ČESKÉ VYSOKÉ
UČENÍ TECHNICKÉ
V PRAZE

FAKULTA
BIOMEDICÍNSKÉHO
INŽENÝRSTVÍ

DIPLOMOVÁ PRÁCE

2019

PAVEL
TŘASÁK

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta biomedicínského inženýrství

Katedra zdravotnických oborů a ochrany obyvatelstva

Modernizace systému centralizované ochrany
Krajského ředitelství Policie Středočeského kraje

Modernization of the centralized system of protection
of the Regional Directorate of the Police of the Central Bohemia Region

Diplomová práce

Studijní program: Ochrana obyvatelstva
Studijní obor: Civilní nouzové plánování

Vedoucí práce: doc. Ing. Karel Hána, Ph.D.

ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

ZADÁNÍ DIPLOMOVÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení:	**Třasák**	Jméno:	**Pavel**	Osobní číslo:	**356036**
Fakulta:	**Fakulta biomedicínského inženýrství**				
Garantující katedra:	**Katedra zdravotnických oborů a ochrany obyvatelstva**				
Studijní program:	**Ochrana obyvatelstva**				
Studijní obor:	**Civilní nouzové plánování**				

II. ÚDAJE K DIPLOMOVÉ PRÁCI

Název diplomové práce:

Modernizace systému centralizované ochrany Krajského ředitelství Policie Středočeského kraje

Název diplomové práce anglicky:

Modernization of the centralized system of protection of the Regional Directorate of the Police of the Central Bohemia Region

Pokyny pro vypracování:

Předmětem diplomové práce bude zhodnocení systému centralizované ochrany Policie České republiky (dále SCO PCR) ve Středočeském kraji před modernizací a po modernizaci. V teoretické části bude popsán historický vývoj SCO PCR ve Středočeském kraji, zhodnocen stav před modernizací z hlediska funkčnosti a pokrytí radiovou sítí v zájmových oblastech. Dále budou popsány kroky k modernizaci SCO, např. nové stanovení zájmových oblastí dle nápadu majetkové trestné činnosti, na základě kterých budou vybrány retranslační stanice pro páteřní síť modernizovaného SCO. V praktické části práce bude prostřednictvím SWOT analýzy zanalyzován stav před a po modernizaci a výsledky následně porovnány. Výsledkem práce bude zhodnocení, zda při modernizaci došlo ke zlepšení funkčnosti a pokrytí systému, případné nedostatky a návrh jejich řešení.

Seznam doporučené literatury:

[1] IVANKA, Ján, Systemizace bezpečnostního průmyslu, Univerzita Tomáše Bati ve Zlíně, 2014, ISBN 978-80-7454-410-1
[2] LUKÁŠ, Luděk, Bezpečnostní technologie, systémy a management V, Verbum, 2015, ISBN 978-80-8750-067-5
[3] LUKÁŠ, Luděk, Bezpečnostní technologie, systémy a management IV, Verbum, 2014, ISBN 978-808-7500-576

Jméno a příjmení vedoucí(ho) diplomové práce:

doc. Ing. Karel Hána, Ph.D.

Jméno a příjmení konzultanta(ky) diplomové práce:

Datum zadání diplomové práce: **01.10.2018**
Platnost zadání diplomové práce: **18.09.2020**

prof. MUDr. Leoš Navrátil, CSc., MBA, dr.h.c.
podpis vedoucí(ho) katedry

prof. MUDr. Ivan Dylevský, DrSc.
podpis děkana(ky)

Kladno, květen 2019

Prohlášení

Prohlašuji, že jsem diplomovou práci s názvem Modernizace systému centralizované ochrany Krajského ředitelství Policie Středočeského kraje vypracoval samostatně pouze s použitím pramenů, které uvádím v seznamu bibliografických odkazů.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu § 60 zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

V Praze dne 14.05.2019

…….
podpis

Poděkování

Mnohokrát děkuji vedoucímu své práce panu doc. Ing. Karlovi Hánovi, Ph.D. za jeho vstřícnost a cenné rady při vedení diplomové práce. Děkuji také svým kolegům z Odboru technické ochrany, kteří mi poskytli podnětné informace. Zároveň děkuji své manželce, která mne podporovala během celého studia.

Abstrakt

Práce se zabývá modernizací Systému centralizované ochrany (SCO) Policie ČR a Krajského ředitelství Policie Středočeského kraje. Definuje SCO jako komplexní bezpečnostní systém, který v těchto rozměrech provozuje v ČR pouze Policie ČR. Také popisuje vývoj SCO na území České republiky v souvislostech s majetkovou trestnou činností.

Součástí práce je analýza stávajícího systému SCO nejen z hlediska funkcí, ale i legislativních podmínek provozu. Ta ukazuje současný stav na hranici životnosti. Odhaluje nedostatky, které má za úkol modernizace vyřešit.

Popis přípravy k modernizaci rozebírá její nedostatky, které komplikují průběh projektu. Analýza modernizovaného systému však poskytuje informace o jasném zlepšení pro SCO a Policii ČR.

Závěr práce hodnotí proces modernizace a potvrzuje stanovené hypotézy o hlavních kladech a celém přínosu projektu.

Klíčová slova

Systém centralizované ochrany; Policie ČR; modernizace; dohledová poplachová přijímací centra; poplachové zabezpečovací a tísňové systémy; SWOT analýza; integrace.

Abstract

This graduation thesis concentrates on the modernization of the Centralized system of protection of the Police of the Czech Republic and the Regional headquarters of the Police of the Central Bohemian region. It defines SCO as a complexed security system, which in this dimension is been practised in the Czech Republic only by the police of the Czech Republic. It also describes the development of SCO within the territory of the Czech Republic in continuities with property criminal activities.

As a part of this document we also present the analysis of the existing system of SCO not only from the point of view of functions but also from the legislative conditions of operations. This shows the actual status on the barrier of lifetime availability. It shows us the absences, which should be then solved by the modernization.

The description of the modernization preparation shows us the analysis of absences, which now complicate the course of the project. The systems modernization analysis therefore supplies us with information about the clear improvement for SCO and for the Police of the Czech Republic.

The closure of the graduation thesis evaluates the process of modernization and confirms the given hypothesis about the main merit and the contribution of the project.

Keywords

Centralized system of protection; modernization; Police of the Czech Republic; monitoring and alarm receiving centre; intrusion and hold-up alarm system ; SWOT analysis; integration.

Obsah

1 ÚVOD

Zabývám se zabezpečovacími technologiemi už 15 let. Od střední školy, kdy jsem se s tématem setkal poprvé, se nepřestávám zajímat o novinky v této oblasti. První fungující DPPC jsem viděl v komerčním sektoru v okrese Louny, které mělo k dispozici pouze dvě zasahující hlídky.

U policie pracuji 7 let, z toho 6 let u OTO SKPV, kde je mojí náplní práce zejména technické zabezpečení objektů. Policie ČR má nejrozsáhlejší systém centralizované ochrany v České republice. Při pohledu na snižující se kriminalitu v oblasti majetku lze říci, že jej využívá úspěšně.

Současná technologie je však za hranicemi své životnosti. Tento stav byl dlouho přehlížen kvůli své finanční náročnosti a také absenci metodického řízení. O modernizaci bylo rozhodnuto zrovna v době, kdy jsem uvažoval o doplnění magisterského vzdělání. Protože jsem nakonec modernizaci ve středočeském kraji dostal na starost, rozhodl jsem se o zpracování své diplomové práce právě na toto téma.

Původní systém má svá omezení a nedostatky, které bych chtěl v rámci své práce odhalit a zajistit, aby se v modernizovaném systému již neobjevili. Vezmeme-li v úvahu letitý rozdíl mezi současným a novým systémem, progres v zabezpečovacích technologiích a finanční náročnosti projektu republikového rozsahu, je více než na místě zhodnotit, zda modernizace přináší příslušný pokrok. Případné nedostatky je potřeba odhalit, analyzovat a navrhnout jejich odstranění.

2 SOUČASNÝ STAV

2.1 Definice Systému centralizované ochrany

Pojem **Systém centralizované ochrany**, dále jen jako SCO, není definován žádnými normami. Platné ČSN normy se zabývají pouze jeho částmi a jejich vzájemnou návazností. V oblasti komerční bezpečnosti si zpravidla zákazník pořizuje pouze jednu či více částí, které následně využívá pro svou potřebu, nebo jimi provozuje služby ostatním. V naprosté většině však nepořizuje celý systém. Policie ČR je natolik rozsáhlá organizace, že je z bezpečnostních, ekonomických a jiných důvodů nucena provozovat a spravovat systém jako celek.

ZPPP č. 115/2009 o výstavbě a provozu systémů centralizované ochrany definuje SCO takto:

"(1) Systém je soubor zařízení umožňující

a) datový přenos z výstupu signalizace (dále jen „signál") sítěmi elektronických komunikací mezi napojeným zabezpečeným objektem (dále jen „střežený objekt") a dispečerským zařízením prostřednictvím přenosových cest systému,

b) zpracování a vyhodnocení signálů,

c) kontrolu a ovládání použitých zařízení." [1]

Tento pokyn je již zastaralý, nepoužívá terminologii, která v rámci norem zaznamenala významné změny. V definici nejsou zahrnuty některé prvky, jako například zabezpečené objekty, které v současné době zároveň tvoří přenosové cesty. V rámci své diplomové práce popíši systém, jak ho vidíme dnes jako technici Odboru technické ochrany (OTO) Služby kriminální policie a vyšetřování Krajského ředitelství Policie Středočeského kraje, spravující SCO.

V případě Policie ČR se jedná o soustavu prvků a funkcí, které zajišťují:

- detekci vzniku události;
- její následné zpracování ústřednou Poplachového zabezpečovacího a tísňového systému, dále jen jako PZTS, nebo jiným zařízením;
- přenos události přenosovými systémy (ATS) a cestami na;
- dohledové a poplachové přijímací centrum (DPPC);
- zpracování události v softwaru DPPC a vyhlášení akce pro obsluhu;
- přijetí události operátorem DPPC;
- reakci na událost;
  - ✓ vyslání hlídky;
  - ✓ kontaktování majitele objektu, v němž vznikla událost atd.;
- vyhodnocení události (pachatel, závada, chybná obsluha), její řešení a ukončení.

Obrázek 1 Systém centralizované ochrany PČR, Zdroj: vlastní

2.2 Prvky SCO

2.2.1 Dohledové a poplachové přijímací centrum

Kombinuje Dohledové centrum a Poplachové přijímací centrum. Jedná se tedy o pracoviště, ve kterém je umístěn hardware a software určený k příjmu, zpracování a řešení událostí, vznikajících v zabezpečených objektech a následné vyhlášení akce, kterou je obsluha povinna ihned přijmout a následně řešit. Každá akce má stanovené instrukce, které je obsluha povinna provést. Účelem je ověřit okolnosti vzniku události, zjistit situaci na místě a zajistit tak

bezpečnost objektu. K zajištění bezpečnosti v místě objektu při poplachové události využívá DPPC zasahují hlídky. [2]

2.2.2 Přenosové cesty

Události z objektů jsou přenášeny prostřednictvím Poplachového přenosového systému (ATS). Komunikaci PZTS objektu na DPPC zajišťuje Poplachové přenosové zařízení (ATE). Nejstarší přenosovou cestou je stále využívaná jednotná telefonní síť. Moderními cestami jsou potom radiové sítě s vlastní licencovanou frekvencí, mobilní operátoři a internet či intranet. Při požadavcích na vysokou spolehlivost, jsou objekty připojovány pomocí dvou a více technologií, se stanovením jejich priorit pro přenos s ohledem na rychlost a stabilitu přenosu (multi path ATS).

2.2.3 Zabezpečené objekty

Objekty vyžadující nepřetržité zajištění bezpečnosti moderními technologiemi, jako jsou systémy PZTS, CCTV, GPS a jiné. Nejrozšířenějšími jsou systémy PZTS.

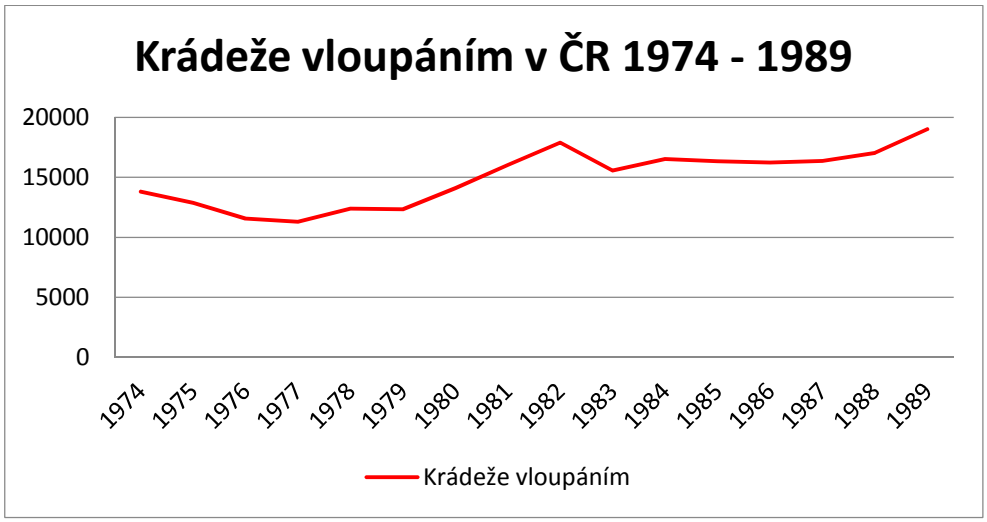
PZTS - *"poplachový zabezpečovací a tísňový systém (intrusion and hold-up alarm system) kombinovaný systém určený k detekci poplachu vniknutí a tísňového poplachu." [3]*

PZTS se skládá z:

- poplachového zabezpečovacího systému - *"poplachový systém sloužící k detekování a indikaci přítomnosti, vniknutí nebo pokusu o vniknutí vetřelce do střeženého prostoru" [3];*
- poplachového tísňového systému - *"poplachový systém poskytující uživateli možnost úmyslného vyvolání poplachového stavu" [3].*

2.3 Historie SCO Policie ČR

Během 70. a 80. let 20. století v Československu postupně narůstá majetková trestná činnost. Jedná se zejména o krádeže vloupáním. Poškozené jsou především hospodářské objekty. Následkem jsou značné škody převážně na státním majetku. Rostoucí trend ukazuje následující graf, ve kterém jsou data od roku 1974, kdy se nápad trestné činnosti začal dělit dle takticko-statistické klasifikace (TSK). [4]



