# ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ

## Fakulta elektrotechnická

### Katedra mikroelektroniky


# Systém tísňového volání


**květen 2016**

**Diplomant:** **Bc. Petr Hrozínek**

**Vedoucí práce:** **Ing. Pavel Bezpalec, Ph.D.**

# Čestné prohlášení

**Prohlašuji, že jsem zadanou diplomovou práci zpracoval sám s přispěním vedoucího práce a konzultanta a používal jsem pouze literaturu v práci uvedenou. Dále prohlašuji, že nemám námitky proti půjčování nebo zveřejňování mé diplomové práce nebo její části se souhlasem katedry.**

**Datum: 26. května 2016** **Bc. Petr Hrozínek**

Rád bych tímto poděkoval vedoucímu práce Ing. Pavlu Bezpalcovi, Ph.D. za pomoc a trpělivost při tvorbě diplomové práce, za jeho připomínky a za čas, který mi věnoval. Dále bych chtěl poděkovat plk. Ing. Vítu Hujovi z Policejního prezidia České republiky, kpt. Ing. Janu Urbánkovi z Generálního ředitelství HZS, plk. Ing. Milanu Zobačovi a kpt. Ing. Petru Štajncovi z HZS Libereckého kraje za odborné rady a věcnou diskuzi.

České vysoké učení technické v Praze
Fakulta elektrotechnická

katedra mikroelektroniky

# ZADÁNÍ DIPLOMOVÉ PRÁCE

Student: **Bc. HROZÍNEK Petr**

Studijní program: Komunikace, multimédia a elektronika
Obor: Elektronika

Název tématu: **Systém tisňového volání**

***Pokyny pro vypracování:***

1. Podrobně a uceleně nastudujte problematiku tisňového volání .
2. Proveďte porovnání realizací této služby u nás i ve světě. Zaměřte se na prostředí "klasické" telefonie i IP telefonie.
3. Zhodnoťte dosažené výsledky jak po stránce technické, tak i ekonomické.
4. Na základě dosažených výsledků rozeberte další možná řešení.

***Seznam odborné literatury:***

[1] Neveřejná dokumentace k projektu TCTV. [dodá vedoucí práce]
[2] E911 - RFC Draft [online], dostupné z <http://www.cs.columbia.edu/sip/drafts/sip/draft-schulzrinne-sip-911-01.txt>.

Vedoucí: **Ing. Pavel Bezpalec, Ph.D.**

Platnost zadání: 31. 8. 2015

L.S.

Prof. Ing. Miroslav Husák, CSc.
vedoucí katedry

Prof. Ing. Pavel Ripka, CSc.
děkan

V Praze dne 14. 2. 2014

# Anotace

Cílem diplomové práce je popsat systém tísňového volání v České republice a v zahraničí. Podrobně a uceleně charakterizovat stávající systémy a popsat možný budoucí vývoj v této oblasti se zaměřením na využití IP telefonie.

Diplomová práce je rozdělena do dvou částí. První část se zabývá systémy tísňového volání v České republice. Podrobně popisuje systém lokalizace polohy, návrh telefonního centra tísňového volání a systém eCall.

Druhá část diplomové práce pojednává o systémech tísňového volání ve Spojených státech amerických a především systémuNext Generation 911, jenž je plně adaptován na příjem tísňového volání pomocí IP telefonie.

# Klíčová slova

Tísňové volání
TCTV
Lokalizace
Identifikace
IP telefonie

# Summary

The purpose of diploma work is to describe the emergency call system in the Czech Republic and abroad. Characterize the existing systems in detail and comprehensively and describe possible future developments in this area with concentration on the use of IP telephony.

The thesis is divided into two parts. The first part deals with emergency call systems in the Czech Republic. It describes the system of localization position in detail, the proposal of PSAP and eCall.

The second part deals with emergency call systems in the United States of America and particularly of Next Generation 911 system, which is fully adapted to receive emergency calls using IP telephony.

# Key Words

Emergency call
PSAP
Localization
Identification
IP-based telephony

# Obsah

# Úvod

Při mimořádných událostech je systém telekomunikací jedním z nejdůležitějších nástrojů pro rychlou odezvu záchranných složek a minimalizaci ztrát na životě nebo majetku. Komunikační systémy zastávají 3 důležité role - tísňová volání, nouzová komunikace a nouzové výstrahy.

Telefonní systémy, ať už založené na veřejném telefonním systému (dále jen PSTN) nebo telefonní systémy spravované státem, jsou nezbytné pro všechny 3 role.
Při přechodu z telefonního systému přepojovaných okruhů na sítě založené na přepínání paketů (IP telefonie) je nezbytné přehodnotit, jak jsou tyto služby k dispozici.

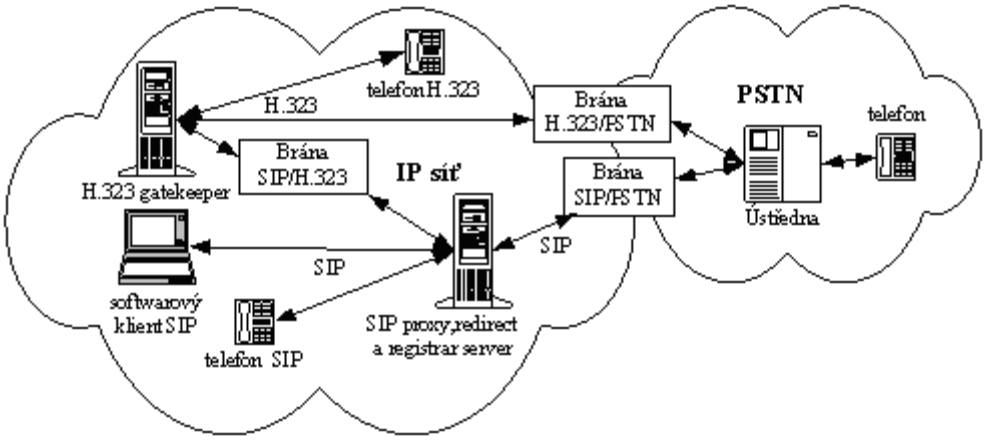
Komunikace prostřednictvím internetu přináší nové možnosti v rozvoji služeb (širší nabídka služeb, větší odolnost sítí, rychlejší reakce), nicméně pozbývá důvěry v nepřetržitém zajištění služby, bezproblémovému provozu a známého umístění terminálu.

Ve většině zemí světa mohou obyvatelé použít telefon k zavolání pomoci, ať už se jedná o zdravotní pomoc, policii nebo hasiče. Všechny tyto systémy mají 4 části:

1. Jednotné telefonní číslo - například linku 112 lze vytočit v 81 zemí světa (především se jedná o evropské země) [1], dále je to linka 911 v USA, Kanadě a několik zemí v Jižní Americe a další;
2. Směrování hovorů – hovory se sejdou ve spádovém telefonním centru tísňového volání (dále jen TCTV), do kterého volající spadá, nebo v případě vytíženosti daného TCTV bude volající automaticky přepojen na jiné (např. při živelných pohromách);
3. Identifikace volajícího – je nutné identifikovat volajícího pro případ zlomyslného volání nebo v případě, že by postižený nemohl sdělit informace ze zdravotních nebo jiných důvodů;
4. Identifikace místa volání – znalost místa události je nezbytná pro urychlení samotného zásahu, v mnoha případech není volající schopen polohu sdělit.

# 1 IP telefonie

Internetová telefonie přenáší audiovizuální záznam v podobě IP paketů po internetu a intranetových sítích. Transport a doručování paketů s audiovizuálními daty je řízeno protokolem RTP (Real-time Transport Protocol) [2] s relacemi vytvořených nejčastěji signalizačními protokoly H.323 [3] a SIP (Session Initiation Protocol) [4,5]. Protokol H.323 byl zaveden organizací ITU-T (International Telecommunication Union), a proto je svým provedením bližší telefonním standardům. Tento protokol je starší a složitější než protokol SIP. Používá binární zápis, což ztěžuje proces ladění. Z toho důvodu se pomalu přechází k protokolu SIP. Protokol SIP vznikl pod záštitou organizace IETF (Internet Engineering Task Force). Jde o textový protokol strukturou podobný například poštovnímu protokolu SMTP nebo protokolu HTTP. Tělo zprávy je tvořeno textovými položkami, které popisují předávané informace. Textová podstata protokolu napomáhá nejen jednoduchému ladění, ale především snadné rozšiřitelnosti.




Obr. 1 Architektura služby SIP[5]

Protokol SIP je typu klient-server, takže komunikace probíhá výměnou dvou typů zpráv, požadavků a odpovědí.

Typy požadavků jsou:

- INVITE: INVITE slouží k přizvání uživatele nebo služby k podílení se na relaci, tělo zprávy obsahuje popis relace (spojení);
- ACK: Potvrzení, že klient v pořádku přijal odpověď na INVITE dotaz;
- BYE: Oznámení protistraně, že hodláme ukončit hovor, metoda BYE může být vyslána jak volaným tak volajícím;

- CANCEL: Metoda CANCEL vyjadřuje přerušení zahájení relace ještě před jejím navázáním;
- REGISTER: Metoda REGISTER je používána k registraci současné adresy klienta u SIP serveru, který jí předá lokalizační službě.

Typy odpovědí jsou:

- 1xx: Prozatímní odpovědi jako požadavek přijat, vyzvání;
- 2xx: Úspěch. Požadavek je přijat, pochopen a akceptován;
- 3xx: Přesměrování. Je třeba vytvořit nový upravený požadavek;
- 4xx: Chyba klienta. Špatná syntaxe požadavku, nebo požadavek nemůže být proveden;
- 5xx: Chyba serveru. Server není schopen provést platný požadavek;
- 6xx: Globální chyba. Požadavek nelze provést na žádném serveru.

Pro funkci protokolu SIP jsou nepostradatelné hlavičky, výběrově to jsou:

- TO: Adresa volaného;
- FROM: Adresa volajícího klienta;
- VIA: Adresa klienta, který vysílá požadavek nebo adresa serverů, přes něž požadavek prošel a kudy se bude vracet odpověď;
- CALL-ID: Unikátní identifikace volání;
- CONTACT: Aktuální skutečná adresa klienta;
- RECORD-ROUTE: Seznam adres serverů, které chtějí dostávat veškerou komunikaci náležející k hovoru;
- ROUTE: Posloupnost adres serverů, přes které je požadavek směrován a klienta, ke kterému má požadavek dorazit;
- REQUEST-URI**:** Aktuální adresát požadavku. Údaj se vyskytuje v první řádce požadavku za metodou (typem požadavku).

Pro vytvoření a řízení relace musí SIP lokalizovat účastníka. Každý účastník každý účastník je buď jednoznačně identifikován pomocí telefonního čísla přiděleného dle doporučení ITU E.164 [6] nebo je identifikován URL adresou (je nezávislá na aktuální IP komunikačních prostředků). Metoda REGISTER se používá pro registraci adresy. Uživatel si může registrovat svou adresu sám, nebo to může za něj provést někdo jiný. Lze upřesnit dobu, po kterou má být adresa registrována.

Nicméně pokud klient tuto dobu neuvede, platí standardní doba jedné hodiny. Klient může zrušit existující registraci specifikováním doby registrace 0 v hlavičce EXPIRES.

Každý účastník má alespoň jeden identifikátor AOR (Address Of Record). Volající zahájí hovor odesláním SIP požadavku INVITE na místní odchozí proxy nebo SIP server v cílové doméně. Pokud je druhá strana ochotná hovor přijmout, odešle zpět odpověď OK a návratový kód „200“. Odpovědí volající strany je zpráva AKN, která potvrzuje přijetí odpovědi volaného. Poté může proběhnout samotný rozhovor. Pro ukončení hovoru musí některý z účastníků odeslat požadavek BYE, na který pro kladné vyřízení odpoví kódem „200“. Proces spojení je kompletní a může začít vlastní hovor.

Jednotlivé zprávy sestávají z posloupnosti textových hlaviček. Vytváření a rozpoznávání těchto zpráv na straně odesílatele resp. příjemce je jednodušší než u binárních zpráv. Odpadá zde problém složitého způsobu ladění s použitím analyzátoru např. ASN.1 [7]. Ukončení spojení je u SIP signalizace provedeno prostřednictvím žádosti BYE. Klient pošle serveru žádost, kterou server potvrdí odpovědí OK.

# 2 Tísňové volání v ČR

Čísla tísňového volání slouží k oznámení událostí, kdy je ohrožen život, zdraví, majetek nebo veřejný pořádek. V České republice jsou provozovány tyto linky:

- 112 Jednotné evropské číslo tísňového volání;
- 150 Hasičský záchranný sbor ČR;
- 155 Zdravotnická záchranná služba;
- 156 Obecní/městská policie;
- 158 Policie ČR [8].

Zneužití těchto linek je označováno jako zlomyslné volání. Uskutečnění zlomyslných volání je přestupkem proti právním normám, za který může Český telekomunikační úřad dle § 119, odst. 1 písm. e), zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, udělit pokutu až do výše 200.000 Kč [9]. Ve zvlášť závažných případech může být takové jednání klasifikováno jako trestný čin poškozování a ohrožovaní provozu obecně prospěšného zařízení [10].

Dle vyjádření Nikoly Šedové z ČTÚ se čísla 150, 155, a 158 se začala zřizovat v souvislosti se zaváděním automatizace meziměstského provozu od roku 1970. Na místní úrovni byla čísla zaváděna již dříve v souvislosti s výstavbou automatických ústředen pro místní provoz – systém P 51. Například v Praze byla čísla 150, 155 a 158 využívána již v roce 1969.

Linka 156 začala být zaváděna až v souvislosti se vznikem obecné policie podle zákona č. 553/1991 Sb., o obecní policii, ze dne 6. prosince 1991. Zřizování této linky bylo postupné, závislé na rozhodnutí jednotlivých obcí a podléhající možnostem směrování v tehdejších telekomunikačních sítích. Např. v Karviné byla linka zavedena v roce 1992, v Ostravě v roce 1993, v Praze koncem roku 1994 a např. v Táboře v roce 1996.

## 2.1 Jednotné číslo tísňového volání „112“

Číslo 112 je číslo tísňového volání, které je dostupné jak v pevných tak i v mobilních sítích na území Evropské unie a také v mnoha dalších státech po celém světě. Používá se v jakékoliv situaci, kdy dochází k ohrožení zdraví, života či majetku. Zejména pak v případech, kdy se jedná o kombinaci výše uvedených faktorů a volající si není zcela jist, kterou konkrétní krizovou linku zvolit. Jednotné evropské číslo tísňového volání tak propojuje všechny složky záchranného integrovaného systému, následkem čehož dochází k rychlému a efektivnímu předání nezbytných informací.

Jednotlivé nastalé situace lze rovněž řešit voláním na tísňové linky, které jsou platné na území ČR. Důležitým faktem je, že volání na tato čísla je vždy bezplatné. U tísňových linek je navíc zabezpečeno volání i v situacích, kdy:

- v telefonním přístroji není vložena SIM karta (Neplatí ve všech zemích. Země, ve kterých se bez SIM nedovoláte jsou např. Německo, Chorvatsko, Slovinsko, Belgie, Francie, Velká Británie) [11];
- volající má nulový stav kreditu [12];
- u přístroje je zablokována klávesnice nebo je volání uskutečňováno z telefonního automatu a volající nemá hotovost.

ČR je rozdělena do 14 územních celků:

- Hlavní město Praha;
- Středočeský kraj;
- Jihočeský kraj;
- Plzeňský kraj;
- Karlovarský kraj;
- Ústecký kraj;
- Liberecký kraj;
- Královéhradecký kraj;
- Pardubický kraj;
- Vysočina;
- Jihomoravský kraj;
- Olomoucký kraj;
- Zlínský kraj;

- Moravskoslezský kraj [13].

Při čemž po vytočení tísňové linky se automaticky dovoláte na příslušné centrum HZS. Je samozřejmé, že jednotlivá telefonní centra jsou navzájem hlasově i datově propojena a v případě přetížení linky nebo jiných situací je tedy hovor automaticky přesměrován na jiné telefonní centrum. Systém tísňového volání je navíc nastaven tak, aby kvalita nebo rychlost spojení nebyla přesměrováním ovlivněna.

### 2.1.1 Operátoři tísňových linek

Nedílnou součástí telefonních center tísňového volání jsou operátoři, kteří tísňové linky obsluhují.

Obr. 2 Centrum tísňového volání Ostrava [14]

Na všechny tyto operátory jsou kladeny vysoké požadavky na koncentrovanost a nelze opomenout ani jazykové požadavky – Anglický a Německý jazyk. Hovory tísňového centra jsou monitorovány a nahrávány k pozdější analýze. Operátor má vždy

k dispozici informaci o telefonním čísle volajícího a jeho přibližné polohu (zobrazenou v mapovém editoru).

Operátoři příslušného centra během hovoru zjistí co možná nejvíce relevantních informací a následně je předají všem zasahujícím složkám. Identifikace místa volání zkracuje čas potřebný pro poskytnutí potřebné pomoci. Na obr. 2 jsou zachyceni operátoři tísňových linek vykonávající dohled nad systémy centra tísňového volání.

### 2.1.2 Doporučená struktura volání

V případě vzniku situace, kdy je ohrožen život, zdraví, majetek vás nebo osob ve vašem okolí nebo životní prostředí a nejste si jisti, jakou složku IZS potřebujete kontaktovat, volejte jednotné evropské číslo tísňového volání 112.

Ať již vytáčíte linku konkrétní složky IZS nebo jednotnou linku 112, stručně a jasně popište situaci, ve které se nacházíte. Zejména uveďte:

- přesnou adresu: město, ulice a číslo popisné;
- co se děje, informace o postiženém případně postižených;
- kdy se událost stala, nebo zda se právě děje;
- informace o volajícím.

Vzhledem k tomu, že se často více volajících snaží ohlásit stejnou událost. Může operátor žádat pouze doplňující informace o události a ukončí hovor. Operátor svým jednáním zabraňuje zbytečnému opakování stejných informací a uvolňuje tísňovou linku pro další hovory.

Vždy je třeba postupovat dle pokynů a rad operátora. Nezavěšovat linku, dokud není volající operátorem tak vyzván. Pokud se situace na místě události zlepší nebo zhorší, je nutné znova kontaktovat tísňovou linku a podat o změně situace zprávu [15].

## 2.2 Zavedení jednotného evropského čísla tísňové volání 112 v ČR

### 2.2.1 Rozhodnutí č. 91/396/EEC

V roce 1991 Rada Evropského hospodářského společenství (EHS, pozn. „European Economic Community“ EEC) vydala rozhodnutí č. 91/396/EEC [16] ze dne 29. července 1991 o zavedení jednotného evropského čísla tísňového volání. Stalo se tak

především z důvodu usnadnění komunikace s tísňovými službami v rámci Evropské unie, protože došlo k výraznému nárůstu pohybu osob v rámci Evropy.

V současnosti používá každý stát svá vlastní tísňová čísla, která jsou pro cizince mnohdy neznámá a při zavolání zpravidla narazí na jazykovou bariéru. Na výše uvedeném čísle proto musí být zabezpečeno, že zpráva o mimořádné události bude přijata a bude zabezpečena adekvátní reakce. Způsob zabezpečení a odbavení musí být upraven tak, aby v daném státu co nejlépe odpovídal národní organizaci jeho nouzových systémů.

Povinnost zavést jednotné evropské telefonní číslo tísňového volání byla uložena všem členským státům s tím, že do konce roku 1996 musí být ve všech státech plně funkční. Pro přístup k tomuto tísňovému volání bylo stanoveno telefonní číslo 112.

V souvislosti se snahou České republiky zapojit se do evropského integračního procesu byly také zde zahájeny příslušné kroky k zavedení jednotného čísla tísňového volání jako jedné z podmínek členství v Evropské unii. Na základě již zmíněného rozhodnutí uvolnil Český telekomunikační úřad (ČTÚ) telefonní číslo 112, na němž byla do roku 1998 provozována služba poskytující informaci o přesném čase (služba přesného času byla přesunuta na tel. č. 14112) [17].

### 2.2.2 Usnesení Vlády ČR č. 391/2000 Sb.

O zavedení jednotného čísla tísňového volání 112 v České republice bylo rozhodnuto v usnesení Vlády ČR č. 391 +P [18] ze dne 19. dubna 2000. Toto usnesení bylo vydáno v souladu s rozhodnutím Rady č. 91/396/EEC. Plánovaný termín zavedení jednotné linky do provozu byl stanoven na 2. leden 2003. Dále bylo rozhodnuto, že v té době již provozované linky 150, 155 a 158 budou zachovány a nově zřízené číslo 112 bude fungovat v souběžném provozu.

V zásadách a harmonogramu zavedení bylo schváleno, že číslo tísňového volání bude svedeno do 6 oblastních telefonních center s místem dislokace Praha, Plzeň, Ústí nad Labem, Hradec Králové, Brno a Ostrava. Jak je uvedeno v tab. 1, budou tato telefonní centra obsluhovat území jednoho nebo i více krajů a jejich obsluhu budou zabezpečovat příslušníci Hasičského záchranného sboru ČR. Potřebný počet příslušníků je řešen nárůstem početního stavu o 116 příslušníků.

| Místo dislokace | Obsluhované území |
|---|---|
| Praha | Hlavní město Praha a Středočeský kraj |
| Plzeň | Plzeňský a Českobudějovický kraj |
| Ústí nad Labem | Ústecký, Karlovarský a Liberec kraj |
| Hradec Králové | Královéhradecký a Pardubický kraj |
| Brno | Brněnský, Jihlavský a Zlínský kraj |
| Ostrava | Ostravský a Olomoucký kraj |

Tab. 1 Oblastní TCTV a jejich obsluhované území

Úlohy telefonního centra budou příjem tísňového volání v české i cizí řeči, vyhodnocení tísňové zprávy a předání nezbytných údajů, které identifikují mimořádnou událost, místně příslušnému operačnímu středisku složky IZS odpovědnému vysílat síly a prostředky k místu mimořádné události.

### 2.2.3 Usnesení Vlády ČR č. 350/2002 Sb.

Usnesení Vlády České republiky č. 350+P [19] ze dne 3. dubna 2002 přineslo změny v předchozím usnesení č. 391 + P v zavádění jednotného evropského čísla tísňového volání 112 v ČR.

Počet telefonních center tísňového volání byl zvýšen z 6 na 14, tj. centra TCTV 112 byla vybudována u krajských operačních a informačních středisek HZS. Pilotní projekt k ověření správné funkčnosti technologie telefonního centra tísňového volání a technologie krajského operačního a informačního střediska HZS byl proveden na území Jihočeského kraje.

K zajištění obsluhy center byl navýšen počet příslušníků o 52 osob. Přijímány jsou pouze osoby s potřebnými jazykovými znalostmi. Obsluhy telefonních center tísňového volání jsou systematicky jazykově a odborně připravovány pro příjem tísňových zpráv v jazyce anglickém a v jazyce německém. Příjem tísňových zpráv v jiných cizích jazycích než angličtina a němčina je řešen softwarovou podporou, spoluprací s nepřetržitými pracovišti provozovatelů veřejných telekomunikačních sítí a s ostatními operačními středisky základních složek integrovaného záchranného systému. Pro zajištění odborné způsobilosti obsluh jsou vybudována školní pracoviště jako součást školního operačního a informačního střediska.

Harmonogram zavedení tísňového čísla zůstal v platnosti dle usnesení Vlády ČR č. 391 + P s tím, že investiční výdaje, původně určené na školní operační středisko, byly

použity pro pilotní projekt na území Jihočeského kraje a na řešení stavební a technologické připravenosti školního operačního střediska pro dodávku technologie a úpravu navazujících a souvisejících technologií.

## 2.3 Architektura informačního systému pro podporu činnosti IZS

Integrovaný záchranný systém je výrazných způsobem ovlivňován informační podporou. Proto by měla být věnována významná pozornost způsobu jejího zabezpečení. Mezi klíčové prvky způsobu zajištění informační podpory lze bezesporu zařadit návrh architektury informačního systému IZS vycházejících z cílů a způsobů jeho činnosti [20].

### 2.3.1 Architektura informačního systému IZS

Architektura informačního systému IZS definuje hlavní prvky jeho struktury a vzájemné vazby mezi nimi. Obecně je možné ho považovat za systém systémů. Základními stavebními prvky jsou informační systémy pro příjem tísňových volání a operační řízení jednotlivých složek IZS. Oba tyto systémy lze považovat za dispečerské systémy k zajištění informační podpory pro řešení jednotlivých akcí záchranného charakteru [20].

Výchozím prvkem architektury je Národní informační systém (dále jen NIS) umožňující celorepublikový příjem tísňových volání z čísel 112, 158, 155 a 150 a současně zajišťuje řízení sil a prostředků při záchranných a likvidačních pracích v rámci jednotlivých krajů. Jednotlivé složky IZS připojené do NIS mezi sebou komunikují pomocí datové věty.

Součástí návrhu architektury je charakteristika jejích základních principů. Při formulaci principů se vychází z celkového konceptu IZS, struktury složek, zásad operačního řízení, technologických možností i výchozího stavu technického řešení informačních systémů jednotlivých složek IZS. Významnou roli sehrály také zahraniční zkušenosti a požadavky EU na tísňové volání 112 [20].

Mezi základní principy, které by měly být v rámci návrhu architektury informační systému IZS respektovány, patří principy:

- princip autonomie zabezpečuje, že daná složka IZS je autonomní a má svůj vlastní informační systém. Vzájemná informovanost složek IZS bude zajištěna přenosem informací ve formě datové věty;
- princip jednoduchosti spočívá v zajištění rychlé informační podpory operačnímu fungování složek IZS;

- princip odolnosti zabezpečuje odolnost systému vůli poruchám, výpadku elektrické energie a ztrátě dat;
- princip integrace vyjadřuje přijetí konceptu systém systémů s jejich vzájemným propojením do určitého celku. Informační systém IZS je tvořen relativně samostatnými informačními systémy složek IZS, které jsou prostřednictvím standardu datové věty integrovány v jeden celek;
- princip otevřenosti zabezpečuje směr dalšího vývoje jak po stránce technologické, tak i funkční. Vývoj by měl být nezávislý na konkrétním dodavateli řešení. Z toho důvodu je nejčastěji volen systém modulární, který umožňuje zapojit více dodavatelů. Nicméně tento postup vyžaduje striktní dodržování stanovených standardů;
- princip rozšiřitelnosti má za úkol zajistit možnost integrace dalších prvků IZS do struktury systému. Jedná se především o systém adresace uživatelů a indexování dat;
- princip standardizace je nevyhnutelnou podmínkou funkční slučitelnosti jednotlivých informačních systémů. Reálně představuje soubor technologických standardů a je rovněž předpokladem k zajištění otevřenosti systémů pro další vývoj a inovace;
- principu udržitelnosti zabezpečuje efektivitu rozvoje tak, aby v případě zavádění nových technologií nebo postupů nedocházelo ke zvyšování nákladů na provoz systému. Naopak vede ke snižování nároků na personál a provozní náklady [20].

### 2.3.2 Datová věta

Pro komunikaci mezi systémy jednotlivých složek IZS je výměna informací pomocí tzv. datové věty zcela zásadní. Datová věta je vytvořena ve standardizovaném formátu XML. Princip datové věty zajišťuje zkrácení doby do vyslání sil a prostředků zejména v případech, kdy je nutný zásah více složek integrovaného záchranného systému.

Datová věta je co nejrychleji předána konkrétním operačním střediskům jednotlivých složek IZS, která jsou k systému TCTV 112 připojena pomocí Integrované telekomunikační sítě Ministerstva vnitra (dále jen ITS), (v minulosti bylo využíváno datové sítě MPLS - Multiprotocol Label Switching). Operační střediska vyšlou,

na základě získaných informací z datové věty, potřebné síly a prostředky na místo mimořádné události.

