady SXS komunikátorů je 22, který disponuje komunikačním GSM modulem Sony Ericsson GR47.

Pro komunikaci v GPRS síti je zde GSM hlásič SXS24.

Jedná se o univerzální zařízení určené k přenosu bezpečnostních a servisních dat elektronických zabezpečovacích systémů na vzdálený pult centrální ochrany (dále jen PCO). Přenos dat probíhá ON-LINE v GPRS datovém provozu libovolného operátora v

pásmu 900/1800MHz. V konfiguraci s LAN komunikátorem může přenos dat probíhat po počítačových sítích.

Deska GSM hlásiče je navíc vybavena osmicí univerzálních vstupů. Hlasič SXS24 komunikuje s PCO obousměrně a pravidelně kontroluje funkčnost spojení mezi nimi. V případě výpadku GPRS signálu je možno přenést požadovaná data z EZS přes záložní datové SMS zprávy. V případě výpadku celé GSM sítě je možno pomocí výstupu SXS24 přepnout EZS na záložní cestu např. pevnou telefonní linku.



Obr. 10 Zařízení SXS24 [13]

5.4 Zařízení Pitbul

Již druhá generace úspěšné řady zabezpečovací ústředny Pitbul využívá k přenosu na PCO též sítě mobilních operátorů GSM/GPRS. Po připojení detektorů dokáže systém pracovat jako ústředna EZS, a nebo ji lze využít pouze jako komunikační zařízení po připojení ke stávající ústředně střeženého objektu. Vzniklé stavy na objektu je možné přenášet na vlastní mobilní telefon (formou SMS nebo hlasovým voláním - prozvoněním) nebo na PCO pomocí GPRS. Pomocí SMS zpráv lze také ústřednu Pitbul dálkově uvést do střeženého nebo nestřeženého stavu.

5.5 Přenos informací pomocí sítě Ethernet

Ten probíhá přes zařízení SXS30/NET, které je určeno k přenosu poplachových a servisních zpráv na PCO on-line pomocí sítě Ethernet. Deska elektroniky tohoto

komunikátoru je osazena šesti dvojitě vyváženými smyčkovými vstupy pro přenos urgentních hlášení na PCO. Zařízení komunikuje s PCO obousměrně a pravidelně kontroluje spojení. V případě výpadku či poruchy sítě Ethernet dokáže přenést požadovaná data z EZS na PCO záložní cestou (např. telefonní linkou). Z PCO lze přenosovou cestu dálkově ovládat. Zařízení je složeno z desky plošného spoje modulu GPRS 3.0, na které je integrován modul pro sítě Ethernet „X Port“ a modul přepínače náhradní přenosové cesty.

5.6 Uživatelský software RADOM SECURITY WRS32

Jedná se o uživatelský software pro PCO. Nabízí současné využití všech přenosových cest a dokáže komunikovat i se zařízeními jiných výrobců (telefonní karta GS51 Matilda, telefonní boxy TF98 NAM systém, telefonní pulty Sur-Gard). Zpracovává téměř všechny telefonní formáty (4/2, 4/3, Contact ID, Ademco Express,...).

Zde je výčet několika dalších užitečných vlastností softwaru WRS32:

- centralizace více PCO do jednoho místa pomocí GSM a sítí TCP/IP (GSM/GPRS, LAN/WAN,...)
- individuální nastavování přístupových práv pro každého operátora
- možnost zpracovávat více čísel sítí na jednom PCO, v každé z nich až 256 základních objektů s možností využití virtuálních objektů
- vyhodnocování a zobrazování síly radiového signálu
- rozlišení až 1024 poplachových smyček na objektech (není nutné zadávat jejich počet)
- více způsobů zobrazování informací o objektech (formát RADOM, řádkové zobrazení, souhrnné informace, diagnostika), poplachové a informační rámečky
- rozmanité filtry pro výběr zobrazovaných a zpracovávaných informací, nastavitelný čas intervalu signalizace ztráty kódu telefonní a sériové linky samostatně pro každý objekt
- nastavitelný čas intervalu signalizace dlouhodobého výpadku sítě
- plánování denních časů vstupů na objekt (signalizace nepřepnutí na den/noc, zakázaný vstup) s možností plánování náhradních časů pro dané období

- tisk zásahové karty s popisem objektu, popisem zón, podrobnými informacemi, trasou, pokyny, atd.
- vytáčení telefonních čísel uvedených v seznamech objektů a kontaktních osob pomocí interního nebo externího faxmodemu
- možnost hlasové komunikace z PCO (náhlavní souprava) při volání z mobilních telefonů na PCO
- automatické odesílání SMS zpráv na vybraná čísla mobilních telefonů při definovaných událostech - volitelně pro jednotlivé objekty
- možnost nastavení samostatného zvuku pro libovolnou událost libovolného objektu
- e-mailový manažer pro odesílání e-mailových zpráv (možnost odesílání e-mailů v sítích LAN i pomocí telefonní linky). [13]

5.7 Shrnutí systému Radom

Společnost Radom přináší na trh vysoce kvalitní a moderní způsob realizace PCO pomocí celé škály komponentů, které pro přenos zpráv využívají všechny již jmenované druhy přenosu. Poskytuje komplexní služby od vývoje, projekci, výroby přes montáž a servis těchto bezpečnostních zařízení. Kromě vlastních produktů využívá i výrobky renomovaných českých a zahraničních firem.

Zpracování poplachových zpráv probíhá výhradně v IBM PC za pomoci softwaru WRS 32. Tento uživatelský program je velmi kompaktní, jelikož dokáže komunikovat i se zařízením jiných výrobců a zpracovávat všechny dnes používané druhy formátů přenosu. Tyto vlastnosti umožňují aplikovat jej na PCO složené z výrobků konkurenční firmy, nebo zvýšit efektivitu PCO náhradou za starý software.

Novinkou je síťové řešení pracovišť pultů centralizované ochrany tzv. RADOMNET. Toto programové vybavení slouží jako systémová nadstavba programu WRS32, umožňující současné ovládání pultů centralizované ochrany z více dispečerských pracovišť. Poskytuje tedy nové funkce a vlastnosti pro zvýšení efektivity práce obsluhy PCO.

Zařízení Pitbul slouží pro kvalitní zabezpečení objektů s přenosem zpráv o narušení střeženého místa na PCO nebo pouze informováním zákazníka na mobilní telefon. Po připojení příslušných detektorů dokáže pracovat i jako ústředna EZS, čímž vzniká relativně levné a spolehlivé řešení pro zabezpečení bytů i větších objektů. Jako komunikační zařízení pracuje v sítích GSM prostřednictvím GPRS pro vhodné uplatnění v místech, kde

není možné použít rádiový přenos (horské oblasti, zarušená prostředí). Komunikace sítí mobilních operátorů se realizuje z důvodu širokého pokrytí signálem operátora.

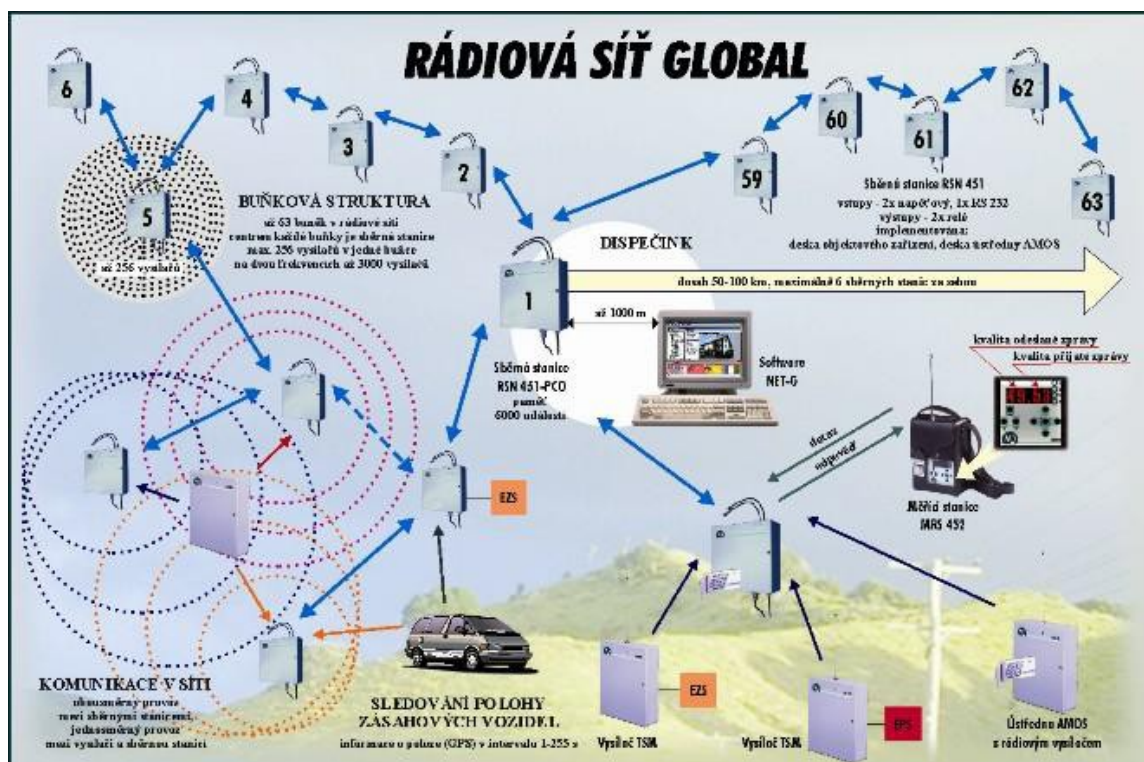
Pro přenos rádiovou sítí, která je v současné době nejčastěji využívána, jsou zde vysílače STX nebo STR 20 pracující na přiděleném kmitočtu 400 MHz a mohou být doplněny retranslací. Obsahují telefonní komunikátor, přímé vstupy nebo sériové vstupy pro snadné připojení k ústředně EZS.