Obrázek 2 Krádeže vloupáním v ČR 1974 - 1989 Zdroj dat: ESSK Policie ČR

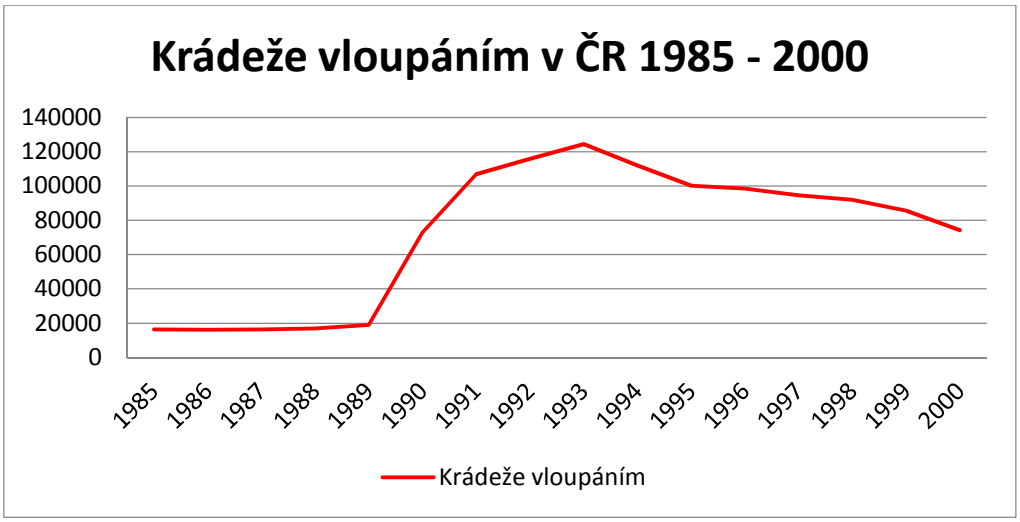
Tuto situaci bylo nutné řešit. Jedním z opatření na ochranu majetku, které přijalo tehdejší Ministerstvo vnitra, bylo rozhodnutí o vybudování SCO, a to po vzoru jiných evropských zemí. První Pult centralizované ochrany (PCO), dle dnešní terminologie DPPC, byl zkoušen od roku 1971 na Federální správě Veřejné bezpečnosti. SCO bylo legislativně podpořeno usnesením vlády ČSSR č. 73/1982 a vyhláškou FMV 135/1983 Sb. o ostraze majetku a centralizaci ochrany zabezpečených objektů. V roce 1976 byl v Příbrami instalován PCO (DPPC) Něva 60, na který se signály dostávaly po telefonních linkách. Protože se osvědčil, byla jeho vylepšená verze CENTR KM rozšířena do většiny krajských měst. Umožňoval napojení až 120 objektů na jedné telefonní ústředně. Skládal se z dispečerského zařízení a výkonového dílu. Dispečerské zařízení,

umístěné na operačním středisku, signalizovalo opticky a akusticky narušení objektu. Výkonový díl byl osazena na telefonní ústředně. Dalším zařízením z tehdejší Bulharské lidové republiky bylo zařízení RONA s kapacitou 240 objektů, přičemž výkonový díl byl pro 60 objektů. To umožňovalo osazení až čtyř telefonních ústředen a napojení objektů na těchto ústřednách. Další vylepšení znamenal pult TCP 60, který již neblokoval linku, protože využíval nadhovorové pásmo. Nicméně byl náročnější na kvalitu linek a jejich neustálou údržbu. [4]

Všechny výše zmíněné pulty byly zahraniční výroby. V roce 1985 přichází český podnik METRA Blansko ve spolupráci s FS VB s pultem jménem TVRZ. Tento pult byl plně automatizovaný, režim střežení byl již ovládán přímo z objektu a nezatěžoval tak operační středisko. Tiskárna zálohovala veškeré informace. Dalším z českých výrobků byl pult GENOVA vyráběný v Novém Jičíně. Umožňoval střežení a přenos událostí i během hovoru. [4]

Veřejná bezpečnost provozovala v roce 1989 na území Československa 79 Systémů centralizované ochrany se 7724 napojenými objekty. Rozvoj byl komplikován materiálovou a cenovou dostupností. [4]

Další rozvoj Systémů centralizované ochrany odstartoval rok 1990. V tuto dobu opět rapidně vzrostla kriminalita v oblasti majetkové trestné činnosti. Tehdejší Obvodní ředitelství Policie ČR ve velké vlně poptávají SCO. Poptávky nemohou být z technických a finančních důvodů uspokojovány. OŘ PČR proto provozují systémy, které nabyly formou darů či zápůjček. Rozšiřování SCO je tedy nesystémové, a dává tak prostor pro rozšiřování soukromých bezpečnostních služeb do oblasti vývoje poskytování služeb centralizované ochrany. [4]



Obrázek 3 Krádeže vloupáním v ČR 1985 - 2000 Zdroj dat: ESSK Policie ČR

V roce 1992, v souvislosti s ohrožením kulturního dědictví v ČR, bylo vydáno usnesení vlády č. 584/1992. Toto usnesení obsahovalo rozhodnutí o vybavení PČR jednotným typem PCO pro všechny okresy České republiky. [4]

Tentýž rok bylo vyhlášeno výběrové řízení, které vyhrála česká firma FIDES Brno s.r.o., jež dodávala systém FAUTOR II, skládající se z vrstvené radiové sítě a PCO (DPPC). Komunikace probíhá v pásmu 160MHz a síť je řízena PCO (DPPC). Vybavení všech OŘ bylo dokončeno v roce 1996 a provoz všech starých zařízení ukončen v březnu 1999. [4]

2.4 Vývoj SCO PČR z FAUTOR II do dnešního LATIS SQL

2.4.1 SCO FAUTOR II

Prvním systémovým a republikově jednotným Systémem centralizované ochrany v Policii ČR se tedy stává systém **FAUTOR II**. Firma Fides Brno s.r.o. dodává kompletní Systém centralizované ochrany. Jedná se o:

- PCO (DPPC) - sestava FA001;
- objektové stanice (PZTS) - včetně radiomodemu, která může také sloužit jako retranslátor (opakovač signálu) a dohromady tvoří radiovou síť.

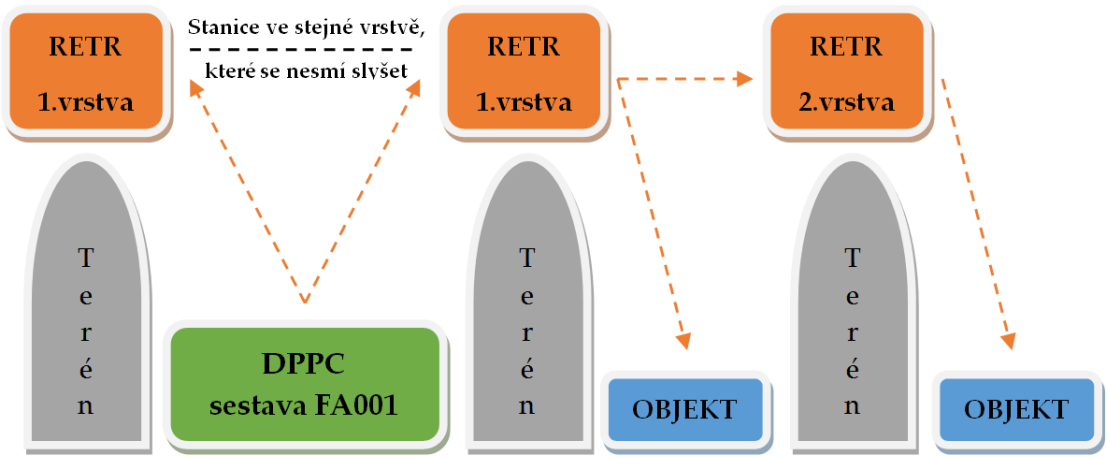
Ze strategických důvodů jsou PCO (DPPC) umisťovány na stávající operační střediska jednotlivých OŘ Policie ČR. Okresům jsou přiděleny jednotlivé kmitočty a také dvouciferná čísla označující síť příslušného okresu. Objekt pak identifikují dvě čísla - číslo sítě a číslo objektu.

Sestava FA001 je složena z PC 486DX, barevného monitoru, klávesnice, myši, záložního zdroje, tiskárny, střediskové antény, oddělovacího transformátoru, kontroleru činnosti PCO a dvou modemových desek. Jedna obsahuje radiový kanál pracovní a záložní. Druhá obsahuje dvě komutované telefonní linky. Na této sestavě běží systém MS-DOS kde je nainstalován program PCO.EXE. Ten zajišťuje organizování základních funkcí, jako je řízení radiové sítě, příjem a zpracování zpráv a vysílání povelů objektům. Program je sestava oken poskytující pouze textové, barevně rozlišitelné informace. Není zde jakákoliv grafická nadstavba. Lze je ovládat pomocí klávesnice nebo myši. Takto vybavená sestava je připravená pro příjem radiové komunikace a komunikace po JTS jako záložní trasy. Program PCO.EXE je schopný zvládnout až 1998

stanic s číslováním od 100 do 4094, přičemž jsou objekty číslovány pouze sudými čísly. Lichá čísla jsou interně využívána pro retranslaci. [5]

Radiovou síť tvoří strategicky umístěné hlavní retranslační body a objekty připojené na PCO (DPPC), mající význam v pokrytí území signálem. Retranslačním bodem či objektovou stanicí jsou zařízení FAUTOR FA101. Těchto zařízení je hned několik typů pro různé druhy použití dle velikosti a tvaru skříně z důvodu velikosti vnitřního záložního akumulátoru. Pro hlavní retranslátory byly využívány hlavně typy FA101a s větším záložním akumulátorem. Síť FAUTOR II složená ze zařízení FA101 byla tvořena dle následujících pravidel:

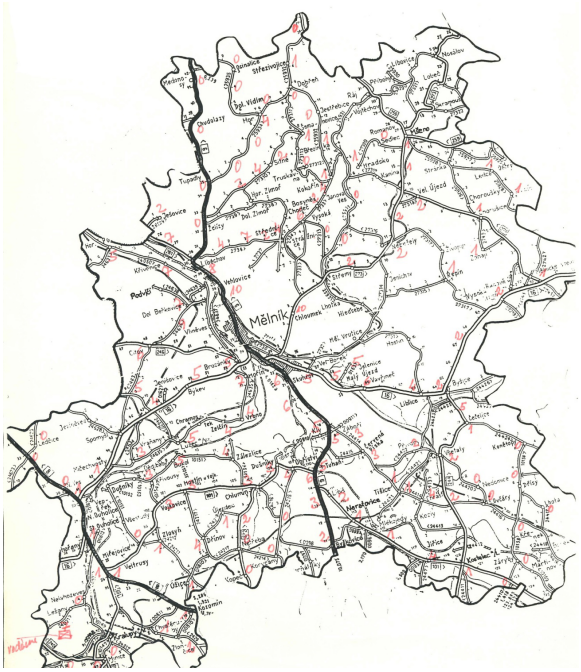
- každá stanice se identifikuje číslem sítě a číslem objektu;
- pro každou stanici je určeno, zda bude retranslátorem;
- stanice mezi sebou komunikují ve vrstvách;
- retranslátory ve stejné vrstvě by se neměly slyšet, aby nedocházelo ke kolizím.



Obrázek 4 Umístění retranslátorů do vrstev, Zdroj: vlastní

Pro umístění neexistoval žádný projekt, ani předběžná měření. Výběr umístění těchto bodů byl postupně prováděn krajskými techniky, ve spolupráci s okresními techniky, na základě místní znalosti terénu a pokrytí signálem

v požadovaných lokalitách. Vlastní montáž si také Policie prováděla sama. V některých okresech pak bylo prováděno měření pokrytí z automobilu, kterým posádka procestovala okres. Výsledkem byla mapa pokrytí, dále využívaná při rozvoji sítě a připojování koncových objektů, včetně těch civilních. Z koncových objektů byly dále vybírány objekty k zapnutí retranslační funkce pro dokrytí zájmových lokalit bez signálu.



Obrázek 5 Mapa pokrytí sítě Fautor II v okr. Mělník 1993 Zdroj: Svazek systému Fautor II ME

Objektová zařízení FA101 jsou komplexní zařízení složená ze zabezpečovací ústředny a radiostanice. Zabezpečovací ústředna má 8 vyvážených smyček a 4 výstupní relé ovládaná dálkově z DPPC či místně. Dále je zde k dispozici komunikátor k připojení na JTS, komunikující formátem ADEMCO a FRANKLIN 4/2. Telefonní spojení přes JTS bylo používáno jako záložní spojení při výpadku komunikace po radiové síti. Na informačním LED panelu nalezneme informace o tom, zda je ústředna online, stav střežení, jestli má ústředna informace v bufferu a další. Ústřednu je možné ovládat připojenou klávesnicí C&K nebo vypínačem připojeným na smyčku k tomu naprogramovanou. [6]

Obrázek 6 Ovládací klávesnice C&K Zdroj: vlastní

Verze ústředny se dělila na policejní a civilní. Zásadní rozdíl byl v možnostech nastavení čísla objektu. Pro policii byla určena čísla objektů 100 až 998, pro civilní objekty čísla 1000 až 4000. Součástí objektového zařízení FA101 byla radiostanice naladěná na kmitočet přidělený příslušnému okresu. Používaly se radiostanice firem MAXON, RAMCO, ONWA, YASU a jiné. [6]

Obrázek 7 Objektové zařízení FA101a. Zdroj: vlastní

Programování ústředny se provádí prostřednictvím čtyř tlačítek umístěných na desce ústředny a připojeným servisním displejem. V pozdější verzi bylo možné programování provádět připojeným počítačem prostřednictvím linky RS232. Na PC bylo možné sledovat i aktuální stav jednotlivých smyček, či relé.

Obrázek 8 Servisní displej pro OZ FA101 Zdroj: vlastní

Je zřejmé, že projekt republikového rozsahu se nemohl obejít bez obtíží. Největší potíže zřejmě přinesla instalace dohledového softwaru. Jak vyplývá z různých stavebních deníků jednotlivých instalací a záznamů jednání s dodavatelskou firmou, trvalo v průměru rok, než se ze zkušebního provozu mohlo přejít na ostrý režim. Zkušenosti s provozem během zkušebního provozu odhalily chyby a nedostatky jak v software, tak hardware. Došlo k naskladnění náhradních dílů k hardwaru pro okamžité řešení poruch například záložních zdrojů. Až u verze 30 se software začal jevit jako stabilní. PČR tedy nenakoupila zcela hotové řešení, ale dodavatel jej v prostředí policie ještě vyvíjel. Celé to dokládá i fakt, že manuály dodavatele jsou datovány až po začátku výstavby.

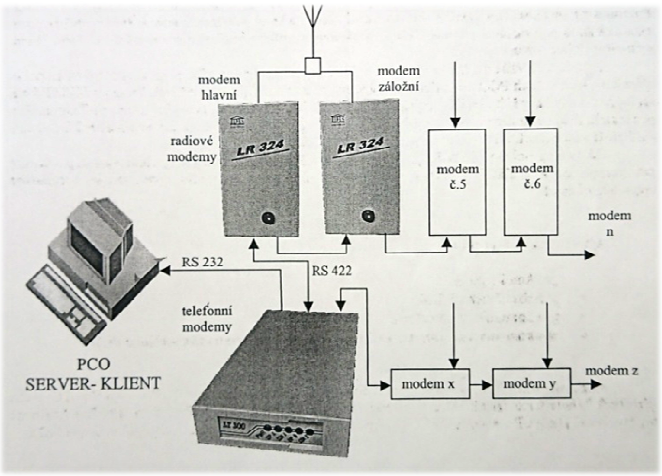
2.4.2 SCO LATIS

S rozvojem informačních technologií si Policie ČR uvědomuje potřebu Systém centralizované ochrany modernizovat a dále rozvíjet. S dodavatelem původního systému uzavírá v roce 1999 smlouvu o modernizaci jednotlivých PCO (DPPC). Technologie přenosové sítě a objektových zařízení zůstávají stejné.

Hlavní body modernizace jsou:

- dva nové radiové moduly LR324 (hlavní a záložní), rychlost 300Bd;
- skříň anténního přepínače LATIS RM s koaxiálním relé;

- nová anténa se svodem;
- telefonní modemy LT300, rychlost 300Bd;
- počítačová sestava (většinou s Windows NT);
- přepěťové ochrany a záložní zdroje;
- software **LATIS** (nyní ve verzi **SERVER** a **KLIENT**).

