Optimalizace činnosti dohledového a poplachového přijímacího centra

The Optimalization of The Activites of a Monitoring and Alarm Reception Centre

Bc. Simona Benedělová

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. Simona Benedělová**
Osobní číslo:	**A12356**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Optimalizace činnosti dohledového a poplachového přijímacího centra**
Téma anglicky:	**The Optimalization of the Activities of a Monitoring and Alarm Reception Centre**

Zásady pro vypracování:

1. **Popište strukturu dohledového a poplachového přijímacího centra hardware, software.**
2. **Zhodnoťte bezpečnost a uchování dat na dohledovém a poplachovém přijímacím centru.**
3. **Proveďte analýzu výrobců dohledových a poplachových center na českém trhu.**
4. **Vyberte jednoho dodavatele a proveďte popis jeho technologie.**
5. **Optimalizujte činnost dohledového a poplachového centra z hlediska dispečera.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **LAUCKÝ, Vladimír. Technologie komerční bezpečnosti I. Zlín: Univerzita Tomáše Bati ve Zlíně, 2004. ISBN 80-7318-231-9.**
2. **JAŠEK, Ph.D., Doc. Mgr. Roman a Ing. David MALANÍK, Ph.D. Bezpečnost informačních systémů [online]. Zlín, 2013 [cit. 2014-01-18]. ISBN 978-80-7454-312-8. Dostupné z: http://dspace.k.utb.cz/handle/10563/25821. Elektronická skripta. Fakulta aplikované informatiky.**
3. **LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management I. 1. vyd. Zlín: VeRBuM, 2011. 316 s. ISBN 978-80-87500-05-7.**
4. **HARPER, Allen, Chris EAGLE, Jonathan NESS a Michael LESTER. Hacking: manuál hackera. 1. vyd. Praha: Grada, 2008, 399 s. Profesionál. ISBN 978-80-247-1346-5.**
5. **JAQUISH, Michael James. The role of the security officer: a compendium of instruction of safety and security for the security profession in America. 2nd ed. Gig Harbor, Wash.: Butterworth-Heinemann, 2010, xxvi, 596 p. ISBN 978-146-6438-446.**
6. **The Professional Protection Officer: Practical Security Strategies and Emerging Trends. Oxford: Butterworth-Heinemann, 2010, xxvi, 596 p. ISBN 18-561-7746-7.**

Vedoucí diplomové práce: **JUDr. Vladislav Štefka**
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 objasnit strukturu dohledového a poplachového přijímacího centra z hlediska hardwaru a softwaru a optimalizovat činnost tohoto centra z pohledu dispečera. Cílem je též zhodnotit bezpečnost a uchovávání dat a navrhnout řešení jejich zabezpečení v dohledovém a poplachovém přijímacím centru.

Klíčová slova:

Dohledové a poplachové přijímací centrum, bezpečnost, ochrana objektu, průmysl komerční bezpečnosti, monitorovací software, poplachový zabezpečovací a tísňový systém, dispečer.

ABSTRACT

The aim of thesis is to clarify the structure of the monitoring and alarm reception centre, both in the view of hardware, software, and to optimize the monitoring activity of monitoring and alarm receiving centre from the perspective of a dispatcher. Further to evaluate the safety and storage of data on this center. To resolve security data used for the monitoring and alarm receiving centre.

Keywords:

Monitoring and alarm reception centre, security, building protection, commercial security industry, monitoring software, intrusion and hold-up system, dispatcher.

Ráda bych poděkovala všem, kteří mi pomohli při zpracování mé diplomové práce. Především děkuji JUDr. Vladislavu Štefkovi za odborné vedení, konzultace a za poskytnuté cenné rady ke zpracování a obsahu práce. Dále pak děkuji svým rodičům a blízkým za jejich podporu po celou dobu mého studia.

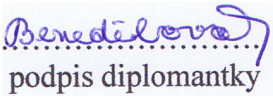
Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové 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 práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byla jsem seznámena s tím, že na moji diplomovou 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 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 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 práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové 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 pracovala samostatně a použitou literaturu jsem citovala. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně 23.5.2014



OBSAH

ÚVOD

Doba jedenadvacátého století nutí člověka stále více zohledňovat faktor bezpečnosti a ochrany nejen života a zdraví, ale také majetku. Díky nasycenému trhu v oblasti zabezpečovací techniky si může každý dle svých představ vybrat zabezpečení šité na míru. V nedávné době prošly zabezpečovací prvky prudkým vývojem a doznaly pokroku v kompatibilitě a propojení s jinými zabezpečovacími prvky. Objevuje se tedy možnost propojovat poplachové zabezpečovací a tísňové systémy s prvky elektrické požární signalizace nebo systémy kontroly vstupu s prvky kamerových systémů. A v případě potřeby nejvyšší kvality je možné využít též integrace třetího stupně a propojit poplachový zabezpečovací a tísňový systém se systémem kamerovým, systémem elektrické požární signalizace, IT technologiemi atd. Existuje široká škála možností, jak vhodně zabezpečovací techniku zkombinovat. Trh v této oblasti je velmi štědrý a není problém najít společnosti, které se touto problematikou zabývají.

Dále je pak nutné zvážit otázku, zda bude využito i dohledové a poplachové přijímací centrum (dále jen „DPPC“), které umožní díky nepřetržitému provozu střežit majetek klienta 24 hodin denně. Poplachový systém může upozornit na případné nebezpečí zasláním SMS zprávy na mobilní telefon klienta. V případě, že klient bude v tuto dobu mimo domov, nebude v dojezdové vzdálenosti, nebo bude jeho firma od bydliště příliš vzdálená, může být už po příjezdu na místo pozdě. Využití dohledového a poplachového centra tak může být podle názoru autorky v těchto i jiných situacích velmi výhodné.

Podle zkušeností autorky získaných během praxe na jednom z takových DPPC přináší napojení objektu na DPPC jen samá pozitiva, a to především s ohledem na výše zmiňovaný problém s dojezdem k vyhlášenému poplachu. Tato centra poskytují i nadstandardní služby, jako je např. zasílání SMS při zapnutí, nebo vypnutí střeženého objektu, či hlídání času, dokdy má být objekt zakódován. Pokud se klient rozhodne využít služeb firmy zabývající se ochranou majetku a osob, která vlastní takové DPPC, musí být velmi obezřetný. V České republice působí velké množství takových firem a úroveň jejich kvality se značně liší. DPPC dříve vznikaly nekontrolovaně a jejich provoz nebyl žádnou právní normou ani jiným způsobem upraven, či regulován. Proto je nutné při napojení objektu na takové DPPC vznést mnoho dotazů, jakým způsobem bude objekt chráněn, za jak dlouho bude hlídka schopna dorazit od vyvolání poplachu k hlídanému objektu a jak je vyzbrojena, kolik dispečerů obsluhuje takové DPPC, jakou formu přenosu dat je tato firma

schopna zajistit atd. Autorka též může z vlastní zkušenosti potvrdit, že napojení na DPPC již v této době není natolik finančně náročné, jak tomu mohlo být dříve, a to především díky rozvinutému trhu a množství společností, které se touto činností zabývají.

I. TEORETICKÁ ČÁST

1 DOHLEDOVÁ A POPLACHOVÁ PŘIJÍMACÍ CENTRA

Potřeba ochrany zdraví i života osob stejně jako snaha minimalizovat škody způsobené majetkovou kriminalitou vedou stále více k nutnosti ochrany a k zabezpečení objektů, a to nejen fyzickým zabezpečením, ale také technickými a mechanickými prostředky ochrany. Díky těmto prostředkům je sice objekt lépe chráněn, je to ale stále nedokonalá ochrana. Pokud napadení nebude nikde zaznamenáno, či se informace o vniknutí do objektu nedostane do povolaných rukou, je takové zabezpečení bezvýznamné. Proto zde hraje velmi důležitou roli dohledové a poplachové přijímací centrum.

DPPC se skládá ze tří základních částí:

- *Dispečerské pracoviště*, pomocí kterého je zajištěn centrální dohled nad střeženými objekty a probíhá zde vyhodnocování jejich stavů. Obsahuje zařízení pro příjem zpráv ze střežených objektů a počítačovou sestavu s uživatelským softwarem (slouží k zobrazení, vyhodnocování a archivaci zpráv ze střežených objektů) [33].
- *Přenosové trasy*, díky kterým se k DPPC dostane informace o tom, co se děje ve střeženém objektu, jinými slovy tedy slouží k přenosu dat mezi DPPC a střeženým objektem [33].
- *Objektová přenosová zařízení,* která plní úlohu sběru informací z poplachového zabezpečovacího a tísňového systému (dále jen PZTS), elektrické požární signalizace (dále jen EPS) a jiných bezpečnostních zařízení s následným přenosem na dispečerské pracoviště DPPC [33].

Každá z těchto tří částí plní v DPPC svoji úlohu, při poruše kterékoliv z těchto komponent není DPPC schopno plnit funkci, pro kterou je určeno [33].

1.1 Mechanické zábranné systémy

Mezi nejznámější mechanické zábranné systémy v průmyslu komerční bezpečnosti (dále jen PKB) patří např. klasické drátěné oplocení, vrcholové zábrany, podhrabové překážky, bezpečnostní oplocení, vstupy, vjezdy, otvorové výplně, stavební prvky budov, komerční úschovné objekty, komorové trezory aj.

1.2 Technické prostředky ochrany

Hlavním cílem těchto prostředků je podpořit realizaci režimových opatření, zkvalitnit činnost fyzické ostrahy a odradit narušitele od jeho činu, popřípadě významně ztížit jeho činnost a prodloužit dobu, která ho dělí od jeho přístupu k chráněným aktivům [1].

1.2.1 Poplachové zabezpečovací a tísňové systémy

PZTS je kombinovaný systém určený k detekci poplachu vniknutí a tísňového poplachu. Do této kategorie ochranných prostředků se řadí prvky, jako jsou např. infračervené závory a bariéry, mikrovlnné bariéry, štěrbinové kabely, magnetické kontakty, vibrační snímače, poplachové fólie a skla, akustické detektory, infrazvukové detektory, snímače pro ochranu skleněných ploch, pasivní infračervené detektory (PIR), aktivní infračervené detektory (AIR), aktivní ultrazvukové detektory (US), aktivní mikrovlnné detektory (MW), tlakové detektory, kontaktní detektory, tahové detektory, kapacitní detektory aj. Tyto prvky ochrany zaznamenávají nestandardní situace ve střeženém objektu a informují o tom DPPC [34].

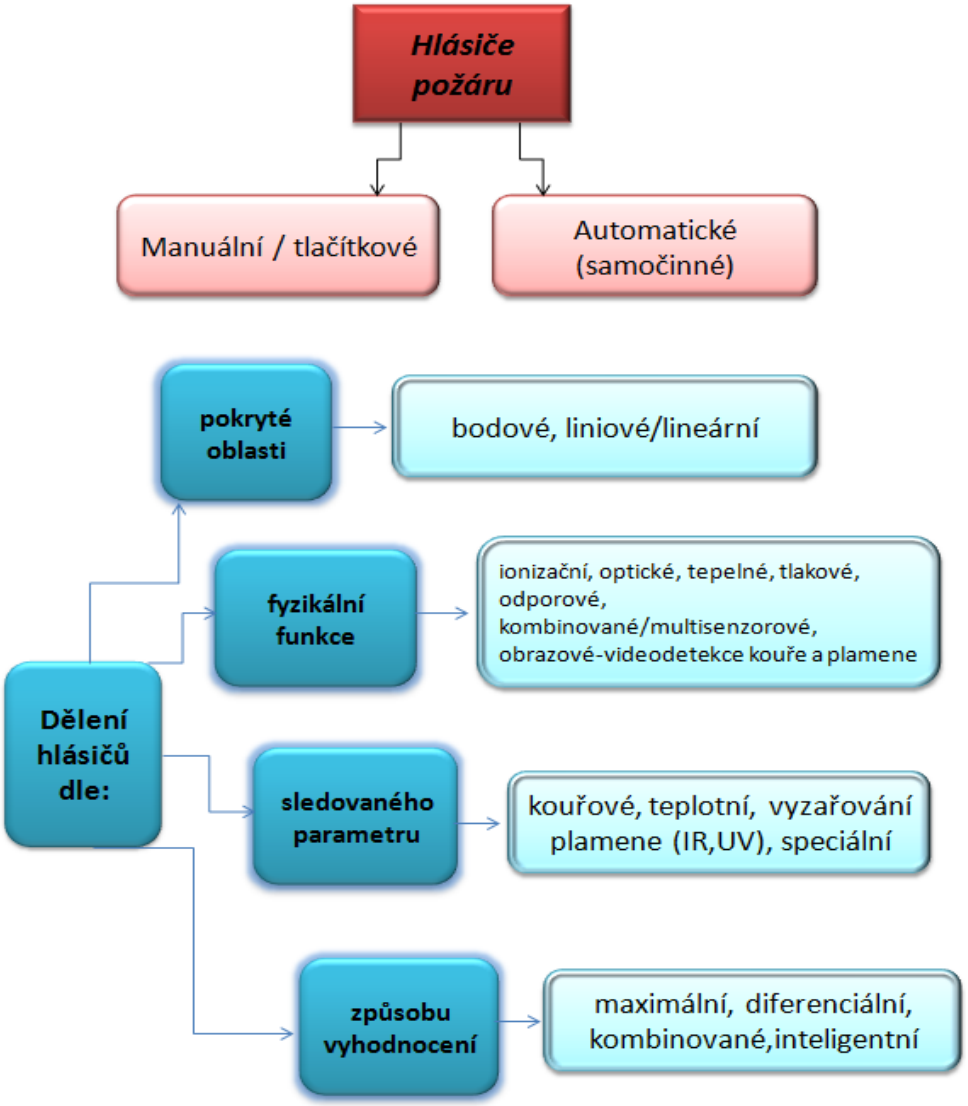
1.2.2 Kamerové systémy

Velmi rozšířený prvek ochrany dnešní doby. Téměř si nelze představit banku, která by tohoto systému nevyužívala. Díky velké rozmanitosti nabízených produktů na trhu si vhodný prvek vybere každý. Mezi nejznámější prvky patří např. TV kamery, IP kamery, záznamová zařízení, videoalarmy aj. Díky kompatibilitě zařízení lze prvky kamerových systémů (dále jen CCTV) propojit s PZTS a tím zvýšit ochranu zabezpečení v objektu. V praxi to funguje tak, že pokud je vyhlášen poplach ve střeženém objektu a zákazník má nainstalovány prvky CCTV, přes webové rozhraní se může ihned zalogovat do systému a zkontrolovat on-line, co se v objektu děje a z jakého důvodu byl vyhlášen poplach. Dokonce i moderní DPPC mají tyto prvky ochrany, dispečer se po vyhlášení poplachu přes webové rozhraní podívá na střežený objekt a zásahovou hlídku směruje přesně na dané místo narušení nebo na místo pohybu osob [34].

1.2.3 Elektrická požární signalizace

Jedná se o velmi účinnou ochranu, která umožní včas upozornit na vznik požáru ve střeženém objektu. EPS je technický prostředek určený k detekci požáru (vznikajícího)

a k automatickému nebo poloautomatickému (za přispění člověka) provedení následných kroků k eliminaci požáru [2]. Objekt lze vybavit hlásiči EPS.



Obr. č. 1. Dělení hlásičů EPS. Zdroj: [2].

1.2.4 Ústředna

Ústřednu lze označit za srdce celého zabezpečovacího systému. Vyhodnocuje stavy z různých detektorů nebo přístupových ovládacích panelů a na základě nastaveného programu reaguje daným způsobem, např. vyhlášením poplachu, spuštěním sirény nebo odblokováním určité zóny. Nutno dodat, že ústředna napájí elektrickou energií i samotné detektory a musí být obzvlášť chráněna, z toho důvodu se umisťuje do instalačních boxů, u kterých jsou dvířka opatřena tamper kontaktem. Je-li s ní neodborně manipulováno, je

vyhlášen tamper neboli sabotáž. Přispět k ochraně ústředny může i sám provozovatel systému tak, že ji vždy umístí do chráněného prostoru, protože jak již bylo zmíněno výše, je srdcem celého systému, pokud by se s ní cokoliv stalo, nelze již chráněný objekt dále střežit [3]. Ústředny PZTS se dělí na:

- smyčkové;
- s přímou adresací detektorů;
- smíšené;
- bezdrátové ústředny.

V případě ústředny EPS je možné dělení na:

- konvenční adresné;
- konvenční neadresné;
- analogové;
- interaktivní.

Z hlediska technického je ústředna plošný spoj, který se skládá z napájecí části, vstupů jednotlivých zón, do kterých se připojují jednotlivé detektory, výstupů pro komunikační prostředky (modul pro připojení na DPPC, GSM modul), systémových konektorů a přepínačů pro nastavování systému [3].

1.2.5 Přenosová zařízení

Je nutné si uvědomit, že samotný systém PZTS je prakticky neúčinný, pokud informace z tohoto systému není včas a spolehlivě přenesena určené osobě či osobám, které mohou na vzniklou událost patřičně reagovat a vyvodit z ní případné důsledky. V rámci zabezpečení se hovoří o DPPC a dispečerovi. K tomuto účelu slouží přenosová zařízení, ke kterým patří např. telefonní komunikátor, GSM komunikátor, GPRS komunikátor, rádiový vysílač nebo Ethernet komunikátor [35].

Telefonní komunikátor

Zpravidla bývá integrovaný na desce ústředny, ale může být řešen i jako samostatný modul. Slouží pro přenos dat na DPPC pomocí telefonní linky. S přijímací stranou DPPC probíhá

komunikace buď pomocí DTMF (Dual-tone multi-frequency), tónové volby (dnes využíváno nejčastěji), nebo pomocí pulzní volby [35].

GSM komunikátor

Slouží pro přenos zpráv prostřednictvím SMS nebo vytáčeného spojení jako náhrada analogové telefonní linky. Funguje v síti GSM a stejně jako u mobilního telefonu potřebuje SIM kartu [35].

GPRS komunikátor

Zařízení, které v GSM síti slouží k přenosu informací z a do ústředny, a to přes internet prostřednictvím připojení přes GPRS. V tomto případě se jedná o oboustrannou komunikaci v GSM síti pomocí datového spojení [35].

Rádiový vysílač

Zařízení, které pracuje na principu vysílání (případně i příjmu) rádiových vln využívajících vyhrazených frekvencí. Komunikace je zde možná jak obousměrná, tak jednosměrná. V praxi je to většinou pouze jednosměrná komunikace, zpravidla na vyhrazené frekvenci v primární síti [35].

Ethernet komunikátor

Jedná se o datovou komunikaci pomocí internetové sítě využívající protokol TCP/IP (*Transmission Control Protocol/Internet Protocol* – „primární přenosový protokol/protokol síťové vrstvy“) [35].

Každé z těchto uvedených zařízení má svá specifika a jejich použití je závislé na typu připojené technologie, dostupnosti přenosové sítě, požadavcích zákazníka a technického vybavení DPPC. Ne vždy však je možné všechna tato zařízení v dané situaci použít.

1.2.6 Přenosové trasy

Pojem přenosová trasa označuje způsob přenosu dat ze střeženého objektu na DPPC. Přenosová trasa je vždy tvořena přenosovým zařízením na straně střeženého objektu

a přijímacím zařízením na straně DPPC. K nejvyužívanějším komunikačním přenosovým trasám dnes patří PSTN, rádiový přenos na vyhrazených frekvencích, přenos po síti GSM a přenos pomocí internetové sítě [36].

PSTN (z angl. Public Switched Telephone Network)

V překladu veřejná komutovaná telefonní síť – zprávy z objektu jsou na DPPC přenášeny pomocí pevné telefonní linky. V dnešní době se sice ještě tato přenosová trasa běžně využívá, skýtá však mnoho zásadních negativ. Tím hlavním je pomalý přenos, přičemž čas přenosu na DPPC hraje velkou roli. Dále pak nefunkčnost telefonní linky, která může způsobit nefunkčnost celého zařízení PZTS, protože to již nemá po čem zprávy ze střeženého objektu posílat [36].