Obsah datové věty:

1. Co se stalo – typ a podtyp události. Jedná se pouze o předběžnou klasifikaci dle toho, co volající nahlašuje, nikoliv o stanovení diagnózy;
2. Poznámka – volnou formou zapsané stručné doplňující informace o události. Př.: Starší muž, 58 let, po pádu na schodech, krátké bezvědomí;
3. Údaj o použitém telefonním přístroji – telefonní číslo, ze kterého bylo voláno, v případě volání z mobilního telefonu bez SIM karty se zobrazuje IMEI (International Mobile Equipment Identity)tohoto mobilního telefonu, jenž je pro každý přístroj jedinečné;
4. Identifikace volajícího – jméno volajícího, z pevných linek automaticky pomocí služby Info 35 (databáze všech telefonních čísel), ze sítí mobilních operátorů pouze, pokud je známo a volající ho sdělí (zadáváno ručně);
5. Místopis – adresa je zadávána ve formátu: stát, kraj, okres, obec, místní část obce, ulice, číslo popisné. Z pevných linek je zadáno automaticky, z mobilních sítí je zadáváno ručně. Pokud je známo nebo pokud volající sdělí, tak lze ručně doplnit patro a číslo bytu;
6. Číslo události v systému TCTV;
7. Jméno a příjmení operátora, jenž odbavoval danou událost;
8. Číslo IP telefonu pracoviště, na kterém byla událost zpracována.

### 2.3.3 Prvky architektury informačního systému IZS

Projekt návrhu informačních systémů výrazným způsobem ovlivnily i podmínky pro zajištění komunikace vymezené zákonem č. 239/2000 Sb. a souvisejících v platném znění [21] a návazné vyhlášky. Vyhláška č. 328/2001 Sb. [22], novelizovaná vyhláškou č. 429/2003 Sb. [23], pro oblast krizové komunikace stanovila, že přenos dat v jednotlivých systémech bude zajištěn především s využitím účelové telekomunikační sítě Ministerstva vnitra.

Na základě uplatnění výše uvedených principů a s uplatněním zásad krizové komunikace tvoří základní prvky architektury informačních systémů IZS:

- informační systém TCTV 112
- informační systém HZS „Výjezd“;

- jednotný systém varování;
- informační systém Policie ČR „Jitka“;
- informační systémy zdravotnických záchranných služeb (3);
- komunikační systém [20].

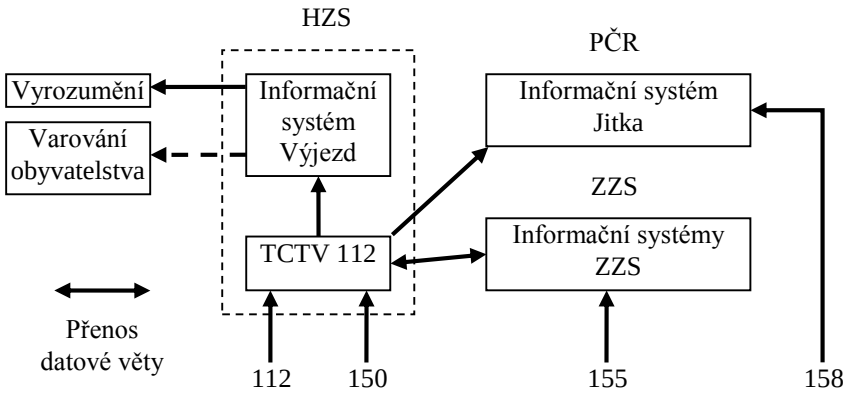
Podporu HZS tvoří dva informační systémy: Dispečer 112 a informační systém Výjezd (dále jen ISV). Dispečer 112 zajišťuje příjem tísňového volání z tísňových linek 112 a150.

Informační systém Výjezd je koncipován pro operační řízení sil a prostředků HZS při realizaci záchranných a likvidačních prací. Systém respektuje krajské uspořádání HZS. Zajišťuje rovněž řízení technologických procesů, umožňujících dálkové ovládání garážových vrat, otevírání a uzavírání výjezdových bran, dálkové ovládání rádiových retranslačních prvků atd.

Významnou oblastí informační podpory ochrany obyvatelstva je oblast varování. Včasné předání informací o vzniklém nebezpečí tvoří základ aktivace sil a prostředků ochrany, případně včasnou akceschopnost k záchraně života a zdraví obyvatelstva a jejich majetku. Za varování se považuje předání informací obyvatelstvu o hrozbě vzniku mimořádné události, případně o mimořádné události, která již nastala. Součástí varování je také informace o možných důsledcích mimořádné události na obyvatelstvo a způsobech jejich eliminace. Varování je zajištěno různými typy sirén, místními informačními systémy a hromadnými informačními prostředky.

Informační systém Policie ČR „Jitka“ představuje komponentu IZS, zajišťující operační řízení Policie ČR při řešení mimořádných událostí jak z hlediska IZS, tak dalších operačních policejních činností. Jedná se o dispečerský systém, zajišťující informační a komunikační podporu operačnímu řízení sil a prostředků na teritoriu. Systém zajišťuje obsluhu tísňové linky 158. Systém je tvořen subsystémy, respektujícími krajské uspořádání.

Všechny kraje používají stejnou softwarovou platformu, viz obr. 3. Systém prošel více než desetiletým vývojem a respektuje požadavky policie na operační řízení. Jeho hlavním rysem je jednoduchost a účelnost realizace informačních činností [20].




Obr. 3 Architektura informačního systému IZS [20]

Informační systémy ZZS zajišťují informační podporu činnosti zdravotnické záchranné služby. Tak jako ostatní informační systémy zajišťují příjem tísňového volání a operační řízení výjezdových skupin ZZS. Operátoři navíc v mnoha případech poskytují volajícímu asistovanou první pomoc, s jejíž podporou by mělo být zajištěno zraněnému její laické poskytování do příjezdu zdravotnické pomoci. Systémy zajišťují obsluhu tísňové linky 155. Systémy jsou organizovány na principu krajského uspořádání. Na rozdíl od předchozích systémů nedošlo ve všech krajích k nasazení jednotného softwarového řešení. V současnosti jsou využívána tři řešení s různou šíří funkčnosti. Do budoucna není z důvodu vložených investic předpoklad, že by došlo k sjednocení softwarové platformy.

První ze systémů je systém označovaný S.O.S. a realizovaný firmou PER4MANCE. Ten představuje se svými 19 moduly jednotnou platformu, která umožňuje integrovat veškerou činnost záchranné služby do jednoho informačního systému. Systém je provozován ve všech krajích s výjimkou Jihočeského kraje, Olomouckého kraje, Moravskoslezského kraje a Zlínského kraje [24]. Výčet některých z modulů, které systém obsahuje - modul Základna, Dispečer, Statistiky, Kniha jízd, Pojišťovny, Mezisklady, Hotovost, Směny. Ze zmíněných modulů je nejdynamičtěji se rozvíjejícím modulem modul Dispečer. Slouží jako hlavní součást řešení krajského zdravotnického operačního střediska. Součástí instalace informačního systému S.O.S. je i záložní datové centrum, které dále zvyšuje spolehlivost a odolnost celého řešení.

Druhým systémem je systém Dispečer ZZS od společnosti RCS Kladno. Je to analogový spojový systém územního střediska záchranné služby Olomouc, Českých Budějovic a Jihlavy. Představuje propojení SW nástrojů pro automatické doručování

hlasových zpráv na platformě Alcatel-Lucent (AMDS) a dispečerských IS operačních středisek složek IZS pro účely vyrozumění osob při řešení krizových situací [25].

V rámci kraje Olomouckého, Zlínského a Moravskoslezského je provozován třetí informační systém ZZS označovaný jako M5ZZS. Tento systém je produktem společnosti Vítkovice IT Solutions [26].

Komunikační systémy zajišťují podporu činnosti IZS v podobě hlasových a datových služeb. Datová část zajišťuje přenos dat v rámci jednotlivých informačních systémů.

Každá ze složek IZS má svůj komunikační systém. HZS má vytvořen komunikační systém, jehož základem jsou digitální telefonní ústředny, prvky sítí přenosu dat a dálkové digitální okruhy. Provoz ústředen a prvků sítí přenosu dat si zajišťuje tato bezpečnostní složka vlastními silami. Digitální okruhy jsou pronajaty od komerčních poskytovatelů. V rámci TCTV 112 zajišťuje přenos hovorů a dat určený poskytovatel (v letech 2004 až 2006 Český Telecom, a.s., 2006 až 2014 O2 Czech Republic, a.s.). Policie ČR využívá ke komunikaci účelovou telekomunikační síť ITS. Všechny výše uvedené systémy je možné obecně charakterizovat jako digitální systémy využívající k dálkovému přenosu technologie PDH (Plesiochronous Digital Hierarchy), SDH (Synchronous Digital Hierarchy), ATM (Asynchronous Transfer Mode) a TCP/IP (Transmission Control Protocol/Internet Protocol). Nasazení datových okruhů vychází z kapacitních požadavků informačních systémů i technologických možností jednotlivých lokalit.

Samostatnou část komunikačního systému představuje zajištění komunikační podpory mobilním uživatelům, nasazeným k zajištění záchranných a likvidačních prací v prostoru mimořádné události. Tuto funkci zajišťuje radiokomunikační síť Pegas [27]. Jedná se o digitální radiokomunikační systém respektující požadavky bezpečnostních složek na zajištění mobilní hlasové a datové komunikace. Technologické řešení vychází z průmyslových standardů Tetrapol. Systém je vybudován na buňkovém principu s možností zajištění rozhlašovacího provozu i dvoubodových spojů. Systém provozuje Ministerstvo vnitra prostřednictvím České pošty, a.s.

### 2.3.4 Pegas – Matra (Tetrapol)

Radiokomunikační síť Pegas zajišťuje komunikační podporu mobilním uživatelům. Její výstavba byla velkým dílem ovlivněna novodobými bezpečnostními hrozbami. Česká republika si zvolila pro zajištění komunikačních potřeb svých bezpečnostních složek systém technologie Tetrapol, jenž je uznávaný radiokomunikační standard v rámci Evropské unie.

Pegas byl původně názvem projektu, nicméně se později stal názvem hromadné radiokomunikační složek IZS, která byla vybudována v České republice v období 1994 až 2003. Jedná se o pozemní radiokomunikační síť, která je svých charakterem určena především pro použití v záchranných a bezpečnostních složkách.

Monopol na výrobu technologických částí a koncových zařízení standardu Tetrapol má evropská společnost EADS (European Aeronautic Defense and Space Company), respektive její divize Cassidian.

Vznik technologie standardu Tetrapol započal ve Francii v osmdesátých letech minulého století, kdy skupina vědců, pracovníků z praxe a odborníků na kryptografii vytvořila radiokomunikační standard, který se později stal světově uznávaným řešením pro mobilní rádiové komunikace bezpečnostních složek.

Základem pro řešení problematiky radiokomunikačního systému složek IZS bylo usnesení Vlády ČR č. 246/1993 [28] ze dne 19. května 1993. Toto usnesení uložilo Ministru vnitra ve spolupráci s ostatními resorty vypracovat návrh technického řešení konektivity stávajících spojovacích prostředků složek IZS. Úkolem se zabývala mezirezortní komise, která doporučila obměnu stávajících sítí složek IZS generačně novým radiokomunikačním systémem. Tento systém měl být sdílen a využíván všemi složkami IZS a to jak za běžných situací, tak i při zásazích v místech mimořádných událostí. Ve výběrovém řízení, které proběhlo v roce 1994, vyšla vítězně firma Matracom Nortel Communication. Ta následně zahájila výstavbu radiokomunikační sítě na bázi technologie Matracom 9600. Výstavba radiokomunikační sítě Pegas byla dokončena v srpnu 2003. Následně byl stanoven datum 1. února 2007 jako závazný termín pro zahájení rutinního provozu na úrovni operačních středisek a mobilní požární techniky (termín zavedení stanoven v dokumentu HZS čj. PO-2975/KIS-2006).

U zdravotnické záchranné služby, i přes snahu pověřeného zástupce Ministerstva zdravotnictví, nedošlo k zavedení této technologie celoplošně do jednotlivých krajů tak, jak tomu je u HZS a PČR. Příčinou tohoto stavu je samostatnost krajských ZZS.

Ministerstvo zdravotnictví řídí ZZS pouze metodicky a je tak proto obtížné přenášet závěry z jednání na jednotlivé zdravotnické záchranné služby v krajích. To v konečném důsledku vede k nejednotnému způsobu komunikace v rámci IZS.

#### 2.3.4.1 Charakteristika radiokomunikační sítě Pegas

Radiokomunikační síť Pegas je plně digitální systém s integrovanými hlasovými a datovými službami. Pracuje v kmitočtovém pásmu 380 – 400 MHz [29] s přístupem FDMA s kanálovým odstupem 12,5 kHz. Přenosová rychlost jednotlivých kanálů pro hlasovou komunikaci je 8 kbps. Přitom je 6 kbps využito pro přenos vlastní hlasové komunikace a 2 kbps jsou vyčleněny pro zabezpečení a vlastní systémové zprávy. Přenos dat může probíhat datovým kanálem s přenosovou rychlostí 3,6 kbps. Zbylá část kapacity rádiového kanálu je využita pro zabezpečení a vlastní systémové zprávy. Veškerá komunikace je zabezpečena proti pokročilým metodám odposlechu. Komunikace probíhá v šifrovaném režimu s automatickou centrální distribucí klíčů. Systém je řešen jako buňkový, kde každá buňka pracuje se svazkem radiových kanálů. Základem buňky je základnová stanice, označovaná též jako base station, umístěná na vhodné terénní dominantě tak, aby bylo možno rádiovým signálem pokrýt požadovaný prostor.

Komunikace mezi základnovou stanicí a uživatelskými terminály probíhá na rádiových kanálech. Tyto kanály se dělí do třech typů:

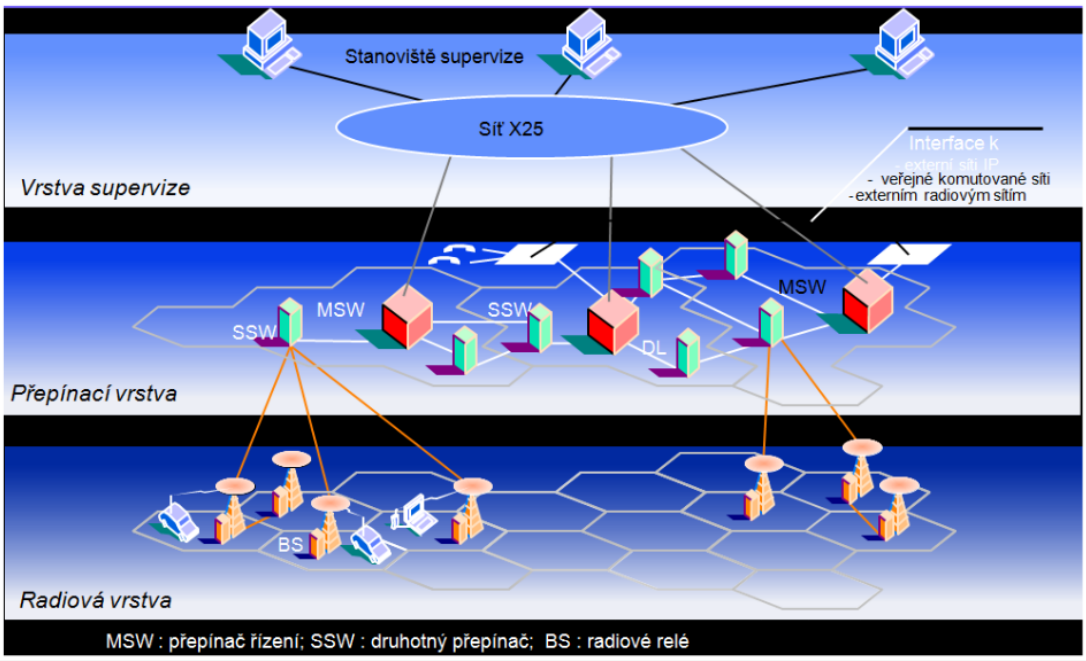
- provozní kanál zabezpečující hlasové komunikace, které jsou dynamicky přidělovány podle provozních požadavků;
- řídící kanál (organizační), který je v rámci buňky jen jeden a zabezpečuje přenos systémových informací mezi koncovými zařízeními (terminály) a infrastrukturou, zároveň zabezpečuje datový přenos mezi terminály a pevnou datovou sítí, díky tomu provozní kanály nejsou blokovány datovými přenosy a jsou plně k dispozici pro hlasovou komunikaci;
- vyčleněný (dedikovaný) datový kanál (DDCH – Dedicated Data Channel), v nové verzi systémového programového vybavení sítě je možno také vyčlenit hovorový kanál jako datový, tím dojde ke zvýšení prostupnosti sítě při více požadavcích na datové komunikace; v jednom datovém kanálu je možné uskutečnit až čtyři nezávislé datové komunikace;

- nevýhodou tohoto řešení je, že již při jedné datové komunikaci je vyčleněn a obsazen celý rádiový kanál, který, pokud není nahrazen, omezuje jeho využití pro hlasové služby.

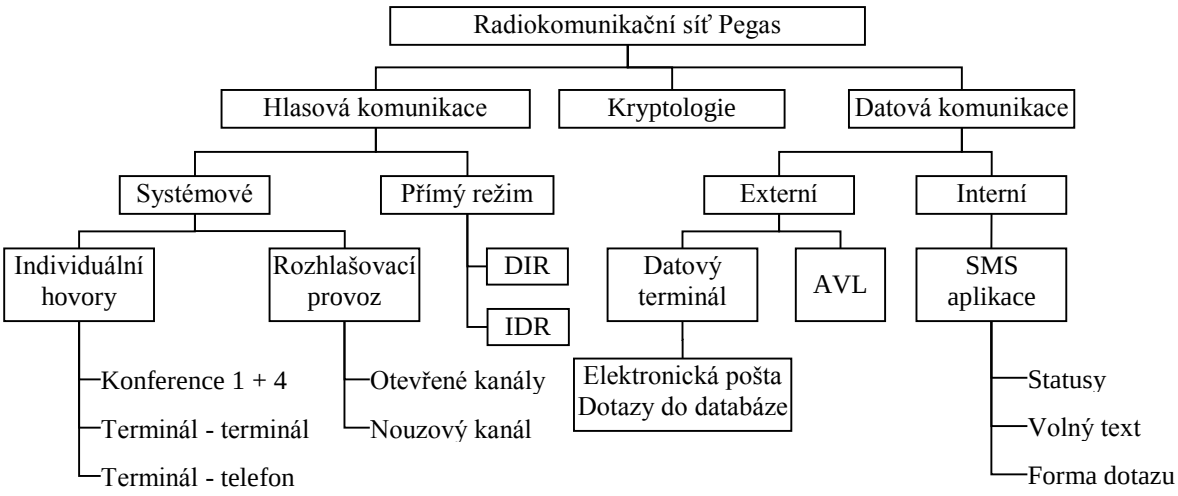
Plošné pokrytí území rádiovým signálem umožňuje automatický přechod mezi buňkami bez nutnosti zásahu obsluhy. Systém umožňuje rovněž souběžně vysílání do několika buněk. Vzájemná komunikace těchto dvou druhů provozu umožňuje reagovat na široké spektrum provozních požadavků. Základem řešení celostátního systému Pegas jsou vzájemně propojené regionální sítě. V daném kmitočtovém pásmu jsou dále vyčleněny kanály pro přímý mód (DIR), na kterých je prováděno samostatné spojení mezi radiostanicemi bez toho, aby byla využita infrastruktura základnových stanic a dalších prvků systému. Na základě požadavků uživatelů se výrobce technologie zabývá také řešením přenosu dat i v přímém režimu. Vychází především z požadavku příslušníků hasičského sboru na přenos stavových informací, monitorující jak základní životní funkce zasahujícího příslušníka, tak veličiny související s činností jeho dýchacího přístroje. V koncepci společnosti Cassidian je v dlouhodobém záměru též možnost integrace čidel základních nebezpečných látek přímo do terminálu.

Systém pegas byl budován v návaznosti na členění území České republiky na okresy. V současné době je však preferováno pokrytí operační oblasti, která může sdružovat jeden či více bývalých okresů. Pokrytí tohoto území je realizováno určitou množinou základnových stanic v závislosti na členitosti terénu. Buňka samotná, území pokryté jen jednou základnovou stanicí, většinou pokrývá území více okresů. Jednotlivé radiové sítě operačních oblastí jsou sdruženy v závislosti na státoprávním uspořádání do regionální sítě s řídícím dohledovým pracovištěm. Souhrn regionálních sítí v rámci České republiky tvoří národní síť, která je řízena z centrálního pracoviště.

Na tomto pracovišti se nastavují organizační parametry s nejvyšší úrovní. Organizační parametry předem definují přístupová práva terminálu v radiokomunikační síti Pegas. Národní síť v podmínkách České republiky realizují sítě krajské, kterých je 14. Krajské sítě jsou propojeny datovou sítí X.25 a digitálními linkami o přenosové rychlosti 2 Mbps. Datová síť X.25 zajišťuje přenos dat pro potřeby správy a řízení celé sítě Pegas. Přenosové okruhy o rychlosti 2 Mbps propojují základnové stanice s ústřednami.




Obr. 4 Vrstvy infrastruktury sítě Pegas [30]




Obr. 5 Přehled základních služeb systému Pegas [20]

Na obr. 5 jsou uvedeny základní způsoby komunikace a služby dostupné v radiokomunikační síti Pegas. Rámci IZS jsou využívány především systémové hlasové komunikace, tzv. otevřené kanály a v přímém režimu pak provoz DIR. Ze služeb datových komunikací je využíváno zasílání SMS, přenos stavových hlášení a u policie pak dotazy do databází. Od roku 2006 se též rozvíjí služba AVL, jenž umožňuje automatickou lokalizaci vozidel. Na systém nezávislým řešením je prostředek

technologie Tetrapol IDR (Independent Digital Repeater) s jehož pomocí lze autonomně vykrýt požadovanou lokalitu rádiovým signálem.

K datu 1. září 2011 bylo území ČR pokrýváno 220 základnovými stanicemi (vykrývači, převaděči), které jsou umisťovány na vybrané kóty a vykrývají signál nejbližší základnové stanice. Prostřednictvím převaděčů jsou vykrývané i zájmové objekty, jako jsou např. železniční či silniční tunely. Pokrytí území signálem je matematickým modelem propočteno na 96% území pro vozidlové terminály. Z ručního terminálu je garantovaná konektivita na infrastrukturu sítě v obcích nad 20 tisíc obyvatel. Počet základnových stanic vychází u usnesení vlády, kde byl tento počet navržen jako střední varianta. V souvislosti se vstupem ČR do Schengenského prostoru jsou umísťovány převaděče v příhraničních oblastech tak, aby mohly být plněny požadavky na komunikační zabezpečení v rámci příhraniční spolupráce.

#### 2.3.4.2 Použití systému Pegas Armádou ČR

Přístup k systému PEGAS (mimo základních složek IZS – podle zákona č. 239/2000 Sb. to jsou PČR, HZS, ZZS) je poskytován i tzv. ostatním složkám pro součinnostní komunikaci, především v oblasti krizového řízení podle zákona č. 240/2000 Sb. Radiokomunikační síť PEGAS-MATRA je jednou z možností předávání signálů pro uvádění vojsk AČR do vyšších stupňů bojové pohotovosti.

Terminály PEGAS jsou přiděleny pro útvary vyčleňované do IZS, Vojenskou policii a ostatní subjekty AČR, využívající VKV rádiový systém PEGAS pro zabezpečení spojení pohyblivých služeb. Na základě „Dohody o využívání systému hromadných rádiových sítí“ mezi MO a MV, čj. SSI-585/110-95 odboru spojení a informatiky MV, mohou tento systém využívat i orgány MO. Provoz základnových stanic (BS) je řízen OKIS MV ČR prostřednictvím hlavních rádiových ústředen (MSW).

Pokyny pro zpracování, uveřejňování, změny a využívání souboru dokumentů stanovuje nařízení Ministerstva vnitra č. 25 ze dne 25. dubna 2012 „Provozní dokumentace systému PEGAS“ a „Bezpečnostní postupy pro práci operátorů (uživatelů) radiokomunikačního systému PEGAS“ (čj. MV-81592-1/SIK5-2013).

## 2.4 Technologické řešení telefonických center tísňového volání

Řešení telefonního centra tísňového volání 112 (dále jen TCTV 112) je založeno na moderní technologii spojující telefonii a informační systém. Vlastní technologie je řešena několika způsoby, aby byla zajištěna efektivita práce s informacemi během mimořádné události.

Výhodným řešením telefonického centra tísňového volání je umístění (centralizované řešení) operátorů jednotlivých složek IZS na jedno společné pracoviště. To je zejména výhodné při koordinaci zásahu u událostí velkého rozsahu. Dalším řešením je řešení distribuované, kde operátoři pracující na oddělených místech a jsou propojeni komunikačními prostředky. Nicméně navenek se systém chová jako celek. Posledním je kombinační řešení, které je kombinací předchozích dvou [31].

Veškeré technologie telefonických center tísňového volání 112 poskytuje společnost O2 IT Services s.r.o., dodavatelem telekomunikačního řešení je společnost Dimension Data Communications Czech s.r.o. a aplikační řešení zajišťuje společnost Vítkovice IT Solutions a.s.

Vítkovice IT Solutions a.s. byla certifikována dle normy ČSN EN ISO 9001 v roce 2001 [32] a dále v roce 2004 byla certifikována Národním bezpečnostním úřadem pro stupeň utajení „Důvěrné“ dle zákona č. 148/1998 Sb., o ochraně utajovaných skutečností [33]. Společnost Vítkovice IT Solutions a.s. nadále pokračuje ve vývoji systémů pro podporu činnosti složek IZS a to v oblastech [34]:

- Příjem tísňového volání - SW pro příjem tísňového volání na linky 112, 150, 155, 156;
- Operační řízení ZZS - SW pro řízení složek zdravotní záchranné služby;
- Operační řízení MěP - SW pro řízení složek městské policie;
- Krizové řízení - SW pro krizové řízení;
- GIS - Grafická podpora IZS;
- IKK - Integrovaná krizová komunikace.

Společnost Vítkovice IT Solutions a.s. je kromě výše uvedené normy, certifikována standardy ČSN EN ISO 14001 (Systém environmentálního managementu) z roku 2005, ČSN EN ISO 27001 (Systém managementu bezpečnosti informací) z roku 2005 a ČSN ISO/IEC 20000-1 (Systém managementu služeb - Informační technologie) z roku 2006 [35].

Společnost Dimension Data Communications Czech s.r.o., je certifikována standardy ČSN EN ISO 9001 (Systém managementu jakosti) z roku 2009, v roce 2005 získala certifikát ČSN EN ISO 14001 (Systém environmentálního managementu), dále certifikát ČSN ISO/IEC 20000-1 (Systém managementu služeb - Informační technologie) v roce 2006 a ČSN EN ISO 27001 (Systém managementu bezpečnosti informací) v roce 2006 [36].

