ODPOVĚDNOST ZA SPOLEHLIVÝ CHOD POPLACHOVÉHO PŘIJÍMACÍHO CENTRA

RESPONSIBILITY FOR RELIABLE OPERATION OF ALARM RECEIVING CENTER

Bc. Pavel Novák

Diplomová práce
2014

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

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

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

Jméno a příjmení:	**Bc. Pavel NOVÁK**
Osobní číslo:	**A10433**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Odpovědnost za spolehlivý chod poplachového přijímacího centra**
Téma anglicky:	**Responsibility for the Reliable Operation of an Alarm Receiving Center**

Zásady pro vypracování:

1. **Vysvětlete základní koncepci systémů dohledových poplachových přijímacích center (DPPC).**
2. **Stručně zpracujte normy týkající se DPPC.**
3. **Zpracujte způsoby realizace DPPC v Česku.**
4. **Zpracujte provozní náklady na DPPC v Česku.**
5. **Zpracujte způsoby servisu DPPC v Česku.**
6. **Vyhodnoťte rizika spojená s využíváním externích servisních služeb.**
7. **Vyhodnoťte odpovědnost dodavatelů technologie a služeb za spolehlivý chod DPPC.**
8. **Naznačte další vývoj v této oblasti.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **DIEM, Walter. Bezpečnostní zařízení. Vyd. 1. Překlad Karel Kopička. Praha: Ikar, 2000, 111 s. Udělej si sám. ISBN 80-720-2604-6.**
2. **KINDL, Jiří. Projektování bezpečnostních systémů. 1. vyd. Překlad Karel Kopička. Zlín: Univerzita Tomáše Bati, 2004, 134 s. Udělej si sám. ISBN 80-731-8165-7.**
3. **JELÍNEK, Josef. Jak zabezpečit byt, dům, chatu, automobil. 1. vyd. Překlad Karel Kopička. Praha: Grada, 2000, 80 s. Udělej si sám. ISBN 80-716-9931-4.**
4. **UHLÁŘ, Jan. Technická ochrana objektů. 1. vyd. Překlad Karel Kopička. Praha: Policejní akademie České republiky, 2001, 205 s. Udělej si sám. ISBN 80-725-1076-2.**
5. **IVANKA, Ján. Systemizace bezpečnostního průmyslu II. Vyd. 1. Překlad Karel Kopička. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009, 86 s. Udělej si sám. ISBN 978-80-7318-863-4.**

Vedoucí diplomové práce: **Ing. Rudolf Drga, Ph.D.**
Ústav bezpečnostního inženýrství

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

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

Ve Zlíně dne 7. února 2014

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Cílem diplomové práce je specifikace odpovědnosti za spolehlivý chod poplachového přijímacího centra (DPPC). V první části je popsaná historie, vysvětlena základní koncepce a jsou stručně zpracovány normy týkající se systémů dohledových poplachových přijímacích center. Důležitou součástí je naznačení jejich dalšího vývoje. Závěr práce tvoří vysvětlení způsobu realizace DPPC v Česku přes zpracování provozních nákladů, způsobů servisu, vyhodnocení rizik spojených s využíváním servisních služeb DPPC. Vyhodnocením odpovědnosti dodavatelů technologie a služeb za spolehlivý chod DPPC vznikl dokument, který stanoví minimální požadavky na DPPC pro jeho spolehlivý chod v České republice.

Klíčová slova:

Dohledové Poplachové Přijímací Centra (DPPC), Pult Centralizované Ochrany Objektů (PCO), Průmysl Komerční Bezpečnosti (PKB), Poplachový Zabezpečovací a Tísňový Systém (PTZS), Soukromá Bezpečností Služba (SBS),

ABSTRACT

The aim of this thesis is to specify the responsibility for reliable operation of the alarm receiving center. The first section describes the history, explains the basic concepts and standards relating to alarm receiving center are briefly treated. The important part is an indication of their future development. The thesis concludes with an explanation of the implementation of ARC in the Czech Republic through processing operating costs, service methods, evaluation of risks associated with the use of service ARC. By evaluating the liability of suppliers of technologies and services for reliable operation of ARC was created a document, which sets minimum requirements for ARC for its reliable operation in the Czech Republic.

Keywords:

Alarm Receiving Centre (ARC), Commercial Security Business, Intruder and Hold – Up Alarm System (I&HAS), Private Agency of Security.

Chtěl bych poděkovat svému vedoucímu diplomové práce, Ing. Rudolfu Drgovi, Ph.D., za odborné vedení 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.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně

podpis diplomanta

OBSAH

ÚVOD

Ve své diplomové práci se budu zabývat specifikací odpovědnosti za spolehlivý chod dohledové poplachového přijímacího centra (DPPC). V teoretické části popíšu historii poplachových přijímacích center, jejich charakteristiku a stručně charakterizuji legislativu týkající se dohledových poplachových přijímacích center. Důležitou součástí bude naznačení dalšího vývoje prostředí DPPC. V praktické části vysvětlím způsob realizace DPPC v Česku včetně popisu systémů DPPC od významných dodavatelů systémů. Zpracuji provozní náklady, způsob servisu, vyhodnotím rizika spojená s využíváním servisních služeb DPPC, vyhodnotím odpovědnost dodavatelů technologie a služeb za spolehlivý chod DPPC. Přínosem diplomové práce bude vznik dokumentu, který stanoví minimální požadavky na DPPC v České republice pro jeho spolehlivý chod. Při psaní diplomové práce budu používat knihy, časopisy, normy a manuály, které jsou běžně pro studenty dostupné.

Při zpracování teoretické části diplomové práce pro mě bude velice užitečná publikace Lukáše L. et al. *Bezpečnostní Technologie, Systémy a Management I,* kde je popsaná historie a charakteristika poplachových přijímacích center. Dalšími zdroji, se kterými budu pracovat, jsou normy ČSN EN 50518 od 1 do 3 o dohledových a poplachových přijímacích centrech. Z těchto zdrojů získám nezbytné informace pro sepsání legislativní části práce. Dále mi zdroje pomohou při vytvoření dokumentu, který bude přínosem mojí práce. Při psaní praktické části budu používat získané manuály, konferenční materiály, prezentace, veškeré publikace a své poznámky ze školení ohledně nejnovějších poptávaných systémů DPPC od známých dodavatelů.

V diplomové práci začnu teoretickou částí, ve které se budu snažit přehledně popsat dohledová poplachová přijímací centra. Práci bude začínat kapitola Historie DPPC, ve které se bude nacházet stručný popis vzniku prvních dohledových a poplachových přijímacích center. V další kapitole se pokusím přehledně charakterizovat koncepci dohledových a poplachových přijímacích center. Díky této charakteristice získám přehled o jejich způsobu provozu. Další kapitola bude zaměřena na stručný popis legislativy dané problematiky. Kapitola bude zaměřena hlavně na představení norem ČSN EN 50518 od 1 do 3 a ČSN EN 50136-9. Teoretickou část uzavře předpověď budoucnosti dohledových a poplachových přijímacích center a naznačím trendy v bezpečnostním prostředí. V druhé části - praktické popíšu nejprodávanější značky DPPC, představím způsoby realizace

dohledových a poplachových přijímacích center v Česku. Účelem práce bude vyzkoumání poskytovaných služeb pro realizaci DPPC v ČR. Pomocí zjištěných informací se pokusím vytvořit standard, který by stanovil minimální požadavky pro spolehlivé DPPC v ČR.

Pro vytvoření diplomové práce budu využívat veškerá skripta, odborné časopisy, literaturu, webové články z prostředí bezpečnostních technologií. Díky těmto zdrojům budu moci vytvořit teoretickou část diplomové práce. Základem, který budu používat pro vytvoření praktické části diplomové práce, bude norma ČSN EN 50518 od 1 do 3 a norma ČSN EN 50136-9. Využívat budu také materiály od dodavatelů DPPC a své poznatky ze školení. Nejprve se budu zabývat systémem DPPC od společnosti RADOM, a pak naznačím koncepce od konkurenční společnosti, firmy NAM system. Po vyhodnocení rizik spojených s provozem DPPC v ČR budu moci určit minimální požadavky pro spolehlivý chod DPPC v ČR.

I. TEORETICKÁ ČÁST

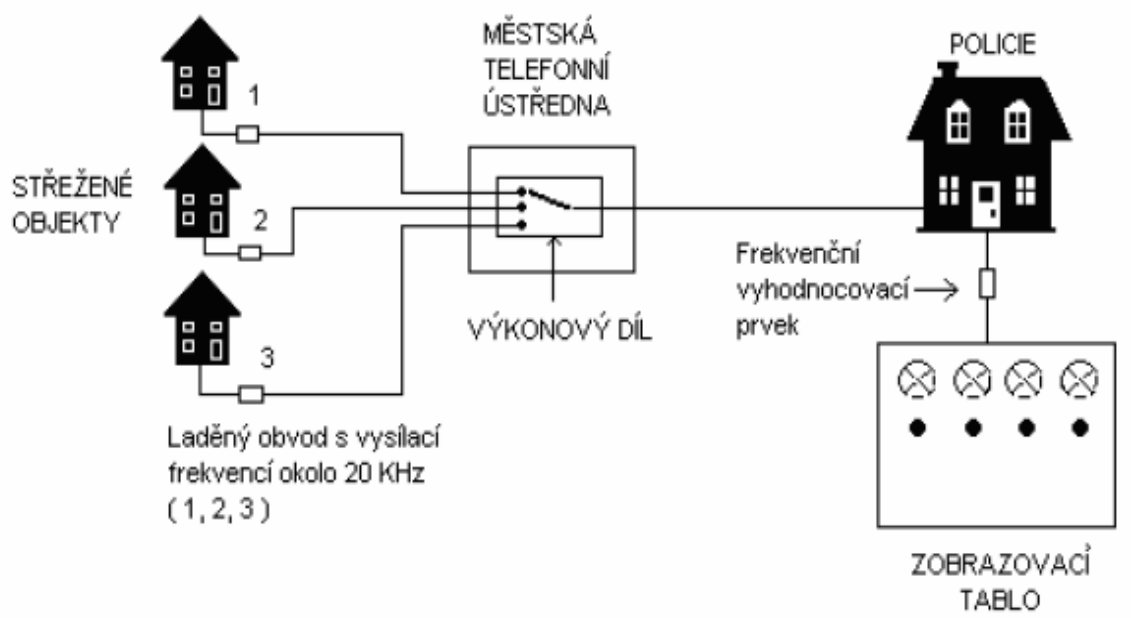
1 HISTORIE DPPC NA ÚZEMÍ ČESKÉ (ČESKOSLOVENSKÉ) REPUBLIKY

V 70. létech 20. století se v Československu projevoval strmý nárůst kriminálních aktivit – především krádeží, loupeží a vloupání do hospodářských objektů. Docházelo tak ke značným škodám na státním majetku. Nárůst této trestné činnosti pokračoval i v 1. polovině 80. let. Z uvedených důvodů přijalo tehdejší vedení Federálního ministerstva vnitra (dále jen „FMV“) řadu opatření, která měla vzniklou situaci řešit. A na základě zkušeností ostatních evropských států se i na našem území začal budovat systém centralizované ochrany. První DPPC byl experimentálně zkoušen na tehdejší Federální správě Veřejné bezpečnosti (dále jen „FS VB“) v roce 1971. K širšímu využívání DPPC došlo po přijetí usnesení vlády č. 73 v roce 1982, které určovalo kategorie důležitosti objektů a z toho vyplývající nároky na složitost EZS a rovněž vyhlášky FMV č. 135 v roce 1983, o ostraze majetku a centralizaci ochrany zabezpečených objektů [1].

První DPPC bylo zkušebně instalováno v Příbrami v roce 1976. Jednalo se o DPPC NĚVA 60 sovětské výroby s přenosem po telefonních linkách, na které byly napojené čerpací stanice, jeden peněžní ústav a sklady trhavin. Postupně se napojovaly rovněž objekty obchodní sítě a kulturního a památkového významu. Po vyhodnocení bylo DPPC rozšířeno do většiny krajských měst. Jednalo se o modernější reléový DPPC CENTR KM, který sestával ze dvou komponent (dispečerské zařízení a výkonový díl). Umožňoval napojení až 120 objektů, situovaných na teritoriu jedné automatické telefonní ústředny (dále jen „ATÚ“). Dispečerské zařízení osazené na operačním středisku Veřejné bezpečnosti (dále jen „VB“) akusticky a opticky signalizovalo narušení objektu. Výkonový díl byl osazen na ATÚ (obvykle v místnosti hlavního rozvodu) a zajišťoval odpojení telefonní ústředny v době střežení. O vzetí objektu pod ochranu a povolení vstupu do objektu žádal pověřený pracovník chráněného objektu telefonicky. Obsluha provedla napojení/odpojení objektu na DPPC manuálně. Další zařízení bylo dodáváno z Bulharska – jednalo se o DPPC typu RONA s kapacitou 240 objektů. Výkonové díly byly vyrobeny pro celkem 60 účastníků, což umožňovalo pokrytí území čtyř telefonních ústředen.[1]

Původní DPPC, vyráběna v Sovětském svazu (NĚVA) a Bulharsku (RONA), byla výlučně linková s přenosem signálu po jednotné telefonní síti v hovorovém pásmu a využívaly se výhradně pro účely střežení státních objektů, které byly mezi sebou propojeny městskou telefonní ústřednou. Zapnutí střežení objektu provedla fyzicky policie na svém

stanovišti sepnutím spínače na PCO, přičemž přerušení spojení (zvednutím sluchátka) indikovalo poplach. Z toho vyplývala i hlavní nevýhoda takového systému, neboť objekt či jeho části se nedaly střežit za provozu, protože v zastřeženém stavu bylo znemožněno telefonování. Celé objemné zařízení sestávalo pouze ze spínačů a kontrolních žárovek, které signalizovaly stav objektu, a jakékoli další možné dělení na podskupiny (grupy) nebo zóny, tak jak je známe dnes, bylo nemyslitelné [2]



Obrázek 1 - Nadhovorový PCO [2]

2 ZÁKLADNÍ KONCEPCE SYSTÉMŮ DPPC

Drga a Šmiraus (2011) uvádějí, že potřeba ochrany zdraví a života osob, jakožto i minimalizace škod způsobených majetkovou kriminalitou, vedly již v minulosti k nutnosti včasného hlášení poplachového stavu na vzdálených objektech. Zařízení sloužící k tomuto účelu, dříve souhrnně označovaná jako pulty centrální ochrany (dále jen „PCO“)[1], jsou dle nové normy ČSN EN 50518-1[2] s účinností od 1. ledna 2011 označována jako dohledová a poplachová přijímací centra (dále jen „DPPC“)[3]. Hlavním argumentem pro změnu názvu na DPPC byla skutečnost, že termín PCO obsahově nevystihuje funkci poplachového přijímacího centra, ale pouze vlastní zařízení pro příjem a zpracování poplachových zpráv (ČSN EN 50531-1, 2007, s. 17). Protože termín DPPC je v systémech hlášení poplachového stavu novinkou a v běžné praxi bezpečnostních agentur i odborné literatuře je široce rozšířeno původní označení PCO, budu pro označení dohledových a poplachových přijímacích center v této práci používat termín DPPC/PCO. V souvislosti s rozvojem nových technologií a souvisejícím rozšiřováním pole působnosti DPPC/PCO se lze v odborné praxi setkat rovněž s termínem Multifunkční dohledová centra (dále jen „MDC“).

2.1 Definice, vymezení souvisejících pojmů

DPPC/PCO jsou součástí tzv. systémů centralizované ochrany (dále jen „SCO“), které lze definovat jako dispečerské pracoviště s nepřetržitým provozem, které sleduje a vyhodnocuje prostřednictvím monitorovacího zařízení zprávy přicházející z EZS ve střeženém objektu, řídí a koordinuje činnost zásahové jednotky. Na SCO jsou přenášeny komunikačním zařízením zvoleným zákazníkem informace o objektu zaznamenané prostřednictvím EZS. Veškerá komunikace mezi SCO a EZS, jakožto i komunikace mezi operátorem SCO a zásahovou jednotkou, nebo operátorem SCO a zákazníkem (kontaktní

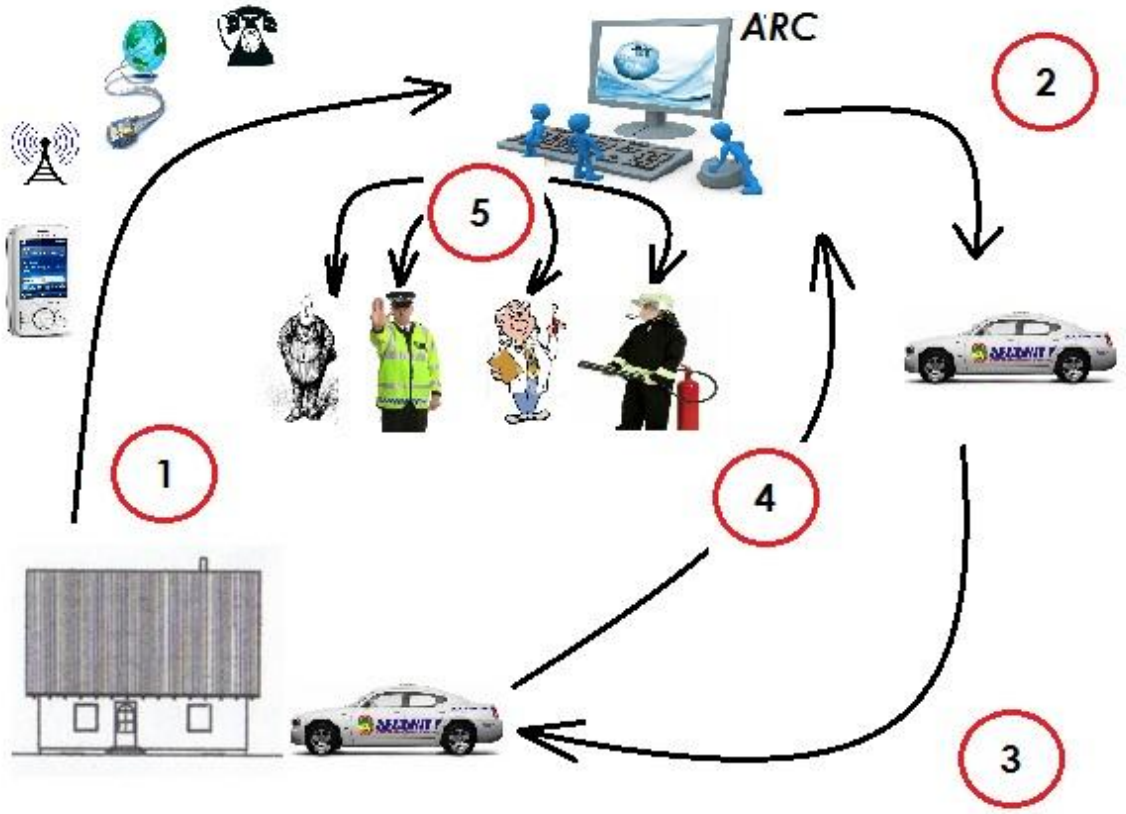
---

[1] Název PCO původně představoval jedno z pracovišť Policie ČR, zpravidla pracoviště dispečerské, které provádělo vyhodnocování signálů elektrické zabezpečovací signalizace. V současnosti má však PCO daleko širší význam a zahrnuje rovněž širší okruh činností.