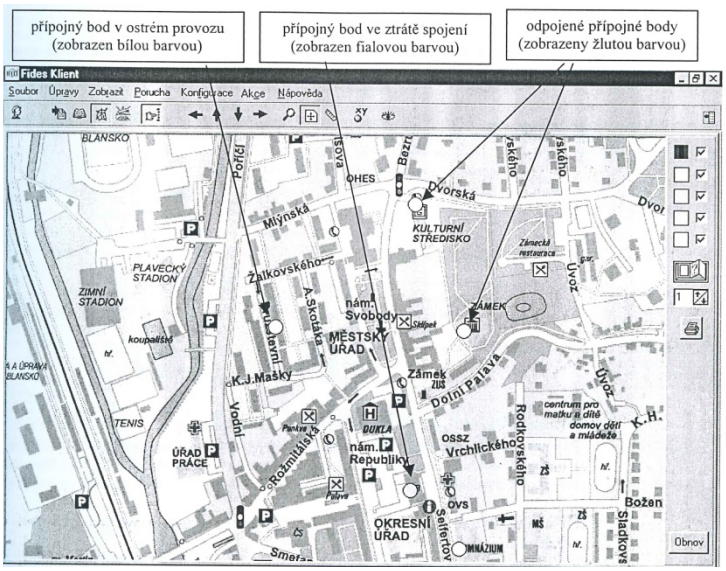


Obrázek 9 Schema systému LATIS [7]

Sestava se zdvojenými komponenty, lepšími přepěťovými ochranami a záložními zdroji, měla zajistit vyšší spolehlivost při poruchách. Software **LATIS** představuje nástroj pro zajištění komunikace přenosových sítí s dispečerským pracovištěm s grafickým, uživatelsky přívětivým rozhranním. Je rozdělen na dvě části: **LATIS SERVER** a **LATIS KLIENT**. LATIS SERVER zajišťuje společně s modemy chod přenosových sítí, sběr veškerých dat, jejich zpracování a vyhodnocení. [7]

LATIS KLIENT zprostředkovává nasbírané informace v grafické podobě trvalé obsluze DPPC a technikům spravujícím informace. Dále umožňuje nastavení celého SCO a odesílání povelů do PZTS. KLIENT v síťové verzi umožňoval připojení do systému z jiných PC, což znamenalo snadnější a pružnější správu, především pro techniky. K programu SERVER lze připojit více programů KLIENT s různými právy a prioritami, přičemž klienti se stejnými prioritami mohou vyhlašované akce přijímat a řešit souběžně.

Systém LATIS umožňuje k objektu vést nejen textové, ale i grafické informace, jakými jsou fotografie objektu, obrázky půdorysů budovy a jiné. Tyto grafické prvky lze v programu Senzored rozšířit o značky jednotlivých detektorů umístěných v objektu. Značky při události mění barvu dle priorit. Tato skutečnost značně usnadňuje identifikaci vzniku události v objektu a popis situace předávaný vyslané hlídce. V případě skutečného napadení pachatelem je možné sledovat jeho pohyb po budově. Ke každému objektu se zapisují GPS souřadnice a objekt je tak možné vidět v mapě. Přehledová mapa ukazovala umístění veškerých objektů a jejich značky při vyhlášení akce měnily barvu dle priority události (typicky červená poplach, modrá technická událost jako například ztráta napájení). [8]



Obrázek 10 Mapa v systému LATIS KLIENT [8]

Během modernizace opět dochází k mnoha potížím. Chyby jako zamrzání programu, ztráty spojení s modemy, nevyhlášené poplachové události a jiné, se objevují v různé míře napříč všemi instalacemi. Potýkají se s nimi tedy zbytečně všechna pracoviště naráz. Například okres Benešov byl dokonce nucen vrátit se k systému FAUTOR II na více než měsíc, aby udržel SCO v chodu. Systém je dodavatelem v podstatě testován v celé republice naráz,

místo toho, aby došlo k otestování na jednom pracovišti, a následnému rozšíření po republice. Dle hlášení a záznamů z porad trvá celé odladění systému ke spokojenosti a spolehlivosti zhruba rok. Operační důstojníci a technici policie jsou zatěžováni a využíváni jako testeři systému. Z tohoto důvodu se dodavatel snaží vyjít vstříc například konkrétním požadavkům k software, požadavkům na cenu za další klientský software nebo vyvinutí modemu pro GSM.

Umístění DPPC z hlediska SCO vždy úzce souviselo s Operačními středisky Policie ČR, protože jsou z Operačních středisek řízeny síly a prostředky PČR, a to v nepřetržitém provozu. Stejně tak jako vše ostatní, prochází si i operační střediska proměnou. S nástupem informačních technologií je trendem integrace. Ta se začíná přenášet i do oblasti operačního řízení již od roku 2000. Postupně se začínají rušit okresní operační střediska a jsou soustřeďována na jednom krajském pracovišti.

Obrázek 11 IOS KŘPS do roku 2014, pouze ÚO PVV, PVJ, PVZ, KL, BE, RA + LTV 158 Zdroj: IOS KŘPS

Tomuto trendu se tedy musí přizpůsobovat i Systém centralizované ochrany. Modemy **LR324**, které byly k počítači připojené sériovou linkou, jsou nahrazeny modernějším modemem **LR324 LAN** ve verzi se síťovým rozhranním. Po intranetu jsou pak z okresu přenášeny informace do PC na krajském operačním středisku.

Obrázek 12 Modem LR324 LAN vlevo, starší LR324 vpravo Zdroj: vlastní

Operační středisko je rozděleno na sektory, ve kterých jsou řízeny dva až tři okresy. Stejným způsobem jsou rozčleněna dohledová pracoviště a umístěna v příslušných sektorech, přičemž na jedné aplikaci KLIENT jsou přístupné objekty ze všech příslušných okresů. Pro rozlišení okresů jsou použity čísla sítí. V přehledu objektů předchází číslu objektu zkratka okresu vycházející z čísla sítě. V praxi pak má objekt tvar *"KL-900 Název objektu"*. Protože jsou již aplikace KLIENT v síťové verzi, mohou okresní technici spravovat objekty na dálku. Integrace, ačkoliv přináší mnohé klady, znamená také komplikace. Jednou ze zásadních komplikací je ztráta místní znalosti. Operační důstojníci spravují různé okresy odkud nepochází a tudíž je neznají. Velkou slabinou při přesunu dohledového pracoviště na krajské ředitelství byl fakt, že spojení s okresní radiovou sítí je zajišťováno přes TCP-IP spojení intranetové sítě. V případě jejího výpadku nemá dohledové pracoviště spojení se všemi objekty. Systém v tomto případě začne vyhlašovat ztrátu spojení všech objektů. To klade velké nároky na obsluhu, která v případě operačního důstojníka policie má na starosti úkony operačního řízení svého sektoru netýkající se zabezpečení objektů.

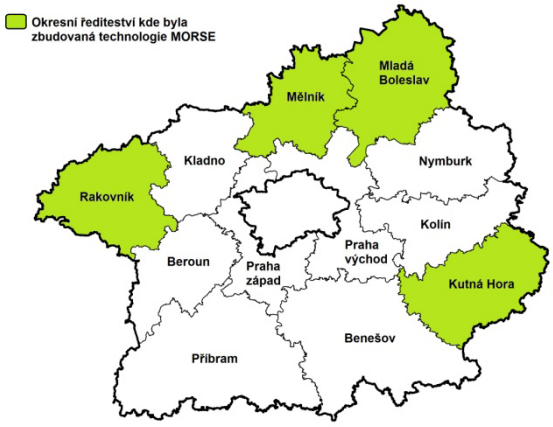
2.4.3 Přenosová síť MORSE

Kolem roku 2004 se začíná jednat o přechodu z pásma 160MHz do pásma 400MHz, kde také funguje komunikační systém Pegas určený pro složky IZS. Důvodem bylo sjednocení frekvencí a uvolnění pásma 160MHz pro jiné účely.

Postupně se začíná stavět modernější síť **MORSE** od firmy RACOM s.r.o.. MORSE je směrovaná paketová síť, kterou již neřídí PCO, ale řídí se samostatně kolizním způsobem. V případě výpadku přenosového bodu je možné konfigurovat záložní trasy tzv. NextHop. Odpadá problém, kdy se retranslační stanice vzájemně slyší. Její přenosová rychlost je 21680 Bd, což oproti 300Bd v síti FAUTOR II je obrovský rozdíl. Rádia MORSE jsou navíc schopna obsluhovat až čtyři sériové porty, dva porty LAN a také integrovaný modul GPS. MORSE bylo vhodné pro připojení více objektů, či umístění v pohyblivém objektu. Používané rádiové modemy mají označení MR400.

Obrázek 13 Rádiový modem MORSE MR400 od firmy RACOM Zdroj: vlastní

Ve Středočeském kraji od roku 2005 postupně přešly na systém MORSE čtyři okresy z celkových dvanácti. Na dobudování nebyly finanční prostředky. Kraje, které nejsou takové rozlohy, jako například Karlovarský kraj, byly schopné dobudovat MORSE síť na celém území.



Obrázek 14 MORSE ve Středočeském kraji Zdroj: šablona z ČSÚ

Český telekomunikační úřad stanovil pro přechod termín, který je později několikrát prodloužen z důvodu finanční náročnosti modernizace v celé Policii ČR.

2.4.4 SCO LATIS SQL

Během let 2004 až 2009 bylo metodické řízení Systémů centralizované ochrany na Policejním prezidiu zredukováno na jednoho policistu. V souvislosti se vznikem Krajských ředitelství Policie, jako samostatných ekonomických subjektů, se krajská pracoviště Odborů technické ochrany spravující SCO musela začít o rozvoj zajímat po své linii. Někteří se rozhodli investovat a rozšiřovat systémy MORSE, jiní pouze udržovali současný stav funkční.

Krajské ředitelství Policie Středočeského kraje se v souvislosti s projektem plné integrace operačních středisek rozhodlo zmodernizovat dohledový software a zakoupit novou verzi systému LATIS, a to LATIS SQL, někdy také označovaný jako LATIS 2. Integrované operační středisko KŘP Stč kraje bylo dokončeno a začíná fungovat v roce 2014. Všechna operační střediska na územních odborech zanikají. Software LATIS SQL je moderním nástupcem předchozího LATIS. Princip je stejný, ovšem LATIS SQL, jak název naznačuje, nyní pracuje s databází Microsoft SQL. Latis SQL je tedy serverovým řešením

běžících služeb, které se starají o oblasti procesů, jako je řízení jednotlivých technologií, automatické činnosti vyhodnocování přijatých informací a podobně. Modernějším způsobem pracuje s informacemi. Stává se univerzálnějším, umožňuje připojení zařízení jakýchkoliv třetích stran. Lépe zpracovává grafickou nadstavbu systému včetně informací o střežených objektech. Ačkoliv byl software známý od roku 2009 a úspěšně nasazen v jiných krajích, neobešla se instalace bez potíží. IOS KŘP Stč kraje bylo navrhnuto jako pracoviště fungující na technologii terminálových serverů. Ačkoliv byl dodavatel na tuto skutečnost upozorněn, při realizaci vyšlo najevo, že systém tuto technologii nepodporuje. Navíc zde byl požadavek na tzv. „sektorizaci", kdy jsou terminály rozdělené do sektorů a dle toho se identifikují zobrazované objekty bez ohledu na přihlášeného operačního důstojníka. Tato funkce ovšem také nebyla dostupná. Bylo proto nutné spojit síly techniků spravujících informační technologie operačního střediska, techniků spravujících technologii SCO a vývojářů dodavatele, aby bylo možné software úspěšně spustit a používat. Funkční výsledek se sice podařil, ale znamenal, že Středočeský kraj má odlišnou verzi software než ostatní, což dodnes komplikuje instalaci aktualizací.

2.5 Stav SCO před modernizací

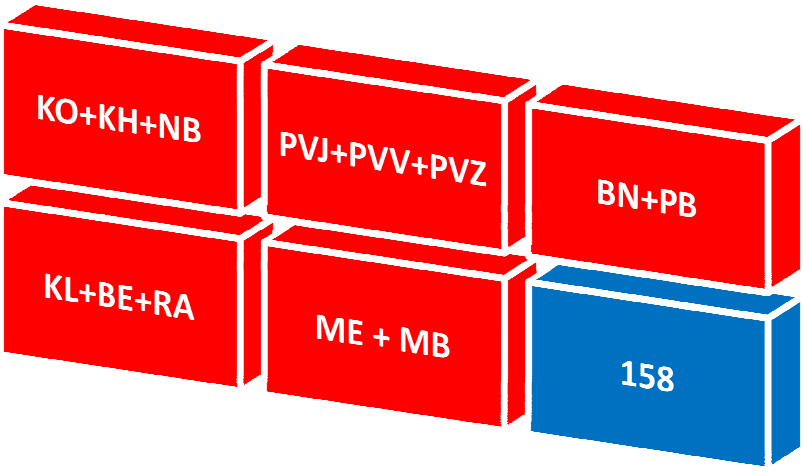
2.5.1 DPPC

Softwarové řešení LATIS SQL běží na vyhrazeném hardware umístěném na ředitelství Územního odboru Mělník. Základem balíku služeb je Modul automatický činností (LAOM), který se stará o celý základ systému. Dále je zde Centrum připojení modemů (LMG), které se stará o spojení s jednotlivými hardwarovými modemy a příjem informací z připojených sítí. V současné době se jedná o příjem z:

- hraničních modemů sítě FAUTOR II;
- hraničních modemů sítě MORSE;
- dvou telefonních modemů (vnitrostátní linka, interní linka policie);
- ústředen ASSET protokolem TCP/IP;
- GPRS modemu pro GPS trackery ke krátkodobé ochraně osob.

Jak bylo již řečeno, LATIS ukládá veškeré informace do systému tabulek v databázi SQL. Pro identifikaci veškerých koncových zařízení je zde zaveden tzv. vyhledávací kód. Ten se skládá z předpony LA označující systém LATIS, čísla sítě a čísla objektu. Pokud má tedy objekt číslo 900 a je ze sítě 52, vyhledávací kód je LA.52.900, pod který systém ukládá informace k objektu.

Integrované operačním středisko Krajského ředitelství Policie Středočeského kraje je umístěno v Praze na Zbraslavi. Zbraslav je propojena s ředitelstvím v Mělníce. Spojení je zajištěno optickým vedením se zálohou po mikrovlnném spoji. Operátoři přistupují k LATIS SQL prostřednictvím programu Latis operator workstation, dále jen jako LOW. IOS je rozčleněno na 6 sektorů, přičemž o příjem událostí z SCO se stará pouze 5 z nich, poslední je určeno pro příjem tísňového volání na linku 158.

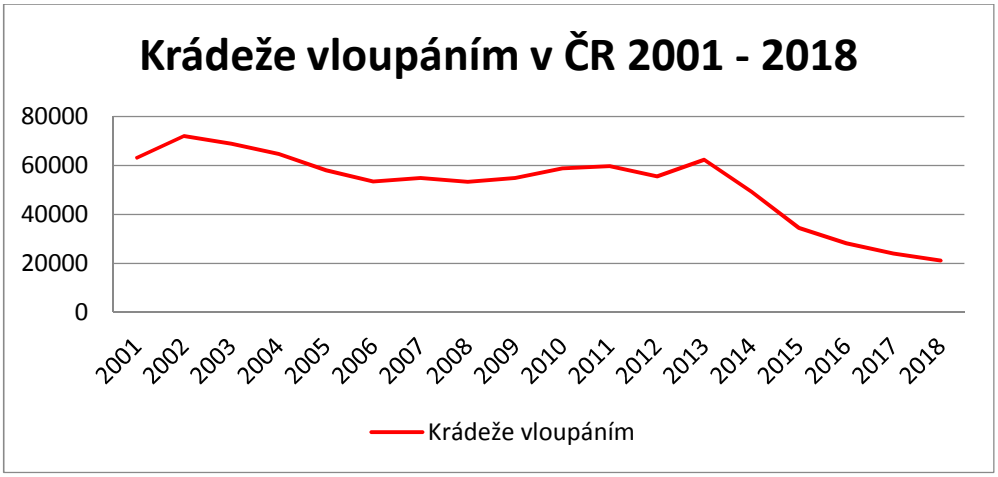


Obrázek 15 Sektorizace IOS KŘPS

Každý sektor má tři terminály. Po přihlášení operátora k terminálu spustí operátor program LOW. Jedná se o klientský software podobný síťové verzi předchozímu programu KLIENT. Připojuje se k serveru a zprostředkovává informace z SCO operačnímu důstojníkovi. Lze mu nastavit parametry jako zobrazení skupin objektů dle již zmíněné sektorizace, příjem konkrétních informací, monitorování vlastního stavu, nepřevzaté události a tak dále. Na každém sektoru lze přijatou událost řešit paralelně na všech třech terminálech. Výhodou je fakt, že pokud jeden z operačních důstojníků musí najednou řešit jinou událost, například netýkající se SCO, dořeší událost ostatní.