6 PCO NAM

NAM system, a.s. je v ČR významným výrobcem a dodavatelem pultů centralizované ochrany. Kromě PCO se specializuje na rádiový přenos dat v aplikacích, jako je teplárství, vodárenství, plynárenství atd. V současné době se zaměřuje i na systémy pro monitorování polohy mobilních objektů. S vývojem radiových PCO firma začala v roce 1991 (První PCO pracoval pomocí IBM PC a využíval operační systém MS DOS. Označení nesl NAM RP 1000). Na základě mnohaletých zkušeností z vývoje, výroby a provozu PCO přišla společnost NAM systém, a.s. v roce 1999 na trh s novým typem radiotelefonního pultu pod označením NAM GLOBAL.

6.1 Struktura rádiové sítě Global

V systému Global neprobíhá hlídání kontroly spojení se střeženým objektem až na PCO, ale tuto úlohu přebírá sběrná stanice. Výhoda spočívá ve snížení rádiového provozu v síti tím, že se nevytváří vždy spojení Objekt – Sběrná stanice – PCO, ale postačuje Objekt – Sběrná Stanice. Sběrná stanice je inteligentní převaděč, který přijímá všechny zprávy z jemu přidělených objektových komunikátorů, ale na PCO posílá pouze významové zprávy. [12]



Obr. 11 Schéma rádiové sítě Global [12]

Rádiová síť Global kombinuje výhody jednosměrných a obousměrných rádiových PCO. Provoz mezi objektovými vysílači a sběrnými stanicemi je jednosměrný, provoz mezi sběrnými stanicemi a sběrnou stanicí PCO je obousměrný. Výhodou jednosměrného provozu je nízká cena objektového vysílače.

Obousměrný provoz umožňuje po páteřní síti přenášet efektivně větší datové toky, ovládat činnost sběrných stanic na dálku a pomocí reléových výstupů, např. zapínat světlo nebo otevírat klíčový trezor. Pro síť s větším počtem vysílačů než 1000 je potřeba přejít na systém Global 2.

Sběrná stanice kontroluje spojení s určenými objekty a předává na sběrnou stanicí PCO významové zprávy a informace o stavu sítě. Rádiová síť Global umožňuje začlenit do systému až 63 sběrných stanic. Sběrné stanice mohou být řazeny až v 6 úrovních za sebou. Tím se zvětšuje dosah rádiové sítě a tím i počet hlídaných objektů. Na jednu sběrnou stanicí lze připojit až 256 objektů tzn. na jednu síť je možno teoreticky připojit $63 * 256 = 16128$ objektů a 63 sběrných stanic.

6.2 Rádiová síť Global 2

Rádiová síť Global 2 je nástupcem osvědčených řešení rádiových sítí Global. Komunikace probíhá prostřednictvím sběrných stanic RSN 451. Systém Global 2 pracuje ve dvou kmitočtech. Jeden kmitočet je vymezen pro zařízení sítě Global, druhý kmitočet je vymezen pro zařízení sítě Radas. Pro správnou funkci systému je požadováno, aby oba pracovní kmitočty byly zvoleny tak, aby nedocházelo ke vzájemnému rušení provozu na jednotlivých kmitočtech.

Na kmitočtu Global probíhá jednosměrná komunikace mezi vysílačem a sběrnou stanicí, na kmitočtu Radas se jedná o obousměrnou komunikaci s potvrzováním mezi sběrnými stanicemi.

Rozdělením přenosu dat na více frekvencí tak několikrát vzrostla kapacita rádiové sítě Global 2 oproti síť Global. Na dvou frekvencích může pracovat až 4000 objektových zařízení nebo sběrných stanic.

Data ze sítě Global 2 je možné přenášet současně na více dispečerských pracovišť.

Základem PCO NAM Global je počítač s monitorovacím softwarem NET-G. Do PCO jsou přenášeny zprávy dle zvoleného přenosového média:

- Vlastní rádiová síť v pásmu 400 až 470 MHz
- Sítě mobilních operátorů
- Telefonní linka
- Internet

6.3 Přenos zpráv na PCO rádiovou sítí v pásmu 400 až 470 MHz

Rádiový vysílač TSM 45 x

Vysílače TSM 452 a 454 jsou rádiová objektová zařízení přenášející data v pásmu 400 – 470 MHz. Propojení s ústřednou EZS je realizováno pomocí přímých vstupů, přes telefonní komunikátor nebo přes sériové rozhraní. Mezi výhody vysílačů patří bezpečnost, cena a rychlost přenosu.

Vysílače se dělí podle výkonu na:

- TSM 452 (0,1 až 1 W)
- TSM 453 (0,02 až 02 W)
- TSM 454 (0,5 až 5 W)

TSM 452 a TSM 454 může fungovat jako zabezpečovací ústředna AMOS 1600. Pak má funkce ústředny, která obsahuje 16 smyček a je dělitelná do 8 sekcí. Vybavena je radiovým vysílačem a telefonním komunikátorem.

Paralelní vstupy

- 8 vyvážených 24 hodinových smyček
- 8 potenciálových smyček -rozepnuto -50 V až 3,5 V, neurčitý stav 3,5 V až 9 V, sepnuto 9 V až 50 V, odběr 1,5 mA při 15 V
- možnost programového vypnutí vstupu
- možnost programové inverze vstupu

- softwarová filtrace rušení na vstupech
- možnost napojení až 8 různých ústředen EZS na všech 16 vstupů. Pro každou ústřednu je pak jeden vstup rezervován pro poplach a druhý vstup na den/noc.

Vstup pro telefonní komunikátor

- vstup pro telefonní komunikátor zpracovává formáty Contact ID, 4+2,4+3, DTMF, rychlostí 10, 20, 40 Bd
- akustická signalizace potvrzení zpráv telefonní komunikace
- indikace přijaté zprávy z telefonního komunikátoru
- možnost připojení až 8 ústředen EZS přes telefonní komunikátor i s jejich rozlišením na PCO

Další možnosti vysílačů TSM 452 / TSM 454

- volba periody vysílání kontrolních telegramů
- akustická signalizace vysílání zpráv rádiem
- volba tichého vysílače
- výběr jedné ze čtyř přednastavených frekvencí

Sběrné stanice RSN 45x

Je to inteligentní převaděč, který přijímá všechny zprávy z jemu přidělených objektových vysílačů, ale dále, směrem k PCO, posílá pouze významové zprávy z objektů, jiných sběrných stanic a vlastní diagnostické zprávy. Kontroluje spojení s objekty, které má definované. Obsahuje dva napěťové výstupy pro připojení externích zařízení. Sběrná stanice jako objektové zařízení může mít rovněž veškeré funkce zabezpečovací ústředny AMOS 1600. Jako další funkci provádí sledování kvality signálu všech připojených objektů.



Obr. 12 Sběrná stanice RSN [12]

Sběrná stanice přijímá zprávy z rádiových vysílačů TSM 45x

6.4 Přenos zpráv na PCO pomocí sítě mobilních operátorů

Vysílač GSM 1

Jedná se o komunikační zařízení, které slouží k přenosu informací z ústředí EZS na pult centralizované ochrany typu Global sítě (GSM/GPRS).

Základní parametry vysílače GSM 1:

- Přenos informací na PCO pomocí GSM sítě mobilních operátorů
- Obousměrná komunikace s potvrzováním příjmu zpráv Sběrnou stanicí PCO
- Kontrola doby spojení vysílače s Sběrnou stanicí PCO

Vysílač GSM 1 je složen ze dvou základních modulů:

- Kodér DTX 04-K
- GPRS komunikátor G1

Modul kodéru DTX 04-K slouží pro příjem informací ze zařízení nainstalovaných na objektech (EZS ústředny). Kodér tyto zprávy převádí a pomocí dalších elektronických zařízení je informace zpracována a odesílána sériovou linkou do GPRS komunikátoru G1. Tento je neustále připojen na síť GSM mobilního operátora. V okamžiku příjmu informace z kodéru DTX 04-K, tuto informaci překóduje do formátu GPRS a odešle ji do GPRS centra. Toto centrum slouží pro směrování zpráv z jednotlivých objektových vysílačů na sběrnou stanici PCO. Stanice PCO zprávu přijme a pošle ji do programu NET-G a zároveň

stejnou komunikační trasou potvrdí vysílač i přijetí zprávy. Stejným způsobem se posílají také kontrolní zprávy, kdy vysílač GSM 1 testuje průchodnost GSM trasy a sběrná stanice kontroluje funkčnost jednotlivých vysílačů. Doba kontroly spojení je nastavena například na hodnotu 15 minut, a pokud sběrná stanice PCO v této době neobdrží žádnou zprávu z vysílače GSM, vygeneruje a odešle do programu NET-G významovou zprávu o ztrátě spojení s objektem.

6.5 Přenos zpráv na PCO využitím telefonních linek

Telefonní karta TF 98 P

Telefonní karta představuje zařízení, umožňující přijímat do pultu centralizované ochrany data ze střežených objektů po telefonních linkách. Na straně objektu je telefonní komunikátor ústředny EZS, který odesílá zprávy po telefonní lince kartě TF 98.

Telefonní karty jsou ukládány do speciálních boxů, kde v jednom boxu jsou maximálně dvě dvoulinkové karty a k jednomu PC je možno připojit dva takovéto boxy. To znamená, že do jednoho počítače přes jeden COM port je možno přijímat data až z osmi telefonních linek.

Další vlastnosti karty TF 98 P:

- umožňuje přijímat všechny tónové i DTMF formáty 3+1 až 4+3 a je vybavena vnitřní pamětí na 2000 zpráv pro každou linku.
- obsahuje ochranu vstupů telefonních linek proti přepětí a nadproudu.
- telefonní karta má analogový výstup každé linky pro účely nahrávání.
- parametry telefonní karty je možno nastavit z PC a statistiky telefonní karty stáhnout do PC.
- statistika poskytuje podrobné informace o přijímaných formátech a kvalitě komunikace.

