Radiokomunikační síť integrovaného záchranného systému Pegas a její technické a kryptografické zabezpečení

Jan Douša

Bakalářská práce
2016

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2015/2016

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

Jméno a příjmení:	**Jan Douša**
Osobní číslo:	**A13262**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Radiokomunikační síť integrovaného záchranného systému Pegas a její technické a kryptografické zabezpečení**
Téma anglicky:	**The Pegas Integrated Rescue System Radio Communication Network and its Technical and Cryptographic Security**

Zásady pro vypracování:

1. **V literární rešerši uveďte historii vzniku a budování jednotné radiokomunikační sítě Pegas.**
2. **Prezentujte strukturu radiokomunikační sítě Pegas.**
3. **Proveďte analýzu zabezpečení sítě Pegas, se zohledněním systémových a technických opatření.**
4. **V závěru se zaměřte na vyhodnocení analýzy, na přednosti a nedostatky zabezpečení radiokomunikační sítě Pegas a na porovnání bezpečnostních opatření s ostatními sítěmi.**
5. **Uveďte možnou budoucnost a další využití sítě Pegas.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **Pramacom [online] http://www.pramacom.cz .**
2. **Radiová síť Pegas [online] soubor odborných článků http://www.kmitocty.cz .**
3. **Sbírka interních aktů řízení generálního ředitele HZS ČR a NMV – částka 41/2004 Řád analogové radiové sítě.**
4. **KESL, Jan. Elektronika. 1. vyd. Praha: BEN – technická literatura, 2003, 113 s. Učebnice – základní studijní materiál pro střední školy. ISBN 80-7300-075-x.**
5. **Prezentace Systému A,B Matra Nortel Communications 24/04/02, PMS PS8442GJA01.**

Vedoucí bakalářské práce: **Ing. Ján Ivanka**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **26. února 2016**

Termín odevzdání bakalářské práce: **30. května 2016**

Ve Zlíně dne 16. února 2016

L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Jan Valouch, Ph.D.
ředitel ústavu

Jméno, příjmení: Jan Douša

Název bakalářské/diplomové práce: Radiokomunikační síť integrovaného záchranného systému PEGAS a její technické a kryptografické zabezpečení

Prohlašuji, že

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

Prohlašuji,

- že jsem na diplomové/bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne

.....
podpis diplomanta

ABSTRAKT

Bakalářská práce se zabývá digitální radiokomunikační sítí Pegas, kterou jako jeden ze svých hlavních komunikačních prvků využívá Ministerstvo vnitra ČR a jeho složky. Tato práce je rozdělena do pěti kapitol. Postupně je představena historie a vznik radiokomunikační sítě a její struktura. Dále je analyzováno zabezpečení sítě a to jak systémové, tak technické. Analýza je dále vyhodnocena a na závěr je shrnuta budoucnost a možnosti rozvoje radiokomunikační sítě Pegas v ČR.

Klíčová slova: Radiokomunikační síť, zabezpečení, Tetrapol, Pegas, radiostanice, terminál, digitální.

ABSTRACT

This bachelor's work is focused on the digital radio network of Pegas. This radio network is used by the Ministry of the Interior and its sections as one of their main communication element. This work is divided into five chapters. Topics as the history of Pegas and its formation of the radio network or the net structure are presented by degrees. Furthermore, both systemic and technical network security is analyzed. Afterwards this analysis is judged, as well. Finally, the future and development opportunities of Pegas radio network are summarized for the area of the Czech Republic.

Keywords: Radio network, security, Tetrapol, Pegas, radio station, terminal, digital.

Rád bych tímto poděkoval panu Ing. Jánu Ivankovi za odborné vedení v průběhu zpracování této bakalářské práce.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Od roku 2008 pracuji u Hasičského záchranného sboru České Republiky (dále jen HZS). V posledním desetiletí prošlo HZS rozsáhlou obnovou a to jak personální, tak i technickou. Snaha o modernizaci HZS je podmíněna především rychlým technickým rozvojem celé společnosti a přiblížením se nejmodernějším trendům, používaným v celé Evropě.

Celé HZS , stejně jako ostatní bezpečnostní složky v ČR, prošlo restrukturalizací. Z HZS se tímto stal moderní bezpečnostní sbor, který je jak na krajské, tak i celorepublikové úrovni centrálně řízen a to především v operační složce řízení. S přechodem k tomuto modelu řízení jednotek bylo potřeba vybudovat zcela novou komunikační síť, která by zvládla nově kladené nároky. Vždyť bez spolehlivého spojení není velení.

Jako příslušník bezpečnostního sboru a především každodenní uživatel komunikačních kanálů si uvědomuji nároky, které jsou kladeny na provoz a správu zabezpečené sítě bezpečnostních sborů. Zároveň jako student Fakulty aplikované informatiky, oboru Bezpečnostní technologie systémy a management mám živý zájem, dozvědět se podrobnosti o zabezpečení komunikačního kanálu Ministerstva vnitra, jehož jsem každodenním uživatelem.

Cílem práce je tedy shrnout historii vzniku a budování radiokomunikační sítě Pegas, prezentování její struktury a analýza jejího zabezpečení, včetně kontrolních bezpečnostních prvků. V závěru se chci zaměřit na další možnosti, které síť nabízí a na její další možnou budoucnost.

I. TEORETICKÁ ČÁST

1 RADIOKOMUNIKAČNÍ SÍŤ PEGAS

Tato část bakalářské práce se snaží o stručné shrnutí a definici pojmu radiokomunikační síť PEGAS a zmapování historie vzniku a budování sítě.

1.1 Obecná definice

Radiokomunikační síť PEGAS je státem budovaná síť, určená pro komunikaci složek IZS a MV. Síť je založena na digitální technologii TETRAPOL, jenž byla původně vyvíjena pro francouzské četnictvo. V roce 1988 byla ve Francii dokončena síť RUBIS, která jako první používá technologii TETRAPOL. Tvorbu sítě prováděly firmy MATRA a NORTEL, spojené do Matra Nortel Communication. Její základní předností je to, že je po celé komunikační dráze, tedy od terminálu po terminál. plně šifrovaná. To platí jak pro síťový režim, tak i pro mimosíťový (přímý) režim provozu. Systém TETRAPOL byl totiž již od počátku konstruován jako neveřejný, určený pro armádní a policejní využití. Další jeho důležitou předností je, že má několikastupňový dohled, který je prováděn jak nad provozem, tak i nad oprávněními uživatelů v síti. Systém má možnost na dálku měnit komunikační kanály. Ty jsou operativně přidělovány a odebírány dle požadavků účastníků komunikace. S menším počtem kanálů lze tedy obsloužit relativně velký počet koncových radiostanic. To tvoří tzv. trtunkovou síť.

V celosvětovém měřítku je systém TETRAPOL rozšířen především v Evropě a severní Americe, kde tvoří jak regionální, tak i celostátní sítě. Malá regionální síť je zbudována např. na letišti Frankfurt nad Mohanem, nebo v Berlíně. Jako zástupce národních sítí lze jmenovat právě český Pegas, slovenskou národní radiokomunikační síť SITNO, POLYCOM švýcarské policie, SIRDE ve Španělsku a IRIS v Mexiku. Vojenské využití našel TETRAPOL při misích NATO KFOR v Kosovu a ISAF v Afgánistánu.

Postupně přechází firma Matra- Nortel Communication pod firmu EADS a její společnosti Connexity, později Cassidian. V roce 2014 jsou i tyto značky zrušeny a celé radiokomunikační oddělení firmy EADS přechází pod novou značku AIRBUS.

Parametry sítě PEGAS II :

- síť TETRAPOL je sítí trunkového typu,
- je vyhrazena pro frekvenční pásmo 380 - 430MHz a 440 - 490MHz,
- v České Republice síť PEGAS II,
- výstupy převaděčů 390.000 - 394.9875 MHz,
- vstupy převaděčů 380.000 - 394.9875 MHz,
- celá síť je členěna do 14 regionálních sítí, a to dle územního členění České Republiky,
- vlastníkem sítě je MV,
- provozovatelem ICT Service,
- výhradním distributorem technologie TETRAPOL je firma Pramacom Prague cz.

1.2 Historie vzniku jednotné radiokomunikační sítě Pegas

- 1993 - Budování národní radiové sítě PEGAS provázelo během jejího vzniku mnoho obtíží. V roce 1993 zadává vláda (usnesením č. 246/1993 - Vypracování návrhu technického řešení propojitelnosti složek IZS) [2] ministru vnitra úkol, vypracovat projekt propojení komunikačních prostředků jednotlivých složek IZS (vznik v roce 2000) a MV. Každá ze složek totiž používá jinou radiovou síť, kdy každá z nich je provozována na jiném frekvenčním pásmu. S nově plánovanou koncepcí IZS (integrovaný záchranný systém, který vchází do praxe společně se zákonem 239/200 Sb.), je zapotřebí sjednotit komunikační prostředky jednotlivých záchranných složek a bezpečnostních sborů státu, pro potřeby společných zásahů a cvičení. V roce 1994 probíhá výběrové řízení , do kterého se přihlásí 4 firmy. A to: Matra- Nortel comunication, Ericson, Ascom, Marconi. Do kola druhého postupují 3 firmy (odpadá firma Ascom). Výběrové řízení vyhrává Matra se standardem TETRAPOL. Součástí a podmínkou výběrového řízení je praktická ukázka funkčnosti systému. Firma Matra spouští na Strahově dočasný převaděč s vysílačem, který dokáže signálem pokrýt 1/2 Prahy.