Autorka by dále chtěla upozornit na fakt, že pokud je zvolen tento způsob přenosu, kontrola spojení se ve většině případů provádí jednou za 24 hodin, což v praxi znamená, že ztráta komunikace s DPPC může být zjištěna až druhý den.[1] To je opravdu závažné zjištění. Během této doby nemá dispečer ze střeženého objektu žádné zprávy a objekt může být po tuto dobu ohrožen. Majitel objektu je o této situaci vyrozuměn, ale – jak již bylo zmíněno – k tomu může dojít až po 24 hodinách. Tento způsob přenosu považuje autorka za finančně značně nákladný, protože každé spojení je zpoplatněno, tzn. že pokud je objekt zaalarmován, zpráva je vyúčtována dle platného tarifu. Denně je třeba systém zapnout a vypnout, provést periodické spojení s DPPC, může se vyvolat falešný poplach nebo nastat jakýkoliv technický problém, každé spojení pak znamená další finanční výdaje. Pokud by se tedy autorka měla vžít do role toho, kdo rozhoduje o vhodném přenosovém způsobu na DPPC, telefonní linku by určitě nezvolila. Někdo může namítnout, že existuje možnost zvolit záložní přenos na DPPC, ale z finančního hlediska je to nerentabilní.

Rádiový přenos na vyhrazených frekvencích

Využívá privátní rádiovou síť a v současné době lze označit za nejbezpečnější způsob připojení. K testování spojení s DPPC dochází každých pět sekund (dle nastavení) a informace o případné ztrátě komunikace je tedy předána téměř ihned. Tento způsob je též

[1] Toto nastavení se využívá nejběžněji z finančních důvodů. Za každé spojení se platí, proto je periodický test přenosu uskutečňován pouze jednou za 24 hodin. Samozřejmě lze nastavit i častější kontrolu spojení.

nejrychlejší, samotné narušení objektu je zaznamenáno DPPC během tří sekund. Je třeba zdůraznit, že přenos jakýchkoliv informací z objektu na DPPC je zdarma, tedy bez plateb za spojení či drahé SMS zprávy (záleží ovšem na provozovateli DPPC, zda si bude něco účtovat). Další velkou přednost tohoto způsobu přenosu zpráv představuje fakt, že rádiová přenosová trasa je jedinou přenosovou trasou, která je určena výhradně pro účely přenosu dat z PZTS na DPPC. Dále je z pohledu autorky důležitý aspekt vlastnictví, ve většině případů jsou totiž právě provozovatelé DPPC majiteli těchto rádiových sítí, i když to pro ně znamená i spoustu povinností. Velkou výhodou též zůstává, že majitelé této rádiové sítě mají celou přenosovou trasu pod kontrolou a nejsou v žádném případě závislí na jiném subjektu. Za předpokladu, že majitelé rádiových sítí o ně řádně pečují, mohou svým zákazníkům garantovat dostupnost přenosové trasy sedm dní v týdnu 24 hodin denně [36].

Autorka však musí upozornit též na negativa. Tento způsob přenosu má omezený dosah sítě a pokrytí území signálem, tzn. že je zde omezena vzdálenost napojovaného objektu na DPPC. Pokud se objekt nachází v lokalitě, kde tento rádiový signál není k dispozici, nemůže být tímto způsobem napojen na DPPC [36].

Rádiové sítě, které jsou určené pro přenos zpráv na DPPC, se v České republice provozují v licencovaných pásmech. Na základě žádosti a vypracovaného projektu rádiové sítě provozovatele DPPC vydává Český telekomunikační úřad tzv. Individuální oprávnění k využívání rádiových kmitočtů, které specifikuje druh a maximálně povolený výkon vysílacích rádiových zařízení. Za využívání tohoto rádiového kmitočtu je provozovatel DPPC povinen hradit roční paušální poplatek, jehož výše se odvíjí od poloměru obsluhované oblasti, počtu základnových a sběrných stanic a povoleného výkonu [36].

Rádiové sítě a přenos zpráv z objektu na DPPC může být koncipován jako jednosměrná, nebo obousměrná rádiová komunikace. U jednosměrné rádiové komunikace není možné potvrzení o doručení zprávy na DPPC. Přenos je tedy závislý na kvalitním signálu a spojení bez výpadku signálu, aby nedocházelo ke ztrátám přenášených zpráv. V praxi to znamená, že pokud je objekt napojen pomocí rádiového signálu, nesmí docházet ke ztrátám signálu. Pokud se tak stane, musí na tuto akci dispečer DPPC ihned reagovat. Pokud totiž ke ztrátě signálu dojde, je objekt po dobu tohoto výpadku nestřežen. U obousměrné rádiové komunikace jsou odesílané zprávy z ústředny potvrzovány ze strany DPPC (potvrzení o doručení přijímací stranou). Pokud toto potvrzení vysílač neobdrží, odesílá zprávu znovu, doručení zprávy je tedy zaručeno. Nevýhodou jsou vyšší pořizovací náklady – komponenty

jsou dražší než u jednosměrné komunikace, avšak výhodou je zde vyšší bezpečnost přenosu zpráv. Z pohledu zákazníka je tento způsob přenosu zpráv sice nejdražším (nutno zakoupit rádiový vysílač), ale také nejbezpečnějším. Jak již bylo zmíněno, zákazník neplatí za žádná přenosová data, a samotný přenos je tedy bezplatný [36].

Přenos po síti GSM – sítě mobilních operátorů

Nastane-li situace, kdy je střežený objekt bez přípojky telefonní linky a nemá ani dosah rádiového signálu, existuje možnost využít sítě GSM (Global System for Mobile Comunications). Tento způsob napojení objektu umožňuje tyto alternativy přenosu zpráv z PZTS na DPPC: napojení pomocí GSM sítě v hovorovém pásmu, napojení pomocí GSM sítě v datovém pásmu pomocí služby GPRS, nebo pomocí SMS zpráv [37].

Přenos po síti GSM v hovorovém pásmu je alternativou přenosu pomocí pevné telefonní linky, GSM modul telefonní linku simuluje a přenos probíhá vytáčeným spojením vůči telefonní lince na DPPC. Nevýhody tohoto spojení jsou stejné jako u přenosu po telefonní lince, navíc je přenos pomocí GSM v hovorovém pásmu dále závislý na poskytovateli GSM sítě a pokrytí signálem v daném místě, kde se střežený objekt nachází [37].

Přenos po síti GSM v datovém pásmu pomocí služby GPRS (General Packet Radio Service) využívá GSM síť. Zprávy z objektu se přenesou pomocí internetu na technologické centrum, odkud jsou přeposílány na DPPC. Velkou výhodou tohoto způsobu připojení je trvalé a dohlížené spojení mezi vysílačem a přijímací stranou a tím i rychlá kontrola a zjištění poruchy komunikace (řádově minuty, zpravidla tři až patnáct minut). Ve srovnání s vytáčeným spojením se jedná o rychlý přenos zpráv, komunikace je obousměrná (potvrzovaný přenos zpráv a možnost vzdálené konfigurace komunikátoru). Výhodou jsou i menší pořizovací náklady, náklady na přenášená data většinou závisí na přenášeném množství [37].

Přenos po síti GSM prostřednictvím SMS (Short message service) je jedním z nejdražších způsobů přenosu zpráv, a to kvůli tarifům mobilních operátorů. Dochází k němu zasláním zprávy SMS na DPPC (zprávy z ústředny jsou převedeny na SMS zprávy a jednotlivě nebo i ve větším množství najednou jsou odeslány na DPPC), nebo na majitelem předem dohodnuté telefonní číslo, pokud si nepřeje být monitorován na DPPC. Lze nastavit též obě varianty zároveň – odeslání SMS na DPPC i mobilní telefon majitele objektu. Je nutné opět upozornit na cenu tohoto přenosu, každá SMS je

zpoplatněna dle tarifu operátora. Dále není zaručena doba (rychlost) doručení zprávy a z hlediska provozních nákladů je nutné udržovat SIM kartu neustále ve funkčním stavu (SIM karta musí mít neustále dostatek kreditu, aby mohly být SMS odeslány, pokud dojde k jeho vyčerpání, nemohou být zprávy přenášeny a objekt se stává zranitelným). Spojení se vzhledem k nákladům testuje zpravidla jednou za 24 hodin jako u telefonní linky, což může znamenat zjištění případné poruchy komunikace až po 24 hodinách. Síť může být také přetížená, zprávy jsou pak v důsledku toho doručeny s velkým zpožděním [37].

Přenos pomocí internetové sítě

Jedná se o v dnešní době hojně využívanou přenosovou trasu, a to i díky rozvoji internetového připojení. Jeho prostřednictvím je možný nejen přenos poplachových zpráv a stavových informací, ale také obrazu a zvuku. Dále umožňuje obousměrnou komunikaci, vzdálený dohled a ovládání systému. Velkým pozitivem je zde rychlý dohled nad ztrátou spojení (obvykle jednotky minut). Díky přenosu obrazu z kamerových systémů jsou eliminovány výjezdy k falešným poplachům. Situace se řeší tak, že se buď dispečer, nebo přímo majitel zaloguje do systému a vzdáleně se podívá, co se u střeženého objektu děje a z jakého důvodu byl poplach vyvolán. K nevýhodám tohoto spojení patří závislost spolehlivosti připojení na poskytovateli internetu a obtížné zajištění zálohování napájení všech aktivních prvků zařazených v přenosové trase [37].

1.2.7 Poplachová přijímací centra

Jsou jedním z nejdůležitějších faktorů, které přispívají k ochraně majetku a osob v PKB. Dříve se používalo označení pulty centrální ochrany, avšak od 1. ledna 2011 jsou tato centra dle normy ČSN EN 50518-1 pojmenována jako dohledová a poplachová přijímací centra [1]. Dále dle této normy jsou DPPC charakterizována jako pracoviště, která slouží k monitorování a/nebo příjmu a/nebo zpracování signálů vyžadujících odezvu v případě mimořádné události. Dále norma uvádí definici PPC jako centra s trvalou obsluhou, do kterého jsou zasílány informace týkající se stavu jednoho nebo více poplachových systémů [4].

Norma ČSN EN 50518-1 stanovuje minimální požadavky na návrh, konstrukci a funkční zařízení pro budovy, ve kterých se uskutečňuje monitorování, příjem a zpracování

(poplachových) signálů generovaných poplachovými systémy, jako integrální část celkového procesu zajištění bezpečí a zabezpečení [4].

Obecně tedy lze říci, že základní funkcí DPPC je vyhodnocovat zprávy z bezpečnostních a jiných zařízení, která jsou umístěna ve střeženém objektu zákazníka a které tyto informace dále odesílají na DPPC. Dispečer pak musí dle typu události či zprávy z objektu učinit takové kroky, které povedou k vyřešení přijaté zprávy či události dle smlouvy (sepsané se zákazníkem před napojením na DPPC) nebo jeho pokynů (např. zasílat SMS při každém zapnutí/vypnutí systému v objektu), či směrnic dané společnosti provozující DPPC [25].

Autorka se nyní bude zabývat problematikou DPPC dle normy ČSN EN 50518, avšak uvede pouze nejdůležitější podmínky pro provoz DPPC dle této normy. Norma se skládá ze tří částí:

- ČSN EN 50518-1 Část 1: Umístění a konstrukční požadavky (rok vydání 2010, prosinec);
- ČSN EN 50518-2 Část 2: Technické požadavky (rok vydání 2011, srpen);
- ČSN EN 50518-3 Část 3: Pracovní postupy a požadavky na provoz (rok vydání 2012, leden) [37].

ČSN EN 50518-1 Umístění a konstrukční požadavky

Úvodní část normy ČSN EN 50518-1 stanovuje minimální požadavky na návrh, konstrukci a funkční zařízení pro budovy, kde probíhá monitorování, příjem a zpracování (poplachových) signálů, které jsou odesílány poplachovými zabezpečovacími systémy (dále jen PZS), jako součást kompletního procesu zajištění bezpečnosti a zabezpečení. Požadavky jsou vztaženy jak na případy dálkové konfigurace, v nichž více systémů přenáší informace do jednoho či více poplachových přijímacích center (dále jen „PPC“), tak na případy jednoho jediného centra určeného pro monitorování a zpracování poplachů generovaných jedním či více poplachovými systémy nacházejícími se v témže perimetru daného příslušného místa [4].

Dále norma upravuje tuto problematiku:

- *Volba místa* – dle normy musí být DPPC situováno v místech s nízkým rizikem vzniku požáru, zaplavení, výbuchu, vandalismu a nebezpečí hrozící z jiných míst. Pokud není DPPC jediným uživatelem objektu, v němž je umístěno, musí toto být od zbytku budovy odděleno fyzickou bariérou sestávající ze stěn, podlah, stropů a nezbytných otvorů [4].
- *Posouzení rizik* – před rozhodnutím vybudovat DPPC je potřeba posoudit veškerá rizika spojená s provozem DPPC. Tento záznam z posouzení rizik je pak nutné archivovat a kdykoliv jej pro potřeby auditu poskytnout k nahlédnutí třetí straně [4].
- *Umístění* – je dalším krokem po posouzení rizika. DPPC musí být umístěno uvnitř objektu, jehož obvodový plášť sestává z vnějších stěn, stropů, podlah, ventilačních kanálů, vstupních a výstupních dveří, zasklených ploch, manipulačního okénka, vstupních otvorů pro kabeláž a potrubí. Dále pak musí obvodový plášť DPPC poskytovat odolnost vůči fyzickým útokům, a to dle tabulky 1. V tabulce uvedené stavební prvky představují minimum pro odolání fyzickému útoku, pokud jsou použity jiné stavební materiály, musí tyto zaručit stejnou úroveň odolnosti [4].

  Dále pak odolnost dveří a zasklených ploch v DPPC musí odpovídat i odolnosti proti útoku střelnou zbraní, a to dle EN 1522 FB3. Vnější plášť DPPC musí mít požární odolnost dle EN 13501-2, která nesmí být nižší než 30 minut. Taktéž musí být vyřešena problematika ochrany proti blesku [4].

Tab. 1. Minimální odolnost DPPC proti fyzickému útoku. Zdroj: [4].

Stavební prvky	**Materiály**	**Tloušťka**
Vnější stěny včetně stěn mezi dispečinkem a vstupní halou (viz příloha B)	plné zdivo	> 200 mm
	litý beton	> 150 mm
	železobeton	>100 mm
	plná ocel	> 8 mm
Vnitřní stěny	žádné požadavky	žádné požadavky
Podlahy a stropy	litý beton	> 150 mm
	železobeton	> 100 mm

- *Přístupnost místa* – přístup do budovy nebo části budovy, kde je umístěno DPPC, musí být výhradně v užívání organizace provozující DPPC [4].

- *Příslušenství* – toalety a umývárny musí být uvnitř prostorů DPPC. Pokud jsou uvnitř DPPC také prostory pro přípravu jídla a pití, musí být odděleny od operační místnosti konstrukcí s požární odolností (ta nesmí být nižší než 30 min.) [4].
- *Otvory* – v konstrukci DPPC jsou povoleny jen tyto otvory: vstup z haly, nouzový východ, zasklené plochy, vstupní otvory pro kabeláže a potrubí, manipulační okénko, ventilace [4].
- *Vstupní předsíň* – musí mít dvoje dveře bezpečnostní třídy 4, které musí být navzájem provázány tak, aby je nebylo možné otevřít současně s výjimkou řízených okolností. Oboje dveře musí být opatřeny zamykatelným systémem, který lze ovládat pouze z prostoru DPPC, a musí být vzájemně provázány a ovládány pouze z DPPC [4].

Norma dále definuje veškeré požadavky na elektronickou detekci pro všechny základní části DPPC a zabývá se těmito událostmi: požár, útok zvenčí (narušitel), plyn, vchod/východ, tíseň (přepadení), komunikace, signalizace elektronických ochranných systémů, monitorování bezpečnosti personálu, CCTV. Veškeré tyto systémy uvedené v kapitole poplachových systémů DPPC musí být splňovat požadavky příslušné normy. Pokud nastane případ, kdy norma neexistuje, musí se údržba provádět dle směrnic výrobce tak, aby byla zaručena trvalá spolehlivost [4].

Poslední část se zabývá napájením DPPC elektrickým proudem a záložními zdroji napájení (síťové napájení, záložní zdroje napájení, záložní akumulátor – UPS, pohotovostní generátor). Tato problematika je řešena v praktické části.

ČSN EN 50518-2 Technické požadavky

Druhá část normy ČSN EN 50518-2 stanovuje technické požadavky týkající se DPPC a taktéž zahrnuje funkční kritéria a ověřování výkonnosti [27].

- *Požadavky na výkonnost* – norma stanovuje výkonnostní kritéria pro poplachové přijímací zařízení a zdroje: v případě tísňových poplachů – 30 s u 80 % přijatých signálů a 60 s u 98,5 % přijatých signálů. V případě všech ostatních poplachů 90 s u 80 % přijatých signálů a 180 s u 98,5 % přijatých signálů. Tohoto souladu musí být dosaženo v průběhu dvanácti po sobě jdoucích měsíců [27].

- *Požadavky na komunikaci* – v DPPC musí být taková zařízení, aby vnější komunikace byla automaticky zaznamenávána s časem i datem a aby ji bylo možno obnovit, zobrazit, znovu přehrát a uchovat po dobu nejméně tří měsíců [27].
- *Příjem signálů* – každý přijatý signál musí být v DPPC samostatně identifikovatelný, zaznamenaný automaticky a poskytovat informace o identifikaci střežených prostorů, datum a čas přijetí signálu a typ signálu. Zásah dispečera, pokud je situací vyžadován, musí být taktéž zaznamenán včetně data i času jeho dokončení a totožnost dispečera, který zásah provedl [27].
- *Testování* – pro pravidelné testování všech zařízení, která jsou potřebná pro provoz DPPC, musí existovat dokumentované postupy. Denně musí být kontrolována činnost těchto zařízení: komunikátor přijímacího centra, komunikační systémy, indikační zařízení, veškeré příchozí a odchozí komunikační linky. Každý týden musí být ověřována správná funkčnost u těchto zařízení: poplachové systémy DPPC, elektrické napájecí zdroje, zařízení pro nouzové osvětlení. Výsledky těchto testů musí být zaznamenávány a pokud nastane jakákoliv závada (zařízení zapojená do příjmu, zobrazení, napájení), musí existovat alternativní řešení, které je uvedeno do provozu automaticky nebo dispečerem DPPC. Toto musí být provedeno do jedné hodiny od okamžiku, kdy se dispečer o závadě dozví [27].
- *Údaje* – je nutné věnovat pozornost evropské směrnici o ochraně osobních údajů, především u kategorií, jako jsou údaje o zákazníkovi, údaje o vnější komunikaci DPPC a záznamy o zákrocích dispečera [27].
- *Uchovávání údajů* – veškeré údaje o klientovi musí být uchovávány po dobu nejméně dvou let, veškeré údaje o vnější komunikaci DPPC musí být uchovávány po dobu nejméně tří měsíců a záznamy zákroků dispečera DPPC musí být uchovávány po dobu nejméně dvou let [27].
- *Nouzový plán* – *v* případě vyřazení DPPC z činnosti, musí být připravený vypracovaný nouzový plán pro vypořádání se s těmito následky. Nouzový plán se musí ošetřovat přiměřeně na základě předvídatelné mimořádné události s potenciálem zhoršení kvality služeb DPPC. Opatření, která budou provedena, musí být jasně vymezena a musí se vztahovat na technické a/nebo jiné havárie. Tento nouzový plán musí obsahovat: kontaktní údaje dodavatelů a poskytovatelů

služeb schopných provést obnovení při zachování dané služby; prostředky, kterými budou pokračovat nebo budou obnoveny dodávky služeb; přezkoumání nouzového plánu ne déle než do šesti měsíců vedením, které musí zdokumentovat a navrhnout všechna nápravná opatření. Mezi abnormální události, které je při sepisování nouzového plánu třeba brát v úvahu, se řadí: úplné selhání schopnosti provádění úkonů; poruchy, nebo poškození technické infrastruktury stanoviště, komunikační zařízení nebo komunikačních okruhů; požár, včetně vystavení ohni v sousedních a přilehlých objektech; povodně nebo jiné průniky vody; poškození při bouřce, včetně přepětí v důsledku blesku při dodávce elektřiny a telefonní vedení; náraz vozidla, včetně kolejových vozidel a letadel; úmyslné poškození; zločinný útok, vyhrožování bombou, nebo jiné situace protiprávního nátlaku [27].

ČSN EN 50518-3 Pracovní postupy a požadavky na provoz

Třetí část normy stanovuje minimální požadavky a postupy na provoz DPPC.