6.6 Přenos zpráv na PCO pomocí sítě Internet

Internetové připojení je dnes již součástí téměř každého objektu, tak jako byla dříve pevná telefonní linka. Realizace takového přenosu dat na PCO je díky stávajícímu připojení jednodušší. Komunikátor Reggae LT využívá pro přenos právě Internet. Komunikace probíhá obousměrně včetně potvrzovacích zpráv po přijetí pro větší bezpečnost.

6.7 Software NET- G

Monitorovací software NET-G se zrodil z narůstajících potřeb zpracovávat data z pultů centralizované ochrany rychle a bezpečně, využívat provoz dispečinků, z potřeby skloubit dohromady střežení objektů ve městě se střežením a monitorováním polohy zásahových vozidel či s monitorováním technologických stavů.

Software je postaven na Interbase SQL databázi. Tato databáze umožňuje kdykoliv za plného provozu provést zálohování nebo využít možnosti provádět aktivní kopii databáze na jiný disk.

Podporován a zároveň doporučován je vzdálený přístup k systému přes modem, což umožňuje správci systému pracovat se softwarem při napojování objektu u zákazníka a nebo řediteli firmy přímo z bydliště ze svého počítače.

Software NET-G je složen z několika modulů. Některé z nich jsou součástí hlavní instalace a některé jsou zvlášť samostatně placené. Kterýkoliv z těchto modulů lze kdykoliv doinstalovat a rozšířit tak možnosti celého systému.

Zde je přehled některých modulů:

- Modul AppPCO - hlavní dispečerský modul sloužící k obsluze, zadávání objektu, výpisům historie apod.
- Modul AppDriver - modul zabezpečující zpracování dat přijatých ze zařízení
- Manuál NET-G - kompletní manuál ve formátu HTML
- Modul AppMail - modul sloužící k hromadnému zpracování výpisu mailem, faxem, tiskem
- Servis Print - modul vznikl na základě požadavku CSN. Pomocí tohoto modulu lze tisknout v režimu ON-LINE uživatelem definované události.
- Servis SMS - díky tomuto modulu se může automaticky při příchodu definované události na definovaný objekt odeslat uživatelem připravená SMS na přednastavená telefonní čísla.
- Servis SMS+ - modul sloužící k hlídání bdělosti operátora a k hlídání času potvrzení důležité zprávy + tísňové volání operátora. [12]

6.8 Shrnutí systému NAM

Akciová společnost NAM systém se zabývá vlastním vývojem rádio-telefonních PCO již od roku 1992 a dnes se řadí k významným výrobcům PCO v ČR. Na základě mnohaletých zkušeností z vývoje, výroby a provozu PCO vznikl radiotelefonní pult s označením NAM GLOBAL.

Základem PCO NAM GLOBAL je vždy počítač s monitorovacím softwarem NET-G, který je navržen jako otevřený systém. Tato koncepce vede k možnosti rozšíření systému o další sběrné stanice či zařízení, nebo programové funkce. Téměř vše co lze v softwaru NET-G definovat, není omezeno a celý systém roste s požadavky a potřebami zákazníků. Do programu NET-G jsou připojeny objekty skrz různá přenosová média. Nejžádanější a nejdokonalejší je rádiový přenos v pásmu 400 MHz.

Rádiová síť Global je kompaktní vícebuňková decentralizovaná síť s kvalitním a zabezpečeným přenosem dat. U rádiové sítě Global je mnoho parametrů volitelných. Jejich vhodným nastavením lze zvýšit kapacitu sítě a kvalitu přenosu dat. Svou strukturou je to velice propracovaný a kvalitní systém pro ochranu objektů v rámci PCO. Jedná se o podobnou buňkovou strukturu používanou pro provoz mobilních telefonů, kdy centrem každé buňky je sběrná stanice. Tato síť umožňuje provozovatelům expandovat do širokého okolí a kvalitně pokrýt i hornatý terén.

V rádiové síti Global může být až 1000 rádiově střežených objektů včetně 63 sběrných stanic. Sběrná stanice komunikuje obousměrně, což uživateli umožňuje dálkovou konfiguraci z PCO. Sběrné stanice je možno řadit za sebe, přičemž maximální počet je šest sběrných stanic seřazených za sebou. K dosažení maximální kapacity této sítě je nutno optimálně nastavovat výkony vysílačů, časy vysílání a časy kontroly spojení. K nastavení optimálního výkonu slouží měřicí stanice MRS 452, zobrazující kvalitu spojení se sběrnými stanicemi.

Pro bezpečný provoz sítě je prováděna nepřetržitá kontrola spojení, zabezpečené rádiové telegramy, měření úrovně šumu pozadí na sběrných stanicích atd.

7 SPOLEČNOST TRADE FIDES

Společnost Trade FIDES, a.s. byla založena v roce 1995. Zabývá se poskytováním komplexních služeb v oblasti bezpečnostních systémů na ochranu osob a majetku. Vhodným výběrem bezpečnostních technologií, které jsou doplněny vlastním vývojem technických prostředků a vzájemnou provázaností technologických zařízení budov se společnost FIDES řadí mezi špičku v poskytování ochrany majetku v ČR.

Specifickou činností je realizace bezpečnostních systémů v kulturních a historických památkách ale i Armádu ČR, policii a orgány státní a veřejné správy.

Společnost Trade FIDES, a. s. je členem následujících asociací:

- Asociace obranného a bezpečnostního průmyslu AOP
- Asociace technických bezpečnostních služeb Grémium Alarm
- Certifikační institut ČAP
- Hospodářská komora ČR

První PCO pod názvem Fautor se díky své progresivitě stal základním stavebním kamenem u dálkového dohledu PČR nad sřeženými objekty. Po dalším vývoji se v roce 1999 dostala na trh nová generace PCO postavená na platformě operačního systému Microsoft Windows s názvem LATIS. Jedná se o systém pro zajišťování komplexní elektronické správy budov. Jde o vzájemné propojení všech hlavních technologií používaných v budovách (bezpečnostní systémy, přístupové, kamerové, požární, vytápění, vzduchotechnika, výtahy, osvětlení). Pokud tyto systémy dokáží komunikovat a lze je řídit z jednoho centrálního pracoviště, jedná se o tzv. Inteligentní budovu.

Hlavním smyslem vytváření struktur inteligentních budov je dát vlastníku nástroj pro efektivní a přehledný proces řízení chodu budovy. Neméně významnou část výstavby inteligentních budov tvoří úspory elektrické energie. Právě pro zajištění správy inteligentních budov společnost Fides prezentuje systém LATIS SQL. [20]

7.1 LATIS SQL

Nejnovějším produktem firmy Trade FIDES, a.s., je monitorovací a integrační systém LATIS SQL, který slouží pro bezpečný chod střežených budov prostřednictvím integrace zabezpečovacích a provozních technologií do centrálního dispečerského pracoviště, tedy pultu centralizované ochrany. Tento systém se liší od svých předchůdců tím, že je postaven na databázové technologii Microsoft SQL Server. Tato koncepce umožňuje efektivní zpracování velkých objemů údajů a rozsáhlé možnosti zabezpečení uložených dat. Systém lze snadno rozšířit o další funkční vlastnosti (otevřený systém).

Systém je schopen pracovat s obrazovou dokumentací objektů a je schopen zpracovávat měřené veličiny či vytvářet grafy. Pro lokalizaci objektů je navázán na mapové systémy což může zpřehlednit situaci na objektu pomocí digitálních grafických podkladů (fotografie, půdorysy, stavební plán objektu).

7.2 Složení LATIS SQL

Konstrukce systému LATIS spočívá ve sledování a vyhodnocování informací z různých datových sítí. Pomocí modemu je vytvořeno rozhraní mezi danou sítí a vstupem do programu LATIS Server. Na PCO je tím možné soustředit informace ze sítí komunikujících různými protokoly a tyto dále zpracovat. Informace mají odlišné vlastnosti, neboť jsou přijímány z různých technických zařízení (EZS, EPS, ACS, atd.).

Integrace je orientována nejen na propojení různých sítí, ale i na integraci pultů centralizované ochrany.

7.3 Struktura LATIS SQL

Síť LATIS SQL je tvořena objektovými stanicemi LATIS 2400 a LATIS 2400N na straně střežených objektů. Pro přenos poplachových a provozních zpráv na PCO lze využít:

- Rádiový přenos
- GSM
- Telefonní linku

Rádiový přenos

Pro přenos zpráv rádiovou cestou je na straně PCO využit modem LR 324 pro obousměrnou datovou komunikaci. Na straně střeženého objektu se nachází objektová stanice LATIS 2400 nebo 2400N.



Obr. 13 Rádiový modem LR 324 [20]

Přenos pomocí sítě GSM

Pomocí sítě mobilních operátorů GSM lze přenášet poplachové zprávy prostřednictvím komunikačního zařízení PZG-1 na straně objektu, pro příjem na straně PCO slouží GSM modem LG100.

Přenos pomocí telefonních linek

Tohoto způsobu komunikace využíváno spíše jako záložní přenosová trasa pro případ, že nelze v určitém okamžiku předat zprávu rádiovou cestou či přes GSM síť.

Telefonní modem MGS 51 umožňuje centrální stanici PCO systému LATIS zajišťovat komunikaci s objekty, které jsou osazeny ústřednami EZS nebo jinými technologickými zařízeními. Data jsou předávána prostřednictvím telefonní linky (JTS) komunikačními formáty Contact ID, 4/2 a 4/4 (Ademco, Franklin aj.).



Obr. 14 Telefonní modem MGS 51 [20]

Obousměrnost sítě je využívána i pro přenosy povelů na objekty. Tímto povelům se myslí spuštění určitého zařízení, jako je kamera, osvětlení nebo zakódování EZS objektu.

Síť LATIS využívá kódovaného přenosu a zpracovává nejen data z ústředen EZS a EPS, ale i data technologického charakteru. Všechny tyto systémy lze monitorovat a ovládat z centrálního pracoviště PCO.