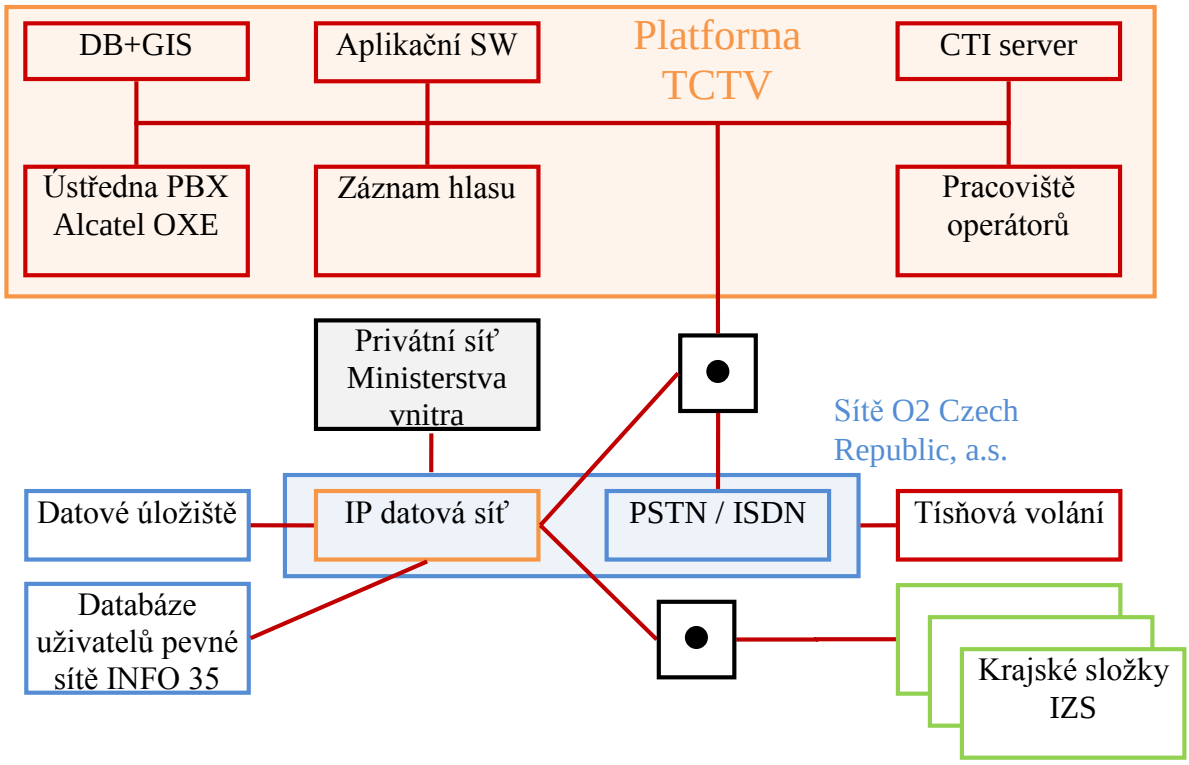
### 2.4.1 Vývoj a realizace systému

Realizace systému byla započata v roce 2001 [17] výstavbou školícího pracoviště na Odborném učilišti požární ochrany Frýdek Místek. Pracoviště je vybaveno simulátorem tísňového volání pro přípravu budoucích operátorů. Tato příprava zahrnovala, kromě výuky ovládání technologie a aplikace příjmu tísňového volání, zvládnutí procesu příjmu hovoru a základního přehledu procesu operačního řízení a dále také jazykovou přípravu operátorů příjmu tísňového volání v anglickém a německém jazyce.

Zároveň s probíhajícím výcvikem budoucích operátorů probíhala v letech 2002 a 2003 výstavba 14 krajských telefonních center tísňového volání dle schématu uvedeném na obr. 6. Centra byla od 6. října 2003 uvedena do testovacího provozu použitím testovacího telefonního čísla.

První TCTV pro linku 112 bylo spuštěno v Praze 20. dubna 2004. Během testovacího provozu byl systém podroben rozsáhlé analýze a zátěžovým zkouškám. V rámci vyhodnocení výsledků testování byly odstraněny zjištěné závady a byla zahájena příprava na pilotní ostrý provoz systému.

Na základě výborných výsledků provozu TCTV Praha byl od 15. června 2004 spuštěn ostrý provoz moderních TCTV na linku 112 v krajích na území Čech a od 22. června 2004 na území Moravy. Výjimkou byl Královéhradecký kraj, kde bylo rozhodnuto o umístění technologie do nové budovy, jejíž stavba byla dokončena v roce 2005, a Moravskoslezský kraj, kde bylo telefonní centrum integrováno do existujících technologií Centra tísňového volání Ostrava. Plné dokončení projektu výstavby telefonních center ve 14 krajích tak nastalo v únoru roku 2005.




Obr. 6 Řešení systému komunikace TCTV 112 [37]

## 2.4.2 Funkční bloky systému

### 2.4.2.1 CTI server

CTI server má za úkol propojit telefonní a počítačovou architekturu. CTI server se funkčně nachází za PBX ústřednou a má za úkol zpracovávat signály a dále je předávat přes architekturu LAN. U TCTV 112 je použit CTI systém od společnosti Genesys, který zajišťuje propojení aplikačního softwaru a telefonních technologií.

Mezi další funkce CTI serveru patří propojení s databázovými systémy, kde musí být dodržena kompatibilita se standardy Open Database Connectivity (ODBC) a programovacím jazykem SQL. Umožňuje nahrávat provoz do digitálních formátů a provádět hodnocení kvality. Další neméně důležitou funkcí je možnost vedení příposlechu operátorů v reálném čase, který je jedním z nástrojů zvyšování kvality služeb (Quality control) nebo zabezpečení výuky nováčků zkušenými operátory. CTI nabízí rozšířené reportovací funkce, jako jsou modifikované grafy a aplikace ukazující informace o hlasovém provozu v reálném čase.

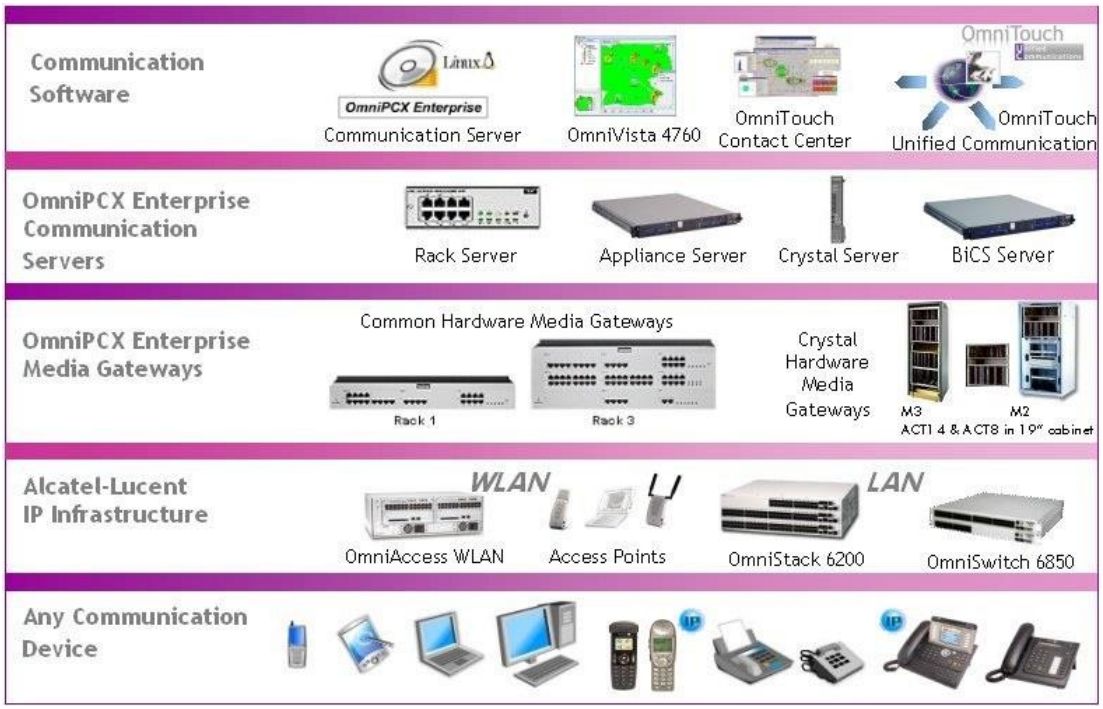
#### 2.4.2.2 Pobočková ústředna

Pobočková ústředna PBX (Private branch exchange) má za úkol sjednocovat výstupní body do telefonní sítě. Pro správnou funkci call centra je nezbytná podpora CTI serverem.

Ústředna PBX je v tomto systému reprezentována systémem Alcatel-Lucent OmniPCX Enterprise. Je to vysoce výkonný, inovační multimediální telekomunikační systém, který je vhodný pro středně velké a velké telekomunikační řešení. Umožňuje přenosy hlasu, dat a obrazů do kapacity 50 000 přípojných portů a připojení do běžných telekomunikačních sítí pomocí analogových, digitálních i ISDN rozhraní.

Řešení Enterprise umožňuje přirozené připojení do datových LAN/WLAN sítí všech typů a přenosy hlasu po sítích ATM, Frame Relay a zejména přenos typu VoIP. Vysoká spolehlivost je zaručena zdvojováním centrálních jednotek a zálohovacími mechanismy pro přenosy signalizace. Jde o systém s dokonalým zabezpečením hlasové i datové komunikace.

Řešení umožňuje vytvářet nejrůznější druhy privátních sítí (včetně virtuálních), podporuje spolupráci s počítačovými aplikacemi a vytváření rozlehlých Call Center. Srdcem OmniPCXEnterprise je sada komunikačního softwaru zahrnující celou řadu komunikačních aplikací pro OS Linux s celkovým počtem 500 nabízených funkcí. Software může běžet na třech typech serverů: Common Hardware CPU (modul "Rack"), Crystal Hardware CPU (modul Crystal) a Standardně dodávané servery (např. IBMx306). Komunikační server podporuje mediální brány pro připojení k veřejné telekomunikační síti nebo dalším zařízením. Pro systémy s velkým počtem spojení se používá brána Crystalhardware [38].




Obr. 7 Architektura komunikačního řešení Alcatel-LucentOmniPCXEnterprise [39]

#### 2.4.2.3 Záznam hovorů operátorů TCTV

Jedním z důležitých systémů z pohledu řízení kvality a z důvodů legislativních je nahrávání provozu TCTV 112. Veškerý hlasový provoz v systému je nahráván výkonným systémem REDAT (do roku 2011 bylo používáno zařízení NICEQuery), který umožňuje on-line přístup k nahrávkám. Tento přístup mají jak operátor TCTV 112, tak i operační střediska složek IZS pro případ zpětného vyhodnocení určité krizové situace nebo upřesnění informací o události. Hovory jsou archivovány po dobu minimálně 12 měsíců (skartační lhůta záznamu) a na každém krajském pracovišti je možné s pomocí speciálního softwaru vyhledat, případně exportovat tyto hovory pro další využití (např. složkami činnými v trestním řízení).

Nahrávání hovorů, případně obrazovek operátora, je řízeno nahrávacími pravidly, která definují podmínky, za kterých má být hovor na monitorovaném zařízení zaznamenán. Nahrávky jsou lokálně uloženy na záznamové komponentě, je ale možné využít i manuální uložení na jiné médium, či systém obohatit o funkcionalitu archivace a vyhovět tak požadavkům na dobu uchování nahrávek. Nahrávky je z důvodu bezpečnosti možné šifrovat.

Kromě fyzického záznamu hovorů bývá řešení vybaveno rozhraním pro CTI integraci s telekomunikačním systémem. Díky ní je vytvářen seznam záznamů o jednotlivých zaznamenaných hovorech.

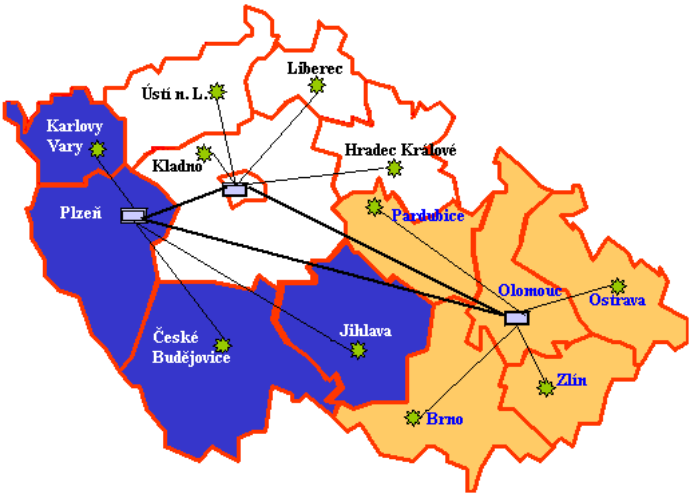
#### 2.4.2.4 Systém propojení TCTV 112

Technologie tísňového volání je řešena jako jednotná a jednotlivá TCTV 112 se vzájemně zálohují. V případě potřeby lze tísňový hovor odbavit z jakéhokoliv TCTV. Toto řešení nicméně vyžaduje jednotnou konfiguraci systému.

Komunikační platformu telefonních center tísňového volání navrženou a dodanou formou subdodávky tvoří tři pobočkové ústředny Alcatel OmniPCXEnterprise 4400 umístěné v Praze, Plzni a Olomouci. Na tyto ústředny je napojeno 11 vzdálených bloků (tzv. remote TCTV) těchto ústředen ve zbývajících krajích ČR, viz níže uvedená tab. 2.

| TCTV platforma | TCTV 112 |
|---|---|
| Praha | Hlavní město Praha<br>Ústecký kraj<br>Liberecký kraj<br>Královéhradecký kraj<br>Středočeský kraj |
| Plzeň | Plzeňský kraj<br>Jihočeský kraj<br>Karlovarský kraj<br>kraj Vysočina |
| Olomouc | Olomoucký kraj<br>Moravskoslezský kraj<br>Zlínský kraj<br>Jihomoravský kraj<br>Pardubický kraj |

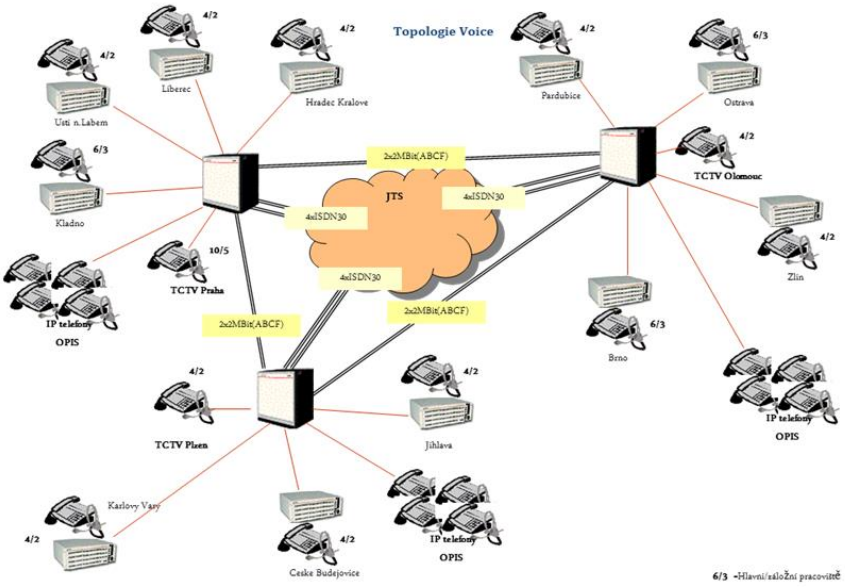
Tab. 2 Rozdělení TCTV platforem a jednotlivých TCTV krajů [40]




Obr. 8 Rozmístění a propojení TCTV 112 v ČR[40]

Na obr. 8 a 9 jsou znázorněna napojení vzdálených pracovišť na jednotlivé platformy. Komunikace mezi platformami je zajištěna pomocí dvojitého, na sobě nezávislého, datového vedení LL-NET s rychlostí přenosu 2 Mbit/s (E1).

Komunikace mezi platformou a vzdáleným (remote) TCTV je zabezpečena datovou linkou LL premium s rychlostí přenosu 2 Mbit/s. Komunikace mezi geograficky vzdálenými připojenými centry je vedená tranzitem přes platformy ležící ve směru spoje. Tímto způsobem je zabezpečena vzájemná komunikace všech TCTV v síti. Dříve byla pracoviště rozdělena na hlavní a záložní. Jejich počet a rozmístění záviselo na velikosti osídlení daného regionu. V současnosti bylo od této koncepce upuštěno a všechna stanoviště jsou považována za hlavní. Celkově je v ČR 106 operátorských pozic.




Obr. 9 Rozmístění a propojení TCTV 112 [41]

#### 2.4.2.5 Aplikace

Aplikační software TCTV (dále jen ASW112) realizuje veškeré uživatelské funkce spojené s příjmem tísňových volání. ASW112 se skládá z funkčních modulů, které pracují nad datovým schématem informačního systému a vytvářejí tak prostředí, v němž mohou dispečeři/ operátoři TCTV řešit zpracování tísňového volání.

### 2.4.3 Systém lokalizace hovoru

Systém byl navržen tak, aby prováděl automatickou lokaci volajícího. Tato funkce operátorům zajišťuje zobrazení polohy volajícího přímo na monitoru počítače v aplikaci Geografického Informačního Systému (dále jen GIS).

Systém GIS a databáze jsou jedny z nepostradatelných součástí systému pro správnou funkci složek IZS. Geografický informační systém GIS je používán více jak 15 let a za tuto dobu došlo k velkému rozmachu do všech činností složek IZS. Systém GIS je nepostradatelný pro podporu jednotek u zásahu, při prevenci a ochraně obyvatel. Vzhledem k tomu, že HZS ČR používá velké množství informací, má proto zřízen Centrální datový sklad, o který se starají pracovníci Institutu ochrany obyvatel v Lázních Bohdaneč (dále jen IOO LB). Data nejsou určena jen pro HZS ČR, ale dle smluv s poskytovateli jsou distribuována i dalším složkám IZS. Správci GIS HZS krajů a pracovníci IOO LB využívají ke správě dat, tvorbě mapových projektů a tištěných výstupů, desktop GIS aplikace ArcGIS, ArcSDE a ArcGIS Server.

GIS je technologie a nástroj, který používá a zpracovává údaje polohově vázané k povrchu Země. Je schopný pracovat s digitálními mapami i s popisnými databázemi, propojit prostorové (grafické) a popisné (negrafické) databázové údaje. Vyhodnocovat požadavky, které kombinují klasické databázové dotazy s geografickými údaji, vyhledávat a analyzovat databázové údaje prvků a výsledky pak přehledně zobrazit ve formě mapových výstupů [42, 43].

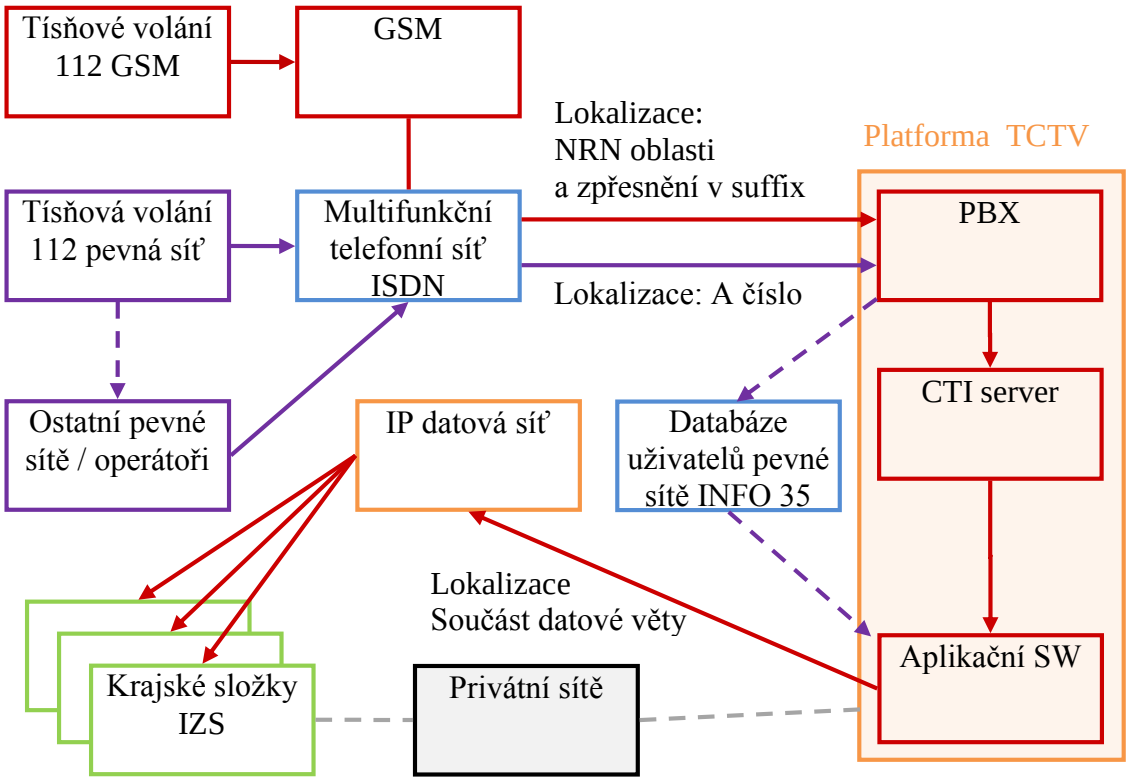
Mezi negrafické databázové údaje například patří:

- historie předchozích výjezdů, registr osob se zdravotním postižením (v současnosti je databáze připravována);
- databáze nebezpečných chemických látek.

Ke grafickým databázovým údajům mimo jiné patří:

- Databáze ulic a čísel popisných;

- speciální geografické databáze zaměřené na výskyt nehod ve skalních oblastech ČR (informace horské služby).




Obr. 10 Systém předávání informace o poloze volajícího [37]

Lokalizace místa volajícího je jednou z nejdůležitějších funkcí GIS klienta. Ta se dá rozdělit na dva způsoby. Jednak je to lokalizace místa volání z pevné sítě a lokalizace ze sítě mobilní. Dispečer (osoba) přijímá hovor na tísňovou linku a spolu s hovorem Call Agent vyhodnocuje „systémovou signalizaci“ hovoru. V případě, že jde o volání z pevné sítě, pak se na stranědispečerské aplikace připraví zpráva, která obsahuje telefonní číslo a pošle se zabezpečeným protokolem v XML formě do tzv. databáze INFO 35.

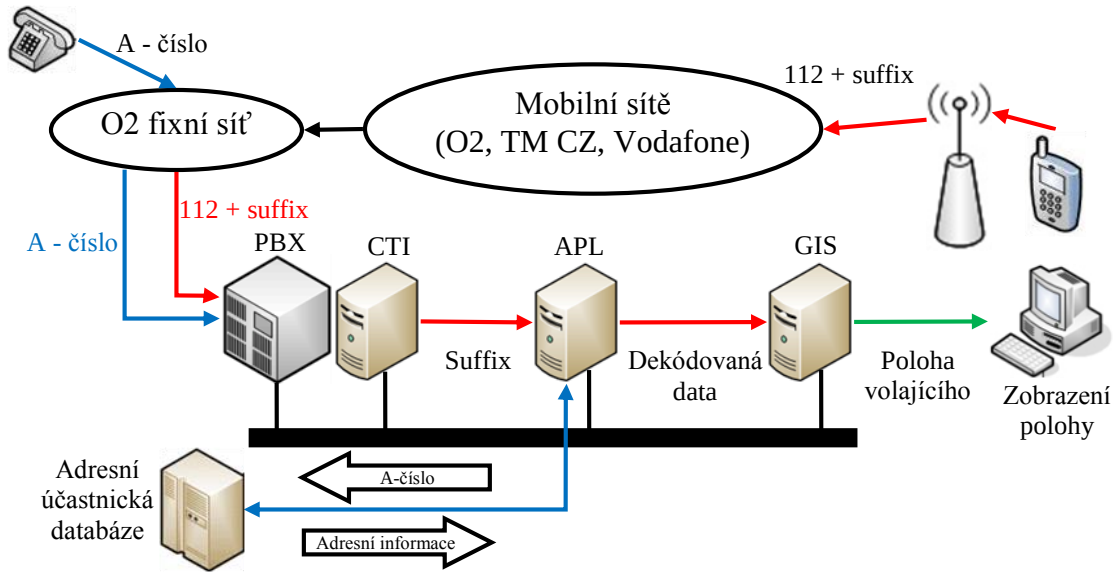
Databáze INFO35 obsahuje lokalizační informace o každé pevné telefonní stanici. To znamená, že ke každému telefonnímu číslu existuje záznam o jeho vlastníkovi a jeho adresa ve strukturované podobě. K určení adresy je použit Registr územní identifikace, adres a nemovitostí (dále jen RÚIAN). RÚIAN zprostředkovává i údaje o vlastnictví z informačního systému katastru nemovitostí. Jako jediný registr vede také nereferenční údaje, kterými jsou tzv. „technickoekonomické atributy“ budov (počet podlaží, výměra, připojení na plyn, kanalizaci, vodu, způsob vytápění, atd.).

Z databáze INFO35 se následně vrací XML dokument, ten je zpracován a všechny důležité informace jsou zobrazeny jak v textové podobě v dispečerském SW, tak v GIS aplikaci.

Jedná-li se o telefonní hovor, který je zprostředkován mobilní sítí, je velmi podstatné jaký operátor volání zprostředkoval. V systému jsou implementovány dva způsoby identifikace místa volání. První je vázán na tzv. indexy oblastí.

V případě druhého přístupu identifikace, je přijata přímo souřadnice v systému WGS84, která opět reprezentuje pravděpodobnost výskytu volajícího. Dispečer však musí být s touto skutečností vhodně obeznámen, aby nenabyl dojmu, že místo je přesné. Jistou míru vágnosti přisuzují přesně vyobrazené souřadnici kruhy, které se zobrazují se středem v přijaté souřadnici. Jejich poloměr je jistým způsobem nepřímo úměrný počtu obyvatel v dané lokalitě.

V obou způsobech interpretace dostává dále dispečer informaci o obci odkud je voláno a zároveň je GIS klientem vyslána informace o lokalitě dispečerské aplikaci. Ta pak v textové podobě „předpřipraví“ místopisné entity pro určení místa události.




Obr. 11 Systém určení polohy volajícího [41]

Volání na příslušnou tísňovou službu využívá směrování pomocí tzv. NIRA (Network Independent Routing Address) kódu. NIRA kód je směrový znak určitého místa v síti (řídící ústředny HOST) v „naddekadickém formátu“. Tento kód jednoznačně určuje, že všechna volání jsou směrována do konkrétní ústředny HOST.

Lokalizace je provedena na základě kraje (oblasti) umístění přípojného koncového bodu. Každé oblasti je ze strany poskytovatele pro linky tísňového volání přiřazen tzv. NRN kód (Network Routing Number), na základě kterého je hovor směrován na příslušné (spádové) TCTV 112. Směrování čísel doplňkových služeb typu 1x… musí být zajištěno ve tvaru NRN + číslo služby (formát směrování Exxxxyyy, např. E2134158. Exxxx vyjadřuje číslo NRN dle směrových tabulek sestavených operátorem. Směrování v síti TCTV je realizováno pomocí TOID ve tvaru: E TOID yyy, kde yyy je např. 150.

TOID jednoznačně určuje, odkud se volání uskutečnilo a je využito ke směrování na operátora v příslušném regionu a představuje sufix polohy.

Suffix je speciální kód, určující přesnou polohu volajícího z mobilní sítě. Volání účastníků ze všech mobilních i fixních sítí jsou směrována k vybranému HOST v síti O2, kam je přes ISDN30 svazky připojen na jeden z 3 platforem TCTV 112. U mobilních sítí systém TCTV 112 využívá tzv. push systém, kdy mobilní operátor on-line předává informaci o zpřesněné poloze volajícího v suffixu B-čísla (112, 150). U sítě pevné linky TCTV 112 na základě A-čísla volajícího posílá dotaz do databáze INFO 35 obsahující adresní informace o všech pevných linkách.

### 2.4.4 Systém eCall 112

Součástí systému tísňového volání 112 je systém eCall. Systém eCall je zaváděn na základě Směrnice evropského parlamentu a rady č. 2010/40/EU ze dne 7. července 2010, o rámci pro zavedení inteligentních dopravních systémů v oblasti silniční dopravy a pro rozhraní s jinými druhy dopravy. V této směrnici byla specifikována opatření pro harmonizované poskytování interoperabilní služby eCall v celé Unii, včetně dostupnosti požadovaných palubních dat ITS, která mají být vyměňována. Dostupnosti nezbytného zařízení v centrech pro tísňová volání, která přijímají data vysílaná z vozidel. A opatření usnadňující elektronické výměny dat mezi vozidly a pro tísňová volání [44]. Impulsem pro zavedení systému byly výsledky analýzy dopravních nehod, při níž bylo zjištěno, že když je dopravní nehoda rozpoznána neprodleně a je rovněž známá i poloha, zkrátí to dobu k poskytnutí pomoci ve městech o 40 % a mimo město až o 50 % [45].

Systému eCall předcházel projekt HeERO (Harmonized eCall European Pilot), jehož úkolem bylo testovat dostupné standardy pro eCall. Projekt HeERO byl spolufinancován prostředky Evropské komise v rámci programu ICT PSP a na jeho zavádění se podílely země jako Chorvatsko, Česká republika, Finsko, Německo, Řecko,

Itálie, Nizozemí, Rumunsko a Švédsko [45]. Součástí projektu HeERO bylo i přeshraniční testování s ruským systémem tísňového volání z vozidla ERA-GLONASS, který je v mnohém podobný systému eCall.