- *Personální obsazení* – DPPC musí být trvale obsazeno nejméně dvěma dispečery. Pokud je DPPC provozováno současně s druhým DPPC a provozní postupy zajišťují stejný efekt jako u DPPC obsazeného dvěma dispečery, je tento požadavek považován za splněný [28].
- *Bezpečnostní prověření* – jedná se o proces kontroly minulosti a zázemí zaměstnanců či potenciálních zaměstnanců [28].
- *Bezpečnostní lustrace* – státní orgán prověřuje rejstříky trestů zaměstnanců a potenciálních zaměstnanců [28].
- *Výcvik* – každá společnost musí pro všechny příslušné zaměstnance zajistit výcvik. Všichni dispečeři musí být před získáním povolení schopní zpracovávat poplachy bez dozoru a absolvovat výcvik zajišťující minimální způsobilost k provádění konkrétních úkolů. Pokud nastane případ, kdy se DPPC opatří novým technickým vybavením či snad nastanou změny provozních postupů, musí být dispečeři znovu proškoleni na danou oblast činnosti [28].
- *Provozní postupy* – předpisy pro provozní postupy musí být dostupné pro všechny dispečery a musí obsahovat postupy pro testování, vstup do a odchod z DPPC,

správu databází, provozní kontinuitu a nouzové stavy, evakuační postupy a zpracování signálů [28].

2 POJEM BEZPEČNOST

Pojem bezpečnost je možné interpretovat mnoha různými způsoby podle toho, v jakém kontextu se o bezpečnosti hovoří. Lze se shodnout na tom, že bezpečnost znamená určitou míru jistoty, která snižuje pocit ohrožení. Bezpečnostní problematika provází lidstvo již od počátků existence. Důvody a metody zabezpečení se v průběhu historie měnily, ale objektem (předmětem) zabezpečení a ochrany byly vždy tyto tři hlavní skupiny:

- zdraví a život (fyzická existence jednotlivce);
- majetek (vše, co je spojeno s vlastnickými vztahy k věcem a předmětům jak hmotného, tak i nehmotného charakteru);
- informace a znalosti na těchto informacích založené (vše, co je spojeno s prosazováním a ochranou zájmů jednotlivých osob a skupin v rámci jejich existence ve společenství) [21].

Obavy z rizika vykradení rodinného domu nebo obavy z rizika ztráty hmotného či nehmotného majetku mají za následek lidskou snahu o minimalizaci těchto rizik. Bezpečnost majetku pak lze zajistit právě již zmiňovaným připojením na DPPC. S tím souvisí i bezpečnost dat či informací, kterými disponují společnosti, které mají chránit své klienty či jejich majetek (společnosti zabývající se ochranou majetku a provozováním DPPC). Všichni pracovníci, kteří pracují s jakýmikoliv daty, by si měli uvědomit, že je musí chránit a předcházet bezpečnostním rizikům, které mohou vzniknout při jejich nesprávném používání [26].

2.1 Informační bezpečnost

Informace lze chápat jako skutečnosti, které mají určitou hodnotu a s nimiž lze nakládat jako s penězi. Lze s nimi i obchodovat, ničit je, poškozovat, transformovat. V dnešní době neexistuje bezcenná informace a vždy lze vyčíslit potenciální zisk, případně ztrátu, kterou může informace pro daného člověka představovat. K informacím by se měl člověk chovat stejně jako k vlastním financím. A toto by měly mít na paměti hlavně společnosti, které disponují velmi citlivými daty či informacemi, mezi které bezesporu patří společnosti provozující DPPC [21].

2.2 Bezpečnost PC

V zájmu minimalizace rizika devastujících útoků jak na PC, tak na běžně využívanou síť je vhodné znát základní způsoby násilných narušení bezpečnostních opatření hackery, kteří tuto činnost považují za své umění. Rovněž by měl být bezodkladně řešen jakýkoliv problém na počítači, ať už podezřele pomalé načítání souborů nebo větší objem nevyžádaných e-mailů. Včasná identifikace a odstranění problémů může přispět k minimalizaci škod v budoucnu, a pokud se to týká počítače, na kterém je provozováno DPPC, musí je dispečer neprodleně oznámit správci DPPC [24].

3 BEZPEČNOST A UCHOVÁNÍ DAT NA DPPC

Informace neboli data využívaná na DPPC patří bezesporu k těm nejcitlivějším, kterými společnosti zabývající se činností v PKB a provozující DPPC disponují. Tyto společnosti musí tato data chránit všemi dostupnými prostředky, neboť jejich zodpovědnost je vzhledem k velkému množství velmi citlivých dat (telefonní číslo majitele, adresa střeženého objektu), kterými disponují, velká. Jejich odcizení či ztráta představují velký problém nejen pro společnost, ve které tato situace nastala, ale taktéž pro její klienty, kteří jí tato data poskytli.

Pokud se někdo rozhodne nechat střežit svoji firmu či rodinný dům, musí mít DPPC při výjezdu k tomuto objektu dostatek informací. Z toho důvodu má tedy každý střežený objekt svou kartu, která obsahuje veškeré dostupné informace, např. název objektu, jeho adresu, číslo, kontaktní osoby včetně čísel mobilních telefonů na majitele, fotografie objektu, plánek rozmístění prvků poplachového zabezpečovacího systému, EPS, zprávy z objektu za aktuální měsíc atd. Tyto informace nesmí být za žádných okolností poskytnuty třetí straně ani využity k jinému účelu, proto je velmi důležité, aby tato data byla velmi dobře chráněna.

Na základě vlastní dlouholeté praxe může autorka konstatovat, že každá společnost provozující DPPC (nebo zabývající se jinými službami) by měla mít jasně stanovená pravidla pro práci s firemními daty a taktéž by měla mít určeného zaměstnance, který se o tuto bezpečnost bude starat. Mezi jeho úkoly může patřit kontrola stavu antivirového programu (aktualizace, prodloužení licence), pravidelné stahování aktualizací na DPPC nebo zálohování firemních dat. Každý zaměstnanec může přispívat k ochraně firemních dat.

3.1 Bezpečnostní software

Dle typu ochrany dat lze bezpečnostní software rozdělit na několik oblastí, kterými mohou být např. autentizace uživatele, správa a ochrana hesel, rodičovská kontrola, přístup k zařízení či zálohování dat [29].

3.1.1 Autentizace/identifikace uživatele

Problematika autentizace uživatele v rámci DPPC znamená v praxi ověření identity uživatele-dispečera nebo správce systému nebo jiných pracovníků DPPC, kteří pracují s informacemi. V praxi je tento problém vyřešen tak, že na každém DPPC by se měl dispečer do systému přihlašovat pod svým heslem a jménem, za žádných okolností by neměl své heslo komukoliv sdělovat. Pokud by totiž došlo k nějakému incidentu, administrátor v systému může zjistit, který dispečer byl v inkriminovanou dobu zalogován, a zodpovědnost za situaci by na něj byla přenesena[2] [29].

Dalším způsobem, jak chránit data na DPPC, je přístupová úroveň do systému. Dispečer má v tomto případě jiné možnosti úprav dat v DPPC než například samotný vedoucí DPPC nebo správce systému. V praxi to funguje tak, že dispečer má do systému přístup, avšak nemá už pravomoc například vymazat kontaktní osobu nebo změnit adresu hlídaného objektu, tyto informace může změnit pouze vedoucí DPPC. Dispečer má k dispozici pouze okno pro zprávy mezi dispečery, které slouží výhradně pro komunikaci mezi nimi. Do tohoto okna pak zapisuje odchylky od normálu, jakými mohou být např. již zmiňovaná změna telefonního čísla u majitele objektu nebo třeba dovolená kontaktní osoby [29].

Významným způsobem může k ochraně dat na DPPC přispět i samotný dispečer, a to tak, že nebude sdělovat žádné informace zákazníkovi, který není uveden v seznamu kontaktních osob střeženého objektu či nezná heslo nebo číslo objektu, na který se dotazuje. Pokud si zákazník žádá jakékoliv informace o střeženém objektu, musí splňovat alespoň jedno z výše uvedených kritérií. Každý majitel střeženého objektu by měl uvést do karty objektu i heslo. Jakékoliv informace mu pak mohou být sděleny až po správném zadání tohoto hesla, dispečer DPPC tak bude mít záruku, že tomuto zákazníkovi (majiteli) může požadované informace poskytnout. Není potřeba zdůrazňovat, že toto heslo by měly znát pouze zainteresované osoby (manželka, dcera, syn atd.) se vztahem k danému objektu.

[2] Že to tak nemusí fungovat v praxi, se autorka přesvědčila při auditu v jedné nejmenované společnosti. Hesla byla volně přístupná, neboť byla nalepena na monitoru počítače. Na dotaz, z jakého důvodu jsou tyto citlivé informace zveřejněny, odpověděl dotyčný pracovník, že si heslo nemůže zapamatovat. Přitom při zadávání hesla si lze zvolit takovou kombinaci znaků, která je pro danou osobu snadno zapamatovatelná, čímž lze předejít těmto bezesporu trapným situacím.

Chránit data na DPPC lze také softwarově. Na počítači, na kterém je provozováno samotné DPPC, je nainstalován program na ochranu proti virům a jinému škodlivému softwaru. Samozřejmostí je též dobrý antivirový program, v žádném případě free verze [29].

3.1.2 Správa a ochrana hesel

Na většině DPPC je správou hesel pověřen supervizor DPPC, který každému z dispečerů v systému vygeneruje login (jméno a příjmení) a přednastavené heslo (například 1234). Po prvním přihlášení do systému si ho dispečer dle vlastního uvážení změní na heslo pro něj snadno zapamatovatelné. Jak již bylo zmíněno, heslo dispečer nikomu nesděluje [29].

3.1.3 Rodičovská kontrola

Název tohoto způsobu kontroly je odvozen od možnosti chránit děti před nebezpečným obsahem na internetu. Její aplikace do podnikové sféry umožňuje správci blokovat určité webové stránky (např. facebook či jiné sociální sítě), nebo omezit čas trávený na internetu, a to dokonce pro každého uživatele zvlášť. Dle názoru autorky by měl mít každý dispečer znemožněn přístup na internet tak, že bude počítač, na kterém je provozováno DPPC, pro tyto účely zablokován. Rovněž by mělo být zákazáno využívání počítače k jakýmkoliv jiným aktivitám, než je samotný provoz DPPC [29].

3.1.4 Přístup k zařízení

Pod tímto typem ochrany se skrývá možnost cíleného řízení přístupu externích zařízení k počítači, zejména přes USB zařízení, u něhož hrozí největší pravděpodobnost přenosu nebezpečného typu software (tzv. malware)[3] a tím i poškození dat v počítači. Podle názoru autorky by každá společnost provozující DPPC měla této funkce využít, protože přispívá k velmi dobrému zabezpečení pracoviště DPPC. Tento zákaz by měl být zanesen ve vnitřních předpisech a přímo na tomto pracovišti by mělo být striktně zakázáno použití USB disků a jiných přenosných zařízení, které by toto řídící centrum mohlo ohrozit.

[3] Malware je společným názvem pro škodlivé kódy či kód, tedy software nebo jiná data, jejichž účelem je poškodit počítač nebo jeho obsah či jej jinak zneužít. Mohou sem být řazeny i programy, které umí jen infiltrovat počítač bez souhlasu jeho uživatele (majitele) [38].

3.1.5 Zálohování

Ke ztrátě dat může dojít kdykoliv, ať už se jedná o nešťastnou nehodu (smazání, přepsání) či plánovanou sabotáž (zcizení). Z tohoto důvodu by měla každá společnost svá data pravidelně zálohovat. Zálohování společně s šifrováním záloh je jediným způsobem, jak data efektivně ochránit. Je také potřeba brát v úvahu možnost poškození daného média, ať už technickou závadou, či úmyslným poškozením, obnova dat z takto poškozeného média je nejen finančně velmi nákladná, ale i nejistá. Přitom lze tomuto problému předejít vhodným a pravidelným zálohováním dat. V dnešní době je trh plně nasycen různorodými zálohovacími softwary, které veškerou práci obstarají samy. Některé tyto programy jsou dokonce i ve freeware verzích, takže nejsou pro uživatele ani finančně náročné. Avšak z pohledu společnosti, která se zabývá ochranou majetku či osob nebo provozuje DPPC, by investice do takového programu měla být samozřejmostí. Nutno dodat, že tyto programy jsou i součástí některých operačních systémů. Autorka se domnívá, že pro žádnou společnost nebude hledání správného softwaru pro zálohování představovat větší problém. Zálohovat data je možné dvěma způsoby:

- prvním je zkopírování dat na externí úložiště, např. druhý disk, externí disk nebo jiné datové úložiště;
- druhým je využití nějakého programu nebo možností operačního systému vytvářet zálohy [22].

První metoda vyžaduje pravidelné ukládání a určitou disciplínu, využití zálohovacího programu je v tomto ohledu pohodlnější – vše ohlídá sám a pravidelně zálohuje data podle nastavených parametrů. V některých případech lze provést kompletní zálohu počítače včetně všech uživatelských nastavení a nainstalovaných programů. Tyto programy také většinou zajistí, že se zálohují pouze nová data nebo změny, takže každá následující záloha už není tak časově náročná.

Hlavním důvodem pro zálohování dat je současná absence alternativy, jak vlastně data stoprocentně chránit. Pro většinu podniků mají data větší hodnotu než jejich počítačové vybavení. Uživatelé se mohou mylně domnívat, že pokud mají dobrý antivirový program a zapnutou bránu firewall, žádné nebezpečí nehrozí. Ztráta dat však může mít mnoho příčin. Za ty nejzásadnější považuje autorka následující:

- *Selhání operačního systému* – mnoho uživatelů má data uložena pouze na disku, který není rozdělen na části, pokud pak dojde k selhání a data i operační systém jsou uložena v jednom oddílu, může uživatel o veškerá tato data přijít [22].
- *Lidské hrozby* – selhání lidského faktoru je jedním z nejčastějších důvodů ztráty dat. Uživatel může např. nechtěně data smazat, zapomenout své přístupové heslo nebo způsobit mechanické poškození pevného disku, např. v důsledku pádu [22].
- *Hardwarová porucha* – nastane-li technický problém (např. výpadek internetové sítě), může být znemožněn přístup k jakýmkoliv informacím, které jsou na vzdáleném uložišti (cloudu) uchovány. Mezi faktory působící negativně na životnost hardwaru lze zařadit např. vlhkost, výkyvy teploty nebo prach [22].
- *Porušení dat na disku způsobené výpadkem napájení počítače* – pokud nastane výpadek elektrického proudu v okamžiku zápisu dat na disk, dojde k jejich ztrátě. Řešením je připojení záložního zdroje neboli UPS ke stěžejním počítačům [22].
- *Chyba aplikačního programového vybavení* – nejčastější chybou uživatelů bývá stahování nejrůznějších aplikací z internetu. Typickým příkladem mohou být hry stahované z nedůvěryhodných serverů, které mění systémové nastavení, a způsobí tak i havárii celého počítače. Například na DPPC, ve kterém autorka působí, je jakékoliv stahování zakázáno [22].
- *Viry a malware* – počítač je nutno zabezpečit dobrým programem (ve firemním prostředí však nepřichází v úvahu freeware) proti virům a spywarům, avšak neméně důležité je také tento program co nejčastěji aktualizovat. Rizikem je neustálý náskok hackerů, a proto objeví-li se nová hrozba, vývojářům antivirových a antispywarových programů vždy nějakou dobu trvá vydání jejich aktualizace [22].

3.2 Zabezpečení dat na dohledovém a poplachovém přijímacím centru

Zabezpečení dat na DPPC by mělo být co nejvyšší, a to jak z pohledu softwaru (kvalitní antivirový program), tak z pohledu hardwaru (špičkové technické vybavení počítačů).

3.2.1 Zabezpečení databáze DPPC

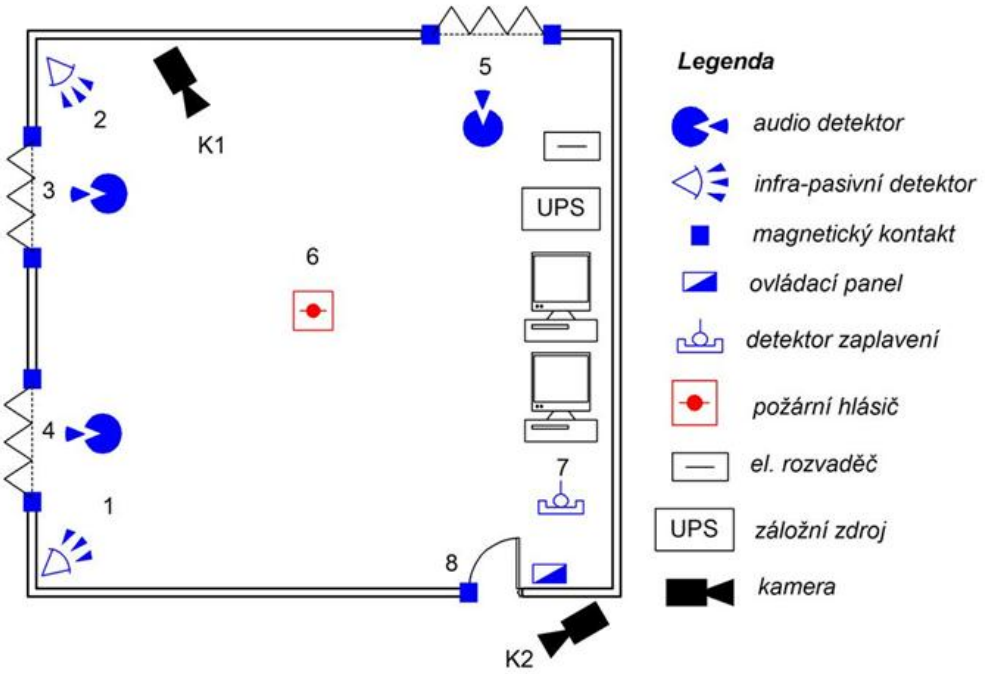
Na DPPC je nejdůležitějším článkem databáze, která obsahuje veškerá data o hlídaných objektech (například zprávy za aktuální měsíc, zprávy od-do atd.). Pokud by došlo ke ztrátě nebo poruše této databáze, přichází DPPC automaticky i o tyto informace. V důsledku absence těchto dat pak kupříkladu nelze dohledat, zda byl před měsícem objekt zaalarmován, či nikoliv. Pokud by si například majitel vyžádal výpis z DPPC a společnost by tyto informace kvůli ztrátě databáze nemohla poskytnout, mohla by tato velmi nepříjemná situace skončit až výpovědí smlouvy o střežení daného objektu. Z tohoto důvodu je velmi důležité, aby tato databáze byla nejen neustále chráněna, ale také pravidelně zálohována. Díky pravidelným zálohám databáze je schopen supervizor kdykoliv při jakémkoliv problému nahrát záložní databázi do DPPC a ztráta dat může být třeba pouze hodinovou záležitostí (například by chyběla data od 12:00 do 13:00). Tato databáze je samozřejmě zálohována na zabezpečený síťový disk, na který má přístup pouze správce systému nebo jím pověřená osoba.

3.2.2 Zabezpečení serveru DPPC

Důležité je i zabezpečení serveru, který zajišťuje provoz DPPC a který musí být oddělen od ostatních serverů. Na tento server nesmí mít přístup nikdo jiný než správce sítě či jím pověřená osoba, místnost tohoto serveru by měla být střežena také fyzickým zabezpečením.

Návrh zabezpečení místnosti serveru DPPC

Místnost serveru je klíčová, je v ní umístěn počítač, na kterém jsou ukládána veškerá ve společnosti využívaná data. Místnost by měla být klimatizována, aby nedošlo k přehřátí počítače serveru DPPC. Na následující straně bude představen autorčin ilustrativní návrh zabezpečení místnosti serveru (viz obr. č. 2).



Obr. č. 2. Návrh zabezpečení místnosti serveru. Zdroj: autorka.