Každé z objektových zařízení LATIS 2400 nebo LATIS 2400N dokáže pracovat jako retranslační stanice. Síť může být tvořena až patnácti objektovými zařízeními v řadě za sebou. Každé takové zařízení v sérii tvoří jednu vrstvu. Všechna pracují na jedné frekvenci. Každé objektové zařízení může být v síti dálkově ovládáno a programováno přímo z PCO.



Obr. 15 Objektová stanice LATIS 2400 [20]

7.4 Systém řízení LATIS SQL

Jádrům celého systému je databázový software Microsoft SQL Server. Administraci LATIS zajišťuje program LAT (Latis Administration Tools), kterým se nastavují téměř všechny parametry systému prostřednictvím sítí LAN. Program pro obsluhu LOW (Latis Operator Workstation) je také síťový nástroj, který lze přizpůsobit dle požadavků uživatele.

LATIS SQL obsahuje také několik dalších modulů, mezi které patří LAOM (Latis Automatic Operation Module), který se stará o všechny automatické operace, které systém vykonává (odesílání povelů, doba střežení atd.). Mezi další služby patří LMG (Latis Modem Gateway) zajišťující spojení s modemy.

Celý systém lze nazvat jako stavebnicové řešení přesně přizpůsobitelné potřebám zákazníka. Jednotlivá centrální pracoviště (PCO) lze libovolně propojit prostřednictvím sítí LAN. Toto propojení celků se využívá např. na letištích, vojenských komplexů či velkých bankovních ústavů.

7.5 Program LOW

Uživatelský program LOW je software, sloužící operátorovi PCO ke komunikaci se systémem LATIS SQL. Po přijetí jakékoli události poskytuje v přehledné formě všechny informace k vyřešení vzniklé události, jako jsou:

- instrukce správného postupu
- telefonní čísla zodpovědných osob
- taktika zásahu
- grafické podklady
- obraz kamery z monitorovaného místa
- přesné místo vzniklého poplachu

V přehledné formě zobrazuje informace o všech událostech a o jejich změnách včetně možnosti vykreslení do grafických podkladů. Postup řešení události je zaznamenán v historii, kterou lze zpětně editovat.

Z každého PCO lze rozesílat vybrané povely na objekty dle nastavených práv uživatelů.

7.6 Shrnutí systému společnosti Fides

Společnost Trade Fides s produktem LATIS SQL patří mezi nejúspěšnější poskytovatele komplexního zabezpečení objektů v ČR. O úspěchu svědčí seznam klientů, ke kterým patří největší státní orgány, ale i památky a bankovní instituce ČR.

Jádrem společnosti je vlastní vývoj a moderní pojetí systému zaměřené na technologie inteligentních budov.

Konstrukce systému LATIS umožňuje sledovat a vyhodnocovat informace z různých datových sítí. Pomocí modemu je vytvořeno rozhraní mezi konkrétní sítí a vstupem do programu LATIS Server. Tím je možno na jeden PCO soustředit informace ze sítí komunikujících různými protokoly a tyto informace jednotně zpracovat. Z připojených sítí je možno zpracovávat informace různého charakteru (zabezpečení střežených objektů, systémy EPS, technologické informace) a ty potom adresně předávat na vyhodnocovací pracoviště operátorům.

Díky své komplexnosti a otevřenosti je LATIS kvalitním nástrojem, který je schopen centralizovat přijatá data od různých systémů a výrobců, které je třeba dle potřeb uživatele vzájemně ovlivňovat a sjednocovat. Velkou výhodou možností systému LATIS SQL je, že v jednom prostředí může dispečer PCO sledovat a ovládat prvky EZS, EPS, CCTV, ACS a další.

8 TRENDY V OBLASTI INFORMAČNÍCH TECHNOLOGIÍ VYUŽITELNÉ PRO PCO

Vývoj informačních technologií, založených na elektronickém zpracování a přenosu informací, se promítá do všech oblastí našeho života. Na počátku komerčního využití výpočetní techniky stály v 60. letech minulého století jednoduché autonomní aplikace. Později došlo ke vzniku prvních systémů řízení bází dat a datových modelů umožňujících vzájemné sdílení dat.

Počítače se v komerční oblasti využívají především k získávání informací a ke správě těchto dat. Pro soubor aplikací, sdílejících podniková data, vznikl termín informační systém, který se postupně rozšířil do všech oblastí. Software i hardware pro sdílení dat a zjednodušování podnikání se neustále zdokonaluje. Internet přinesl nové způsoby komunikace, získávání informací a aplikace pro správu informačních systémů.

Technologie pro použití v bezpečnostních technologiích se také neustále zdokonalují, za trendy lze považovat spíše nové softwarové řešení a integrace již stávajících systémů. Zde je uvedeno několik moderních technologií s možností aplikace na pulty centralizované ochrany.

8.1 Vzdálená správa a monitorování

Z jednoho místa lze sledovat a nastavovat prvky informačních technologií a v případě nutné opravy či údržby lze tuto činnost provést vzdáleně. Tím vzniká pro správce systému výrazná časová úspora. Mohou pracovat na správě informačního systému, aniž by cestovali z místa na místo.

Pro vzdálenou správu se využívají aplikace s webovým rozhraním bez nutnosti instalace agenta na PC. (jako příklad lze uvést software Citrus GoToAssist).

V rámci PC je moderní software Intel vPro. Např. díky této technologii lze nefunkční operační systém zotavit na dálku. (zapnutí nebo vypnutí PC, nastavení BIOSu, sledování operačního systému atd.).

8.1.1 Využití pro PCO

Využívání informačních technologií jako součást provozu pultů centralizované ochrany je v dnešní době nezbytné. Jelikož je PC na straně PCO v provozu nepřetržitě, musí být

zaručen pravidelný servis a dá se očekávat, že tento systém může selhat. Vzdálené monitorování dokáže zrychlit opravu a servis včetně všech aktualizací s ohledem na bezpečnost. Obsluha PCO se tak může věnovat jen uživatelské práci a správu PC provádí servisní pracovník dálkově, aniž by ovlivňoval provoz PCO.

8.2 Trendy v oblasti zpracování obrazové informace

V této oblasti se jedná především o stále se zdokonalující digitální IP kamery. Tyto kamery se připojují přímo do počítačové sítě buď bezdrátově nebo kabelovým vedením. Při kabelovém připojení není podmínkou použití napájecího adaptéru v místě, kde je třeba kameru instalovat. Funkce PoE umožňuje přenášet obrazová data a napájet kameru po společném kabelu. IP kamery mají také vlastní inteligenci. Dokáží například vyhodnocovat pohyb v obraze nebo automaticky odesílat obrázky.

Možnosti sledování obrazu:

- pomocí internetového připojení
- využití záznamového zařízení
- pomocí mobilního telefonu

Výhodou IP kamer je to, že pro přenos dat využívají standardů běžné počítačové sítě (kabelové připojení, Wi-Fi). Díky tomu je lze provozovat opravdu kdekoli.

8.2.1 Využití pro PCO

V této oblasti není využívání IP kamer žádnou novinkou. Kamerový dohled může ušetřit zbytečné výjezdy zásahových jednotek, pokud ovšem máme kvalitní obraz a můžeme kameru dálkově ovládat. Výrobce kamerových systémů VIVOTEK nabízí několik nových funkcí těchto zařízení. Kamery obsahují i výstupy, pomocí kterých lze ovládat i jiná externí zařízení např. zhasnout osvětlení v místnosti.

Moderní sledování obrazu je pomocí mobilního telefonu s datovým připojením. Nabízí se dvě možnosti, přímo v telefonu uživatel zadá adresu kamery ve speciálním formátu do mobilního prohlížeče internetu a obraz z kamery se objeví na displeji. Druhou možností je využít JAVA aplikace firmy Koukaam, která dále nabízí možnost zadat až 4 adresy kamer

a snadno mezi nimi přepínat, popřípadě otočné kamery ovládat. Tuto službu může snadno využít zákazník či posádka zásahové jednotky. Funkce je však závislá na dokonalosti a softwarové schopnosti mobilního telefonu.



Obr. 16 Možnost sledování IP kamer mobilním telefonem [14]

8.3 Řešení GeoVision

Systém s označením GeoVision se zabývá integrací informačních a komunikačních technologií v rámci bezpečnostních aplikací. Jedná se především o kamerové systémy v kombinaci s vybraným datovým či textovým řetězcem. Jako příklad lze uvést snímání čárových kódů nebo porovnání pokladničních transakcí s aktuálním videozáznamem. Toto srovnání nám jasně ukáže, kdo a kdy tuto transakci provedl a zda byla v souladu se všemi pravidly. Data a videosekvence lze archivovat dle požadavku uživatele. Tato data jsou využitelná jak v místě instalace, tak vzdáleně v rámci TCP/IP sítě LAN nebo Internetu. Získaná data jsou uložena přímo do videozáznamu kamery, sledující příslušné místo či objekt a poté jsou ukládána v systémové databázi, odkud je lze následně dohledávat.

Systém GeoVision nabízí jak software tak hardwarové vybavení a příslušenství (videorekordéry, IP kamery, disková pole, přístupové systémy).

8.3.1 Využití pro PCO

Myšlenka kombinace videozáznamů s daty uloženými v jednom okamžiku je aplikovatelná v případě dohledávání určité události. Jelikož PCO přijímají stavové informace od bezpečnostních zařízení v objektech, kterými se myslí např. uzamčení dveří, zastřežení objektu, uzamčení bankomatu atd. Lze v případě neoprávněného vstupu nebo manipulace s přístupovým systémem přesně určit, kdo se v tento časový interval u zařízení pohybuje a tyto snímky by bylo po neoprávněném použití přístupového systému okamžitě odeslat na PCO. Podobně by systém pracoval v kombinaci s EZS. Do prostoru, kde pohybový

detektor vyhlásí poplach, se automaticky nasměruje nejbližší kamera a následně je tato událost přenášena na PCO.