[2] Jedná se o českou verzí evropské normy EN 50518-1:2010. Překlad byl zajištěn Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví. Má stejný status jako oficiální verze.

[3] ČSN EN 50518 se vztahuje na veškerá dohledová a poplachová přijímací centra , sloužící k monitorování a/nebo příjmu a/nebo zpracování signálů vyžadujících odezvu v případě mimořádné události – angl. monitoring and alarm receiving centre (dále jen „MARC“). Protože však ve všech existujících dokumentech řady 50131-1 zpracovaných technickou komisí CLC/TC 79, Poplachové systémy, je používán termín alarm receiving centre (dále jen „ARC“) zkratka ARC, v českém překladu normy je používána zkratka ARC (ekvivalent MARC).

osobou) je monitorována (nahrávána). Pro potřeby koordinace zásahu muže být objekt fotograficky zdokumentován (Tyco Fire & Integrated Solutions/ADT, 2010). Dle Uhláře (2005) jsou SCO ze strukturálního hlediska tvořeny soustavou objektů, chráněných EZS, a soustředěním jejich poplachového signálu do jednoho centra, na DPPC/PCO. Vytvoření SCO zahrnuje kromě instalace vlastního DPPC/PCO ještě celý komplex dalších opatření (např. informační tok, zásahová dokumentace, zásahová skupina a její kvalifikovaný zákrok), která zpětně podmiňují efektivní provoz celého systému (Uhlář, 2005, s. 142). Řetězový diagram celkového postupu poplachového systému je zachycen na obrázku 2.



Obrázek 2 - Řetězový diagram celkového postupu poplachového systému [18]

Definice DPPC/PCO se různí. Např. Evropská konfederace bezpečnostních služeb, angl. Confederation of European Security Services (dále jen „CoESS“) popisuje DPCC/PCO jako činnost operátora, který elektronickou cestou shromažďuje informace z různých zdrojů, analyzuje je a přiměřeným způsobem interpretuje. Následně rozhodne o vhodné reakci na vzniklou situaci (intervence ze strany bezpečnostních jednotek, video

ověření apod.) a incident vyřeší, přičemž informuje všechny zúčastněné strany (Alarm Receiving Centres: A Central Function in the European Security Landscape, 2009, s. 7). Podobnou definici lze nalézt na webových stránkách bezpečnostní agentury Henig, v jejímž pojetí představuje DPPC/PCO monitorovací centrum, do kterého jsou nepřetržitě přenášeny veškeré údaje z bezpečnostních systémů. Operátor tyto události vyhodnocuje na základě pevně stanovených pravidel a podle zvolené služby klientem. V případě zjištění odchylky od běžného stavu je iniciováno přiměřené opatření – výjezd mobilní hlídky, předání informace určené osobě, zajištění technického servisu, atd. (Pult centrální ochrany, 2013) Poměrně obsáhlou definici DPPC/PCO uvádí ve své publikaci z roku 2005 Uhlář, který pod pojmem DPPC rozumí soubory zařízení umístěné v objektech provozovatele a případně ve vybraných objektech umožňující přenos, příjem a vyhodnocení signálů ze zabezpečených objektů (EZS) a dále kontrolu a ovládání technického stavu použitých zařízení a přenosových cest. Signály jsou přenášeny přenosovými zařízeními jednotnou telekomunikační sítí (JTS), Internetem, LAN sítěmi, elektrickou rozvodovou sítí rádiovým přenosem nebo sítěmi GSM/GPRS[4] a slouží k získání a přenosu informací potřebných zejména k odvrácení útoků proti objektům chráněným tímto systémem. Dle Kocábka a Koníčka (2006), kteří pro DPCC/PCO používají označení MDC, se jedná o centra vybavená špičkovými technologiemi a obsluhovaná zkušenými pracovníky na vysoké odborné úrovni. *„Mimořádná pozornost je v tomto případě věnována bezpečnosti a spolehlivosti. MDC mají úzké kontakty na příslušné organizace a složky a představují tak neocenitelné spolupracovníky krizových štábů připojených organizací (jsou součástí jejich krizových plánů) atd. Jsou pověřována určitými samostatnými činnostmi nebo jejich organizováním či zajišťováním. Zajišťování provozuschopnosti, ochrany majetku a zdraví a životů osob, požární ochrany, ochrany před ekologickými haváriemi prostřednictvím multifunkčních dohledových center představuje v současné době v této oblasti nejvyšší možnou známou úroveň“* [2].

Navzdory rozdílnosti všechny uvedené definice obsahují totožné prvky a při určitém stupni zobecnění lze DPCC/PCO definovat v souladu s normou ČSN EN 50131-1 Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 1: Systémové požadavky[5] jako trvale obsluhované dohledové pracoviště, do kterého jsou předávány

[4] V současnosti je spektrum mobilních datových sítí obsáhlejší, kromě uvedených zahrnuje EDGE, 3G, HSDPA, HSUPA, HSPA (plus), LTE.

[5] Česká verze evropské normy EN 50131-1:2006.

informace z jednoho nebo více poplachových zabezpečovacích a tísňových systémů (dále jen „PZTS“)[6].

2.2 Komponenty DPPC/PCO

DPPC/PCO jsou obvykle koncipována dvěma způsoby:

- jako autonomní (samostatný) systém s vlastním síťovým napájením a zálohováním,
- jako integrální součást osobního počítače. [9]

Obrázek 3 - Možná podoba DPPC

Systémy autonomní jsou schopné plnohodnotného provozu bez dalších přístrojů. Obvykle jsou vybavené displejem a tiskárnou. Jejich součástí je napájecí zdroj se zálohovaným akumulátorem. Pro uživatelsky přívětivější obsluhu a využití různých softwarových kombinací se k systému připojuje počítač (Uhlář, 2005, s. 156). Pro podporu DPPC je přednostně využíván software, který umožňuje sledovat různé doplňkové funkce, především stav akumulátorů, stav ústředny, detektorů, napájení. Pro vlastní práci operátora

[6] PZTS je normami stanoveným novým označením elektrické zabezpečovací signalizace (dále jen „EZS“). Zkratka EZS byla používána pro pojem „elektrická zabezpečovací signalizace“ až do roku 2002, následně se změnila na „elektrické zabezpečovací systémy“. V roce 2009 byla v důsledku zavedení nové normy ČSN EN 50131-1 ed. 2:2007 rozlišující mezi dvěma odvětvími poplachových systémů EZS nahrazena novými termíny „poplachové systémy pro detekci vniknutí“ (IAS – intruder alarm system, resp. PZS – poplachový zabezpečovací systém) a „poplachové systémy pro detekci přepadení“ (HAS – hold-up alarm system, resp. PTS – poplachový tísňový systém). V celkovém pojetí oboru, resp. po spojení obou odvětví, se pak používá označení I&HAS – intruder and hold-up alarm system, resp. PZTS – poplachový zabezpečovací a tísňový systém.

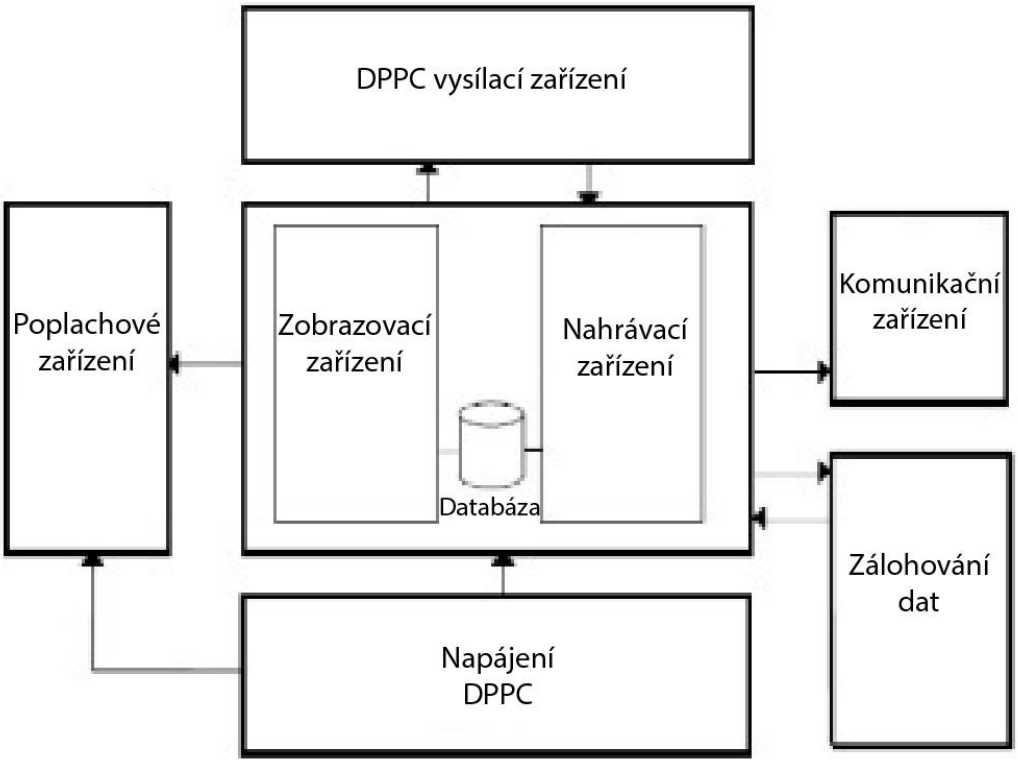
DPPC se využívá především zobrazování map a plánků střeženého objektu a okolí, případné trasy a přístup k objektu. Dále přímo konkrétních plánů jednotlivých střežených budov, podlaží, místností apod. Jakmile dojde k výpadku napájení, je zařízení mimo této signalizace schopno předat veškeré potřebné informace dispečinku, rovněž při výpadku napájení na dispečinku je zařízení zálohováno z akumulátoru. Po dobu výpadku sice zpravidla nelze použít doplňky software, nespornou výhodou je však okamžitá a levná záloha DPPC/PCO, neboť vhodný akumulátor umožňuje překlenout bez problému i výpadek 24 i více hodin [9].

Systémy integrované vyžadují ke svému provozu plný provoz osobního počítače. Při poruše harddisku, na němž je základní software uložen, dochází ke kompletnímu kolapsu funkcí DPPC. Totéž se stane v případě poruchy softwarového charakteru, kterou vzhledem ke složitosti operačního systému nelze vyloučit. U tohoto systému je rovněž podstatně složitější zajistit podmínku bezporuchového provozu při výpadku síťového napětí [1]. Přestože existují zdroje nepřerušovaného napájení, angl. uninterruptible power systems (dále jen „UPS“), problém je v jejich kapacitě a ceně. Nejlepší řešení v tomto případě představuje UPS kryjící pouze dobu nastartování benzinového nebo naftového generátoru. Tento systém je složitější a dražší [9].

Specifikace technických požadavků na poplachové přenosové systémy a zařízení používaná pro DPPC/PCO s přihlédnutím k vlastnostem jednotlivých přenosových soustav a přístrojů tvořících konfiguraci DPPC/PCO je zachycena na obrázku 3.

DPPC/PCO obvykle sestávají z následujících částí:

1) receiving centre tranceiver (dále jen „RCT“),
2) vybavení pro vyhlášení poplachu,
3) napájení (včetně záložních zdrojů),
4) záznamové zařízení,
5) komunikační zařízení,
6) zařízení pro potvrzení alarmu – volitelná část. [10]



Obrázek 4 - Uspořádání jednotlivých komponent v rámci DPPC/PCO [10]

RCT představuje zařízení DPPC/PCO pro přenos signálu, které zahrnuje rozhraní zařízení pro vyhlášení poplachu a rozhraní jedné nebo více přenosových sítí. RCT by mělo mít dostatečnou kapacitu na příjem všech signálů z kontrolovaných prostor. Všechny signály přijímané DPPC/PCO by měly být zaznamenány buď RCT nebo hlásícím zařízením. Všechny signály obdržené RCT by měly být neprodleně předány zařízení pro vyhlášení poplachu [10].

Zařízení pro vyhlašování poplachu v DPPC/PCO by mělo mít dostatečnou kapacitu pro příjem a zobrazování všech signálů z kontrolovaných prostor. Informace lze zobrazit na terminálu a to s jasnými nebo jednoduše kódovanými zprávami. Prioritní kódy by měly být dodávány tak, aby došlo k okamžitému vyslání poplachového signálu, a měly by být zobrazeny až do ukončení poplachu. Vyhlašovací zařízení by mělo disponovat takovými prostředky, aby operátor mohl řídit poplach [10].

Jako hlavní zdroj elektrické energie pro DPPC/PCO lze použít napájení ze sítě. K dispozici musí být záložní zdroj energie. Přepnutí na, nebo z pohotovostního zdroje nesmí způsobit poškození zařízení. V provozní oblasti musí být k dispozici údaje o aktuálně využívaném zdroji energie. Síťové napájení musí mít dostatečný výkon pro běžné zatížení DPPC/PCO a simultánní dobíjení staničních baterií do požadované kapacity v rámci 24 hodin. Pohotovostní napájecí kabely vně pláště DPPC/PCO musí být chráněny proti mechanickému poškození a požáru. [6]

Pohotovostní režim napájení musí mít dostatečnou kapacitu pro nepřetržitý provoz veškeré komunikace, signalizace, sledování, nahrávání, základního větrání a základního osvětlení, včetně energie potřebné pro 24 hodinový provoz centra (stanovuje se jako jeden a půl násobek průměrné poptávky).

Může mít podobu:

- Záložní baterie s přidruženým nabíjecím zařízením: Záložní baterie musí být uvedena do provozu automaticky ihned po poklesu primárního napětí pod úroveň požadovanou pro provoz DPPC/PCO. Po obnovení primárního napětí se DPPC/PCO musí vrátit do základního provozu a záložní baterie se musí začít automaticky dobíjet. Záložní baterie musí být chráněny pojistkami nebo jističi. Baterie musí být v souladu s ČSN EN 50272-2 (364380) – Bezpečnostní požadavky pro akumulátorové baterie a akumulátorové instalace – Část 2: Staniční baterie. Použije-li se záložní generátor, musí být kapacita záložních baterií dostatečná pro napájení DPPC/PCO na minimálně 2 hodiny (stanovuje se jako jeden a půl násobek průměrné poptávky). Použije-li se druhý záložní generátor, kapacita baterie musí být taková, aby poskytla požadovanou energii pro minimálně 30 minutový provoz [6].
- Záložního generátoru nebo generátorů podporovaných pohotovostními bateriemi a souvisejícím nabíjením zařízením: Generátor situovaný uvnitř pláště DPPC/PCO musí být oddělen od provozní oblasti ohnivzdornou konstrukcí. Všechny záložní generátory musí být vybaveny takovým množstvím paliva, aby dokázaly udržovat centrum v provozu po dobu nejméně 24 hodin. Všechny záložní generátory musí mít nezávislý způsob spouštění, který musí být automaticky aktivován, pokud normální napájení

selže. Baterie potřebné pro aktivaci záložního generátoru musí být napájeny z primárního zdroje. Pokud není záložní generátor nainstalována uvnitř DPPC/PCO, musí být umístěn v prostoru s omezeným přístupem, který je chráněn proti vniknutí a požáru. [6]

Dle ČSN 50518-3 by záložní baterie a další podobné zdroje energie měly být umístěny uvnitř pláště DPPC/PCO.

2.3 Činnost DPPC/PCO

DPPC/PCO lze označit za jedno z nejdůležitějších pracovišť průmyslu komerční bezpečnosti. Chrání bezpečnost klientů bezpečnostních agentur 24 hodin denně 7 dní v týdnu a v případě, že dojde k aktivaci systému, zajišťují jejich okamžitou informovanost a realizaci vzájemně dohodnutých postupů.

DPPC/PCO jsou v pravidelném kontaktu se zákazníky, instalátory bezpečnostních systémů a zásahovými jednotkami a to následujícími způsoby:

- odesíláním denních zpráv o aktivacích, k nimž došlo v průběhu uplynulých 24 hodin,
- informováním klientů, kteří náhodně spustili poplachové systémy (včetně poskytování asistenčních služeb klientům, kteří mají problémy s monitorovaným poplachovým zařízením v jejich vlastnictví),
- informováním zásahových jednotek o případných aktivacích instalovaných poplachových systémů,
- vyřizováním požadavků záchranné služby na poskytnutí většího množství informací o případné aktivaci. [11]

DPPC/PCO jsou velmi důležitá pro organizace, jako jsou např. pojišťovny, které je využívají na sledování jimi pojištěných systémů. Maloobchodníci využívají DPPC/PCO k ochraně svých prostorů, majetku a personálu. Z výše uvedeného vyplývá, že DPPC/PCO představují plnohodnotnou součást soukromých bezpečnostních služeb, o čemž svědčí skutečnost, že ve většině evropských zemí jsou tyto činnosti zahrnuty ve vnitrostátních soukromých bezpečnostních právních předpisech. [11]

DPPC/PCO jsou schopna monitorovat bezpečnostní situaci, servisní potřeby, technologické i logistické procesy, kontrolovat, řídit a koordinovat činnosti související

s bezpečností na jednotlivých objektech, jakož i celku jako takovém. Veškeré přicházející informace jsou do nich svedeny různými druhy komunikačních tras, které jsou vždy dvoj až trojnásobně zálohovány. Jedná se zejména o informace hlasové a datové, hlášeny jsou stavy technologických zařízení, bezpečnostních systémů a v neposlední řadě i informace o stavu a pohybu vozidel nebo jiných mobilních objektů, možné je sledovat i pohyb osob. Veškerá propojení jsou realizována na úrovni přímé integrace do infrastruktury poskytovatelů, ať již telekomunikačních nebo jiných služeb. Řešení komunikace umožňuje ten nejbezpečnější přístup k informacím zejména vlastním servisním pracovníkům, kteří kdekoliv v terénu mají všechny potřebné informace okamžitě k dispozici. Klienti mají neustálý přehled o stavu na jednotlivých objektech prostřednictvím SMS zpráv, které dostávají přímo na své mobilní telefony v reálném čase prostřednictvím bezpečného přenosu. Totéž platí o jednoduché komunikaci klientů s DPPC/PCO[7] [2]

Zabezpečení objektů je zahájeno rozčleněním prostoru do sledovaných úseků. Ve stanovených zónách jsou strategicky umístněna detekční zařízení (EZS, EPS). Při nestandardní situaci (např. pohybu) se tato zařízení zaktivují spolu s nejbližší nainstalovanou bezpečnostní kamerou, která bezprostředně začne snímat záznam z místa nečekaného dění. Zachycený záznam je ve stejnou dobu přenášen do DPPC/PCO, kde operátoři pultu centrální ochrany ve směnách sledují a hlídají 24 hodin denně střežené objekty. Operátor na základě monitoringu a rozboru událostí vyhodnotí závažnost narušení objektu. Pakliže to situace vyžaduje, reaguje operátor dle smluvního ustanovení a požadavků například okamžitým výjezdem zásahové jednotky PCO, kontaktuje majitele či správce objektu, případně přivolá policii k dopadení pachatele. Při hromadném napadení objektu či střeženého prostoru využívá operátor výhod několika současně přenášených záznamů z více bezpečnostních kamer najednou. Nejúčinnějším doplňkem dálkové ostrahy DPPC/PCO jsou pak reproduktory zabudované v hlídaném objektu, které hlasem upozorní pachatele na skutečnost, že je sledován. Ve většině případů je to dostatečně účinný prostředek pro zajištění bezproblémového odchodu narušitele. Sledování střežených objektů pomocí nepřetržitého monitoringu PCO pomáhá do značné míry k dopadení pachatele. Záznamy bezpečnostních kamer, které se po určitý čas archivují, jsou přímými důkazy kriminálních stop pachatele a jejich rozborem je možné nastínit také identitu zločince. [2]

[7] MDC umožňují klientům kontakt prostřednictvím tzv. jednotného čísla, díky kterému se dovolají vždy a z každého místa v republice za cenu místního poplatku přímo na operátora, který má k dispozici veškeré potřebné informace a je schopen zajistit jakoukoliv smluvní službu.