- 1995 - ČTÚ vydává povolení Ministerstvu vnitra ke zřízení radiové sítě v pásmu 390 MHz.
- 1997 - Budování sítě má veliké zpoždění. Naprogramováno je pouze 2200 radiostanic, což představuje asi tak 1/10 stanic potřebných pro PČR.
- 1999 - v provozu je pouze 21 RBS (v současnosti jich je 220 a k tomu velké množství lokálních opakovačů).
- 2000 - Vychází požadavek na přebudování celé sítě (od MV) na síť II. generace. Tento požadavek je způsoben především rozsáhlými problémy při pořádání "Mezinárodního měnového fondu v Praze".
- 2001 - Přechod na síť II. generace. Znamená to kompletní změnu technologie a radiostanic. Zároveň to znamená přešifrování celé sítě a všech terminálů
- 2002 - Je prodloužen termín výstavby . Rozhodnuto, že k plnému pokrytí signálem bude třeba 215 RBS (v současnosti 220).
- 2003 (31.8.) - Dobudována základní forma sítě, nákladem 6 miliard Kč. [1]

Obr. 1. Radiostanice
typu G1.
[zdroj vlastní]

2 STRUKTURA RADIOKOMUNIKAČNÍ SÍTĚ PEGAS A JEJÍ SLUŽBY

Celá síť se dá rozčlenit ze dvou hledisek. Z hlediska technického a z hlediska organizačního.

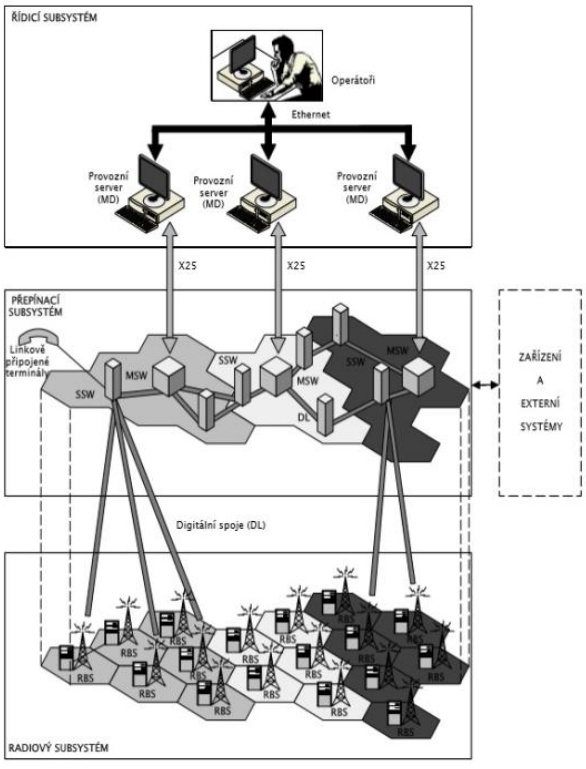
2.1 Technická struktura sítě

Celá síť by se dala jako kompaktní systém rozdělit do tří závislých subsystémů. Řídící a přepínací subsystém jsou propojeny páteřní sítí X25 (standard Mezinárodní telekomunikační unie X.25), na níž jsou napojena dohledová a provozní centra, servery a řídící jednotky (Main Switch - MSW), jenž ovládají regionální podsítě .

2.1.1 Řídící subsystém

Základem řídícího subsystému jsou servery využívané řídícími klientskými aplikacemi, které jsou nainstalovány na různých stanovištích (PC).

Řídící subsystém v sobě zahrnuje provozní a řídící stanoviště, která jsou fyzicky přítomná na PC nebo provozních stanicích s operačním systémem LINUX, nebo UNIX.



Obr. 2. Hierarchie sítě. [4]

Řídící subsystém obsahuje tyto složky:

- provozní server MD,
- stanoviště technického dohledu TMP , TDP,
- stanoviště taktického řízení TWP,
- samostatné dispečerské stanoviště SADP,
- stanice programování terminálů TPS,
- stanice programování mikropočítačových karet SCPS,
- stanoviště kontroly technických údajů a událostí EPC,
- stanoviště klíčového hospodářství KMC,
- jednotka pro zavádění klíčů KLU.

2.1.2 Přepínací subsystém

Přepínací subsystém tvoří dva typy ústředen. Jsou to:

- MSW - Hlavní ústředna (Main Switch),
- SSW - Vedlejší ústředna (Secondary Switch).

Přičemž v regionální síti je vždy jen jedna hlavní ústředna MSW a zpravidla několik vedlejších ústředen SSW. Síť PEGAS je v ČR dělena do čtrnácti regionálních podsítí, dle územního dělení České Republiky. Z této podstaty vychází, že v ČR je celkem 14 MSW.

Jedním z úkolů MSW je monitoring sítě a distribuce místních šifrovacích klíčů. MSW taktéž provádí autorizaci při přihlašování terminálů do sítě.

Hlavní ústředna MSW provádí:

- řízení databáze hlavní ústředny,
- řízení šifrování,
- propojování s ethernetovou sítí v případě datových komunikací,
- propojování se sítí X25 v případě spojů s provozní a údržbovou sítí a s ostatními regionálními sítěmi,
- řízení a monitorování sítě ve spolupráci se síťovými operátory,
- sběr informací o provozu, alarmech a účastnících,
- přepínání okruhů u hlasových komunikací,
- přepínání paketů u datové komunikace,

- zpracování hovoru,
- řízení datového přenosu,
- řízení připojených zařízení.

Vedlejší ústředna SSW provádí:

- přepínání okruhů u hlasových komunikací,
- přepínání paketů u datové komunikace,
- zpracování hovoru,
- řízení datového přenosu,
- řízení připojených zařízení.

Č. reg. sítě	Č. MSW	Lokace
RN0	MSW 101	Praha
RN1	MSW 125	Středočeský kraj
RN2	MSW 222	Jihočeský kraj
RN3	MSW 322	Plzeňský kraj
RN4	MSW 362	Karlovarský kraj
RN5	MSW 422	Ústecký kraj
RN6	MSW 462	Liberecký kraj
RN7	MSW 522	Královéhradecký kraj
RN8	MSW 562	Pardubický kraj
RN9	MSW 262	Kraj Vysočina
RN10	MSW 622	Jihomoravský kraj
RN11	MSW 662	Zlínský kraj
RN12	MSW 762	Olomoucký kraj
RN13	MSW 722	Moravskoslezský kraj

Tab. 1. Rozdělení MSW v krajích. [zdroj vlastní]

2.1.3 Radiový subsystém

K MSW jsou připojeny jednotlivé RBS (Radio Base Station - radiové základny). Ty vysílače tvoří samostatné buňky a zaručují radioelektrické pokrytí signálem. K nim se pak připojuje samotný terminál (radiostanice). Základnových radiostanic je v současnosti v České Republice 220, přičemž z 80% jsou umístěny na společném vysílacím stožáru s ostatními komerčními vysílači.

Známe tři základní typy buněk.

1. S jedinou samostatnou stanicí (Stanice metra).
2. Několik stanic - tzv. překryvná buňka, kterou vytváří několik podřízených základnových stanic označovaných SS, T - SS. Pracují se stejným kmitočtem, který je synchronizován signálem GPS. Tato infrastruktura je z uživatelského hlediska a z hlediska využití radiových kanálů nejvýhodnější.
3. Nezávislá izolovaná buňka - tvořená nezávislým digitálním opakovačem IDR. Zřizuje se v případě dlouhodobých zásahů v místech, kde není základní územní pokrytí signálem. [4]

Obr. 3. BTS maskovaná v lesním porostu. [10]

2.2 Organizační struktura sítě

Z hlediska organizačního, lze celý systém rozdělit do deseti tzv. flotil, jenž představují skupiny uživatelů.

Každá koncová radiostanice je pak označena svým jedinečným identifikátorem, obdobou čísla sim- karty v GSM síti. Toto číslo se nazývá RFSI číslo. [7]

1	PČR (s působností po celé ČR)
2	PČR okresní
3	rezerva pro PČR
4	Městské policie, nestátní subjekty
5	HZS
6	rezerva pro HZS
7	ZZS
8	AČR
9	Bezpečnostní informační služba
0	MV školy a servis sítě

Tab. 2. Rozdělení flotil.

[zdroj vlastní]

RFSI číslo je složeno takto:

RRRFSSIII.

Přičemž jednotlivé složky RFSI odpovídají:

- RRR - číslo regionální sítě, ke které terminál přísluší,
- F - číslo flotily, do které je terminál zařazen,
- SS - číslo skupiny, které se významem liší dle flotily. U HZS je to číslo kraje, u PČR číslo oddělení, pod které terminál spadá,
- III - samostatný identifikátor v rámci kraje, nebo oddělení.

2.3 Typy radiových přenosů

Jako další součást této kapitoly, bych chtěl představit základní typy přenosů, které jsou v radiokomunikační síti PEGAS provozovány mezi terminály.

Jsou to následující typy přenosů.

2.3.1 Síťový režim

Každá základnová stanice BTS má k dispozici maximálně 24 kanálů. Kanály v tomto režimu provozu jsou duplexní. Kanály se dále dělí do dvou kategorií a to:

- řídící kanály CCH,
- provozní kanály TCH.

Řídící kanály jsou vyhrazeny pro přenos signalizace a dat.

Provozní kanály přenášejí komunikaci mezi jednotlivými účastníky komunikace. Dělí se do dvou typů:

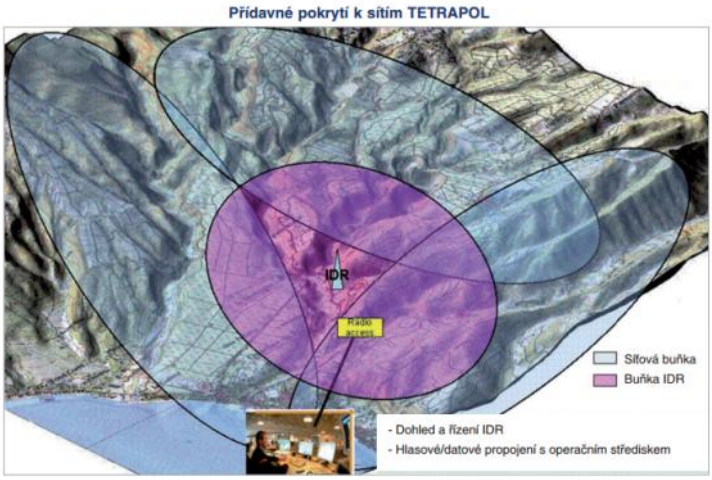
- hlasový VCH,
- datový DCH.