V oblasti kamerových systémů je využívána tzv. „inteligentní analýza obrazu“ nebo také „detekce pohybu v obraze“. Tato funkce kombinuje kamerové systémy se systémem střežení a lze ji použít při detekci osoby či automobilu v chráněném prostoru. Na základě vyhodnoceného pohybu lze odeslat snímek nebo krátké video na e-mail či www stránku (FTP server). Detekce pohybu dokáže významně uspořit kapacitu nutnou pro záznam a tím prodloužit jeho délku.

8.4 Navigační technologie GPS

Navigační technologie GPS zažívá v poslední době velký rozmach. Původně vojenský projekt se postupně rozšířil do širokého spektra oborů (silniční a letecká doprava, turistika, pomoc nevidomým atd.).

Kromě přesné lokalizace nás dokáže tento systém společně s digitální mapou dovést do předem zadaného cíle. Vzhledem k poklesu ceny a miniaturizace GPS přijímačů se tato technologie stává stále dostupnější a dá se očekávat, že za nedlouho bude součástí běžně dostupných mobilních telefonů.

8.4.1 Funkce systému GPS

Systém GPS je založen na třech samostatných segmentech. První z nich jsou družice, které krouží kolem Země ve výšce 20200 km a mají přesně určenou oběžnou dráhu i vzájemnou polohu. Pro správnou funkci systému je na oběžné dráze 24 družic.

Druhou část tvoří řídicí segmenty a monitorovací stanice, které se starají o správu družic, korekci odklonů z předepsané oběžné dráhy a správnou funkci celého systému.

Třetí segment tvoří koncová zařízení, tedy GPS přijímače.



Obr. 17 Schéma funkce GPS

8.4.2 Využití pro PCO

Kromě standardní, již běžně využívané funkce, navigace zásahové jednotky k napadenému objektu je možné využívat technologie, které se zaměřují na nejkratší čas dojezdu či komunikace s jinými aplikacemi dopravního systému. Tím se rozumí stav, kdy zásahovou jednotku může na cestě k ověření poplachové zprávy potkat dopravní nehoda či uzavírka. Navigace by v takovém případě měla posádku včas upozornit na takovou situaci a nabídnout náhradní trasu.

Při skutečném napadení objektu je čas příjezdu zásahové skupiny rozhodující a proto je nezbytné tento čas pomocí informačních technologií neustále zkracovat.

8.5 Geografické informační systémy (GIS)

Geografický informační systém je charakterizován prací s prostorovými daty. Jedná se speciální formu informačního systému, aplikovanou na prostorová data.

IS nám dávají informace o objektech na zemském povrchu (občan má trvalé bydliště, objekt, město). Tyto objekty jsou v prostoru s jinými objekty a navzájem se ovlivňují. GIS nám napomáhá k propojení těchto objektů (pomáhá nám například odpovědět na otázky typu, jak daleko jsou města od sebe?). [11]

Proč je problematika GIS aktuální

- GIS poskytuje novou technologii při práci s geografickými informacemi
- mapy - stejně jako mapy v počítači - jsou velmi využívané zdroje informací
- GIS vzrůstá zájem v geografii a v geografickém vzdělávání
- GIS je důležitý prostředek pro porozumění životnímu prostředí a pro jeho spravování

Oblasti, ve kterých se geografické informační systémy používají:

- GIS založené na uliční síti (vyhledávání adres, sledování a navádění vozidel, návrh evakuačních plánů)
- GIS podporující správu přírodních zdrojů (správa vodních toků, rekreačních zdrojů sledování záplav, analýza vlivů na životní prostředí)
- GIS založené na parcelách (evidenze pozemků a jejich vlastníků, územní plánování)
- GIS pro podporu správy technického vybavení (umístění inženýrských sítí).

8.5.1 Využití pro PCO

Zobrazování výsledků geografických informačních systémů je ve formě map nebo tabulek. I takové informace se dají efektivně uplatnit v oblasti PCO. Jak už bylo zmíněno výše, GIS nám napomáhá k určitému propojení objektů. To je rozhodující informace pro správnou orientaci v terénu a navigaci zásahové jednotky v časové tísni k narušenému objektu. Pracovník obsluhy PCO by měl mít tato geografická data správně zpracována, aby byl schopen výjezdovou skupinu přesně a rychle navést k napadenému objektu. Práce a celková znalost map by měla být samozřejmostí. Pracovníci musí dokonale znát oblast a nejrychlejší trasu ke hlídaným objektům. Sledování aktuální dopravní situace v dané lokalitě je také dobrou prevencí. Novinkou v této oblasti jsou i 3D mapy, umožňující ještě dokonalejší a názornější pohled na dané místo. Geografická data mají určitou měrou vliv na časový dojezd výjezdové skupiny a orientaci zejména ve větších městech.

V rámci těchto organizačních činností v průmyslu komerční bezpečnosti je vhodné do map umístit i prvky EZS, umístění a množství škodlivých nebo výbušných látek, vyznačení únikových cest atd.

8.6 Databáze

Databáze můžeme definovat jako soubor vzájemně souvisejících dat, s nimiž pracujeme jako s ucelenou jednotkou. Zjednodušeně lze říci, že jde o určitý registr v elektronické podobě. Mezi jednotlivými produkty a různými výrobci databázových systémů existuje značná variabilita.

System řízení báze dat (SŘBD) je obecný softwarový systém, který řídí sdílený přístup k databázi, a poskytuje mechanismy pomáhající zajistit bezpečnost a integritu uložených dat.

Databázový systém (DBMS) tvoří data + SŘBD.

Databázový systém je software, dodávaný příslušným výrobcem databází.

Nejvýznamnější produkty:

- Microsoft Access
- Oracle Corporation
- Microsoft SQL server
- My SQL
- Sybase

Proč se databázové systémy používají:

- Možnost sdílení dat
- Znovuvyužitelnost dat
- Integrita a ochrana dat
- Řízená správa dat
- Transakční zpracování
- Paralelní přístup více uživatelů

8.7 Databáze a PCO

Databázové systémy se již do problematiky PCO pomalu dostávají, a to především díky zaměření na tzv. inteligentní budovy. V této oblasti je zpracovááno velké množství dat a kvalitní informační technologie jsou již nezbytné. Pokud jsou tyto budovy ovládány a data z nich centralizována do jednoho pracoviště, je třeba pro jejich zpracování a ukládání využít právě databázové programy. Jádrem systému je databázový software (např. Microsoft SQL Server), kterým se definují téměř všechny parametry systému, požadavky uživatele atd. Společná správa zařízení na jednom operačním pracovišti vyžaduje jednotné komunikační a vizualizační prostředí s monitorováním stavu jednotlivých zařízení. Data, získaná z jednoho systému, slouží pro správnou činnost systémů ostatních.

Databáze mají jedinečnou schopnost nabízet různým uživatelům stejných a pouze jedenkrát uložených podkladových dat různé, samostatné pohledy na tato stejná data. Tím se

databáze také odlišují od klasických tabulkových programů. V databázích jsou obsaženy zvukové dokumenty, videosekvence, výkresy, virtuální trojrozměrné modely a mnoho dalšího. Za tím se samozřejmě skrývá masivní vývoj podpůrných technologií, komunikačních prostředků a speciálních datových formátů, který zaznamenal prudký rozvoj a přinesl v mnoha oblastech nepřehlédnutelné výsledky.

8.8 Cloud Computing

Základní myšlenkou cloud computingu je, že všechny aplikace pracují přímo na webu, a to od jednoduchého softwaru až po kompletní operační systémy. Uživatel si v tomto případě nemusí obstarávat žádný drahý hardware, nemusí se starat o aktualizaci systému a nepotřebuje ani kupovat žádný software. Zní to spíše jako budoucnost, ale některé prvky této technologie jsou již k dispozici. Nástroje Office, e-mailová kontrola, kalendář a další programy pracují nezávisle na platformě ve webovém prohlížeči. Všechny programy a data se nacházejí na serverech Googlu a jsou nahrávány podle potřeby. Zařízení velkých firem jako je Microsoft, Gogole, Amazon nebo IBM disponují mnohem větším výkonem, než mohou spotřebovat. Vzniká tak nevyužitý výpočetní čas, který stojí peníze, aniž by přinášel zisk. Firmy proto nabízejí svou výpočetní sílu zákazníkům. Jedná se o obchodní tah, který se vyplatí oběma stranám. Zákazník neplatí za licence k programům nebo za server, ale za spotřebovaný výkon.

Pro využívání této technologie je tedy je tedy uživatel závislý na internetu, na poskytovateli aplikace a jeho zabezpečení. Na druhou stranu se může spolehnout, že při přechodu z počítače na počítač nebude mít problémy s kompatibilitou. [17]

8.8.1 Využití pro PCO

Vznikne určitá možnost spolupráce a centralizace pracovišť PCO tak, jak se již někteří provozovatelé dlouho snaží uskutečnit. Software bude společný pro všechny pracoviště a s pomocí přístupových práv se může zákazník kdykoli podívat, co se na jeho objektu děje. Provozovatel pultu by v podstatě ani nepotřeboval kupovat uživatelský software, jen by si jej „pronajímal“ na webovém serveru. Otázkou je, zdali by se mu takový provoz finančně vyplatil.

8.9 3D virtuální realita

Virtuální realita umožňuje popsat trojrozměrnou virtuální scénu, do které může uživatel PC zasáhnout a stát se tak její součástí. Hlavní výhodou je interaktivita scény, díky které lze s předměty pohybovat a otáčet. Do scény lze vložit také zvuk, video nebo animaci. Další předností je datová nenáročnost scény, z čehož vyplývá uplatnění v internetových aplikacích. Zde je snadné prezentovat vizualizaci libovolného zboží, společnosti, navigaci v budovách atd.

Virtuální 3D aplikace se převádějí z klasických 2D podkladů. Trojrozměrný model kancelářské budovy může obsahovat obraz každého podlaží včetně nábytku a pracovních míst zaměstnanců. Na modelu lze interaktivně plánovat přesuny objektů a to v čase a v různých scénářích.

Tyto 3D aplikace pracují s databází, do které lze nahlížet přes systém CISadmin. Tento software umožňuje upravovat data pomocí formulářů, filtrovat zobrazení na scéně a importovat další prvky či budovy. Program umožňuje i 2D pohled na půdorys podlaží hodící se pro tisk plánů.