Vlastní činnost DPPC/PCO zahrnuje:

- napojení různých bezpečnostních systémů na multifunkční dohledové centrum všemi dostupnými prostředky,
- přímé spojení a úzkou spolupráci s IZS,
- nepřetržitý bezpečnostní monitoring objektů zahrnující napadení, požár, signály tísní, signály ze stanovišť místní ostrahy atd.,
- bezpečnostní a logistický monitoring vozidel,
- vyrozumění oprávněných osob o poplachu v objektu,
- identifikaci pohybu osob,
- výjezd a zásah stálé výjezdové skupiny,
- zadržení pachatele, který se nachází v napadeném objektu a jeho předání policii ČR (dále jen „PČR“),
- reakci a součinnost při řešení mimořádných událostí v celé ČR,
- přenos technických a provozních zpráv (výpadky elektrického proudu apod.),
- dálkový dohled a servis napojených systémů,
- kontrolu přenosové cesty dle výběru uživatele, možnost zdvojení přenosových tras dle požadavků pojišťoven a norem ČSN EN,
- technickou pomoc uživatelům,
- možnost sledování určených časů uzamčení (zakódování) systému,
- dálkovou kontrolu překročení technických stavů (teplota, zaplavení, úniky plynů, vlhkost apod.) se zajištěním adekvátní reakce,
- monitoring a zajištění výjezdu v případech havárie plynu, vody, v krizových situacích (povodeň, požár),
- zajištění datových sítí,
- střežení objektu do příjezdu odpovědné osoby nebo policie,

- služby spojené s požární ochranou a prevencí,
- provádění plánovaných a termínovaných kontrol objektu,
- dovoz odpovědných osob,
- klíčová služba k objektům,
- poskytnutí pravidelného či jednorázového výpisu událostí, jednotný systém pro vyúčtování pro více objektů,
- zajištění informační bezpečnosti dle normy ČSN ISO/IEC 17799 (369790) Informační technologie – Bezpečnostní techniky – Soubor postupů pro management bezpečnosti informací,
- zpracování zprávy v případě napadení objektu,
- spojení na oficiální linky pomoci,
- poradenství,
- help line 24 hodin denně [2].

Prostřednictvím centralizace informací lze získat rovněž informace důležité pro provádění preventivních opatření na úrovni obce či na příslušném teritoriálním policejním pracovišti, např. o počtu mimořádných událostí vzhledem ke dni v týdnu. Výhody DPPC/PCO se dají velmi dobře skloubit s nejmodernějšími prvky inteligentních budov a mohou tak jednoznačně přispívat k dokonalému využití techniky a lidského potenciálu k ochraně osob a majetku, tedy k bezpečným lokalitám v různých obcích či částech větších měst [2]

2.4 Provozovatelé DPPC/PCO

V českém prostředí lze DPPC/PCO v širším slova smyslu rozdělit na:

- pracoviště PČR, kde se soustřeďují informace z technických bezpečnostních systémů,
- pracoviště obecní policie (zpravidla městské) sloužící k témuž účelu,

- pracoviště Hasičského záchranného sboru (dále jen „HZS“), kde se soustřeďují informace o vzniklém požárním nebezpečí získané z technických prostředků Elektrické požární signalizace (dále jen „EPS“),
- pracoviště integrovaného záchranného systému (dále jen „IZS“) kraje/okresu/oblasti, kde se soustřeďují informace z různých technických zařízení sloužících pro řízení IZS – I&HAS, EPS, uzavřené televizní okruhy (dále jen „CCTV“)[8] apod.,
- pracoviště firem podnikajících v průmyslu komerční bezpečnosti, kde jsou soustřeďovány informace z různých technických bezpečnostních systémů a současně je zde organizován represivní zásah a následný informační tok k zákazníkovi a součinnostním složkám, tedy PČR, obecní policii, HZS, IZS apod. [9]

Provozování systému centralizované ochrany PČR upravují interní normativní akty, čímž byly vytvořeny potřebné předpoklady nutné k ujednocení podmínek připojení civilních objektů na policejní DPPC/PCO. Na ty jsou napojovány především objekty s vyššími riziky na daném teritoriu (např. peněžní ústavy) a podle kapacitních a technických možností i další objekty se zvýšenými riziky. O zřízení DPPC/PCO rozhoduje a za jeho provoz odpovídá ředitel příslušného útvaru PČR. O napojení objektů mohou přímo žádat vlastníci významných a důležitých státních, hospodářských, kulturních a dalších objektů přímo ředitele PČR za taxativně vymezených podmínek. Při posuzování účelnosti napojení objektu na DPPC/PCO se vychází především z potřeb bezpečnostní situace v teritoriu provozovatele a z významu objektu.

Přihlíží se především k:

- vyšším rizikům ohrožení objektu krádežemi, vloupáním nebo loupežemi,
- výši chráněných hodnot a charakteru provozních prostředků – preferovány jsou objekty uchovávající vyšší finanční hotovost, cenné materiály, kulturními památkami, s utajovanými skutečnostmi a informačními soubory, se zbožím nebo materiály nebezpečné povahy a jaderná zařízení. [1]

[8] Z angl. closed circuit television

Předmět podnikání	**Požadovaná odborná a jiná zvláštní způsobilost podle § 27 odst. 1 a 2**	**Podmínky, jejichž splnění se vyžaduje podle § 27 odst. 3**	**Poznámka**
ostraha majetku a osob	a) vysokoškolské vzdělání, b) vyšší odborné vzdělání právnického, bezpečnostního nebo obdobného zaměření, c) střední vzdělání s maturitou v oboru bezpečnostním nebo právním a 3 roky praxe v oboru, d) střední vzdělání s maturitou, 3 roky praxe v oboru a osvědčení o rekvalifikaci nebo jiný doklad o odborné kvalifikaci pro příslušnou pracovní činnost vydaný zařízením akreditovaným podle zvláštních právních předpisů, zařízením akreditovaným MŠMT, nebo ministerstvem, do jehož působnosti patří odvětví, v němž je živnost provozována, nebo e) střední vzdělání s maturitní zkouškou, 3 roky praxe v oboru a profesní kvalifikace pro činnost strážný podle zvláštního právního předpisu*)	spolehlivost podnikatele, statutárního orgánu nebo členů statutárního orgánu**) a bezúhonnost všech osob, které pro podnikatele předmětnou činnost vykonávají (ust. § 6 odst. 2 živnostenského zákona)	*) zákon č. 179/2006 Sb., o ověřování a uznávání výsledků dalšího vzdělávání a o změně některých zákonů, ve znění pozdějších předpisů **) ust. § 1 odst. 5 živnostenského zákona

Tabulka 1 - Podmínky pro výkon koncesované živnosti „Ostraha majetku a osob“[12]

Informace o napojení objektu a parametry systému a signalizace napojených objektů podléhají utajení. Konečný souhlas ředitele PČR s napojením objektu na

DPPC/PCO je vázán na to, aby žadatel splnil všechny podmínky potřebné k napojení objektu. Rovněž se přihlíží k posouzení vypracovanému speciálními pracovišti služby kriminální policie a vyšetřování. Uhlář (2005) uvádí, že počet civilních objektů napojených na DPPC/PCO PČR činí cca 4500, přičemž nejvýznamnějšími druhy napojených objektů jsou peněžní ústavy (42 %), objekty státní správy (17 %) a objekty s movitým kulturním dědictvím (10 %). Zájem o napojení civilních objektů je značný, což se odvíjí od bezplatného poskytování zákroku a obsluhy. Autor upozorňuje na skutečnost, že zde dochází k rozporu mezi koncepcí prevence kriminality, která považuje SCO za významný prostředek situační prevence, a aktuální situací v PČR, kdy jsou omezené síly a prostředky především v oblasti pořádkové služby zajišťující zákrok.

Kromě civilních objektů se na DPPC/PCO PČR napojují rovněž objekty Ministerstva vnitra ČR (dále jen „MV ČR“) a PČR. DPPC/PCO se využívají rovněž k vyhodnocování výstupů z objektů, kde je policií použita zabezpečovací technika jako podpůrný operativně pátrací prostředek. Jak vyplývá z ust. § 70 odst. 2 zákona č. 278/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů (dále jen „zákon o PČR“): *„Získávání poznatků ze zájmového prostředí je činnost policisty, který se zastíráním skutečného účelu své činnosti aktivně vyhledává, dokumentuje a vyhodnocuje poznatky o zájmovém prostředí a osobách v něm se pohybujících. V rámci této činnosti je policista oprávněn využívat podpůrné operativně pátrací prostředky.“* Zájmovým prostředím se pro účely zákona o PČR rozumí prostředí, v němž lze důvodně předpokládat získání poznatků důležitých pro zamezování, odhalování a dokumentování trestných činů, ke zjišťování jejich pachatelů a k předcházení těmto trestným činům (ust. § 70 odst. 1 zákona o PČR).

Jiná je situace v případě policie obecní. Taxativní výčet činností strážníka obecní policie při zabezpečování místních záležitostí veřejného pořádku v rámci působnosti obce uvádí zákon ČNR č. 553/1991 Sb., o obecní policii, ve znění pozdějších předpisů (dále jen „zákon o obecní policii“):

- přispívá k ochraně a bezpečnosti osob a majetku,
- dohlíží na dodržování pravidel občanského soužití,
- dohlíží na dodržování obecně závazných vyhlášek a nařízení obce,

- podílí se v rozsahu stanoveném zákonem o obecní policii nebo zvláštním zákonem na dohledu na bezpečnost a plynulost provozu na pozemních komunikacích,
- podílí se na dodržování právních předpisů o ochraně veřejného pořádku a v rozsahu svých povinností a oprávnění stanovených tímto nebo zvláštním zákonem činí opatření k jeho obnovení,
- podílí se na prevenci kriminality v obci,
- provádí dohled nad dodržováním čistoty na veřejných prostranstvích[5)] v obci, odhaluje přestupky a jiné správní delikty, jejichž projednávání je v působnosti obce, poskytuje za účelem zpracování statistických údajů MV ČR na požádání údaje o obecní policii (ust. § 2 zákona o obecní policii).

Podle zákona o obecní policii tedy strážníci přispívají k ochraně bezpečnosti osob a majetku, nicméně s odkazem na obsah ust. § 35 odst. 2 zákona č. 128/2000 Sb. o obcích (obecní zřízení), ve znění pozdějších předpisů (dále jen „zákon o obcích“), který uvádí výčet záležitostí v samostatné působnosti obce a s přihlédnutím k ust. §§ 84, 85 a 102 téhož zákona, nelze považovat nepřetržitou ostrahu majetku právnických či fyzických osob (za úplatu), za plnění úkolů obce v samostatné působnosti, resp. za zabezpečování místních záležitostí veřejného pořádku, neboť obce podle zákona o obcích nenesou odpovědnost za majetek svých občanů. Z výše uvedeného vyplývá, že obecní policie má ve smyslu zákona o obecní policii v těchto případech pouze podpůrnou úlohu, omezenou na požadavky bezprostředního zákroku, neodkladného úkonu či provedení jiného opatření, zpravidla ve prospěch PČR [2].

Na základě uvedených skutečností nelze než se ztotožnit s výroky odboru bezpečnostní politiky MV ČR, který konstatuje:

1. Obec nemůže zajišťovat nepřetržitou ostrahu majetku fyzických a právnických osob na komerční bázi prostřednictvím DPPC/PCO obsluhovaným strážníky obecní policie, ani zaměstnanci obce zařazenými do obecní policie, kteří sice vykonávají „podpůrnou“ činnost pro strážníky, nicméně vždy se bude jednat o úkony spadající do věcné působnosti obecní policie.

2. Strážníci obecní policie nejsou oprávněni v době svého zaměstnání provádět nepřetržitou ostrahu majetku fyzických a právnických osob na komerčním základě.
3. Na druhé straně je ovšem strážník povinen v mezích zákona o obecní policii provést zákrok nebo úkon, nebo učinit jiné opatření, je-li páchán trestný čin nebo přestupek či jiný správní delikt anebo je-li důvodné podezření z jejich spáchání. To znamená, že pokud strážník obecní policie obdrží oznámení, že na území obce je pácháno zmíněné protiprávní jednání, je povinen odpovídajícím způsobem zakročit [2].

Obecní policie je tedy zřízena za účelem zabezpečování místních záležitostí veřejného pořádku a nelze ji tedy považovat za subjekt oprávněný provozovat koncesovanou živnost, ani za instituci, která by se na předmětné komerční činnosti mohla přímo spolupodílet. Navíc zaměstnanci obce zařazení k obecní policii (strážníci) musí pro výkon svého povolání splňovat jiná kritéria, než jaká stanoví u zaměstnanců výše uvedených soukromoprávních subjektů živnostenský zákon [2].

Mezi stanovená kritéria objektů s možností připojení na DPPC/PCO patří především:

- objekt je majetkem obce nebo města;
- objekt není využíván ke komerčním účelům a není v něm provozována žádná komerční činnost;
- objekty ani jejich části nejsou pronajímány ani zapůjčovány jiným právním subjektům;
- možnost připojení objektu na DPPC/PCO posoudí odborní pracovníci obecní policie;
- potřebné technické zařízení a připojení na DPPC/PCO zaplatí provozovatel objektu;
- ve sporných případech rozhodne o připojení objektu na DPPC/PCO orgán obce/města [1]

2.5 Umístění a konstrukční požadavky DPPC/PCO

2.5.1 Umístění

V umisťování DPPC/PCO hraje zásadní roli proces hodnocení rizik, což je řada logických kroků týkající se identifikace nebezpečí a analýzy rizik s nimi spojených. Mělo by se jednat o kontinuální proces. Dle Raise (2006) představuje hodnocení rizik neustálé zvažování poškození aktivit, která mohou být způsobena naplněním hrozeb, přičemž je nutno vzít v úvahu veškeré potenciální důsledky, a reálné pravděpodobnosti výskytu takových rizik z pohledu převažujících hrozeb, zranitelnosti a aktuálně implementovaných opatření. Záznamy o posouzení rizik musí být udržovány a k dispozici pro případný audit. [6]

DPPC/PCO musí být umístěno uvnitř trvalé stavby na místě s nízkým rizikem požáru, výbuchu, záplavy, vandalismu a jiných nebezpečí. Nezabírá-li celou budovu, ve které se nachází, je třeba jej od zbývající části budovy fyzicky oddělit. Přístup do budovy nebo části budovy, v níž se DPPC/PCO nachází, by měl být obsazen pouze společností centrum provozující. [6]

2.5.2 Konstrukce

Plášť DPPC/PCO tvoří obvodové stěny, podlahy, stropy, dveře, okna, klimatizace, vstupních body pro servisní kabely a potrubí. DPPC/PCO musí být chráněno proti:

- fyzickému útoku: parametry odolnosti proti fyzickému útoku jsou uvedeny v tabulce 2, odolnost pro dveře, okna a další uzávěry musí být v souladu s normou EN 1627[9] **(**třída odolnosti 4);
- útoku střelnou zbraní: odolnost pro dveře, okna a další uzávěry musí být v souladu s normou EN 1522 FB4[10];
- ohni: plášť DPPC/PCO musí mít požární odolnost v souladu s EN 13501-2[11] (ne méně než 30 min);

[9] Uvedená norma byla do normalizačního systému ČR zavedena v ČSN P ENV 1627 Okna, dveře, uzávěry – Odolnost proti násilnému vniknutí – Požadavky a klasifikace. Tato předběžná norma určuje požadavky na odolnost proti násilnému vniknutí u dveří, oken a uzávěrů. Vztahuje se na následující způsoby otevírání: otáčení, sklápění, skládání, otevírání a sklápění, posunování (vodorovné a svislé) a navinování jakož i na pevné konstrukce..

[10] Uvedená norma byla zavedena v ČSN EN 15022:2000 (74 6006) Okna, dveře, uzávěry a rolety – Odolnost proti průstřelu – Požadavky a klasifikace.

[11] Uvedená norma byla zavedena v ČSN EN 13501-2+A1:2010 (73 0860) Požární klasifikace stavebních výrobků a konstrukcí staveb – Část 2: Klasifikace podle výsledků zkoušek požární odolnosti kromě vzduchotechnických zařízení.