2.3.2 Přímý režim

Přímý režim slouží k přímé komunikaci mezi terminály, která není prováděna přes BTS, nebo IDR opakovač. Při tomto typu komunikace jsou všechny kanály simplexní. Znamená to, že k vysílání i příjmu se využívá jediného kmitočtu.

2.3.3 Převaděčový režim

Převaděčový režim se používá tehdy, je-li potřeba zřídit pokrytí signálem tam, kde základní pokrytí BTS chybí. Stává se tak zpravidla při dlouhodobých a rozsáhlých zásazích IZS.



Obr. 4. Příklad pokrytí IDR opakovačem. [9]

K vytvoření signálu, v podstatě nezávislé buňky, se používá nezávislý digitální IDR opakovač. Ten má jediný duplexní kmitočet a komunikace tak probíhá stejně, jako v síťovém režimu.

V ČR má každý HZS kraje k dispozici vlastní nezávislý IDR opakovač. [5]

Obr. 5. Nezávislý IDR opakovač. [5]

2.4 Další služby, které síť typu TETRAPOL nabízí

Radiokomunikační síť PEGAS, jenž je vybudována podle mezinárodního standardu TETRPOL, nabízí mnoho služeb. Ne všechny jsou v síti PEGAS využívány a nabízí se tím otázka budoucího rozvoje této sítě.

Zde jsou uvedeny některé z nabízených služeb.

2.4.1 Hovorová skupina

Hovorová skupina (Talk Group - TKG), je skupinovou komunikací účastníků, jenž do skupiny náležejí a nacházejí se uvnitř předem nadefinované geografické oblasti (skupina buněk).

Tato služba má v současnosti v ČR veliký význam. Začátkem roku 2016 začal HZS přecházet na systém hovorových skupin, které jsou vytvářeny v samotných RN regionálních sítích a zpravidla představují členění účastníků dle okresní příslušnosti.

Obr. 6. Radiostanice G3, registrovaná v Talk group. [zdroj vlastní]

2.4.2 Tísňové volání

Každý z terminálů je vybaven tlačítkem tísňového signálu. Tísňový signál upozorňuje ostatní účastníky komunikace speciálním vyzváněním a zobrazením popisu na display terminálu.

Při aktivaci tísňového volání v síťovém režimu dojde k otevření speciálního kanálu. Tento kanál má dvě varianty.

1. Nešifrovaný tísňový otevřený kanál ESOCH, jehož pokrytí náleží buňce, v které se volající radiostanice nachází a který je přístupný všem náležejícím radiostanicím bez ohledu na příslušnost k hovorové skupině, nebo flotile.
2. Krizový otevřený kanál EMOCH, který pokrývá několik buněk a je přístupný pouze pro hovorovou skupinu, v níž je daný terminál naprogramovaný.

Který z kanálů se otevře, je dáno konfigurací sítě nastavené operátorem.

Je-li terminál mimo pokrytí sítě, nebo v přímém režimu, sestaví se hovor, jehož pokrytí je omezeno radioelektrickým dosahem daného terminálu.

2.4.3 Slučování skupin

Slučování skupin je funkce, která umožňuje vytvoření hovorové skupiny, do které jsou přiřazeni příslušníci jiných hovorových skupin. Uvedené funkce se v budoucnu bude využívat při rozsáhlých zásazích IZS, kdy bude tímto způsobem vytvořena samostatná hovorová skupina pro daný zásah a nebude tak rušit radioprovoz ve zbytku sítě.

2.4.4 Scan

Scan umožňuje terminálům současnou přítomnost v několika skupinových komunikacích a to v hovorových skupinách nebo v otevřených kanálech, zadaných do seznamu scanovaných komunikací.

Scanována je potom každá aktivní komunikace. V praxi potom máme tři druhy scanování:

- neprioritní scanování,
- prioritní scanování,
- scan s prioritním poslechem.

2.4.5 Datové služby

Datové služby v síti PEGAS se v souvislosti s všeobecným rozvojem využití interaktivních systémů, založených na datovém přenosu, rozvíjejí i zde. Zatímco HZS datové služby ve své flotile využívá pouze velice omezeně, a to v rámci zasílání tzv. kódů typizované činnosti, PČR využívá těchto služeb daleko efektivněji.

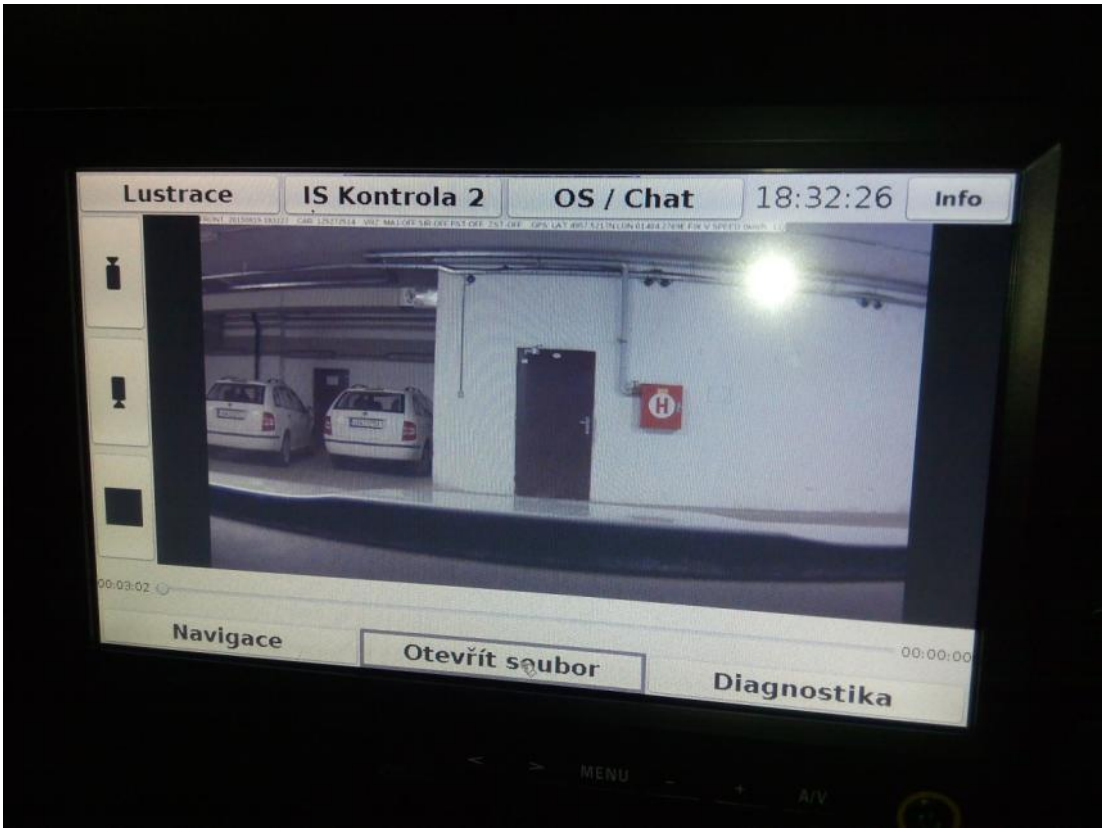
V roce 2015 a 2016 bylo pro PČR vysokými náklady, které plynuly z evropských dotací, získáno veliké množství rozšiřujících prvků pro využití datových přenosů v rámci sítě PEGAS. V současnosti PČR využívá datových přenosů nejen k dotazům do centrálních databází, ale také k přenosům obrazového záznamu a k provozu navigačního systému koncových operačních jednotek PČR.

HZS pro podobné aplikace využívá komerčních GSM a datových sítí, které nemusí obsahovat takové bezpečnostní prvky, jako síť PEGAS a především jsou zatíženy datovými toky civilních účastníků komunikace. Zbytečně tak vynakládá prostředky na vývoj stejných aplikací pro civilní sítě, jako používá PČR na terminálech PEGAS.

Systém TETRAPOL nabízí tři typy datových přenosů:

- datové služby IP,
- krátké textové zprávy SMS,
- datové přenosy.

Všechny typy datových přenosů jsou po celé dráze komunikační linky volitelně šifrované.



Obr. 7. Terminál G3 ve vozidle PČR vybavený monitorem. [zdroj vlastní]

2.4.6 Systém automatické lokace vozidel (AVL)

Systém automatické lokace vozidel slouží k distribuci dat o pozici vozidla, jenž je vybaveno vozidlovou radiostanicí s modulem pro snímání signálu systému GPS, který je vysílán družicemi z oběžné dráhy planety Země. AVL systém poskytuje monitorovací služby na kartografických stanicích.

Radiostanice vybavené AVL systémem a přijímačem GPS signálu odesílají datovou informaci o své poloze na řídící stanoviště dohledu nad regionální, nebo národní radiokomunikační sítí. Díky tomu lze efektivně v operačním procesu řízení jednotky směřovat a sledovat přímo až k místu zásahu.

Výše uvedeného systému využívá efektivně PČR k navigaci svých jednotek k místu zásahu a HZS ke sledování jednotek na stanovišti KOPIS. [4]

Obr. 8. Aplikace pro navigaci vozidel PČR, připojená na terminál G3. [zdroj vlastní]

II. PRAKTICKÁ ČÁST

3 ANALÝZA BEZPEČNOSTI A OCHRANY SÍTĚ PEGAS

Pro radiokomunikační systém TETRAPOL, na jehož standardu je v České Republice síť PEGAS provozována, je zabezpečení komunikace jednou z prioritních otázek. Tento systém používají všechny bezpečnostní sbory v ČR, včetně Policie ČR a BIS.