8.9.1 Využití pro PCO

Tyto interaktivní scény by bylo možno využít pro seznámení posádky zásahového vozidla i obsluhy PCO s daným objektem. Výhoda 3D scény je v názornosti a dokonalé prezentaci určitého místa. Pokud by v této prezentaci střeženého objektu byly zaznamenány všechny vstupní otvory (okna, dveře) včetně prvků systému EZS, zasahující pracovník by se v objektu snadněji orientoval a rychleji by našel místo vzniku poplachové události. Ideální případ nastane, jestliže se v případě poplachu na monitoru PCO okamžitě zobrazí vygenerovaný 3D obraz se zvýrazněným detektorem hlásící narušení a nejbližší cesta k danému místu.

Kromě prezentací by byly pro posádku zasahujícího vozidla využitelné i 3D fotografie, se kterými se může zasahující pracovník seznámit pro lepší orientaci v narušené lokalitě.

8.10 Program Newton

Po mnoha letech práce na vývoji je na světě program, který bude moci i běžný uživatel využít k diktování textu přímo do počítače. Nový program s názvem NEWTON Dictate

vznikl ve spolupráci s Libereckou technickou univerzitou a dokáže přepsat diktovaný text do PC. Úspěšnost velmi závisí na mluvčích schopnostech uživatele a také na nastaveném slovníku (obecný slovník, právnícký, lékařský).

Čeština je velmi složitým jazykem díky své ohebnosti, skloňováním a časováním. Díky tomu a díky požadavku na výkonnost PC se objevil tento produkt v ČR až nyní. [15]

8.10.1 Využití pro PCO

Tato technologie by byla v první fázi využitelná pro sestavování smluv, nařízení výkonu služeb, sepisování protokolů o mimořádných událostech atd. Jelikož je diktování textu mnohem rychlejší než psaní na klávesnici, přináší tento software velkou časovou úsporu.

System by se stal dokonalým, pokud by se tato technologie dostala na úroveň zadávání příkazů do PC pouze řečí. I když se dá předpokládat, že v budoucnu se ovládání PC pomocí klávesnice a myši zcela vytratí, není ještě tato technologie na takové úrovni, abychom o ní uvažovali v rámci PCO. Obsluha dispečerských počítačů se bude vyvíjet současně s běžnými uživateli PC.

8.11 Malé softwarové aplikace použitelné pro provoz PCO

Některé programy nabízené na internetu volně ke stažení nebo po zakoupení licence můžou pomoci i provozovatelům PCO. Příkladem může být AUTOPLAN Kniha jízd 2009 RE1. Tento software slouží k evidenci a vyhodnocování provozu firemních i soukromých vozidel. U těchto vozidel je možné evidovat kromě jízd také nákupy PHM a ostatní náklady na provoz. Aplikace vypočítá průměrnou spotřebu a následně ji porovnává se zadanou normou spotřeby vozu. Další funkce jsou kontrola termínů pro STK či pravidelný servis, součtové tabulky, grafy, podpora databází atd.

Užitečné můžou být aplikace pro vedení účetnictví nebo uzavírání smluv, kdy program eviduje a dohlíží nad termínem záruk a smluv a včas upozorní uživatele. Tyto programové prostředky opět využívají výše popsané databázové aplikace. [18]

8.12 Shrnutí IT

Všechny výše popsané aplikace jsou možností pro další zdokonalování oblasti pultů centralizované ochrany a v částečné míře se dá očekávat i jejich realizace. Podobné

softwarové aplikace se také neustále vyvíjejí vlivem opravdu velkého růstu informačních technologií.

Informační technologie se patrně budou dále orientovat na řešení aplikačního internetového portálu. Operační systém s pracovní plochou, kde má uživatel aplikační programy a jejich data může sdílet, se patrně přesune do prostředí internetu, a proto není výše popsaná oblast Cloud Computingu daleko od reality. Internetový portál bude aplikace zpřístupňovat v tzv. režimu klient/server.

I v oblasti obrazového přenosu informace je internetová síť stále využívanějším kanálem, i když je zde stále řešena otázka velkého objemu přenášených dat.

Protože se všechny informační technologie a systémy například v inteligentních budovách neustále spojují a navzájem integrují, je třeba dbát také na bezpečnost. Řídící systém je třeba zabezpečit proti závadě hardwaru a základního softwaru. Poruchy hardwaru jsou sice fatální, ale vyskytují se spíš zřídka. Chyby softwaru jsou daleko častější a v průmyslu komerční bezpečnosti jsme proti nim často bezbranní. Riziko chyby operačního systému, databázového programu a podobných aplikací lze v podstatě snížit pouze jejich vhodným výběrem už ve fázi návrhu systému. Určitým pomocníkem v tomto případě může být právě vzdálená správa a monitorování systému. Drtivou většinu selhání řídicích systémů má na svědomí nedokonale odladěný aplikační software.

Hlavním cílem aplikačního softwaru by tedy mělo být nalezení takové metodiky, která by dokázala v krátké době lokalizovat vzniklé závady, opravit chyby a to všechno pokud možno bez přerušování chodu systému. Protože je zpracovávaných informací na PCO stále více a obsluha se již nebude věnovat jen poplachům ze systému EZS, vznikne určitá potřeba využívání databázových programů, které nám z velkých objemů získaných dat vytvoří zásadní událost nebo řadu událostí, na kterou budeme schopni efektivně reagovat a provést příslušná opatření.

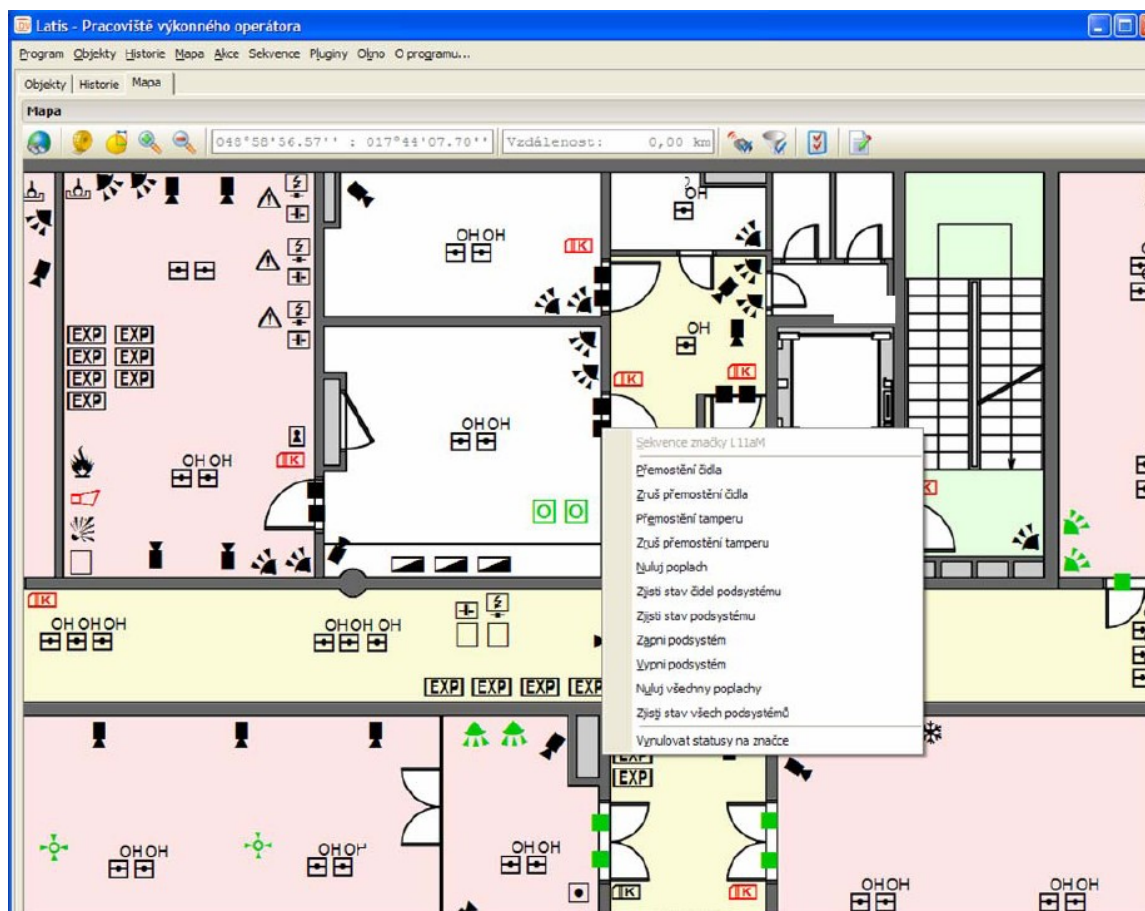
9 TRENDY V OBLASTI PCO

V oblasti PCO dochází k velkému rozšíření služeb, jelikož požadavky zákazníků se neustále zvyšují a pouhé dálkové střežení objektů s výjezdovou skupinou v záloze již nestačí. Na provozovatele jsou kladeny vyšší nároky především na technické vybavení i personální obsazení. Menší bezpečnostní agentury se často spojují, protože nejsou schopny jít s dobou a nabídnout služby větších konkurenčních společností. Trendem v této oblasti je aplikace na tzv. inteligentní budovy. Myšlenka inteligentních budov roste v závislosti na rozvoji technologií. Na toto pracoviště nepřicházejí jen zprávy z EZS, ale monitorují se zde veškerá technologická zařízení (přístupové systémy, CCTV, vzduchotechnika, vytápění, osvětlení, systém měření a regulace) a další technologie, které chce majitel objektu v co největší míře automatizovat a pod dohledem obsluhy ovládat. To přináší vyšší zabezpečení a finanční úspory. Provozovatelé PCO se tedy budou muset určitým způsobem přizpůsobit tak, aby majitelé nových „inteligentních“ budov stali se právě jejich zákazníky. Tato integrace technologií vyžaduje i vyšší nároky na obsluhu a odborné personální obsazení těchto pracovišť.