- proti bleskům: doporučuje se chránit DPPC/PCO před účinky úderu blesku v souladu s 301 EN 62305; Pro každý jednotlivý ARC by měla být udělána analýza rizik v souladu s EN 62305-2[12] . [6]

konstrukční prvky	materiály	tloušťka
obvodové stěny včetně zdi mezi stanicí a vstupní halou	masivní zdivo	> 200 mm
	litý beton	> 150 mm
	železobeton	> 100 mm
	masivní ocel	> 10 mm
vnitřní stěny	žádné požadavky	žádné požadavky
podlahy a stropy	litý beton	> 150 mm
	železobeton	> 100 mm

Tabulka 2 - Minimální hodnoty proti fyzickému útoku [6]

Ve struktuře DPPC/PCO jsou povoleny pouze následující otvory:

- Vstupní hala: skládá se ze dvou dveří, jejichž rozměry nesmí překročit 2,5 m na výšku a 1,1 m na šířku a podlahové plochy, která nesmí překročit 6 m^2. Dveře musí být zajištěny, aby se zabránilo jejich otevření ve stejnou dobu (s výjimkou kontrolní činnosti). Dveře mezi DPPC/PCO a vstupní halou se musí otvírat do vstupní haly, externí dveře vstupní haly se musí vždy otevírat směrem ven. Jedny dveře musí být ohnivzdorné v souladu s EN 13501-2. Druhé dveře musí splňovat třídu odolnosti 4 (v souladu s EN 1627). Zámky musí být v souladu s EN 12209[13], zámkové válce v souladu s EN 1303[14] a klikové páky a knoflíky nábytku v souladu s EN 1906[15]. Oboje

[12] Soubor EN 62305 byl zaveden v souboru ČSN EN 62305 (34 1390) Ochrana před bleskem.

[13] Uvedená norma byla zavedena v ČSN EN 12209:2004 (16 5124) Stavební kování – Zámky a střelkové zámky – Mechanicky ovládané zámky, střelkové zámky a zapadací plechy – Požadavky a zkušební metody

[14] Uvedená norma byla zavedena v ČSN EN 1303:2005 (16 5191) Stavební kování – Cylindrické vložky pro zámky – Požadavky a zkušební metody.

[15] Uvedená norma byla zavedena v ČSN EN 1906 (165776) - Stavební kování - Dveřní štíty, kliky a knoflíky - Požadavky a zkušební metody.

dveře musí být vybaveny odblokovacím zařízením provozu schopném pouze z DPPC/PCO, a musí být opatřeny samočinnými uzavíracími a zajišťovacími mechanismy. Dveře musí být elektricky blokované, aby se zabránilo případnému současnému nezajištění. [6]

- Zajišťovací mechanismus – rozlišuje se mezi zámkem elektromechanickým a mechanickým. Elektromechanické zajišťovací zařízení se v souladu s klasifikací 2-R-2-B-0-C-7-HB-3-E-4-3 EN 14846[16] používá k zajištění dveří vstupní haly. Jsou-li dveře v zavřené poloze, upevňovací šrouby musí být chráněny proti neoprávněným zásahům. Mechanické ovládání pro nouzové uvolnění musí být chráněno před náhodným použitím. Mechanické zajišťovací zařízení se v souladu s klasifikací 2-R-2-1-0-C-7-HB-3-E v EN 12209 používá k zajištění ostatních dveří. [6]
- Nouzový východ: dveře únikových východů včetně pantů, rámů, držáků a zajišťovacích zařízení musí splňovat stejné požadavky na sílu a odolnost, jako v případě mechanických zajišťovacích zařízení. Dveře nouzového východu se musí otevírat směrem ven a musí být opatřeny odemykacím mechanismem v souladu s EN 179[17], který může být spuštěn pouze v případě nouze. Odblokování zařízení musí být možné pouze zevnitř. [6]
- Prosklené plochy: musí poskytovat odolnost proti fyzickému útoku a útoku střelnými zbraněmi v souladu s EN 356 klasifikací P6B a EN 1063 klasifikací BR 4 – S, v případě odolnosti vůči požáru platí stejná pravidla jako pro plášť DPPC/PCO. Důležité je, aby interiér DPPC/PCO nebylo možné spatřit z žádného místa vně budovy. [6]
- Ventilace: z bezpečnostních důvodů musí být DPPC/PCO přísně nekuřácké. Větrací systémy pro DPPC/PCO musí být v souladu s EN 13779[18]. Vnitřní kvalita vzduchu musí odpovídat „malé kancelářské místnosti“. Výše uvedené normě musí odpovídat rovněž použití vzduchových filtrů (kvalita

[16] Uvedená norma byla zavedena v ČSN EN 14846:2009 (16 5192) Stavební kování – Zámky a střelkové zámky – Elektromechanicky ovládané zámky a zapadací plechy – Požadavky a zkušební metody

[17] Uvedená norma byla zavedena v ČSN EN 179:2008 (16 6237) Stavební kování – Nouzové dveřní uzávěry ovládané klikou nebo zařízením s tlačnou plochou pro používání na únikových cestách – Požadavky a zkušební metody.

[18] Uvedená norma byla zavedena v ČSN EN 13779:2010 (12 7007) Větrání nebytových budov – Základní požadavky na větrací a klimatizační zařízení

venkovního ovzduší ODA 1, kvalita vnitřního ovzduší IDA 3), podobně je tomu i v případě osobami produkovaného tepelného zatížení. Tlak musí být (30-40) dB (A). Otvory ve struktuře DPPC/PCO pro větrací systémy by měly splňovat požadavky pro odolnost proti fyzickým útokům. Překročí-li průměr příčného průřezu větracího vstupu nebo výstupu 0,02 m^2, musí být vybaven poplachovým systémem schopným včas odhalit jakýkoli pokus o vstup. Vstupní a výstupní větrací otvory v plášti DPPC/PCO musí být chráněny. [6]

- Dopravní poklop/skluz: mohou být umístěny přímo ve zdi DPPC/PCO nebo ve vstupní hale a jejich průměr nesmí překročit 0,02 m^2. Když se poklop/skluz nacházejí ve stěně DPPC/PCO, měla by se otevírat do chráněné oblasti. Otvor musí být konstruován takovým způsobem, aby odpovídal normám pro DPPC/PCO. Vstup by měl být blokován, aby se zabránilo přímému přístupu, a jeho otvírání a zavírání musí být kontrolováno z DPPC/PCO. Vnější vchod se vždy musí otevírat směrem ven. Nachází-li se poklop/skluz ve vnitřní stěně vstupní haly DPPC/PCO, musí být provozován s jedním vstupním bodem, který musí být blokován na dveřích vnější haly takovým způsobem, že poklop/skluz ani vstupní dveře nelze otevřít ve stejný čas. Otevírání a zavírání musí být kontrolováno z DPPC/PCO. Poklop musí být konstruován v takovém standardu, aby byla umožněna komunikace mezi provozní oblasti DPPC/PCO a vnějším vstupem. [6]
- Servisní vstupy a výstupy: Porušení v plášti DPPC/PCO pro přijetí jakýchkoli servisních kabelů nebo potrubí nesmí překročit 0,02 m^2 v průřezu. Průměr otvoru kolem kabelu nebo potrubí by neměl přesáhnout 1,5 mm. Tam, kde je průměr otvoru kolem kabelu nebo potrubí vyšší než 1,5 mm, musí být vyplněn materiálem ekvivalentní specifikace. [6]

Co se týká vybavenosti z hlediska potřeb obsluhy, součástí DPPC/PCO musí být WC a umývárny. K dispozici by měly být rovněž zařízení pro přípravu potravin a nápojů a musí být umístěna v DPPC/PCO. Případné spotřebiče (rychlovarná konvice, vařič apod.) musí být odděleny od provozní oblasti. [6]

2.5.3 Poplachové systémy

Elektronická detekce pro všechny základní prvky ARC musí vypadat následovně:

- Externí útok (útočník): nachází-li se DPPC/PCO jinde než v přízemí, event. může-li být přístup umožněn z nižších pater (např. ze suterénu), musí být poplašným systémem chráněna rovněž podlaha DPPC/PCO. Areál budovy, ve které sídlí společnost, která DPPC/PCO provozuje, a ve kterém se DPPC/PCO nachází, musí být chráněn systémem EZS instalovaným v souladu s ČSN EN 50131-1. Takové systémy EZS musí obsahovat výstražné zařízení k varování ARC zaměstnance ihned po vyhlášení poplachu. Doporučení pro projektování, plánování, provozu, instalaci a údržbu těchto zařízení jsou uvedeny v normě ČSN CLC/TS 50131-7 (334591) Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 7: Pokyny pro aplikace. Hodnocení rizik by mělo být provedeno určit stupeň zabezpečení systému EZS. [6]

- Oheň – systém detekce požáru musí obsahovat komponenty certifikované dle souboru ČSN EN 54 (34 2710) Elektrická požární signalizace a musí být instalován v souladu s ČSN EN 54-1 Elektrická požární signalizace – Část 1: Úvod. [6]

- Přístup/exit – slyšitelný nebo viditelný alarm se musí spustit, když některé ze vstupních dveře na PCO nebo do vstupní haly nejsou zajištěny. Alarm musí být signalizovat rovněž v případě, že došlo k nouzovému otevření dveří nebo jsou dveře do vstupní haly a ARC otevřeny ve stejnou dobu. [6]

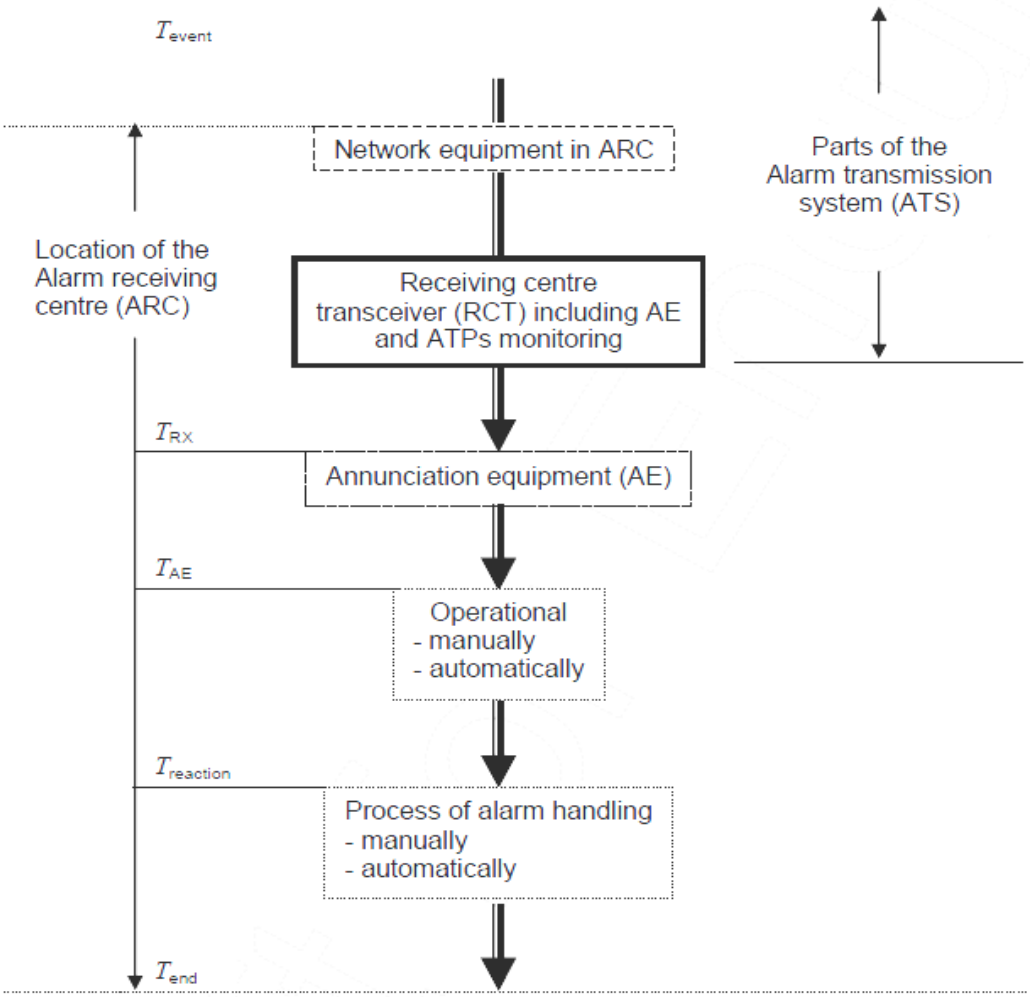
- Plyn – DPPC/PCO musí být vybaveno detekčními systémy minimálně pro stanovení oxidu uhelnatého, která upozorní zaměstnance v případě dosažení koncentrace plynu vyžadující evakuaci. [6]

- Komunikace – všechny spojovací kabely a bezdrátové připojení přenášející informace mezi DPPC/PCO a vzdálenými zabezpečovacími systémy musí být chráněno proti případným interferencím v souladu s ČSN EN 50136-1 (334596) – Poplachové systémy – Poplachové přenosové systémy a zařízení – Část 1: Obecné požadavky na poplachové přenosové systémy [6]

- Vloupání – zařízení na ochranu proti vloupání instalovaná v souladu s ČSN EN 50131-1 ed. 2 (334591) – Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 1: Systémové požadavky. se musí nalézat uvnitř DPPC/PCO na pozicích přilehlých k vstupní hale, nouzovému východu a provozní oblasti centra. [6]
- Pracovníci k monitorování bezpečnosti – bezpečnost a zabezpečení personálu DPPC/PCO musí být automaticky sledováno v maximálně 60 minutových intervalech. V případě absence odpovědi na bezpečnostní kontrolu v rámci 60 sekund je případný poplach automaticky posílán na další DPPC/PCO. [6]
- Signály z ochranných elektronických systémů – DPPC/PCO nesmí být umístěno v budově, ze které přijímá informace, nebo v její bezprostřední blízkosti. Signály z ochranných systémů musí být předávány do DPPC/PCO duálním systémem přenosu v souladu s výkonnostními parametry stanovenými ČSN EN 50136-1 (334596) – Poplachové systémy – Poplachové přenosové systémy a zařízení – Část 1: Obecné požadavky na poplachové přenosové systémy. [6]
- CCTV – systém musí být uspořádán tak, aby všechny přístupy k budově, ve které se nachází DPPC/PCO, bylo možné monitorovat zevnitř. Kontrola je nezbytná z důvodu identifikace oprávněných osob před vstupem do haly, monitoringu činnosti v hale a zajištění bezpečného odchodu. Dozor slouží rovněž k tomu, aby bylo možné identifikovat všechny zaměstnance při využití poklopu/skluzu. [6]

2.6 Technické požadavky

Norma CSN 50518-2 stanovuje u DPPC/PCO mimo jiné požadavky na výkonnost.



Obrázek 5 - Sekvence operací [8]

Vysvětlivky:

T_{event} čas počátku události

T_{RX} čas předání výstupního signálu transceiverem DPPC/PCO poplachovému zařízení

T_{AE} čas obdržení signálů poplachovým zařízením

$T_{reaction}$ čas zahájení akce ze strany operátora

T_{end} čas ukončení akce operátorem

Obrázek zobrazuje sled operací v rámci kompetencí DPPC/PCO použitelných pro jakýkoliv signál generovaný I&HAS po dokončení zpracování v RCT. Všechny signály musí být v souladu s ČSN EN 50136-1 (334596) – Poplachové systémy – Poplachové přenosové systémy a zařízení – Část 1: Obecné požadavky na poplachové přenosové systémy.

Dodatečná externí komunikační zařízení a prostředky musí být splňovat následující výkonnostní parametry:

- čas mezi T_{AE} a $T_{reaction}$ musí splňovat následující kritéria účinnosti – v případě přepadení vyhlášení poplachu do 30 vteřin pro 80 % obdržených signálů a 60 vteřin pro 98,5 % obdržených signálů;
- ostatní podmínky pro vyhlášení poplachu: 90 vteřin pro 80 % obdržených signálů a 180 vteřin pro 98,5 % obdržených signálů. [7]

2.7 Pracovní postupy a požadavky na provoz

2.7.1 Audit

Dle Evropského výboru pojistitelů (Comité Européen Des Assurances, CEA) existují nejméně tři rozdílné důvody pro audit provozu DPPC/PCO:

- poruchový stav, rozbití, apod.;
- nedobrovolné chyba, nedbalost, atd.,
- počítačová kriminalita.

CEA ve svém doporučení z roku 2002 uvádí, že audit DPPC/PCO s příslušnou dokumentací by měl být realizován v periodách, jejichž délka by neměla přesáhnout 6 měsíců po dobu nejméně 3 let od data zahájení provozu. [10]

Dle normy ČSN EN 50518-3 by tento audit měl být v souladu s ČSN EN 45011 (015256) Všeobecné požadavky na orgány provozující systémy certifikace výrobků[19]. Tyto orgány dále stanoví všeobecné požadavky, které musí splňovat třetí strana provozující systém certifikace výrobků, má-li být uznána způsobilou a spolehlivou, a ČSN EN ISO/IEC 17020 (015260) Posuzování shody – Požadavky pro činnost různých typů orgánů provádějících inspekci, která obsahuje obecná kritéria pro odbornou způsobilost orgánů

[19] Platnost této normy byla ukončena ke dni 1. dubna 2013. Nahrazena byla ČSN EN ISO/IEC 17065 (015256) Posuzování shody – Požadavky na orgány certifikující produkty, procesy a služby.

provádějících inspekci a pro prokázání nestrannosti a důslednosti jejich inspekčních činností. Zdroj hlavního a záložního napájení zařízení, obvody a příslušenství, ochrana instalace aj. by měly být z hlediska správného provozu kontrolovány minimálně 1x týdně. Je nutné rovněž ověřovat (např. pomocí kontrolního seznamu), zda operátor provedl kontrolu vzdálených zařízení DPPC/PCO pro monitorování a příslušných technických listů týkajících se hardware a software zařízení, na která jsou napojena vzdálená monitorovací zařízení (EPS, CCTV atd.). Ověřuje se rovněž stav smluv o údržbě programového vybavení uvnitř monitorovacího centra a dostupnost zdrojového kódu. Do průběhu auditu musí být zařazena i kontrola činnosti hospodářských subjektů. Za správný průběh kontrolních postupů je odpovědný manažer. [10]

3 NORMY TÝKAJÍCÍ SE DPPC

Fungování DPPC/PCO se ode dne 1. ledna 2011 řídí českou technickou normou ČSN EN 50518. Tato norma byla připravena Evropským výborem pro normalizaci v elektrotechnice, z angl. European Committee for Electrotechnical Standardization (dále jen „CENELEC“). ČSN EN 50518 definuje umístění a konstrukční požadavky, požadavky na technické řešení a pracovně-provozní podmínky fungování DPPC/PCO. Centra tak musí v souladu s předmětnou normou například splňovat předepsanou sílu zdí, okna s balistickou a požární odolností, detekční zařízení plynu, dostatečné množství bezpečných datových úložišť, komunikačních tras a hardwaru jakož i automatizovanou zálohu napájecích okruhů pro případ velkoplošného výpadku elektrického proudu [2].