V následující kapitole je uveden výpis základních bezpečnostních rizik a opatření, jenž tyto hrozby eliminují, nebo je minimalizují.

Na bezpečnostní rizika hrozící síti PEGAS, lze pohlížet ze dvou hledisek.

Jsou to :

- technické poškození vysílacích a přenosových prvků infrastruktury sítě PEGAS,
- systémová a radiová napadení a narušení systému PEGAS.

3.1 Technické poškození vysílacích a přenosových prvků infrastruktury sítě PEGAS

Fyzickým poškozením vysílacích a přenosových prvků infrastruktury sítě, je myšleno:

- úmyslné mechanické poškození jedné, nebo několika součástí systému, jenž zajišťuje pokrytí území radioelektrickým signálem,
- poškození přívodu elektrické energie.

Výše uvedené způsoby jsou v podstatě ty nejsnadnější možné, kterými lze celistvost sítě porušit. Podmínkou k uskutečnění je znalost polohy vysílačů BTS. Větší problémy by však způsobilo napadení několika BTS současně. To by však vyžadovalo součinnost organizované skupiny pachatelů a dlouhodobou přípravu skupiny.

Systém sám má proti technickému způsobu napadení vytvořenou ochranu:

- záložní napájení BTS, zajištěné pomocí bateriového napájení a následného snížení vysílacího výkonu BTS,
- některé bezpečnostní sbory si v provozu ponechávají analogové radiokomunikační sítě, jako zálohu pro případ výpadku sítě PEGAS,
- přepnutí řetězců.

Právě přepínání řetězců je jako ochranný prvek v síti PEGAS, určený k ochraně při poruše nebo mechanickém napadení, nejpropracovanější.

Přepínání řetězců se týká redundantních modulů, uspořádaných do dvou řetězců. Ty jsou zařazeny v režimu aktivní - pasivní, přičemž v daném okamžiku pracuje vždy jen jeden z nich. Pasivní řetězce jsou v pohotovostním režimu.

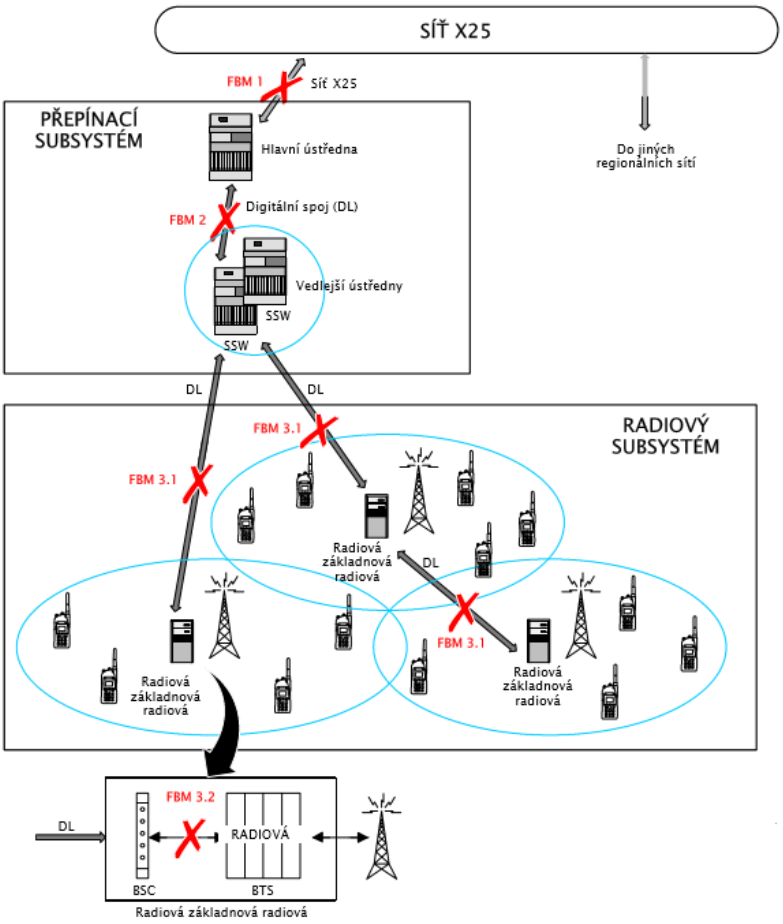
Přepínání řetězců se děje :

- automaticky - pokud aktivní řetězec vyhlásí chybu,
- místním, nebo dálkový zásahem operátora.

Je - li systém narušen, je komunikace přesměrována a je vedena jiným, dostupným okruhem. Systém se pak automaticky přepne do nouzového režimu, způsobí-li závada nebo poškození výpadek části systému. [4]

Nouzové režimy známe čtyři.

1. FBM 1 - Regionální síť, v níž došlo k výpadku spojení s páteřní sítí X25. V rámci regionální sítě je možné dále komunikovat.
2. FBM 2 -Vedlejší ústředny SSW, které ztratily spojení s hlavní ústřednou MSW. Jedna z ústředen přebírá funkci hlavní ústředny a shromažďuje informace o přihlášených terminálech. Není možné provádět datové přenosy.
3. FBM 3.1 - Radiová buňka BTS, odpojená od řídící ústředny MSW (SSW). Individuální a datové komunikace jsou přerušeny, terminály se nemohou nově přihlašovat. Nelze sestavit komunikace v síťovém režimu.
4. FBM 3.2 - U BTS dojde k přerušení spojení mezi radiovou částí stanice a částí tvořící rozhraní se sítí. Dojde k přerušení všech sestavených komunikací. Všechny terminály v pokrytí izolované buňky se stávají účastníky otevřeného jednobuňkového kanálu. Ostatní provozní kanály jsou deaktivovány. V odpojené buňce se terminál nemůže nově zaregistrovat.



Obr. 9. Grafické znázornění nouzových režimů. [4]

3.2 Systémová a radiová napadení a narušení systému PEGAS

Systému PEGAS, na kterém probíhá komunikace bezpečnostních složek MV hrozí několik rizik. Především pak:

- neoprávněný přístup k systémovým zdrojům,
- narušování sítě z vnějšku, rušení,
- napodobování účastníka,
- odposlouchávání,
- zjišťování provozu,
- odcizení, ztráta terminálu.

Systém poskytuje několik bezpečnostních mechanizmů, které eliminují možnost narušení:

- autentizace terminálů,
- šifrování komunikace,
- důvěrnost informací,
- zablokování práva provozu nebo přístupu k terminálu.

Riziko	Bezpečnostní mechanizmus
Narušení sítě Napodobování Neoprávněný přístup	Autentizace terminálů
Napodobování Odcizení, ztráta	Zákaz přístupu, provozu
Odposlouchávání Analýza provozu	Šifrování, klamání,důvěrnost

Tab. 3. Bezpečnostní mechanizmy. [zdroj vlastní]

Uvedené bezpečnostní mechanizmy jsou dále samostatně popsány.

3.2.1 Autentizace terminálu

Nový terminál, než je uveden do provozu a přidělen koncovému uživateli, prochází procesem tzv. personalizace. V praxi to znamená, že do něj musí být nainstalován příslušný firmware, který je nezbytný pro autentizaci terminálu v síti. Tento proces se provádí na stanici TPS (Terminal Programming System). Celý proces programování má několik kroků.

1. Do stanice TPS se nahraje základní projekt systému PEGAS.
2. Do stanice se nahrají základní personalizační informace, jako RFSI číslo.
3. Do terminálu se nahrají základní šifrovací klíče. (viz. 3.2.2.).
4. Na stanici TPS je vygenerován konfigurační soubor daného terminálu, který je přenesen na stanici taktického dohledu TWP (Tactical Working Position).
5. Definiční soubor je přenesen zpět na stanici TPS a do terminálu.
6. Sanice TWP aktualizuje databázi v příslušném MSW, pod který terminál spadá.

Z uvedeného postupu vyplívá, že terminál, který neprošel personalizací se nemůže do sítě přihlásit. Přihlašování terminálu do sítě poté probíhá následovně.

1. Terminál odesílá RFSI číslo, sériové číslo terminálu a TMK klíč.
2. MSW ověřuje přijatá data terminálu, pokud je terminál regionálně příslušný. Pokud tak není, dotazuje se MSW, pod který terminál patří.
3. Je-li radiostanice korektně identifikována, dostává povolení spustit uživateli nakonfigurované funkce. Zároveň je do její RAM nahráno několik klíčů s časově omezenou kryptoperiodou. (Aktualizovaný TMK, OAK, RNK, ORNK, ONNK, NNK).

Celý systém autentizace terminálů v síti je velice náročný a představuje kvalitní ochranný prvek.

3.2.2 Šifrování komunikace

Šifrování komunikací probíhá po celé délce přenosu informace a je jednou z hlavích výhod systému TETRAPOL.

Šifrování probíhá:

- v celé síti pro hlasové komunikace,
- v regionální síti pro datové komunikace,
- mezi terminály v přímém a převaděčovém režimu (IDR).

Šifrování neprobíhá:

- při provozu tísňových otevřených kanálů ESOCH,
- při komunikaci v izolovaných buňkách v nouzovém režimu FBM 2/3.

Uživatel se může rozhodnout, že nevyužije šifrování a to jak v přímém, tak i v převaděčovém režimu. Systém dokáže řídit komunikace šifrované i nešifrované.

Šifrování v síti TETRAPOL je založeno na výměně klíčů mezi terminálem, MSW a KMC. Klíče jsou generovány KMC a MSW. Každý z klíčů má jinou kryptoeriodu. Obměnu klíčů podle typu provádí buď operátor, nebo síť sama automaticky.

Do oblasti kryptografického zabezpečení spadá i středisko klíčového hospodářství a Jednotka pro zavádění klíčů.

3.2.2.1 Středisko klíčového hospodářství KMC

Je to počítač vybavený operačním systémem UNIX, v němž je uložen systém řízení databáze a aplikace KMC.