9.1 Integrace bezpečnostních technologií

Zde se pomalu začíná aplikovat obrazová verifikace. Po přijetí poplachu by mělo být možné okamžitě prověřit narušený prostor a podle toho provést případná opatření a zásah. To znamená, že okamžitě po přijetí zprávy o narušení konkrétní místnosti v objektu by měl být dispečer schopen pomocí CCTV systému s dálkovým ovládním prověřit daný prostor a v případě skutečného vloupání informovat zásahovou jednotku společně s PČR. K tomuto účelu jednoduše poslouží grafická nástavba uživatelského softwaru PCO.

Na obrázku č.12. je ukázán příklad zobrazení mapových podkladů na operátorském pracovišti systému LATIS SQL společnosti Trade Fides. Zde je možné prvky systémů EZS, EPS, CCTV a ACS pomocí grafického prostředí snadno sledovat a ovládat.



Obr. 18 Příklad zobrazení objektu s více technologiemi [20]

Na monitoru je střežený objekt znázorněn formou půdorysů, ve kterých jsou přehledně zobrazeny všechny detektory a signalizován jejich stav. Detektory lze také kliknutím myši jednoduše ovládat (vypnutí, zapnutí, přemostění atd.) Současně je vhodné v těchto půdorysech zobrazit všechny kamery, přístupové systémy a požární hlásiče. Výhodou je to, že několik technologií dispečer jednoduše ovládá z jednoho grafického prostředí. Jednotné ovládání a zobrazování v mapových podkladech je velkým usnadněním práce. Do půdorysů je možné připojit textovou, případně zvukovou zprávu s podrobnějšími informacemi (kontakt na majitele, seznam oprávněných osob apod.).

9.2 Další možnosti uživatelského softwaru

Růst informačních technologií se výrazně promítá i do softwarových možností PCO. Trendem v tomto odvětví je kvalitní zobrazovací program s velkým množstvím efektivních funkcí, možností rozšíření a aktualizace. S rostoucím množstvím zpracovávaných informací je třeba využívat programy s databázovým jádrem, grafickými podklady a možností dálkového ovládání jednotlivých technologií. Díky rozdílným přístupům

společností se prostředí PCO přizpůsobuje těm technologiím, které daná firma přímo vyvíjí a aplikuje do objektů. Výrobci PCO většinou propagují vlastní software navrhnutý pro zpracování signálů svých výrobků. Tyto programy se budou neustále rozšiřovat, jelikož se postupem času bude zpracovávat více informací a stavových hlášení. Protože v nových tzv. inteligentních budovách jsou technologie nejrůznějších značek a výrobců, pro komunikaci bude tedy nutné, aby byl uživatelský software dostatečně kompatibilní, využíval příslušné standardy, přenosové formáty a dokázal tak všechny tyto technologie monitorovat a ovládat.

9.3 Vytěžování informací z technických zařízení

V tomto odvětví se jedná o způsob získávání informací z technických zařízení, které nám mohou poskytnout informace nové, sloužící při rozhodování a preventivních opatřeních. Dnešní přístupové systémy a vůbec celý systém EZS funguje na principu ukládání velkého množství stavových a poplachových hlášení, a pokud se nejedná o poplach, ve většině případů tomu nikdo nevěnuje pozornost.

Z hlediska vytěžování informací přístupových systémů například v kancelářské budově se jedná o zkoumání časů příchodů a odchodů zaměstnanců, počet vstupů do chráněných prostor, kdo chodí do zaměstnání jako první či vychází poslední a zda k tomu nemá nějaký důvod.

Podobný princip poslouží při prohlížení kamerových záznamů. Pokud se nedohledává krádež nebo nějaký incident, záznamy ve většině případů nikdo neprohlíží a za nějakou dobu dojde k jejich přemazání. Namátkové sledování zaměstnanců však může přinést nečekaná odhalení (nepřiměřená délka přestávek, kouření, pochybné přesčasy apod.).

Jelikož jsou tyto zprávy často předmětem dálkového přenosu, týká se vytěžování i PCO. Zkoumání příčiny poplachových zpráv je samozřejmostí, ale pod určitým dohledem by měly být zprávy všeho typu.

Další řešenou problematikou v PCO je snížení nákladů výjezdové skupiny ve vztahu ke zbytečným výjezdům. Převážná část výjezdů zásahových skupin je v reakci na tzv. falešný poplach. Ten je například způsoben špatným nastavením citlivosti detektorů, nekvalitním systémem nebo problém vznikl již při návrhu zabezpečení. Zde vzniká určitý problém, kdy se na poskytovatele dálkového střežení obrátí zákazník, který již má v objektu instalovaný

system EZS a jelikož siréna už nevzbuzuje nikterak velký zájem, chtěl by ústřednu připojit na PCO. Provozovatel však počítá s tím, že úroveň zabezpečení a kvalita EZS nemusí být na takové úrovni, jako by jej zajistila vlastní firma a tím vzniká daleko vyšší riziko vzniku falešných poplachů. I zde je na místě, vyžádat si historii poplachů zabezpečovacího systému v daném objektu a provést příslušná opatření. To vše má vliv na zbytečné výjezdy a vyšší finanční náklady majitele objektu. Proto je na místě snaha o odstranění těchto nežádoucích výjezdů.

9.4 Bezpečný dům firmy Beta Control, výtahové systémy

Na rozdíl od moderních, převážně administrativních inteligentních budov, které předpokládají lokální centra svojí správy, upřednostňuje Beta Control koncept dálkového dohledu. Ten je používán u výtahových systémů jejich i spolupracujících firem. Tento dům se potom skládá z několika základních částí.

Dohledové centrum je technicky realizováno jako aplikační program nad serverem, připojeným bezpečně k síti internet. Tím pádem můžou být tyto centra umístěna kdekoli v republice (pro Beta Control zajišťuje tuto úlohu firma ADT Security Center). Na takové pracoviště jsou přijímány alarmy a nouzové signalizace. Po přijetí tohoto hlášení se příslušná bezpečnostní služba postará o vyproštění osob.

Jedná se tedy o relativně novou službu PCO, kdy má výjezdová skupina po přijetí nouzové signalizace za úkol prověřit dané výtahové systémy a v případě „uvěznění“ osob se postarat o jejich vyproštění. Tato služba je však spíše použitelná v budovách, kde není zajištěn trvalý dohled objektu bezpečnostní službou.

9.5 Trendy v oblasti přenosu

V oblasti přenosu k výrazným změnám nedochází. Výrobci se spíše zaměřují na zrychlení a zvýšení bezpečnosti již osvědčených přenosových tras a technologií, jako jsou rádiové sítě, GSM sítě, sítě LAN a telefonní linky. Obecně v oblasti komunikací dochází ke stále se rozšiřujícím možnostem internetu. Tato síť nabízí obrovské možnosti přenosu dat a proto je stále více využívána i v PKB. Pro pulty centralizované ochrany se tedy nabízí vzdálená správa PC, možnost ovládání kamer, vizualizace, ovládání provozních technologií atd. Nelze přesně odhadnout, kam se bude tento trend dále odvíjet. Internet má však určitou nevýhodu, a to je možnost napadení virovými a jinými škodlivými aplikacemi.

9.6 Vzájemné propojení PCO

V této problematice jde o vytvoření určité sítě obsluhovaných pracovišť tzn. že několik velkých komplexů lze svázat do jednoho velkého nadřazeného systému. Tento pak může podřazené celky monitorovat, případně je může i ovládat se stejnými nebo jinými právy, tak jak se tyto operace provádí na lokálních pracovištích. Nastavením uživatelských práv na různých úrovních se docílí toho, že uživatelé pracují pouze s daty, které jsou jim určeny. Existuje možná zástupnost střežení, kdy se například po vzniku poplachové události očekává reakce operačního pracovníka na podřazeném pracovišti. Pokud tento nezačne do určité doby událost řešit, je automaticky předána na jiné, vybrané nadřazené pracoviště, které tuto akci zabezpečí. Pokud se systém bude vyvíjet tak, že na PCO bude přicházet vlivem rozšiřujících služeb a požadavků zákazníků stále větší množství informací, může tento případ nastat a obsluha PCO opravdu nestihne okamžitě zareagovat. I když poplachové zprávy mají určité prioritní seřazení dle důležitosti reakce, při větším množství je možné některé informace přenést na další PCO. V tomto případě musí být zajištěna určitá součinnost, aby nedošlo k situaci, kdy dvě obslužná pracoviště budou současně reagovat na stejnou událost.

V systému může pracovat i několik nezávislých pracovišť, které mohou být zřizována dle různých kategorií, např. podle významu střežených objektů, podle typu připojených technologií nebo podle významu příchozích zpráv. V systému tedy mohou být PCO sledující pouze požární poplachy, jiné pro příjem poplachů z EZS, další pro poruchové zprávy atd.

Takové propojení celků do jednoho nebo i několika větších center se využívá na letištích, u vojenských komplexů, bankovních ústavů, objektů státní správy atd.

9.7 Shrnutí

Úroveň pultů centralizované ochrany se neustále zvyšuje ostatně stejně jako úroveň a profesionalita kriminálního prostředí. Pokud by se v této oblasti určitým způsobem zpomalil vývoj, mělo by to fatální následky. Po zavedení dálkového dohledu nad svým objektem počítá majitel s tím, že bude jeho majetek v bezpečí a při pokusu o vloupání dojde k příslušnému zásahu a zadržení pachatele. Není v podstatě možné tohle očekávání splnit na 100 %, jelikož se zde vždy objeví určitý časový interval od narušení objektu do

příjezdu zásahové jednotky. Proto se všichni výrobci a bezpečnostní agentury, poskytující tyto služby, snaží tento časový úsek co nejvíce zkrátit. Často zde bývá chyba již při analýze a návrhu zabezpečení, kdy se nezajistí ochrana okolí budovy (perimetru) a často se šetří na ochraně vstupních otvorů mechanickými zábrannými systémy. Pokud systém EZS hlásí poplach až v době, kdy je pachatel již v objektu, ve většině případů dochází k určité krádeži nebo škodě na majetku.