ČSN EN 50518 se skládá ze tří částí

- ČSN EN 50518-1 (334599) Dohledová a poplachová přijímací centra – Část 1: Umístění a konstrukční požadavky: Tato norma stanoví požadavky na umístění DPPC/PCO a na ohodnocení rizik. Dále jsou v normě uvedeny stavební požadavky na DPPC/PCO z hlediska odolnosti proti napadení a proti požáru.
- ČSN EN 50518-2 (334599) Dohledová a poplachová přijímací centra – Část 2: Technické požadavky: Tato norma stanoví technické požadavky týkající se DPPC. Dále zahrnuje funkční kritéria a ověřování výkonnosti.
- ČSN EN 50518-3 (334599) Dohledová a poplachová přijímací centra – Část 3: Pracovní postupy a požadavky na provoz: Tato norma stanoví požadavky na personál, pracovní postupy a provoz DPPC/PCO, požadavky na výcvik, bezpečnostní prověření a lustraci personálu, požadavky na testování center, správu databází a likvidaci údajů a požadavky na řízení nouzových stavů evakuačních postupů a audit DPPC/PCO.

Jako související normy je třeba jmenovat:

- ČSN EN 1154: 1998 (166232) Stavební kování – Zavírače dveří s řízeným průběhem zavírání – Požadavky a zkušební metody.
- ČSN EN 50131 (soubor) (334591) Poplachové systémy – Poplachové zabezpečovací a tísňové systémy.

- ČSN EN 50132 (soubor) (334592) Poplachové systémy – CCTV sledovací systémy pro použití v bezpečnostních aplikacích.
- ČSN EN 50133 (soubor) (334593) Poplachové systémy – Systémy kontroly přístupu pro použití při bezpečnostních aplikacích.
- ČSN EN 50134 (soubor) (334594) Poplachové systémy – Systémy přivolání pomoci.
- ČSN EN 50136 (soubor) (334596) Poplachové systémy – Poplachové přenosné systémy a zařízení.
- ČSN EN 61000-4-2 (333432) Elektromagnetická kompatibilita (EMC) – Část 4-2: Zkušební a měřicí technika – Elektrostatický výboj – Zkouška odolnosti

ČSN EN 50136-9

Norma pro komunikaci ústředen PZTS a EPS s DPPC, ČSN EN 50136-9 Protokol pro přenos zpráv z objektových zařízení na DPPC pomocí internetu. Norma je v platnosti od července 2013.

Tento protokol je nejmodernějším protokolem pro komunikaci po datových sítích. Vznikl z iniciativy Asociace pro požární ochranu v USA a Kanadě ve spolupráci s dalšími významnými institucemi SIA, FIPS, NIST. Převzalo jej více než 60 předních světových firem (např. Honeywell, ASIS, Bosch, Siemens atd.). Zavádí nové a velmi silné možnosti šifrování zpráv (AES 192 pro objekty zvláštní důležitosti). Uvnitř svého formátu může přenášet všechny známé komunikační formáty objektových zařízení. Rovněž obsahuje rozsáhlé možnosti verifikace událostí vzniklých ve střeženém objektu.

Přední světoví výrobci tento protokol již běžně používají ve svých zařízeních (např. Tecnoalarm, Texecom atd.).

Existence takové normy má zásadní vliv na průhlednost veřejných zakázek v bezpečnostním oboru. Vyřešení mnoha úloh z oblasti PZTS a EPS se stává nezávislé na hardware. Unikátní komunikace konkrétního spojení vznikne použitím soukromého šifrovacího klíče (16 nebo více náhodných znaků).

Norma je použitelná pro obory:

- Zabezpečovací a tísňové systémy / Poplachové přenosové systémy a zařízení / Systémy přivolání pomoci.
- Elektrická požární signalizace.
- Informační a komunikační technologie / Inteligentní budovy & integrované systémy.
- V současné době norma ANSI/SIA DC-09-2007 po obtížných 11 měsících prací nad ní je schvalovaná ÚNMZ.

Norma zásadně ovlivňuje veřejné zakázky. Po schválení normy stačí pouze jedno přijímací centrum pro všechny výrobce. Unikátnost komunikace se zajišťuje použitím šifrovacího klíče, který může být pro každý objekt jiný a je kdykoli vyměnitelný.

4 VÝVOJ DPPC

S přihlédnutím k okolnostem dalšího možného vývoje lze očekávat, že provozovatelé DPPC budou v rámci snižování provozních nákladů stále častěji tíhnout ke komplexním řešením. Dočkali jsme se vzniku celostátních DPPC/PCO (projekt KRUH), které se snaží provádět akvizice, a jejich podíl na trhu se bude zvyšovat. U klasických regionálních provozovatelů DPPC/PCO poptávka po výjezdových silách klesá. Mnohé zanikají, a proto hledají pomoc např. i u neziskových organizací.

Pro získání nových zákazníků se budou stále více využívat moderní marketingové nástroje, které známe z trhu se spotřebním zbožím (prodej zařízení na splátky, zapůjčení zařízení na dobu trvání smlouvy apod.). V úvahu připadají také doplňkové služby, o které zákazník bude mít zájem, a které bude možné obchodně realizovat (střežení vozidel, internet providing, časově omezené střežení objektu, řízení ovládání spotřebičů v objektech apod.).

V oblasti komunikací dochází ke stálému rozšiřování možností prostřednictvím rozvíjejícího se internetu. Tato síť nabízí obrovské možnosti přenosu dat, a proto je stále více využívaná i v PKB. Proto lze v přenosových cestách mezi střeženými objekty a DPPC/PCO očekávat patrný a stále vetší odklon od analogových linek na úkor radia, GPRS, internetu a dalších novějších technologii. Výrobci se budou snažit vylepšit technologie tak, aby správa přenosových tras byla pro provozovatele co nejjednodušší a počet výpadků co nejnižší (automatická konfigurace síti, redundantní provoz, automatické testování atd.). Nelze přesně odhadnout, kam se bude internet dále odvíjet, má však určitou nevýhodu, a to je možnost napadení virovými a jinými škodlivými aplikacemi. Ale díky novým technologiím se počítá se vznikem provozu bezpečného a cenově přijatelného systému.

Současný stav monitorovacích softwarů moderních DPPC/PCO je nadčasový a mnozí provozovatelé nevyužívají veškeré jeho možnosti ani z poloviny. Očekává se, že další vývoj bude stále více směřovat do oblasti internetu. 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 DPPC/PCO přizpůsobuje technologiím, které daná firma přímo vyvíjí a aplikuje do objektů. Výrobci DPPC/PCO většinou propagují vlastní software navržený 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. Proto se předpokládá, že monitorovací software bude umožňovat přístup koncových uživatelů služeb k záznamům o provozu na jejich zařízeních (sestavám událostí, logům apod.). Správu upgradu softwaru bude v rámci outsourcingu provádět specializovaná firma a provozovatele DPPC/PCO budou v budoucnu moci stále častěji přistupovat ke svým datům vzdáleně. [5]

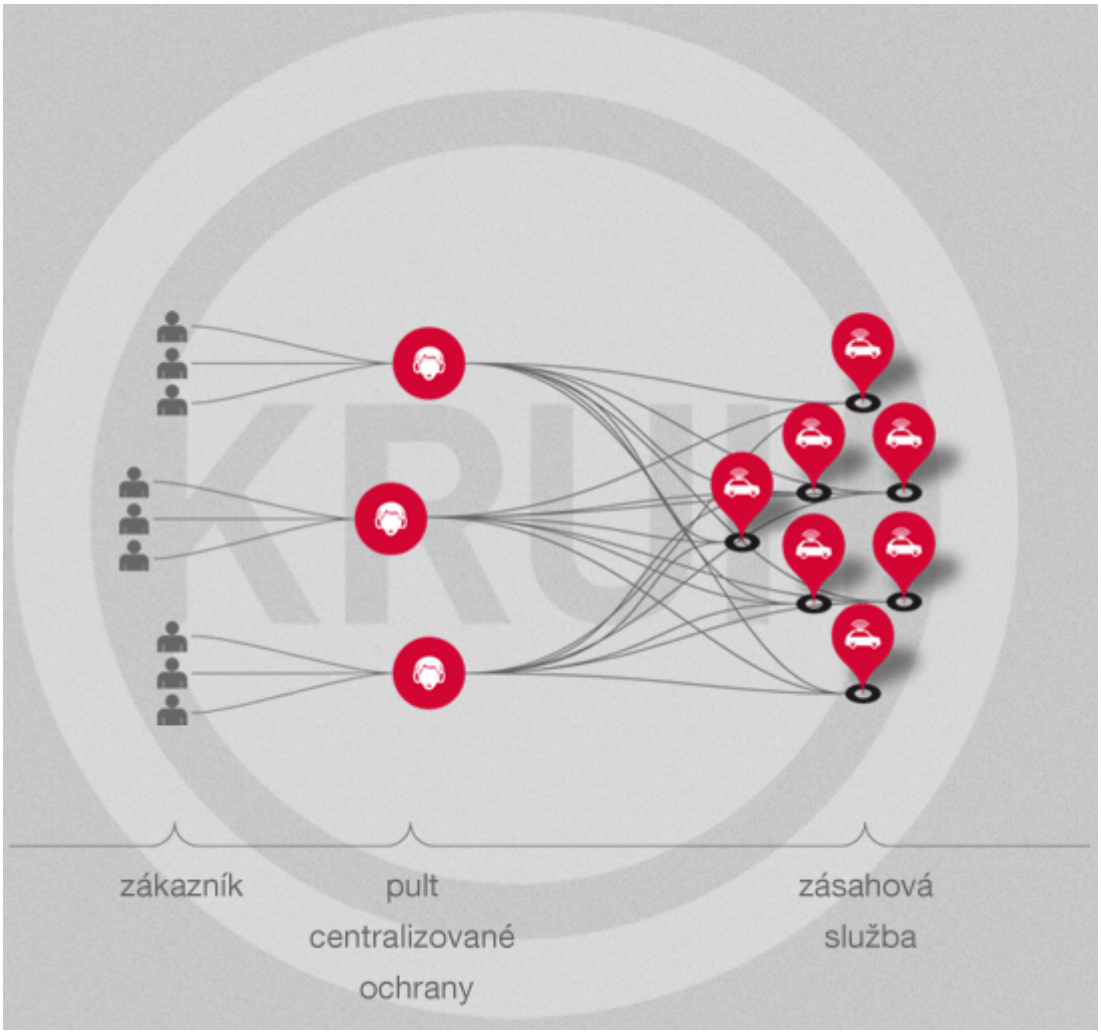
Lze očekávat, že dalším trendem vývoje DPPC/PCO bude vznik celonárodních DPPC/PCO.

4.1 Projekt KRUH

KRUH je platformou, která vytváří celorepublikovou síť provozovatelů zásahových služeb s jednotným standardem kvality. Provozovatelům DPPC/PCO zajišťuje služby zásahu kdekoliv na území České republiky.

Společnost Zásahová služba s.r.o. je součástí holdingu JABLOTRON a vznikla za účelem vytvoření jednotného celorepublikového systému poskytování služeb zásahu - projektu pod názvem "KRUH - zásahová služba". Zásahová služba s.r.o. nedisponuje vlastními prostředky zásahu (neprovozuje zásahová vozidla), ale využívá k zajištění služeb výhradně smluvní dodavatele zapojené do projektu v různých kategoriích partnerství.

Společnost Zásahová služba s.r.o. zajišťuje služby bezpečnostního zásahu pro více než 80 provozovatelů Pultů centralizované ochrany resp. pro bezmála 27 000 objektů jejich zákazníků po celé České republice. Společnost je výhradním smluvním dodavatelem služeb zásahu pro JABLOTRON SECURITY a.s.. V dubnu 2013 byla uzavřena smlouva o „generálním partnerství“ v projektu KRUH se společností SECURITAS ČR s.r.o., která se stala nejen odběratelem služeb v rámci projektu, ale zároveň i dodavatelem služeb zásahu v dohodnutých lokalitách. [14]



Obrázek 6 - Jak KRUH vznikl a jak funguje [14]

Klady:

1. možnost expanze po celé ČR
2. optimalizace nákladů a efektivní nakládání se zdroji
3. snížení nákladů spojené se servisem zásahových vozidel (údržba, pojistka)
4. větší jistota akvizice zákazníků

Zápory:

1. ztráta identity společnosti
2. vysoké vstupní náklady spojené se změnou vizuální identity firmy
3. ceny za výjezd snížené na minimum

Bezpečnostní agentury vstupují do projektu KRUH kvůli obavám z krachu v souvislosti s nedostatkem zakázek. Vysoké vstupní náklady a ztráta identity po začlenění do KRUH-u brání tomuto projektu v úspěšnosti. Jako opozice vznikají konkurenční projekty. V současné době na nich pracují neziskové organizace a soukromé firmy, které vytvářejí pulty DPPC/PCO. V těchto projektech se klade za cíl zachování identity a pomoc firmám.

II. PRAKTICKÁ ČÁST

5 ZPŮSOBY REALIZACE DPPC/PCO V ČESKU

V této kapitole se budu zaměřovat na popis způsobu realizace DPPC/PCO v České republice. Na příkladu největších dodavatelů DPPC/PCO na trhu ČR popíšu veškeré nabídky jaké mají na výběr běžné firmy, které začínají podnikaní v soukromých bezpečnostních službách. Aby mohly firmy začít provozovat DPPC/PCO, je nutné splnit základní legislativní podmínky.

Z hlediska legislativy je nutné splnit následující podmínky:

- **Zřízení koncesní listiny pro ochranu majetku a osob**, která zahrnuje poskytování služeb spojených s ostrahou a ochranou nemovitého a movitého majetku, ostrahou při přepravě peněz a jejich zpracování, cenností či jiného majetku, ochranou osob a právních zájmů, zajišťováním pořádku v místech konání veřejných shromáždění, slavností, sportovních podniků nebo lidových zábav podle pokynů objednatele, vyhodnocováním bezpečnostních rizik a provozováním centrálních pultů ochrany.
- **Zajištění prostor pro umístění dispečinku DPPC/PCO**, správně dle normy ČSN EN 50518-1.
- **Zřídit minimálně 2 až 3 státní telefonní linky** pro spojení přivedené na dispečink.
- **Zřídit připojení k internetu s pevnou IP adresou**. Z hlediska zajištění spolehlivosti funkčnosti internete se doporučuje připojení přes pevné linky ADSL nebo DSL se stálým připojením.
- Zabezpečit **zálohování napájení** pro případ výpadku síťového napájení 230V. Pro krátkodobé výpadky postačí **záložní zdroj UPS minimálně 900 VA**. Ten pokryje výpadek síťového napájení cca do 20 min. Při delších výpadcích je dobré instalovat **benzinový nebo dieselový agregát**, který vykryje výpadky napájení delší než 20 min. *Ideální je jeho umístění ve venkovních prostorách z důvodu odvodu zplodin.*

5.1 ZPŮSOBY REALIZACE DPPC/PCO OD FIRMY RADOM

5.1.1 Přenosové trasy od společnosti RADOM :

- **po pevných telefonních linkách** - tento přenos není bezpečný z hlediska kontroly spojení přenosové trasy (pouze 1x za 24 hod.)

- **v privátní rádiové síti 400 MHz** - stále nejbezpečnější přenosová trasa, častá kontrola spojení (např. 16 kontrolních zpráv během 5 minut).
- **po sítích operátorů GSM** - datové kódované SMS. Dnes používán převážně GPRS přenos. SMS používá jen jako záložní trasa (není zaručeno doručení SMS zprávy). U GPRS je možnost časté kontroly spojení např. každou minutu, obousměrný přenos - možnost dálkového ovládání.
- **po datových sítích LAN/WAN - Ethernet, Internet,** intranet - prakticky stejné jako u GPRS přenosu. Výhoda je v provozních nákladech. Stálý paušální poplatek za připojení k síti Internet.[16]

5.1.2 Software PCO RADOMNET II

Radomnet II je aplikační vybavení pro pulty centralizované ochrany. Integruje střežení statických objektů, EZS i EPS a mobilních objektů, vozidel a osobních jednotek. Je to modulární client-server pro střežení a správu objektů, jejichž stavy jsou přenášeny do multifunkčního operátorského pracoviště DPPC/PCO.

RADOMNET II poskytuje uživatelsky modifikovatelné prostředí pro vyhodnocování událostí zpracovávaných ze střežených objektů. Střeženými objekty mohou být:

- Statické objekty (banky, domy, chaty, atp.) vybavované objektovými zařízeními.
- Mobilní objekty (vozidla vybavovaná vozidlovou jednotkou z produkce RADOM, osoby, zvířata a předměty) vybavované jednotkou Personal Tracker HESTIE

V ethernetových sítích umožňuje vytvořit několik oddělených operátorských pracovišť, která mohou nezávisle na sobě řešit vzniklé události, a tak sledovat a spravovat velké množství střežených objektů.

Systém RADOMNET II lze provozovat variantně – jako samostatné pulty pro střežení jednotlivých typů objektů (statické a mobilní) nebo v kombinované variantě (statické a mobilní objekty společně).

RADOMNET II je kompatibilní se stávajícími podporovanými operačními systémy od společnosti Microsoft. Jednotlivé části systému jsou realizované jako služby MS Windows s možností dálkové správy. Toto umožňuje provozovat na serverech odděleně od operátorského pracoviště.

RADOMNET II lze použít pro různá nasazení lišící se požadavky na počet střežených objektů, typem, úrovní zabezpečení, počtem operátorů, apod.

Provozní režimy systému RADOMNET II:

- S jedním klientským pracovištěm (menší provoz, desítky až stovky střežených objektů).
- Variabilní počet klientských pracovišť (vysoký provoz, stovky až tisíce objektů).
- Specializované pracoviště s ohledem na vyšší stupeň bezpečnosti provozu (vysoký výkon, variabilní počet klientských pracovišť, provoz jednotlivých služeb systému RADOMNET na dedikovaných serverech – databázový, mapový, apod.). [16]

5.1.3 Základní funkce systému RADOMNET II:

- Příjem událostí a dat z objektu prostřednictvím:
  - privátních radiových sítí,
  - veřejných telefonních sítí,
  - GSM/SMS zpráv,
  - GSM/GPRS přenosu dat,
  - Ethernetových sítí (LAN/ WAN).
- Využití mapových podkladů dodaných zákazníkem.
- Propojení s kamerovými systémy.[16]

5.1.4 Další funkce systému RADOMNET II:

- Zobrazení a rozložení oken klienta na jednom nebo více monitorech.
- Zobrazení informací o událostech (události „k řešení“ – odbavení, podrobnosti vybrané události, „Aktivní archív“ – průběžné zobrazování všech událostí vznikajících na serveru) o objektu (stav objektu, vlastnosti objektu).
- Uživatelské definice vlastních typů událostí (např. překročení teploty, porucha chlazení, atp.).