Hlavní úlohou je generovat a řídit klíče nezbytné pro šifrování komunikací.

Je tvořen:

- komunikačním prostředím X25, které slouží k distribuci klíčů do hlavní ústředny přes síť X25,
- šifrovací deskou, která šifruje a slouží jako generátor náhodných klíčů.

Seznam hlavních klíčů.

1. PK - úvodní programovací klíč obsahující šifrovací parametry ASICu hlavní ústředny a terminálu
2. MK - základní klíč KMC používaný k ochraně důvěrných dat, uložených na harddisku KMC.
3. MMK - základní klíč k MSW, používaný ke vzájemné autentizaci mezi KMC a MSW, zajišťuje zabezpečený přenos citlivých informací mezi dvěma RN.
4. TMK - základní klíč terminálu používaný k autentizaci mezi terminálem a domácí MSW, domácí MSW obsahuje všechny klíče TMK terminálů v regionální síti.
5. TKK - distribuční klíč terminálu, sloužící k šifrování a dešifrování ostatních klíčů.
6. OAK - autentizační klíč terminálu v organizaci.
7. RNK - šifrovací klíč komunikací mezi různými organizacemi stejné regionální sítě, může být použit při individuálním hovoru v několika regionálních sítích.
8. ORNK - šifrovací klíč komunikací členěných podle organizací.
9. NNK - šifrovací klíč komunikací, společný pro všechny organizace v síti.
10. ONNK - šifrovací klíč komunikací jedné organizace na úrovni národní sítě.
11. DMK - šifrovací klíč komunikací v přímém nebo převaděčovém režimu. Uživatel může klíč změnit přes MMI na svém terminálu.
12. INK - klíč sloužící ke vzájemné autentizaci mezi MSW a k šifrování při výměně klíčů mezi regionálními sítěmi.

Název	Počet klíčů	Generování klíče	Distribuce klíče
PK	1 na projekt	KMC (přes MMI) nebo MSW (přes KLU) pro sítě bez KMC	Ke každé MSW: přes KLU. Ke každému terminálu: přes TPS.
MK	1 na KMC	KMC (přes MMI)	
MMK	1 na MSW	KMC (přes MMI) nebo MSW (přes KLU) pro sítě bez KMC	Ke každé MSW: přes KLU.
TMK	1 na terminál	MSW (automaticky nebo přes MMI na TWP)	Ke každému terminálu: přes TPS. K síti: přes KLU.
TKK	1 na rad. Term.	MSW (automaticky nebo přes MMI na TWP)	Ke každému terminálu přes radiové rozhraní.
OAK	1 na org. a RN	MSW (automaticky)	Ke každému terminálu přes radiové rozhraní.
RNK	1 na RN	MSW (automaticky)	Ke každému terminálu přes radiové rozhraní,
ORNK	1 na org. a RN	MSW (automaticky)	Ke každému terminálu přes radiové rozhraní.
NNK	1 na síť	KMC (automaticky nebo přes MMI)	Ke každému terminálu přes radiové rozhraní, k MSW přes X25.
ONNK	1 na organizaci	KMC (automaticky nebo přes MMI)	Ke každému terminálu přes radiové rozhraní, k MSW přes X25.
DMK	1 na organizaci	KMC (přes MMI) nebo MSW (přes KLU) pro sítě bez KMC	Ke každému terminálu přes TPS.
INK	1 na RN	KMC (automaticky nebo přes MMI)	K MSW přes X25.

Tab. 4. Seznam hlavních klíčů. [zdroj vlastní]

- Žlutě označený klíč je generován v páru (N, N+1).
- Červeně označené klíče jsou generovány v trojici (N-1, N, N+1).

3.2.2.2 Jednotka pro zavádění klíčů KLU

Jednotka pro zavádění šifrovacích klíčů je počítač s operačním systémem Windows. Má za úkol přenášet šifrovací klíče mezi KMC, MSW a terminály. Je vybavena spojovacími komponenty pro spojení s KMC, MSW a terminály.

3.2.3 Důvěrnost informací

Důvěrnost je zajišťována dvěma způsoby.

1. Přenosem vyplňovacích rámců, což znamená, že do některých kanálů se odesílají prázdné rámce simulující provoz.
2. Používáním dočasné identity terminálu. V tomto případě síť propůjčí terminálu dočasnou identitu, které využívá vždy při komunikaci se sítí. Není potom nutné přenášet adresu terminálu. Identita se propůjčuje na nespecifikovanou dobu.

3.2.4 Zablokování práv a přístupů

Terminály mohou být v případě ztráty nebo odcizení blokovány. Známe dva stupně blokování:

1. Pozastavení provozu terminálu operátorem TWP. Při pozastavení terminál ztrácí možnost přenášet komunikaci v kterémkoliv systémovém režimu, zůstává však zaregistrován, aby bylo možné ho v síti lokalizovat. Opětovné uvedení do provozu provádí operátor TWP vzdáleně.
2. Zablokování terminálu operátorem TWP. Terminál ztrácí možnost vysílat nebo přijímat komunikace v kterémkoliv systémovém režimu. Opětovné uvedení do provozu se provádí v servisním středisku.

Terminály je dále možné vybavit vstupním PIN kódem.

3.3 Další ochranné a bezpečnostní prvky

Mezi jeden z dalších bezpečnostních prvků, používaných u HZS jistě patří režim hospodaření s terminály. U HZS jsou terminály ke každodenní práci přidělovány po ranní zkoušce proti podpisu. HZS provozuje 24 hodinový režim pracovní doby a k předávání terminálů dochází vždy při střídání sloužící směny. Tento fakt zaručuje, že odcizený, nebo ztracený terminál je pohřešován vždy nejdéle za 24 hodin.

Dalším bezpečnostním prvkem, který je instalován přímo v terminálech, je omezení doby zaklíčování. Nemůže se tedy stát, že by terminál zůstal zaklíčován, například chybou obsluhy a vyřadil by tak z provozu zbytek sítě, používající sejný kmitočet, na dobu delší než jedna minuta.

Jako poslední bych chtěl zmínit možnost vyhledávání signálů rušení kmitočtového pásma.

HZS Středočeského kraje provozuje speciální vozidlo spojové služby, jenž je vybaveno dvojicí speciálních přijímačů:

- všeobecný širokopásmový přijímač,
- přijímač s pevnou azimutární anténou.

Vyhledávání probíhá tak, že se nejdříve změří přesná frekvence rušivého zdroje a ten je pak postupným zaměřováním z více různých míst pomocí triangulace určen s přesností +/- 50m. Zaměřovací směrová anténa je pevná. Je proto nutné vozidlo vždy orientovat přesně na sever, nebo změřit a vypočítat korekční odchylku zaměření signálu.

Vozidlo je dále vybaveno dvojicí digitálních a analogových terminálů a nabíjecí soupravou pro několik ručních stanic.

Obr. 10. Vozidlo spojové služby. [zdroj vlastní]

Obr. 11. Radiokomunikační vybavení vozidla spojové služby.

[zdroj vlastní]

4 VYHODNOCENÍ BEZPEČNOSTNÍ ANALÝZY

Vzhledem k tomu, že standard sítě TETRAPOL byl již od samého počátku vyvíjen jako zabezpečený a neveřejný, tedy předem určený pro použití bezpečnostními složkami pro utajenou komunikaci, lze předpokládat jeho vysoký stupeň odolnosti proti napadení.

Přímo se tak nabízí možnost porovnání jeho zabezpečení s jinými systémy, jenž jsou na území České republiky provozovány (GSM), nebo bylo o jejich zřízení uvažováno.

Proto je vhodné si tyto systémy alespoň krátce představit.

4.1.1 GSM

GSM (Globální Systém pro Mobilní komunikaci, Groupe Spécial Mobile) je mezinárodní, nejrozšířenější, standardizovaný systém pro komunikaci mobilními telefony. Zaregistrován byl v roce 1982 a v současnosti ho používá více než 5 000 000000 účastníků.

Systém GSM je buňkový, fungující na několika radiových frekvencích, struktura sítě je hvězdicová.

Bezpečnostní GSM standard je založen na čtyřech základních bodech:

- autentizace uživatele,
- utajení identity uživatele,
- utajení signalizace,
- utajení přenášených dat (šifrování).

4.1.2 TETRA

TETRA je radiokomunikační systém vyvíjený od roku 1989 pro užití v civilním sektoru. Systém TETRA má najít využití především v oblasti velkých průmyslových firem, taxislužeb, servisních týmů apod.

Výhodou systému TETRA (ale i systému TETRAPOL), oproti sítím GSM je nezávislost komunikace při absenci pokrytí sítí v přímém režimu spojení.

V současnosti je systém TETRA používán jak pro komerční účely (v ČR 13 sítí), tak i pro zabezpečení národních komunikačních sítí (v ČR TETRAPOL) v některých Evropských státech.

Síť TETRA je sítí trunkového typu s hvězdicovou architekturou, v České Republice provozována firmou Pramacom Prague (stejně jako TETRAPOL),dodavatelem zařízení je firma Airbus Groupe (stejně jako TETRAPOL).

Zabezpečení sítě je podobné jako u TETRAPOLU. [8]

4.2 Zabezpečení z hlediska možného systémového napadení sítě

Systémové zabezpečení sítě PEGAS je podrobně popsáno v oddílu 3.2

Sítě typu GSM i TETRPOL nabízejí obdobné systémy zabezpečení, vyskytují se zde však jisté odchylky.

Výhody TETRAPOLU jsou dány především jeho kryptografickým zabezpečením. Komunikace je zde standardně šifrována po celé dráze přenosu, což např. systém TETRA neumožňuje. Webové stránky firmy Pramacom nabízejí E2EE (End to End) šifrování na smart kartách, podrobnosti o tomto uváděném faktu se však nepodařilo získat. E2EE šifra by měl být založena na Diffie - Hellman protokolu.