Spíše než vytváření nových technologií dochází k určitému zdokonalování a integraci technologií stávajících. Důkazem je propojení systému EZS, CCTV, přístupových systémů a dokonalé, graficky doplněné, softwarové nadvstavby. V případě narušení pláště objektu (např. překonáním plotu) ochrana perimetru detekuje přesné místo napadení, které se zobrazí na mapě programu PCO. Ve stejné chvíli je možno dát v nočních hodinách pokyn systému MaR, který v daném místě zapne osvětlení a současně se všechny dostupné kamery zaměří do místa napadení a obraz je přenesen na PCO.

Bezpečnost objektů a celkový systém PCO se stále vyvíjí a zdokonaluje, nelze přesně odhadnout, kam budou tyto technologie směřovány ale v nejbližší budoucnosti určitě na střežení a příjem zpráv z tzv. inteligentních budov. Mnoho těchto budov nebude budovat vlastní dispečerské zařízení, ale budou se především orientovat na dálkový přenos. Provozovatel musí být připraven na zvyšující se tlak ze strany zákazníka pro vyšší účinnost těchto zařízení a celkově rostoucí nabídku poskytovaných služeb. Je proto třeba neustále sledovat oblasti nových trendů a oborů, které se postupně k této zabezpečovací technice připojují.

ZÁVĚR

Diplomová práce nabízí celkový pohled, funkci a možnosti využití PCO jako prostředek dálkového střežení objektů. Specifikuje současné trendy, možnosti softwarového řešení a oblast vývoje celého systému PCO.

Stejně, jako se zdokonalují všechny technické oblasti, bude se vyvíjet i tato problematika. Tím se myslí další prvky bezpečnějšího přenosu, grafického zobrazení, možnosti dálkové správy systému a ověřování narušení objektu.

Dá se předpokládat, že vlivem rostoucích nákladů na realizaci, provoz, nákup pohonných hmot a dalších požadavků na PCO dojde k dalšímu slučování provozovatelů a integraci technologií.

Aplikace na moderní objekty bude náročnější než doposud. Inteligentní budova je charakterizována správně fungujícími technickými a měřicími zařízeními, které je třeba správně ovládat, vyhodnocovat a přijímat opatření ke snižování nákladů na provoz a naopak zvyšování komfortu, bezpečnosti a řízeného pohybu přítomných osob v objektu.

Pro tuto funkci je z výše uvedených výrobců nejbližší systém Latis společnosti Fides, která se nyní do oblasti inteligentních budov nejvíce angažuje. Lze však předpokládat, že ji všichni ostatní výrobci a vývojáři PCO budou následovat a do celého systému zavedou pro ně charakteristické a osvědčené způsoby realizace PCO.

Neméně důležitou částí každého PCO je právě obsluha. I zde jsou kladeny vysoké nároky na technické znalosti, profesionalitu a metodiku zásahu. Se zvyšujícím se množstvím příchozích zpráv, ovládaném zařízení a softwarovou vizualizací je kvalitní dispečerská práce stejně důležitá, jako bezporuchový přenos, kvalitní zabezpečovací systém budovy a správně fungující výjezdová skupina.

ZÁVĚR V ANGLIČTINĚ

This extended essay offers a complete view, function and opportunity of CES implementation as

a device for distant (commercial) buildings monitoring and protection. It specifies current trends, possibilities of a software solution and a field of evolution of the whole CES system.

As with an innovation in all technical systems or fields, the same points at issue will arise here. Those include more secure transmissions, graphical and video interface, possibility of distant system management and verification of secured area's alerts and/or alarms.

It can be assumed that the influence of ever growing costs of realization, operation, fuels and other demands from CES will initiate further synergizing of businesses and technology integration.

CES application will be more demanding than ever before at the modern buildings/properties. Smart building is characterized by correct functions of technical and measuring equipment which need to be managed and evaluated correctly, taking measures to lower the operational costs and raising the level of comfort, safety and controlled movement of people present in the building/property.

System Latis from Fides company, who currently strongly engages in the field of smart buildings, is the most suitable for this function out of all aforementioned manufacturers. However, it may be presumed all other manufacturers and designers of CES will follow and integrate characteristic and proven methods of CES realization.

Also, end user plays very important part of each CES. Even here, high demands are put on a technical knowledge, professional approach and methodology of action. With the amount of incoming messages on the rise, equipment operation and software visualization complexity the operator's responsible attitude, knowledge and error-free work is just as important as error-free data transmission, quality security system in the building and correctly functioning strike unit.

SEZNAM POUŽITÉ LITERATURY

- [1] ČSN EN 50136-1- x: *Poplachové systémy- Poplachové přenosové systémy a zařízení*. Vydání: Červen, 1999.
- [2] ČSN EN 50136-2-x: *Poplachové systémy – Poplachové přenosové systémy a zařízení*. Vydání: Červen, 1999.
- [3] ČAP P 103 (1): *Pulty centralizované ochrany, aplikační směrnice, požadavky*, 1. vyd., CI ČAP v Praze: Prosinec, 2004.
- [4] UHLÁŘ, J. *Technická ochrana objektů*, II. díl – Elektrické zabezpečovací systémy, Praha: PA ČR 2001.
- [5] Kindl, J.: *Projektování bezpečnostních systémů I*. 1. vyd. Univerzita Tomáše Bati ve Zlíně, Zlín 2004.
- [6] Čandík, M.: *Objektová bezpečnost II*. UTB – Academia centrum Zlín, 2004.
- [7] KŘEČEK, S. a kolektiv: *Průručka zabezpečovací techniky*. Blatenská tiskárna s.r.o., Blatná: 2003. ISBN 80-902938-2-4.
- [8] LAUCKÝ, V. *Technologie komerční bezpečnosti I.* Zlín: Univerzita Tomáše Bati ve Zlíně, 2004. 64 s. ISBN 80-7318-194-0.
- [9] VYORÁLEK, R. *Pulty centralizované ochrany*. Zlín, 2005. 59 s. Univerzita Tomáše Bati ve Zlíně. Bakalářská práce.
- [10] LUČAN, J. *Tvorba edukačního materiálu s prvky e-learningu systému PCO GLOBAL*. Zlín, 2007. 94 s. Univerzita Tomáše Bati ve Zlíně. Bakalářská práce.
- [11] Vašek, V. *Geografické informační systémy*, Zlín, 2009. Univerzita Tomáše Bati ve Zlíně (studijní materiály).
- [12] *Produkty společnosti NAM SYSTEM* [cit. 2009-10-04]. Dostupné z: <<http://www.nam.cz>>
- [13] *Pulty centralizované ochrany*. [cit. 2009-04-10]. Dostupné z: <<http://www.radom-cz.cz/index.php?ref=2&id=3>>
- [14] *Produkty* [cit. 2009-09-02]. Dostupné z: <<http://koukaam.se/koukaam/products.php>>

- [15] KUBEŠ, R. Počítač vás poslechne na slovo. *technet.idnes.cz* [online]. 2009 [cit. 2009-04-10]. Dostupný z WWW: <<http://technet.idnes.cz/pocitac-vas-poslechne-na-slovo-a-to-doslova-f2x-/>>.
- [16] VŠETEČKA, R. Konec datlování. *technet.idnes.cz* [online]. 2009 [cit. 2009-04-10]. Dostupný z WWW: <<http://technet.idnes.cz/konec-datlovani-prichazi-program-ktery-umi-prepsat-i-ceskou-mluvu-do-pc-1n8-/>>.
- [17] SCHREIBER, M. Práce v oblacích. *Měsíčník CHIP*. 2009, 03, s. 30-31.
- [18] DVOŘÁK, J. Zkuste programy, které vám mohou pomoci v řemeslu či podnikání. *technet.idnes.cz* [online]. 2008 [cit. 2009-04-10]. Dostupný z WWW: <<http://technet.idnes.cz/zkuste-programy-ktere-vam-mohou-pomoci-v-remeslu-ci-podnikani-p68-/>>.
- [19] *Pulty centralizované ochrany společnosti MATILDA BIS s.r.o.* [cit. 2009-03-20]. Dostupné z: <<http://www.matilda.cz/pulty.html>>.
- [20] PANÁČEK, R. *LATIS SQL jako součást inteligentní budovy*. Brno, 2009. Trade FIDES, a.s.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ČAP	Česká asociace Pojišťoven
EZS	Elektrická zabezpečovací signalizace.
HW	Hardware
JTS	Jednotná telefonní síť
NAM	Výrobce pultů centralizované ochrany
PC	Osobní počítač
PCO	Pult centralizované ochrany
PKB	Průmysl komerční bezpečnosti
SW	Software
MaR	Systemy měření a regulace

SEZNAM OBRÁZKŮ

Obr.1 Blokové schéma poplachového přenosového systému (dle ČSN 50 136-1-1)	22
Obr.2 Typy přenosů na PCO	25
Obr.3 Telefonní karta GS51 od firmy Matilda	26
Obr.4 Blokové schéma PCO	30
Obr.5 Jednoduché schéma funkce střežení	34
Obr.6 Monitorovací software NET-G	36
Obr.7 Karta objektu SW Radom	37
Obr.8 Příklad zobrazení mapových podkladů operátora LATIS SQL	38
Obr.9 Telefonní karta GS51 (Radom)	43
Obr.10 Zařízení SXS24 (Radom)	45
Obr.11 Schéma rádiové sítě Global	49
Obr.12 Sběrná stanice RSN (NAM)	53
Obr. 13 Rádiový modem LR 324 (FIDES)	59
Obr.14 Telefonní modem MGS 51 (FIDES)	59
Obr.15 Objektová stanice LATIS 2400	60
Obr.16 Možnost sledování IP kamer mobilním telefonem	65
Obr.17 Schéma funkce GPS	67
Obr.18 Příklad zobrazení objektu s více technologiemi	75