Místnost serveru autorka nejdříve zabezpečila dvěma infra-pasivními detektory, které reagují na pohyb, a tyto prvky umístila k hlavním dveřím a na protější stranu serveru. Místnost serveru je navržena tak, že vnější stěny jsou přístupné zvenčí. Proto jsou na všech oknech umístěny audio detektory, které zaznamenávají tříštění skla. Okna jsou dále zabezpečena magnetickými kontakty monitorujícími neoprávněné otevření, dále pak také mřížemi a bezpečnostní fólií. Místnost serveru je dále situována přímo pod střechou objektu, z tohoto důvodu je tato místnost opatřena záplavovým detektorem – pro případy, že by došlo k havárii vody nebo do této místnosti zateklo ze střechy. Další magnetický kontakt chrání vstupní dveře před neoprávněným otevřením. Velmi důležité je upozornit na případný vznik požáru v místnosti, za tímto účelem je instalován požární hlásič umístěný na stropě místnosti. Nedílnou součástí zabezpečení je využití kamerového systému. Autorka zvolila zabezpečení dvěma kamerami, a to jak při vstupu do místnosti, tak hlídání pohybu v prostoru místnosti. Záznam z těchto kamer se zaznamenává na DVR a ukládá se do počítače správce sítě, kam má přístup pouze on a majitel firmy. Autorka počítá s tím, že by všichni zaměstnanci byli na tuto situaci upozorněni a byla by s nimi podepsána klauzule o monitorování této místnosti pomocí CCTV.

Celý systém bude připojen k náhradnímu zdroji (UPS), který se v případě výpadku elektrické energie automaticky zapne a začne tento systém napájet energií. Seznam smyček by tedy vypadal takto:

1) prostor server levá část – infra-pasivní detektor;
2) prostor server – infra-pasivní detektor;
3) okno 1 vstup od firmy – audio detektor;
4) okno 2 vstup od firmy – audio detektor;
5) okno 3 směr parkoviště – audio detektor;
6) požár server – požární hlásič;
7) vnik vody do serveru – záplavový detektor;
8) vstup server – magnetický kontakt.

Pokud by byl vyhlášen poplach na jakémkoliv detektoru nebo hlásiči, zpráva by se zobrazila dispečerovi DPPC a ten by začal tuto událost řešit.

4 STRUKTURA DPPC Z HLEDISKA HARDWARU A SOFTWARU[4]

DPPC se skládá ze softwarové a hardwarové části, přičemž jedna bez druhé nemůže plnit svoji funkci, každá z těchto částí má svá specifika.

4.1 Softwarová část DPPC

Softwarová část DPPC se zabývá programovým vybavením DPPC. Na českém trhu je nespočet monitorovacích softwarů, které mají svá specifika a jiná uživatelská rozhraní. Tyto programy slouží k zobrazení, vyhodnocení a archivaci zpráv ze střežených objektů.

Uživatelský software vznikl pro potřebu rychle a bezpečně zpracovat větší množství přijatých zpráv (informací) na DPPC. Hlavním úkolem uživatelského softwaru je přehledně, jasně a stručně zobrazit přijaté zprávy na DPPC tak, aby dispečer byl schopen v co nejkratší možné době zareagovat na vzniklou událost. Důležitou vlastností je přehlednost a názornost zobrazené zprávy, barevné odlišení či zvukový doprovod aj. Program lze doplnit o celou škálu dalších užitečných funkcí pro efektivnější fungování. V dnešní době se tyto aplikace již neobejdou bez velkého množství grafických prvků, kterými mohou být např. mapy, schémata, fotografie nebo různé modely, díky kterým se stává práce ještě přehlednější. Jádrem systému je databázová aplikace, která dokáže zpracovat a bezpečně uchovat velké množství dat (informací). Nejčastěji se využívá Microsoft SQL Server, který se osvědčil díky své spolehlivosti.

Uživatelský software je stejně jako většina aplikací složen z několika modulů. Tyto moduly představují určité ovládací a funkční vlastnosti. Moduly lze do programu doinstalovat, a rozšířit tak funkce celého systému. Každý z těchto modulů zastává určené operace (např. modul pro automatické funkce, modul pro příjem zpráv, modul dálkové komunikace nebo modul pro hromadné zpracovávání výpisů z DPPC).

V praxi to na DPPC poté funguje tak, že zprávy zaslané z ústředny střeženého objektu přes přenosovou cestu jsou daným komunikačním kanálem přijaty ke zpracování příslušným modulem systému (modem) a pomocí SQL Serveru jsou uloženy do databáze. Zde jsou pod přihlášením zabezpečeny tak, aby nedošlo k jejich neoprávněnému užití. Poté se

[4] Při psaní této kapitoly autorka vycházela z vlastních zkušeností na pozici dispečerky v konkrétním DPPC a ze školení, jimiž prošla v průběhu své praxe.

uživatelský software v pravidelném časovém intervalu dotazuje databáze na aktuální stav. Pokud je v databázi nový údaj, zobrazí se na obrazovce monitoru obsluhujícího dispečera.

Mezi základní vlastnosti, které by měl takový software nabídnout, autorka řadí například:[5]

- *Přihlášení do DPPC* – do systému DPPC se přihlašuje dispečer pomocí loginu a hesla. To je velmi důležité pro zpětnou kontrolu toho, který dispečer měl daný den službu nebo který dispečer řešil danou událost. Pokud nastane nějaký incident na DPPC, tento systém vše ukládá a zaznamenává, administrátor je potom schopen veškerá tato data zpětně dohledat.
- *Okno událostí* – je jednou z nejdůležitějších částí aplikace, zobrazuje zprávy zaslané ze střežených objektů do systému DPPC.
- *Karta objektu* – slouží k identifikaci každého střeženého objektu, jsou zde o něm uvedeny veškeré informace, např. kontaktní osoby včetně telefonních čísel, adresa střeženého objektu, stav objektu (stav sítě, baterie a komunikace), fotografie objektu, půdorys objektu s vyznačenými prvky ochrany, číslo střeženého objektu.
- *Historie zpráv* – umožňuje nahlédnout do seznamu příchozích zpráv. Měla by zde být nabídka výpisu zpráv za aktuální měsíc (vygeneruje pouze zprávy za zvolený měsíc) nebo v určeném časovém intervalu od-do (zobrazí historii zpráv z objektu např. za poslední tři měsíce nebo dle zvolených parametrů).
- *Grafické zobrazení* – mapy, fotografie, půdorysy objektu atd., tedy materiály sloužící k bližší identifikaci střeženého objektu. Příkladem může být fotografie střeženého objektu s vyznačenými hlídanými sekcemi.
- *Servisní funkce* – jedná se o informace technického charakteru, např. výpadek komunikace, výpadek elektrické energie, porucha baterie ve střeženém objektu nebo jiné důležité poruchy či události. Dispečer na ně musí včas a řádně zareagovat, např. vyrozuměním majitele nebo vysláním zásahové jednotky k objektu, pokud to daný technický problém vyžaduje.

Podle názoru autorky mezi nejrozšířenější monitorovací softwary patří:

[5] Následující výčet autorka sestavila na základě zkušeností a vlastní praxe v oboru.

- monitorovací SW NET–G od společnosti NAM System, a. s.;
- monitorovací SW WRS32, RADOMNET a RADOMNET II od společnosti RADOM, s. r. o.;
- monitorovací SW LATIS® SQL od společnosti Trade Fides, a. s.

4.2 Hardwarová část DPPC

DPPC je ve většině společností provozováno na osobním počítači. Aby mohl plnit svou funkci a poskytnout potencionálním zákazníkům široký výběr možností připojení střeženého objektu na DPPC, měl by tento počítač být vybaven hardwarovými prostředky popsanými v následujícím textu.[6]

4.2.1 Přijímací strana

Přijímá zprávy ze střežených objektů z bezpečnostních systémů (PZTS, EPS). Každé DPPC by mělo být vybaveno minimálně těmito hardwarovými prostředky:

- *Přijímač telefonních linek* – díky němu může počítač DPPC přijímat zprávy z objektů, které jsou napojeny pomocí telefonní linky. Každá společnost by měla mít k dispozici aspoň tři telefonní linky, aby v případě obsazení jedné z nich bylo možné využít jiné a střežený objekt neměl problém spojit se s DPPC.
- *Rádiový přijímač* – slouží objektům napojeným na DPPC rádiovou cestou a tyto zprávy přijímá na privátní síti.
- *Přijímač GPRS REGGAE* – je určený pro objekty, které jsou napojeny na DPPC rádiovou cestou pomocí GPRS komunikátorů, a tyto zprávy přijímá po síti NSG.
- *Přijímač HaSaM* – tento hardware je vhodný pro objekty, které jsou napojeny na DPPC pomocí SMS komunikátoru a komunikují prostřednictvím zasílání SMS zpráv na přijímací stranu DPPC.

[6] Následující výčet autorka sestavila na základě dlouholetých zkušeností a vlastní praxe v oboru.

4.2.2 Driver

Jedná se o program, který převádí přijaté zprávy a zapisuje je do databáze, tedy o program, který se SW NET-G umožňuje současně příjem zpráv ze všech střežených objektů, zpracování a překódování příchozích zpráv, jejich přiřazení a rozklíčování a následné vyvolání akce na DPPC [31].

4.2.3 Záložní síťový disk

Slouží k zálohám konfigurací a dat z celého serveru, který DPPC používá [32].

4.2.4 Zdroje energie

Síťové napájení

Dispečink DPPC musí být napájen ze sítě, která slouží jako hlavní zdroj elektrické energie. Pokud je využito jakékoliv jiné spolehlivé alternativy, musí být na pracovišti DPPC indikováno, jaký je aktuální zdroj napájení. Síťové napájení musí být dimenzováno tak, aby byl zajištěn dostatečný příkon pro napájení veškerého zařízení DPPC a aby zároveň umožnilo nabíjení záložních akumulátorů k dosažení požadované kapacity do 24 hodin [4].

Záložní zdroj napájení

Záložní zdroje napájení musí mít takovou kapacitu, aby umožňovala nepřerušovanou funkčnost veškerých přenosů, signalizaci, záznam, monitoring, základní větrání a osvětlení (včetně osvětlení pro kamerový dohled) po dobu 24 hodin při zatížení 1,5 násobkem průměrného odběru. Tento zdroj nesmí při přepínání na nebo ze záložního zdroje napájení ovlivnit normální provoz zařízení. Záložním zdrojem napájení je buď záložní akumulátor, záložní generátor, nebo generátory podporované záložním akumulátorem. Záložní akumulátory a veškerá zařízení, která slouží k automatickému přepínání z hlavního na záložní zdroj nebo zdroje, musí být umístěny na dispečinku DPPC [4].

Záložní akumulátor (UPS)

Tento záložní akumulátor musí být automaticky uveden v činnost, jakmile napětí primárního zdroje napájení poklesne pod úroveň nutnou pro provoz DPPC. DPPC musí přejít zpět na primární zdroj napájení, jakmile je dodávka proudu z tohoto zdroje opět

obnovena. Pokud je pro nouzové napájení využíván záložní generátor, musí být jeho kapacita dostatečná pro napájení DPCC po dobu nejméně deseti minut [4].

Pohotovostní generátory

Jakýkoliv takový generátor umístěný uvnitř prostoru DPPC musí být od zbytku pracovního prostoru DPPC oddělen stavební konstrukcí, která je odolná vůči požáru. Veškeré tyto generátory (či generátor) musí být zásobeny palivem pro činnost trvající nejméně 24 hodin. Generátory musí mít nezávislé prostředky pro automatické startování, jakmile dojde k výpadku zdroje napájení. Činnost záložních generátorů musí být ohlášena v DPPC [4].

4.2.5 PC klient

Pomocí tohoto klienta je možné se připojit do databáze DPPC.

II. PRAKTICKÁ ČÁST

5 VÝROBCI DPPC NA ČESKÉM TRHU

Na českém trhu působí řada společností zabývajících se dodáváním či výrobou DPPC, které v rámci DPPC nabízejí různé služby. Každá bezpečnostní agentura nebo společnost uvažující o zřízení takového DPPC určitě najde vhodného dodavatele. Autorka oslovila několik firem,[7] které poskytují služby v rámci PKB a provozují služby spojené s DPPC. Mezi hlavní aktéry na trhu označily tyto společnosti NAM System, a. s., RADOM, s. r. o., JABLOTRON, s. r. o., Trade FIDES, a. s. Autorka má osobní zkušenost s DPPC dodaným společností NAM System, a. s. Na základě tohoto výběru budou výše zmíněné společnosti v následujících podkapitolách stručně představeny a bude popsána technologie jejich výrobků.

5.1 RADOM, s. r. o.

Hlavní oblasti činnosti této společnosti spočívají v zabezpečení a střežení objektů, signalizačních systémech přivolání pomoci, lokalizaci vozidel a osob na bázi GPS, systémech pro kolejovou dopravu, telemetrických systémech, úpravě společných televizních antén (STA) pro digitální TV vysílání. Pro tyto oblasti zajišťují vývoj hardwaru a softwaru, projekci, výrobu, montáž, dodávky, servis a technickou podporu [5].

Společnost je členem sdružení AGA (Asociace technických bezpečnostních služeb Grémium Alarm – 1991, oficiální založení 6. 5. 1992), členem Českého klubu bezpečnostních služeb (dále ČKBS), Cechu EPS (vznikl 25. 2. 1993), Hospodářské komory České republiky (dále HK ČR) [5].

5.1.1 Technologie výrobků společnosti

K výrobkům v oblasti zabezpečení a střežení objektů této společnosti patří DPPC RADOM SECURITY A RADOM SECURITY FIRE (EPS), oba tyto typy DPPC jsou tvořeny, jak bylo popsáno v teoretické části, třemi základními celky (dispečerské pracoviště, přenosové trasy, objektová přenosová zařízení). Společnost nabízí tyto druhy DPPC:

[7] Telefonicky bylo osloveno několik bezpečnostních agentur ve Zlínském kraji, jako například Bezpečnostní agentura ASTREMA, spol. s r.o. (Ing. Zbyněk Štěrba), nebo společnost System plus Zlín, s.r.o. (Ing. David Polášek). Shodli se na výše uvedených hlavních aktérech.

- *dispečerské pracoviště DPPC* – zajišťuje centrální dohled nad střeženými objekty a vyhodnocování jejich stavů, je tvořeno zařízeními pro příjem zpráv ze střežených objektů a počítačovou sestavou s uživatelským softwarem (pro zobrazení, vyhodnocování a archivaci zpráv ze střežených objektů RADOMNET II, software DPPC, který je díky rádiovým přijímačům SRX10/400 a GSM přijímačům SRX10G nebo telefonní kartě GS51 a TF98 schopný přijímat zprávy ze střežených objektů), co se týče softwaru DPPC, společnost nabízí WRS32, RADOMNET a RADOMNET II;
- *přenosová trasa* – určena k přenosu dat mezi DPPC a střeženými objekty (retranslační stanice SRE40);
- *objektová přenosová zařízení* – slouží ke sběru informací z PZTS a EPS (např. alarm při narušení objektu, informace o technickém stavu zařízení) s následným přenosem na dispečerské pracoviště DPPC (rádiové vysílače STX20, STX23/400, STX23A, STX23A/F, GSM komunikátory SXS23, SXS24, SXS25, SXS26, SXS26 SE, SXS30 a internetový komunikátor INET; zabezpečovací ústředny TAR, TAR mini, TAR mikro, SXS26 SE, PITBUL II) [6].

5.1.2 Nabídka DPPC

Společnost nabízí DPPC jak pro bezpečnostní agentury, tak pro další subjekty formou komplexní služby, počínaje objektovými přenosovými zařízeními přes technologická vybavení přenosových tras až po modulární řešení dispečerských pracovišť [6].

5.2 Trade FIDES, a. s.

Společnost je na trhu od roku 1995. Její hlavní podnikatelský záměr již od počátku spočíval v poskytování služeb v oblasti bezpečnostních systémů pro ochranu osob a majetku. Realizovala zabezpečení v takových objektech, jakými je např. soubor budov Státního hradu a zámku Český Krumlov (zapsán na Seznam světového kulturního dědictví UNESCO), administrativní budova centrály České spořitelny nebo zastupitelský úřad v Moskvě. Specifickou činností této společnosti je řešení bezpečnostních systémů pro Armádu České republiky, Policii České republiky a orgány státní a veřejné správy. Tato společnost má prověrku pro práci s utajovanými skutečnostmi do stupně „TAJNÉ“. Je

členem Asociace technických bezpečnostních služeb Gremium Alarm, Cechu EPS, pracovní komise Sdružení pro jakost Czech Made a certifikační komise PZTS [7].

Počátky historie monitorovacích systémů společnosti FIDES (později přejmenované na Trade FIDES, a. s.) spadají do roku 1992, kdy vyvinuli a uvedli do provozu první DPPC s názvem FAUTOR. Toto DPPC se stalo záhy základním stavebním kamenem systému dálkového dohledu objektů střežených Policií České republiky. V roce 1999 uvedla společnost na trh novou generaci DPPC, která byla postavená na platformě operačního systému Microsoft Windows s dnes známějším názvem LATIS® [7].

Poté společnost začala dodávat služby v oblasti DPPC se systémem LATIS® SQL (předchůdcem byl právě výše zmiňovaný LATIS®), který se pyšní podrobnou grafickou nástavbou a instrukcemi k danému objektu, umožňuje přesný a rychlý zákrok při pomoci střeženému objektu. Dále je v tomto systému možné vkládání fotografií, půdorysů objektů, komunikačních tras a veškerých technických událostí, které jsou v dnešní době již nezbytností [7].

5.2.1 Technologie výrobků společnosti

Integrační a monitorovací systém LATIS® SQL společnost vyvinula na základě předchůdce tohoto systému, kterým byl LATIS®. Produkt LATIS® SQL převzal od svého předchůdce veškeré důležité vlastnosti, které byly osvědčené. Tento systém umožňuje integraci a monitoring všech technologií, kterými jsou např. PZTS, EPS, ACS, systémy MaR (ventilace, klimatizace, výtahy atd.), CCTV a další. Právě díky řídícímu systému LATIS® SQL jsou tyto systémy propojeny prostřednictvím jejich komunikačních kanálů a jsou integrovány do jednoho celku. Cílem této integrace je komfort uživatele, který spočívá v efektivní správě z jednoho pracoviště, na kterém jsou všechna data a informace přístupné v jednotné a uživateli srozumitelné podobě. Tento systém LATIS® SQL lze sestavit a upravit dle přání uživatele a je možné jej využít jako lokální grafickou nadstavbu nebo jako dálkový dohled objektů (DPPC) s různými komunikačními kanály. Samozřejmě lze využít i kombinaci těchto variant [8].

Společnost k monitorovacímu a integračnímu systému vyrábí a dodává objektové stanice, u nichž je k dispozici široký sortiment přenosových kanálů, kterými jsou např. pevná telefonní linka, sítě GSM SMS, GSM GPRS, několik variant rádiových sítí a kanály RS323/422/485 až po síť LAN/WAN. Díky tomu, že jde o produkt, který společnost sama

vyvíjí, není dle vyjádření společnosti žádný problém jeho doplnění o nové funkce dle jakýchkoliv požadavků zákazníka [8].

5.2.2 Síť LATIS

Je tvořena objektovými stanicemi LATIS 2400 a LATIS 2400N na straně střežených objektů a rádiovým modemem LR 324 pro (hlavní) rádiovou komunikaci a telefonním modemem LT 300 pro záložní komunikaci na straně centrální stanice tohoto systému. Tato síť je sítí řízenou, to znamená, že provoz probíhá na principu „výzva-odpověď“ a je řízen centrální stanicí (DPPC). Samozřejmostí je oboustranná komunikace se všemi objekty. Tato síť komunikuje rychlostí 2400 Bd s kódovaným přenosem dat a může zpracovávat data z ústředen PZS a EPS, ale taktéž data technologického charakteru [8].

Síť LATIS	
počet objektových zařízení LATIS 2400	2 000
počet přenášených událostí z jednoho objektu	maximálně 65 535
typ komunikace	obousměrná, řízená centrální stanicí SCO
rychlost komunikace	2 400 Bd
přenos dat	kódovaný na všech úrovních
počet kanálů pro prioritní přenos	2
retranslace	kterákoliv objektová stanice může pracovat jako retranslátor
počet retranslátorů v sérii	15
celkový počet retranslátorů v síti	není omezen

Obr. č. 3. Charakteristika sítě LATIS. Zdroj: [8].