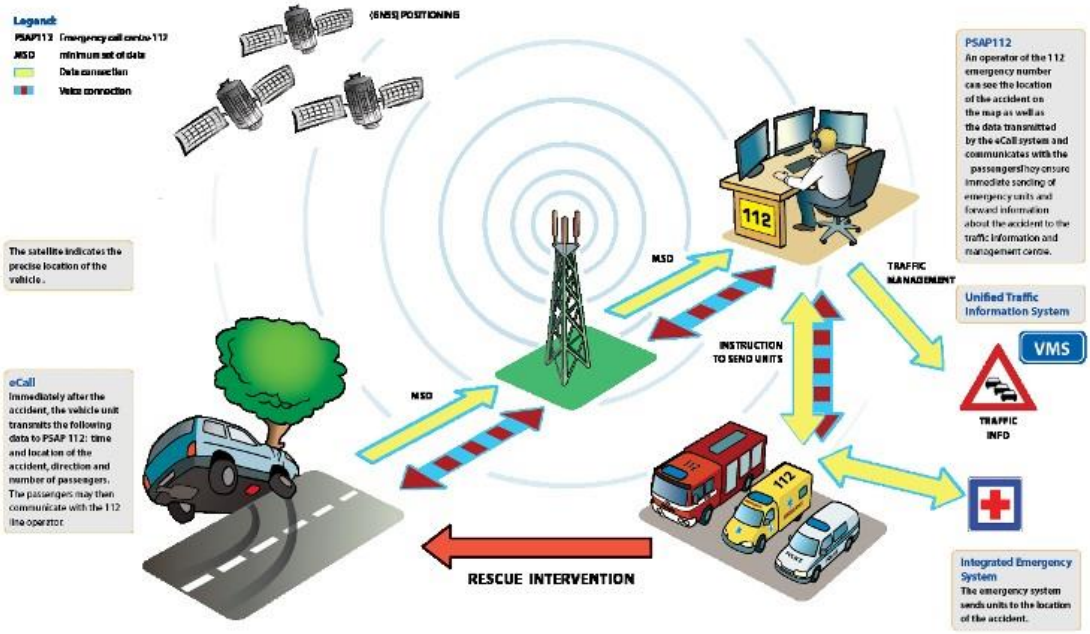
Testování probíhalo s více než 100 vozidly, která simulovala dopravní nehody. Přičemž bylo ověřováno, zda přenos dat o nehodě a hlasové spojení na tísňové centrum 112 funguje bez závad. Projekt byl v ČR od roku 2011 úspěšně realizován a testován GŘ HZS, Ministerstvem dopravy a společností Telefónika O2.Dále se na vývoji PSAP podílely společnosti NextiraOne Czech (telekomunikační část PSAP), MediumSoft (aplikační část PSAP) a Telematix (návrh OBU jednotky, konzultace v oblasti telematických služeb a ITS). Především se kladl důraz na ověření realizace příjmu a zobrazení eCall dat na testovacím systému služby TCTV 112 a jejich předávání v reálném čase ostatním složkám IZS podílejících se na zásahu. V rámci testování ČR provedla jako jediná země provedla ověření funkčnosti systému eCall prostřednictvím reálného crash testu vozidla vybaveného prototypem jednotky eCall dne 18. září 2013. Projekt HeERO byl ukončen k poslednímu dni roku 2013[46].

Zavedení služby eCall do života bylo určeno vydáním Rozhodnutí evropského parlamentu a rady č. 585/2014/EU ze dne 15. května 2014, o zavedení interoperabilní služby eCall v celé EU [47]. Nejpozdější termín zavedení byl v článku č. 1 stanoven na den 1. října 2017. Dále bylo nařízeno, aby vyřizování volání v rámci služby eCall bylo pro uživatele v celé Unii bezplatné.

Neméně důležitým legislativním prvkem zavedení služby eCall je Nařízení evropského parlamentu a rady č. 2015/758 ze dne 29. dubna 2015, o požadavcích na schválení typu pro zavedení palubního systému eCall využívajícího linku tísňového volání 112 a o změně směrnice 2007/46/ES [48]. V tomto nařízení je stanoveno, že vybavení stávajících typů vozidel, jež budou vyrobena po 31. březnu 2018, palubním systémem eCall využívajícím linku tísňového volání 112 by mělo být podpořeno v zájmu většího rozšíření systému. U typů vozidel, které budou schváleny před 31. březnem 2018, existuje možnost dovybavit je tímto systémem na základě dobrovolnosti. Dále je z důvodu poskytování přesných a spolehlivých informací o poloze požadována kompatibilita s programy Galileo a EGNOS (European Geostationary Navigation Overlay Service).

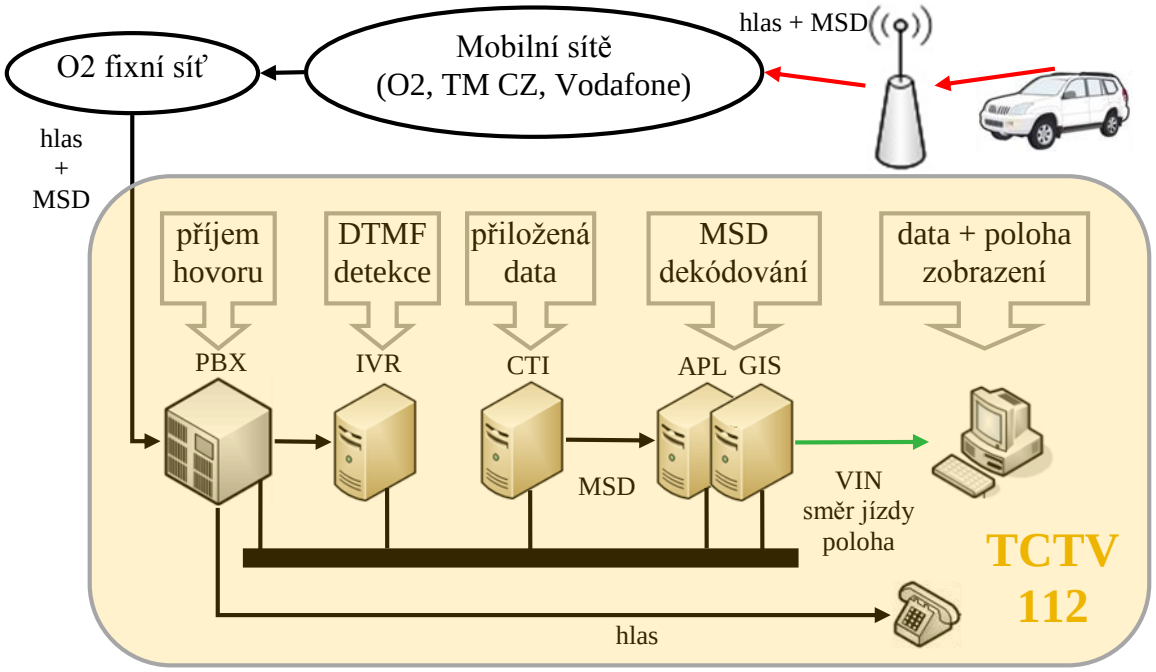
Systém eCall je aktivován v případě dopravní nehody a s využitím linky 112 požádá o pomoc. Složky IZS tak automaticky získají informace o nehodě díky datového

souboru, než je odeslán. Systém automaticky naváže hlasové spojení mezi osádkou dopravního prostředku a operátorem TCTV 112 [49].




Obr. 12 Princip fungování služby eCall [49]

Speciální jednotka eCall (OBU), jenž je vybavená SIM kartou, při aktivaci minimálně dvou čidel (airback, nárazové senzory, bezpečnostní pásy) sestaví spojení s tísňovou linkou 112.Kromě toho je možné zavolat o pomoc manuálně pomocí tlačítka umístěného v automobilu. Prostřednictvím sestaveného spojení jsou odeslána data o dopravní nehodě (pro kontrolu přijetí dat na TCTV 112 je zpět odesláno potvrzení) a zároveň s datovým připojením je sestaven hlasový kanál k operátorovi linky 112.




Obr. 13 Průběh eCall volání [49,50]

Telekomunikační část platformy tvoří dva komunikační ústředny Alcatel-Lucent OmniPCX Enterprise a CTI nadstavba Genesys. Aplikační část je rozdělena do tří funkčních částí – dispečerská, administrátorská a grafická část. Komunikační část musela splnit podmínku souběžného přenosu dat MSD mezi OBU a PSAP a hlasovým spojením. Dále byl splněn požadavek, aby informaci z eCall operátor viděl na již zaběhlém procesním modelu odbavení tísňového čísla 112. Projekt HeERO se potýkal s absencí konečných standardů služby eCall (standardy transportního protokolu pro přenos MSD.

Přenos MSD dat má na starosti blok IRV. V rámci projektu HeERO byl zkoušen multifrekvenční přenos DTMF, nicméně doba přenosu informace byla nevyhovujících 40s. Z toho důvodu bude přenos dat realizován modulací do hlasového pásma (INBAND přenos), u které se předpokládá přenos okolo 4s [51]. CTI nadstavba Genesys byla upravena, aby bylo možno zpracovat MSD data [50] a následně zobrazit v systému operátora. Obsahem MSD dat jsou zeměpisná délka a šířka místa události, směrový vektor(jednotka OBU obsahuje paměť uchovávající informaci o 5s jízdy, z těchto dat je vypočítán směrový vektor), časové razítko, VIN vozidla (z toho lze zjistit typ vozidla, stáří a barvu, pokud nebyla od výroby změněna) a jaký typ aktivace spustil systém eCall (automaticky nebo manuálně). V tab. 3 jsou uvedeny bližší informace o obsahu a velikosti

MSD zprávy, nicméně se jedná o zjednodušenou verzi. Úplný obsah a technické řešení MSD dat je řešeno evropskou technickou normou EN15722.

| *Name* | *Size* (bytes) | *Type* | *Validation* | *Description* | *Note* |
|---|---|---|---|---|---|
| Control | 1 | Integer | no | Bit7: Automatic activation<br>Bit6: Manual activation<br>Bit5: Test call<br>Bit4: No confidence in position<br>Bit3-Bit0: Reserved | 2.1.1 |
| Vehicle identification | 20 | String | The number consist of 17 characters not including the letters I, O or Q. | VIN number according to ISO 3779 | 2.1.2 |
| Time stamp | 4 | Integer | value >= 0 | UTC seconds | 2.1.3 |
| Location | 4 | Integer | -324000000 ≤ value ≤ 324000000 | Latitude (WGS-84) in milliarcseconds | 2.1.4 |
| | 4 | Integer | -648000000 ≤ value ≤ 648000000 | Longitude (WGS-84) in milliarcseconds | |
| | 1 | Byte | 0 ≤ value ≤ 255 | Direction in degrees. The nearest integer of 360.0*value/255.0 | |
| Service provider | 4 | Byte[4] | IPV4 format or blank field | Service provider IP Address or blank field | 2.1.5 |
| Optional data | 102 | String | no | Further data (e.g. crash information) or blank field | 2.1.6 |
| *Total bytes:* | *140* | | | | |

Tab. 3 Obsah datové zprávy MSD [52]

Operátor TCTV 112 zpracuje událost na základě MSD dat a pokud vyhodnotí, že se nejedná o planý poplach nebo testovací volání, zadává v systému TCTV 112 událost s příslušnou klasifikací.Vzniklá datová věta je rozeslána na jednotlivé složky IZS.
Systém eCall je navržen pro zajištění rychlé pomoci, nicméně by mohl do budoucna zajišťovat i další služby jako:

- elektronický mýtný systém;
- sledování provozu firemních automobilů;
- sledování automobilů převážejících cenný nebo nebezpečný náklad;

- zajišťovat technickou podporu speciálním druhům pojištění;
- funkce „černé“ skříňky (sledování rychlosti, připoutání bezpečnostními pásy.

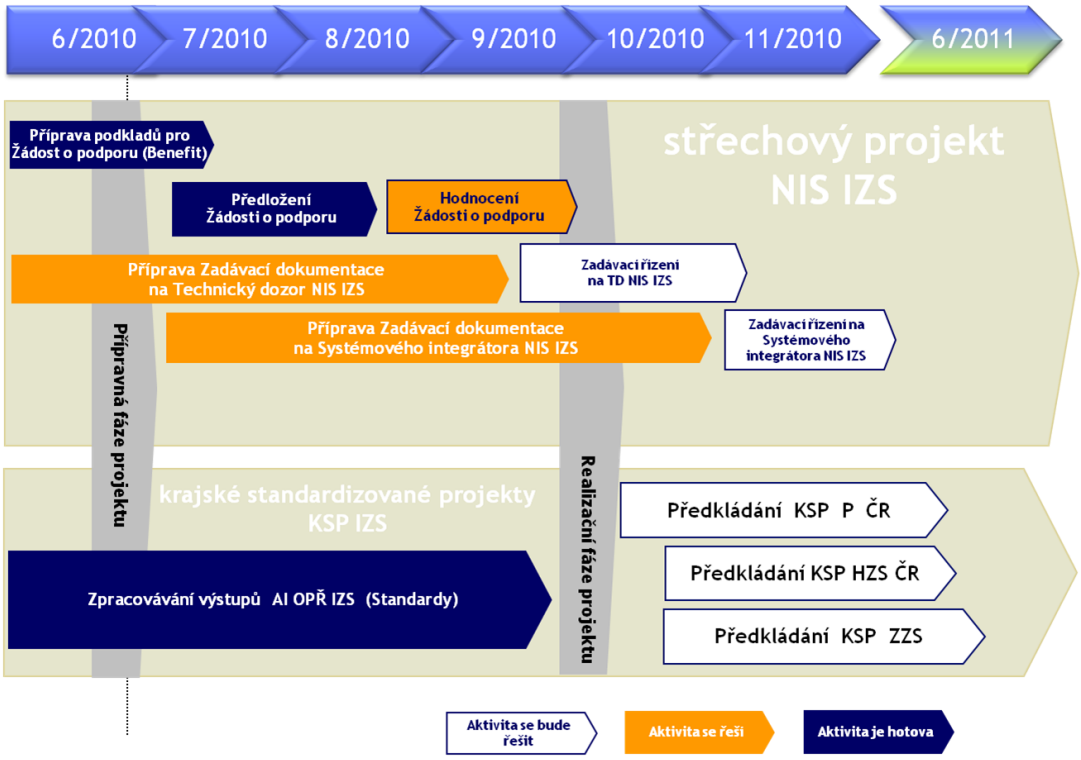
Tyto doplňkové funkce nejsou platnou legislativou schváleny a jejich zavedení se v nejbližší době nepředpokládá.

## 2.5 Program IS IZS

Při spuštění technologie TCTV 112 byly postupně získány informace o nedostatcích vyplývající z návrhu. Nebyla oddělena role operátora a dispečera u některých ZZS a nejsou zavedeny jednotné standardy vybavení. Příkladem může být i nejednotná klasifikace mimořádných událostí u všech složek IZS. Složité sdílení informací o událostech mezi jednotlivými složkami IZS (ruční zadání vlastní události). Problematická byla rovněž součinnost na místě zásahu, protože nebyla dostatečně sdílena poloha sil a prostředků zasahujících sil IZS. Jednotky neměly společný mapový základ a nebyla sdílena vlastní operační situace uvádějící prostory zásahu, rozsah zamoření, polohu velitele zásahu, dílčí uzávěry, atd.

Velitel zásahu tuto situaci musel řešit zřízením štábu zásahu, kde byly zástupci podílející se složek IZS. To v přímém důsledku vedlo ke ztížení možnosti se na daný zásah v předstihu připravit. Docházelo ke zdržení při zahájení součinnosti a řízení společných zásahů bylo obtížné.

Z výše uvedených důvodů byla zahájena práce na vývoji programu jednotného Informačního systému IZS. Záměr projektu byl formulován už v roce 2006. Nicméně projekt byl intenzivně připravován od roku 2008 definováním základních vstupů od jednotlivých složek IZS, vymezením pravidel vzájemné spolupráce a celkového plánu projektu [53, 54, 55]. V roce 2009 byla dokončena Analýza technického řešení projektu IS IZS k bližší specifikaci projektu NIS IZS a v průběhu roku 2010 byla připravena Analýza interoperability operačního řízení základních složek IZS, jenž sloužila jako základní vstup pro přípravu jednotlivých krajských standardizovaných projektů [56]. Více informací o jednotlivých fázích realizace je na obr. 14.




Obr. 14 Harmonogram realizace programu IS IZS [59]

### 2.5.1 Struktura programu IS IZS

Základní ideou struktury Informačního systému IZS byla vzájemná provázanost všech složek IZS. Zavedení společných technologií a standardů všude tam, kde jednotlivé složky vykonávají obdobnou činnost. Počet dílčích projektů v rámci programu IS IZS byl veliký s ohledem na počet zúčastněných subjektů a nutnost respektovat vlastnické vztahy s ohledem na dotační titul programu.

Gestorem programu IS IZS bylo Ministerstvo vnitra - generální ředitelství HZS ČR (dále jen MV –GŘ HZS ČR). Subjekty zapojené do přípravy jednotlivých projektů byly HZS ČR, Policie ČR, ZZS jednotlivých krajů, kraje ČR, Asociace krajů ČR a Ministerstvo zdravotnictví.

Rozpočet na realizaci Programu IS IZS byl stanoven na přibližně 2 miliardy Kč. Náklady na realizaci programu z 85% hradí strukturální fondy (SF) Evropské unie a zbylých 15 % způsobilých nákladů pokrývá rozpočtem ČR [57].

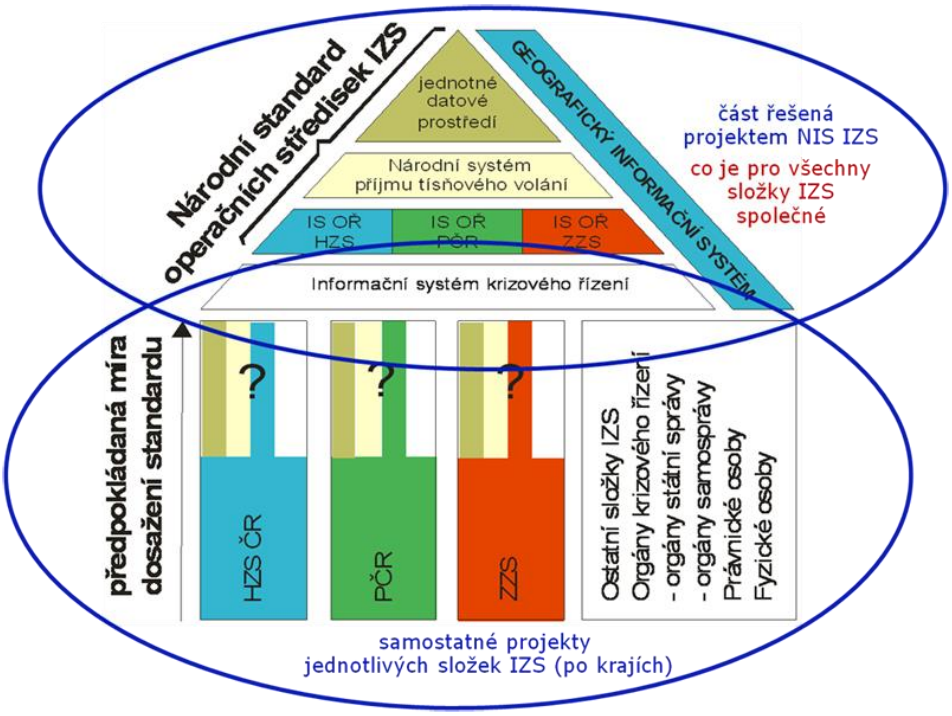
Program IS IZS byl složen z dílčích projektů:

Střechový projekt - Národní Informační Systém IZS.
Příjemcem dotace bylo MV-GŘ HZS ČR a uživateli výstupů jsou základní složky IZS a Ministerstvo zdravotnictví. Rozpočet na pokrytí realizace projektu činí 527 miliónů Kč.

Krajské standardizované projekty programu IS IZS. Příjemci dotace byly jednotlivé základní složky IZS krajů. Krajské standardizované projekty (dále jen KSP) byly realizovány ve struktuře:

- 13 x KSP HZS kraje, 1x projekt Centrální operační středisko HZS ČR + řešení společná pro složku HZS ČR, 1x KSP hl. m. Prahy (tento projekt nebyl uznán způsobilým pro financování ze SF EU, proto byl pokryt z rozpočtu HZS ČR), plánovaný rozpočet byl stanoven na 464,239 milionů Kč[58].;
- 13 x KSP Krajské ředitelství policie (KŘP), 1x projekt Centrální operační středisko PČR + řešení společná pro složku PČR, 1x KSP PČR hl. m. Prahy (tento projekt nebyl uznán způsobilým pro financování ze SF EU, proto byl pokryt z rozpočtu PČR), plánovaný rozpočet byl stanoven na 530 milionů Kč;
- 13 x KSP ZZS krajů, 1 x ZZS hl. m. Praha (tento projekt nebyl uznán způsobilým pro financování ze SF EU, proto byl pokryt z rozpočtu Magistrátu hl. města Prahy), plánovaný rozpočet byl stanoven na 494 milionů Kč.

Celkově se tedy jednalo o 45 dílčích projektů, z toho bylo 42 projektů spolufinancovaných ze strukturálních fondů Evropské unie [57].




Obr. 15 Struktura programu IS IZS [57]

Na obr. 15 je názorně zobrazena struktura programu IS IZS a funkční návaznost jednotlivých dílčích projektů. Struktura programu naznačuje funkční propojení jednotlivých součástí IZS. Jednotná struktura umožňuje sjednocení složek IZS pod jeden výkonný orgán IZS. Struktura byla navržena tak, aby akceschopnost a interoperabilita nebyla závislá na umístění.

### 2.5.2 Střechový projekt NIS IZS

Hlavním záměrem tohoto projektu bylo snížení následků mimořádných událostí v případě společných akcí více složek IZS díky rychlejším a provázanějším zásahům. To umožňuje plně dostupné tísňové volání, přesnější určení místa mimořádné události, okamžité zahájení činnosti potřebných složek, rychlejší a koordinovaná přeprava na místo incidentu.

Předpokládalo se využití jednotné technologie tísňového volání a GIS, univerzálního toku operačních dat včetně možnosti vizualizace společné operační situace a podpora pro široké využívání navigačních systémů. Proto součástí projektu NIS IZS byla i modernizace technologií, která by byla specifikována na základě informací od jednotlivých složek IZS.

Za generálním dodavatele NIS IZS (jeden ze dvou projektů) byla Vládou ČR stanovena Česká pošta s.p.. Respektive její součást Odštěpný závod ICT služby (dále jen ČP OZ ICT).

#### 2.5.2.1 Cíle projektu NIS IZS

**Nezvýšit provozní náklady IZS** - zavedením nových technologií nesmělo dojít ke zvýšení nákladů na údržbu a obnovu zařízení, ani na nákup služeb. Z důvodu udržitelnosti projektu nesmělo dojít k zvýšení počtu pracovníků (mzdové náklady) a k zvýšení počtu operačních středisek (režijní náklady).

**Zlepšit poskytování pomoci občanům při MU** - cílem projektu bylo zlepšit spolupráci složek IZS a tím dosáhnout zkrácení reakčního času pro poskytnutí pomoci postiženým.

**Zvýšit účinnost operačního řízení**- rychlost a spolehlivost operačního řízení při společných zásazích je především dána kvalitou technologií pro příjem tísňového volání a schopností sdílet operační data v reálném čase. Zavedením standardů a modernizací technologií by došlo k eliminaci prodlev a celkovému zkrácení zahájení společného zásahu.

**Zvýšit účinnost tísňového volání** - účinnost tísňového volání je dána dostupnými kanály, kterými může občan složky IZS kontaktovat. Důležitou roli hraje dostupnost GSM signálu a především rychlostí sestavení telefonického hovoru a schopností občana se na tísňovou linku dovolat jak za normální, tak za krizové situace. V případě osob hovořících cizím jazykem je nutné s co nejkratším zpožděním vyhledat operátora, který je schopen tísňové volání přijmout.

Z toho důvodu byla plánována změna při využívání jednotlivých operátorů a to ve smyslu zrušení regionálního uspořádání. V případě potřeby by byl volající spojen s jakýmkoliv volným operátorem nezávisle na území.

**Zvýšit přesnost lokalizace místa vzniku MU** - využitím kvalitního GIS, lepších možností lokalizace místa MU a sdílením dat mezi složkami IZS mělo dojít ke zpřesnění místa nasazení SaP. Tento cíl souvisí s plněním požadavků EU [60].

**Zrychlit zahájení činnosti všech nezbytných základních složek IZS** - cílem bylo minimalizovat časovou prodlevu do zahájení činnosti dalších nezbytných složek IZS.

**Zkrátit čas přepravy sil a prostředků na místo MU** - použitím moderních navigačních systémů a jednotného GIS monitorovat pohyb nasazených SaP a zkrátit tak průměrné dojezdové časy na místo zásahu.

**Zajistit využití ITS MV všemi složkami IZS** - sdílením operačních dat v reálném čase mělo dojít ke značnému zvýšení nároků na přenosy dat. Tyto dodatečné nároky, které by následně zvyšovaly provozní náklady, by byly eliminovány převedením vzájemné komunikace mezi složkami IZS na již vybudovanou infrastrukturu ITS MV.

**Zajistit jednotnou technologii pro příjem tísňového volání** - na základě analýzy možnosti útlumu národních čísel tísňového volání, kterou provedla Vláda ČR dne 23. července 2008, bylo rozhodnuto o zachování stávajících národních čísel tísňového volání. Důvodem pro toto rozhodnutí byla možnost nechat občana využít jen jednu ze složek IZS při řešení mimořádné události [61]. Uniformní vybavení všech složek IZS by umožnilo hlasové i datové sdílení i předání identifikovaných údajů kooperující složce IZS.

**Zajistit jednotný GIS** - nejednotné řešení mapových podkladů ztěžuje společnou lokaci MU v reálném čase. Jednotný GIS společný jak pro tísňové volání, tak pro podporu operačního řízení, umožní sdílená data lépe znázornit.

**Zajistit všestranný tok operačních dat** - cílem bylo zajistit přechod od hlasové komunikace ke komunikaci datové a zajistit tak plné sdílení dat o mimořádné události mezi operátory složek IZS.

**Vytvořit podmínky pro nasazení navigačních systémů** - cílem projektu bylo zavést do praxe obousměrný tok lokalizačních dat mezi zasahujícími jednotkami a systémem operačního řízení a docílit tak efektivního řízení SaP.

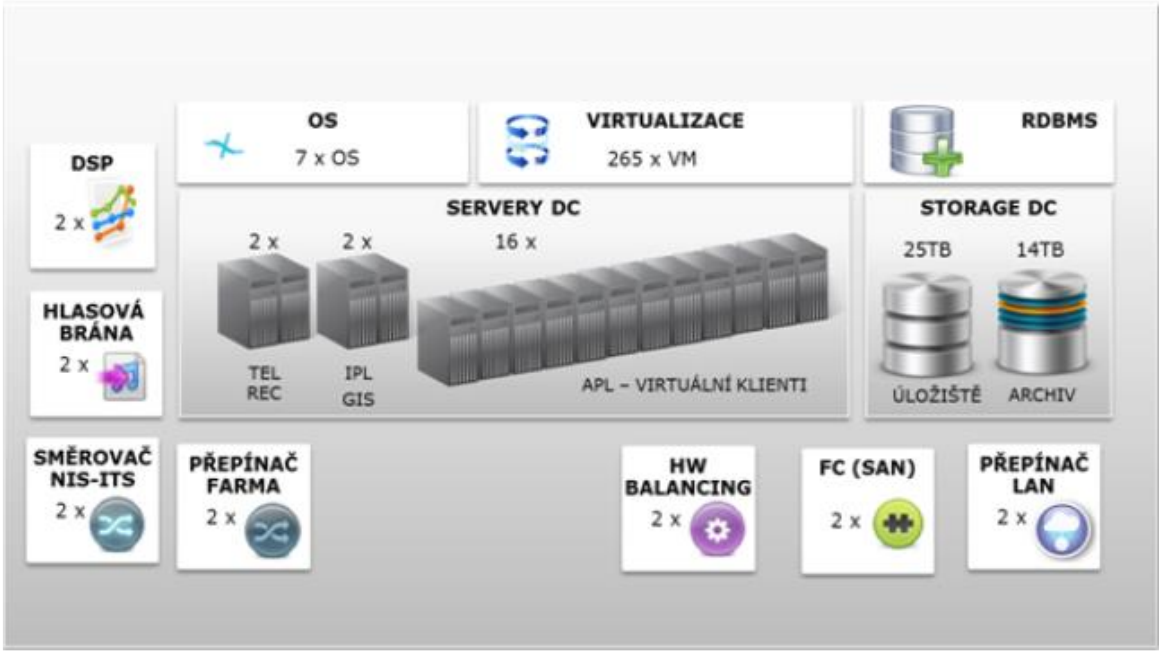
**Zajistit sdílení vizualizace operační situace** - účelem bylo zajistit pro všechny zasahující složky IZS společnou vizualizaci operační situace, která zahrnuje zobrazení místa události, hranice kontaminované oblasti, místo velitelského stanoviště, aktuální pozice velitelů anebo vedoucích složek IZS, pozici SaP složek IZS - mobilní (např. hlídky pro uzavření komunikací), zvýraznění směrů dopravy (příjezd a odjezd složek IZS, dálková doprava vody) a účelový prostor [62].