Obrázek 16 Integrované operační středisko KŘPS 2014 Zdroj: IOS KŘPS

V SCO Středočeského kraje je nyní napojeno 406 objektů, z toho je 114 vlastních objektů policie, 58 hlavních retranslátorů, 109 objektů civilních, 10 objektů pro ochranu osob. Zbytek je využíván pro účely SKPV jako zabezpečovací opatření při předcházení trestné činnosti, především v oblasti majetku. Zhruba 200 objektů ubylo v posledních 5 letech z důvodu poklesu trestné činnosti.



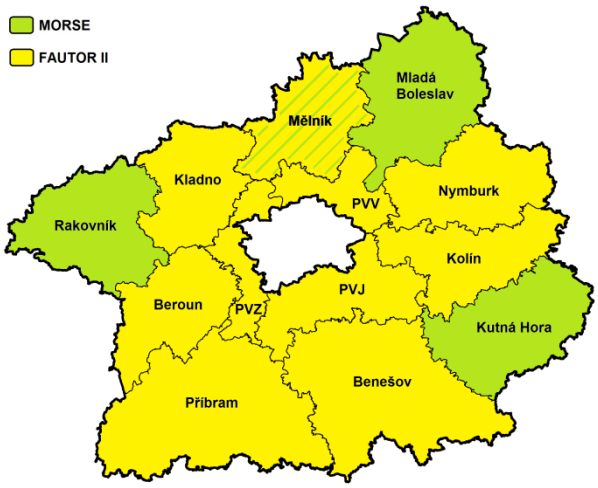
Obrázek 17 Krádeže vloupáním v ČR 2001 - 2018 Zdroj dat: ESSK Policie ČR

2.5.2 Přenosové cesty

Radiová síť pokrývající zhruba 80% Středočeského kraje je v současné době složená ze dvou již zmíněných technologií, kterými jsou:

- MORSE v pásmu 400MHz;
- a FAUTOR II v pásmu 160MHz.

Technologie MORSE je používána územními odbory Kutná Hora, Mělník, Mladá Boleslav, Rakovník. Technologie FAUTORII je používána územními odbory Beroun, Benešov, Kladno, Kolín, Mělník, Nymburk, Praha venkov a Příbram. Ano, územní odbor Mělník používá obě technologie. MORSE zde nebylo dobudováno, aby pokrylo celý územní odbor, proto jsou používány technologie obě.



Obrázek 18 Radiové technologie ve Středočeském kraji Zdroj: šablona z ČSÚ

Další využívanou trasou je telefonní síť. Ve většině případu je využívána jako záložní trasa, nicméně jsou i objekty (zhruba 3% z napojených), které využívají telefonní linku jako hlavní trasu. Je využívaná veřejná telefonní síť komerčních poskytovatelů pro příjem z civilních objektů s modemem LT300, který je na veřejnou síť připojen. A dále vnitřní telefonní síť policie pro objekty vlastní, opět s přijímacím modemem LT300, ovšem připojeným na telefonní síť policie.

Trasy přenosů GSM a GPRS zajišťují mobilní operátoři. GSM komunikaci zprostředkovává zařízení firmy Trade Fides a.s. PZL10, které má integrovaný GSM modem. GPRS přenosy přijímá LTE modem firmy Racom s.r.o., který nese označení M!DGE. Veřejné sítě sebou nesou rizika, která nejsme schopni ovlivnit. V případech výpadků jsme odkázáni na operátora. Mnohdy je jeho nedostatečné pokrytí je takřka neřešitelné.

V současné době je velkým trendem komunikace přes TCP/IP protokol. Mnoho zařízení jej podporuje, a proto poslední sítí, kterou využíváme je intranet policie potažmo internet. Vstupy pro zařízení z internetu jsou spravovány Centrálním místem služeb a zabezpečené příslušným firewallem Barracuda.

Za nejspolehlivější považuji vlastní radiovou síť. I proto se v současné době modernizuje. Vlastní síť je možné monitorovat, spravovat a opravovat dle vlastních potřeb směřujících k jedinému účelu, a to spolehlivému přenosu informací z připojených PZTS. Datové sítě komerčních poskytovatelů, kteří jí poskytují pro různé účely, nemohou dosáhnout spolehlivosti takovéto jednoúčelové sítě ve vlastní správě.

2.5.3 Zabezpečené objekty

Typy objektů, které mohou být připojeny na DPPC Policie ČR vychází ze ZPPP 115/2009 o výstavbě a provozu systémů centralizované ochrany. Článek 1 odstavec 2 říká:

„K systému lze napojit:

a) areály nebo jejich části, v nichž jsou dislokovány útvary Ministerstva vnitra (dále jen „ministerstvo"), policie, organizační složky státu a státní příspěvkové organizace (mimo Zařízení služeb pro Ministerstvo vnitra) zřízené ministerstvem k plnění úkolů v oboru jeho působnosti nebo zřízené právním předpisem, ke kterým ministerstvo vykonává zřizovatelské funkce, nebo jejich organizační články (dále jen „vlastní objekt"),

b) výstupy z technických prostředků používaných policií (dále jen „technický objekt"),

c) objekty státních orgánů a organizací, právnických a fyzických osob, jejichž napojení je stanoveno právním předpisem nebo dohodou schválenou Policejním prezidiem České republiky nebo ministerstvem (dále jen „povinný objekt"),

d) objekty zvláštního významu pro vnitřní pořádek a bezpečnost (dále jen „zvláštní objekt"),

e) objekty, které mohou ovlivnit vnitřní pořádek a bezpečnost na daném území (dále jen „rizikový objekt"), a které stanovili ředitelé krajských ředitelství policie (dále jen „krajský ředitel") nebo jimi pověření příslušníci policie." [1]

Objekty mají dané své přesné číslování, aby bylo možné tvořit skupiny a určit, o jaký typ objektu se jedná. Číslování je upraveno pokynem ředitele centrály informatiky a analytických procesů SKPV PP ČR 8/2010, kterým se upravuje postup příslušníků specializovaných pracovišť Policie České republiky při provozování systémů centralizované ochrany. Článek 6 stanoví:

*„**Číslování napojených objektů***

Napojené objekty se v systému číslují dosavadním způsobem, a to v následující doporučené podobě:

a) objekty technické od 102 do 498 (pouze sudá čísla),

b) objekty vlastní a zvláštní od 500 do 898 (pouze sudá čísla),

c) trvalé opakovače od 900 do 998 (pouze sudá čísla),

d) objekty povinné a rizikové od 1000 do 4092.“ [9]

V první řadě si KŘPS střeží vlastní objekty. Z finančních důvodů nelze zabezpečit všechny prostory, které KŘPS vlastní. Zpravidla jsou zabezpečovány budovy či jejich části, u kterých to vyžaduje legislativa. Jedná se o zbrojní sklady, oblasti pro práci s utajovanými informacemi, sklady cenin a zabavených věcí, kanceláře vedoucích pracovníků, technologické místnosti a podobně.

Současný stav zabezpečení vychází z historie budování sítě FAUTOR II. Objekty vlastní i civilní byly zabezpečovány již zmíněnými ústřednami FAUTOR FA101, přičemž se využívaly především typy FA101a a FA101b. Je neuvěřitelné, že po 30 letech jich pořád ve středočeském kraji funguje téměř 300. Z těchto je přibližně 50 instalováno na vlastních objektech, a zbytek je využíván pro zabezpečovací opatření SKPV. Mají ovšem svou životnost za sebou, některé je potřeba často resetovat, či měnit častěji záložní akumulátory. Někdy se dokonce po výpadku proudu zcela smažou, což vyžaduje nové naprogramování.

Kolem roku 2003, při rekonstrukcích především Obvodních oddělení Policie, byly k zabezpečení využívány nové ústředny firmy Trade Fides a.s. s označením **PZM**. Tato ústředna je modulovým řešením. Samotná ústředna se skládá z modulu **Nucleus**, který propojuje moduly **MULL100**, **PIO** a **CONVAY**. CONVAY překládá komunikaci ústředny radiovému modemu. Existují dva typy: CNV-FN pro radiovou síť FAUTORII a CNV-MN pro radiovou síť MORSE. PIO 8/2 vytváří ze sestavy malou ústřednu s osmy vyváženými smyčkami a dvěma relé. Armování se provádělo sepnutím smyčky. MULL100 vytváří ze sestavy velkou zabezpečovací ústřednu. Byl osazen linkou RS485, na kterou je možné připojovat klávesnice, linkové moduly smyček, moduly reléových výstupů a další. Limit těchto modulů je 32, z toho 4 klávesnice. Touto ústřednou je možné zabezpečovat rozsáhlejší objekty. V současnosti jich ve středočeském kraji funguje přibližně 50 na vlastních objektech a další k využití pro zabezpečovací opatření.

Asi 5 rozsáhlejších objektů bylo zabezpečeno ústřednami **Galaxy** od firmy Honeywell. Tyto jsou už nyní zrekonstruované novými ústřednami ASSET firmy Trade Fides a.s..

Od roku 2010 jsou vlastní objekty rekonstruovány ústřednami **ASSET**. Jde o poslední ústřednu, firmy Trade Fides a.s., která je již velice moderní. Je vybavena komunikační linkou RS485, kterou lze libovolně rozšiřovat, a tím pádem připojovat neomezené množství modulů. ASSET navíc podporuje klávesnice a moduly smyček připojované k ústředně PZM. Při rekonstrukci toto usnadňuje situaci, kdy je možné vyměnit pouze ústřednu, a ostatní prvky s kabeláží ponechat. Komunikace ústředny s DPPC probíhá přes ethernetové rozhranní a intranet. Záložní trasa není zbudována. Novými a často používanými moduly jsou **ASSET10** a **ASSET20**. Toto jsou dveřní moduly určené pro elektronickou kontrolu vstupu (EKV). V KŘPS se velmi dbá na

systém EKV a jeho rozšiřování do všech vlastních objektů, a to alespoň na vstupy do budov. Je tomu tak z důvodu zvyšování zabezpečení vlastních objektů, a z důvodu propojení systému EKV s docházkovým systémem. K ústředně je k dispozici aplikace ASSET SERVER, která umožňuje plnou správu ústředen na dálku, včetně příjmu událostí a programování. Programování na dálku přináší značnou úsporu času vzhledem k rychle se rozšiřujícímu se počtu uživatelů a faktu, že ve Středočeském kraji programují ústředny ASSET pouze dva technici. Uživatelé značně narůstají kvůli použití PZTS také jako EKV. V případě poslední rekonstrukce Územního odboru Kladno se jednalo o zhruba 700 uživatelů. Nejedná se jen o nové uživatele, ale také o jejich neustálou migraci. Tato situace se stupňuje, a bude ji třeba řešit personálním posílením Odboru technické ochrany SKPV. V současné době je zrekonstruováno 51 vlastních objektů. Zbylých 64 objektů musí OTO zrekonstruovat co nejdříve, protože současné ústředny FA101 a PZM jsou za hranicí své životnosti. Odhadovaná částka na rekonstrukci je přibližně 2,5 milionu korun. Roční rozpočet OTO je kolem 900 000,-, přičemž na SCO je využita zhruba polovina. Pokud se nenajdou finanční prostředky navíc, bude celý kraj zrekonstruován nejdříve za pět let, což stávající zařízení stará i 30 let nemusí zvládnout. V rámci úspor za montáž si OTO v drtivé většině případů zajišťuje rekonstrukce těchto PZTS vlastními techniky.

3 CÍL PRÁCE A HYPOTÉZY

3.1 Cíl práce

Cílem mé práce bude:

- zhodnocení stavu před modernizací;
- příprava na modernizaci;
- stanovení testovacího regionu;
- stanovení zájmových oblastí k pokrytí;
- výběr retranslačních bodů;
- SWOT analýza modernizovaného systému.

3.2 Hypotézy

1. hypotéza: nový systém bude lépe pokrývat území Středočeského kraje za použití menšího počtu páteřních retranslačních stanic, a tím uspoří finanční prostředky vynaložené na pronájem prostor pro jejich umístění.

2. hypotéza: nový systém přinese rychlejší přenos informací a zálohované trasy tak, aby výpadky částí sítě neznamenaly kritické selhání SCO.

4 METODIKA

Při plnění prvního cíle mé práce - zhodnocení stávajícího stavu, využiji své šestileté znalosti systému a především znalosti a zkušenosti svých kolegů, protože někteří tu byli už při jeho prvním spuštění. Dále prostuduji archivované svazky jednotlivých okresních systémů ze kterých dnešní SCO vychází.

Takto nasbírané informace taktéž použiji k plnění cíle druhého. Právě zkušenosti s dříve nasazovanými systémy by měly udat správný směr postupu při modernizaci a poukázat na chyby, kterých je třeba se vyvarovat. A to od samotného návrhu, přes přípravu, až po samotnou realizaci projektu. Ke stanovení zájmových oblastí kromě zkušeností navíc použiji systém Mapa Kriminality Policie ČR, pro stanovení lokalit se zvýšeným nápadem majetkové trestné činnosti. Výběr bodů pro retranslační stanice bude probíhat tak, že OTO dodá množinu vhodných bodů, ze kterých dodavatel vybere ty nejvhodnější na základě matematického modelu pro maximalizaci pokrytí při minimálním počtu.

SWOT analýzou obou systémů a jejich porovnání bych chtěl dojít k závěru, zda nový systém nepostrádá některé z kladů starého systému. Zda dosáhneme zlepšení nedostatků původního systému. A návrh opatření, kterým by byly nedostatky odstraněny.

Na modernizaci se nejen podílím, ale ve Středočeském kraji ji také celou řídím. Poskytuje mi to jedinečný pohled, který zohledním v diskuzi celé problematiky.

5 VÝSLEDKY

5.1 Analýza systému SCO před modernizací

5.1.1 Legislativní rámec pro SCO v PČR

Možnosti použití technologií v SCO Policie ČR upravuje zákon a interní předpisy, kterými jsou:

- Zákon č. 273/2008 o Policii České republiky;
- ZPPP 115/2009 o výstavbě a provozu systémů centralizované ochrany;
- Pokyn 8/2010 ředitele centrály informatiky a analytických procesů SKPV PP ČR, kterým se upravuje postup příslušníků specializovaných pracovišť Policie České republiky při provozování systémů centralizované ochrany;
- ZPPP 16/2009 kterým se upravuje jednotný postup příslušníků Policie České republiky při vyžadování použití zabezpečovací techniky;
- ZPPP 17/2009 kterým se upravuje postup specializovaných pracovišť při použití zabezpečovací techniky.

Prvním zakotvení použití technologií pro SCO existuje v zákoně o Policii, kde jsou nazvány velmi obecně jako **zabezpečovací technika** a zařazeny pod **Podpůrné operativně pátrací prostředky**. Dle paragrafu §76 zákona č. 273/2008 o Policii České republiky se zabezpečovací technikou rozumí *„technické prostředky, zařízení a jejich soubory používané za účelem předcházení nebo odstranění ohrožení veřejného pořádku a bezpečnosti.“ [10]*

Takovéto obecné zakotvení dává v podstatě neomezené možnosti při výběru použitých zařízení, což je velice důležité vzhledem k rychlosti dnešního rozvoje informačních, komunikačních a zabezpečovacích technologií. Tím pádem není nutné zákon v tomto směru upravovat.

Závazné pokyny policejního prezidenta 16 a 17 z roku 2009 dále upravují použití zabezpečovací techniky a její nasazení specializovanými pracovišti. Zde jsou opět použity obecné termíny zabezpečovací technika, tudíž z hlediska SCO zde nejsou důvody k novelizaci.

Závazný pokyn policejního prezidenta 115/2009 byl zpracován již neexistující Centrálou informatiky a analytických procesů služby kriminální policie a vyšetřování Policejního prezidia České republiky. Odpovědnost za metodické řízení SCO není zcela jasně stanovena, nicméně pracovníci zodpovědní za metodiku k SCO byli přesunuti pod Odbor informatiky a provozu informačních technologií na policejním prezidiu. Zde nakonec zůstali pouze dva (jeden policista a jeden občanský zaměstnanec), přičemž v začátku modernizace byly posíleni o dva policisty z krajských pracovišť. Závazný pokyn užívá v normách ČSN neexistující pojmy, které by bylo dobré nahradit. Ve výkladu pojmů v článku 2 se píše že:

- **signalizací** je *„soubor zabezpečovacích elektronických a elektromechanických prvků včetně ústředny, kterými je střežený objekt zabezpečen,“* [1];
- **dispečerským zařízením** je *„indikační a ovládací část systému zajišťující*
  - ✓ *1. příjem, zpracování a vyhodnocení signálů ze střežených objektů,*
  - ✓ *2. ovládání a kontrolu stavu systému, signalizace a přenosových cest,“* [1].