Objektové zařízení LATIS 2400 nebo LATIS 2400N může pracovat jako retranslační stanice, dále zde může pracovat až 15 objektových zařízení v řadě za sebou, tzn. 15 vrstev (pro vykrytí území velikosti okresu je obvykle potřeba pět retranslačních vrstev). Počet retranslátorů v jednotlivých vrstvách není omezen. Pokud nastane výpadek na jakémkoliv retranslátoru, je zde propracovaný režim automatického nalezení nové cesty spojení s DPPC střeženého objektu. V síti LATIS pracují všechna objektová zařízení na jedné frekvenci a každé objektové zařízení může být v této síti dálkově ovládáno a programováno přímo z centrální stanice. Tato síť pracuje ve třech základních režimech, kterými jsou:

1. předávání poplachových událostí (priorita č. 1) s typickou dobou přenosu 3 s;
2. předávání nepoplachových (oběžníkových) událostí přednostně (priorita č. 2);
3. předávání nepoplachových (oběžníkových) událostí standardním způsobem [8].

Společnost Trade FIDES a. s. má na trhu zabezpečovací techniky velkou výhodu díky tomu, že je výhradním dodavatelem DPPC pro Policii České republiky, to znamená, že pokud chce být jakýkoliv objekt Policie České republiky připojen na DPPC, musí využít služeb společnosti Trade FIDES a. s. [8].

5.3 JABLOTRON, s. r. o.

Společnost JABLOTRON je na trhu od roku 1990 a patří k významným dodavatelům služeb v oblasti ochrany osobního majetku. Do hlavní nabídky alarmů této společnosti patří JABLOTRON 100, JABLOTRON 80 a AZOR. Pracovníci společnosti jsou schopni napojit na svoji Tísňovou linku (společnost takto nazvala své DPPC) jakýkoliv alarm [9].

Společnost Tísňovou linku spustila v listopadu roku 2011. Jedná se o bezpečnostní centrum, které střeží více jak 16 000 objektů a je k dispozici 24 h denně 365 dní v roce. Tísňová linka vznikla díky investici do nákupu služeb pultu centrální ochrany společností SV-Agency a Jablosec (dříve divize ADT Security Center společnosti Tyco International), z nichž fúzí vznikla společnost JABLOTRON SECURITY [10].

5.3.1 Technologie výrobků společnosti

Společnost na trh uvedla následující produkty:

- JABLOTRON 100 je revoluční bezdrátový systém určený k ochraně objektů, který je vhodný jak pro obytné prostory, tak i pro obchody, sklady, kanceláře, dílny apod. Je schopen hlásit tyto akce: vloupání, zdravotní obtíže, požár, přepadení a případně další rizika dle nabídky společnosti nebo přání zákazníka. Tento systém nabízí i domovní automatizaci (ovládání spotřebičů na dálku, řízení topení, řízení klimatizace, zapínání spotřebičů detektorem pohybu, detektorem otevření nebo dálkovým ovladačem) [11].

- JA-80 je prověřený bezdrátový systém, který se hodí k ochraně objektů od obytných prostor, obchodů, kanceláří, skladů až po dílny apod. Může hlásit vloupání, požár, zdravotní obtíže, přepadení a případně další rizika [12].
- Azor je jednoduchý bezdrátový alarm s intuitivním ovládáním, ideální pro byty, chaty, garáže, kanceláře a malé obchody [13].

5.3.2 Nová prodejní taktika společnosti

Společnost JABLOTRON, s. r. o. v současnosti využívá novou prodejní taktiku. Nabízené služby (výrobky) ve většině případů realizuje pomocí svých SIM karet, zákazníkům nabízí možnost bezplatného monitorování na DPPC po dobu tří měsíců. Po uplynutí této doby se zákazník rozhodne, zda chce být dále monitorován na DPPC, nebo si po dodání vlastní SIM karty řeší monitorování prostřednictvím SMS zasílaných do mobilního telefonu [39].

5.4 NAM System, a. s.

Posledním velkým dodavatelem na českém trhu je společnost NAM System, a. s.

5.4.1 Historie společnosti

Společnost vznikla v roce 1991 a je významným dodavatelem DPPC v České republice i na Slovensku. Dále se tato společnost významným způsobem zabývá rádiovým přenosem dat v nejrůznějších aplikacích, jakými jsou např. teplárenství, vodárenství, plynárenství nebo měřící a regulační technika. V současnosti se intenzivně věnuje systémům pro monitorování polohy mobilních objektů [14].

Společnost již prodala více než 300 DPPC na trzích v České a Slovenské republice, Rusku, Maďarsku a na Ukrajině. Za kvalitu a vysokou technickou inovaci svých výrobků byla společnost několikrát oceněna na odborných výstavách a veletrzích, jichž se pravidelně účastní (Zlatý Ampér, Safety, Křišťálová koule VZT, čestné uznání Pragoalarm).

5.4.2 Kvalita nabízených služeb společnosti NAM system, a.s.

Samozřejmostí je pečlivé ověřování, testování a certifikace veškerých produktů společnosti dle příslušných norem a homologací. Společnost NAM system, a. s. byla v roce 2000 vytvořena z firmy NAM-Tomčala, která působila na trhu od roku 1990 [14].

K hlavním uživatelům systémů NAM patří:

- bezpečnostní agentury;
- městské policie;
- hasičské záchranné sbory;
- velké průmyslové podniky;
- teplárenské podniky;
- taxislužby;
- komunální podniky [14].

Kolem roku 2010 se oddělila jedna větev společnosti NAM System a začala vyvíjet vlastní produkty, což vedlo ke konkurenčnímu boji. Konkurence ale měla za následek zkvalitnění nabízených služeb a snížení cen na trhu, z čehož v konečném důsledku těžil zejména koncový zákazník. Společnost se v r. 2012 přestěhovala do nově zrekonstruovaných prostor. Společnosti NAM system, a.s. se bude autorka dále blíže věnovat v následující kapitole.

6 SPOLEČNOST NAM SYSTEM, A. S. A JEJÍ TECHNOLOGIE

Díky praxi ve společnosti využívající služeb tohoto významného dodavatele je společnost NAM System, a. s. autorčiným favoritem mezi společnostmi dodávajícími DPPC. Důvodů pro výběr této společnosti k bližšímu popisu jejich technologie je několik. Jedním je její politika vnějších vztahů se zákazníky (v případě jakýchkoliv dotazů se autorka vždy setkala s příjemným způsobem komunikace), druhým její dlouholetá praxe v tomto oboru a v neposlední řadě její komplexní řešení služeb v rámci DPPC.

6.1 Popis technologie společnosti

První DPPC, které tato společnost uvedla na trh, bylo zařízení s typovým označením NAM RP 1000, které pracovalo v režimu DOS. Avšak díky rychle rostoucímu počtu nově vznikajících bezpečnostních agentur vznikl i radiotelefonní DPPC NAM System 2000, který se prodává od roku 1995 až dosud. Základní konfigurací tohoto DPPC je vyhodnocovací jednotka se zobrazovacím tablem. Jako nadstavbu zde lze využít software PCO 2000 (nebo i jeho předchůdce TW PCO), který již pracuje v rámci operačního systému Windows. V roce 1999 společnost uvedla na trh DPPC NAM Global se zcela novým pojetím a odlišnou buňkovou koncepcí rádiové sítě. Základem tohoto systému je:

- monitorovací software NET-G;
- rádiová síť Global a Global 2 v pásmu 420-470 MHz;
- telefonní karta TF 98P;
- GPRS část Global;
- NET-CAR Local – systém sledování polohy zásahových vozidel [14].

Společnost dodává DPPC, na která lze připojit střežené objekty všemi dostupnými trasami, mezi které patří např. telefonní linka, rádiový signál, GPRS, IP com, SMS kanál aj. [14].

6.1.1 Dispečerské pracoviště – software NET-G

Tento monitorovací software vznikl díky narůstající potřebě zpracovávat data z DPPC rychle a bezpečně, využívat provoz dispečinků a skloubit dohromady střežení objektů ve městě se střežením a monitorováním poloh zásahových vozidel nebo technologických stavů [30].

Software NET-G je založen na databázi Interbase SQL, která umožňuje kdykoliv za plného provozu provést zálohování, vytvářet aktivní kopie databáze na jiný disk a mít vzdálený přístup k systému přes modem, díky čemuž může správce systému pracovat s tímto softwarem při napojování objektu u zákazníka. Rovněž majitel zabezpečeného objektu může díky službě MojePCO nahlížet do zpráv přijatých DPPC ze svého počítače [30].

Tento software je složen z několika modulů, některé jsou již součástí základní instalace, jiné je možné zakoupit zvlášť. Kterýkoliv z těchto modulů lze kdykoliv doinstalovat, a rozšířit tak možnosti celého tohoto systému [19]. Autorka dále uvádí výčet některých modulů:

- modul AppPCO – dispečerský modul monitorovacího SW NET-G (aktuální verze 1.22) pro prohlížení a správu událostí;
- modul AppDriver – zabezpečuje komunikaci s hardwarovými přijímači a počítačem, jinými slovy slouží k zajištění příjmu zpráv z přenosových cest (např. rádio, telefonní karta) a jejich zápisu do databáze (aktuální verze 1.16);
- modul AppMAIL – určený k hromadnému zpracování výpisů, umožňuje automatické zasílání e-mailových zpráv, např. pravidelné výpisy z DPPC (aktuální verze 1.1);
- modul AppServis – zpracovává data pro podpůrné služby (např. ServisSMS);
- NET-G Print Service – zajišťuje tisk dat či výpisů z DPPC;
- NET-G Servis SMS – umožňuje odeslat událost z DPPC jako krátkou textovou zprávu nebo zaslat SMS na dispečerem určené telefonní číslo;
- NET-G Sound Service – slouží ke zvukové prezentaci událostí z DPPC (při obdržení poplachové zprávy DPPC přehraje audio zprávu „poplach“ nebo jakoukoliv jinou dle potřeb dispečera);
- NET-G Servis COM – je server zpracovávající události NET-G a provádějící odesílání těchto událostí formou volitelných paketů přes sériové rozhraní počítače dle konfigurací příslušných spustitelných objektů a jejich vlastností;
- NET-G Statistika – tento modul vyvinula společnost NAM System, a. s. pro statistické zpracování položek v databázi událostí NET-G; umožňuje definovat

a používat SQL dotazy pro výběry dat, tyto odesílat do programu MS Excel a automaticky z nich tvořit grafy, z událostí vhodných pro statistické zpracování lze jmenovat např. kvalitu signálu objektů, výpadky spojení, poplachové události, kvalitu pozadí atd. [19].

SW NET-G je velmi přehledný uživatelský software, který díky svému jednoduchému a intuitivnímu ovládání představuje pro dispečery vhodný pracovní nástroj. Samozřejmostí je u něj možnost přizpůsobit si vzhled dle představ dispečerů (např. zobrazení příchozích zpráv, velikost panelů). Software NET-G umožňuje obrazovku počítače rozdělit na dva panely oken události, kde horní panel slouží k přijímání hlavních zpráv (klávesa F3) ze střežených objektů (poplach, tíseň, objekt nekomunikuje, výpadek elektrické energie, porucha baterie atd.), prostřednictvím dolního panelu okna událostí (klávesa F2) je možné přijímat hlavní i pomocné zprávy (kódování ve střeženém objektu, obnovení komunikace, obnovení baterie aj.). Jinými slovy horní panel slouží k upozorňování na významné události, dolní panel zobrazuje pomocné události. Délku těchto panelů si dispečer může nastavit dle svých potřeb. Tím dosáhne např. toho, že v panelu významných událostí se zobrazí více zpráv než v panelu méně významných.

Co se týká významných událostí, tento software umožňuje barevné odlišení příchozích zpráv, které napomáhá k jejich efektivnímu rozlišování podle důležitosti. Podle potřeby dispečera je pak možné barevně specifikovat příchozí zprávy do DPPC, např. takto:

- *Červená barva* – může signalizovat velmi významnou událost, jakou je např. poplach, tíseň, tamper (sabotáž), požár, otevření ústředny a jiné důležité události, na které musí dispečer neprodleně reagovat. Tyto zprávy aktivují i akustickou signalizaci (sirénu) a dispečer musí přijetí této zprávy potvrdit klávesou F9. Po jejím stisku tato akustická signalizace ustane a čas potvrzení se zaznamená do karty objektu, odkud přišla tato významná událost.
- *Černá barva* – také může označovat významnou událost, například když PZTS nekomunikuje, není spojení s objektem nebo když je vysílač v objektu resetován. Na tyto zprávy musí dispečer reagovat, avšak na splnění a vyřešení události má jistý časový limit.

- Modrá barva – může vyjadřovat výpadek elektrické energie, poruchu baterie a jiné technické události, které indikují, že ve střeženém objektu došlo k mimořádné události z technického hlediska.
- Fialová barva – může sloužit k označení události typu sekce neuzavřena, porucha expandéru, objekt nekomunikuje.

Software umožňuje nastavení barev dle potřeb uživatele, avšak výše uvedené barevné označení se autorce této práce v praxi potvrdilo jako vhodné. Jakákoliv zpráva, která dojde do horního panelu (důležité události), aktivuje akustickou signalizaci a dispečer ji musí odbavit, jinak se akustická signalizace nevypne.

Po odbavení příchozí události má dispečer pro snažší rozhodování, jak s příchozí zprávou naložit, možnost najet pomocí klávesy F7 do karty objektu, kde jsou uvedeny veškeré informace o tomto střeženém objektu. Jedná se např. o informace tohoto typu [40]:

- *Kontaktní osoby* – tyto osoby jsou informovány o případných mimořádných událostech ve střeženém objektu (např. narušení objektu nebo ztráta komunikace s tímto objektem). Optimální situací je, když je kontaktních osob uvedeno hned několik. Pokud by nastala situace, kdy by se např. první kontaktní osobě nebylo možné dovolat, měl by dispečer možnost kontaktovat další z uvedených osob.
- *Hlídaný objekt* – v této sekci jsou uvedeny veškeré informace potřebné pro zásah v tomto objektu, jako je název objektu, telefonní spojení do objektu, číslo objektu, jeho adresa, pokyny pro operátora, zásahová jednotka, dohledová vzdálenost objektu MKDS (městský kamerový dohledový systém). K dispozici mohou být i doplňující údaje, např. servisní služba, datum napojení objektu, specifikace sběrné stanice, v níž je objekt umístěn, výrobní číslo vysílače, číslo smlouvy, poplachový plán objektu, který slouží pro upřesnění případného zásahu v tomto objektu. Může být uvedena i délka času příjezdu ke střeženému objektu, pokyny pro hlídku (např. pozor, v objektu je pes), informace o tom, zda je v objektu nainstalována tíseň, požární signalizace, speciální dohody (vyčkání do příjezdu majitele k objektu), klíče od střeženého objektu (branka, vrata) atd.
- *Stav objektu* – může se jednat o informace specifikující technické parametry týkající se objektu, např. stav baterie, stav sítě, stav komunikace. Informace umožňují

rychlejší orientaci dispečera při řešení technických problémů s tímto objektem. Ten zde vidí i seznam smyček a počet hlídaných sekcí na tomto objektu.

- *Technický stav objektu* – takové informace slouží k okamžitému zjištění stavu komunikace vč. zaznamenání data a času.
- *Mapa příjezdu k objektu* – specifikuje příjezdovou trasu ke střeženému objektu.
- *Fotografie objektu* – aktuální snímek střeženého objektu, vč. zakreslení hlídaných prostor.
- *Plán objektu* – půdorys střeženého objektu se zakreslenými prvky elektrické ochrany, vč. popisu přístupových cest do střeženého objektu.
- *Zprávy za aktuální měsíc* – opět informace, které dispečerovi usnadňují práci při hledání informací o objektu. Jedná se o veškeré příchozí zprávy z objektu v daném měsíci, jako jsou např. periodické testy přenosu, zapnutí/vypnutí systému, specifikace kódu, který zapnul, či vypnul systém, a času, v němž k tomu došlo, poplachy, technické zprávy (výpadek sítě, baterie, komunikace). Taktéž se sem zaznamenávají zprávy, které řešil dispečer.
- *Zprávy od-do* – díky těmto zprávám je dispečer schopen zjistit jakékoliv informace z objektu dle zadaných parametrů, např. co se dělo před dvěma či třemi měsíci a jak bylo v rámci této situace postupováno.
- *Servis a revize* – tato sekce je oddělena od ostatních, protože zahrnuje upřesňující údaje o střeženém objektu v rámci technických specifikací. Může zde být uveden typ ústředny, typ komunikace (rádio, linka), číslo telefonu připojeného k PZTS, sirény (venkovní, vnitřní), správce PZTS v objektu, telefonní spojení na správce PZTS, další zařízení ve střeženém objektu (CCTV, DT, KVS) atd.

Podle autorky je výše zmíněný výčet informací dostačující k tomu, aby dispečer správně rozhodnul o dalším postupu. Software NET-G dále umožňuje přednastavení zpráv, které jsou dispečery nejčastěji používány, a po stisknutí klávesy F11 se dispečerovi zobrazí tabulka, z níž jen vybere událost, která je pro danou situaci nejvhodnější. Po jejím potvrzení se tato událost zapíše do karty střeženého objektu („zprávy za aktuální měsíc“ a taktéž „zprávy od-do“, pokud by se chtěl někdo v pozdějším období na tuto zprávu podívat).

V praxi to funguje tak, že po obdržení zprávy (např. výpadek sítě) dispečer najede do karty objektu, podívá se, zda nejsou k dispozici nějaké podrobnější informace o této události. Pokud nejsou, ihned klikne na první kontaktní osobu a telefonicky ji o této situaci vyrozumí. Jakmile tak učiní, pomocí klávesy F11 vybere zprávu „vyrozuměn majitel“ a potvrdí ji. Tím zanese do systému informaci o tom, co udělal pro vyřešení dané situace. Pokud by vyvstaly jakékoliv otázky ohledně způsobu řešení dané události, je z této historie patrné, pro jaké řešení se dispečer rozhodl.

Do přednastavených zpráv lze zařadit jakoukoliv zprávu, která je k řešení dané situace vhodná. Pod klávesou F11 se mohou objevit např. tyto přednastavené zprávy: přivolána hlídka bezpečnostní agentury, vyrozuměn majitel, provedena fyzická kontrola objektu, objekt bez narušení, objektu narušen, zahájen servis, zahájena pravidelná revize, přivolán technik, majitel nezastižen, přivolána hlídka Policie České republiky, odvolání zásahové jednotky, planý poplach – ověřeno telefonicky, technická závada PZTS, testování systému, ukončení servisního zásahu, ukončení pravidelné revize. Klávesa F12 umožňuje smazání již vyřešené akce, tím se zpráva z horního panelu odstraní [40].

6.1.2 Přenosové trasy – sběrná stanice RSN 451

Jedná se o inteligentní převaděč, který přijímá všechny zprávy z jemu přidělených objektových vysílačů, ale dále směrem na dispečink DPPC posílá pouze významné zprávy (poplach, výpadek elektrické energie, porucha baterie, sabotáž, požár atd.) z objektů, z jiných sběrných stanic a vlastní diagnostické zprávy. Dále kontroluje spojení s objekty, které má k tomu předdefinované. Na sběrné stanici RSN 451 je také možné nastavit čtyři časové limity pro kontrolu spojení podle důležitosti objektu a časového intervalu vysílání nastaveného na vysílači. Při výpadku spojení vygeneruje sběrná stanice zprávu „výpadek spojení“ a odešle ji na DPPC [15].

Obsahuje dva napěťové vstupy (24hodinové poplachové smyčky), respektive výstupy (relé) pro připojení externích zařízení. Tato sběrná stanice jako objektové zařízení může fungovat rovněž jako zabezpečovací ústředna AMOS 1600. Umožňuje skenovat objekty v okolí a zjišťovat kvalitu spojení s objekty, které nepřevádí, dále taktéž umožňuje konfigurovat rádiovou cestou všechny sběrné stanice v síti [15].

Obsahuje vyrovnávací paměť, do které se ukládají zprávy pro případ, že je použita jako sběrný modem DPPC. Kapacita vyrovnávací paměti je 6000 zpráv včetně času vzniku [15].