#### 2.5.2.2 Technické řešení NIS IZS

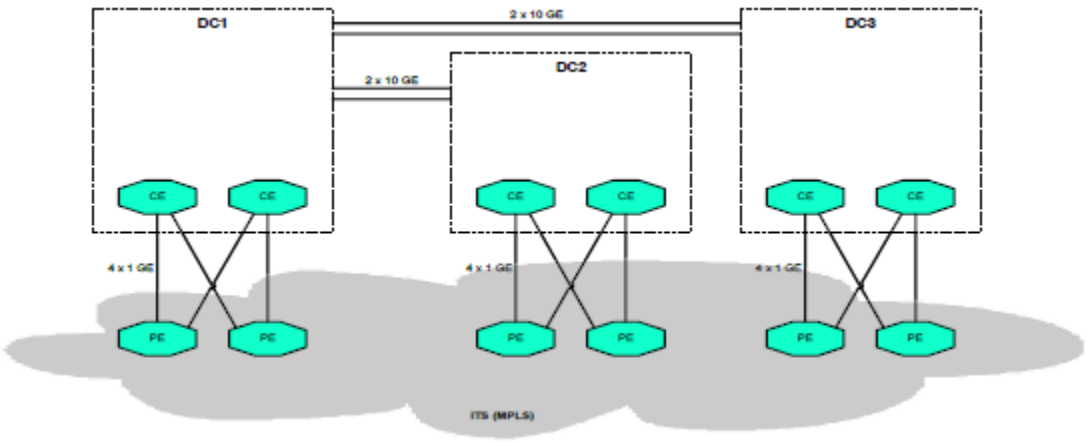
Technické řešení ČP OZ ICT vychází ze stavu z roku 2009. V rámci území byly vybudovány 3 hlavní platformy TCTV s pobočkovou ústřednou (Praha, Plzeň, Olomouc) a k těmto 3 platformám je připojeno 11 vzdálených TCTV. Projekt měl za úkol odstranit

nedostatky v komunikaci jednotlivých složek, které jsou zapříčiněny používáním nejednotných standardů.

Logický koncept řešení počítal s vybudováním tří datových center na stávajících hlavních platformách TCTV 112. U jednotlivých krajů měla být vybudována krajská operační střediska národního systému příjmu tísňového volání (NSPTV). Důležitou roli v tomto systému měl zastávat jednotný geografický informační systém. Výsledný produkt měl zajistit vzájemné sdílení informací o událostech, požadavky na součinnost a sdílení operační situace. Na obr. 16 je znázorněno plánované technické řešení datových center a na obr. 17 je předvedeno jejich vzájemné propojení.

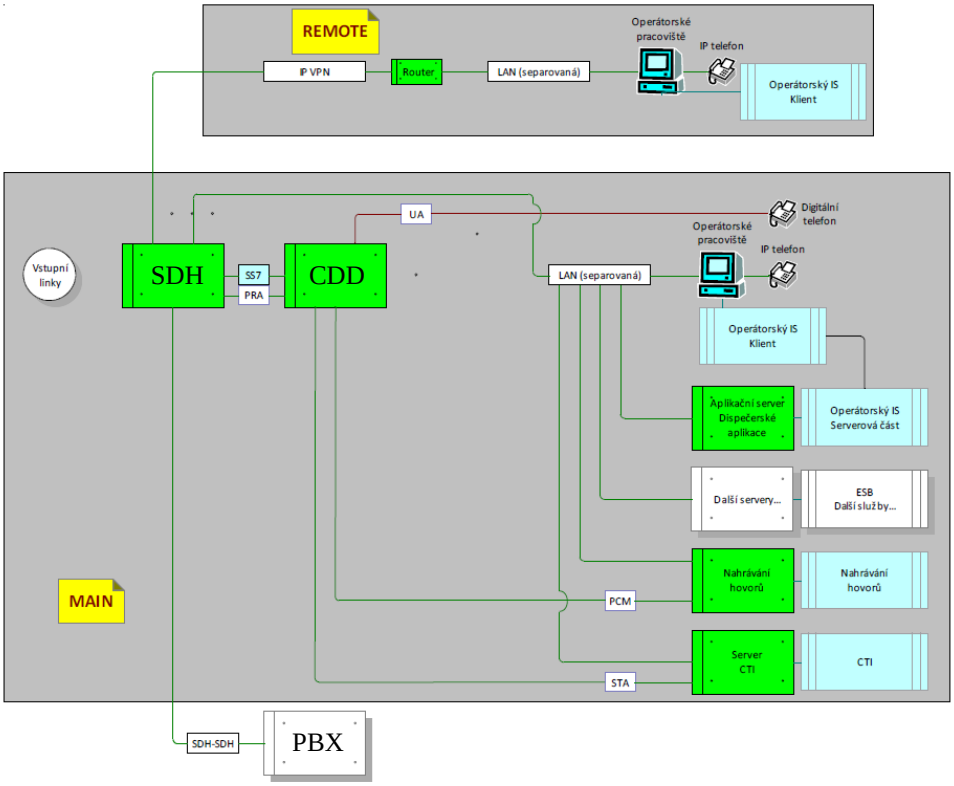



Obr. 16 Technické řešení datového centra projektu NIS IZS dle návrhu ICT služby [63]



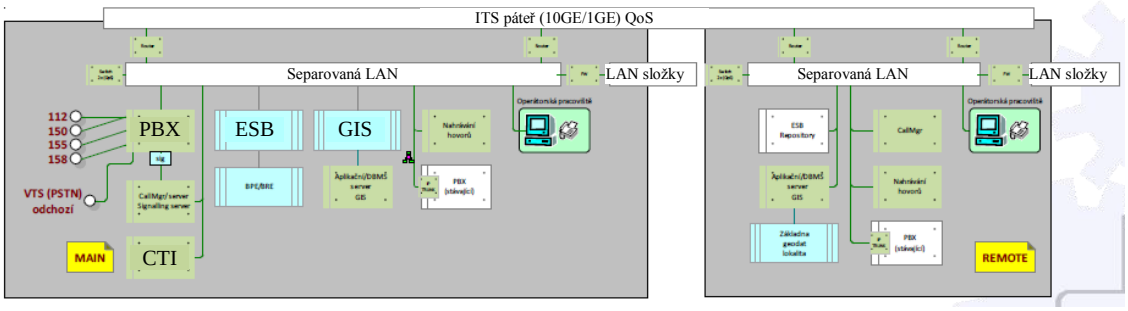

Obr. 17 Vzájemné propojení datových center [63]

Navrhovaný základní technický koncept měl plně využít výhod IP telefonie nebo využít duálního přenosu hlasu a dat nebo dokonce kombinovat oba systémy. Duální telefonie pro MAIN a plnou IP telefonii pro REMOTE. Volba konkrétního řešení měla být závislá na finančních prostředcích a licenčním podmínkám, viz obr. 18.




Obr. 18 Architektura NSPTV – kombinovaná duální telefonie [62]

NSPTV mělo být vedeno po separátní LAN a všechny klíčové prvky konektivity zdvojeny. Platformy MAIN měly fungovat jako vstupní body do systému z veřejné služby. Podle výstupu simulace měly postačit zachování stávajícího celkového počtu vstupních linek. Každá MAIN lokalita měla být připojena čtyřmi 2,048 Mbit/s ISDN30 kanály, z toho 3 by byly použity pro příchozí hovory a 1 pro hovory odchozí. V celém systému mělo být k dispozici 3x90 vstupních kanálů a 3x30 kanálů výstupních. Odchozí hovory nesnižují vstupní kapacitu systému.




Obr. 19 Architektura NSPTV – IP telefonie [62]

Vzhledem k tomu, že jediná MAIN platforma měla být schopna uřídit celou republiku, bylo nutné počet vstupních linek rozšířit na každé platformě na 270 vstupních a 90 výstupních kanálů. Lokalita primárních platforem měla být pravděpodobně zachována s ohledem na existující zdvojené připojení k veřejné síti. Minimálně platformy MAIN měly mít přímé propojení do ITS a do hlasové sítě HZS.

V rámci dalšího pokračování projektu mělo být rozhodnuto, zdali nevybudovat v Hradci Králové další MAIN platformu. Ta by sloužila během implementace pro vývoj pilotního řešení a návazně buď pro rozložení zátěže, nebo jako platforma pro vývoj a testování.

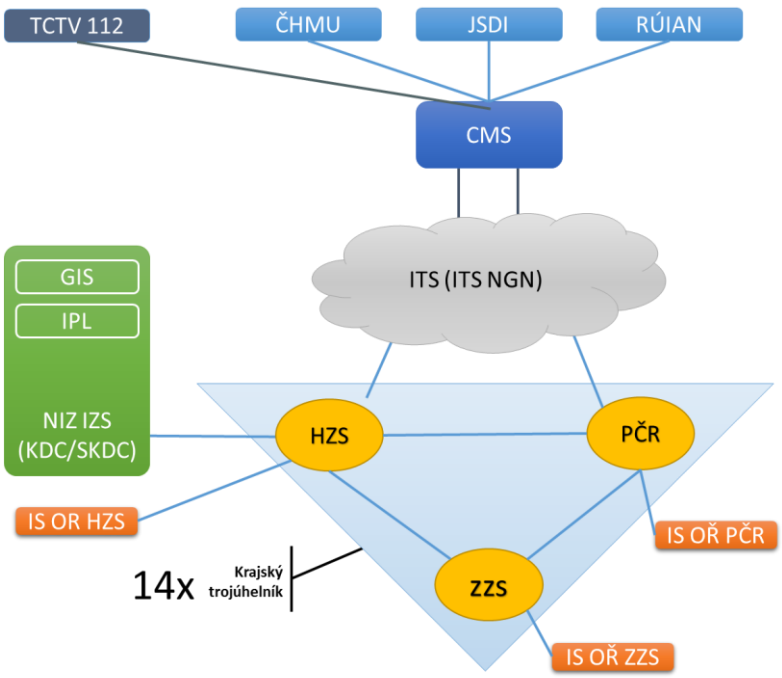
### 2.5.3 Hybridní varianta NIS IZS

V průběhu spolupráce společnosti ČP OZ ICT a GŘ HZS na vývoji NIS IZS vyvstaly pochybnosti v realizovatelnosti celého projektu ve stanoveném technologickém rozsahu a v požadovaném termínu. V rámci vývoje byl s výrazným časovým zpožděním dodán prototyp řešení NSPTV a následně byl další vývoj ukončen. Hlavním problémem při vývoji NSPTV byla nedostatečná úroveň zkušeností s projekty takového to rozsahu. Jako i častá obměna vývojového týmu i řídících manažerů, kde nově příchozí lidé na tyto pozice nastupovali s nulovou znalostí problematiky. Tyto překážky například vedly ke vzniku problémů s výběry subdodavatelů pro dodávky HW a SW vybavení. Nicméně vzhledem k tomu, že už byly realizovány některé projekty, bylo dne 16. září 2014 rozhodnuto na Ministerstvu vnitra o vytvoření hybridní varianty NIS IZS, která umožňuje minimalizovat finanční ztrátu [64].

V dubnu 2015 byly dokončeny dodávky SW a HW vybavení datových center. Dodávky byly směřovány jak ke krajským datovým centrům, tak i k 3 super-krajským datovým centrům v Hradci Králové, Plzni a Olomouci. Dodávky byly složeny z diskových polí, serverové technologie, síťových prvků a aplikací. Po instalaci bylo zahájeno testování HW a SW [65].

Ke dni 30. listopadu 2015 skončila realizační fáze krajských standardizovaných projektů HZS krajů a Centrálního standardizovaného projektu GŘ HZS. Realizace projektů probíhala mezi roky 2010 až 2015 se spolufinancováním ze strukturálních fondů EU. Projekty byly navrženy s cílem dosáhnout dokonalého propojení všech operačních středisek základních složek IZS mezi sebou bez ohledu na jejich rozmístění.

Ke dni 31. prosince 2015 skončila realizační fáze projektu NIS IZS a byl zahájen jeho provoz.




Obr. 20 Architektura hybridní varianty NIS IZS [66]

Hybridní varianta NIS IZS představuje kompromis mezi technologickými požadavky a cíli původního projektu NIS IZS. Projekt NIS IZS zahrnuje následující logické dodávky:

- Integrační platforma IZS (dále jen IPL);
- Geografický informační systém.

Integrační platforma představuje sjednocující technologickou platformu pro řízení výměny dat základních složek IZS. Lze ji rozčlenit na 3 části:

- distribuce informací o vizualizaci operační situace;
- distribuce informací o silách a prostředcích jednotek IZS;
- distribuce informací o událostech.

Infrastruktura NIS je distribuována do 14 krajských lokalit. Tři z těchto lokalit, Hradec Králové, Plzeň a Olomouc, plní také centrální funkce systému a jsou označovány jako Super krajská datová centra (dále jen SKDC). Jejich součástí je: databáze IPL; konektory na externí systémy; funkcionality pro správu a distribuci mapových podkladů; archivace záznamů a logů.

Ostatní lokality jsou označovány jako krajská datová centra (dále jen KDC). Služby umístěné v KDC je možné čerpat i z jiného KDC nebo SKDC, vyjma krajských GIS, ve kterých jsou ukládány specifické mapové podklady. Systém je navržen tak, aby se všechny SKDC mohla vzájemně v případě výpadku zastupovat [66].

Přínos projektu pro složky IZS spočívá především na efektivní výměně a sdílení dat a lepší koordinaci jednotek IZS při zásahu.

V původním projektu NIS IZS byl navíc jednotný systém pro příjem tísňového volání, který počítal s využitím principu IP telefonie. Nicméně z důvodu složitého technologického řešení bylo od záměru upuštěno.

# 3 Tísňové volání 911 v USA

Služba záchranného volání 911 se stala synonymem pro veřejnou bezpečnost v celé Severní Americe a stala se páteří záchranného systému. Tvoří důležitou součást reakce na nastalé mimořádné události, jako jsou větrné bouře, povodně, sesuvy půdy, úniky chemikálií velkého rozsahu a další.

V posledních deseti letech číslo 911 prošlo složitým vývojem ve snaze udržet krok s rozvíjejícími se formami komunikace. Stále více uživatelů používá mobilní telefony, satelitní telefony, systémy s automatickou funkcí oznámení havárie a IP telefonii. Příchod nových technologií vyžaduje změnu stálých operačních postupů, modernizaci prostředků a vybavení a přehodnocení způsobu informování obyvatel.

NENA (National Emergency Number Association) je profesionální nezisková organizace výhradně zaměřená na podporování výzkumu, plánování, školení a rozvoje technologií tísňového volání v USA a Kanadě. Spolupracuje s výzkumnými pracovníky z univerzit a podílí se na zavádění nařízení komise FCC (Federal Communications Commission) do života.

## 3.1 Historie

První použití tísňové linky 911 je zaznamenáno v únoru 1968 ve městě Haleyville ve státě Alabama. Nicméně cesta k zavedení linky tísňového volání 911 začala mnohem dříve.

Zavádění tísňového volání inicializovala komise pro vymáhání práva a výkonu spravedlnosti (Commission on Law Enforcement and Administration of Justice) v únoru 1967.Tutokomisisestavil 36. prezident Spojených států amerických Lyndon Baines Johnson. Komise doporučila, aby policejní složky měly jediné celostátně platné číslo, na které by obyvatelé v případě nouze volali. Doporučení se v této době týkalo především metropolitních oblastí země, ale do budoucna mělo být zavedeno po celém území. Po tomto opatření volala především asociace hasičů, která reagovala na vyšší počet úmrtí při požárech v porovnání s okolními státy.

Dne 3. června 1967 Komise pro vědu a technologii vydala závěrečnou zprávu [67] určenou Komisi pro prosazování práva a výkonu spravedlnosti. Ve zprávě je popisován vzorový případ, kdy postižený byl lupičem okraden o veškerou hotovost a nemá možnost

volat policii pomocí běžné linky. Většina velkých měst má síť policejních telefonních přístrojů „call boxes“. Nicméně tyto přístroje byly nenápadné a veřejnosti nepřístupné. Z provedené analýzy vyplynulo, že zpřístupnění policejních call boxů veřejnosti nepřinese dostatečný užitek. Při pokusu o zavolání policie z běžného telefonu byl volající konfrontován s ohromující řadou policejních jurisdikcí a souvisejících telefonních čísel (50 telefonních čísel na policejním oddělení v rámci Los Angeles Country). Komisí bylo doporučováno zavedení jednotného čísla tísňového volání po vzoru Velké Británie, kde je zavedeno univerzální číslo tísňového volání 999.

V listopadu 1967 proběhlo jednání mezí Bílým domem a komisí FCC a závěry byly podstoupeny společnosti AT & T, jenž byla v té době hlavním poskytovatelem telefonního spojení. Dne 12. ledna 1968 představitelé společnosti AT & T na tiskové konferenci ve Washingtonu DC představili číslo 911 jako univerzální číslo tísňového volání [68]. Systém byl adaptován a rozvíjen několika telekomunikačními společnostmi až do nynější podoby Enhanced911 (dále jen E911).

SystémE911 automaticky zjistil polohu a identitu volajícího. První takto upravený systém byl spuštěn ve městě Chicago v roce 1976 [69] a poskytoval služby hasičských jednotek a jednotek policie. Služba tísňového volání E911 je nyní přístupná prakticky ve všech metropolitních oblastech USA a Kanady.

Dne 26. října 1999 byl vydán důležitý Zákon o bezdrátových komunikacích a veřejné bezpečnosti (The Wireless Communications and Public Safety Act 106–81) [70], nicméně je znám jako Zákon 911. Tento zákon posílil roli tísňového čísla 911 ve všech státech unie jak u pevných telefonních linek, tak i bezdrátových telefonů.

## 3.2 Telefonní systémy USA

Telefonní sítě USA se v mnoha aspektech liší od sítí, které jsou provozovány v evropských zemích. V České republice a ve většině dalších zemí po celém světě jsou telefonní sítě spravovány organizacemi, které patří státu a jsou tak přímo řízeny zákonnými normami. V USA jsou vlastníky a provozovateli spojových prostředků (včetně veřejných telefonních sítí) různé komerční organizace, které poskytují spojové služby. Podstatné přitom je, že tyto instituce, označované jako Common Carriers (CLEC), nejsou státními institucemi, ale organizacemi soukromého sektoru.

Stát si zachoval právo tyto instituce regulovat a provádět nad nimi technický dozor. Další podstatnou věcí je, že určuje maximální výši poplatků za poskytované spojové služby, které si tyto organizace mohou účtovat. Za účelem řízení a technického dozoru byla v roce 1934 založena jediná organizace s celofederální působností, Federal Communications Commission. Do pravomocí FCC spadají komunikace z/do zahraničí a komunikace mezi jednotlivými státy v rámci USA. V každém z těchto států je pak instituce nazývaná Public Utilities Commission (dále jen PUC), která má místní působnost [71].

Poskytovatelů spojových služeb je v současné době v USA kolem 1200 [72]. Mezi největší patří firmy AT&T, Bell, MCI Communications, US Sprint a General Telephone and Electronics. Existence více poskytovatelů spojových služeb znamená jejich vzájemnou konkurenci, a v důsledku toho i existenci různých tarifů za spojení mezi stejnými místy.

### 3.2.1 Problémy vzniklé zaváděním IP telefonie

Přechodem na IP telefonii přestalo mít mnoho předpokladů, na nichž fungoval stávající systém tísňového volání 911, smysl. Problémy vznikají v pojetí technologie Public-Safety Answering Point (dále jen PSAP), kdy PSAP pracuje přímo s IP telefonií nebo IP telefonii pracuje jen přes gateway. Hovoříme tedy o PSAP, které pracují s IP telefonií, anebo „staré“ PSAP (Legacy PSAP). Současný systém je založen na soukromých subjektech, které zabezpečují aktualizace lokalizačních dat (adresy atd.). Nicméně v IP telefonii nespravuje systém mapování pouze jediná spádová společnost. IP služby lze získat od jedné společnosti a adresy (např. SIP URL) zase od jiné společnosti.

### 3.2.2 Lokalizace IP zařízení

Stejně jako u e-mailových adres, SIP URL nejsou spojeny s jedním místem nebo dokonce s konkrétní IP adresou. PSAP navržené pro práci s IP telefonií již nepotřebují při přijímání SIP přístup k IP adrese nebo MAC adrese od té doby, kdy SIP signalizace zpravidla prochází více routery. Jinak řečeno, žádný z běžných identifikátorů, které jsou zhruba ekvivalentem telefonních čísel, nemůže spolehlivě identifikovat přístroj volajícího a jeho umístění. Zapojením VPN sítí se tento problém ještě prohloubí, protože to může

způsobit, že terminály mohou být pokládány za součást místní sítě LAN, třebaže jsou fyzicky umístěny v úplně jiné síti.

Bez ohledu na architekturu sítě musíme být schopni zjistit polohu IP zařízení. Pro identifikaci polohy bude použito několik níže uvedených metod, které jsou rozděleny s ohledem na technickou náročnost, spolehlivost a na slučitelnost se stávajícími systémy. Federální komise FCC požaduje, aby poloha mobilních zařízení byla v 67 % případů zjištěna s přesností v okruhu 50 m a pro oblast 150 m v 95 % případů [73]. Na druhou stranu ale neexistuje norma pro specifikaci informací o nadmořské výšce, ačkoliv tento aspekt je u výškových budov podstatnou informací.

Metody pro určení polohy je možné rozdělit do 3 následujících skupin: metoda založená na cílovém místě (target-based), metoda založená na dotazu (querier-based) a hybridní metoda.

- Metoda mechanismu cílového místa – zařízení, které má být lokalizováno, určí vlastní polohu, a pak ji odešle přes komunikační kanál tazateli.
- Metoda založená na dotazu – metoda pracuje na opačném principu, poloha je určena pomocí dotazů na terminálové zařízení.
- Hybridní metoda kombinuje přístup obou předchozích metod.

Metoda založená na dotazu spojuje správu sítě pomocí protokolu CDP (dále jen Cisco Discovery Protocol) [74], příkaz traceroute protokolu ICMP (dále jen Internet Control Message Protocol) [75] a protokol ARP (Address Resolution Protocol - používá se pro převod síťové adresy IPv4 na fyzickou adresu MAC) do jediné funkce mapping. Funkce mapping, jak již název napovídá, mapuje jméno zařízení (host name) nebo IP adresu rozhraní a výrobní číslo zařízení. Je při tom použita funkce traceroute, která je používána k nalezení posledního routeru před koncovým zařízením.

V závislosti na nastavení tato adresa může být použitelná pro SNMP dotazy (Simple Network Management Protocol je protokol určený pro správu sítí, umožňující sběr dat a jejich následné vyhodnocování). Pokud dané zařízení vyrobila společnost Cisco, bude využit protokol CDP, který umožňuje identifikovat další zařízení připojená za tímto routerem a jejich rozhraní pro správu.

Dalším nástrojem pro zjištění polohy jsou dotazující se protokoly SNMP. Používají se ke zjištění fyzické MAC adresy zařízení prostřednictvím ARP protokolu

routeru. Stanovení MAC adresy je zabezpečeno pomocí dotazů. Dotazy na zjištění MAC adresy se žádají pro každou virtuální LAN až do té doby, než je známa kýžená fyzická MAC adresa.

IP telefon může být připojen přímo do LAN nebo může být připojen přes další síťový prvek. Za tímto účelem se používá tracer,který se pokouší určit uspořádání pomocí protokolu CDP. Tento protokol, jenž je nezávislý na přenosovém mediu a funguje na druhé vrstvě referenčního modelu ISO/OSI, běží v drtivé většině síťových zařízení a je používán pro sdílení informací o jiných přímo připojených sousedních zařízeních. Protokol CDP se používá k získání HW platformy, IP adresy a názvu rozhraní sousedních zařízení.

Každé zařízení, které je konfigurované pro CDP posílá periodické zprávy, tzv. oznamovače. Oznamovače obsahují různé informace jako je: HW platforma, IP adresa a název rozhraní a dobu uchování (hold-time), což je čas, po který si přijímací zařízení ponechá konkrétní CDP informaci předtím, než ji smaže. Každé zařízení také zjišťuje obsah CDP zpráv odeslaných z jiných zařízení, aby zjistilo informace o jednotlivých sousedech.

Mezi často využívané protokoly patří protokol LLDP (dále jen Link Layer Discover Protocol). Stejně jako protokol CDP, pracuje i LLDP na 2. vrstvě (linková vrstva), ale patří mezi otevřené standardy. Je standardizován dle IEEE 802.1AB-2009 a je používán mnoha výrobci (např. HP, Juniper). Jedná se o jednocestný protokol, který pouze vysílá informace pomocí multicastu a přitom nedochází k žádnému potvrzování přijatého oznámení nebo k navazování spojení. Aktivní prvek pomocí protokolu LLDP odesílá přes své porty informace o sobě ostatním zařízením v síti. K odesílání dochází periodicky (nejčastěji každých 30 nebo 60 vteřin) nebo při změně na aktivním prvku.

V oznámení může být poměrně dost informací, povinné jsou:

- MAC adresa;
- ID portu, přes který bylo oznámení odeslané;
- TTL – doba platnosti.

Dále se mohou posílat informace o názvu zařízení, verzi softwaru, IP, VLAN apod.

Každý záznam má časově omezenou platnost. Po přijetí nového oznámení se platnost prodlouží. Pokud oznámení přestane přicházet, tak je po vypršení času takové zařízení zapomenuto[76].

Informace o okolních zařízeních lze rovněž získat pomocí sledování portů. Jeden port s mnoha MAC adresami ukazuje, že je další switch nebo jiný síťový prvek v cestě k IP telefonu nebo jinému zařízení[77]. Hlavní omezení tohoto přístupu je, že je pravděpodobně omezeno dotazování uvnitř stejné administrativní domény.

Jakmile určíme zásuvku v síti, pomocí databáze zařízení zjistíme přesné umístění každého zařízení. Bohužel toto funguje pouze u řízených hubů a switchů, navíc to vyžaduje přesnou a aktualizovanou databázi struktury sítí. Protože, i když je zjištěna poloha aktivního prvku, díky délce navazujícího vedení (UTP, optický kabel) může být koncové zařízení vzdálené i stovky metrů.

U IP telefonie lze použít i jiné mechanismy pro určení polohy koncových zařízení, jako například kombinace z následujících:

**Ruční vstup**–u tohoto mechanismu se počítá s tím, že je uživatel nucen uvést svoji polohu. Tento princip má nespornou výhodu, není-li dané zařízení často stěhováno. Pokud je zařízení neustále přemísťováno, může ověřit, zdali je umístění platné.

**Ethernetové vylepšení** – funkce ethernetových switchů mohou být rozšířeny tak, aby pravidelně posílaly pakety s polohou z každého portu. V typických více switchových sítích ethernet, by mělo každé zařízení přijímat pakety s polohou. Pakety samotné už ale poskytují jen přídavnou informaci (např. číslo popisné budovy, patro, číslo zásuvky, atd.). Taková funkce je užitečná pro správu majetku. Dokonce i bez úpravy switchů, může být tento přístup snadno implementován pro hrubou (nepřesnou) lokaci uvnitř objektu, pokud není síť vyvedena ven z budovy.