Označení **signalizace** je v tomto případě příliš obecné, dle normy ČSN se jedná o **Poplachový zabezpečovací a tísňový systém** (intrusion and hold-up alarm system) tedy PZTS (I&HAS). Žádný jiný, nesplňující normy, by k SCO neměl být připojen. Není proto důvod tuto komponentu jakkoliv zobecňovat.

Dispečerským zařízení je dle normy Dohledové a poplachové přijímací centrum (DPPC). Není zapotřebí rozepisovat funkčnost této komponenty, protože ji dostatečně opět popisuje platná norma ČSN.

Zálohování systému je určeno Odboru technické ochrany. Ovšem s ohledem na fakt, že systém využívá a bude využívat k ukládání veškerých informací databázovou strukturu SQL, kterou spravuje Odbor informačních a komunikačních technologií, je potřeba toto ustanovení změnit. Taktéž daná velká denní frekvence zálohování není pro systém SQL vhodná.

Pravidla správy systému, připojování objektů a vedení informací k nim jsou pospána naprosto dostatečně. Bohužel nejsou v praxi striktně dodržována. Informace vedené k objektům jsou ovlivněny velkou fluktuací lidských zdrojů, proto se stává, že zejména kontaktní osoby nejsou aktuální a to především u objektů civilních.

Dalším velkým nedostatkem je zpracovávání dokumentace zákroku k objektům. *„Zákrokovou dokumentaci zpracovává pověřený pracovník místně příslušného pracoviště policie, které bude provádět zákrok.“* [1] Tuto funkci často suplují technici Odboru technické ochrany, kteří pouze podávají souhrn informací k objektu (přístupové trasy, pes, ostnatý drát,...), nikoliv k samotnému zákroku v případě napadení objektu.

Velkou slabinou se stává fluktuace lidských zdrojů a jejich nedostatek. To má za následek nedostatečnou činnost v pravidelných funkčních zkouškách, kontrolách a revizích, především retranslačních stanic a vlastních objektů. Také pokulhává systém školení operátorů, kteří dnes nabývají znalosti více sami a od zkušenějších kolegů, než ze vstupního kurzu pro operačního důstojníka nebo pravidelných školení OTO, které se prakticky nedějí.

Článek 20 ZPPP 115/2009 stanoví:

„Zmocnění

(1) Ředitel metodického pracoviště se zmocňuje k vydání pokynů, kterými stanoví

a) jmenování poradního orgánu složeného ze zástupců vedoucích krajských odborů a metodického pracoviště; jednání poradního orgánu se uskutečňuje podle aktuální potřeby, nejméně však jednou za kalendářní rok,

b) technické podmínky provozu jednotlivých typů a komponentů systému,

c) rozsah provádění předepsaných periodických revizí dispečerského zařízení a použitých zařízení přenosových cest včetně antén a anténních svodů,

d) konkrétní sledované ukazatele využívání systémů,

e) programové vybavení pro vedení přehledu a statistik provozu systémů a zpracování pololetních hlášení,

f) rozhraní pro propojení ústředny s přenosovým zařízením,

g) rozsah a formu vedení elektronické podoby dokumentů k systému a střeženým objektům.

(2) Krajský ředitel vydá pro potřebu specializovaného pracoviště seznam rizikových objektů a aktualizuje jej vždy k 1. lednu každého kalendářního roku.“ [1]

K tomuto článku je bývalým pracovištěm vydaný výše zmíněný Pokyn 8/2010. Tento by měl být kompletně přepracován. Jednak používá starou terminologii, například pult centralizované ochrany, který je dnes dle normy označován jako DPPC. A také obsahuje spoustu pravidel, jež nemohou být dodržena. Hned článek 1 hovoří o poradním orgánu v čele s vedoucím skupiny pultů centralizované ochrany, přičemž tato skupina již dlouhou dobu neexistuje.

V článku 2 jsou v rámci zachování jednotné koncepce stanoveny komponenty pro SCO, kterými jsou:

- FAUTOR II;
- MORSE.

Použití jiných systémů dále podléhá schválení metodickému pracovišti, které však neexistuje. V tomto článku bude nutné přidat technologii RIPEX, se kterou firma Trade Fides a.s. vyhrála výběrové řízení na modernizaci SCO. Také by bylo vhodné, aby článek upravoval komponenty pro DPPC a radiovou síť, místo pro celé SCO. V SCO jsou užívány další komponenty, například komunikující přes sítě mobilních operátorů. Všechny tyto komponenty nelze a není výhodné do pokynu zahrnout.

Komunikace PZTS s přenosovým zařízením po RS232 zůstává, nicméně stanovené protokoly budou s modernizací muset projít revizí a doplněním.

Již zmíněné číslování objektů musí projít také úpravou. V novém systému bude možné využívat i lichá čísla, což zvětšuje prostor pro napojené objekty.

Jsou zde stanovené podmínky zálohování, které je třeba upravit pro možnosti zálohování SQL databází spravovaných jiným odborem než OTO.

5.1.2 DPPC

Policie ČR má DPPC umístěná dle ZPPP 115/2009 vždy na operačních střediscích. Můžeme se v zásadě potkat se dvěma modely obsluhy DPPC. První model zavedený v Praze a Ostravě má DPPC jako uzavřený sektor a operační důstojníci mají na starosti pouze dohled nad SCO. Druhý model aplikovaný na IOS KŘPS znamená již zmíněnou sektorizaci a operační v sektoru nejen řídí hlídky PČR, ale starají se i o obsluhu DPPC. Oba modely mají své výhody i nevýhody.

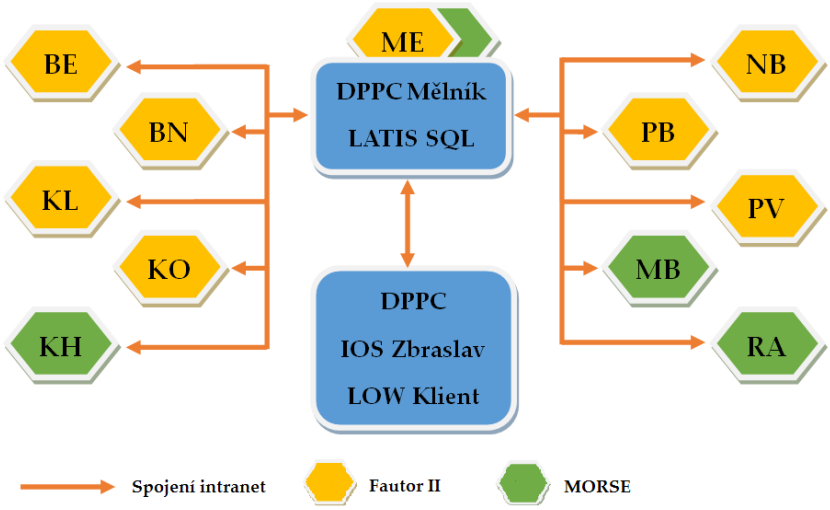
Největší výhodou modelu izolovaného pracoviště DPPC, je získání dobrého přehledu operátorů o systému, připojených objektech a jejich režimech. Operátoři prvního modelu jsou schopni lépe popisovat vzniklé problémy, předávat informace technikům o poruchách a zajistit tak jejich rychlé odstranění. Nevýhodou je izolace a nepřímý kontakt se zasahující hlídkou, kterou řídí jiný sektor.

Druhý model integrace operačních středisek sebou kromě kladů ohledně zrychlení řízení a toku informací, přinesla také nevýhodu, kdy se okresní technici nepotkávají s operátory DPPC. Jsou při odstraňování poruch odkázáni pouze na historii systému. Do té často kvůli jiným činnostem nemají operátoři čas zapisovat události podrobně. Jsou na ně tedy kladeny vyšší nároky v oblasti schopností, paměti a psychické stability.

Je zřejmé, že výhody prvního modelu jsou nevýhodami druhého rozšířenějšího modelu a naopak.

5.1.3 Přenosové cesty

V současnosti je DPPC propojeno s okresy po nezálohované intranetové trase. Intranet PČR je velice vytížený kvůli stále se rozrůstajícímu systému ETŘ (evidence trestního řízení), přenosům ze systémů PZTS, EKV, CCTV a spousty jiných systému, které Policie využívá.



Obrázek 19 Spojení přenosových sítí okresů s DPPC Zdroj: vlastní

Dále využívané trasy mobilních operátorů se jeví jako běžně spolehlivé co do přenosu informací. Co se týká pokrytí, je KŘPS limitováno operátorem O2, se kterým má smlouvu. Ve středočeském kraji se potýkáme s nedostatečným signálem v odlehlých lokalitách. Zejména jde o chatové oblasti, kde v případě absence signálu již zmíněného operátora, nelze objekty napojit. Většinou jsou tyto lokality pokryté naší radiovou sítí. Pokud jde o objekty, které lze připojit k DPPC pouze prostřednictvím GPRS, jako v případě tísňových tlačítek pro ochranu osob, je třeba poučit chráněné osoby, aby se těmto předem stanoveným lokalitám vyhnuli.

5.1.4 Zabezpečené objekty

Objekty **vlastní** zrekonstruované technologií ASSET jsou připojené přes intranet a postrádají záložní trasu. Již zmíněné výpadky sítě se podepisují na spojení, což by mělo být napraveno záložní trasou. Záložní trasu stanovuje závazný pokyn policejní prezidenta 115/2009 pouze u objektů povinných a rizikových, jednoduše řečeno civilních.

Objekty **technické** používané v rámci zabezpečovacího opatření SKPV k předcházení a odhalování trestné činnosti jsou zabezpečovány především

ústřednami FAUTOR FA101 připojené radiovou technologií FAUTOR II a ústředny PZM připojené technologií MORSE. Vzhledem k tomu, že zabezpečovací opatření je prováděno na 6 měsíců s maximálním prodloužením o dalších 6 měsíců, je zapotřebí montáž provádět rychle a bez větších zásahů do objektu. Zmíněné ústředny jsme tedy začali doplňovat o bezdrátové prvky, které se velice osvědčili. Využívané komplety však neumožňují bezdrátové klávesnice, pouze detektory. V dnešní době integrace a minimalizace rozměrů jsou námi využívané technologie na hranici využitelnosti.

Zvláštním typem technického objektu jsou tísňové systémy. Používáme je při Krátkodobé ochraně osob dle §50 zákona č. 273/2008 o Policii ČR. Systém tísňových tlačítek s určování polohy dle GPS dodala firma Trade Fides a.s., jedná se o čínský výrobek integrovaný do DPPC LATIS SQL. V souvislosti s úkolem vyplývající pro Policii ČR z **Akčního plánu prevence domácího a genderově podmíněného násilí na léta 2015 – 2018**, jsou tato zařízení využívána v projektu prevence a pomoci při domácím násilí. Policisté v rámci vykázání z obydlí nabízejí tísňová tlačítka poškozeným osobám. Projekt byl naplánován na šest měsíců v roce 2019 a probíhá pouze ve dvou územních odborech. Za 4 měsíce vychází nasazení jednou týdně většinou ve večerních hodinách. Prozatím se o technické zabezpečení starám sám, což znamená být k dispozici 24/7 na telefonu a mít připravené pc pro vzdálený přístup. OTO SKPV nemá placený dosah. Za práci mohu být ohodnocen pouze formou odměn.V současné době a při stávajícím počtu techniků si nedovedu představit plošné nasazení projektu.

Objekty **zvláštní** spravované Ochrannou službou jsou ve středočeském kraji napojovány velice zřídka. Za šest let u odboru si pamatuji napojení pouze dvou těchto objektů, přičemž jsou Ochrannou službou vždy perfektně zpracovány.

Objekty **povinné** a **rizikové,** jinak označované jako civilní, jsou zabezpečovány odbornými komerčními firmami a připojovány na DPPC ve spolupráci s firmou Trade Fides a.s.. Civilní firmy se drží stanovených norem, provádějí pravidelné revize, a proto nebývají s těmito objekty potíže po technické stránce věci. Potíže jsou zejména při chybné obsluze, která je dána velkou fluktuací lidí a nedostatečným proškolování.

5.1.5 SWOT analýza stávajícího systému

Tabulka 1 SWOT analýza stávajícího systému

Vnitřní původ	**Silné stránky** ➢ obsluha DPPC na IOS; ➢ šíření signálu v pásmu 160MHz; ➢ množství zasahujících hlídek; ➢ PZTS zahrnující EKV; ➢ přibližně 80% pokrytí kraje;	**Slabé stránky** ➢ pomalý přenos dat; ➢ komunikace řízená DPPC; ➢ legislativa; ➢ nezálohované spojení rekonstruovaných PZTS; ➢ vysoký počet páteřních RETRů;
Vnější původ	**Příležitosti** ➢ rostoucí nároky na zabezpečení; ➢ ukončení licence pro pásmo 160MHz;	**Hrozby** ➢ nezálohované spojení okresů s DPPC; ➢ konec životnosti komponent; ➢ nejsou náhradní díly; ➢ nedodržování legislativních povinností;

V rámci hodnocení stanovím stupnici 1 až 5 pro silné stránky a příležitosti (5 - nejvyšší spokojenost). Slabé stránky a hrozby stanovím dle stupnice -1 až -5 (-5 pro nejvyšší nespokojenost).

Tabulka 2 SWOT analýza stávajícího systému - hodnocení

silné stránky	**váha**	**hodnocení**	**součin**
obsluha DPPC na IOS	0,2	4	0,8
šíření signálu v pásmu 160MHz	0,2	5	1
množství zasahujících hlídek	0,2	4	0,8
PZTS zahrnující EKV	0,1	2	0,2
přibližně 80% pokrytí kraje	0,3	4	1,2
		součet:	4

slabé stránky	**váha**	**hodnocení**	**součin**
pomalý přenos dat	0,3	-5	-1,5
komunikace řízená DPPC	0,1	-2	-0,2
legislativa	0,1	-3	-0,3
nezálohované spojení rekonstruovaných PZTS	0,3	-4	-1,2
vysoký počet páteřních RETRů	0,2	-5	-1
		součet:	-4,2

příležitosti	**váha**	**hodnocení**	**součin**
rostoucí nároky na zabezpečení	0,5	4	2
ukončení licence pro pásmo 160MHz	0,5	5	2,5
		součet:	4,5

hrozby	**váha**	**hodnocení**	**součin**
nezálohované spojení okresů s DPPC	0,3	-5	-1,5
konec životnosti komponent	0,3	-4	-1,2
nejsou náhradní díly	0,3	-4	-1,2
nedodržování legislativních povinností	0,1	-3	-0,3
		součet:	-4,2

Tabulka 3 SWOT analýza stávající systému - součet

Vnitřní část	-0,2
Vnější část	0,3
Součet	0,1

Z nepříliš dobrého výsledku je vidět, že je SCO stále funkční, ale zastaralé. Příliš mnoho důležitých slabých stránek ukazuje na fakt, že je nutné systém zásadně modernizovat.

5.2 Přípravná fáze modernizace

Modernizace SCO Policie ČR se intenzivně začíná řešit v roce 2016, kdy Český telekomunikační úřad (ČTÚ) dává poslední termín opuštění technologií v pásmu 160MHz, tedy FAUTOR II. Posledním termínem vypnutí je konec roku 2020 s tím, že v roce 2017 se již musí začít stavět. V tuto chvíli republikový projekt začíná řešit jediný zbylý člen původního metodického pracoviště pplk. Ing. Jan Řehořovský. Na prezidiu a MV se rodí různé nápady jak situaci řešit. Kromě různých verzí vlastní mobilní sítě se objevovaly tlaky na převzetí modemů Matra (systém Pegas), které mají též odslouženo. Po předložení nespočtu argumentů mluvících proti navrhovaným technologiím, dosáhl pan pplk. Řehořovský rozhodnutí o vypsání veřejné zakázky na zcela novou technologii SCO. Výběrového řízení se účastní pouze dva dodavatelé. První nejmenovaný dodavatel napadl veřejnou zakázku s tím, že se jedná o zakázku na již předem připravené řešení. Dodal, že na vývoj vlastní technologie potřebuje čas. S tímto však neuspěl a veřejnou zakázku vyhrává Policii dobře známý dodavatel Trade Fides a.s. s nabídkou vlastní technologie (software LATIS 3, hardware PZL10) podpořené radiovou technologií RIPEX firmy RACOM s.r.o..