6.1.3 Objektová přenosová zařízení – TSM, komunikátory REGGAE

Rádiový vysílač TSM 452 a TSM 454 přenáší data v pásmu 420-470 Mhz. Jedná se o objektové rádiové zařízení, které slouží k přenosu informací z ústředen PZTS nebo EPS na DPPC rádiovou cestou. Vysílač TSM 452 a TSM 454 může také fungovat jako zabezpečovací ústředna AMOS 1600. Mezi výhody vysílačů patří bezesporu bezpečnost, cena a rychlost přenosu [16]. Paralelní vstupy:

- osm vyvážených 24hodinových smyček;
- osm potenciálových smyček (rozepnuto 50 V až 3,5 V, neurčitý stav 3,5 V až 9 V, sepnuto 9 V až 50 V, odběr 1,5 mA při 15 V);
- možnost programové inverze vstupu;
- možnost programového vypnutí vstupu (není nutno zakončovat jej odporem);
- možnost napojení až osmi různých ústředen PZTS na všech šestnácti vstupech (pro každou ústřednu je jeden vstup rezervován pro poplach a druhý vstup na den/noc);
- softwarová filtrace rušení na vstupech [16].

Vysílače dále umožňují:

- výběr jedné ze čtyř přednastavených frekvencí;
- volbu periody vysílání kontrolních telegramů;
- akustickou signalizaci vysílání zpráv rádiem;
- volbu tichého vysílače [16].

6.1.4 Komunikátor REGGAE GRT

Jedná se o novou generaci komunikátorů (vysílačů), které nahrazují starší modely TSMxxx. Jsou to zařízení umožňující příjem zpráv a událostí ze zabezpečovacích ústředen PZTS, EPS a jejich následný přenos různými kanály na DPPC. K příjmu zpráv z ústředen PZTS dochází přes telefonní linku, jedná se o sériovou linku prostřednictvím EPS převodníků třetích stran. Příjem událostí je zajištěn izolovanými vstupy. Zprávy a události jsou na DPPC přenášené kanálem rádia (RF 400), anebo kanálem GPRS, případně pomocí SMS (kanálem GSM). REGGAE GRT dokáže komunikovat s ústřednami PZTS ve všech

běžných pulzních a DTMF formátech. Tyto komunikátory jsou schopny zjistit poruchu na veřejné telekomunikační síti, odpojit tuto síť, nadále přijímat zprávy z PZTS a přenášet je na DPPC kanálem GPRS. Konfiguraci a diagnostiku provozních a poruchových stavů těchto komunikátorů je možné provádět jak vzdáleně kanálem GPRS, tak lokálně přes sériovou linku. Komunikace těchto zařízení s DPPC probíhá obousměrně přes GPRS s potvrzováním příjmu zpráv z DPPC, nebo jednosměrně přes kanál RF 400 bez potvrzování. Spojení mezi komunikátory a DPPC je při přenosu zpráv oběma výše zmíněnými kanály pravidelně kontrolováno, v případě výpadku komunikace je tato situace okamžitě hlášena na DPPC zprávou „objekt nekomunikuje“ [23].

6.1.5 Komunikátor REGGAE GLT

I tento typ komunikátoru umožňuje příjem zpráv a událostí jak z ústředen PZTS, tak z ústředen EPS a jejich následný přenos různými kanály na DPPC. Zprávy jsou přijímány přes telefonní nebo sériovou linku, příjem událostí je opět zajištěn izolovanými vstupy. Zprávy a události jsou na DPPC přenášeny počítačovou sítí (LAN - lokální síť; WAN - internet), datovým kanálem GPRS nebo pomocí SMS (kanálem GSM). REGGAE GLT je komunikuje s ústřednami PZTS ve všech běžných pulzních a DTMF formátech. Příjem vytáčení telefonního čísla z PZTS může být pulzní i DTMF. Tento komunikátor je schopen zjistit poruchu na veřejné telekomunikační síti, odpojit tuto síť a dále přijímat zprávy z PZTS a přenášet je na DPPC kanály LAN/WAN a GSM/GPRS. Konfiguraci komunikátoru a diagnostiku jeho provozních a poruchových stavů je možné provádět vzdáleně kanály LAN/WAN a GPRS, nebo lokálně přes sériovou linku. Komunikace těchto vysílačů s DPPC probíhá obousměrně s potvrzováním příjmu zpráv z DPPC. Spojení mezi komunikátory a DPPC je při přenosu zpráv kanály LAN/WAN a GPRS pravidelně kontrolováno. Následný výpadek komunikace je na DPPC zaznamenán vyhlášením zprávy „objekt nekomunikuje“ [23].

Za významné změny komunikátorů REGGAE oproti vysílačům TSMxxx lze podle názoru autorky označit:

- REGGAE má osm napěťových vstupů (vysílače TSM mají osm napěťových plus osm vyvážených).
- REGGAE neumí fungovat jako zabezpečovací ústředna.

- REGGAE obsahuje i GPRS modem, u tohoto vysílače je tedy možnost využít i GPRS záložní trasu. V praxi tedy mohou být data přenesena jednak přes rádiovou síť, jednak přes síť GPRS (technologické centrum). GPRS modem může sloužit též pro servisní účely (nastavení konfigurace vysílače, nebo pro dočasné zapnutí záložní trasy).

6.1.6 Rádiová síť GLOBAL

Tato síť slouží k přenosu dat z objektů vybavených PZTS, PZS nebo EPS a k přenosu dat o poloze vozidel. Pracuje v pásmu 420-470 MHz a je svou strukturou podobná buňkové síti používané pro provoz mobilních telefonů. Na jedné frekvenci může být až 63 buněk a centrem každé buňky je sběrná stanice (RSN 451) [17].

V rádiové síti Global může být až 1000 rádiových objektů včetně 63 sběrných stanic. Sběrné stanice je možno řadit za sebe, přičemž maximální počet je šest stanic seřazených za sebou. Tím se zvětšuje jak dosah rádiové sítě, tak i počet hlídaných objektů. Na jednu sběrnou stanici je možné připojit až 256 objektů, tzn. teoretickou možnost napojení až 16128 (63*256 = 16128) objektů a 63 sběrných stanic na jednu síť. K dosažení maximální kapacity rádiové sítě Global je nutné optimálně nastavovat výkony vysílačů, časy vysílání a časy kontroly spojení. Při nastavení optimálního výkonu lze bez vzájemného rušení docílit souběžné komunikace vysílačů v sousedních buňkách na jedné frekvenci. Pomůckou při nastavování výkonu vysílače je měřící stanice MRS 452, která ukazuje kvalitu spojení se sběrnými stanicemi [17].

Rádiová síť Global kombinuje výhody jednosměrných a obousměrných rádiových DPPC. Provoz mezi objektovými vysílači a sběrnými stanicemi je jednosměrný, provoz mezi sběrnými stanicemi, sběrnou stanicí DPPC a mobilními objekty je obousměrný. Za výhodu jednosměrného provozu lze považovat nízkou cenu objektového vysílače. Obousměrný provoz umožňuje po páteřní síti přenášet efektivně větší datové toky, ovládat činnost sběrných stanic na dálku a pomocí relé výstupů, např. zapínat světlo nebo otevírat klíčový trezor [17].

Bezpečnostní prvky sítě Global jsou navrženy tak, že maximálně ztěžují úmyslnou odbornou sabotáž systému. Dále má síť tyto přednosti:

- vysoce zabezpečené rádiové telegramy;
- identifikace provozu druhého stejně nadefinovaného ilegálního vysílače;
- neustálá kontrola spojení rádiového objektu s některou ze sběrných stanic, doba kontroly spojení je nastavitelná, a to již od dvou minut;
- nepřetržitá kontrola spojení sběrných stanic se sběrnou stanicí DPPC;
- pokud jsou mezi sběrnými vysílači vybudovány kvalitní směrové spoje s vysokou intenzitou signálu, je celá síť odolnější vůči rušení;
- měření úrovně šumu pozadí na všech sběrných stanicích;
- při použití ústředny AMOS 1600 je výhodou rychlost přenosu informace od čidla až na dispečink DPPC;
- frekvence vysílačů a sběrných stanic jsou předdefinovány u výrobce [17].

6.1.7 Rádiová síť GLOBAL 2

Pokud nastane situace, že má provozovatel DPPC v síti větší počet vysílačů (více než 1000), je potřeba přejít na systém Global 2. Rádiová síť Global 2 je nástupcem, nadstavbou, rozšířením rádiové sítě Global. Rádiovou cestou umožňuje přenášet různé druhy dat jako např.:

- data z objektů s PZTS, PZS;
- data z objektů s EPS;
- data o poloze, stavu a rychlosti mobilních objektů
- data z měřících, regulačních a dalších technologických zařízení [18].

Rádiová síť Global 2 je několikafrekvenční sítí využívající jak výhod jednosměrného, tak obousměrného rádiového přenosu. Data z rádiových objektových zařízení jsou na jedné frekvenci (např. pod označením f1) přenášena do páteřní sítě sběrných stanic RSN 451, přenos v páteřní síti pak probíhá na frekvenci druhé (např. pod označením f2). Díky rozdělení přenosu dat na více frekvencí tak je kapacita rádiové sítě Global 2 oproti původní síti Global několikrát větší. V síti Global 2 může fungovat na dvou frekvencích až 4000 rádiových objektových zařízení či sběrných stanic [18].

Komunikace mezi sběrnými stanicemi je obousměrná, mezi objektovými zařízeními a sběrnými stanicemi jednosměrná. Obousměrný provoz umožňuje po páteřní síti přenášet efektivně velké datové toky, konfigurovat a ovládat činnost sběrných stanic na dálku. Velkou výhodou jednosměrného provozu je nízká cena objektového zařízení, velká kapacita sítě a odolnost vůči místnímu rušení [18].

Velkou výhodou této sítě je, že data ze střežených objektů lze přenášet současně na několik dispečerských pracovišť. Umožňuje směrovat zprávy z objektů na příslušný dispečink a tím, že může ve sběrné stanici RSN 451 fungovat více rádiomodemů, také propojit dvě nebo i více sítí Global nebo Global 2. Díky tomu je možné vyřešit i jinak složité situace. Příkladem může být střežený objekt, v němž došlo k problému a který se nachází v místě, kde dané DPPC nemá dostatečný signál sítě. Poskytovatel DPPC může připojit tento střežený objekt přes sousední rádiové spojení jiného provozovatele (spolupracující společnost) a pro přenos signálu z této lokality využít jeho rádiovou síť [18].

Síť Global 2 zahrnuje bezpečnostní prvek, díky němuž je síť schopna identifikovat provoz druhého stejně nadefinovaného ilegálního vysílače. S každým rádiovým objektem je neustále kontrolováno spojení, přičemž dobu kontroly lze nastavit již od dvou minut [18].

Rádiová síť Global 2 kombinuje stejně jako síť Global výhody jednosměrných a obousměrných DPPC. Provoz mezi objektovými vysílači a sběrnými stanicemi je jednosměrný, zatímco provoz mezi sběrnými stanicemi v páteřní síti je obousměrný s potvrzením. Za výhodu jednosměrného provozu lze považovat nízkou cenu objektového vysílače, velkou kapacitu sítě a odolnost vůči lokálnímu rušení. Obousměrný provoz umožňuje po páteřní síti přenášet efektivně větší datové toky, ovládat činnost sběrných stanic na dálku a pomocí relé výstupů např. zapínat světlo nebo otevírat klíčový trezor v objektu [18].

6.1.8 Rádiová síť NSG

Rádiová síť NSG slouží k přenosu zpráv z objektů, které jsou vybaveny GSM/GPRS vysílači, jedná se o GPRS část DPPC Global [20].

Tato vysoce zabezpečená síť v rámci sítí GSM mobilních operátorů je určená pro přenosy zpráv z podporovaných objektových zařízení (vysílačů GSM 1) na DPPC Global a taktéž pro přenosy zpráv ze sběrných stanic GPRS. Řídící jednotkou této sítě je GPRS centrum,

jehož hlavním úkolem je zabezpečení správného směrování zpráv mezi jednotlivými uzly sítě (vysílač GSM 1, sběrná stanice RSN 451 SMG1, sběrná stanice RSN 451 SM1 DMG1). V současnosti síť podporuje mobilního operátora Vodafone, avšak do budoucnosti plánuje společnost NAM system, a. s. podporu všech mobilních operátorů působících na českém trhu. Zákazník tedy bude mít možnost volby operátora, avšak bude to záviset i na tom, který z těchto operátorů bude mít v dané lokalitě kvalitnější signál, kde se bude instalovat vysílač GSM 1 nebo sběrná stanice RSN 451 SMG1, resp. RSN 451 SM1 DMG1 (schéma rádiové sítě NSG viz příloha č. 2) [20].

Síť NSG je možné využít pomocí níže uvedených služeb [20]:

- *NSG Agentura* – tuto službu společnost NAM System, a. s. poskytuje provozovatelům DPPC Global. Předmětem služby je zabezpečení komunikace mezi monitorovacím SW NET-G uživatele a GPRS centrem sítě NGS. V rámci této služby je provozovatelům DPPC zdarma zapůjčeno zařízení umožňující příjem zpráv z přidělených objektů a kontrolující spojení s přidělenými objekty.
- *NSG DataRSN* – služba poskytovaná provozovatelům DPPC Global. Předmětem služby je zabezpečení komunikace mezi sběrnou stanicí RSN 451 SMG1 a GPRS centrem sítě NSG. Zde si uživatel musí zakoupit sběrnou stanici RSN 451 SMG1, která umožňuje příjem zpráv z přidělených objektů a kontrolu spojení s přidělenými objekty, a dále si musí pořídit driver GPRS.
- NSG Stanice – jedná se opět o službu, která se poskytuje provozovatelům DPPC Global. Jejím předmětem je zabezpečení komunikace mezi GPRS centrem sítě NSG a sběrnou stanicí vybavenou GPRS a rádiovým modemem uživatele (RSN 452 SM1 DMG1). V rámci této služby společnost NAM System, a. s. provozovatelům DPPC zdarma zapůjčí zařízení umožňující příjem zpráv ze sběrných stanic RSN 451 SM1 DMG1 a kontrolu spojení s těmito sběrnými stanicemi.
- NSG Objekt – služba poskytovaná provozovatelům DPPC Global, zahrnuje zabezpečení komunikace mezi objekty koncových zákazníků uživatele (provozovatele DPPC Global) a GPRS centrem sítě NSG.

Mezi komponenty sítě NSG patří [20]:

- Sběrná stanice GPRS (RSN 451 SMG1) – je vybavena GPRS modemem, který umožňuje přijímat zprávy z objektových zařízení GSM1. Dále pak významové zprávy odesílá přes sériovou linku do monitorovacího SW NET-G.
- Sběrná stanice vybavená modemem GPRS a rádiovým sběrným modemem (RSN 451 SM1 DMG1) – jedná se o klasickou sběrnou stanici používanou v rádiové síti Global 2, avšak vybavenou sběrným modemem SM1 a datovým modemem DMG 1. Tato sběrná stanice hlídá rádiové objekty (vysílače TSM 452 a TSM 454). Datové zprávy z rádiových objektů a vlastní zprávy sběrné stanice jsou posílány po sériové lince do DMG1 datového modemu. Ten pak data dále posílá GPRS cestou na dispečink DPPC. Tyto zprávy jsou opět potvrzované.

Ve snaze o shrnutí[8] je možné zjednodušeně říct, že pokud chce být objekt střežen na DPPC, musí v něm být instalován poplachový zabezpečovací systém (PZS nebo PZTS, EPS), který zahrnuje ústřednu, detektory, hlásiče a ovládací prvky (ovládací panel). Pro zastřežení uživatel pomocí klávesnice uvede ústřednu do pohotovostního stavu, po provedení tohoto úkonu ústředna reaguje na podněty (poplachy, sabotáž atd.), které zaznamenají detektory nebo hlásiče. Detektor či hlásič tedy zašle informaci o poplachovém stavu ústředně a ta následně tento poplach vyhodnotí. V případě narušení ústředna tuto zprávu dále předá do komunikátoru (rádiový, telefonní, IP atd.), který tuto zprávu přenese na DPPC. Na straně DPPC je zpráva přijata (přes rádiový přijímač, přijímač NSG, telefonní kartu, IP com atd.) a dojde k jejímu předání do driveru. Driver zpracuje příchozí zprávu (zprávu může zahodit, předat dál atd.) a zapíše ji do databáze. Zde už přichází na řadu SW (NET-G), který nové zprávy v databázi vyhodnotí, přiřadí ke konkrétnímu objektu a zprávu zobrazí na dispečerském pracovišti.

V případě využití rádiových vysílačů (TSMxxx) probíhá komunikace tím způsobem, že ústředna předá zprávu rádiovému vysílači a z důvodu jednosměrné komunikace je pro vyšší zabezpečení přenosu zpráva vysílána opakovaně (např. desetkrát, dle vlastního nastavení každé bezpečnostní agentury). Sběrná stanice přijme tuto zprávu, ověří, zda k tomu tento

[8] V následujícím textu vychází autorka z vlastních zkušeností a znalostí práce na DPPC.

konkrétní vysílač má oprávnění (číslo vysílače je uloženo ve sběrné stanici). Pokud ano, je tato zpráva předána dále. Vzhledem k charakteristice sítí GLOBAL 2, v nichž se sběrné stanice za sebou mohou řetězit, je zpráva předávána dál dle zadané cesty až na přijímací stranu DPPC.

V případě využití vysílačů REGGAE GPRS/IP je zpráva z komunikátoru předána do technologického centra, které tyto zprávy zpracovává a odesílá je do přijímače NSG. Přenos zpráv do technického centra je závislý na typu REGGAE (GPRS, IP, popř. záložní kanál SMS). Z NSG jsou zprávy primárně přenášeny přes internet, záložní trasa je přes GPRS. Přijímač NSG zprávu předá driveru a postup je dále stejný, jako bylo popsáno výše.

Nutno doplnit, že k provozování DPPC je nezbytná síť, po které budou objekty komunikovat (Global, Global 2, NSG) a která bude sloužit pro přenos dat ze střežených objektů na DPPC.

6.1.9 Původní koncepce DPPC[9]

Původní koncepce DPPC od společnosti NAM system, a. s. je založena na architektuře desktop. To znamená, že jeden počítač zajišťuje funkci databázového serveru, zpracovávání těchto dat a zároveň je používán i jako dispečerské pracoviště. K tomuto počítači jsou připojeny i všechny periferie pro příjem signálu (telefonní karta, GSM modul, IP modul atd.). Vzhledem k využití jednoho počítače pro více funkcí spočívala výhoda tohoto řešení v nižší pořizovací ceně. V praxi se pro tyto účely používaly běžné počítače, které byly zálohovány pomocí UPS. Kontrola běhu všech důležitých systémových funkcí (funkce driveru) byla softwarově kontrolována pomocí aplikace Watch Dog. V případě výpadku driveru nebo aplikace AppPco (NET-G) byl dispečer upozorněn zvukovým signálem. Toto řešení však neumožňovalo zajistit chod celého počítače, pokud například došlo k ukončení nebo zamrznutí aplikace Watch Dog. Dispečer se o této situaci mohl dozvědět až se zpožděním, navíc nebyl monitorovaný samotný hardware. V případě kolapsu celého počítače bylo nutné obnovit zálohu včetně všech nastavení. Tato obnova je časově velmi náročná.

---

[9] V následujícím textu vychází autorka z vlastních zkušeností a znalostí práce na DPPC, kdy si odzkoušela činnost práce dispečera jak na původní koncepci DPPC, tak nyní pracuje na DPPC v koncepci 1BOX.

Tato koncepce umožňovala připojení více dalších klientských pracovišť. Provoz NET-G byl kontrolován pomocí hardwarového klíče, na kterém byly nahrány licence služeb, které si zákazník pořídil (byl zde omezen počet dispečerských pracovišť). Tato původní koncepce DPPC nesplňovala normy pro provoz DPPC ČSN EN 50518-3 [28].

V původní koncepci DPPC SW NET-G byly při obdržení jakékoliv události ze střeženého objektu (horní panel) tyto zprávy řazeny za sebe. Pokud tedy například z objektu 123 Rodinný dům Benedělová došla zpráva o výpadku sítě, zobrazila se na monitoru dispečera. Pokud z téhož objektu přišla další informace, opět se objevila jako nová událost. Dispečer tedy měl u téhož objektu v horním panelu zaznamenané již dvě akce, z nichž každou musel potvrdit (a následně odstranit) zvlášť. Naproti tomu u nové koncepce DPPC se tyto události již neřadí pod sebe, ale překrývají se. Pokud dojde k další události u téhož objektu, operátor je na to pouze upozorněn (zvukovou signalizací). Musí sice tuto událost potvrdit, ale již nemá na obrazovce dvě události, nýbrž pouze jednu. Pro dispečera DPPC je to obrovská výhoda.