**Chytré zásuvky** – samy zásuvky jsou aktivními zařízeními s funkcí switche a dotazují se na MAC adresu připojených zařízení, vyrábí např. společnost Panduit [77].

**Téměř bezdrátové přístupy** – standardní GPS zařízení nefunguje v budovách, proto lze k odečtení polohy použít signál stanic BTS. Zjištěná poloha je s přesností na 100m, což je zejména ve výškových budovách s desítkami nebo dokonce stovkami pater nedostatečné.

**Bezdrátové sítě LAN** – některé IP telefony používají standardy IEEE 802.11a/b/g/n technologie Wi-fi [79] pracující na 2,4 a 5 GHz ke komunikaci s místními

sítěmi LAN. Použití těchto technologií je limitováno dosahem, proto odhad polohy IP telefonu vychází z polohy základnové stanice. Odhad polohy může být zlepšen měřením intenzity signálu jedné nebo dokonce i více základnových stanic a následným porovnáním s mapou pokrytí signálem.

### 3.2.3 PSAP pro IP telefonii

Přechod center tísňového volání na IP telefonii přináší nové možnosti, ale zároveň i nové problémy. PSAP, spolupracující se s internetem, umožňuje nabídnout daleko bohatší nabídku komunikačních služeb, např. operátoři pomocí video-hovoru mohou mluvit s osobami znakovou řečí nebo mohou získat lepší přehled o situaci na místě zásahu a účinněji tak poskytnout odborné vedení při poskytování první pomoci. Momentálně je možné pomocí speciálního zařízení Telecommunications Device for the Deaf (dále jen DDT) [80] poslat textovou zprávu s pokyny, ale tato zařízení nejsou dostupná široké veřejnosti. Další možností, kterou lze uskutečnit pomocí internetu, je přenos biometrických dat od pacienta, který je doma, přímo operátorovi.
Stávající PSAP požadují vysoce specializovanou infrastrukturu. Kdežto PSAP pracující s IP telefonií si vystačí pouze se síťovým připojením na počítač, což může být praktické například v případě nezbytných přesunů při živelných pohromách. Protokol SIP umožňuje příchozí hovor distribuovat na více míst najednou nebo postupně do té doby, než někdo odpoví na hovor. Paralelní distribuce hovoru umožňuje rovnoměrně rozdělit zatížení jednotlivých PSAP. Zatím co sériové distribuování hovorů vytváří fronty, u kterých je hovor po jisté době čekání automaticky přepojen na záložní PSAP.

Problémy u PSAP pracující s IP telefonií jsou podobné jako u starších verzí PSAP. I přes přidané opatření, technologie IP telefonů nemůže zajistit průchod hovoru na jakékoliv PSAP ve všech případech. Níže je uvedena architektura, pomocí které jsou tyto problémy řešeny. Pro porovnání technologického vybavení jsou na obr. 21 - 23.

Obr. 21 Komunikační centrum na počátku 80. let [81]

Obr. 22 Komunikační centrum v roce 2007 [81]

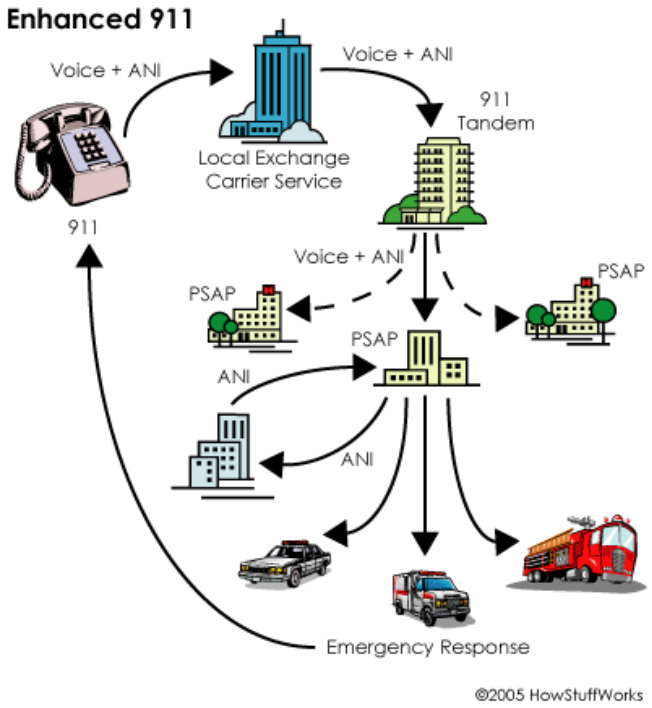
Obr. 23 Současné komunikační centrum [81]

### 3.2.4 Určení polohy u systému E911

Určení polohy je pro správnou funkci systému E911 nezbytné a využívá se k tomu databáze ALI (dále jen Automatic Location Information) [82]. Databáze je aktualizována

místními soukromými telefonními společnostmi ILEC (Incumbent Local Exchange Carrier) pod hlavičkou místních samospráv. Mezi největší patří společnost Verizon [83]. Databáze ALI navíc slouží jako zdroj informací pro databázi MSAG (Master Street Address Guide), která je používána ke směrování tísňového hovoru na příslušné centrum tísňového volání.

Po vytočení tísňové linky hovor prochází přes veřejnou telefonní síť PSTN na uzlovou telefonní ústřednu označovanou jako Class 4 nebo Tandem. Toto zařízení umožňuje navázat spojení s dalšími zařízeními typu Class 4 nebo Class 5 a používá se k přepínání na dálkové hovory. Typickým zástupcem je zařízení 4ESS nebo novější N4E od společnosti Alcatel-Lucent [84]. Ústředna pro svoji funkci používá výběrové směrování pro vyhledávání v databázích SRDB (Selective Routing Database) a MSAG (Master Street Address Guide). Porovnává telefonní číslo na základě vzniku výzvy k umístění v síti nebo porovnává číslo záchranné služby ESN (Emergency Service Number) příslušného centra tísňového volání PSAP. Když hovor dorazí na příslušné centrum tísňového volání, proběhne porovnání polohy s databází ALI. Výsledek je odeslán zpět na centrum tísňového volání (PSAP), kde operátor tyto výsledky porovná s výzvou volajícího na PC. Celý systém je zobrazen na obr. 24.




Obr. 24 Systém E911 [85]

Určení polohy závisí na tom, byla-li pro zavolání použita pevná linka či bezdrátový (mobilní) telefon. Dále závisí na typu sítě, kterou daný hovor procházel.

Pevná E911 (WirelineE911) je určena pro zařízení, která jsou trvale připojena k PSTN. Bezdrátová E911(WirelessE911) je určená pro mobilní zařízení jako jsou mobilní telefony. VoIP E911poskytují soukromé komerční společnosti prostřednictví sítě Internet. Pro použití VoIP E911 je nezbytné použít IP telefonní přístroj a pro tyto účely vyvinutý software. Telefonní systém MLTS (Multi-line Telephone System) nachází uplatnění na podnikových telekomunikačních sítích. Pro určení polohy volajícího, na těchto jednotlivých systémech, je nezbytné přizpůsobit a aktualizovat databázi ALI.

## 3.3 Centra tísňového volání E911 (PSAP)

Centrum tísňového volání je cílem hovoru. Jedna ústředna může obsluhovat více PSAP nebo jedno PSAP může spadat pod vícero ústředen. Území pokryté pouze jediným centrem tísňového volání je zabezpečeno složkami policie, hasičů a zdravotníků daného území. Každé centrum tísňového volání má přiděleno jedinečné číslo ESN (Emergency Service Number).

Informace o lokalitě volajícího je znázorněna systémem CAD (Computer Assisted Dispach) dispečera. První systémy CAD poskytovaly adresu volajícího v textové podobě, historii volání a dostupné jednotky záchranného systému. Nicméně v roce 1994 se poprvé podařilo na obrazovku CAD zobrazit adresu volajícího, dostupné jednotky záchranného systému a další důležité informace jako rozmístění hydrantů nebo uskladnění nebezpečných materiálů a to vše v reálném čase [86]. Krátce poté byl systém mapových podkladů standardem ve všech CAD a vyvíjen spolu s linkou 911.

### 3.3.1 Propojení PSAP

Každý poskytovatel služby (ILEC) má alespoň dvě obousměrné záložní linky o přenosové kapacitě 64 kbit/s (DS0) propojující každou ústřednu s centrem tísňového volání. Tyto linky jsou buď napojeny na centra napřímo nebo přes speciální telefonní switch na jednotlivá PSAP. Tyto speciální telefonní switche jsou známy jako 911 Selective Routers. Jejich použití je čím dál tím častější, protože zjednodušují propojení mezi sítěmi s protokolem ISUP/SS7 (ISDN User Part) a staršími systémy PSAP.

Systém centra tísňového volání si při identifikaci telefonního čísla musí umět poradit jak s impulsní volbou, tak i s tónovou volbou telefonního čísla.

### 3.3.2 Funkce E911 u pevné linky

Číslo volajícího (calling party number nebo A-number) je použito k získání informace, pod které centrum tísňového volání volající spadá. Pro zjištění polohy je PSAP telefonní číslo porovnáno s databází ALI. Samotná databáze ALI je od PSTN oddělena (zcela záměrně) a zajištěna. O databáze se starají soukromé společnosti ILEC dle smlouvy s PSAP. Databáze ALI je u každé ILEC jedinečná (mají různé formáty).

Kromě databáze ALI se používá databáze MSAG, která mimo jiné obsahuje seznamy ulic a čísla popisná. Když je vytvářen nový účet, tak je ke konkrétní adrese v MSAG hledáno číslo ESN, na které by měl být hovor nasměrován. Jiné Společnosti CLEC (Competitive Local Exchange Carriers) a další poskytovatelé pevných linek žádají o přístup do databáze ALI na základě dohody s ILEC.

V případě, že telefonní číslo volajícího není v databázi ALI (selhání databáze ALI), je hovoru přiděleno defaultní číslo ESN, které je pro tento případ od PSAP vytvořeno. Operátor v rámci hovoru s volajícím požádá o sdělení adresy a následně ho přesměruje na jeho spádové PSAP. Takovéto selhání databáze ALI jsou společnosti ILEC postihovány.

### 3.3.3 Požadavky komise FCC

FFC má několik požadavků na zabezpečení spojení jak linkovými telefony, tak i telefony mobilními:

- Základní 911: Všechny hovory na telefonním čísle 911 musí být předány do call centra, bez ohledu na to, jaký mobilní telefon nebo síť je použita.
- Fáze 1 E911: Operátor PSAP při příjmu volání z bezdrátového telefonu musí maximálně do 6 minut určit telefonní číslo, ze kterého je voláno, ale i identifikovat BTS oblasti, ve které se volající nachází.
- Fáze 2 E911: Nejpozději do 31. 12. 2005 mělo být lokalizovatelných službou 911 minimálně 95 % telefonních přístrojů. Tato podmínka nebyla splněna

3 poskytovateli (Sprint Nextel, Alltel a USCellular), proto jim FCC uložila pokutu v celkové výši 2.830.000 dolarů [87].

- Fáze 3: Fáze 3 pouze odráží stav, kdy jednotliví poskytovatelé nebyli schopni přejít na potřebnou technologii. Proto byl stanoven konečný termín implementace nejpozději do září 2012.

Provozovatelé bezdrátových linek musí ke zjištění pozice volajícího odečíst zeměpisnou šířku a délku s nepřesností maximálně 300 m během 6 minut od požadavku PSAP. Poloha není určena pouze pro složky záchranářů, aby se dostali co nejrychleji na místo, ale rovněž slouží k přesměrování na konkrétní PSAP (u mobilů).

## 3.4 Systém NG911

Podmět k vývoji nového systému tísňového volání vzešel ze strany Ministerstva dopravy (USDOT), které zároveň poskytovalo finanční prostředky pro jeho vývoj. Cílem tohoto projektu je umožnit široké veřejnosti přístup ke službám tísňové linky 911 a to nezávisle na použitém zařízení (klasické pevné telefony, mobilní telefony, VoIP telefony nebo jiných zařízeních založených na IP komunikaci). NG911 navazuje na systém E911 a přidává nové technologie založené na využití otevřených standardů (standardy, které nejsou vázány na konkrétního výrobce nebo skupinu výrobců).

Nový systém poskytuje větší schopnost požádat o pomoc nebo sdílet důležitá data s poskytovatelem záchranného systému z libovolného místa. Kromě komunikace s místním PSAP, je možné přenášet tísňové volání i na jiné PSAP kvůli sdílení důležitých údajů.


Obr. 25 Oficiální logo Next Generation 911 [88]

### 3.4.1 Účel zavedení NG911

Jak už bylo řečeno výše, rozvoj počítačových technologií a sítě internet vedl k požadavku na nový systém, který umožní jak bezproblémový provoz systémů E911, tak zároveň bude podporovat technologie založené na IP komunikaci. Velký důraz byl kladen na architekturu, která by byla založena na využití volného standardu protokolu IP/SIP.

Systém tísňového volání 911 je i přes provedené modernizace založen na desítkách let staré technologii, která nestíhá držet tempo s trendem vývoje počítačových technologií. Příkladem je nemožnost zaslání fotografií nebo videa přes stávající komunikační kanály. V tab. 4 jsou porovnány možnosti systému E911 s možnostmi NG911.

| Enhanced 911 | Next Generation 911 |
|---|---|
| Zdrojem informací je primárně hlasový hovor prostřednictví telefonu. | Zdrojem informací je hlas, text, snímky nebo video, případně kombinace uvedených, prostřednictví mnoha typům komunikačních zařízení. |
| Hlasová komunikace poskytuje minimální údaje. | Snadný přenos dat poskytuje řadu možností. |
| Místní správa systému, přenos dat a zálohování. | Je umožněn vzdálený přístup, přenos a sdílení dat a zálohování. |

Tab. 4 Porovnání možností systému E911 a NG911 [89]

Omezení systému E911 vyplývá z použité technologie – sítě s přepojováním okruhů. Kdy veškerá komunikace probíhá po předem sestaveném okruhu.

### 3.4.2 Předpoklady zavedení NG 911

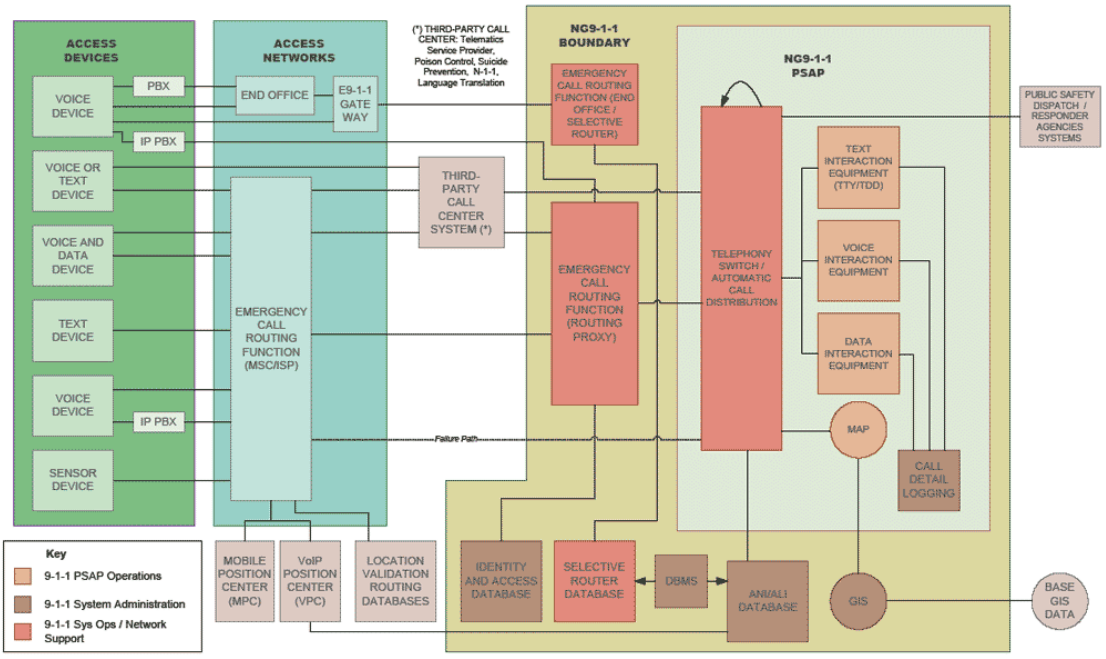
Před zahájením práce na vývoji systému byly stanoveny čtyři hypotézy, které měly zásadní dopady na samotný koncept.

- Prvním předpokladem bylo stanoveno, že bude zachována role místní samosprávy na provozování PSAP. PSAP budou moci přijímat, analyzovat a přesměrovávat hovory linky 911na místní záchranné složky.
- Druhým předpokladem bylo stanoveno, že komunikační služby budou založeny hlavně na IP telefonii.
- Třetím předpokladem bylo stanoveno, že architektura systému NG911 bude založena na využití otevřených standardů a technologií, aby byla zabezpečena budoucí flexibilita a podpora pro upgrade.

- Čtvrtým předpokladem byla stanovena podpora potřeb hendikepovaných obyvatel (úplná nebo částečná hluchota), kteří budou používat pokročilé technologie na bázi IP (např. video a interaktivní text), ale bez přímé vazby na PSAP.

### 3.4.3 Definování rozsahu projektu NG911

Pro realizacinávrhusystému NG911 bylo nutné na základě požadavků definovat samotný rozsah projektu a to především z pohledu požadavků na technologii. Požadavky na záchranné služby se můžou lišit v závislosti na místních potřebách a organizační struktuře. Nicméně každá místní NG911 síť by měla obsahovat jedno nebo více PSAP a odpovídat požadavkům na zajištění veřejné bezpečnosti. Síťová rozhraní musí umožnit příjem tísňových hovorů a zprostředkovat přenos hovoru na jiné PSAP nebo na dispečink mimo lokální síť. Dále tato rozhraní zabezpečují přístup k externím službám a databázím (např. zdravotní údaje, mapové podklady pro GIS, identifikace osob). Ačkoliv volající může poskytnout informaci o poloze, je nutné tuto skutečnost ještě verifikovat operátorem PSAP.




Obr. 26 Návrh systému NG911 [90]

Hlavní součásti systému NG911 jsou:

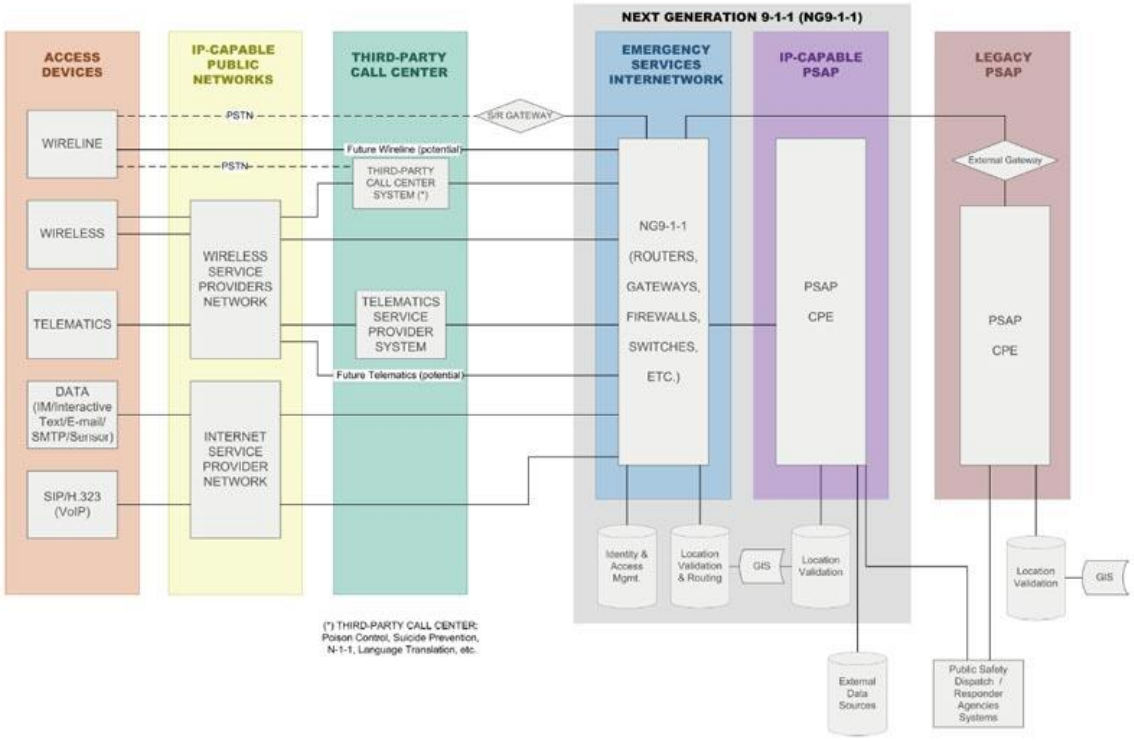
- prostředky pro zpracování přijatých dat z jiných systémů, přijatá data mají podobu textu, hlasu, obrazových dat nebo videa;
- telefonní switche a automatické přepínače hovorů ACD (Automatic Call Distributor);
- monitorovací zařízení (Call detail logging);
- systém pro zobrazení mapových podkladů a GIS;
- systém pro směrování hovorů;
- databáze pro identifikaci uživatelů, databáze selektivního routeru a databáze automatické identifikace tel. čísla ANI a automatické zjištění polohy ALI;
- rozhraní, která propojují části NG911 PSAP s dalšími podpůrnými systémy, bez kterých by nebyly doručeny nezbytné informace.

### 3.4.4 Rozhraní systému NG911

Vnitřní uspořádání mezi síťovými komponenty NG911 a vnější rozhraní je zobrazeno na obr. 27. Vzhledem ke stále probíhajícímu vývoji se toto uspořádání může změnit.

Návrh jednotlivých rozhraní systému NG911 vychází z národních i mezinárodních standardů. Tyto standardy souvisí s aplikacemi a protokoly IP komunikace systému NG911. Na vývoji standardů se především podílely standardizační organizace SDO jako IETF (Internet Engineering Task Force), ATIS - ESIF (Alliance for Telecommunications Industry Solutions - Emergency Services Interconnection Forum),ITU, TIA (Telecommunications Industry Association), 3GPP (3 rd Generation Partnership Project), APCO (Association of Public-Safety Communications Officials International) a NENA.

Je vyvíjena snaha tato jednotlivá rozhraní standardizovat a zajistit tak bezproblémovou spolupráci na hranicích jednotlivých států. Standardizace by rovněž přinesla větší počet navzájem zaměnitelných systémů, snížení ceny a širší nabídku trhu. Z toho důvodu je mezi standardizačními organizacemi i ETSI [91].




Obr. 27 Uspořádání systému NG911 (Boundary NG911) [90]

Vnitřní uspořádání obsahuje:

- rozhraní mezi PSAP CPE (Customer Premises Equipment) a síťovými prvky, rozhraní umožňuje přímé připojení centra tísňového volání k internetové síti;
- rozhraní mezi PSAP CPE a vnitřními datovými zdroji mapovacího software a databázemi GIS, zajišťuje správnou funkci mapové podpory operátory PSAP;
- rozhraní mezi síťovými prvky a databázemi systému pro zabezpečení identifikace osob, správu dat, ověřování polohy volajícího a směrování dat;
- rozhraní člověk – stroj HMI (Human Machine Interface) mezi příjemcem hovoru a prostředky pro komunikaci (např. mikrofon, sluchátky, klávesnice, kamera).

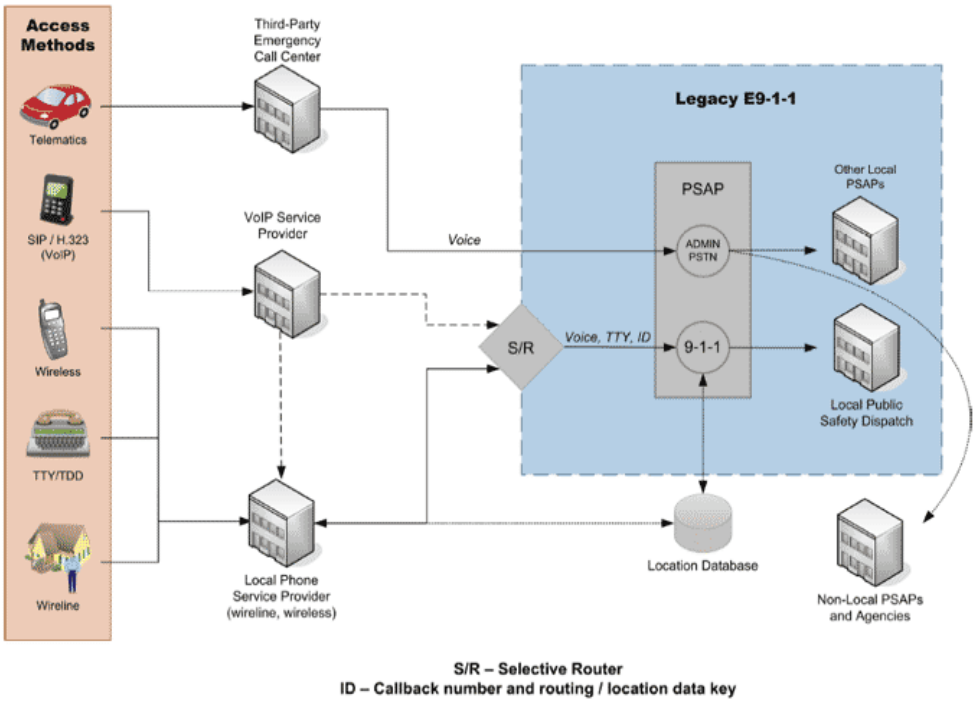
Jedno z možných vnějších uspořádání obsahuje:

- rozhraní mezi aplikacemi nebo zařízeními určenými pro IP komunikaci a síťovými prvky pro směrování hovorů ke spádovému PSAP. Toto rozhraní je vlastně souborem rozhraní, které umožňují realizovat IP komunikaci;
- rozhraní k propojení starších verzí komunikačních aplikací s aplikacemi zajišťujícími internetovou komunikaci. V průběhu přechodu na systém NG911 je provozovatelům sítí nadále povoleno používat selektivní routery;
- rozhraní mezi jinými call centry a sítí určenou pro IP telefonii;

- rozhraní mezi PSAP podporující IP komunikaci a externími databázemi (např. databáze s telematickými daty, daty geografického systému GIS nebo zdravotními databázemi);
- rozhraní mezi PSAP podporující IP komunikaci a složkami záchranného systému;
- rozhraní mezi staršími verzemi PSAP a záchrannými službami komunikujícími prostřednictvím IP komunikace. Starší typy PSAP by byly připojeny k systému NG911 prostřednictvím externí brány [90].

### 3.4.5 Porovnání komunikace systémů NG911 a E911

Níže uvedené diagramy, na obr. 28 a 29, umožňují přehledně porovnat datovou a hlasovou komunikaci staršího systému E911 se systémemNG911.