Smlouvu s dodavatelem podepsalo Ministerstvo vnitra 7. června 2017, a to na čtyřleté období za částku 285 000 000,- Kč bez DPH. Většinu práce na přípravu smlouvy odvedl pan pplk. Řehořovský sám. Jeho odvedená práce je obdivuhodná, nicméně projekt takového rozsahu měl od počátku řídit větší tým. Nedostatky bylo nutné řešit dodatky ke smlouvě. Další dodatek ohledně vyhovujícího zařízení pro **technické** objekty je v řešení. Následně byla

rozkazem policejního prezidenta 145 ze dne 12. června 2017 zřízena skupina k zajištění realizace modernizace SCO, která má 30 členů. Rozkaz, mimo jiné, určoval skupině stanovit harmonogram realizace modernizace. V praxi se tato skupina schází pouze 2x za rok. Smlouva určuje pověřující zadavatele, kteří mohou ze smlouvy čerpat dle přiděleného rozpočtu. Kromě samozřejmých článků Policie ČR jsou zde například ČNB, BIS, HZS, soudy, muzea, OSZ, ŘSD a další. Jsou zde proto, aby se mohli nechat dodavatelem připojit přes novou technologii RIPEX.

Rozdělování financí bylo na svém začátku odhadnuto panem Řehořovským dle následující tabulky:

Tabulka 4 Odhadnutý rozpočet pro KŘPS Zdroj: data z OIPIT

rok	částka s DPH	předpokládaný účel
2017	150 000,-	projekt radiové sítě
2018	17 000 000,-	výstaba páteřních RETRů a připojení vlastních objektů
2019	5 000 000,-	pořízení zařízení k zabezpečovacímu opatření
2020	685 000,-	dobudování systému

Modernizace byla rozdělena do několika fází:

1. fáze - výstavba sítě RIPEX v testovacím regionu;
2. fáze - nasazení software pro DPPC LATIS 3 v testovacím regionu;
3. fáze - připojování objektů v testovacím regionu;
4. fáze - výstavba sítě RIPEX v krajích;
5. fáze - nasazení software pro DPPC LATIS 3 v krajích;
6. fáze - připojování objektů v krajích;
7. fáze - odpojení a demontáž technologie FAUTOR II.

Některé fáze se překrývají, některé musejí navazovat.

5.3 Testovací region

S dodavatelem Trade Fides a.s. má Policie ČR mnohaleté zkušenosti. Proto byla správě zvolena cesta nasazení v testovacím regionu, místo plošné výstavby v celé republice, jak tomu bylo v minulých modernizacích. Cílem je samozřejmě otestování nasazených komponent tak, aby plošné rozšíření probíhalo bez zásadních chyb.

O to, stát se testovacím regionem, tak úplně nikdo nestál ze zřejmých důvodů. Vybrán byl nakonec region Praha, a to ze tří zásadních důvodů:

- oddělené pracoviště obsluhy DPPC;
- malá rozloha;
- lokalita blízko policejního prezidia.

Region Praha s velkým počtem vlastních objektů na malém území dosáhl umístění páteřních RETRů pouze na těchto objektech. Tím se vyhnul velkým výdajům za pronájem stožárů a jiných vhodných stanovišť. Původní počet RETRů musel být oproti návrhu zdvojnásoben. Šíření v hustě zastavěných oblastech se s matematickým modelem příliš neshoduje.

Při modernizaci je nutné přejít na nový software bez možnosti návratu ke starému. Proto k instalaci softwarového řešení DPPC byly požadováni i programátoři dodavatele, aby případné chyby hned opravili. Ačkoliv se s nasazením začalo hned ráno, přechod byl dokončen až druhý den odpoledne. Při nasazení se objevila spousta chyb, které programátoři opravovali na místě. Povedlo se sice systém uvést do chodu, nicméně se stále objevují chyby, které ani po téměř roce nejsou odstraněné. Software nasazovaný ve verzi 9 má nyní verzi 18, přičemž verze 15 měla být první stabilní, vhodná k rozšíření do všech regionů.

5.4 Realizace modernizace ve Středočeském kraji

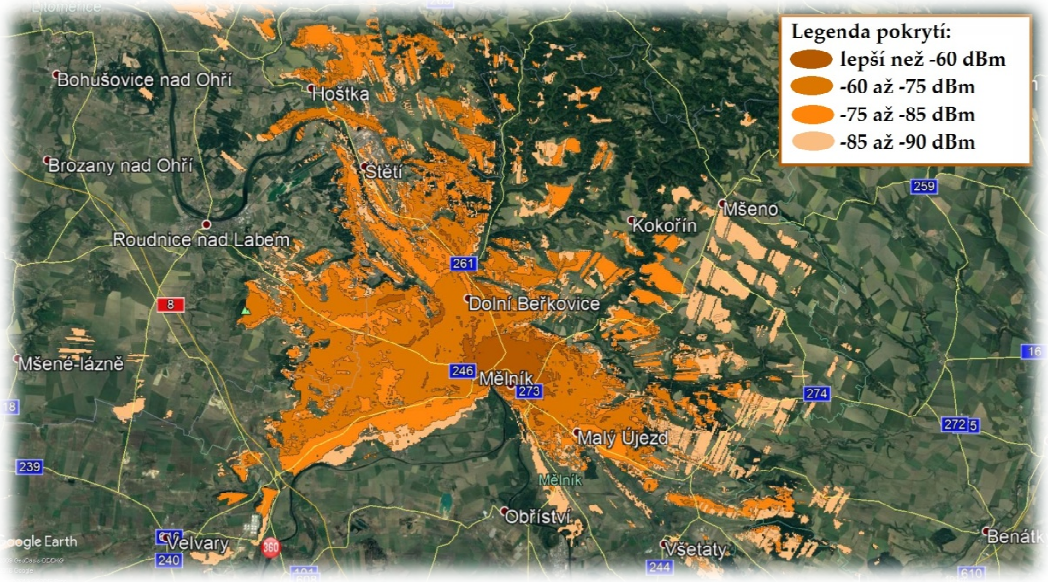
Rozdělování financí se neustále měnilo a mění dle toho, jak jsou jednotlivé kraje schopné stavět, potažmo přidělené finance proinvestovat. Prozatím ve středočeském kraji rozpočet vypadá dle následující tabulky:

Tabulka 5 Rozdělení rozpočtu pro KŘPS Zdroj: vlastní

rok	částka s DPH	předpokládaný účel
2017	150 000,-	projekt radiové sítě
2018	11 000 000,-	výstavba páteřních RETRů
2019	10 000 000,-	připojení vlastních objektů a pořízení zařízení k zabezpečovacímu opatření
2020	4 000 000,-	dobudování systému (pokrytí, objekty vlastní)

V roce 2017 se projet radiové sítě neuskutečnil, proto jsme byli nuceni peníze proinvestovat jinak. Zvolil jsem nákup dvou radií RIPEX, abychom se s nimi mohli dopředu seznámit. Rozpočet, ačkoliv snížený oproti původnímu plánu, byl pro rok 2018 nakonec dostačující pro výstavbu hlavních RETRů.

Co se týká projektu radiové sítě, očekávalo se, že dodavatel provede analýzu terénu, následná měření a naprosto samostatně přijde s umístěním RETRů, jejichž minimální počet zajistí maximální pokrytí. Toto řešení by zabralo čas a zdroje, na které nebyl dodavatel připraven. Přistoupili jsme proto na kompromis, který znamenal poskytnutí informací o stávajících RETRech a jejich umístění. Z tohoto souboru informací pak dodavatel vytvořil matematický model pokrytí všech těchto bodů. Následně stanovil základní soubor stanovišť a jejich směrování. Matematické modely nám byly poskytnuty a na základě jednání o pokrytí v zájmových oblastech jsme počet stanovišť rozšířili.

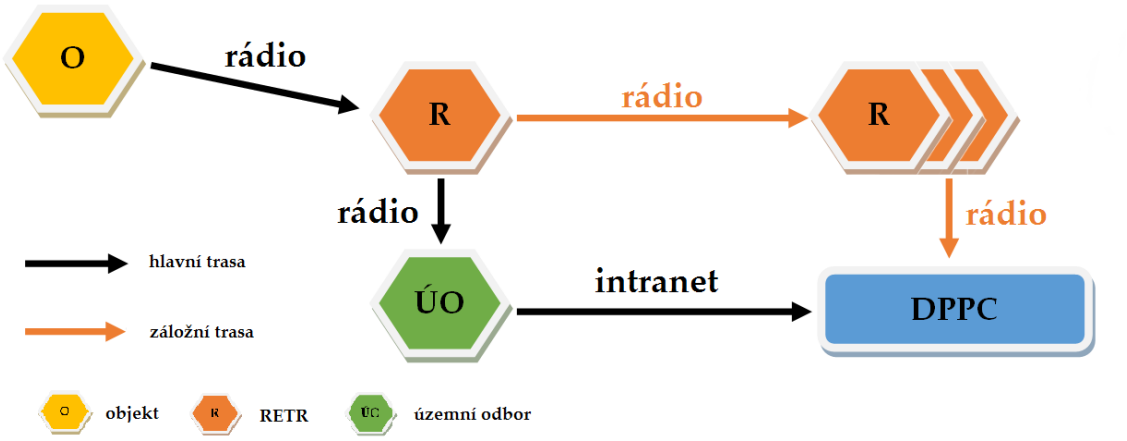


Obrázek 20 Model pokrytí RETRem řediteství ÚO Mělník Zdroj: mapa - Google Earth, data - Trade Fides a.s.

Stanovení zájmových rizikových oblastí dle nápadu trestné činnosti krádeže vloupáním jsem provedl pomocí systému Mapa kriminality Policie ČR. Tento systém umožňuje zobrazení nápadu trestné činnosti v mapě, přičemž sám stanoví rizikové oblasti formou čtverců o straně 5km. Tyto mapy jsou v přílohách č. 1 až 13. Kromě porovnání s rizikovými oblastmi šlo také o zkušenosti. Proto se práce s mapami teoretického pokrytí k určení stanovišť pro RETRy zúčastnili všichni technici OTO Středočeského kraje. Na požadavky jednotlivých techniků byli do výběru rizikových oblastí zahrnuty hlavně odlehlé chatové oblasti, které dle zkušeností bývají postihovány zpravidla přes zimu sériovou trestnou činností.

Koncepce radiové sítě byla od počátku zamýšlena tak, aby informace z PZTS byla směrována co nejrychleji do intranetu PČR a dále na DPPC. V případě výpadku intranetu pak musí informace doputovat záložními trasami po radiovém spoji až na DPPC. K tomuto účelu jsou mezi hlavní RETRy zahrnuta všechna ředitelství územních odborů. Ta fungují jako hranice mezi radiovou sítí a intranetem. Předpis o intranetu zakazuje takovéto spojování cizích sítí

s intranetem, proto je v intranetu pro SCO zavedena VLAN síť s názvem VRF SCO.



Obrázek 21 Systém záložních tras Zdroj: vlastní

Konečný počet páteřních RETRů byl stanoven na 40. Z toho je umístěno 13 na ředitelství územních odborů, 1 na krajském ředitelství, a 26 na strategických výškových bodech ve vlastnictví například ČRa a O2. Výstavba v roce 2018 začala opožděně. Do května se čekalo na stanovení jednotného postupu měření páteřních spojů, spolupráci s dodavatelem a vlastníky jednotlivých bodů (stožáry, rozhledny, ...). V květnu se s dodavatelem začalo plánovat měření páteřních spojů. Středočeskému kraji byla přidělena pražská pobočka dodavatele, který současně pracoval na testovacím regionu Praha. Tím vzniklo tříštění sil prostředků dodavatele, které později zpomalilo celou modernizaci. Mylně jsem se domníval, že dodavatel zajistí měření páteřních spojů bez naší spolupráce. Po několika výměnách názorů mezi kraji, metodickým řízením modernizace z policejního prezidia a dodavatelem, jsme museli vzít postup v měření do vlastních rukou. Ve středočeském kraji jsem společně se dvěma kolegy převzal řízení měření. Domluvili jsme termín prohlídky a měření s vlastníkem. Oznámili jsme termín dodavateli, který si musel svůj harmonogram přizpůsobit. Abychom měření urychlili, poskytli jsme dodavateli vlastní techniky a kufry pro měření. Takto se v jednom termínu

proměřilo více tras najednou. Na základě těchto měření dodavatel zpracovával projekty, které jsme předkládali vlastníkům spolu s žádostí o souběh našich zařízení do roku 2020, kdy bude stará technologie odpojena. Zpracování projektu trvalo dodavateli vždy 2 až 4 týdny. Každý vlastník v projektu požadoval jiné změny a detaily. Jeden vlastník chtěl dokonce pro různá stanoviště různé detaily, jak v projektu, tak v následujícím dodatku ke smlouvě o pronájmu. Jednání o umístění našich technologií na jedno stanoviště trvalo v průměru měsíc. Největší komplikace provází jednání se společností CETIN. Jednání o umístění mezi dodavatelem, PČR a vlastníky jednotlivých bodů byla nejnáročnější z celé modernizace. Znamenala zdržení stavby oproti plánu, kdy páteř měla být v roce 2018 dokončená a přes zimu otestovaná. K odstranění případných nedostatků mělo dojít v prvním pololetí 2019.

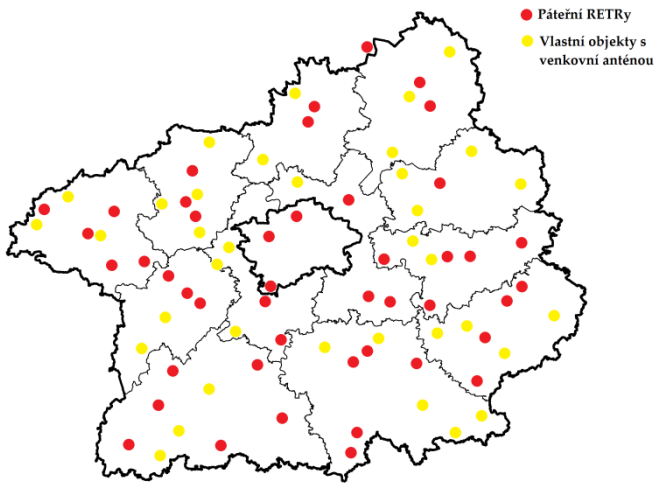
Dodavatel nestíhal stavět ani schválené projekty, proto jsem v srpnu za Středočeský kraj navrhl nasazení vlastních prostředků k vybudování RETRů na ředitelství územních odborů. OTO SKPV si tak vystavělo 13 RETRů samo, dodavatel dodal pouze komponenty. S dodavatelem byla dohodnuta záruka na tyto RETRy za předpokladu dodržení přesně stanovených podmínek montáže. V rámci montáží jsme byli nuceni zakoupit komponenty pracovně polohovacích a zádržných systémů a absolvovat školení pro práci ve výškách a nad volnou hloubkou.

Během stavby a následných měření vyšly najevo velké rozdíly mezi skutečným pokrytím a matematickými modely, dle kterých byla síť navržena. Při jednání s dodavatelem o důvodech těchto velkých rozdílů bylo zjištěno, že matematický model počítal s všesměrovou anténou se ziskem 7dB, která je vhodná pro montáž na samotný vrchol stožáru. V praxi není tuto montáž možné skoro nikdy provést, protože jsou tyto pozice zpravidla obsazeny. Použita byla na všech páteřních RETRech offsetová anténa ATT Plus typ

OV401.2, která dosahuje sice zisku až 7.4 dB, ale pouze v přímém směru. Zhoršuje se tedy signál do boků a pokud je zadní lalok směřován do stožárové konstrukce, signál tato konstrukce značně pohltí.