Sítě typu GSM jsou zabezpečeny pro radiový přenos protokoly A3 - A8, jenž jsou definovány standardem GSM. V České republice je používán protokol A5. Tento protokol je od roku 2009 plně prolomitelný a to dokonce v reálném čase. Prolomení protkolu A5 bylo popsáno Ianem Goldbergem a Davidem Wagnerem z University of California.

Samotný útok na GSM síť pak probíhá způsobem "main in the middle". V praxi to znamená umístění zařízení do dráhy přenosu, které se pro telefon tváří jako vysílač BTS a pro skutečnou BTS jako telefon. Celý proces je v podstatě jednoduchý a realizovatelný díky slabině šifry A5 a faktu, že síť se nemusí telefonu nijak autorizovat. Odposlech pak probíhá v reálném čase. Navíc lze tímto postupem odbourat i další bezpečnostní prvek GSM sítě a tzv. frequency hopping, jenž je v praxi realizován pseudonáhodnou sekvencí změn radiových frekvencí, používaných ke komunikaci.

Všichni poskytovatelé GSM sítí jsou navíc zákonem povinováni zřídit tzv. legální odposlech (LI - legal interception). Ten pak již kontrolován operátorem není.

Zrážející je potom fakt, že více než třetina důležitých služebních hovorů PČR probíhá po sítích GSM. [7]

V závěrečném shrnutí této podkapitoly je tedy možné konstatovat, že zabezpečení radiokomunikační sítě PEGAS, typu TETRAPOL, z hlediska systémového, je nejsilnější ze všech porovnávaných sítí a v praxi je téměř neprolomitelné.

4.3 Zabezpečení z hlediska technického napadení jednotlivých částí sítě

Z bezpečnostního hlediska, jsou nejohroženějšími prvky celé infrastruktury sítě vysílací stanice BTS. Na nich se nacházejí nejen vysílače, ale i antény pro mikrovlnné spojení s řídícími prvky sítě.

Vzhledem k tomu, že se 80% vysílačů BTS z celkového počtu 220 nachází na společných stožárech jako ostatní komerční vysílače (jak GSM, tak i TETRA), lze předpokládat, že útok, který by byl veden na komerční vysílač by rovněž poškodil i vysílač PEGASu.

Většina komerčních vysílačů je především kvůli svému odlehlému umístění zabezpečena systémy PZTS. Styl a způsob provedení zabezpečení je různý.

Stále je však možné nalézt vysílače, které jsou jednak nevhodně umístěny, ale i nezabezpečeny.

Z vlastní zkušenosti mohu uvést příklad. Jedná se o BSS umístěnou na sdruženém stanovišti s ostatními komerčními vysílači. Všechny vysílací a spojové prvky jsou umístěny na střeše objektu, kde město Hořovice provozuje sociální byty.

Komerční vysílače jsou zabezpečeny, jediný vysílač PEGAS má pojistkovou skříň přívodu elektrické energie umístěnou na volně přístupné chodbě a označenou nápisem Policie ČR.

Tato pojistková skříň navíc není nijak monitorována, nebo jinak zabezpečena proti vniknutí.

Při podrobném pátrání by se takovýchto nedostatečností dalo jistě nalézt mnoho po celém území ČR.

V technickém zabezpečení radiokomunikační sítě PEGAS tedy spatřuji největší slabinu celého systému.

Obr. 12. Budova s nezabezpečeným vysílačem BSS. [zdroj vlastní]

5 BUDOUCNOST A DALŠÍ MOŽNÝ ROZVOJ RADIOKOMUNIKAČNÍ SÍTĚ PEGAS

Vývoj mobilních technologií prodělal za posledních třicet let obrovský technologický skok. Od hovorových přenosů a krátkých sms zpráv se dostáváme k datovým službám, které se neustále zrychlují. Přenos obrázků a videozáznamů ve vysokém rozlišení v reálném čase není ničím neobvyklým.

Výše uvedené skutečnosti jsou si řídící a bezpečnostní složky státní moci vědomé a v modernizaci a přechodu k novým technologiím vidí budoucnost radiokomunikační sítě PEGAS.

V tomto směru proběhlo v roce 2014 zakázkové porovnání pro MV. Jeho cílem bylo finanční a funkční porovnání dvou systémů a to TETRAPOL a TETRA. Předmětem zkoumání bylo zabezpečení přenosů obou systémů a porovnání nákladů na modernizaci sítě TETRAPOL, nebo vybudování zcela nového systému standardu TETRA.

Z výsledku zkoumání zcela jasně vyplívá, že ekonomičtější a bezpečnější je použití stávající infrastruktury a přestavba sítě PEGAS na síť nové generace.

Zmiňované porovnání je přiloženo jako příloha.

V současnosti je realizován přechod k novým terminálům typu G3 a k systému tzv. Talk groupe, které svojí podstatou odlehčují provoz a zatížení sítě.

Rovněž sbory dobrovolných hasičů by měli být do budoucna vybavovány terminály TETRAPOL generace G2 a měla by pro ně být vyčleněna samostatná flotila na stávající pozici 6 - záloha HZS.

V programovacím období 2014 - 2020 je plánována výměna hardwaeru sítě PEGAS tak, aby bylo možné spustit technologie IP Broadband a LTE Professional.

Tím by se několikanásobně zvýšil možný datový tok sítí a její využití by přinášelo nový smysl jejímu provozování.

Technologie IP Broadband je součástí terminálů G3. které jsou v současnosti uváděny do provozu a pokrytí území touto technologií bylo na konci roku 2015 hotovo z 11%. Tento projekt byl financován Evropskou Unií a celkové náklady dosáhly 354 646 635Kč. Doplnění technologií LTE Professional by mělo probíhat od roku 2018.

Celkové náklady, které v sobě představují výměnu hardweru, poplatky za licenci jsou odhadnuty na 1,15 mld. Kč a je plánováno je čerpat z dotací Evropské Unie IROP.

Lze tedy konstatovat, že budoucí využití a rozvoj radiokomunikační sítě PEGAS v České republice je zaručen a s největší pravděpodobností bude financován z prostředků Evropské Unie.

Obr. 13. Zástavba terminálu G3 ve vrtulníku PČR.

[zdroj vlastní]

ZÁVĚR

Cílem této bakalářské práce mělo být představení a zhodnocení bezpečnostních prvků radiokomunikační sítě PEGAS. Na zabezpečení bylo nahlíženo jak z hlediska technického, tak i z hlediska systémového.

Výsledky této analýzy byly následně porovnány se dvěma druhy radiokomunikačních sítí, které se v České republice používají.

V celkovém shrnutí lze konstatovat, že systémové zabezpečení sítě PEGAS je na velmi vysoké úrovni a z porovnávaných sítí dosahuje nejlepších výsledků.

Zabezpečení technické naopak zaostává za konkurenty a vykazuje hrubé nedostatky. Doufejme, že společně s probíhající modernizací sítě bude pamatováno i na technické zabezpečení základních prvků infrastruktury systémy PZTS.

Vzhledem k nákladům, které již byly na vybudování radiokomunikační sítě PEGAS vynaloženy a budou nejbližší době investovány do celkové modernizace a transformace do sítě III. generace, by bylo jistě vhodné pomýšlet i na ochranu základních prvků systému. Radiokomunikační síť PEGAS, je základním prvkem krizové infrastruktury a tak by se k němu mělo i přistupovat.

Výsledky bakalářské práce ukazují, jak snadno narušitelný je komunikační prvek, jenž je určen pro dorozumívání a řízení bezpečnostních složek, zasahujících jak při živelných pohromách, tak i při zásazích kriminálního charakteru.

Tvorba této bakalářské práce pro mě byla v mnoha ohledech velice přínosná.

Při sledování základních bezpečnostních prvků jsem se dozvěděl spoustu zajímavých a profesně přínosných informací nejen o radiokomunikačním systému PEGAS, ale o radiokomunikaci obecně. Stejně přínosnou pro mě byla tato bakalářská práce i v oblasti kryptografie, která mě osobně zajímá.

Získané poznatky bych v budoucnu jistě rád převedl do praxe a na nalezené nedostatky upozornil odpovědné osoby.

SEZNAM POUŽITÉ LITERATURY

[1] BC. HÁNA, Ivo. *Digitální radiokomunikační systémy Tetrapol a Tetra*. Ostrava, 2009. Diplomová práce. Vysoká škola báňská - Technická univerzita Ostrava. Vedoucí práce Doc. Dr. Ing. Aleš Dudáček.

[2] ČESKÁ REPUBLIKA. Vypracování návrhu technického řešení propojitelnosti složek IZS. In: *Usnesení vlády ČR*. 1993, ročník 1993, číslo 246.

[3] G3 TPH 700 - Jupiter: Spojová služba. *HZS* [online]. Praha: HZS ČR, 2014 [cit. 2016-05-23]. Dostupné z: http://www.hzscr.cz/clanek/g3-tph-700-jupiter.aspx

[4] MATRA NORTEL COMMUNICATIONS. *Provozní dokumentace PMR*. Bois d´Arcy, France : EADS Defence and Security Networks, 2002.