- Zobrazování základních informací o objektech a času posledních příjmů událostí z objektu.
- Zobrazování přehledu všech sledovaných objektů.
- Řešení provozních situací (přebírání událostí operátorem, odbavování událostí, vkládání komentářů).
- Přístup k archivu událostí (vyhledávání dle parametrů, výběr událostí aktuálního objektu, výběr historie komentářů).
- Zobrazování objektu v mapě (statických objektů, vozidel, skupin vozidel), možné použití uživatelských mapových podkladů.
- Prohlížení a konfigurace provozních parametrů vozidel.
- Vyhledávaní objektů dle vybraných parametrů.
- Zobrazování plánů statických objektů včetně rozmístění čidel.
- Automatické párování některých typů událostí.
- Vytáčení telefonních čísel.
- Zobrazování kamer umístěných na statických objektech.
- Generování, export a tisk, konfigurovatelných tiskových sestav.
- Automatizované odesílaní tiskových sestav e-mailem.
- Odesílání SMS správ (automatizované, uživatelsky definované).
- Dočasné „vypnutí“ vybraných událostí (smyček, či celých objektů). [16]

5.1.5 Možnosti dalších rozšíření systému RADOMNET II:

- přenos událostí do Integračních nadstaveb (IN),
- možná integrace jiných datových rozhraní pomocí tzv. „Konektorů“,
- On-line/ Off-line záložní provoz,
- replikace databází (lokálně, případně mimo budovu centrály),
- přístup do systému prostřednictvím VPN. [16]

5.1.6 RADOMNET II v praxi

Základem dispečerského pracoviště DPPC/PCO je software PCO RADOMNET II postavený na architektuře server - klient.

Na serveru je nainstalován software RADOMNET server, který má za úkol zabezpečit příjem, zpracování, vyhodnocení a archivaci událostí přicházejících ze střežených objektů. Je zde také nahrána databáze SQL, ve které jsou uloženy data (informace) od jednotlivých objektů.

Pro příjem zpráv ze střežených objektů po různých přenosových trasách jsou na serveru nainstalovány speciální programy ("konektory"). Pro každý druh přenosové trasy je speciální konektor.

Pro práci operátorů je pak software RADOMNET klient. V tomto případe, mohou najednou pracovat až desítky klientských pracovišť. (tzn. DPPC/PCO s napojením několik desetitisíců objektů).

Běžně se používají dva klienti. Dle normy by měli být ve službě minimálně dva operátoři.

Pro začínající DPPC/PCO stačí jeden klient a může být nainstalován i na serveru.

Pomocí sítě internet lze použít i vzdálené klienty, které jsou mimo operátorské pracoviště.

Pro bezpečný provoz je dobré umístit server do jiné místnosti (servrovny - klimatizované) než je pracoviště operátorů. Operátoři tak pomocí softwaru RADOMNET klient sledují stavy připojených objektů a sledují příchozí události z objektu. Přicházející zprávy mohou být alarmové, upozorňující, informativní nebo běžné kontrolní telegramy.

Alarmová zpráva je zvýrazněna barevně (většinou červená) a je akusticky doprovázena zvukem. Operátor musí na tuto zprávu okamžitě reagovat a řídit se pokyny pro daný objekt. Ty jsou uloženy v informacích k danému objektu. Operátor musí na objekt vyslat zásahové vozidlo a alarmovou zprávu odbavit s přidaným komentářem. Upozorňující zprávy jsou např. typu: výpadek síťového napájení nebo ztráta komunikace s objektem apod. I na tyto zprávy musí operátor reagovat a držet se pokynů pro daný objekt a po vyřízení zprávu odbavit s patřičným komentářem.

Informativní zprávy jsou např. typu: objekt přešel z odstřeženého stavu ("den") do zastřeženého stavu ("noc"). Na tyto zprávy nemusí operátor nijak reagovat.

Pro bezpečný provoz DPPC/PCO je důležité zálohování. Nutná je záloha serveru, kde jsou uložena data od objektů. Používá se zrcadlení disků, tj. pro data.

Nejlepší je mít však celý záložní server, na kterém je také spuštěn program RADOMNET server. Zálohování pak může být on-line, zde je dobré používat placenou verzi databáze SQL. Data přicházející z objektu a zároveň se ukládají na oba servery. Tedy při výpadku hlavního serveru se přepne přijímací hardware na záložní server a může se hned pokračovat na záložním serveru prakticky bez ztráty dat.

Pokud by byla použita Free verze databáze SQL, lze zálohovat pouze Off-line, tedy data přichází na hlavní server a každé tři hodiny se uloží na záložní server. Pokud pak vypadne hlavní server, tak je nutné opět přepojit přijímací hardware DPPC/PCO na záložní server a může se pracovat, ale data nemusí být přímo aktuální, mohou být až 3 hodiny stará. [16]

5.1.7 Přijímací hardware PCO RADOMNET:

Pro příjem telefonních zpráv používá PCO RADOMNET telefonní karty GS 51 nebo TF98. Tyto karty jsou dvoulinkové (připojují se na dvě státní telefonní linky). Karty přijímají zprávy z objektů z ústředen PZTS. Ústředny PZTS vysílají v definovaných protokolech zprávy, která telefonní karta přijme a dekóduje pro zpracování softwarem RADOMNET server. V dnešní době se většinou požívá formát s tónovou volbou (rychlý) Contact ID (CID). Dříve se používaly pomalejší pulsní formáty Ademco slow 4.2, 4.3 (10 až 40 bps)

Pro několik stovek připojených objektů je možno použít další telefonní kartu, pokud jsou k dispozici další dvě volné pevné telefonní linky. Karty se umísťují do Boxu, ve kterém mohou být až 4 tel. karty.

U privátní rádiové sítě se pro příjem zpráv používá vysokofrekvenční přijímač s modemem SRX10/400, kde 400 značí kmitočtové pásmo 400 MHz. Příjem zpráv z vysílačů je realizován přes anténní systém do přijímače. Zprávy z objektových vysílačů jsou vysílány zakryptovaným protokolem "RADOM". Jakmile jsou zprávy přijaty na přijímači, modem je zpracuje a předá k vyhodnocení do softwaru RADOMNET server. Vysílače pracují v hvězdicové rádiové síti, tj. zprávy se zasílají přímo na přijímač, nebo prostřednictvím retranslační stanice, která se instaluje pro zvýšení dosahu. Retranslací může být použito několik a mohou se řetězit za sebou. Takto je možné vytvořit rozsáhlou

rádiovou síť, např. krajské sítě, které se používají pro Hasičské záchranné sbory ČR. Kmitočty, na kterých vysílače, retranslace a přijímače pracují, jsou v pásmu 400 MHz. Přiděluje je a schvaluje ČTÚ Praha. Pro oblasti blízko hranic je nutná koordinace a schvalování se sousedními zeměmi (Polsko, Německo, Rakousko, Slovensko).

U GSM sítí se pro příjem zakódovaných SMS zpráv používá přijímač SRX10G s modemem GSM, který SMS zprávy přijme, dekóduje a předává ke zpracování do softwaru RADOMNET server.

Pro příjem GPRS zpráv se používá APN (přístupový bod k síti) RADOM. To znamená, že je vybudované pevné spojení na operátora sítě GSM tzv. "tunel", který je zakryptovaný. Podobný tunel se pak buduje na provozovatele PCO. Rozdělení příchozích zpráv pro PCO je realizováno pomocí statické IP Adresy. Tedy z objektu se z ústředny EZS vyšle pomocí komunikátoru GPRS RADOM (SXS26, SXS24) zpráva, která se šíří přes centrum operátora GSM sítě (v tomto případě T-Mobile) tunelem na server a odtud dalším tunelem na patřičný PCO. Provozovatel má možnost vybudovat si přes operátora sítě GSM vlastní APN, a pak se mu doručují zprávy na PCO přímo tunelem od operátora GSM sítě. Zde je nutná investice do vybudování APN. RADOMNET tento tunel nabízí k využití za měsíční paušál.

U příjmu po síti Internet se opět používají zakryptované zprávy, které se kryptují pomocí routerů. Pro přenos zpráv z ústředen EZS se používají komunikátory INET nebo SXS26 a SXS24. [16]

5.1.8 Provozní náklady

Nejnižší provozní náklady jsou u přenosu po datových sítích (Internetu). Pokud je již připojení k síti Internet vybudováno a hradí se paušální poplatek, cena zůstává stejná, tedy za přenosy se neplatí.

Dále je v privátní rádiové síti zpoplatněn kmitočet ČTÚ ročním paušálním poplatkem, který je např. pro síť v okruhu do 10 km cca 7 000 Kč ročně. Nezáleží zde na počtu připojených objektů.

U přenosu po GPRS se účtují přenesená data z každého objektu (každé SIM karty). Vzhledem k velkému množství používaných SIM karet má společnost RADOM od operátora tarif, ve kterém je 5 MB přenesených dat za měsíc zdarma. Do tohoto množství se prakticky vejdou přenesená data z objektu při intervalu kontroly spojení každou minutu.

Zákazníkovi se tak účtuje poplatek od 99 Kč do 150 Kč podle počtu připojených objektů (SIM karet), přičemž je v ceně i poplatek za využívání APN serveru RADOM.

U přenosu GSM ve formě zakódovaných SMS zpráv se hradí každá SMS. Tarif společnosti RADOM má 50 SMS/měsíc zdarma. Další SMS se účtují částkou 0,50 Kč.

U pevných telefonních linek se účtuje každá přenesená zpráva. Tarify zde nejsou přesně určeny, protože jsou hrazeny koncovými uživateli přímo O2. [16]

5.1.9 Servis

Společnost RADOM nabízí servis s dojezdem do 12 nebo 24 hodin ve všech dnech. Zákazník platí za servisní pohotovost do 12 hod. paušální poplatek 1 500 Kč/měsíc a do 24 hod. platí 750 Kč/měsíc.

Servis se většinou provádí u zákazníka výměnným způsobem. Chybné díly jsou opravovány v servisech společnosti RADOM. [16]

5.1.10 Záruka

Společnost RADOM běžně poskytuje záruku 24 měsíců na veškeré komponenty. Výjimečně poskytují i vyšší záruku, např. na software 36 měsíců, nebo na server 36 měsíců. [16]

5.1.11 Shrnuti:

Pokud se zákazník rozhodne pro realizaci svého DPPC/PCO zvolit společnost RADOM, budou mu stanoveny níže uvedené orientační ceny: (Ceny se vždy počítají na konkrétní konfiguraci DPPC/PCO, je to stavebnice.)

a. Software PCO RADOMNET II server + 1 klient **83 000 Kč až 100 000 Kč**

b. Cena za kompletní server + operační SW + příslušenství **40 000 Kč až 50 000 Kč**

c. Telefonní karta s boxem na 2 státní linky **20 000 Kč až 25 000 Kč**

d. Rádiový přijímač SRX10/400 včetně modemu **28 000 Kč až 35 000 Kč**

e. GSM přijímač SRX10G (pro SMS) **7 000 Kč až 15 000 Kč**

f. Router CISCO pro zakryptování tunelu od PCO na APN RADOM **9 000 Kč**

Software PCO RADOMNET II server + 1 klient	83 000 až 100 000 Kč bez DPH
Kompletní server + operační SW + příslušenství (značkový DELL nebo HP)	40 000 až 50 000 Kč bez DPH
Telefonní karta s boxem na 2 státní linky	20 000 až 25 000 Kč bez DPH
Rádiový přijímač SRX10/400 včetně modemu	28 000 až 35 000 Kč bez DPH
GSM přijímač SRX10G (pro SMS)	7 000 až 15 000 Kč bez DPH
Router CISCO pro zakryptování tunelu od PCO na APN RADOM	9 000 Kč bez DPH

Tabulka 3 - Cenová nabídka od společnosti RADOM [16]

5.2 ZPŮSOBY REALIZACE DPPC/PCO OD FIRMY NAM system

5.2.1 PCO 1 Box

Technické řešení monitorovací technologie 1Box je postaveno na moderních softwarových a hardwarových technologiích (instalace ve virtuálních prostředích, oddělené instalace monitorovacího a diagnostického software, video verifikace, navigace zásahových vozidel na objekty, instalace na serverech, podpora 32 a 64 bitových operačních systémů WINDOWS).

Technologie DPPC/PCO jsou především založeny na základním požadavku, tj. že monitorovací technologie je provozována v non-stop režimu.

Při návrhu technického řešení 1Box byl kladen důraz na:

- minimalizaci výpadků technologie (dlouhodobou stabilitu chodu technologie) v non-stop režimu,

- režimu – výkonné serverové řešení,
- kvalitní zabezpečení,
- snadné ovládání,
- rychlý přechod na záložní systém – instalace ve virtuálních prostředích,
- podporu různých operačních systémů,
- vzdálený dohled technologie DPPC/PCO.

Při realizace DPPC/PCO společnost NAM zákazníkům zajišťuje:

- hardware a software, který takový provoz podporují,
- technologické služby,
- servis. [15]

5.2.1.1 1Box RACK – Hardware pro provoz PCO

Jako první společnost v České a Slovenské republice nabízí společnost NAM řešení hardware DPPC/PCO, který dodává formou služby 1Box RACK. Společnost NAM system poskytuje tak svým zákazníkům kompletně vybavený rack, který je vybaven vším potřebným pro provoz DPPC/PCO. V tomto racku je pouze ověřený hardware a software předních světových IT firem, který je nastaven právě pro toto použití. Zařízení je dodáváno za nulových vstupních nákladů, hrazen je pouze přívětivý měsíční poplatek za pronájem této technologie.

Obrázek 7 - I Box RACK [15]

1Box RACK obsahuje:

- 19“ rack,
- Server Supermicro (Intel XEON 3,1 GHz 4core, 8GB RAM, 2x HDD, 3x LAN),
- UPS APC,
- SWITCH CISCO,
- převodník MOXA LAN/2xCOM,
- Převodník SILEX LAN/2xUSB,
- Modem GSM pro odesílání SMS,
- Externí zálohovací NAS disk,
- Operační systém Windows 7 Pro 64 bit,
- Operační systém Linux Debian,
- Antivir ESET NOD,
- Virtualizační software VMware,
- Diagnostický software ZABBIX.

Zákazník musí ve svém DPPC/PCO pro instalaci technologie 1Box připravit:

- vhodný prostor pro rack (rozměry racku jsou š 670 x h 620 x v 700 mm),
- připojení do sítě LAN (s napojením na internet),
- zásuvku 230V (napojenou na zálohované napájení),
- SIM kartu do modemu pro příjem a odesílání SMS,
- PC klienta, který bude zapojen v interní LAN síti (1 Gbit/s).

Společnost NAM pak klientovi doručí sestavený a nainstalovaný 1Box. Dále zajišťuje jeho spuštění a zaškolení operátorů na obsluhu monitorovacího systému NET-G. [15]

5.2.1.2 DOHLEDOVÉ CENTRUM NAM

Hlavní předností tohoto řešení je monitorování systémem ZABBIX a připojení na **Dohledové centrum NAM**, které monitoruje a řeší veškeré kritické provozní stavy. ICT odborníci NAM system a.s. jsou připojeni k hardwaru DPPC/PCO 24 hodin denně. V případě poruchy se řeší problém dálkově nebo výměnou náhradního dílu. V současné době jsou servisní sklady v Havířově a Mladé Boleslavi.

Servis techniky od společnosti NAM systém:

- 1x ročně (při revizi) **kompletní profylaxi** technologie na DPPC/PCO (vyčištění, fyzickou kontrolu HW, kontrolu instalovaného SW),
- 1x za 3 roky **nový server**, původní zůstane jako záložní,
- 1x za 3 roky **výměna akumulátoru** v UPS,
- 1x za 3 roky **výměna větrací jednotky.** [15]

5.2.1.3 Software NET-G – software pro provoz PCO

Software NET−G pro monitorování byl vyvinut hlavně z narůstajících požadavků Policie České republiky a soukromých bezpečnostních služeb zpracovávat data z DPPC/PCO rychle a bezpečně, používat síťový provoz dispečinků, skloubit dohromady hlídání objektů v metropoli se střežením a monitorováním umístění zásahových jednotek nebo s monitorováním technologických stavů atd.

Software NET-G je postaven na Inter-base SQL databázi, která je poměrně bezpečná, o čemž svědčí i její používání ve zdravotnictví a armádě USA. Tato SQL 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 pomocí modemu, což umožňuje správci systému pracovat se softwarem při napojování objektů u zákazníka. Zároveň je společnost NAM schopná servisně podporovat tento systém. [17]

Díky tlaku konkurence byla společnost NAM system nucená provést u Software NET–G řadu změn. V současnosti je software silným konkurentem na trhu DPPC/PCO. Je stále modernizován a přizpůsobován potřebám zákazníků.

5.2.1.4 Možnosti software NET-G

Zpracování poplachů v akcích

Nový způsob zpracování poplachů, kdy první poplachová zpráva zakládá akci a další poplachové zprávy z objektu již nevyvolávají nutnost okamžitého potvrzení. Toto zpracování poplachů se vyznačuje až 30% úsporou času dispečera.

- významné snížení zátěže dispečera v provozní špičce,
- minimalizace chyb,
- vysoká přehlednost zobrazení.

Propojení akcí s navigací GARMIN

Zásahové vozidla mohou být vybaveny střežícími jednotkami ONI systému, které jsou propojeny s navigací GARMIN. Obsluha DPPC/PCO tak může odeslat do navigace informaci o napadeném objektu a jeho poloze. Výjezdová skupina ve vozidle tím získá přesnou lokalizaci objektu a je na něj naváděna.

- jednoznačný cíl zásahu do navigace,
- zpětná vazba o stavu zásahu pro dispečera,
- automatické podklady pro evidenci zásahu,
- vyhodnocení práce zásahové skupiny a dojezdových časů.

Napojení na Google mapy

Po zadání souřadnic hlídaných objektů do systému je možné získat přehledné zobrazení objektů v mapě.

Hlídání uzavření objektu

Software automaticky vyhodnocuje stav, kdy nedojde k uzavření objektu ve stanoveném čase. V takovém případě dochází ke vzniku akce a kontaktování zákazníka. A to s přesností na minuty a s možností zadání pracovních dnů a výjimek v kalendáři.

Videoverifikace poplachů

Operátor může kdykoliv zobrazit obraz IP bezpečnostních kamer přímo z formuláře objektu a získat tak náhled na dění v objektu v případě vzniku poplachu.

N**ahrávání hovorů do sw NET-G.**

Jedná se o aplikaci, která provozovatelům DPPC/PCO umožní jak nahrávání hovorů na dispečinku DPPC/PCO, tak zároveň plní funkci pobočkové telefonní ústředny monitorovacího dispečinku.