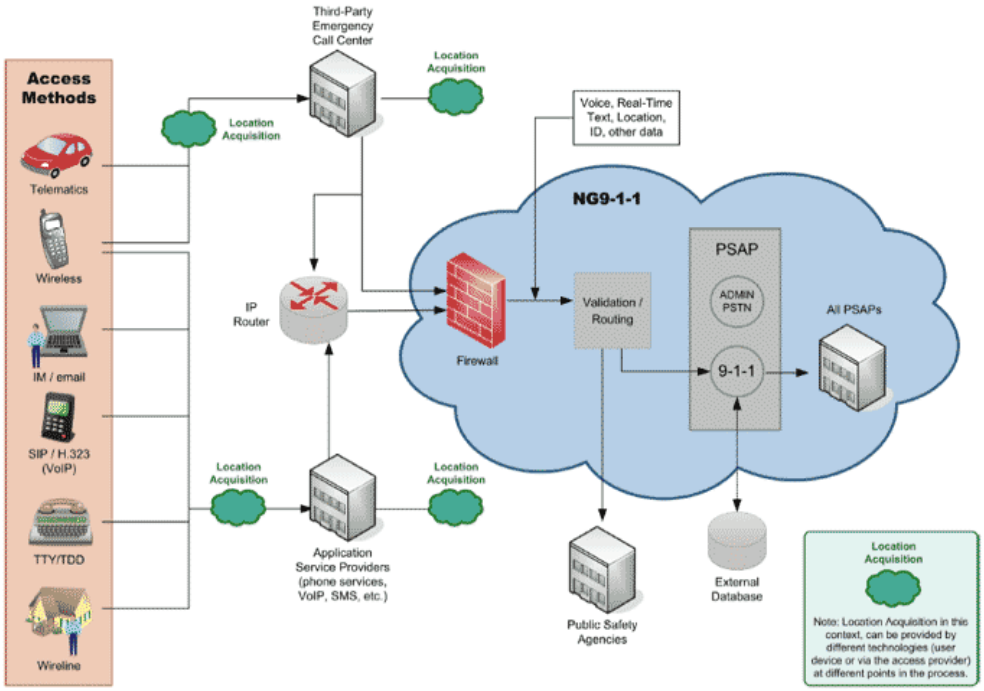



Obr. 28 Blokové schéma systému E911 [90]

Funkce volání a přenos dat u staršího systému E911 může být popsána následujícím způsobem:

- volající vytočí telefonní číslo 911 za pomoci libovolně možných komunikačních prostředků;
- hovor je rozpoznán systémem a prochází dále spolu s omezeným množstvím informací (informace o předvolbě telefonního čísla a zpětnou volbou). Poté hovor prochází až na selektivní směrovač;
- selektivní směrovač porovnává data s databází ANI, porovnává telefonní číslo a jeho předvolbu se záznamem, který má o daném místě;

- cizí PSAP mohou přistoupit do jiného PSAP prostřednictvím desetimístného čísla nebo pomocí selektivního routeru;
- poté co hovor dospěje k vybranému PSAP, koncové zařízení CPE doručí hovor a data spojená s hovorem operátorovi linky;
- ve stejnou chvíli, kdy je hovor přijat centrem tísňového volání, proběhne ověření polohy a informace o poloze je odeslána zpět do PSAP pro zobrazení na displeji operátora;
- v závislosti na charakteru tísňového hovoru nebo v jakékoliv závislosti na mimořádné události, může být hovor přepojen na jiné PSAP nebo na jiné místo příjmu, tento postup může zpřístupnit lokální i externí databáze pro zjištění dalších informací.




Obr. 29 Blokové schéma systému NG911 [90]

Funkce volání a přenos dat u systému NG911 může být popsána následujícím způsobem:

- volající vytočí telefonní číslo 911 nebo může poslat nouzovou zprávu libovolným komunikačním prostředkem;
- hovor je rozpoznán a počátečním zpracováním dat, je získáno číslo pro zpětné volání a poloha volajícího nebo kód místa volajícího, to vše prostřednictvím příslušné přístupové sítě nebo vstupem do sítě záchranného systému přes firewall;
- přístupová síť spojená připojením k síti záchranného systému může být založena na bázi IP protokolu;
- směrovací IP protokoly jsou užívány k identifikaci a směrování hovoru nebo zprávy do příslušné PSAP, nebo jsou dynamicky vybrána záložní PSAP identifikovaná směrovými tabulkami;
- poté, co hovor dorazí do vybrané PSAP, koncové zařízení CPE v PSAP doručí hovor a data spojená s hovorem operátorovi;

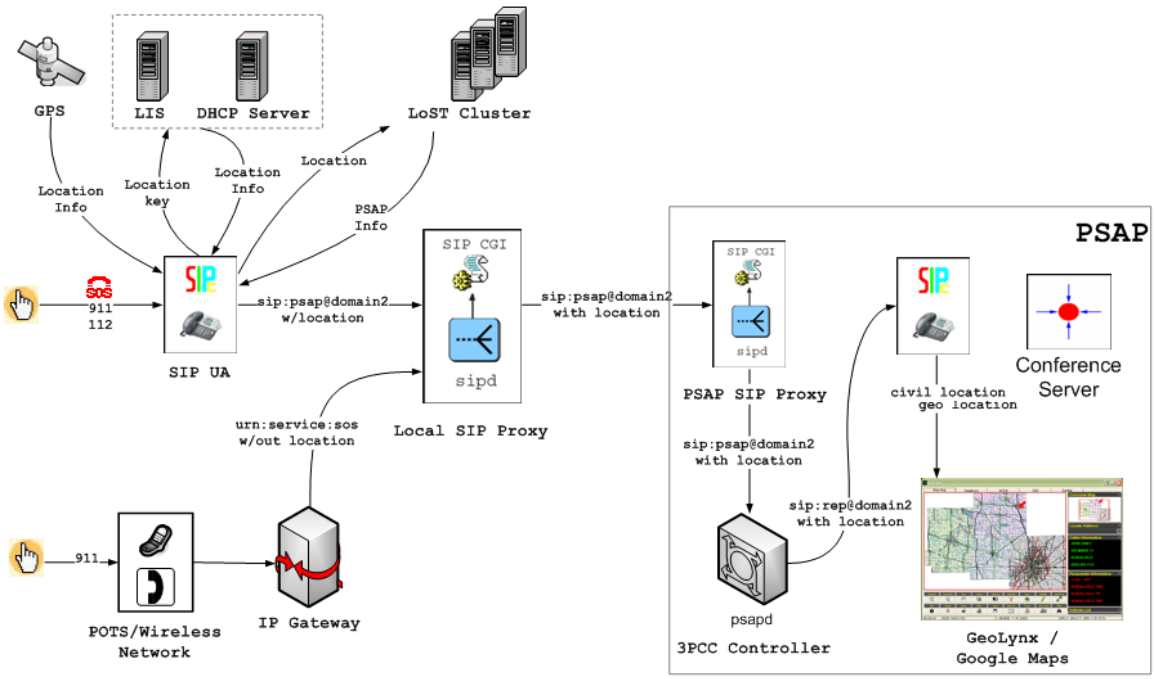
- ve stejnou dobu, kdy hovor přijde do PSAP, je operátorovi zobrazena poloha volajícího;
- v závislosti na charakteru tísňového hovoru nebo v jakékoliv závislosti na mimořádné události, může být hovor přepojen na jiné PSAP nebo na jiné místo příjmu, tento postup může zpřístupnit lokální i externí databáze pro zjištění dalších informací.

Oba dva systémy nicméně pro správné odbavení hovoru vyžadují propracovanou správu dat a systém řízení řídících procesů

### 3.4.6 Fáze zavádění NG911

#### 3.4.6.1 Fáze 1: léto 2005 – jaro 2007

Na vývoji a realizaci základní architektury NG911 a jejích jednotlivých součástí se podílelo mnoho organizací. Mezi hlavní patří NENA, Americké Ministerstvo dopravy (USDOT), Kanadská Radio-televizní a telekomunikační komise (CRTC), IETF, řada telekomunikačních společností, atd. Hlavními oblastmi vývoje byly průběhy hovorů, směrování hovorů v závislosti na poloze a podpora širokého spektra multimédií.




Obr. 30 Základní architektura Next Genaration 911[92]

Základním předpokladem rychlého odbavení tísňového hovoru je určit co nejpřesněji polohu volajícího a přesměrovat hovor na příslušné PSAP. Pro nalezení řešení

byla definována služba URN (Uniform Resource Name). Ta je použita prostřednictví dotazu URI protokolu SIP.

Samotné tísňové volání je identifikovatelné díky informaci v hlavičce TO protokolu SIP. Dalším produktem vývoje je protokol LoST (Location to Service Translation Protokol), který má za úkol směrování hovoru v rámci dané lokality.

Služba URN poskytuje spektrum služeb bez nutnosti určit, kdo tyto služby poskytuje vzhledem k aktuální poloze volajícího. Např. turista bude schopen použít mobilní telefon k vytočení čísla tísňového volání (911 nebo 112) bez znalosti toho, v jaké zemi se nachází.

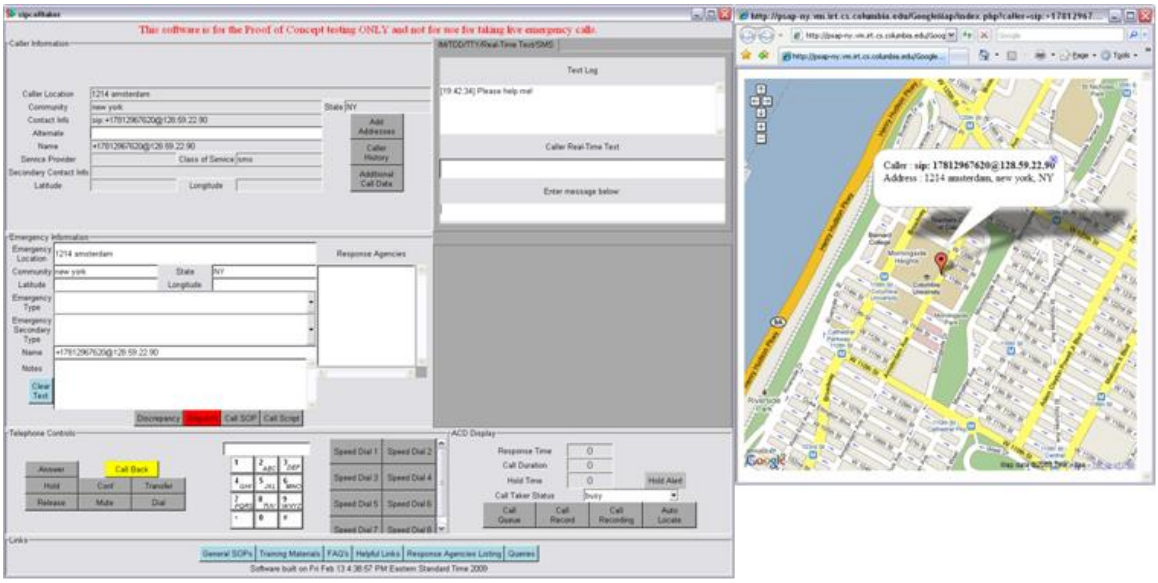
Nicméně služba URN se netýká pouze tísňového volání, ale lze s ní zpřístupnit mnoho dalších služeb jako: telefonní adresář a opravárenské služby (411 a 611), státní informační služby (311), služby právní (1 800 LAWYER), asistenční služby, dodávkové služby atd. Bohužel tyto služby jsou omezeny nabídkou telefonního poskytovatele dané země nebo skupiny zemí a navíc jsou stejné identifikátory použity k jiným účelům.

URN identifikuje služby nezávisle na konkrétním protokolu, který se používá k poskytnutí služby [93].

#### 3.4.6.2 Fáze 2: podzim 2007 – léto 2008

Kromě prototypu vyvinutého v první fázi výstavby, byl vybudován systém POC (Proof of Concept) pro Americké Ministerstvo dopravy. Hlavním cílem projektu bylo sjednotit různé formáty podpůrných dat přicházejících z mnoha sítí (každý poskytovatel/firma má trochu rozdílné systémy. Uživatelské rozhraní, které používá operátor, vyšlo právě z tohoto projektu.

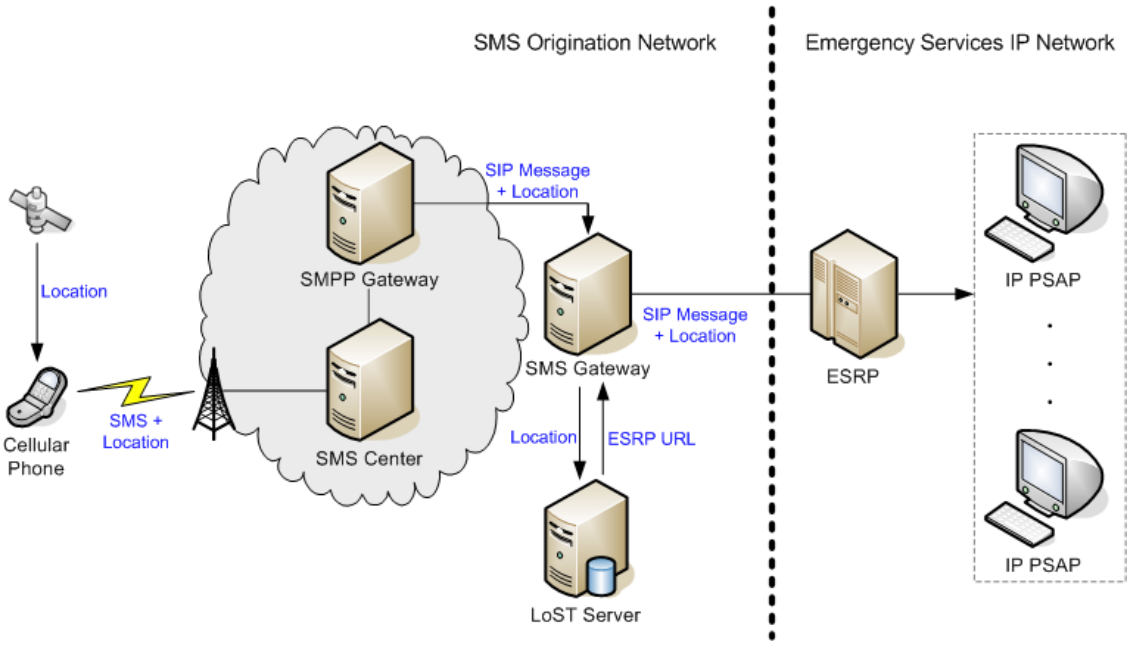
Aplikace POC musí umět zpracovat hovory z mnoha rozdílných zařízení: IP telefonů, přenosných počítačů s aplikacemi pro IP telefonii (např. Skype, ZoiperClassic, Nimbuzz), mobilních telefonů atd. Jako i podpůrná data popisující typ hovoru nebo instrukce pro používání sítě ESInet (Emergency Services IP Network), které se používají je směrování hovorů k jednotlivým PSAP nebo informace o poloze volajícího.



Obr. 31 Aplikační rozhraní operátora (Call taker software) [92]

### 3.4.6.3 Fáze 3: podzim 2008 – jaro 2009

Hlavním cílem třetí fáze NG911 byla integrace textové komunikace do systému NG911. Pracovníci vývoje posuzovali několik modelů textové komunikace, než byl jeden vybrán a to jak pro chat – Instant Messaging (IM), tak i pro Short Messaging Service (SMS).




Obr. 32 Next Generation 911 3. fáze [92]

U IM komunikace museli vývojoví pracovníci vyřešit problém v podobě vlastnických práv. Právě nejpopulárnější IM protokoly jsou vlastněny a toto je neslučitelné s tezí NG911. Proto byl vytvořen model na základě protokolu SIP. Další překážkou bylo doručení mnoha zpráv příjemci najednou. Tento problém byl vyřešen mechanismy, které příchozí zprávy uchovají ve třech různých součástech architektury NG911.

Přenos SMS zpráv představoval další tři problémy v samotném návrhu. Jednalo se o přenos polohy, úprava protokolu SIP a současné doručení více zpráv příjemci. Řešením bylo souběžné odeslání informace o poloze s textem zprávy. Druhý problém byl vyřešen zavedením SMS brány. Třetí problém byl vyřešen stejným způsobem jako u IM komunikace zavedením udržovacích mechanismů.

#### 3.4.6.4 Fáze 4:jaro 2009 - dosud

Ve čtvrté fázi bylo zahájeno testování. Především byla sledována spolehlivost komunikačního systému na bázi protokolu SIP.

### 3.4.7 Studie nákladů NG911

Studie nákladů na vývoj a provoz NG911 ze září 2011 je uvedena v dokumentu White Paper: A Next Generation 911 Cost Study. Hlavními autory nákladového modelu jsou Pat Amodio, Dr. Henning Schulzrinne a Jennifer A. Manner [94].

Celonárodní systém tísňového volání 911 umožňuje veřejnosti požádat o pomoc v nouzi. Důležitou vlastností je spolehlivost, která zachraňuje životy a předchází vzniku následných škod. Systém E911 nebyl chopen plně podporovat vývoj IT technologií v oblasti multimédií, na něž se stále více obyvatel spoléhá. Pro správné fungování je potřeba zavést širokopásmové připojení na všechna PSAP. Poskytování tohoto připojení na celostátním měřítku bude vyžadovat značné finanční prostředky. Výše uvedený dokument představuje dva modely pro dosažení požadovaného připojení, přičemž druhý z nich je více rentabilní.

Studie nákladů zkoumá dva modely nákladů na financování výstavby a průběžné náklady na celostátní širokopásmové připojení NG911 k síti a směrování hovorů mezi PSAP a ILEC. Nákladový model byl vytvořen a jeho předpoklady byly ověřeny pomocí

technické analýzy, která používala data získaná od několika velkých poskytovatelů komerčních služeb, jejich konkurence a prodejců.

Vstupy pro oba modely obsahují množství PSAP v USA, požadavky na šířku pásma, požadavky na materiál, instalační náklady a náklady na provoz.

Z důvodu měřitelnosti nákladů jsou centra PSAP rozdělena do 3 kategorií dle velikosti (počtu operátorů):

- malé PSAP → 5 nebo méně operátorů;
- střední PSAP → 6 až 49 operátorů;
- velké PSAP → 50 nebo více operátorů.

Studie nákladů rovněž předpokládá, že každé PSAP bude poskytovat služby NG911použitím jednoho ze dvou řešení síťové architektury:

Vyhrazená síť (Dedicated network solution) – provozovatel PSAP vlastní a provozuje celou síť (směrování hovorů, vlastní vybavení pro zpracování hovorů, pronájem datových okruhů).

Hostitelská síť (Hosted network solution)–provozovatel PSAP uzavře smlouvu s majitelem sítě a pronajme si veškeré služby včetně vybavení.

Základní model (varianta A) – předpokládá se, že výrazná většina malých center PSAP vybere hostované NG911 řešení; polovina středních PSAP vybere hostované řešení a vzhledem k velikosti a rozsahu center tísňového volání ve velkých městech, vyberou všechna velká PSAP vyhrazené řešení (Dedicated solution).

Úsporný model (varianta B) - předpokládá se, že konsolidace PSAP bude mít za následek 35 % snížení počtu PSAP. Model také předpokládá větší spolehlivost u hostitelského řešení s 50% velkých PSAP a 75% středních PSAP.

Analýza nákladů nejprve určuje počet PSAP v každé velikostní kategorii: malé, střední a velké PSAP. Dále se pak počítají jednorázové a opakující se náklady v rámci každého modelu založené na rozdělení mezi centry tísňového volání těchto dvou architektonických řešení a na celkovém počtu PSAP, které vyžadují přístup k širokopásmovému optickému vláknu.

Pro jednorázové zpřístupnění připojení, studie bere v úvahu náklady na upgrade z TDM (Time Division Multiplexing) na IP-over-Fiber, procento center tísňového volání PSAP, které je třeba upgradovat na IP-over-Fiber, procento

z center PSAP, která jsou rozšířena z jedno-vláknového připojení na duální pro zlepšení spolehlivosti a procento center tísňového volání vyžadujících speciální konstrukční nároky k připojení nebo upgrade širokopásmového vlákna do centra tísňového volání.

Opakující se náklady zahrnují výdaje na propojení přístupu všech PSAP, které mají typicky formu měsíčních poplatků vztažených k určité šířce pásma.

Na základě odhadu běžných nákladů pro celostátní provoz E911, je možná roční úspora v rozsahu od 26 do 55 milionů dolarů při plném zprovoznění sítí NG911. Odhad je založen na přiměřeném odhadu počtu trunků. Každé PSAP mělo v roce 2011 v průměru 5 až 7 trucků a měsíční sazba byla ve výši 65 až 100 dolarů za jeden truck.

Pro výše uvedený model A (model základní) jsou náklady za 10 let v celkové výši2,68 miliardy dolarů (včetně jednorázových a opakujících se nákladů), viz tab. 5.

| Všechna PSAP | Neperiodické náklady (NRC) |
|---|---|
| Malá PSAP | $302.000.000 |
| Střední PSAP | $776.000.000 |
| Velká PSAP | $153.000.000 |
| Všechna PSAP – celkové náklady | $1.231.000.000 |
| | |
| Všechna PSAP – celkové periodicky se opakující náklady za 10 let | $1.450.000.000 |
| | |
| Všechna PSAP – celková náklady za 10 let | $2.680.000.000 |

Tab. 5 Kalkulace celkových nákladů varianty A [94]

V tab. 6 jsou celkové měsíční opakující se náklady rozdělené do 3 velikostních kategorií PSAP. Předpokládané náklady jsou kalkulované na dobu 10 let. Hodnoty nákladů po první 3 roky jsou pro tuto metodu typicky nízké díky menšímu přenosu dat.

| | Total Monthly Recurring Costs (MRC) | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Year 1 | Year 2 | Year 3 | Year 4 | Year 5 | Year 6 | Year 7 | Year 8 | Year 9 | Year 10 |
| Small PSAP | $5,957,050 | $15,885,465 | $31,770,931 | $61,556,178 | $107,226,892 | $163,143,730 | $194,120,387 | $206,511,050 | $206,511,050 | $206,511,050 |
| Medium PSAP | $2,325,930 | $6,202,481 | $12,404,962 | $24,034,615 | $41,866,748 | $63,699,482 | $75,794,321 | $80,632,256 | $80,632,256 | $80,632,256 |
| Large PSAP | $663,802 | $1,770,138 | $3,540,276 | $6,859,285 | $11,948,432 | $18,179,317 | $21,631,086 | $23,011,794 | $23,011,794 | $23,011,794 |
| Total | $8,946,782 | $23,858,085 | $47,716,169 | $92,450,078 | $161,042,071 | $245,022,529 | $291,545,794 | $310,155,100 | $310,155,100 | $310,155,100 |
| Net Present Value (NPV) | -$1,448,431,006 | | | | | | | | | |
| | | | | | | | | | | |
| US 10-Year Treasury Yield rate | 3.03% | | | | | | | | | |

Tab. 6 Kalkulace celkových periodických měsíčních nákladů varianty A [94]

V tab. 7 na následující straně jsou shrnuty jednorázové náklady pro variantu A.

| Summary of Non-Recurring Costs (NRC) | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Access Connectivity Cost (NRC) | | | | | | | Hosted Cost | | Dedicated Solution (IT infrastructure, ESInet, etc) | | | | |
| PSAP Size | Bandwidth (BW) Connection | TDM to IP Install (NRC) | Total % PSAP's (S, M, L) | Total % Upgraded PSAP's | Total % New PSAP's | Total % PSAP's for Special construction | Total NRC Cost | Total NRC (per PSAP) | Total NRC - All PSAPs | Low Dedicated Network Cost NRC - (per PSAP) | High Dedicated Network Cost NRC - (per PSAP) | Dedicated Network Cost NRC - All PSAPs | Equipment Refresh and Replacement | Total |
| Small | 10 Mb/s | $1,100 | 80% | 55% | 25% | 45% | $143,998,668 | $10,000 | $54,888,000 | $500,000 | $750,000 | $61,749,000 | $41,701,707 | $302,337,375 |
| Medium | 10 Mb/s | $1,100 | 19% | 75% | 25% | 40% | $41,617,111 | $25,000 | $16,294,875 | $750,000 | $1,500,000 | $611,057,813 | $107,035,168 | $776,004,966 |
| Large | 100 Mb/s | $2,800 | 1% | 100% | 0% | 30% | $3,149,199 | $0 | $0 | $1,500,000 | $3,000,000 | $128,643,750 | $21,086,872 | $152,879,821 |

Tab. 7 Kalkulace celkových neperiodických nákladů varianty A [94]

U výše uvedeného modelu B (úsporný model) předpokládáme, že všechna PSAP sjednotí provoz, jak se blíží k plnému zprovoznění systému NG911. Dále se předpokládá častější využití pronájmu sítí od místních poskytovatelů.

V tab. 8 jsou znázorněny jednotlivé náklady ve třech velikostních kategoriích PSAP a předpokládané jednorázové náklady. Díky konsolidaci center dojde k redukci počtu PSAP o 35% a v případě častějšího využití hostovaného řešení velkými a středními PSAP, dojde ke snížení neperiodických nákladů.

| Všechna PSAP | Neperiodické náklady (NRC) |
|---|---|
| Malá PSAP | $203.000.000 |
| Střední PSAP | $297.000.000 |
| Velká PSAP | $56.000.000 |
| Všechna PSAP – celkové náklady | $556.000.000 |
| | |
| Všechna PSAP – celkové periodicky se opakující náklady za 10 let | $888.000.000 |
| | |
| Všechna PSAP – celková náklady za 10 let | $1.444.000.000 |

Tab. 8 Kalkulace celkových nákladů varianty B [94]

Tab. 9 ukazuje celkové měsíční periodicky opakující se náklady pro tři velikostní kategorie s předpokládanými kalkulacemi na 10 let. První 3 roky jsou nízké náklady na paušál, díky probíhajícímu přechodu k NG911.

| | Total Monthly Recurring Costs (MRC) | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Year 1 | Year 2 | Year 3 | Year 4 | Year 5 | Year 6 | Year 7 | Year 8 | Year 9 | Year 10 |
| Small PSAP | $3,872,082 | $10,325,553 | $20,651,105 | $40,011,516 | $69,697,479 | $106,043,424 | $126,178,252 | $134,232,183 | $134,232,183 | $134,232,183 |
| Medium PSAP | $1,245,898 | $3,322,395 | $6,644,789 | $12,874,279 | $22,426,164 | $34,120,993 | $40,599,663 | $43,191,130 | $43,191,130 | $43,191,130 |
| Large PSAP | $365,847 | $975,593 | $1,951,186 | $3,780,423 | $6,585,253 | $10,019,340 | $11,921,747 | $12,682,709 | $12,682,709 | $12,682,709 |
| Total | $5,483,828 | $14,623,540 | $29,247,080 | $56,666,218 | $98,708,896 | $150,183,758 | $178,699,661 | $190,106,023 | $190,106,023 | $190,106,023 |
| Net Present Value (NPV) | -$887,799,225 | | | | | | | | | |
| | | | | | | | | | | |
| US 10-Year Treasury Yield rate | 3.03% | | | | | | | | | |

Tab. 9 Kalkulace celkových periodických měsíčních nákladů varianty B [94]

Tab. 10 představuje jednorázové náklady pro variantu B.

| | Summary of Non-Recurring Costs (NRC) | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Access Connectivity Cost (NRC) | | | | | | | Hosted Cost | | Dedicated Solution (IT infrastructure, ESInet, etc) | | | |
| PSAP Size | Bandwidth (BW) Connection | TDM to IP Install (NRC) | Total % PSAP's (S, M, L) | Total % Upgraded PSAP's | Total % New PSAP's | Total % PSAP's for Special construction | Total NRC Cost | Total NRC (per PSAP) | Total NRC - All PSAPs | Low Dedicated Network Cost NRC - (per PSAP) | High Dedicated Network Cost NRC - (per PSAP) | Dedicated Network Cost NRC - All PSAPs | Equipment Refresh and Replacement | Total |
| Small | 10 Mb/s | $1,100 | 80% | 55% | 25% | 45% | $93,599,134 | $10,000 | $35,677,200 | $500,000 | $750,000 | $40,136,850 | $33,778,383 | $203,191,567 |
| Medium | 10 Mb/s | $1,100 | 19% | 75% | 25% | 40% | $27,051,122 | $25,000 | $15,887,503 | $750,000 | $1,500,000 | $198,593,789 | $55,770,813 | $297,303,227 |
| Large | 100 Mb/s | $2,800 | 1% | 100% | 0% | 30% | $2,046,979 | $50,000 | $1,114,913 | $1,500,000 | $3,000,000 | $41,809,219 | $10,569,277 | $55,540,388 |

Tab. 10 Kalkulace celkových neperiodických nákladů varianty B [94]

Z údajů tab. 5 a tab. 8 jednoznačně vyplývá, že model založený na pronájmu sítí a vybavení od místních poskytovatelů má poloviční náklady na provoz. Z finančního hlediska je tedy výhodnější.

# 4 Závěr

Cílem této práce bylo popsat problematiku tísňového volání v České republice a v zahraničí. Podrobně a uceleně charakterizovat stávající systémy a popsat možný budoucí vývoj v této oblasti se zaměřením na využití IP telefonie.