6.1.10 1BOX – žhavá novinka v koncepci DPPC

Nová koncepce DPPC je již založena na architektuře server-klient. Toto řešení se prodává pod obchodní značkou 1Box RACK a splňuje novou normu pro provoz DPPC: ČSN EN 50518-3. Hlavní změna oproti předchozí generaci DPPC spočívá v tom, že je zde oddělena funkce dispečerského (klientského) pracoviště od funkce databázového serveru.

Technicky je tato koncepce řešena tak, že všechny součásti DPPC kromě klientského jsou umístěny v jednom racku. Využívá se zde funkce virtuálních serverů, na jednom fyzickém serverovém počítači tedy běží instance virtuálních serverů. Hlavní virtuální server běží na platformě Windows, zajišťuje provoz databázového serveru a jsou na něm založeny jak procesy driveru, tak další služby potřebné pro provoz DPPC. Druhý virtuální server zajišťuje hardwarový dohled nad funkcí hlavního virtuálního serveru, v případě jakéhokoliv selhání se informace přenáší na DPPC společnosti NAM system, a. s. a dále se zobrazuje na všech klientských pracovištích.

Třetí virtuální server je již volitelný a využívá se např. pro vzdálené připojení nebo pro provoz dalších služeb. V tomto případě je to software zpracovávající informace z IP komunikátorů HaSaM. Dále je v racku umístěn síťový disk, na který jsou ukládány zálohy systému (databáze, virtuální servery, nastavení atd.). V racku jsou dále umístěny všechny

přijímací prvky (přijímací strana rádiové sítě, telefonní karta, GSM modem atd.). Toto řešení má výhodu v tom, že pokud dojde k poruše serveru, velmi jednoduše se po výměně vadného hardwaru obnoví kompletní systém včetně dat do původního stavu před poruchou.

Do budoucna společnost NAM system, a. s. plánuje i nasazení druhého redundantního serveru, jehož funkce budou moct být při selhání hardwaru okamžitě nahrazeny záložními. Toto řešení umožňuje i vzdálený dohled technologického centra, při jakémkoliv výpadku či problému jsou zprávy přenášeny do technologického centra společnosti NAM system, a. s., a to dispečerskému pracovišti (či pracovištím) a formou SMS správcům DPPC. Všechna zařízení v racku jsou umístěna v lokální oddělené síti a jsou zálohovány UPS.

Bezpečnost je zde zvýšena i oddělením lokální LAN v racku a vnitropodnikové LAN. Licence k provozu SW NET-G je uložena v hardwarovém klíči. Standardně se v tomto řešení počítá s pěti licencemi pro připojení pěti dispečerských pracovišť. Dispečerské pracoviště musí mít nainstalovaný software NET-G stejně jako u předchozí generace DPPC. Připojuje se a data si stahuje z racku (virtuální databázový server). V současné době společnost NAM system, a. s. preferuje a dodává koncepci 1Box-rack a všechny nové služby jsou již podporovány pouze v rámci ní. Jak tato novinka vypadá (1Box), je vyobrazeno v příloze č. 3.

7 ČINNOST DISPEČERA NA DPPC

Autorka může z vlastní zkušenosti konstatovat, že činnost dispečera na DPPC je velmi náročná. Během služby se potýká s nejedním rozhodnutím, jak správně reagovat na danou událost či události. Musí se během okamžiku rozhodnout a své rozhodnutí poté obhájit. Jakýkoliv dispečer by měl mít všeobecné znalosti týkající se PZTS, CCTV, EPS, KVS atd., aby byl schopen zodpovědět veškeré dotazy majitele objektu. Vždy musí mít nadhled nad situací a vyřešit situaci vždy ke spokojenosti všech. Samozřejmostí je účast na periodickém školení, které by měla společnost provozující DPPC organizovat. V praxi činnost dispečera spočívá především ve vyřizování telefonátů, jejichž předmětem jsou dotazy či žádostí týkající se střežených objektů, či dotazy a prosby potencionálních zákazníků, kteří ještě nejsou na DPPC připojeni. Denně dispečer reaguje na množství rozmanitých otázek, které musí umět zodpovědět, či je předat kompetentním osobám. Na dispečink DPPC se může denně dovolat až 500 osob.

Činností dispečera je dále obsluha samotného DPPC a reakce na obdržené poplachové či technické zprávy. Dispečer se musí velmi rychle rozhodovat a řešit situace spojené s běžným chodem DPPC. Je v kontaktu s Hasičským záchranným sborem, Policií České republiky, ale také s jinými DPPC a samozřejmě se smluvními výjezdovými skupinami (dále jen SVS).

7.1 Optimalizace činnosti DPPC z technického hlediska

V původní koncepci DPPC pracují všechna tato centra tak, že po obdržení poplachové zprávy dispečer tuto zprávu převezme a zahájí úkony k vyřešení této situace. Pokud nastane situace, kdy na střežený objekt vyjíždí SVS, dispečer musí o této situaci toto DPPC informovat. Dispečer si zapíše čas oznámení poplachové zprávy, číslo objektu, z něhož přišla, adresu daného objektu a bližší určení místa, kde daný poplach vznikl (např. vstupní dveře, prostor kuchyně atd.). To vše zabere téměř tři minuty. Jak dispečer DPPC, na které poplachová zpráva došla, tak dispečer DPPC, které je o výjezd žádáno, musí být velmi obezřetní, aby nedošlo k nedorozumění či modifikaci jakékoliv informace, která je hlášena. V praxi může nastat situace, že dispečer při hlášení podrobností jinému dispečerovi DPPC SVS přeslechne např. číslo místnosti a při zásahu nejprve kontroluje jinou kancelář, zatím však ubíhá čas, který mohl být využit k dopadení pachatele. Z tohoto důvodu autorka práce

považuje nabídku společnosti NAM system, a. s., která uvedla na trh službu CONNECT, za obrovský pokrok v činnosti DPPC. V následující kapitole se bude autorka věnovat činnosti práce dispečera, její možné optimalizaci a identifikaci problémů, s nimiž se dispečeři na DPPC v praxi potýkají.

7.1.1 Služba CONNECT

Tato služba spočívá v propojení bezpečnostních agentur provozujících DPPC stejných technologií s využitím koncepce DPPC 1BOX. Pokud tedy společnosti provozující DPPC, které pořídily od společnosti NAM system, a. s., spolupracují díky této službě, dispečer při obdržení poplachové zprávy má možnost tuto obdrženou zprávu kliknutím odeslat na spolupracující DPPC, zde již dispečer tuto zprávu potvrdí a okamžitým oznámením zásahové jednotce provede činnosti potřebné k zásahu v tomto objektu. Tedy žádné volání spřátelenému DPPC, žádné nahlašování čísla objektu, adresy objektu atd., ušetří se zejména dojezdový čas a pomoc napadenému objektu je rychlejší.

7.1.2 Služba GUARD

Veškerá komunikace s výjezdovou skupinou v současnosti funguje tak, že pokud dispečer DPPC obdrží poplachovou zprávu (pomocí telefonu, nebo vysílačky), informuje o této situaci výjezdovou skupinu. Opět nahlásí veškeré dostupné informace důležité k výjezdu k tomuto objektu, což může znamenat ztrátu minimálně dvou minut. A zde je prostor pro ideální optimalizaci této problematiky pomocí služby GUARD, která bezesporu patří mezi velmi významné funkce koncepce DPPC 1BOX.

Modul GUARD počítá s výjezdovými vozidly, která jsou vybavena GPS navigací a propojena přes systém ONI (GPS sledování vozidel), a umožňuje tak příjem zpráv z DPPC. Při přijetí poplachové zprávy dispečer v DPPC aktivuje modul GUARD, vybere si vozidlo, které má uskutečnit výjezd k objektu. Po aktivaci se zobrazí na GPS souřadnice střeženého objektu a zároveň je řidič vyzván k zásahu. Po přijetí výzvy k zásahu je na DPPC odeslána informace o této události a vozidlo může vyjet ke střeženému objektu. Při dojezdu k objektu je automaticky odeslána zpráva o tom, že vozidlo se již nachází u střeženého objektu. Všechny tyto informace se zobrazují dispečerovi na obrazovce DPPC a jsou zpětně dohledatelné. Výjezdová jednotka nemusí například při příjezdu ztrácet čas s nahlášením příjezdu k objektu. Dispečer DPPC má možnost do navigace zasílat i vlastní

textové zprávy (např. bližší určení poplachové zprávy). Tato funkce je dostupná pouze u GPS navigací od firmy GARMIN.

Dle názoru autorky této práce jsou výše uvedené prostředky velmi vhodné pro bezpečnostní agentury, které chtějí v rámci svých služeb svým zákazníkům poskytnout maximální služby. A nutno dodat, že pro dispečery DPPC jsou tyto možnosti skutečně velkou oporou v každodenním řešení zpráv na DPPC. Osvojit si ovládání těchto funkcí přitom pro dispečery není složité.

7.2 Optimalizace činnosti DPPC z hlediska uživatele[10]

Dispečer je nejdůležitější složkou DPPC. Ve službě se potýká s nejedním rozhodnutím, jak správně danou událost vyřešit či jak nejlépe napadenému objektu zajistit pomoc. Autorka však může z vlastní zkušenosti konstatovat, že dispečerům DPPC často chybí odborná způsobilost, a to i díky finanční stránce. Zaměstnavatelé se snaží u svých pracovníků kumulovat funkce, což se nevyhýbá ani dispečerům DPPC, tím jim však v některých případech znemožňují plně se věnovat obsluze DPPC.

Dalším velmi častým problémem je úplná absence směrnic nebo postupů, které by se zabývaly řešením situací, k nimž může při výkonu služby na DPPC dojít. U mnoha společností v PKB provozujících DPPC je směrnice k dispozici pouze ve velmi jednoduché písemné, nebo dokonce ústní formě. To je podle autorky této práce naprosto nedostačující. Každý dispečer DPPC by měl mít základní manuál či směrnici pro vyhodnocování zpráv na DPPC.

Autorka v následující podkapitole představí směrnici, kterou vytvořila pro nejmenovanou společnost (směrnice pro vyhodnocení příchozích zpráv na DPPC z objektů napojených na OPIS HZS Zlínského kraje). Z důvodu výhradního dodavatele služeb v rámci připojování objektů na DPPC ve spolupráci s Hasičským záchranným sborem Zlínského kraje (dále jen HZS Zlínského kraje nebo HZS). Tato spolupráce fungovala tak, že z objektů, které měly být střeženy na DPPC HZS Zlínského kraje, zprávy chodí jak na toto DPPC, tak záložní cestou na DPPC výhradního dodavatele. Pokud by tedy selhalo první DPPC, na druhé DPPC je přenos zprávy zajištěn a toto DPPC ihned začne konat potřebné

[10] Celá podkapitola vychází z vlastních zkušeností autorky.

kroky. Nutno upřesnit, že na DPPC HZS Zlínského kraje jsou směrovány pouze požární poplachy, kdežto na výhradního dodavatele a jeho DPPC chodí veškeré zprávy, tedy včetně technických zpráv. A tyto řeší pouze výhradní dodavatel.

7.3 Směrnice pro vyhodnocení zpráv

Tato směrnice bude obsahovat základní zprávy, s nimiž se může dispečer v rámci střežení objektů na DPPC ve spolupráci s HZS Zlínského kraje setkat.

7.3.1 Požár

Pokud dispečer obdrží tuto zprávu, okamžitě informuje DPPC HZS Zlínského kraje, zda k nim taktéž tato zpráva dorazila. Pokud ano, další kroky již zajišťuje DPPC HZS Zlínského kraje. Pokud však zpráva na DPPC HZS Zlínského kraje nedorazila, je třeba okamžitě nahlásit číslo objektu, název objektu, adresu střeženého objektu a bližší určení místa, kde v objektu k požáru došlo (pokud je toto uvedeno). Cca po třech minutách od tohoto nahlášení se dispečer DPPC opět telefonicky obrátí na DPPC HZS Zlínského kraje s dotazem ohledně výsledku zásahu.

7.3.2 Porucha baterie

Dispečer okamžitě informuje zákazníka střeženého objektu a společnost, která pro tento objekt zajišťuje servis. Po třech hodinách od zápisu poruchy musí dispečer ověřit u servisní společnosti stav řešení. Servisní technik musí dodržet lhůty pro servis.

7.3.3 Porucha sítě

Dispečer okamžitě vyrozumí majitele objektu a o situaci ho informuje. Pokud je majitel s výpadkem elektrické energie obeznámen, vše je v pořádku a pouze je třeba od něj zjistit čas, kdy se elektrická energie obnoví. Pokud však majitel o žádném výpadku elektrické energie neví, je třeba jej požádat o kontrolu objektu a následné vysvětlení, z jakého důvodu elektrický proud v objektu nefunguje (vypadlý jistič, plánovaná odstávka elektrické energie).

7.3.4 Objekt nekomunikuje

Pro objekty, které jsou napojeny na DPPC, existují karty objektu, v nichž je uvedeno, jakým způsobem je objekt napojen (zda přes rádiový signál, nebo GPRS, či kombinací obojího). Pokud je objekt připojen více způsoby, musí být alespoň jedno připojení funkční. Pokud tedy dojde ke ztrátě komunikace, musí dispečer nejprve zjistit, jakým kanálem se komunikuje se střeženým objektem, a poté učinit následující kroky:

- *Pokud střežený objekt komunikuje pouze přes rádio:* při ztrátě komunikace je třeba ihned informovat zákazníka o dané situaci. Pokud zákazník neshledá jakýkoliv problém na zařízení dálkového přenosu, dispečer ihned vyrozumí servisní organizaci, která v objektu zajišťuje servisní zásah. Jakmile je servisní zásah proveden, komunikace opět funguje a majitel se servisního zásahu neúčastnil (např. pověřil kolegu či kompetentní osobu, která má v objektu daný problém na starosti), informuje jej dispečer o výsledku servisního zásahu a o obnově komunikace.
- *Pokud střežený objekt komunikuje pouze přes GPRS:* při ztrátě komunikace je třeba ihned informovat zákazníka o dané situaci. Pokud zákazník neshledá jakýkoliv problém na zařízení dálkového přenosu, dispečer ihned vyrozumí servisní organizaci, která v objektu zajišťuje servisní zásah. Jakmile je servisní zásah proveden, komunikace opět funkční a majitel se servisního zásahu neúčastnil (např. pověřil kolegu či kompetentní osobu, která má v objektu daný problém na starosti), informuje jej dispečer o výsledku servisního zásahu a o obnově komunikace.
- *Pokud střežený objekt komunikuje přes rádio i GPRS:* pokud dojde ke ztrátě komunikace po GPRS a objekt dále komunikuje přes rádio, není zatím nutné informovat majitele střeženého objektu. Pokud nefunguje rádio, ale GPRS ano, ani tehdy zatím není nutné informovat majitele. Pokud však vypadne rádio i GPRS, je třeba zákazníka ihned informovat o dané situaci. Pokud zákazník neshledá jakýkoliv problém na zařízení dálkového přenosu, dispečer ihned vyrozumí servisní organizaci, která v objektu zajišťuje servisní zásah. Jakmile je servisní zásah proveden, komunikace opět funkční a majitel se servisního zásahu neúčastnil (např. pověřil kolegu či kompetentní osobu, která má v objektu daný problém

na starosti), informuje jej dispečer o výsledku servisního zásahu a o obnově komunikací (rádio i GPRS).

7.3.5 Porucha, porucha 1, centrální porucha

Dispečer neprodleně informuje majitele střeženého objektu o poruše na zařízení. Majitel musí zavolat svoji servisní organizaci, aby zjistila, jaký problém nastal. Servisní zásah na takovém objektu musí být proveden v co nejkratším možném čase, protože systém EPS nemusí být funkční, v tomto případě by informace o požáru nemusela dojít ani na jedno DPPC. Dispečer na tuto variantu majitele upozorní a požádá jej, aby jej informoval v případě jakékoliv změny.

7.3.6 Vysílač otevřen

Pokud dispečer obdrží tuto zprávu, aniž by na objektu byl zahájen zásah buď servisního technika, nebo revizního technika, okamžitě o této situaci vyrozumí majitele. Pokud majitel potvrdí, že se zařízením nikdo nemanipuloval, dispečer upozorní majitele na nutnost kontroly tohoto zařízení.

7.3.7 Vzdálený test ZDP

Dispečer na tuto zprávu nemusí nijak reagovat, pouze ji odbaví a zapíše do knihy DPPC. Tato zpráva slouží pouze pro testování funkčnosti komunikace střeženého objektu s DPPC.

7.3.8 Test ZDP

Tato zpráva slouží pro testování systému EPS tlačítkem (fyzicky člověkem). Majitel objektu by si měl tímto způsobem pravidelně testovat komunikaci mezi střeženým objektem a DPPC. Pokud zákazník dopředu nahlásí tento test, dispečer mu pouze potvrdí, že zpráva byla doručena, pokud však zákazník test nenahlásí, není nutno kontaktovat majitele objektu, protože se nejedná o poplachovou událost. Pokud však nastane situace, že zákazník dopředu nahlásí takový test a tato zpráva se na DPPC neobjeví, musí se informovat servisní organizace, aby situaci napravila. To znamená, že test ZDP po stisknutí tlačítka EPS musí dojít na DPPC.

7.3.9 Autoreset komunikátoru

Tato zpráva se objeví nejčastěji při provedení vzdáleného testu, vzdáleného nastavení nebo vzdálené konfigurace ze strany společnosti, která provozuje technologické centrum. Dispečer na tuto zprávu nijak nereaguje. Pokud však dojde k situaci, že tyto zprávy začnou chodit opakovaně za sebou, dispečer o této situaci ihned vyrozumí správce DPPC.

7.3.10 Reset vysílače v objektu

Tato zpráva se též objevuje nejčastěji při provedení vzdáleného testu, vzdáleného nastavení nebo vzdálené konfigurace ze strany společnosti, která provozuje technologické centrum. Dispečer na tuto zprávu nijak nereaguje. Pokud však dojde k situaci, že tyto zprávy začnou chodit opakovaně za sebou, dispečer o této situaci ihned vyrozumí správce DPPC.

7.3.11 Výpadek sběrné stanice

Pokud dispečer obdrží tuto zprávu na DPPC, okamžitě informuje o této situaci servisní službu a ta zahájí úkony k opětovné obnově komunikace sběrné stanice.

7.3.12 Provádění údržby, servisního zásahu, pravidelné revize

Pokud majitel informuje dispečera o těchto zásazích do zařízení EPS, dispečer o této situaci ihned informuje DPPC HZS, aby až do odvolání nereagovali na příchozí zprávy. Jakmile se majitel opět spojí s dispečerem a oznámí mu ukončení těchto prací, dispečer opět informuje DPPC HZS s tím, že střežený objekt je opět v ostrém režimu.

Výše uvedené zprávy jsou na DPPC jedny z pravidelně se objevujících, nelze však bohužel vytvořit směrnici, která dispečera připraví na vše. Toto může sloužit pouze jako podpůrný materiál, který dispečerovi dodá nadhled a upřesní, co která zpráva znamená. Při monitorování objektů na DPPC může totiž nastat mnoho nepředvídatelných situací a pak záleží na konkrétním dispečerovi, jeho zkušenostech a schopnostech, jak danou situaci vyhodnotí. Tato směrnice by měla dispečerům sloužit jako „první pomoc“ při jejich rozhodování, poté už je vše jen otázkou jejich vlastní praxe.

ZÁVĚR

Předložená diplomová práce nabízí v rámci teoretické části detailní pohled na technické řešení DPPC s přihlédnutím na platnost nově vydaných norem, které upravují jeho provoz, současně využívané přenosové trasy a přenosová zařízení.

V praktické části autorka provedla analýzu výrobců dohledových a poplachových přijímacích center v rámci nabídky na trhu v České republice. Na základě dlouholeté praxe v oboru a vlastního výzkumu vyhodnotila jako nejlepšího dodavatele těchto služeb společnost NAM system, a. s. a popsala technologie jejích výrobků a služeb. Jednou z nejsilnějších stránek tohoto dodavatele je technická podpora v oblasti DPPC a přehledný software pro dispečery (především služba ONI systém, kdy má dispečer přehled o poloze zásahových, servisních a revizních vozidlech a v případě řešení jakékoliv situace může poslat k zásahu nejbližší možné vozidlo).