Jedinečnost aplikace 1Box PBX je v tom, že po jejím nainstalování se jedná o integrální součást DPPC/PCO 1Box. Na českém trhu se jedná o jediné řešení nahrávání hovorů propojené s DPPC/PCO. Nahrávky hovorů jsou aplikací automaticky přiřazovány k hlídaným objektům a akcím na objektech.

Další možnosti:

- Automatické nebo ruční odesílání SMS zpráv,
- Ovládání kamerových systémů – přepínání, natáčení po sériové lince,
- VoIP telefonie – vytočení telefonního čísla z formuláře objektů,
- Automatické zpracování e-mailových výpisů.

Komunikační trasy systému NET-G jsou:

- **Rádio** - rádiová síť Global a Global 2,
- **Rádio** - rádiová síť Elektronreg,
- **GSM (GPRS/SMS)** - síť NSG,
- **IP (LAN)** - síť NSG,
- **VTS** - telefonní karta TF 98,
- **VTS** - telefonní karta GS 51,
- **VTS** - telefonní karty SURGARD,
- **SMS** - SMS modul,
- **SurGard protokol** - otevřený standard komunikace (SVK-Gregor, ENIGMA, IPR512, SMET256, ...). [15]

5.2.1.5 Servisní podpora

Služby podpory provozu DPPC/PCO se vykonávají formou servisní smlouvy, která zajišťuje 24 hodinovou podporu vyškolených techniků a přístup k náhradním dílům umístěných v servisních skladech. Servisní smlouva obsahuje roční revizi na DPPC/PCO, kde je provedena kompletní diagnostika technologií NAM. [15]

5.2.1.6 Rádiová síť Global

Rádiovou síť Global tvoří soustava sběrných stanic (retranslací), které vytváří tzv. buňkovou strukturu (podobná jakou budují mobilní operátoři), jež pokryje jakoukoliv lokalitu. Sběrných stanic může být v síti Global 63.

Konfigurace rádiové sítě Global tvořená více retranslačními sběrnými stanicemi je vysoce odolná proti ztrátám spojení oproti konfiguraci rádiové sítě tvořené pouze přijímačem nebo přijímačem a jednou retranslací. Lze tady sběrné stanice libovolně

rádiově řetězit za sebou v maximálním počtu 6 stanic tj., lze využít 5 rádiových skoků. Celá rádiová síť pracuje na jedné frekvenci. [15]

Popis komunikace

Komunikace mezi sběrnými stanicemi je obousměrná a umožňuje dálkově konfigurovat páteřní síť sběrných stanic. Správně odladěná rádiová síť Global (vhodná rádiová konfigurace, minimální dostatečný výkon objektových vysílačů) umožňuje provozovat 800 vysílačů na jedné frekvenci. Sběrná stanice kontroluje spojení s definovanými objekty a předává na přijímací sběrnou stanici významové zprávy a informace o stavu sítě. Pokud se přejde na dvoufrekvenční síť Global 2, vzroste kapacita sítě na cca 3.000 vysílačů.

Komunikace mezi vysílači na hlídaných objektech a sběrnou stanicí je jednosměrná. Zabezpečení přenosu je řešeno systémem kontrolních telegramů, které jsou generovány přibližně ve 30 vteřinových intervalech. Objekty mají nastavenou dobu kontroly. Nejčastěji to bývá 5 minut. V této době musí sběrná stanice přijmout alespoň jeden kontrolní telegram z hlídaného objektu. V opačném případě vygeneruje sběrná stanice poplachovou zprávu „Ztráta spojení s objektem“. Po přijetí kontrolního telegramu sběrnou stanicí, vynuluje sběrná stanice časovač pro příslušný objekt. Stejný mechanismus kontroly funguje i v síti sběrných stanic. [15]

Přijímací sběrná stanice je hlídána monitorovacím sw NET-G, který hlídá v nastavené době kontroly 2 minuty příjem alespoň 1 datového paketu. V opačném případě vyhlásí sw NET-G „Ztrátu spojení se sběrnou stanicí“. Výhodou jednosměrného provozu je nízká cena objektového vysílače, velká kapacita sítě a odolnost vůči lokálnímu rušení. Obousměrný provoz umožňuje po páteřní síti efektivně přenášet větší datové toky, dálkově konfigurovat sběrné stanice či na dálku ovládat reléové výstupy sběrné stanice.

Pro zajištění spolehlivého přenosu zpráv z EZS/EPS na DPPC/PCO, vysílače každou přijatou zprávu vysílají celkem 15 krát. Protokol v sobě dále nese informaci, která se mění podle speciálního algoritmu. Tento algoritmus se ve sběrné stanici vyhodnocuje a slouží k odhalení případných ilegálních vysílačů v rádiové síti. Zpráva je z EZS/EPS na DPPC/PCO doručena do 2-3 vteřin. K rádiové síti Global je dodáváno speciální mobilní diagnostické zařízení (měřící stanice), pomocí které můžeme rychle a spolehlivě diagnostikovat různé parametry v rádiové síti např. úroveň spojení, úroveň rušení. Pomocí měřící stanice lze naleznout na objektu nejvhodnější místo pro vysílač. Ve spojení

s notebookem je možné dálkově provádět konfigurace v rádiové síti, zadávat převáděné objekty do sběrných stanic apod.

Přenos a zpracování zpráv v rádiové síti je plně digitální. Přenosy zpráv jsou kryptovány a doplněny o samoopravné mechanizmy.

K výhodám rádiové sítě Global patří:

- Rychlý přenos (4 800 b/s) velkého množství dat a to formáty Contact ID (s rozlišením na jednotlivé grupy), 4+2, 4+3, 4+4,
- Sběrné stanice mohou být zároveň i objektovými vysílači,
- Z 95% se provádí montáž interních antén,
- Nízký výkon vysílačů snižuje možnost rušení jiných objektů. [15]

5.2.1.7 Komunikační řešení NSG

Technologické centrum NAM (zkratka TC NAM) je řešením pro přenos zpráv ze zabezpečených objektů v sítích GSM (GPRS/SMS) a po Internetu na PCO.

TC NAM zprostředkovává spojení PCO se systémem pro střežení vozidel ONI systém a s Dohledovým centrem NAM. PCO se propojí s TC NAM pomocí komunikačního přijímače NSG receiver **dvěmi zabezpečenými komunikačními trasami (internet a GSM/3G/GPRS).** Poté je možné napojovat jakékoliv objekty. Veškeré komunikace jsou řešeny formou služeb, jejichž cena se odvíjí od doby kontroly spojení s objektem. Na výběr je doba kontroly 3, 5 nebo 15 minut.

GSM komunikátory obsahují v dodávce aktivovanou SIM kartu. Datové přenosy jsou zahrnuty v ceně služby. Do sítě NSG jsou dodávány ověřené komunikátory REGGAE a SAMBA.

V síti NSG jsou veškeré přenosové trasy zálohovány.

- **Komunikace mezi PCO a technologickým centrem probíhá primárně přes zabezpečené internetové připojení. Záložní trasou je 3G nebo GPRS kanál přes síť GSM.**
- **Komunikace mezi objektem a technologickým centrem je zálohována přes sítě dalších mobilních operátorů (služba multiSIM) nebo přes telefonní linku.**

Síť NSG je možné využít pomocí následujících služeb:

NSG Agentura

Tato služba řeší **napojení technologie 1Box na dohledové centrum NAM** a požadavky provozovatele PCO na **přenos zpráv pomocí GPRS a LAN** a **navigaci zásahových vozidel.** V rámci této služby je provozovateli instalováno **pronajaté** přijímací zařízení **NSG receiver.** Služba umožňuje zobrazování zpráv došlých z přidělených objektových zařízení v sw NET-G. Objektová zařízení (komunikátory REGGAE) musejí mít aktivovanou službu NSG Objekt.

Služba NSG Agentura obsahuje:

- Technologický dohled – napojení na dohledové centrum NAM,
- Pronájem přijímače NSG receiver,
- Neomezené datové přenosy,
- Podpora příjmu GPRS a IP komunikátorů REGGAE a SAMBA,
- Podpora navigace zásahových vozidel na hlídané objekty,
- 1Box connect.

NSG Objekt GSM

Tato služba umožňuje přenášet data z objektů vybavených komunikátory řady REGGAE (REGGAE GT, REGGAE mini GT, REGGAE GLT, REGGAE amos, REGGAE alarm a REGGAE eps DATA) přes technologické centrum na určený přijímač NSG receiver. Je nezbytnou podmínkou pro nasazení objektových komunikátorů řady REGGAE (tzn. bez této služby nelze přenášet data z těchto komunikátorů). Služba je vždy hrazena provozovatelem PCO.

Služby NSG Agentura a NSG Objekt GSM využívají APN zřízené společností NAM system. Vlastníkem SIM karet je NAM system, a.s.

MultiSIM

V případě výpadku GSM sítě umožňuje MultiSIM automatické přepínání mezi sítěmi mobilních operátorů v celé Evropské unii. MultiSIM řeší otázku záložních přenosových tras z hlídaného objektu a je možné připojovat na ni objekty v pohraničí nebo v zemích Evropské unie. Doplňkovou službou je Služba SMS. Služba SMS je záložní přenosovou trasou v případě výpadku hlavní přenosové trasy GPRS.

V ceně služby NSG Objekt GSM je 5 SMS zpráv zdarma. V ceně služby multiSIM jsou 2 SMS zprávy zdarma. [15]

5.2.1.8 Telefonní karta

Pro příjem zpráv na DPPC/PCO ze zabezpečovacích systémů prostřednictvím veřejné telefonní sítě (VTS) je určena telefonní karta TF 98P. Jedná se o prověřenou telefonní kartu, která je přizpůsobena na provoz v telefonních sítích v ČR a SR.

Umožňuje přijímat všechny známé formáty jak v pulsních, tak i v DTMF formátech. Karty jsou plně konfigurovatelné pro různé typy linek a obsahují diagnostiku provozu.

TF 98P je dodávána jako jednolinková TF98/P1 nebo dvojlinková TF98/P2. Karty se vkládají do BASIC boxu, kde je možné umístit až dvě karty po dvou linkách, celkem tedy 4 linky.

Zařízení je možné pořídit formou nákupu, nebo pronájmem. [15]

5.2.1.9 mojePCO

MojePCO je *webová aplikace pro majitele hlídaných objektů*. Webová aplikace mojePCO je Služba umožňující okamžitou kontrolu hlídaného objektu přes internet.

Je možné zkontrolovat, zda je objekt uzamčen, kdo objekt zakódoval, zda na objektu nedošlo k výpadku napájení, stav záložního akumulátoru, prohlédnout si kompletní historii objektu.

Obrázek 8 - aplikace mojePCO

Pomocí služby mojePCO je možné ovládat různé spotřebiče, například zapínat topení, otevírat vjezdovou bránu, spouštět žaluzie nebo zapínat zavlažování.

Služba moje PCO je určena pro provozovatele DPPC/PCO a majitele hlídaných objektů.

Služba je omezena dostupností připojením k síti internet. Službu je také možné ovládat pomocí mobilních zařízení, jako jsou tablety a chytré telefony. **Aplikace umožňuje ovládání výstupů komunikátorů REGGAE. (V ceně služby je podpora jak verze pro PC, tak i pro mobilní telefony a platí pro všechny objekty v databázi.)** [15]

5.2.2 Instalace technologie 1Box

Po instalaci společnost NAM nabízí zaškolení operátorů na obsluhu monitorovacího systému NET-G.

Součástí dodávky technologie 1Box je 5 licencí AppPCO sw NET-G (tj. 5 pracovišť – klientský software).

Instalace klientů probíhá na počítačích PC s nainstalovaným operačním systémem Windows, které jsou zapojeny v interní LAN síti (1 Gbit/s). Software NET-G je nainstalován jako řešení server/klient. Na serveru běží virtuální prostředí VMware s nainstalovaným operačním systémem Windows.

Do virtuálního prostředí VMware je nainstalována databáze Firebird a komunikační driver. Driver R460 – rádiová síť Global COM ,driver NSG – GPRS a IP komunikátory

REGGAE a SAMBA LAN, driver SMS – příjem a odesílání SMS COM a Driver TF98 – telefonní karta NAM TF98P. V dalším virtuálním prostředí VMware je na serveru nainstalován na Linux serveru diagnostický systém ZABBIX, který je napojen na Dohledové centrum NAM.

Základní konfigurace technologie 1Box obsahuje následující software:

- modul pro odesílání a příjem SMS (verze pro 1Box),
- modul pro odesílání e-mailů App MAIL (verze pro 1Box),
- modul EINO pro rychlou definici objektů (kopírování objektů),
- webovou aplikaci mojePCO.

Základní konfiguraci technologie 1Box je možné rozšířit o aplikaci vzdáleného přístupu k PCO.

Vzdálený přístup k PCO:

Vzdálený přístup umožňuje přístup k PCO odkudkoliv, kde je dostupné připojení k síti Internet. Přístup je nezávislý na operátorovi PCO.

Pokud existuje požadavek na vzdálený přístup k PCO pomocí sítě Internet, je možné ho provést dvěma způsoby.

- **Na fyzickém klientovi** – Klient AppPCO se nainstaluje na PC sestavu s nainstalovaným operačním systémem Windows a připojením k síti Internet s veřejnou IP adresou. Tento PC běží 24 hodin denně. Na Klient AppPCO je možnost připojovat se pomocí sítě internet na vzdálenou plochu.
- **Na virtuálním klientovi na serveru (virtuální pracoviště)** – šetří investici do nákupu PC sestavy a spotřebu elektrické energie PC. Nainstalované virtuální pracoviště AppPCO se dodá včetně nainstalovaného operačního systému. V místě instalace 1Boxu se připraví připojení k síti Internet s veřejnou IP adresou. K virtuálnímu klientovi se přistupuje rovněž jako na vzdálenou plochu PC.

Virtuálního klienta pro vzdálený přístup je možné vybrat ve verzi:

- **s 1 licencí** (jeden současný přístup),
- **s multilicencí** (vícenásobný současný přístup). [15]

5.2.3 CENOVÁ NABÍDKA

Cena služby 1Box je závislá na konkrétní konfiguraci technologie podle požadavku zákazníka.

V ceně pronájmu je zahrnuta:

- kompletní technologie 1Box,
- služba NSG Agentura,
  - podpora služby **1Box connect,**
  - podpora příjmu GPRS a IP objektů,
  - podpora navigace zásahových vozidel,
- pronájem sw NET-G,
- driver R460,
- driver TF 98,
- servisní podpora,
- kompletní instalace,
- dovoz,
- nasazení u zákazníka,
- technologický dohled – dohledové centrum NAM.

Po dobu pronájmu technologie 1Box klient obdrží:

- rozšíření sw NET-G – na 5 licencí AppPCO (5 pracovišť PCO),
- rozšíření sw NET-G – o aplikaci na příjem a odesílání SMS (verze pro 1Box),
- rozšíření sw NET-G – o modul AppMail (odesílání e-mailů – verze pro 1Box).

Mimo pronájmu technologie 1Box klient obdrží:

- software pro rychlou definici objektů (kopírování objektů) – Modul EINO,
- webovou aplikaci mojePCO.

Mimo pronájmu technologie 1Box je dodávka DPPC/PCO spojena s kompletními školeními, dodávkou hardwarového klíče a programovacích kabelů pro komunikátory REGGAE a vysílače TSM. K PCO.

V ceně servisní smlouvy má zákazník již zaplacenou 1x ročně fyzickou revizi PCO, roční „hot-line¨ podporu i aktualizace software. [15]

1Box® RACK	1 990 Kč bez DPH/měsíc
Software NET-G pro 100 objektů (5 klientů)	499 Kč bez DPH/měsíc
NSG Agentura	1 250 Kč bez DPH/měsíc
Instalace technologie - jednorázová investice	11 830 Kč bez DPH

Tabulka 4 - Cenová nabídka společnosti NAM system

5.2.3.1 KOMUNIKÁTORY REGGAE

Komunikátory REGGAE disponují integrovaným telefonním komunikátorem, který umožňuje připojení libovolné ústředny EZS (přenosový formát 4+2 i CID). Konfigurace je prováděna pomocí sítě internet nebo lokálně. [15]

Typ komunikátorů	Komunikace				Počet vstupů	Počet výstupů	Ceny bez DPH	
	GPRS	IP	SMS	Tel. linka			Za 1 ks	Projektové ceny
REGGAE mini GT	ano	ne	ano	ne	2	1	1790,- Kč (včetně antény)	1432,- Kč (včetně antény)
REGGAE GT	ano	ne	ano	ano	8	2	2090,- Kč	1672,- Kč
REGGAE GLT	ano	ano	ano	ano	8	2	3590,- Kč	2872,- Kč

Obrázek 9 - Komunikátory REGGAE [15]

5.2.4 Shrnuti

Pokud se zákazník rozhodne zvolit společnost NAM system pro realizaci svého DPPC, bude mu stanovena individuální cena podle jeho požadavků na služby. Každý zákazník od společnosti NAM system určitě získá hardware s pracovním názvem One box, který zahrnuje veškerá potřebná zařízení k provozu poplachového centra v jednom místě. Kromě toho může zákazník získat v základní nabídce software kompatibilní s operačním systémem od společnosti Microsoft, servisní podporu, která je dostupná 24 hod/den. Jako bonus pro své zákazníky nabízí společnost NAM system výhodnější ceny svých výrobků.

6 RIZIKA SPOJENÁ S VYUŽÍVÁNÍM SERVISNÍCH SLUŽEB

V servisních společnostech funguje nepřetržitě centrum péče o zákazníky. Dnešním trendem je speciální nabídka servisní firmy, která umožňuje přímou komunikaci operátora DPPC se servisním oddělením společnosti. Díky tomu může operátor kdykoli požádat servis např. o:

- vytvoření nových driverů,
- objednání zakázky na servis,
- upgrade systému (pokud vyšla nová verze),
- dohled nad prací techniků při dálkových servisech.

Normou se stává, že správce DPPC/PCO obdrží pomocí mailů nebo SMS informaci o ukončení servisních prací na DPPC/PCO. Vznikají aplikace, které umožňují rychlou reakci na vzniklou poruchu systému u operátora DPPC. Programy také hodnotí chování programu u operátora a při vzniku jakékoliv havárie (přeplnění disku, výpadek služby) programy poruchy signalizují.

Nevýhodou implementace tohoto typu řešení je, že servisní pracovnicí podpory softwarů mají přístup k počítačům a ke všem datům svých zákazníků (DPPC/PCO), kteří provozují zabezpečení objektů připojených na DPPC/PCO. Ohrožení spočívá v možnosti výskytu nepovoleného přístupu do systému DPPC/PCO, kde se mohou vyskytovat utajované informace o zabezpečených objektech. Proto by SW systémy měly poskytovat svým zákazníkům výběr úrovně zabezpečení přístupu servisních pracovníků podpory. Vzdálený přístup pomocí modulů se u některých starších softwarů DPPC/PCO provádí v „uzavřeném prostoru“. Data DPPC/PCO zákazníka jsou většinou zálohované v databázi. Díky tomu máji společnosti plný přístup k datům DPPC/PCO zákazníka. Některé firmy poskytující servisní podporu řeší problém pomocí toho, že vzdálený přístup lze v libovolné chvíli zablokovat a hlídání objektů lze provozovat bez nutnosti poskytování informací o objektech pro servisní oddělení.