[5] Nezávislý digitální opakovač - IDR. *HZS* [online]. Praha: HZS ČR, 2014 [cit. 2016-05-23]. Dostupné z: http://www.hzscr.cz/clanek/nezavisly-digitalni-opakovac-idr.aspx

[6] Radiokomunikační síť integrovaného záchranného systému „PEGAS“: PEGAS. *MVCR* [online]. Praha: Ministerstvo vnitra ČR, 2016 [cit. 2016-05-23]. Dostupné z: http://www.mvcr.cz/clanek/radiokomunikacni-sit-integrovaneho-zachranneho-systemu-pegas.aspx

[7] Radiová síť PEGAS: Tetrapol. *Kmitočty: Original Czech Radiomonitoring Website* [online]. Praha: Martin Kukla, 2014 [cit. 2016-05-23]. Dostupné z: https://www.kmitocty.cz/?p=198

[8] Srovnání Tetra Tetrapol. *Pamacom* [online]. Praha: MVCR, 2016 [cit. 2016-05-23]. Dostupné z: www.mvcr.cz/soubor/srovnani-tetra-tetrapol-pdf.aspx

[9] Systém PEGAS. *Pamacom* [online]. Praha: Pramacom, 2016 [cit. 2016-05-23]. Dostupné z: http://www.pramacom.cz/cs/system-pegas

[10] Zajímavé BTS: Dublinský BTS lesík. *GSMweb* [online]. Praha: GSM web, 2009 [cit. 2016-05-23]. Dostupné z: http://www.gsmweb.cz/blog/category/zajimave-bts/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AČR	Armáda ČR
ASIC	Digitální obvod navržený pro specifické použití
AVL	Systém automatické lokace vozidel
BIS	Bezpečnostní informační služba
CCH	Řídící kanál
ČTÚ	Český telekomunikační úřad
ČR	Česká republika
DCM	Datový kanál
E2EE	End to End kryptografický protokol
EMOCH	Krizový otevřený kanál
EPC	Stanoviště kontroly a technických údajů a událostí
ESOCH	Nešifrovaný otevřený tísňový kanál
EU	Evropská unie
GPS	Globální poziční systém
GSM	Globální systém pro mobilní komunikaci
HZS	Hasičský záchranný sbor ČR
IDR	Nezávislý digitální opakovač
IP	Internetový protokol
IROP	Systém řízení dotací Evropské unie
IZS	Integrovaný záchranný systém
KLU	Jednotka pro zavádění klíčů
KOIPS	Krajské operační a informační středisko
KMC	Stanoviště klíčového hospodářství
LI	Legal interception - legální odposlech

LTE	Lomg Term Evolution - technologie vysokorychlostního internetu
MD	Provozní server
MMI	Multi media interface
MSW	Main switch - řídící jednotka
MV	Ministerstvo vnitra
PC	Personal computer - osobní počítač
PČR	Poicie ČR
PIN	Personal identification number - bezpečnostní vstupní kód terminálu
PZTS	Poplachové zabezpečovací a tísňové systémy
RAM	Operační paměť
RBS	Radio base station - Radiová základnová stanice
RFSI	Identifikátor radiostanice
RN	Regional network - regionální síť
SADP	Samostatné dispečerské stanoviště
SCPS	Stanice programování mikropočítačových karet
SMS	Short message service - krátká textová zpráva
SS, T-SS	Podřízené základnové stanice
SSW	Secondary switch - vedlejší radiová základna
TCH	Provozní kanál
TMP,TDP	Stanoviště technického dohledu
TKG	Talk group - hovorová skupina
TPS	Stanice programování terminálů
TWP	Stanoviště taktického řízení
VCH	Hlasový kanál
X25	Standardní komunikační linka
ZZS	Zdravotnická záchranná služba

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: SROVNÁNÍ MODERNIZACE STÁVAJÍCÍ RADIOKOMUNIKAČNÍ SÍTĚ S VARIANTOU POŘÍZENÍ ZCELA NOVÉ RADIOKOMUNIKAČNÍ SÍTĚ

Srovnání modernizace stávající radiokomunikační sítě s variantou pořízení zcela nové radiokomunikační sítě

Zdroj textu: MV et eNovation. Studie proveditelnosti projektu *Rozvoj radiokomunikační sítě integrovaného záchranného systému PEGAS.* Praha, leden 2014

V případě, že by v současné době bylo rozhodnuto realizovat nový systém na bázi jiné technologie, přicházela by v úvahu pouze technologie TETRA, neboť jde o jedinou další existující technologii, která umožňuje srovnatelné funkcionality a úroveň zabezpečení jako technologie Tetrapol.

Systém **Tetrapol** byl vyvíjen od roku 1987 a byl **vytvořen pro specifické potřeby ochránců bezpečnosti** – umožňuje skupinové komunikace, snímání komunikace a slučování různých flotil, tísňová volání (rovněž v přímém režimu), hovory s vyšší prioritou umožňující vynucené obsazení zdrojů nebo zabezpečené datové přenosy.

Systém **TETRA** byl vyvíjen od roku 1989 a byl **vytvořen pro operátory veřejně přístupných mobilních radiokomunikačních systémů** (PAMR) jako jsou taxislužba, autobusy, servisní týmy atd.

Obě technologie vycházejí z principů moderních digitálních TDMA/FDMA (CDMA) sítí typu GSM s tím rozdílem, že umožňují kombinovat hlavní výhody klasických analogových radiostanic s výhodami stanic komunikujících v digitálních sítích.

Jednou ze zásadních předností radiostanic TETRA i Tetrapol je jejich **nezávislost na síti v mobilním provozu**, tedy možnost přímého spojení dvou blízkých radiostanic bez zprostředkování převaděčem (základnovými stanicemi a ústřednami), včetně možnosti spojení ruční nebo vozidlové stanice, která se nachází mimo dosah základnových stanic (převaděčů) na převaděč přes jinou ruční nebo vozidlovou radiostanici.

Oba systémy dokážou pracovat v režimu skupinových volání a umožňují datové přenosy, včetně automatické lokalizace poloh vozidel či hlídek (služba AVL).

Provoz hlasových i datových služeb v obou sítích je šifrovaný (po celé cestě přenosu však pouze u technologie Tetrapol) a sítě jednotlivých uživatelů jsou zabezpečeny samostatnými šifrovacími klíči, díky kterým není možné zařízení z jedné uzavřené sítě provozovat v jiné uzavřené síti. Zabezpečení je vícestupňové a tak zajišťuje pro civilní, také vládní i vojenské účely vysoký stupeň utajení přenášených dat a hlasové komunikace.

Technologie TETRA byla představena tři roky po technologii Tetrapol a tím se stala konkurenčním systémem. Zatímco technologie Tetrapol má jediného výrobce a pouze ten může také provádět servis veškerého hardware, protokol a systém TETRA jsou zveřejněny, standardizovány a proto se touto technologií zabývalo více výrobců současně (Motorola, Rohde & Schwarz, Sepura, Nokia, HYT, SELEX, Teltronic…). Mezi výrobci technologie TETRA byla po akvizici firmy Nokia i firma EADS, která byla rovněž monopolním výrobcem technologie Tetrapol. Nástupcem firmy EADS, a tedy nynějším výrobcem technologie TETRA i monopolním výrobcem technologie Tetrapol, byla firma Cassidian, v posledních měsících pak firma Airbus.

V ČR je v současné době v provozu 13 sítí na bázi technologie TETRA. První síť od roku 2002 (summit NATO) má hlavní město Praha, kde je registrováno více než 4000 radiostanic (městská policie cca 1500, dopravní podnik cca 2500, krizový štáb cca 100,

technická správa komunikací cca 80). Dalšími sítěmi disponují letiště Praha-Ruzyně, vojenské letecké základny Kbely, Čáslav, Pardubice a Přerov, vojenské prostory Doupov a Libavá, městské radiové systémy jsou v Brně, Liberci a Českých Budějovicích a podnikové radiové systémy mají Hyundai Nošovice a Chemopetrol Litvínov.

Tab. 1. Technické srovnání technologií Tetrapol a TETRA

Technologie	Tetrapol	TETRA
Modulace	GMSK[1] (na bázi GSM)	π/4 DQPSK[2] (na bázi DAMPS)
Přístupová metoda	FDMA[3] (jednodušší realizace)	TDMA[4] (menší pokrytí)
Odstup nosných kmitočtů	10 kHz nebo 12,5 kHz	25 kHz
ETSI[5] 300 113 – koexistence s analogovým rádiem	ANO	NE
Schválení FCC[6]	ANO	NE
Citlivost příjmu základnových stanic (statická / dynamická)[7]	-121 dBm / -113 dBm	115 dBm / -106 dBm
C/I dynamická	15 dB	19 dB
Poloměr buňky (dosah základnové stanice) pro ruční terminál / předměstí[8]	8 km (hlas i data)	3,8 km (jen hlas)
Poloměr buňky (dosah základnové stanice) pro vozidlový terminál / venkov	28 km (hlas i data)	17,5 km (jen hlas)

Zdroj: TETRAPOL versus TETRA. Bezpečnost obyvatelstva. EDSN short presentation – version 03. EADS Telecom. Ppt prezentace.

U technologie TETRA je díky jiné technologii přenosu digitalizovaných toků hlasové a datové komunikace nutné počítat cca **s trojnásobným počtem základnových stanic**, tj. cca 800 základnových stanic, kdežto v síti Pegas se provozuje 222 základnových stanic, optimum by bylo cca 250. Konsorcium EADS, které bylo výrobcem obou technologií, uvádí, že **síť Tetrapol je levnější o cca 30 % v kapitálových a o cca 40 % v provozních nákladech než síť TETRA**.[9]

[1] Gaussian Minimum Shift Keying

[2] Differential Quadriphase Shift Keying

[3] Frequency Division Multiple Access. Mnohonásobný přístup do sítě, kdy jeden účastník je od ostatních účastníků oddělen frekvenčně – celé frekvenční pásmo je rozděleno na určitý počet radiových kanálů, které jsou přiřazovány jednotlivým účastníkům, každý účastník má pro sebe po celou dobu spojení vyhrazeno nepřetržitě celé frekvenční pásmo radiového kanálu.

[4] Time Division Multiple Access. Mnohonásobný přístup do sítě, kdy jeden účastník je od ostatních účastníků oddělen v čase – každý účastník má pro sebe po dobu spojení vyhrazen v celém frekvenčním pásmu radiového kanálu jeden nebo více časových intervalů (timeslotů), do kterých je vkládána přenášená informace.

[5] European Telecommunications Standards Institute. Nejvyšší evropský standardizační úřad v oblasti pevných i mobilních telekomunikačních technologií.