Byla optimalizována činnost dispečera v rámci dohledového a poplachového přijímacího centra jak z pohledu technického, tak z pohledu uživatele. Dále byla vytvořena základní směrnice pro vyhodnocení nejčastějších příchozích zpráv na DPPC z objektů napojených na Hasičský záchranný sbor Zlínského kraje. Tato směrnice může být užitečná pro dispečery DPPC, kteří se zabývají obdobným oborem.

Důležité je si uvědomit, že tato pracoviště centralizují různé systémy, ať už jde o systémy PZTS, EPS, CCTV či jiné. Stále rostou technické požadavky na hardwarovou složku DPPC a s tím i požadavky na kvalifikovanost obsluhy těchto pracovišť. Doba, kdy na pozici dispečera pracoval zaměstnanec v důchodovém věku na poloviční úvazek, je dávno minulostí. V současné době jsou již požadavky na pozici dispečera mnohonásobně vyšší a firmy při výběru zaměstnanců do svých řad vyžadují od nových členů především technickou způsobilost, psychickou odolnost a schopnost se správně a rychle rozhodovat.

Cílem této diplomové práce bylo především podat ucelený obraz o činnosti DPPC a vytvořit základní manuál pro dispečery, aby byli snáze schopni správně reagovat na situace, které mohou na dispečinku takového centra vzniknout.

CONCLUSION

The diploma thesis in the theoretical part provides a detailed look at the technical solution of a monitoring and alarm reception centre considering the validity of newly issued standards that govern its operation, current use of transmission lines and transmission equipments.

In the practical part, the author analysed producers of surveillance and monitoring and alarm reception centre within the supply on the market in the Czech republic. NAM system was chosen as the best supplier of these services based on author’s many years of experience in the industry and own research. Its technology of products and services were described in the thesis. One from the supplier's strengths is the technical support in the monitoring and alarm reception centre area and transparent software for dispatchers (mainly ONI system service where the dispatcher has good overview about the position of emergency, servicing and inspecting vehicles and can dispatch the nearest possible vehicle in case of any critical situation).

In the thesis dispatcher activity within monitoring and alarm reception centre was optimized in terms of technical and user's perspective. Furthermore, a fundamental guideline for the most frequent evaluation of incoming messages from objects connected to the Fire Brigade of the Zlín Region to monitoring and alarm reception centre was created. The guideline may be useful for monitoring and alarm reception centre dispatchers dealing with a similar field of activity.

It is very important to understand that these offices centralize various systems whether it is PZTS system, CCTV or others. Technical requirements for monitoring and alarm reception centre hardware component are still growing as well as the requirements for operator‘s qualification. The time when the dispatcher was an employee in retirement age is past now. Currently requirements for dispatcher‘s position are many times higher and companies require from new employees mainly technical competences, psychical resilience and ability to make decisions quickly and correctly.

The aim of this thesis was to provide a comprehensive picture about monitoring and alarm reception centre activities and create a basic manual for dispatchers to be more easily able to respond to situations that may arise in the dispatching center.

SEZNAM POUŽITÉ LITERATURY

[1] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management I.* Zlín: VeRBuM, 2011. ISBN 978-80-87500-05-7.

[2] VÍTEK, Tomáš. *Požární bezpečnost, základy EPS – Elektrická požární signalizace* [online prezentace]. 2010 [cit. 2014-02-07]. Dostupné z: http://www.micro.feld.cvut.cz/home/X34EZS/prednasky/Zaklady%20EPS.pdf.

[3] NOVÁK, Vladimír a Věra NOVÁKOVÁ ZACHOVALOVÁ. Princip fungování EZS. In: *Ladinn.cz* [online]. 2013-03-28 [cit. 2014-02-07]. Dostupné z: http://www.ladinn.cz/ostatni/technika/princip-EZS.html.

[4] ČSN EN 50518-1. *Dohledová a poplachová přijímací centra: Část 1: Umístění a konstrukční požadavky.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2010.

[5] RADOM, S. R. O. O společnosti. *Radom.eu* [online]. © 2014 [cit. 2014-03-29]. Dostupné z: http://www.radom.eu/o-spolecnosti.htm.

[6] RADOM, S. R. O. Zabezpečení a střežení objektů. *Radom.eu* [online]. © 2014 [cit. 2014-03-29]. Dostupné z: http://www.radom.eu/produkty-a-sluzby/ochrana-majetku.htm.

[7] TRADE FIDES, A. S. Profil společnosti. *Fides.cz* [online]. [cit. 2014-03-16]. Dostupné z: http://www.fides.cz/cs/profil/.

[8] TRADE FIDES, A. S. Síť LATIS. *Fides.cz* [online]. [cit. 2014-03-16]. Dostupné z: http://www.fides.cz/cs/pco-latis-sql/sit-latis.

[9] JABLOTRON ALARMS, A. S. O nás. *Jablotron.com* [online]. [cit. 2014-03-29]. Dostupné z: http://www.jablotron.com/cz/o-jablotronu/o-nas/.

[10] JABLOTRON SECURITY, A. S. Profil společnosti. *Celkovaochrana.cz* [online]. © 2004-2014 [cit. 2014-03-29]. Dostupné z: http://www.celkovaochrana.cz/o-spolecnosti.

[11] JABLOTRON ALARMS, A. S. Jablotron 100. *Jablotron.com* [online]. [cit. 2014-03-29]. Dostupné z: http://www.jablotron.com/cz/alarmy/jablotron-100/.

[12] JABLOTRON ALARMS, A. S. Jablotron 80. *Jablotron.com* [online]. [cit. 2014-03-29]. Dostupné z: http://www.jablotron.com/cz/alarmy/jablotron-80/.

[13] JABLOTRON ALARMS, A. S. Azor. *Jablotron.com* [online]. [cit. 2014-03-29]. Dostupné z: http://www.jablotron.com/cz/alarmy/azor/.

[14] NAM SYSTEM, A. S. Historie společnosti. *Nam.cz* [online]. © 2010 [cit. 2014-04-13]. Dostupné z: http://nam.cz/texts.asp?category=3.

[15] NAM SYSTEM, A. S. Sběrné stanice. *Nam.cz* [online]. © 2010 [cit. 2014-04-13]. Dostupné z: http://nam.cz/texts.asp?category=15&sub=9.

[16] NAM SYSTEM, A. S. Vysílače řady TSM. *Nam.cz* [online]. © 2010 [cit. 2014-04-13]. Dostupné z: http://nam.cz/texts.asp?category=16&sub=1.

[17] NAM SYSTEM, A. S. Rádiový PCO: Rádiová síť Global. *Nam.cz* [online]. © 2010 [cit. 2014-04-13]. Dostupné z: http://nam.cz/texts.asp?category=15&sub=6.

[18] NAM SYSTEM, A. S. Rádiový PCO: Rádiová síť Global 2. *Nam.cz* [online]. © 2010 [cit. 2014-04-13]. Dostupné z: http://nam.cz/texts.asp?category=15&sub=7.

[19] NAM SYSTEM, A. S. Verze software. *Nam.cz* [online]. © 2010 [cit 2014-04-19]. Dostupné z: http://www.nam.cz/texts.asp?category=20.

[20] NAM SYSTEM, A. S. GPRS PCO. *Nam.cz* [online]. © 2010 [cit. 2014-04-20]. Dostupné z: http://www.nam.cz/texts.asp?category=15&sub=2.

[21] JAŠEK, Roman a David MALANÍK. *Bezpečnost informačních systémů*. Zlín: UTB ve Zlíně, Fakulta aplikované informatiky, 2013. ISBN 978-80-7454-312-8. Dostupné také z: http://dspace.k.utb.cz/handle/10563/25821.

[22] HAMALOVÁ, Jana. *Způsoby zabezpečení dat v PC a metody pro jejich obnovu*. Zlín, 2011. Bakalářská práce. UTB ve Zlíně, Fakulta aplikované informatiky. Vedoucí práce David Malaník.

[23] NAM SYSTEM, A. S. Manuály ke stažení. *Nam.cz* [online]. © 2010 [cit. 2014-04-25]. Dostupné z: http://www.nam.cz/texts.asp?category=12.

[24] HARPER, Allen, Chris EAGLE, Jonathan NESS a Michael LESTER. *Hacking: manuál hackera*. Praha: Grada, 2008. ISBN 978-80-247-1346-5.

[25] LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti I.* Zlín: Univerzita Tomáše Bati ve Zlíně, 2004. ISBN 80-7318-231-9.

[26] *The Professional Protection Officer: Practical Security Strategies and Emerging Trends*. Oxford: Butterworth-Heinemann, 2010. ISBN 18-561-7746-7.

[27] ČSN EN 50518-2. *Dohledová a poplachová přijímací centra: Část 2: Technické požadavky*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011.

[28] ČSN EN 50518-3. *Dohledová a poplachová přijímací centra: Část 3: Pracovní postupy a požadavky na provoz*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2012.

[29] AMENIT, S. R. O. Bezpečnostní software: Základní definice. *Antivirovecentrum.cz* [online]. © 1998-2014 [cit. 2014-05-12]. Dostupné z: http://www.antivirovecentrum.cz/nastroje-pro-zabezpeceni.aspx.

[30] NAM SYSTEM, A. S. *Monitorovací software NET-G verze: 1.22: Manuál správce*. [online]. [cit. 2014-05-12]. Dostupné z: http://www.nam.cz/download/manualy/Manual%20NET-G%201.22.pdf.

[31] HEROS GROUP, S. R. O. PCO - PULT CENTRALIZOVANÉ OCHRANY. *Heros.cz* [online]. © 2014 [cit. 2014-05-10]. Dostupné z: http://www.heros.cz/nase-sluzby/bezpecnostni-sluzby/ostraha-a-ochrana-objektu/dohledove-centrum/pult-centralizovane-ochrany/.

[32] RANDÁK, Milan. *Odborná praxe 01: Zálohování a ochrana dat* [online prezentace]. [cit. 2014-05-01]. Dostupné z: http://www.google.cz/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=1&ved=0CDUQFjAA&url=http%3A%2F%2Fwww.pbvos.cz%2Fvzdelavaci_programy%2FFP%2520-%2520sylaby%2C%2520opory%2C%2520prezentace%2FOdborn%25E1%2520praxe%2FPrezentace%2FPrezentace%2520ODP%252001.pptx&ei=UkFzU-DNLITH7AbLg4GIBw&usg=AFQjCNFi8JEqQllFkoeK4kwICdVQ41HV1w.

[33] RADOM, S. R. O. Pulty centralizované ochrany (PCO) - RADOM SECURITY a RADOM SECURITY FIRE. *Radom.eu* [online]. © 2014 [cit. 2014-03-29]. Dostupné z: http://www.radom.eu/produkty-a-sluzby/ochrana-majetku/pulty-centralizovane-ochrany-pco-.htm.

[34] VALOUCH, Jan. *Projektování integrovaných systémů*. Zlín: Univerzita Tomáše Bati ve Zlíně, FAI, 2013. ISBN 978-80-7454-296-1. Dostupné také z: http://dspace.k.utb.cz/handle/10563/25814.

[35] NAM SYSTEM, A. S. PCO NAM Global. *Nam.cz* [online]. © 2010 [cit. 2014-03-17]. Dostupné z: http://www.nam.cz/texts.asp?category=15.

[36] VYORÁLEK, Radim. *Pulty centralizované ochrany*. Zlín, 2009. Bakalářská práce. UTB ve Zlíně, Fakulta technologická. Vedoucí práce Marek Čandík.

[37] KŘEMÉNKOVÁ, Jana. *Technické řešení dohledového a poplachového přijímacího centra*. Zlín, 2013. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně. Vedoucí práce Milan Adámek.

[38] Informace o malware: Co je malware. *Malwarebytes.cz* [online]. [cit. 2014-03-10]. Dostupné z: http://www.malwarebytes.cz/malwarebytes/co-je-malware.

[39] JABLOTRON SECURITY, A. S. Nabídka ochrany. *Celkovaochrana.cz* [online]. © 2004-2014 [cit. 2014-03-01]. Dostupné z: http://www.celkovaochrana.cz/ochrana-objektu-pro-fyzicke-osoby/cenik.

[40] NAM SYSTEM, A. S. Monitorovací SW NET-G. *Nam.cz* [online]. © 2010 [cit. 2014-04-25]. Dostupné z: http://www.nam.cz/texts.asp?category=15&sub=4.

[41] NAM SYSTEM, A. S. Přenosová trasa GPRS. Služby sítě NSG. *Nam.cz* [online]. © 2010 [cit. 2014-04-25]. Dostupné z: http://www.nam.cz/images/gprspco_full.jpg.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

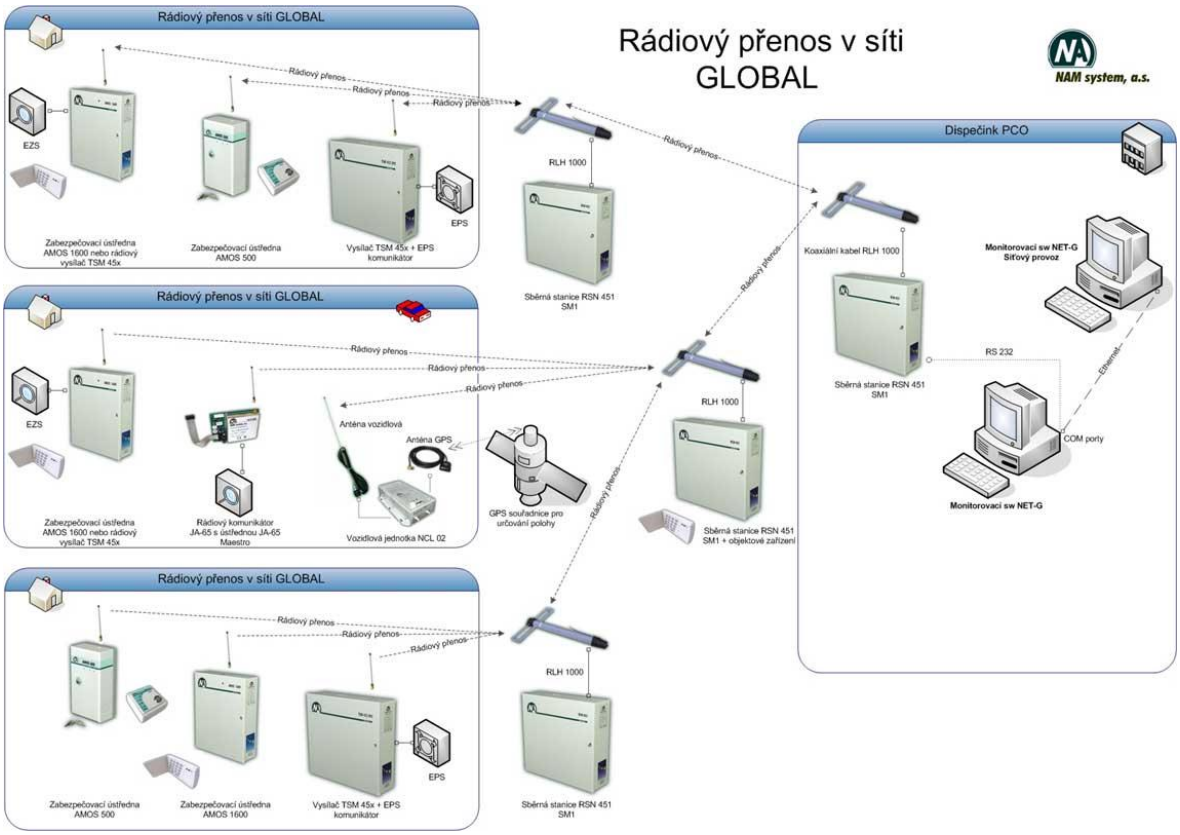
ACS	Access Control system
AIR	Aktivní infra-červený detektor
CCTV	Closed Circuit Television
DPPC	Dohledové a poplachové přijímací centrum
DTMF	Dual-tone multi-frequency
DVR	Digital video recording
EPS	Elektrická požární signalizace
GPRS	General Packer Radio Service
GSM	Global System for Mobile Communications
IP	Internet Protocol
LAN	Local Area Network
PC	Personal Computer
PIR	Pasiv Infra Red detector
PKB	Průmysl komerční bezpečnosti
PSTN	Public Switched Telephone Network
SIM	Subscriber Identity Module
SMS	Short Message Service
STA	Společná televizní anténa
TCP	Transmission Control Protocol
USB	Universal Serial Bus
WAN	Wide Area Network

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

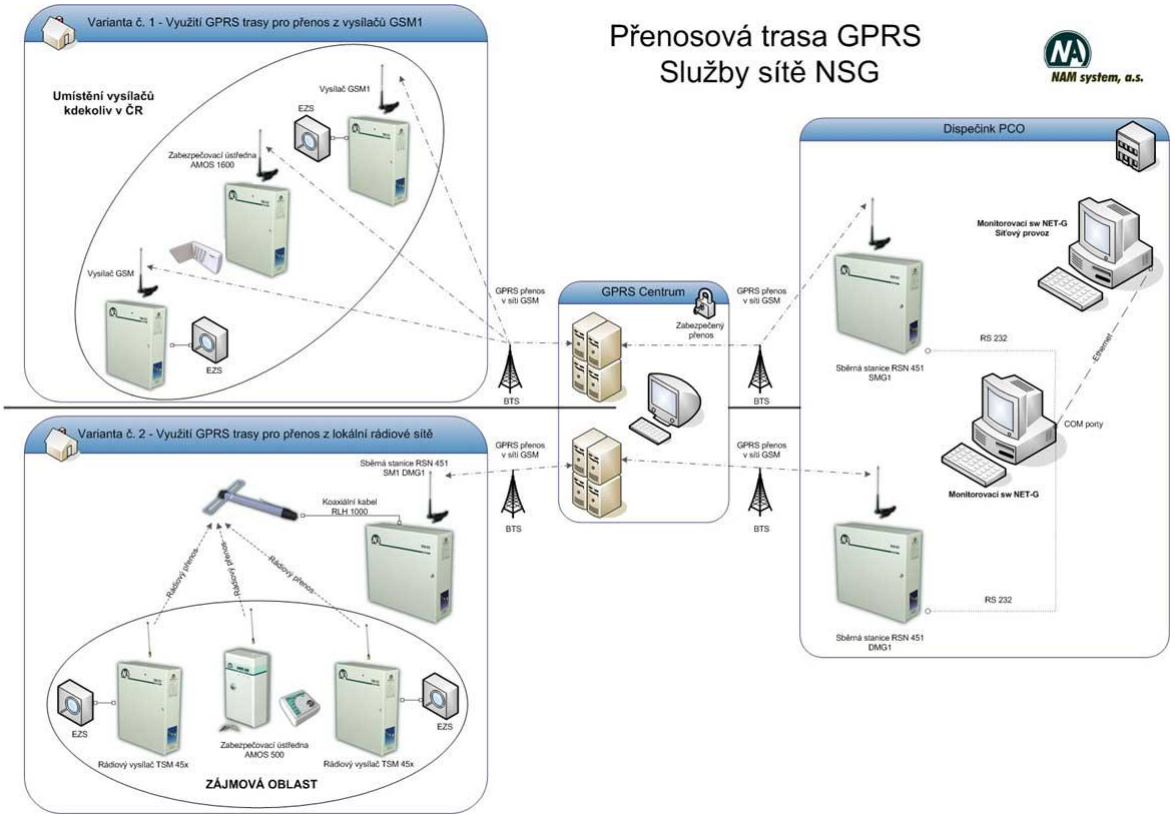
SEZNAM PŘÍLOH

PŘÍLOHA P I: SCHÉMA RÁDIOVÉ SÍTĚ GLOBAL



Příloha č. 1. Schéma rádiové sítě GLOBAL. Zdroj: [17].

PŘÍLOHA P II: SCHÉMA RÁDIOVÉ SÍTĚ NSG



Příloha č. 2. Schéma rádiové sítě NSG. Zdroj: [41].

PŘÍLOHA P III: UKÁZKA ŽHAVÉ NOVINKY 1BOX-FOTO

Příloha č. 3a. Ukázka žhavé novinky 1BOX. Zdroj: autorka.

Příloha č. 4b. Ukázka žhavé novinky 1BOX. Zdroj: autorka.