Technologie tísňového volání má v dnešní době důležitou roli při ochraně obyvatel a majetku. Z toho důvodu se při vývoji dbá na zajištění efektivity systému a na bezpečnost, ať už se jedná o opatření proti výpadku elektrické energie nebo organizovaným IT útokům z vnějšího prostředí.

**Systémy tísňového volání v ČR**

Vývoj technologií tísňového volání v České republice je možné posoudit podle 2 informačních systémů. Je to informační systém telefonního centra tísňového volání TCTV 112 a nástupnickým informačním systémem je národní informační systém NIS IZS. Kromě těchto dvou informačních systému se v práci zabývám projektem eCall, který od roku 2018 poskytne automatickou pomoc řidičům při dopravní nehodě nejenom v ČR, ale v rámci celé EU.

**Informační systém TCTV 112**

Zavedením technologie TCTV 112 v ČR bylo umožněno složkám IZS využívat soubor nových služeb. Analýza síťové signalizace umožnila identifikaci volaného čísla a identifikaci čísla volajícího účastníka. V souvislosti s přenositelností čísel se stala nepostradatelnou služba identifikace telefonního operátora. Díky spolupráci HZS s provozovateli telefonních sítí v České republice byla zavedena služba identifikace adresy pevné telefonní stanice a identifikace polohy mobilního telefonu. Takto získané informace jsou pro záchranné složky nezbytné a to především v případech, kdy volající ze zdravotních či jiných důvodů tuto informaci operátorovi sdělit nemůže.

Uniformní řešení systémů TCTV 112 ve všech 14 krajích umožnilo použít jednotný geografický systém (GIS), vzájemnou zastupitelnost jednotlivých TCTV 112, vzájemné zálohování technologií pro případ výpadku a možnost vzájemné jazykové podpory operátorů. V rámci budování datových sítí bylo vytvořeno nezávislé telefonní spojení mezi systémem příjmu tísňových volání a jednotlivými operačními středisky základních složek integrovaného záchranného systému.

### Informační systém NIS IZS

Už v době zavádění technologie TCTV 112 bylo jasné, že je potřeba vyvinout nový systém. Toto tvrzení se opírá o analýzy, popisující obtíže s posílání sdílených dat mezi jednotlivými prvky IZS. Nemalý vliv na provoz měl i velký počet informačních systémů, kdy každá složka IZS měla minimálně jeden vlastní informační systém a zároveň využívala nejednotný systém GIS.

Postup, který by tyto nedostatky odstranil, byl viděn ve vývoji a realizaci „střechového“ informačního systému NIS IZS. Cílem tohoto vývoje bylo zavést systém uceleného spojení a podpory sil a techniky jednotek IZS. Vývoj systému NIS IZS lze rozdělit na 2 etapy. V první etapě mělo být navrženo řešení, které by poskytlo: 1) Jednotnou technologii tísňového volání založenou na IP telefonii; 2) Jednotný geografický informační systém (GIS); 3) Systém integrační platformy IZS (IPL) – softwarové řešení pro integraci externích systémů pro NIS. Vývojem tohoto systému byla v roce 2010 pověřena společnost ČP OZ ICT. Tato etapa byla v roce 2014 ukončena na základě rozhodnutí zadavatele. Důvodem pro toto opatření bylo nesplnění celého rozsahu zadání, respektive prototyp informačního systému byl dodán s velkým zpožděním.

Druhá etapa představuje hybridní řešení informačního systému NIS IZS. Projekt byl zeštíhlen o jednotnou technologii tísňového volání a zachoval informační systém TCTV 112 a zajišťuje komunikaci mezi informačními systémy jednotlivých složek IZS. Přínosem je zavedení jednotné platformy GIS a systému Integrační platformy. Od systému NIS je očekávána snadnější a rychlejší komunikace. Efektivnější řízení sil a prostředků. Rovněž nelze opomenout výhody jednotného geografického systému. Bližší specifikace hybridní varianty není veřejně dostupná z důvodu utajení.

### Projekt eCall

Nezávisle na národních systémech tísňového volání v rámci celé Evropské unie a dokonce i některých států mimo ni, je připravován a realizován projekt eCall. Tento projekt, jenž je realizován na základě nařízení Evropské komise, od roku 2018 přinese vyšší bezpečnost automobilové dopravy. Automatickým zasíláním informací o dopravní nehodě zajistí rychlejší a vzájemně koordinovanou reakci složek IZS.

### Systémy tísňového volání v USA

Vývoj technologií tísňového volání v zahraničí, respektive v USA, je z mého názoru na vyšší úrovni díky zavedeným technologiím a dlouhodobým vývojem jednotlivých systémů. Vzhledem rozloze a k velkému počtu států je samotná telefonie řešena rozdílněji. Důraz je kladen na využívání (pronájem) telekomunikačních systémů soukromých společností Common Carriers, které působí v rámci lokální regionů. Rozvoj a technologická vybavenost jednotlivých sítí je ponechána na rozhodnutí zřizujících společností. Nicméně systémy musí poskytovat služby tísňového volání, jejichž rozsah a úroveň je definována Federální komunikační komisí.

V diplomové práci jsem se popsal informační systémy Enhanced 911 a Next Generation 911, který je stávajícím informačním systémem tísňového volání v USA založeným na používání pronajatých telekomunikačních sítí a používající IP telefonii.

### Informační systém Enhanced 911

Systém E911 prošel během své existence 3 fázemi vývoje. Jednotlivé fáze odrážely požadavky Federální komunikační komise na zabezpečení služeb tísňového volání. Ke své činnosti využívá databáze, které slouží v identifikaci volajícího a jeho lokalizaci. Principy, které jsou k tomuto využívány, jsou prakticky identické s těmi z informačního systémem TCTV 112, který je provozován v České republice.

### Informační systém Next Generation 911

Informační systém Next Generation 911 je technologicky nejvyspělejším komunikačním systémem, který je v této práci popsán. Představuje nový milník v systémech tísňového volání. Byl navržen tak, aby umožnit široké veřejnosti přístup ke službám tísňové linky 911 a to nezávisle na použitém zařízení – klasické pevné telefonní linky, telefonů sítě GSM, VoIP telefonů, nebo jiným přístrojům, umožňující volání pomocí IP protokolů. Systém navazuje na předchozí generaci E911 a přidává nové technologie založené na využití otevřených standardů.

Tímto opatřením lze docílit snížení nákladů na vývoj a údržbu systému. Dále je zajištěno, že se na zabezpečení technologických dodávek nebude podílet výrobce, který má na tuto technologii patentová práva. Neméně důležitou stránkou je technologický tlak na jednotlivé dodavatele a tím podpořený výzkum v oblasti IP telefonie.

**Další možný vývoj IS tísňového volání v ČR**

Budoucí vývoj IS tísňového volání jde podle mého názoru rozdělit na dvě fáze. První fáze bude ovlivněna výsledky provozu hybridní verze NIS IZS a pokračováním jeho vývoje vzhledem k vynaloženým nákladům na nákup potřebných technologií. V dnešní době a v prostředí ČR je z hlediska bezpečnosti nevýhodné zavést systémy tísňového volání pracující s VoIP. Na straně pracovníků HZS převládají obavy, že by byl systém vystaven působení hackerů a počítačovým virům. Nicméně proti tomuto tvrzení vypovídá úspěch několika projektů, založených na technologiích internetu, např. aplikace záchranka.

Druhá fáze dle mého názoru bude jednoznačně kopírovat vývoj systému NG911. Technologie IP telefonie přináší mnoho inovací do systémů tísňového volání. Umožňuje příjem tísňového volání nejen hlasem ale třeba i video-hovorem. To umožňuje získat více informací k poskytnutí kvalitní a rychlé pomoci. Využití otevřených standardů představuje výhodný směr rozvoje nejen s pohledu finančního, ale i technologického. V budoucnosti si dokáži u složek IZS představit nasazení dronů, jakožto relativně levného vysoce mobilního prostředku pro získávání informací.

# 5 Seznam obrázků

# 6 Seznam tabulek

# 7 Zkratky

ACD – Automatic Call Distributor

ALI – AutomaticLocationIdentification

ANI–AutomaticNumberIdentification

AOR–AddressOfRecord

AVL – AutomaticVehicleLocation

CAN–Controller Area Network

CRTC–CanadianRadio-television and TelecommunicationsCommission

CTI – ComputerTelephonyIntegration

ČTÚ–Český telekomunikační úřad

DTMF – Dual Tone MultiFrequency

E911–Enhanced 9-1-1

EGNOS – European Geostationary Navigation Overlay Service

ETSI –EuropeanTelecommunicationsStandards Institute

EU – Evropská unie

FCC – Federal Communications Commission

GIS – GeographicInformation Systems/ Geografický informační systém

GPS –Global Positioning System

GSM –GlobalSystemfor Mobile Communications

HeERO – Harmonized eCall European Pilot

HMI–Human-Machine Interface

HZS ČR – Hasičský záchranný sbor České republiky

ICT – Informační a komunikační technologie

IM – Instant Message (Chat)

IMEI –*International Mobile Equipment Identity*

*IP–InternetProtocol*

ISDN–*IntegratedServices Digital Network*

ISO –InternationalOrganizationforStandardization

ISV – Informační systém Výjezd

IT – InformationTechnogy / Informační technologie

ITS MV – Integrovaná telekomunikační síť Ministerstva vnitra

ITU –InternationalTelecommunication Union

IVR – InteractiveVoice Response

IZS – Integrovaný záchranný systém

LAN – Local Area Network

MPLS – Muliprotocol Label Switching

MSD–Minimum Set of Data

MU – Mimořádná událost

NENA – NationalEmergencyNumberAssociation

NG911 – NextGeneration911

NIS IZS – Národní informační systém IZS

OBU–OnBoard Unit

OPIS – Operační informační středisko

OSI–OperatingSystem Interface

PBX – Public Branch Exchange

PČR – Policie České republiky

PSAP –Public SafetyAnswering Point

PSTN –Public SwitchedTelephoneNetwork

RÚIAN – Registr územní identifikace, adres a nemovitostí

SaP – síly a prostředky

SDO – StandardsDevelopmentOrganization

SIM – Subscriber Identity Module

SIP –SessionInitiationProtocol

SMS – ShortMessageService

TCTV – Telefonní centrum tísňového volání

TV – Tísňová volání

UDP - *User Datagram Protocol*

USDOT – United StatesDepartmentofTransportation

VIN – VehicleIdentificationNumber

VoIP – Voiceover Internet Protocol

ZZS – Zdravotnická záchranná služba

# Literatura


1. 112 (emergencytelephonenumber)[online]. [vid. 1.5. 2015]. Dostupné z: http://en.wikipedia.org/wiki/112_%28emergency_telephone_number%29
2. Real-time Transport Protocol[online]. [vid. 12. 3. 2015]. Dostupné z: http://cs.wikipedia.org/wiki/Real-time_Transport_Protocol
3. H.323[online]. [vid. 12.3. 2015]. Dostupné z: http://cs.wikipedia.org/wiki/H.323
4. Session InitiationProtocol[online]. [vid. 12. 3. 2015]. Dostupné z: http://cs.wikipedia.org/wiki/Session_Initiation_Protocol
5. SIP [online]. [vid. 12.3. 2015]. Dostupné z: https://sip.cesnet.cz/cs/protokoly/sip
6. E.164 : Theinternational public telecommunicationnumberingplan[online]. [vid. 12.3. 2015]. Dostupné z:http://www.itu.int/rec/T-REC-E.164-201011-I/en
7. Abstract Syntax NotationOne[online]. [vid. 12. 3. 2015]. Dostupné z: http://cs.wikipedia.org/wiki/Abstract_Syntax_Notation_One
8. Tísňová volání v České republice [online]. [vid. 8. 5. 2016]. Dostupné z: http://www.hzscr.cz/clanek/tisnova-volani-v-ceske-republice
9. Zákon č. 127 ze dne 22. února 2005 o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronickýchkomunikacích),§ 119, odst. 1 písm. e). Dostupný také z: http://www.zakonyprolidi.cz/cs/2005-127#p119
10. Zákon č. 40 ze dne 8. ledna 2009, Trestní zákoník, § 276, Poškození a ohrožení provozu obecně prospěšného zařízení
11. Článek deníku Nový čas ze dne 4. července 2011, Pri volaní na 112-ku si vypočujete najprv upozornenie na vysokú pokutu[online]. [vid. 8. 5. 2016]. Dostupné z: http://www.cas.sk/clanok/201660/pri-volani-na-112-ku-si-vypocujete-najprv-upozornenie-na-vysoku-pokutu/
12. Zákon č. 127 ze dne 22. února 2005 o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), § 33 Přístup k jednotnému evropskému číslu tísňového volání a národním číslům tísňových volání, odst. 1
13. Ústavní zákon č. 347 ze dne 3. prosince 1997 o vytvoření vyšších územních samosprávných celků a o změně ústavního zákona České národní rady č. 1/1993 Sb.
14. Centrum tísňového volání Ostrava [online]. [vid. 20. 1. 2015]. Dostupné z:http://mobil.idnes.cz/foto.aspx?foto1=RJA24f90d__MG_1657.JPG
15. Tísňová volání v České republice, bod č.3 Jak volat [online]. [vid. 8. 5. 2016]. Dostupné z: http://www.hzscr.cz/clanek/tisnova-volani-v-ceske-republice.aspx?q=Y2hudW09Mw%3d%3d
16. 91/396/EEC: CouncilDecisionof 29 July 1991 on theintroductionof a single Europeanemergency call number[online]. [vid. 29. 1. 2015]. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31991D0396:EN:HTML

17. kpt. Ing. Urbánek, Jan: 10 let provozu telefonních center tísňového volání 112. Časopis 112, 2014, roč. 13, č. 4, s. 10-12. Dostupné také z: http://www.hzscr.cz/clanek/casopis-112-rocnik-xiii-cislo-4-2014.aspx?q=Y2hudW09Mw%3D%3D
18. USNESENÍVLÁDY ČESKÉ REPUBLIKY č. 391 + P ze dne 19. dubna 2000 [online]. [vid. 29. 1. 2015]. Dostupné z:http://kormoran.odok.cz/usneseni/usneseni_webtest.nsf/0/578EC0A62D7E8F26C12571B6006C4515
19. USNESENÍVLÁDY ČESKÉ REPUBLIKY č. 350 + P ze dne 3. dubna 2002 [online]. [vid. 29. 1. 2015]. Dostupné z:http://racek.vlada.cz/usneseni/usneseni_webtest.nsf/0/6C4ED7EE2B5C08CAC12571B6006C24CD
20. LUKÁŠ, Luděk a kolektiv. *Informační podpora integrovaného záchranného systému*. Edice SPBI Spektrum, 2011. ISBN 978-80-7985-105-7
21. Zákon č. 239 ze dne 28. června 2000, o integrovaném záchranném systému a o změně některých zákonů
22. Vyhláška Ministerstva vnitra č. 328 ze dne 5. září 2001, o některých podrobnostech zabezpečení integrovaného záchranného systému
23. Vyhláška č. 429 ze dne 27. listopadu 2003, kterou se mění vyhláška č. 328/2001 Sb., o některých podrobnostech zabezpečení integrovaného záchranného systému
24. Zdravotnická záchranná služba Plzeňské kraje – Informační systém [online]. [vid. 9. 5. 2016]. Dostupné z: http://www.zzspk.cz/operacni-stredisko/informacni-system.html
25. RCS Kladno [online]. [vid. 9. 5. 2016]. Dostupné z: http://www.rcs-kladno.net/
26. ZZS – systém pro podporu činností zdravotnické záchranné služby[online]. [vid. 9. 5. 2016]. Dostupné z: http://www.vitkovice.cz/operacni-rizeni-zzs
27. Rádiová síť PEGAS [online]. [vid. 2. 2. 2015]. Dostupné z: http://www.kmitocty.cz/?p=198
28. USNESENÍVLÁDY ČESKÉ REPUBLIKY č. 246 + P ze dne 19. května 1993[online]. [vid. 2. 2. 2015]. Dostupné z:http://racek.vlada.cz/usneseni/usneseni_webtest.nsf/0/C94E8F831385066EC12571B6006D0A6A
29. Katalog otevřených dat [online]. [vid. 2. 2. 2015]. Dostupné z: http://www.ctu.cz/otevrena-data/katalog-otevrenych-dat-ctu.html
30. Hasiči Pozďatín [online]. [vid. 2. 2. 2015]. Dostupné z: http://www.sdhpozdatin.cz/dokumenty.html
31. Řízení prostředků [online]. [vid. 2. 4. 2015]. Dostupné z: http://www.zachrannasluzba.cz/odborna/0304_rizeni.htm,
32. Vítkovice IT Solutions[online]. [vid. 2. 4. 2015]. Dostupné z:http://www.czechict.cz/clenstvi/aktuality-o-clenech/vitkovice-it-solutions-as.htm
33. Medium Soft[online]. [vid. 5. 4. 2015]. Dostupné z: http://www.czechict.cz/clenstvi/aktuality-o-clenech/medium-soft-as.htm

34. Přehled systémů pro podporu činností složek IZS [online]. [vid. 5. 4. 2015]. Dostupné z: http://itsolutions.vitkovice.cz/37/cs/node/2093
35. Standardy [online]. [vid. 5. 4. 2015]. Dostupné z: http://itsolutions.vitkovice.cz/37/cs/node/2108
36. Certifications[online]. [vid. 5. 4. 2015]. Dostupné z: http://www.dimensiondata.com/cs-CZ/AboutUs/Company-Highlights/Stranky/Certifications.aspx
37. Telekomunikační řešení TCTV 112 [online]. [vid. 5. 4. 2015]. Dostupné z: http://wcz2.nextiraone-eu.com/store/fdf00219b4.pdf
38. Alcatel Oxe vlastnosti[online]. [vid. 6. 4. 2015]. Dostupné z: http://www.dto.cz/dokumenty/alcatel_oxe/alcatel_oxe_vlastnosti.pdf
39. OmniPCXEnterprise - OXE [online]. [vid. 6. 4. 2015]. Dostupné z: http://www.altel.cz/index.php?goto=text&sekce=NYydaIs8&tid=a5LXNtKH&lng=cz
40. Organizační struktura oddělení KOPIS [online]. [vid. 6. 4. 2015]. Dostupné z: http://archiv.hzszlk.eu/aktuality7/0710/
41. Školení pracovníků IZS [online]. [vid. 5. 4. 2015] Dostupné z: httphttp://www.voip-forum.cz/archiv/Frank-SmerovaniTisnovychHovoru.pdf
42. GIS HZS ČR [online]. [vid. 5. 4. 2015]. Dostupné z:http://gis.izscr.cz/wpgis/sample-page/
43. GISel IZS [online]. [vid. 5. 4. 2015]. Dostupné z: http://gis.izscr.cz/wpgis/gisel-izs/
44. Směrnice evropského parlamentu a rady 2010/40/EU ze dne 7. července 2010,o rámci pro zavedení inteligentních dopravních systémů v oblasti silniční dopravy a pro rozhraní s jinými druhy dopravy
45. O projektu HeERO[online]. [vid. 10. 4. 2015]. Dostupné z: http://www.heero-pilot.eu/view/cs/heero.html
46. Pilotní ověření funkčnosti celoevropského automatického systému tísňového volání z paluby vozidla „eCall 112“ bylo úspěšně dokončeno[online]. [vid. 10. 5. 2016]. Dostupné z: http://www.czechspaceportal.cz/3-sekce/its---dopravni-telematika/pilotni-overeni-funkcnosti-celoevropskeho-automatickeho-systemu-tisnoveho-volani-z-paluby-vozidla-ecall-112-bylo-uspesne-dokonceno.html
47. Rozhodnutí evropského parlamentu a rady č. 585/2014/EU ze dne 15. května 2014, o zavedení interoperabilní služby eCall v celé EU
48. Nařízení evropského parlamentu a rady č. 2015/758 ze dne 29. dubna 2015, o požadavcích na schválení typu pro zavedení palubního systému eCall využívajícího linku tísňového volání 112 a o změně směrnice 2007/46/ES
49. O systému eCall[online]. [vid. 10. 4. 2015]. Dostupné z:http://www.heero-pilot.eu/view/cs/ecall.html
50. eCall-celoevropský systém tísňového volání z vozidel[online]. [vid. 10. 4. 2015]. Dostupné z: http://www.czechspaceportal.cz/files/files/storage/eCall/ecall_doprava_03_08_.pdf

51. eCallWhitepaper[online]. [vid. 10. 5. 2016]. Dostupné z: https://www.qualcomm.com/media/documents/files/ecall.pdf
52. eCall MSD[online]. [vid. 15. 4. 2015]. Dostupné z: http://www.ecall.fi/eCall_msd_en_022007.pdf
53. Podklad za Policii ČR[online]. [vid. 12. 4. 2015]. Dostupné z: http://is-izs.izscr.cz/wp-content/uploads/2012/02/Vstup_PCR.pdf
54. Podklad za HZS [online]. [vid. 13. 4. 2015]. Dostupné z:http://is-izs.izscr.cz/wp-content/uploads/2012/02/Vstup_HZS.pdf
55. Podklad za ZZS [online]. [vid. 13. 4. 2015]. Dostupné z: http://is-izs.izscr.cz/wp-content/uploads/2012/02/Vstup_ZZS.pdf
56. Program IS IZS Krajské standardizované projekty [online]. [vid. 13. 4. 2015]. Dostupné z: http://is-izs.izscr.cz/?page_id=85
57. Jednotná úroveň informačních systémů operačního řízení a modernizace technologií pro příjem tísňového volání základních složek integrovaného záchranného systému[online]. [vid. 13. 4. 2015]. Dostupné z:http://www.hzscr.cz/clanek/jednotna-uroven-informacnich-systemu-operacniho-rizeni-a-modernizace-technologii-pro-prijem-tisnoveho-volani-zakladnich-slozek-integrovaneho-zachranneho-systemu-402999.aspx
58. HZS ČR – Možnosti čerpání prostředků z fondů EU [online]. [vid. 13. 4. 2015]. Dostupné z:http://www.msline.cz/index.php?page=review-pro-obranny-a-bezpecnostni-prumysl&cislo=review-pro-obranny-a-bezpecnostni-prumysl-1-2014&clanek=hzs-cr---moznosti-cerpani-prostredku-z-fondu-eu
59. Přehledový harmonogram [online]. [vid. 13. 4. 2015]. Dostupné z: http://is-izs.izscr.cz/wp-content/uploads/2012/02/aktivity-1024x782.png
60. Směrnice Evropské unie č. 2002/22/ES [online]. [vid. 13. 4. 2015]. Dostupné z:Směrnice EU č. 2002/22/ES, čl. č. 26, http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32002L0022&from=CS
61. Usnesení Vlády ČR č. 923 ze dne 23. 7. 2008 [online]. [vid. 13. 4. 2015]. Dostupné z: https://apps.odok.cz/djv-agenda?date=2008-07-23
62. Analýza technického řešení projektu Koncept TO – BE [online]. [vid. 13. 4. 2015]. Dostupné z:http://is-izs.izscr.cz/wp-content/uploads/2012/02/ISIZS_Vystup_TOBE_090702_FINAL.pdf
63. Nové technologie pro tísňové volání [online]. [vid. 13. 4. 2015]. Dostupné z: http://www.isss.cz/archiv/2013/download/prezentace/mvcr_prudil.pdf
64. Zpráva o realizaci Integrovaného operačního programu za období 1. 10. 2014 – 16. 4. 2015[online]. [vid. 5. 5. 2016]. Dostupné z: www.strukturalni-fondy.cz
65. Zaoralová, Nicole: Realizační fáze projektu Národní informační systém IZS končí k 31. 12. 2015[online]. [vid. 5. 5. 2016]. Dostupné z: http://is-izs.izscr.cz/
66. Interní dokumentace – školení vedoucích složek kraje, ze dne 30. 9. 2015
67. Taskforce[online]. [vid. 5. 3. 2015]. Dostupné z: http://www.911dispatch.com/911/history/task_force_rpt.html

68. HistoryofEmergency calling [online]. [vid. 5. 3. 2015]. Dostupné z: http://www.911dispatch.com/911/history/
69. Historyof 911 [online]. [vid. 5. 3. 2015]. Dostupné z:http://www.countyofunion.org/site/cpage.asp?cpage_id=180009766&sec_id=180003667
70. The Wireless Communications and Public Safety Act 106–81 [online]. [vid. 5. 3. 2015]. Dostupné z:http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ081.106.pdf
71. FCC: Whatwe do[online]. [vid. 5. 3. 2015]. Dostupné z:https://www.fcc.gov/what-we-do
72. PermittedCarriers[online]. [vid. 5. 3. 2015]. Dostupné z:http://www.utc.wa.gov/regulatedIndustries/transportation/Pages/PermittedCarriers.aspx
73. FCC ACTS TO PROMOTE COMPETITION AND PUBLIC SAFETY IN ENHANCED WIRELESS 911 SERVICES, 99-245[online]. [vid. 5. 3. 2015]. Dostupné z:https://transition.fcc.gov/Bureaus/Wireless/News_Releases/1999/nrwl9040.html
74. Token ring switching[online]. [vid. 5. 3. 2015]. Dostupné z:http://docstore.mik.ua/cisco/pdf/Token-Ring-Switching.pdf
75. ICMP protocol[online]. [vid. 5. 3. 2015]. Dostupné z:http://www.isgmlug.org/icmp-protocol-exploit-loki.htm
76. LLDP protocol[online]. [vid. 5. 3. 2015]. Dostupné z:http://en.wikipedia.org/wiki/Link_Layer_Discovery_Protocol
77. CCNA exploration – Směrování, koncepce a protokoly [online]. [vid. 10. 3. 2015]. Dostupné z:http://www.spsmt.sk/download/d7f9a2f5-2011-11-03.pdf
78. Inteligent hardware [online]. [vid. 10. 3. 2015]. Dostupné z:http://www.panduit.com/en/products-and-services/software-intelligence/intelligent-hardware
79. Wi-Fi[online]. [vid. 10. 3. 2015]. Dostupné z:http://www.techrepublic.com/blog/10-things/10-things-you-should-know-about-voip-over-wireless/
80. Telecommunicationdevices[online]. [vid. 10. 3. 2015]. Dostupné z:http://www.deafwebsites.com/technology/telecommunication-devices.html
81. Communicationcentres[online]. [vid. 10. 3. 2015]. Dostupné z:http://www.howardco911.com/pictures.htm
82. ILEC [online]. [vid. 10. 3. 2015]. Dostupné z:http://en.wikipedia.org/wiki/Incumbent_local_exchange_carrier
83. Verizon [online]. [vid. 10. 3. 2015]. Dostupné z:http://www.verizon.com/wholesale/clecsupport/contracts/attachments/cbtoh.pdf
84. ProductsofLucent[online]. [vid. 10. 3. 2015]. Dostupné z:https://support.alcatel-lucent.com/portal/productContent.do?productId=null&entryId=1-0000000003777
85. Locationtracking[online]. [vid. 10. 3. 2015]. Dostupné z:[1]http://electronics.howstuffworks.com/everyday-tech/location-tracking4.htm
86. About911Mapping[online]. [vid. 10. 3. 2015]. Dostupné z:http://www.911mapping.com/About911Mapping.htm
87. FCC Penalty[online]. [vid. 10. 3. 2015]. Dostupné z:http://www.fiercewireless.com/story/sprint-alltel-usc-fined-missed-e911-deadline/2007-08-31
88. NextGeneration911[online]. [vid. 10. 3. 2015]. Dostupné z:http://www.its.dot.gov/ng911/
89. NG911 conceptoperation[online]. [vid. 10. 3. 2015]. Dostupné z:http://www.its.dot.gov/ng911/pubs/concept_operations.htm

90. NG911 [online]. [vid. 10. 3. 2015]. Dostupné z:http://www.911dispatch.com/911/nextgen_911.html
91. ETSI [online]. [vid. 10. 3. 2015]. Dostupné z:http://www.its.dot.gov/ng911/pubs/concept_operations.htm
92. Project NG911[online]. [vid. 10. 3. 2015]. Dostupné z:http://www.cs.columbia.edu/irt/project/ng911/
93. Phases NG911[online]. [vid. 10. 3. 2015]. Dostupné z:http://tools.ietf.org/html/rfc5031
94. Cost study [online]. [vid. 10. 3. 2015]. Dostupné z:https://www.fcc.gov/document/pshsb-next-generation-911-cost-study