Obrázek 22 Anténa ATT Plus OV401.2 - montáž, při které je zadní lalok směřován do konstrukce stožáru
Zdroj: vlastní

Ačkoliv jsou páteřní spoje v přímých směrech zcela v pořádku, kontrolní měření ukázala nedostatečné pokrytí. Navyšování RETRů by znamenalo vynaložení dalších finančních prostředků a ustoupení od stanovené úspory za nájmy. Středočeský kraj má 114 zabezpečených vlastních objektů (a to buď ve vlastních nebo pronajatých prostorách). Tyto objekty měli být připojeny pouze pomocí malých vnitřních antén. Navrhl jsem tedy řešení, kdybychom zvýšili počet RETRů a umístili je na vlastních objektech. Společně s kolegy z OTO jsme probrali možnosti, jako umístění technologií v objektech, montáž antén na střešní stožáry a ustanovili jsme 45 vlastních objektů vhodných k montáži s venkovními anténami ATT Plus OV401.2. Ani tak ovšem nebylo pokrytí některých oblastí vyřešeno. Bylo nutné do páteřní sítě oproti plánu zahrnout ještě 4 výškově strategická stanoviště. Ostatní objekty se osazují malými vnitřními anténami.



Obrázek 23 Mapa páteřních RETRů doplněných o vlastní objekty Zdroj: šablona ČSÚ, data vlastní

Při montáži jsme narazili na fakt, že Policií využívaný systém Pegas pracuje v pásmu 400MHz, tudíž je nutné dodržet distanční vzdálenost antén. V případě montáže na stožáry s buňkami systému Pegas jsme museli také požádat Zařízení služeb ministerstva vnitra o svolení, umístit zde technologie RIPEX. Montáž na vlastních objektech komplikovala také změť antén, většinou od starých nefunkčních technologií.

Síť RIPEX je nativně IP síť, kterou je nutné routovat. Právě routováním s funkcí záložních tras bude dosaženo již popisovaného požadavku zálohovaného spojení. Komunikace je zajišťována šifrováním na několika úrovních a její maximální přenosová rychlost, při šířce kanálu 25 kHz, je 55,56 kbit/s. Pro celý region je stanovena pouze jedna frekvence, což přináší výhody při minimalizaci počtu RETRů, které jsou společné pro celý kraj, nikoliv pouze pro okres, jako tomu je u původního systému.

Software LATIS 3 byl ve středočeském kraji nainstalován na KOTEC IOS (konsolidované technologické centrum), ve vytvořeném testovacím prostředí. Umístěním přímo na IOS odstraňujeme rizika výpadků spojení klientských stanic se serverem, které hrozí současnému systému. Instalace testovací verze LATIS byla provedena, abychom měli možnost systém dopředu projít

a seznámit se s ním. Také jsme měli možnost již vystavěné páteřní RETRy připojit a kontrolovat jejich stav. Instalace verze 19, ve které by měly být odladěny všechny podstatné chyby, je naplánovaná na konec června. Protože zároveň znamená přechod z původního systému, bude spojena se školením operačních důstojníků. IOS funguje na 4 směny. Plán je tedy v jednom týdnu uskutečnit školení i přechod, aby měla školená obsluha informace v živé paměti. V plánu původně nebylo školení techniků OTO, které jsme si vyžádali. Dohromady se tedy jedná o školení pro přibližně 130 lidí rozdělené do 5 dní. Databáze napojených objektů bude konvertována na nový systém.

Objekty připojované na DPPC budou připojovány prostřednictvím zařízení označovaného jako PZR-1. Jedná se o sestavu rádia RIPEX, modulu PZL10 a zdroje se zálohou. PZR-1 dokáže spojit již jakýkoliv PZTS s DPPC. Vlastní objekty tak budou připojené dvěma přenosovými kanály - rádio a intranet. Ostatní objekty budou připojené kanálem rádio a záložní trasou, kterou může být internet nebo telefonní linka.

Podoba sestavy určená pro zabezpečovací opatření, využívané SKPV pro předcházení a odhalování trestné činnosti, nebyla ve smlouvě dopředu popsána. Na poradách k modernizaci jsem se k tématice několikrát dotazoval. Vždy mi bylo odpovězeno, že není čas se podobou sestavy zabývat. Ze zkušeností s dodavatelem a vývojem jeho produktů mi bylo jasné, že je potřeba začít řešit toto téma dopředu. Nabídl jsem se, že vypracuji požadavky pro vytvoření této sestavy. Většina požadavků vychází ze samotného principu užití zabezpečovacího opatření, které je na omezenou dobu. Probral jsem možnosti s krajskými i mimo-krajskými kolegy. Výsledek vypadal následovně.

Zabezpečovací opatření, dříve označované jako **nástraha,** je využíváno jako PZTS malého až středního rozsahu pro krátkodobé nasazení s minimálními

změnami v prostředí (bourání, vrtání, lepení,...). Po demontáži se prostředí uvádí do původního stavu. U PZTS se striktně zamezuje jakékoliv vizuální či zvukové signalizaci. Tichý poplach je odesílán na DPPC, přičemž zasahující hlídky mají dle nařízení při příjezdu vypnout výstražné zvukové a rozhlasové zařízení (VRZ). Hlavním účelem je pachatele zadržet na místě.

Obrázek 24 Sestava Zabezpečovací opatření

1. **Objektové zařízení**
   1.1. Zdroj - zálohovaný na 230V pro provoz při výpadku el. energie s akumulátorem 7Ah;
   1.2. Ústředna
      1.2.1. 4 drátové smyčky s vyvážením (zpožděná, okamžitá, 24 hodin, ovládací ZAP/VYP);
      1.2.2. připojení klávesnice pro max. 8 uživatelů;
      1.2.3. připojení vypínače nebo autonomní klávesnice s reléovým výstupem;
      1.2.4. přijímač pro 8 bezdrátových prvků (detektory, univerzální vysílače, klíčenky ZAP/VYP);
   1.3. Vhodný obal - velký důraz na minimalizaci rozměrů. Odolný a vhodný pro časté přenášení. Dobrým příkladem jsou kufry od firmy PELI.

2. **Detektory**
   2.1. Drátové - možnost použití jakéhokoliv detektoru;
   2.2. Bezdrátové - PIR, duální detektor PIR/MW, magnetický kontakt, univerzální vysílač.
3. **Ovládání** - klávesnice drátová/bezdrátová, vypínač, autonomní klávesnice s reléovým výstupem.
4. **Anténa** - menší rozměry, slabý kabel, vše do černých, případně tmavých barev.

Prototyp sestavy splňující všechna kritéria je nyní testován v regionu Praha. Pokud bude funkční a metodické pracoviště jej schválí, bude nutné vytvořit dodatek ke smlouvě, abychom z přidělených financí mohly sestavy pořídit.

5.5 SWOT analýza modernizovaného systému SCO

Tabulka 6 SWOT analýza modernizovaného systému

Vnitřní původ	**Silné stránky** ➢ jedna frekvence pro celý kraj; ➢ systém zálohovaných tras; ➢ rychlost přenosu dat; ➢ připojení nových technologií k DPPC; ➢ přibližně 80% pokrytí kraje;	**Slabé stránky** ➢ šíření signálu v pásmu 400 MHz; ➢ legislativa; ➢ souběh s technologií Pegas;
Vnější původ	**Příležitosti** ➢ připojování více objektů; ➢ zkvalitňování SCO;	**Hrozby** ➢ napadení IP technologie sítě; ➢ závislost na technologii KOTEC IOS;

V rámci hodnocení opět stanovím stupnici 1 až 5 pro silné stránky a příležitosti (5 - nejvyšší spokojenost). Slabé stránky a hrozby stanovím dle stupnice -1 až -5 (-5 pro nejvyšší nespokojenost).

Tabulka 7 SWOT analýza modernizovaného systému - hodnocení

silné stránky	**váha**	**hodnocení**	**součin**
jedna frekvence pro celý kraj	0,25	5	1,25
systém zálohovaných tras	0,25	5	1,25
rychlost přenosu dat	0,2	5	1
připojení nových technologií k DPPC	0,1	3	0,3
přibližně 80% pokrytí kraje;	0,2	4	0,8
		součet:	4,6

slabé stránky	**váha**	**hodnocení**	**součin**
šíření signálu v pásmu 400 MHz	0,4	-4	-1,6
legislativa	0,3	-3	-0,9
souběh s technologií Pegas	0,3	-2	-0,6
		součet:	-3,1

příležitosti	**váha**	**hodnocení**	**součin**
připojování více objektů	0,4	3	1,2
zkvalitňování SCO	0,6	5	3
		součet:	4,2

hrozby	**váha**	**hodnocení**	**součin**
napadení IP technologie sítě	0,5	-3	-1,5
závislost na technologii KOTEC IOS	0,5	-4	-2
		součet:	-3,5

Tabulka 8 SWOT analýza modernizovaného systému - součet

Vnitřní část	1,5
Vnější část	0,7
Součet	2,2

Analýza nového SCO ukazuje na jednoznačné zlepšení. Systém má mnoho silných stránek, které budou dlouhodobě stálé. Také nevykazuje větší množství slabých stránek. Slabina v podobě legislativních podmínek bude napravena

v nejbližší době, jelikož o návrhu nových závazných pokynů k provozu SCO již probíhají jednání. Zajištění jeho dodržování je otázkou lidského faktoru a důslednosti v kontrolách, jak metodickým pracovištěm, tak strukturou nadřízených. Souběh s technologií Pegas je při problémech řešen dutinovými filtry. Toto téma se týká pouze momentální stavby páteře a připojování vlastních objektů. Ostatní objekty se s touto problematikou nesetkají. Horší šíření ve vyšším frekvenčním pásmu bylo vyřešeno stavbou vlastních objektů s venkovní anténou, která je užívána pro páteřní síť. Dosáhneme tak minimálně původního pokrytí.

6 DISKUZE

Ačkoliv je v normách pojem **Systém centralizované ochrany** nepodchycený, existuje již dlouhou řadu let a je velmi rozšířený jak ve státní, tak civilní sféře. Jiné pojmy v oblasti zabezpečení zaznamenaly značné proměny. Zkratku EZS pro elektronické zabezpečovací systémy normy neznají od začátku roku 2010 a byla nahrazena zkratkou PZTS (v angličtině I&HAS). I přesto většina lidí z oboru nemluví o ničem jiném, než o EZSce, což se v nejbližší době jen tak nezmění.

O novelizovaném souboru norem se vedou dlouhé diskuze. Osobně se přikláním k názoru, že jsou normy nesourodé. Špatně se v nich orientuje, jednotlivé názvy jsou jednou používané česky, podruhé zas anglicky. Informace se v nich několikrát zbytečně opakují.

Systém centralizované ochrany vznikal jako prostředek k ochraně objektů před majetkovou trestnou činností. Při pohledu na statistiky majetkových trestných činů, především krádeží vloupáním, je naprosto zřejmé, že se jednalo o krok správným směrem. A to jak z hlediska rozvoje Policie ČR, která má hlavní odpovědnost za tuto problematiku, tak z hlediska rozvoje v soukromých bezpečnostních službách. Rozvoj v soukromém sektoru umožnil nejen větší počet zabezpečených objektů, ale ovlivnil také kvalitu zabezpečení. Policie ČR má tak možnost z větší části řešit zabezpečení pouze strategicky důležitých a jiných zájmových objektů.

Trend snižování majetkové trestné činnosti ovšem nemusí být trvalý. Vezmeme-li v úvahu aktuální politickou situaci v ČR i ve světě nebo problémy představující vlny migrace, může se situace s nápadem trestné činnosti rychle změnit. Současné vytváření velkého počtu pracovních příležitostí zahraničními firmami, které není možné pokrýt místními obyvateli, lákají pracovní sílu

především z východu. Nejen z těchto důvodů je třeba oblasti zabezpečení věnovat další pozornost a dále ji rozvíjet v trendu moderních technologií.

Mnoho diskutované je téma integrace v oblasti bezpečnostních technologií. Podíváme-li se na integraci operačních středisek, jsou zde na první pohled vidět jasné výhody z hlediska toku informací a operačního řízení. Vedoucí směny IOS má naprostý přehled o situaci v celém kraji. Vytvořit ucelený soubor informací z jednotlivých okresních operačních středisek dříve trvalo příliš dlouho. Stejně tak je dnes možné lépe řídit jednotlivé hlídky z jednoho místa a poslat je i na výpomoc sousednímu okresu. Do systému JITKA, ve které se vede operační řízení, jsou integrovány všechny potřebné informace. Rozvoj tohoto systému trochu stagnoval, nicméně se již jedná o jeho dalším rozvoji. V současné době lze do systému JITKA přenést jednosměrně balík informací v případě vzniku události. Informace obsahují název objektu, včetně čísla a podrobnou adresu s GSP souřadnicemi. Operační neradi obsluhují více systémů najednou a proto nás zahrnují dotazy, zda by nešlo přeposlat událost z SCO automaticky a odbavit ji již v JITCE. K tomuto se metodické řízení pro IOS vyjádřilo s rozhodnutím, že JITKA není určena pro SCO. SCO musí fungovat jako samostatný systém. Informace jsou přeposílány do JITKY jen z důvodu povinnosti zapisovat úkony operačního řízení. Tak nemusí operační důstojník přepisovat událost ručně. Z toho tématu vznikla jedna podnětná záležitost. Ačkoliv jsou přeposílány GPS souřadnice, objekt se v mapě systému JITKA neobjeví. Vzhledem k tomu, že hlídky řídí operátor na této mapě, bylo by při navigaci hlídek na místo vhodné, vidět tento objekt také v mapě JITKA.

Integrace ovšem v případě operačního řízení přináší i své nevýhody. Práce v IOS je velice náročná, což klade velké nároky na operační důstojníky. Na sále bývá velice rušno, proto byly jednotlivé stoly v roce 2018 doplněny o protihlukové zástěny, které přinesly malé zlepšení. Celý sál IOS by si zasloužil

akustickou studii a lepší řešení tlumení hluku. Při střídání na různých sektorech nemají operační důstojníci takový přehled, jako měli na okresech díky velkým místním znalostem. Místní znalost nemohou nahradit i sebelepší mapové podklady, i když jsou v dnešní době velice přesné.

Integraci v oblasti zabezpečovacích technologií korigují normy a legislativa. Jde o striktní rozdělení systémů jako jsou EPS, PZTS, CCTV a další. Z pohledu uživatelů jde v integraci zejména o zjednodušení prostředí a jeho ovládání. Ideálem je jeden systém, který bude umět vše. Výrobci ústředen PZTS jdou touto cestou, když integrují další záležitosti, jako například řízení topení, okenních rolet a podobně. Dělají tak své produkty pro cílového zákazníka atraktivní.

Z pohledu technologie jde hlavně o spolehlivost. Pokud máme více systémů zabezpečení jako PZTS a CCTV, snižujeme riziko překonání obou systémů zároveň nebo jejich selhání. V případě jednoho integrovaného systému můžeme při poruše přijít jak o zabezpečení detektory, tak o přehled z kamer. Tyto důvody jednoznačně mluví proti integraci. Pokud jde tedy o zabezpečovací systémy, držel bych se striktního rozdělení. Podíváme-li se na integraci funkcí do PZTS, jako zmíněné ovládání topení nebo rolet, jsou zřejmá hlavně pozitiva. Samozřejmě za předpokladu, že selhání podružných systémů neovlivní ten zabezpečovací. V praxi se tento problém zpravidla neobjevuje, protože se jedná většinou o reléové výstupy nebo komunikaci ústředny PZTS s ústřednou pro topení po sériové lince. Integrace má tedy smysl, ovšem za určitých podmínek. Jedná se o dlouhý proces pokusů a omylů, než dojdeme ideálního řešení řízení. Tento proces je o to složitější, o co je rychlejší vývoj informačních technologií.