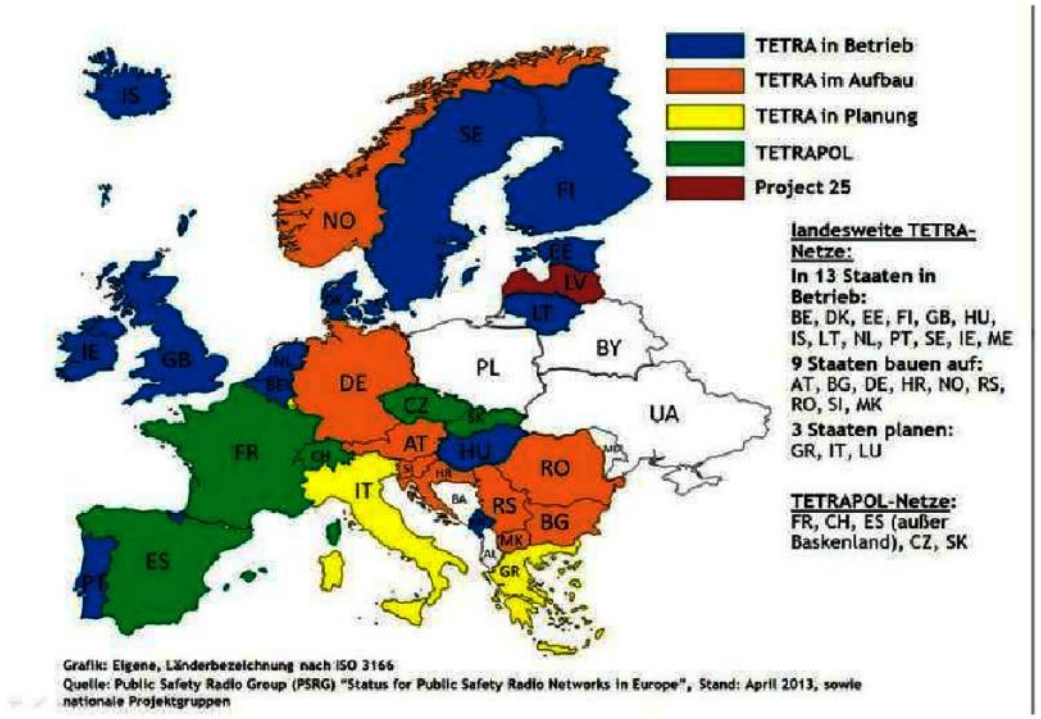
[6] The Federal Communications Commission of the United States.

[7] zpráva ERO/CEPT (The European Conference of Postal and Telecommunications Administrations) 52, prosinec 1997

[8] zpráva ITU-R M. 2014 (International Telecommunications Union – Mezinárodní telekomunikační unie, nejvyšší standardizační telekomunikační úřad), březen 1998

[9] Ppt prezentace firmy EADS.

Obr. 1. Celostátní sítě Tetrapol a TETRA v Evropě



Zdroj: http://www.bdbos.bund.de/DE/Digitalfunk_BOS/Digitalfunk_in_Europa/digitalfunk_in_europa_node.html#Start

V rámci přípravy projektu PEGAS bylo provedeno **několik odhadů investiční náročnosti případné výstavby nového národního radiokomunikačního systému IZS na bázi technologie TETRA**:

- Odborný odhad České pošty, a. s., Odštěpný závod ICT služby, která je provozovatelem sítě informačních a komunikačních technologií Ministerstva vnitra, uvádí částku **cca 5,5 mld. Kč bez radiostanic**.
- Srovnáním s výstavbou celostátní sítě TETRA resortu vnitra Spolkové republiky Německa lze, při cca 4,5násobné rozloze SRN oproti ČR odhadnout, že v ČR by zřízení sítě TETRA stálo 5,1 mld. €[10] / 4,5 = **okolo 28 mld. Kč**.
- Srovnáním s výstavbou celostátní sítě TETRA resortu vnitra Rakouské republiky lze, při srovnatelné rozloze Rakouska jako ČR odhadnout, že v ČR by zřízení sítě TETRA stálo 0,6 mld. €[11] = **okolo 15 mld. Kč**. Původní rozpočet rakouského ministerstva vnitra na síť TETRA Adonis byl dvojnásobný, tj. **okolo 30 mld. Kč**, a mj. i proto byl po dvou letech tento projekt zrušen.
- Srovnáním s výstavbou celostátní sítě TETRA britské policie lze, při cca 3,1násobné rozloze Velké Británie oproti ČR odhadnout, že v ČR by zřízení sítě TETRA stálo 2,9 mld. £[12] / 3,1 = **okolo 34 mld. Kč**. Britská síť má 3 roky zpoždění v realizaci a nyní ji využívá pouze 15 % policejních sil.

[10] http://de.wikipedia.org/wiki/Digitalfunk_der_Beh%C3%B6rden_und_Organisationen_mit_Sicherheitsaufgaben
[11] http://de.wikipedia.org/wiki/Funksystem_der_BOS_in_%C3%96sterreich
[12] http://www.tetrawatch.net/national/index.php

Tab. 2. Přehled významných realizovaných a plánovaných výdajů v síti Pegas

Investice MV a jeho složek	Tetrapol (Pegas) v běžných cenách	z toho financováno z fondů EU	TETRA (odpovídající investice by dnes byla)
již realizované			
do roku 2003 na straně provozovatele i na straně uživatelů (Policie, HZS, ZZS) v poměru cca 2:3 • 219 základnových stanic • 25 opakovačů • 43 rádiových ústředen • digitální trasy a další technologie a software • 1868 dispečerských pracovišť • 16 269 ručních radiostanic • 7 659 vozidlových radiostanic • 1 191 vozidlových adaptérů pro ruční radiostanice • 390 aplikací GPS	**5,26 mld. Kč**	---	**cca 5,5 mld. Kč jen na straně provozovatele sítě (optimistický odhad)**
doplnění 2004–2006 • obdobné položky jako do roku 2003 (viz výše)			
výměna zastaralých zařízení a další menší investice v síti v letech 2007–2010 • nedokončená výměna radiostanic 1. generace za radiostanice 2. a 3. generace • nový datový portál PEGAS (2010)			
schválené a probíhající			
propojení složek IZS na síť PEGAS v rámci projektu IOP *Technologie pro operační řízení operačních středisek Policie ČR, HZS ČR a zdravotních záchranných služeb krajů* (2011–2014)	**0,06 mld. Kč**	**0,05 mld. Kč**	
pořízení 4 411 kompletů lokalizačních a záznamových zařízení do služebních vozidel krajských ředitelství Policie ČR v rámci 13 krajských projektů *Lokalizační a záznamová zařízení Policie ČR* (mimo Prahu)	**0,31 mld. Kč**	**0,23 mld. Kč**	
pořízení 4 700 ručních radiostanic sítě PEGAS pro pořádkovou a dopravní službu PČR v rámci projektu *Moderní technika a technologie Policie ČR*	**0,15 mld. Kč**	**0,13 mld. Kč**	
pořízení 1 000 ks ručních a vozidlových radiostanic sítě PEGAS v rámci 14 krajských projektů operačních středisek ZZS	**0,10 mld. Kč**	**0,09 mld. Kč**	
CELKEM dosud investováno nebo připraveno	**5,88 mld. Kč**	**0,50 mld. Kč**	
tento projekt	**0,36 mld. Kč**	**0,29 mld. Kč**	
navazující aktivity			
projekt MORAS – nezávislé opakovače signálu a ruční a vozidlové radiostanice umožňující nové funkcionality pro P ČR, HZS ČR	**0,60 mld. Kč**	**0,56 mld. Kč**	
další investice do infrastruktury systému PEGAS k optimálnímu naplnění uživatelských požadavků (nyní nejsou administrativně připraveny) • 20 nových základnových stanic • přechod na technologii IP a LTE Professional	**1,05 mld. Kč**	**0,89 mld. Kč**	

Zdroj: Ministerstvo vnitra; Policejní prezídium ČR; Pramacom, spol. s r. o. Věstník veřejných zakázek

Na základě výše uvedených informací se lze s vysokou jistotou domnívat, že odhad ceny vybudování sítě TETRA na území České republiky by byla **nejméně cca 5 mld. Kč na straně provozovatele sítě**. Tato částka zahrnuje pouze základnové stanice („vysílače") a přepínače („ústředny"), nezahrnuje radiostanice a další nutná zařízení.

Celkové náklady zde předkládaného projektu jsou 355 mil. Kč, což představuje **pouze necelých 6,5 % již realizovaných a připravených výdajů**, a cca 1-6 % odhadovaných výdajů na vybudování zcela nové radiokomunikační sítě na bázi technologie TETRA.

Kromě dříve realizovaných investic do systému PEGAS také nyní probíhají 3 investiční akce, které jsou spolufinancované z Integrovaného operačního programu a které jsou uvedeny v následující tabulce, spolu s již realizovanými výdaji na vybudování systému. **Vyřazení systému PEGAS z provozu a jeho nahrazení jiným systémem by z pohledu financování projektů z IOP znamenalo porušení podmínky pětileté udržitelnosti pořízených systémů**, a také zejména zmaření investic vložených do těchto projektů.

Závěr

Vybudování zcela nové radiokomunikační sítě na bázi jiné technologie než Tetrapol by znamenalo:

- výběr technologie TETRA,
- investiční náklady cca 5,5–34 mld. Kč, což je až 100x více než je hodnota předkládaného projektu,
- trojnásobné provozní náklady,
- zrušení udržitelnosti několika souběžně realizovaných projektů financovaných z Integrovaného operačního programu, které počítají s technologií Tetrapol.

Z výše uvedených důvodů se přechod na jinou technologii jeví jako neproveditelný a **jediným obecně platným řešením je modernizace radiokomunikační sítě na bázi nyní používaného standardu Tetrapol**.