Trendy:

- Rozšíření nabídky poskytovaných služeb společností prodávajících systémy DPPC. Trend je vynucen požadavkem klientů, kteří chtějí kromě nízkých cen získat i více služeb. Hlavním bodem v poptávkách po službách je bezpečnost zasílání dat a servis systémů (hardwarů i softwarů).

- Aby firmy poskytující DPPC/PCO mohly poskytovat servisní služby, musí zajistit velké množství servisních techniků. Zaměstnání každého dalšího technika zvyšuje náklady, proto firmy využívají služby externích techniků, které ve své společnosti certifikují na provádění servisu DPPC/PCO své značky u zákazníka. Takoví technici mohou provést servisní práce na DPPC/PCO většinou jen do určité míry. Hranice servisu určují výrobci DPPC/PCO a externí firmy. Při vážnějších poruchách mohou provádět servis pouze technici od společností, od kterých byl zakoupen DPPC/PCO. Z pohledu firem prodávajících DPPC/PCO je toto řešení levnější, ale vzniká při něm určité riziko. Externí firmy, které zajišťují provedení servisu na DPPC/PCO u klienta, mají přístup k hardwaru, se kterým mohou fyzicky manipulovat. Je důležité, aby firmy, které certifikují své servisní partnery pro provádění servisních prací, přijali do určité míry opatření, které by eliminovalo hrozby provádění jakýchkoliv manipulací s hardwarem a softwarem nad rámec domluvený ve smlouvě. Kompletní servisní práce bývají vykonávané pouze pomocí techniků od společnosti, od které byl systém zakoupen. Každá společnost má ale takových techniků pouze v omezeném počtu. Často se stává, že technici musí dojíždět k opravám, při kterých nemůže zasáhnout externí firma i několik set kilometrů.

- Vážnější poruchy DPPC/PCO nejsou externí technici ani technici prodejce schopni odstranit u zákazníka během 24 hodin. Při takovýchto typech poruch je nutno samotné zařízení převézt do servisních center daného prodejce DPPC/PCO. Při takovém typu servisu nabízí prodejce při prodeji DPPC/PCO záložní systémy, které po dobu servisu hlavního zařízení udrží základní funkce provozu DPPC/PCO. Díky službě tohoto typu má klient možnost pokračovat v provozu DPPC/PCO a servisní technici mohou odstranit poruchu systému.

- Novinkou je, že systémy DPPC/PCO obsahují svůj vlastní server, který pracuje pouze pro klienta a nemá nutnost posílání dat zákazníka do centrálního serveru. V současnosti bývá dostupnost k pultu pro provedení servisních prací a dohledu nad

správností práce DPPC/PCO pomocí sítě Internet. Pokud se ale provozovatel DPPC/PCO rozhodne provozovat systém bez dohledu servisního střediska, může přístup zakázat za cenu omezení poskytovaných servisně-dohledových prací. Nabízená služba závisí na vývoji trhu a nespolehlivém, napadnutelném internetu. V současné době provozovatel DPPC/PCO rozhodne o tom, jaká úroveň zabezpečení jeho dat je nejvhodnějším řešením.

- Trendem je také využívání webových aplikací pro správu, servis DPPC/PCO a komunikaci mezi DPPC/PCO a zabezpečeným objektem. Z důvodu snižování nákladů je snaha prodejců DPPC/PCO integrace zařízení, které dokážou zajišťovat více funkcí najednou. Pro takové zařízení vznikají webové aplikace, které dané zařízení dokážou řídit. Hardware, na kterém bude program provozován, musí být spolehlivý. Každá webová aplikace vyžaduje připojení k síti Internet, čímž vzniká riziko napadení systému. Stejně jako pro přístup servisních technologií na DPPC/PCO, i tady se využívá sítě Internet. Z důvodu hrozby napadení a vykradení dat o klientech provozovatele DPPC/PCO, je kladen požadavek na velice bezpečný systém využívající co nejkvalitnější šifrovací metody.

Jednoznačně jsem dospěl názoru, že menším rizikem vykradení informací o klientech a nespolehlivého chodu DPPC/PCO je volba interních servisních služeb. Servisní technici mají přístup do velmi citlivých dat, a proto je nutné vyhodnotit, koho si pro servis DPPC/PCO zvolit. Před zvolením správného dodavatele DPPC/PCO je nutné se ujistit, zdali umožňuje nabízený systém bezpečné posílání dat, a zdali systému umožňuje funkci omezení přístupu k datům.

7 MINIMÁLNÍ POŽADAVKY NA DPPC/PCO PRO JEHO SPOLEHLIVÝ CHOD

Body kontroly	Nároky		Hodnoceni	
			ANO	NE
Univerzální nároky	koncese na vykonávaní činnosti v oblasti Ostrahy majetku a osob zapsaná v obchodním rejstříku			
	alespoň jeden operátor je odborně vyškolen			
Nároky na zabezpečení prostor dispečinku	kombinace mechanického a elektronického zabezpečení pro kontrolu přístupu osob do prostoru, ve kterém se dispečink nachází			
	permanentní spojení dispečinku s IZS			
Technologické nároky dispečinku	**Napájení**	založené síťové napájení na 230 V pro spolehlivý chod dispečinku a komunikaci:		
		napájení z UPS (minimálně 10 min. provozu)		
		agregát pro dlouhodobé výpadky energie		
		minimálně jedna osoba zaškolená na obsluhu generátoru		
	Server	pojištění pro případ poruchy části systému a samotného serveru		
		zkonfigurovaný záložní hardware pro obnovení provozu DPPC/PCO *(v servisní smlouvy s dodavatelem)*		
		záložní databáze stará max. 24 hodin		
		software DPPC/PCO a veškeré konfigurační soubory *(servisní smlouvy s dodavatelem)*		
		zabezpečeni serveru		
		Firewall		
		Antivir		
		opatření proti fyzickému napadení systému nežádoucími osobami		
	Klientská část	klientské pracoviště dispečinku určené pro vyhodnocení signálů z objektů		

		záložní PC s softwarem klient DPPC		
		zabezpečeni klientské části		
		Firewall		
		Antivir		
		opatření proti fyzickému napadení systému nežádoucími osobami		
	Komuni-kace	přijímací zařízení určené pro příjem dat *(servisní smlouvy s dodavatelem)*		
		ochrana proti neoprávněné manipulaci		
		pro případ poruchy zařízení zajistit náhradní zařízení do 12 hodin od výpadku		
	Záloha dat	zálohování dat na DPPC minimálně jednou za 24 hodin na bezpečný zdroj		
		zálohy ze zdrojů 1x v měsíci odkládané mimo prostor DPPC na bezpečné místo		
Bezpečnostní plány	bezpečnostní plány na záchranu před možnými riziky:			
	přepadení třetí osobou			
	požár			
	povodeň			
	vodovodní havárie			
	porucha napájení			
	porucha DPPC/PCO *(servisní smlouvy s dodavatelem)*			
	plynová havárie (pokud se taková instalace v objektu nachází)			
Bezpečnostní politika	smlouva se všemi pracovníky obsluhy DPPC/PCO o zachovávání mlčenlivosti o DPPC/PCO a připojených objektech			
Nárok na zásahové jednotky	zajištění výjezdu na objekty (interní nebo externí zásahovou skupinou)			
	kvartální proškolení pracovníků výjezdu			
	kompletní dokumentace o objektu (datum a čas vzniku poplachu, datum a čas dostavení hlídky na objekt, doba kontroly objektu a její výsledek, datum a čas ukončení zásahu)			
	Vyhodnocení *(pokud se v tabulce vyskytne NE alespoň jednou, standard nebude splněn)*		ANO	NE

Tabulka 5 - Minimální požadavky na DPPC/PCO pro jeho spolehlivý chod

ZÁVĚR

První DPPC/PCO vznikly v roce 1853 v New Yorku. V Československu bylo první použití zabezpečovací techniky zaznamenáno v roce 1933. Od roku 1939 byl provoz bezpečnostních systémů pouze v kompetenci Ministerstva vnitra. Hlavním komerčním dodavatelem bezpečnostních systémů byla společnost TESLA. V 70. letech se již začínají prodávat i zahraniční výrobky, což vedlo k obohacení českého trhu. Roku 1990 začal narůstat vliv komerčního sektoru, ke kterému také patřil průmysl komerční bezpečnosti. Takto začal intenzivní rozvoj DPPC/PCO na trhu.

Pro přenos poplachových signálů na DPPC/PCO je využívána telefonní linka, rádiový přenos, nebo GSM/GPRS systém. Stále populárnějším způsobem přenosu dat je přenos po rádiových sítích, který ale bývá v současnosti nahrazován sítí Internet. Aby kvalita nabízených služeb v celém prostředí PKB neklesla pod určitou úroveň, jsou stanoveny normy, jako např.: ČSN EN 50131, ČSN EN 50518 1-3 a od roku 2013 norma ČSN EN 50136-9.

Z důvodu vysoké konkurence v prostředí průmyslu komerční bezpečnosti, je současným trendem poskytovat co nejvíce služeb za co nejnižší ceny. Bezpečnostní agentury proto snižují ceny za poskytnutí ochrany objektu na minimum. Toto vede ke zvýšení tlaku na dodavatele technických služeb pro bezpečnostní agentury, které musí také snižovat ceny za poskytnutý hardware. V současné době je trendem licenční pronájem zařízení DPPC/PCO. Tlak vedený na snížení ceny, ale bohužel vede ke snížení kvality poskytovaných služeb. Bezpečnostní agentury proto na střežení objektů zaměstnávají hlídače se zdravotním hendikepem, nebo seniory. Dodavatelé hardwaru pro bezpečnostní agentury nakupují komponenty z Číny, z důvodu snížení vlastních nákladů. Do popředí se dostávají webové aplikace instalované v chytrých zařízeních, které nahrazují drahý hardware pro zabezpečení objektu a řízení DPPC/PCO. Značnou nevýhodou tohoto typu řešení je však jeho závislost na síti Internet. Vznikají velké bezpečnostní agentury, jejichž cílem je konsolidace menších firem.

Po teoretické části navazovala část praktická, ve které jsem se snažil zjistit úroveň služeb poskytovaných bezpečnostními agenturami pomocí srovnání nabídek největších dodavatelů DPPC/PCO v České republice. Pro vyhodnocování poskytovaných servisních služeb na trhu PKB v ČR a vyhodnocování rizik spojených s využíváním jejich služeb, jsem stanovil dokument, ve kterém jsou určené minimální požadavky na DPPC. Tyto

požadavky musí bezpečnostní agentury splnit, aby zajistily spolehlivý chod svého DPPC. Zjištěná kritéria jsou určena s ohledem na současnou situaci na trhu DPPC. S pomocí tohoto dokumentu může bezpečnostní agentura snížit riziko výskytu poruch chodu celého pultu, čímž si zaručí, že bude působit na své zákazníky jako důvěrná firma vhodná ke spolupráci.

K tomuto závěru jsem dospěl po důkladné analýze trhu PKB. Díky spolupráci se zástupci společností provozujícími systém DPPC/PCO, jsem se obohatil o informace v oblasti vývoje systému DPPC/PCO. Za velice užitečné považuji konzultace s bezpečnostními komorami a bezpečnostními agenturami, díky kterým jsem získal důvěryhodné informace o stavu PKB v České republice. Veškeré získané informace byly velice prospěšné a užitečné při tvorbě mé diplomové práce.

ZÁVĚR V ANGLIČTINĚ

First ARC were formed in 1853, in New York. The first use of security technology was registered in 1933 In Czechoslovakia. Since 1939, the operation of security systems was only in competence of the Ministry of Interior. The main commercial supplier of security systems ,was the TESLA company. However in the 70s, began to sell even foreign products, what caused the enrichment of the Czech market. Since 1990, despite an increase of commercial sector, part of which was also the commercial security industry, it began an intensive development of ARC in the market of Commercial security industry .

To transmit alarm signals to the ARC, we use a phone line or GSM / GPRS system . Still popular way to transfer data and transmission is transfer over radio networks, which is starting to replace less expensive internet. In terms of ARC equipment, system is on the highest technical level in terms of hardware and software yet. In order to quality of services offered throughout the Commercial security industry environment does not drop below a certain level, what cause high competition in the market, are established standards, such as: ČSN EN 50131, ČSN EN 50518 1-3, and from 2013 standard EN 50136-9 . The Commercial security industry is obviously missing the Law about the security services, which would establish a unique business conditions in Commercial security industry.

Due to the highly competitive environment in the commercial security industry, there is a trend of providing the most services at the lowest prices. Therefore Security agencies reduce the prices for protection of objects to a minimum. Supplier of technical services for security agencies must adapt to the trend that cause hardware sales for minimal rates. Currently, the trend is a license lease of ARC equipment. On one side are the services at the lowest prices, but unfortunately, at the cost of quality. Security agencies thus employed for guarding objects guard with disabilities and make business on the border of the Act to avoid losing market position. Security agencies hardware vendors buy components from China to reduce production costs. The trend is becoming a web application installed in smart devices that replace expensive hardware to secure the building, driven by ARC. The minus of this type of solution is its dependence on an unsafety Internet. In addition arise major security agencies that consolidate smaller companies that are not resistant to fight with constantly falling prices for services.

The theoretical part was followed by the practical part, in which using comparison of offers of largest ARC suppliers in the Czech Republic, I tried to determine trends of

services for security agency. When evaluating the services provided for the Commercial security industry market in the Czech Republic and risk assessment with the use of their services, I determined chapter, which specify the minimum requirements for ARC, which security agencies need to fulfill to ensure reliable operation of ARC with regard to the current situation on the ARC market. With this guidance a security agency reduces the risk of occurrence of a fault running of the whole counter, so the company will operate as confidential and attractive to their customers.

The conclusion I have reached after a long and thorough analysis of the Commercial security industry market. Thanks to cooperation with representatives of ARC system companies, I was enriched with information about the developments of DPPC. I consider it a very useful that I could consult my diploma work with the security chambers, through which I received a sufficient information about the state of ARC in the Czech Republic. All information obtained was for me very beneficial and helpful in creating my thesis.

SEZNAM POUŽITÉ LITERATURY

[1] Uhlář, J.: Technická ochrana objektů , II. díl – Elektrické zabezpečovací systémy, PA ČR, Praha 20001, ISBN 80-7251-076-2

[2] LUKÁŠ, L. et al. *Bezpečnostní technologie, systémy a management I*. 1. vyd. Zlín: VeRBuM, 2011. ISBN 78-80-87500-05-7.

[3] *Naše téma: Monitorování objektů.* Magazín SECURITY, květen/červen 2003, roč. X, č. 3/2003, s. 7-27. ISSN 1210-8723

[4] VYORÁLEK, Radim. *Pulty centralizované ochrany.* Univerzita Tomáše Bati ve Zlíně, 2005. UTB Zlín. Bakalářská práce.

[5] ZAPLETAL, Pavel. *Perspektiva PCO.* Univerzita Tomáše Bati ve Zlíně, 2009. UTB Zlín. Diplomová práce.

[6] ČSN EN 50518-1. Dohledová a poplachova přijímací centra – Část 1: Umístění a konstrukční požadavky. Praha: Česky normalizační institut, 2010.

[7] ČSN EN 50518-2. Dohledová a poplachova přijímací centra – Část 2: Technické požadavky. Praha: Česky normalizační institut, 2011.

[8] ČSN EN 50518-3. Dohledová a poplachova přijímací centra – Část 3: Pracovní postupy a požadavky na provoz. Praha: Česky normalizační institut, 2012.

[9] JUDr. LAUCKÝ, Vladimír.: Technologie komerční bezpečnosti I. a II. díl, Univerzita Tomáše Bati ve Zlíně, ISBN 80- 7318-231-9

[10] Recommendations For Remote Monitoring Centres. 2002.

[11] Alarm Receiving Centres: A *Central Function in the European Security Landscape*. 2009.

[12] Příloha č. 3 živnostenského zákona

[13] ČSN EN 50136-9. Protokol pro přenos zpráv z objektových zařízení na DPPC pomocí internetu. Praha: Česky normalizační institut, 2013.

[14] Co je projekt „KRUH – zásahová služba“. [online]. [cit. 2013-09-21]. Dostupné z: http://www.zasahovasluzba.cz/cs/

[15] Firemní materiály čs. výrobce NAM a.s. Havířov

[16] Firemní materiály čs. výrobce RADOM s.r.o. Pardubice

[17] NAM systém, a.s., Orlová. Monitorovací software NET-G: Manuál správce. 1.22. vyd. Orlová, 2012.

[18] BOGDAŃSKI, Wojciech. Koncepce systému Kronos a porovnání s jinými systémy poplachových přijímacích center. Univerzita Tomáše Bati ve Zlíně, 2012. UTB Zlín. Diplomová práce

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ARC	Alarm Receiving Centre (Dohledové poplachové přijímací centrum)
BRI	Basic Rate Interface (Základní přípojka)
CCTV	Closed Circuit Television (Uzavřený televizní okruh)
ČR	Česká Republika
DNS	Domain Name Systém (Hierarchický systém doménových jmen)
DPPC	Dohledové Poplachové Přijímací Centrum
EPS	Elektrická Požární Signalizace
GPS	Global Positioning System (Globální polohovací systém)
GPRS	General Packet Radio Service (Obecná paketový rádiový systém)
GSM	Global System for Mobile Communication (Globální systém pro mobilní komunikaci)
HW	Hardware
IP	Internet Protocol (Protokol Internetu)
IZTS	Integrated Services Digital Network (Digitální síť integrovaných služeb)
IZS	Integrovaný Záchranný Systém
MDC	Multimediální Dohledové Centrum
PCO	Pult Centralizované Ochrany
PKB	Průmysl Komerční Bezpečnosti
PPC	Poplachové Přijímací Centrum
PZTS/I&HAS	Poplachový Zabezpečovací a Tísňový Systém (Intruder and Hold up Alarm Systém)
RFID	Radio-Frequency Identification (Identifikace na rádiové frekvenci).
SBS	Soukromá Bezpečnostní Služba.
SW	

TCP	Software.
UPD	Transmission Control Protocol (TCP protokol).
UTC	User Datagram Protocol (UPD protokol).
	Coordinated Universal Time (Koordinovaný světový čas).

SEZNAM OBRÁZKŮ

SEZNAM TABULEK