Systém centralizované ochrany vznikl na základě majetkové trestné činnosti, tedy ochrany objektů před napadením. K tomuto se postupně přidává ochrana

před vnějšími vlivy v podobě detekce požáru, zaplavení nebo úniku plynu. Komerční DPPC poskytují další služby v podobě monitorování CCTV systémů, pohybu vozidel (například při přepravě hotovosti, cenin, nebezpečného materiálu atd.). Monitorováním vozidel je v současné době také možné vytvářet knihy jízd. Toto se všechno týká majetku. V poslední době se ovšem začíná cílit i na oblast zajištění osob. U osob se jedná buď o násilnou trestnou činnost nebo pomoc seniorům či zdravotně tělesně postiženým. Typ zabezpečení je ovšem stejný. Jedná se o zařízení či aplikaci v mobilním telefonu, pomocí které si osoba přivolá pomoc. Tato oblast je poměrně hodně v začátcích. Současná zařízení mají svá omezení, hlavně co se týká výdrže akumulátoru a pak přesnosti zaměření dle GPS. Přináší tak v ochraně života a zdraví nástroj k podstatnému zrychlení poskytnutí pomoci a zjištění informací o osobách, které jsou již předem zaneseny v DPPC. Operátor tak může posádce na místě sdělit zásadní informace pro úspěšný zásah. V případě zdravotnické záchranné služby to mohou být užívané medikamenty, či zdravotní stav. Pro policii při zásahu u domácího násilí to budou informace ohledně vykázané osoby, například zda vlastní zbraň nebo je uživatelem OPL. V dnešní uspěchané době, kdy se lidé ženou za výdělkem a nemají čas starat se o své bližní, bude tato služby stále žádanější.

SCO Policie ČR má za sebou historii dlouhou půl století. Myšlenka přijatá v Čechách na základě zahraničních zkušeností se ukázala jako nákladná, ale přínosná. Starý SCO KŘP Středočeského kraje, který bude kompletně ukončen do konce roku 2020, prošel během 30 let nemalým vývojem. Přesto většina základních částí, jako přenosové sítě a koncová zařízení, vydržela úctyhodných 30 let. S tímto dlouholetým odstupem lze říci, že ačkoliv začátky systému provázely značné problémy, dlouhodobě se vyplatil.

Analýza však ukazuje jeho dnešní nedostatky. Starší prvky systému vyžadují čím dál častější údržbu. Nedostatečná reakce na změny v IOS je příčinou výpadků spojení s objekty v celém okrese kvůli absenci záložní trasy. Stagnující legislativa zabraňuje jakékoliv iniciativě ve vývoji mimo stanovené technologie. Toto vše je důsledek absence metodického pracoviště. Pokus o řešení nastal v podobě technologie MORSE. Projekt nebyl centrálně podpořen hlavně z finanční stránky, a tak došlo k roztříštění jednoty technologií mezi jednotlivými územními odbory. K dokončení v celé Policii ČR se celých 14 let finanční prostředky nenašly. Situace se začala řešit až po hrozbě ČTÚ pokutou. Tento extrém zapříčinil nedostatečnou přípravu projektu modernizace a zkomplikoval tak její průběh. Až když byla podepsána smlouva, byl stanoven tým pro podporu modernizace. Během stavby v testovacím regionu se konečně rozšířil tým, kterému je metodické řízení svěřeno. Na základě těchto zkušeností by bylo vhodné vytvořit opět samostatné pracoviště. Toto by se mohlo věnovat nejen metodické činnosti po stránce SCO, ale i podpoře SKPV policejního prezidia v poskytování zabezpečovacích opatření. Policejní prezidium se v současné době obrací na ÚZČ nebo na krajská pracoviště OTO.

Z analýzy současného systému vyplývají i zápory, které se přenesou na systém nový, protože se netýká hardwaru SCO, ale jeho řízení. Nedostatečná pravidelná školení obsluhy DPPC, nedodržování oznamovací povinnosti o kontaktních osobách ze strany civilních objektů i nedůsledná kontrola informací k objektům ze strany techniků OTO SKPV komplikují celý provoz SCO.

Projekt radiové sítě byl součástí veřejné zakázky na modernizaci, což považuji za nešťastné řešení, z již popsaných důvodů. Pro jakýkoliv obdobný projekt bych doporučil nejdříve zpracování projektové dokumentace, na které by měl zadavatel intenzivně spolupracovat, nikoliv však udávat stanoviště pro

RETRy. Dodavatel takového řešení by měl sám provést studii terénu a vybrat nejvhodnější stanoviště a konkrétní umístění i druh antén. To vše za účelem dosažení perfektního pokrytí s minimalizovanými náklady na stavbu i následný pronájem stanovišť. S takto dobře zpracovaným projektem lze dále přesněji stanovit podmínky veřejné zakázky na konkrétní řešení.

V rámci modernizace ve středočeském kraji se podařilo snížit počet pronajímaných stanovišť z 58 pro původní technologii na 29 pro technologii RIPEX. Teoreticky by to mělo znamenat úsporu 50% z nájemného, po skončení staré technologie. Skutečná úspora bude ovšem jen zhruba 40%. Může za to jednání o dodatcích k nájemním smlouvám. Při žádání o souběh technologií na jednotlivých stanovištích, bylo KŘP Stč kraje navýšeno nájemné za přidané technologie, které se samozřejmě po demontáži již na původní částku nevrátí.

Z hlediska zkušeností s nasazováním nového softwaru pro DPPC byla zvolena cesta testování ve vybraném regionu. Z současné situace byl naprosto správně zvolen region Praha, který má všechny výhody pro hladké nasazení. Ani tak se proces neobešel bez problémů. Pokud by se s modernizací nemuselo tolik pospíchat kvůli ultimátu ke staré technologii, navrhl bych zcela jinou strategii. Pomineme-li záložní trasy, je rádiová síť v každém kraji stavěna jako pyramida. Vrchol pyramidy je vždy umístěn na DPPC příslušného kraje a tedy i na síti intranet respektive na VLAN VRF SCO. Stavba sítě by měla za předpokladu dobré přípravy probíhat od vrcholu pyramidy směrem dolů. Takto by byla zajištěna návaznost a zároveň připojení na DPPC. Testovací DPPC bych umístil na metodickém pracovišti, kde by bylo možné systém otestovat. RETRy jsou zároveň objekty. Ty by zajišťovaly generování potřebných dat. Stavba nových RETRů by umožnila testování úkonů spojených s připojováním nových objektů na DPPC. Protože je intranet Policie ČR propojený napříč republikou, mohl by systém monitorovat objekty ze všech krajů. Připojování na

centrální pracoviště by také přineslo přehled o postupu stavby, který nebyl vždy dobře znám.

Pro hlášení problémů či chyb týkajících se modernizace byl popsán jednotný standardizovaný postup. Systém Helpdesk firmy Trade Fides a.s. byl stanoven jako výhradní komunikační kanál pro hlášení závad. Ten byl následně zpřístupněn všem krajům. Někteří technici jej již znali v souvislosti s poskytování podpory pro systém LATIS SQL a ústředny ASSET. Všichni mají možnost sledovat založené události a jejich řešení. Tento postup měl zamezit zdvojování hlášení. Myšlenka byla určitě správná, bohužel velký počet hlášených nedostatků z počátku způsobil trochu chaos a dodavateli trvalo dlouhou dobu, než všechny události zpracoval.

Instalace systémů na testovací prostředí pro jednotlivé kraje hodnotím velice kladně. Mohli jsme již vystavěné RETRy připojit na testovací DPPC a začít tak naše seznamování se systémem, který jsme po ostrém nasazení systému měli perfektně znát a ovládat. Díky tomu jsem získal cenné zkušenosti, které jsem si potvrdil a upřesnil na následném školení pro administrátory systému LATIS 3 od dodavatele.

Školení na LATIS 3 bylo třeba udělat pro 2 až 4 techniky na kraj. Celkem se jednalo o zhruba 50 lidí. Na základě dohody o tom, že školení může proběhnout pro skupinu o maximálním počtu 10 lidí, bylo stanoveno pět skupin a pět termínů. Dvoudenní školení probíhalo formou teorie a praxe, se závěrečným testem a vydáním certifikátu administrátora systému. Teoretická část obsahovala dostačující informace k provozu a údržbě systému. Od praktické části jsme čekali zaměření na ovládání prostředí, jeho přizpůsobení potřebám IOS, zakládání objektů a vkládání informací k nim. Účastnil jsem se prvního školení, při kterém se praktická část převážně

zabývala tvorbou grafického projektu pro objekt (půdorysy, umístění značek a podobně). Po upozornění na tento nedostatek byl pro ostatní termíny koncept pozměněn.

Školení k sytému RIPEX jsme požadovali od výrobce, tedy od firmy RACOM a.s.. Náš požadavek byl nakonec schválen. Tvůrcem konceptu sítě, její adresace, směrování a kompletního vzoru konfigurací pro různé druhy objektů (RETRy, civilní, technické, vlastní objekty) je technik z metodického pracoviště policejního prezidia. Proto také část školení prováděl. Stejně tak vypracoval k problematice obsáhlý manuál.

Ve Středočeském kraji jsme v roce 2018 čekali na instrukce k výstavbě páteřní sítě. Ztratili jsme tak téměř půl roku v domnění, že dodavatel pracuje na měření. Ve většině ostatních krajů již od února probíhali jednání o umístění technologií RIPEX. Po republikové poradě v červnu jsem dostal modernizaci ve Středočeském kraji na starost. Dohoda o stavbě RETRů na územních odborech nám umožnila nasazení vlastních prostředků. Ztracený čas jsme tak dohnali a ještě jsme při tom ušetřili finanční prostředky vynaložené na montáž. I přesto se nám nepodařilo páteř v roce 2018 dostavět. Jednání o umístění v lokalitách kde je vlastníkem O2 jsou příliš zdlouhavá. Ačkoliv požadují přesné zakreslení námi instalovaných technologií, vlastní technologie již umístěné na stožárech zakreslené nemají. Montáž prvního ze čtyř stanovišť je povolena teprve začátkem května 2019. Další by měli následovat. Výhled kompletní dostavby je zhruba začátkem července 2019. Do konce roku 2019 bychom mohli síť kompletně otestovat a umožnit připojení objektům na DPPC přes novou technologii RIPEX. Během roku 2020, kromě připojování objektů, musíme připravit vypnutí staré technologie. Po zkušenostech s montáží očekávám stejně náročnou demontáž. Jedná se o dvojnásobek stanovišť

a opětovné řešení nájemních smluv. Výhled dokončení demontáže je tedy koncem roku 2022.

Analýza nového systému v silných stránkách, přímo ukazuje zlepšení oproti tomu starému. Přináší tři důležité klady, kterými jsou: zálohované trasy, jedna frekvence pro celý kraj a rychlost přenosu dat. Zálohované trasy jsou důležitým faktorem bezpečnosti přenosu. Kromě toho, že se nebudeme potýkat s výpadky, dostojíme tak i normativním a legislativním požadavkům. Jedna frekvence pro celý kraj znamená retranslační body využívané všemi územními odbory naráz. Z toho vyplývá již zmíněná úspora financí. Znamená to ale i výpomoc mezi územními odbory v zabezpečovacích opatřeních. Například kolegové z Mělníka mohu nasadit zabezpečovací opatření v jiném územním odboru, aniž by to místní technici věděli. Toto poskytuje výhodu vynechat konkrétní techniky, kteří mohou být v řešeném případu zainteresováni, či znát některé dotčené osoby. Rychlost přenosu dat zkrácená z půl minuty na pouhou vteřinu přispívá k bezpečnosti, rychlosti zásahu a v konečném důsledku k odstranění hrozícího nebezpečí.

V slabých stránkách zaslouží největší pozornost legislativa, na které se v současné době pracuje. Policie ČR poskytuje možnost připojení na DPPC určitým objektům, které jsou pod smlouvami s PČR nebo MV, a to zcela zdarma. Například Slovensko poskytuje tyto služby za poplatek. Protože modernizace stála mnoho finančních prostředků a služba poskytovaná Policií ČR je nejprofesionálnější v ČR, stálo by za úvahu některým objektům službu zpoplatnit. Pásmo 400 MHz je stanoveno ČTÚ a je neměnné. Nevýhoda oproti pásmu 160 MHz spočívá v takzvaném "horším ohýbání", což způsobuje horší vertikální šíření. Nedostatky ukáže až podrobné měření a praxe. Problémy se mohou týkat hlavně velkých převýšení v okolí vodních toků, jako jsou Slapy a Orlík, nebo hornatého terénu na Rakovnicku a Berounsku. Souběh

s technologií Pegas, která se nachází ve stejném frekvenčním pásmu, znamená slabinu pouze ve fázi stavby sítě a jejího ladění. Je však otázkou, co bude se sítí Pegas dál. Hovoří se o jejím skončení či modernizaci. Ta by mohla negativně ovlivnit síť RIPEX. Případnou modernizaci či změny v technologii je třeba vést v patrnosti, abychom se vyhnuli vzájemnému ovlivňování, a tím způsobených problémů.

Příležitosti SCO spočívají v připojování významných rizikových objektů, a tím zkvalitňují bezpečnostní situaci v celé ČR. Navyšování celkového počtu objektů napojených na DPPC Polici ČR by mohlo přinést vývoj pracovišť integrovaných operačních středisek. Modely na řízení DPPC se napříč republikou různí. Aby bylo celé řízení zkvalitněno, musí dojít k jeho sjednocení a stanovení nejlepšího řešení. Školení pro operační důstojníky sloužící v identických systémech bude možné zlepšit.

Hrozby pro systém a jeho nepřetržitou funkčnost souvisí s informačními technologiemi. Radiová síť je postavena na IP technologii, která je mnohem více známa lidem, kteří by ji mohli chtít napadnout, ovládnout či poškodit. Software DPPC je závislý na informačních technologií, takže je jen tak robustní, jak je robustní software a hardware na kterém běží.

S budováním moderních technologií si na nich vytváříme více či méně závislost. Chytré technologie spojované internetem najdeme dnes naprosto všude. Je proto nutné ve vývoji, obzvláště při integraci systémů, upínat pozornost k co největší robustnosti a zabezpečení. Pád jednoho obrovského systému, mající pod kontrolou různé oblasti řízení, by jednou mohl mít katastrofální následky v oblasti ochrany života a zdraví osob.

7 ZÁVĚR

Hodnocení stavu před modernizací jasně ukazuje nutnost systém modernizovat. Ačkoliv fungoval dlouhých 30 let, je u konce své životnosti. Za tento krajní stav nese zodpovědnost absence metodického pracoviště s týmem alespoň o šesti členech.

Příprava modernizace a veřejná zakázka nebyly provedeny dost detailně a nepostihly plně všechny požadavky pro perfektní SCO. Bylo nutné smlouvu upravovat dodatky, což je ve státním sektoru problematické. Za tímto opět stojí absence metodického pracoviště.

Po zkušenostech přechodu LATIS na LATIS SQL byl naprosto správně zvolen testovací region. V případě existence metodického pracoviště, by bylo vhodnější otestovat DPPC zde, nikoliv na živém DPPC.

Zájmové oblasti byly stanoveny složením rizikových oblastí dle trestné činnosti a zkušeností kolegů s jejich regiony. Tyto oblasti byly při výběru stanovišť pro retranslátory dle matematického modelu pokryty signálem nové přenosové sítě. Při měření vyšlo najevo, že skutečné pokrytí neodpovídá matematickému modelu. Bude proto nutné zájmové oblasti detailněji změřit.

První hypotéza o zmenšení počtu retranslačních stanic, a tím uspoření financí na pronájem, se naprosto potvrdila.

Druhou hypotézu lze také potvrdit. V rámci testů a zkušeností z testovacího regionu můžu říci, že rychlost přenosu dat je oproti starému systému až třicetinásobná. Systém zálohovaných tras je také funkční, jen bude chtít příslušné ladění na živém souboru objektů.

8 SEZNAM POUŽITÝCH ZKRATEK

ATE - alarm transmission equipment (poplachové přenosové zařízení)

ATS - alarm transmission system (poplachový přenosový systém)

BE - Beroun

BIS - Bezpečnostní informační služba

BN - Benešov

ČNB - Česká národní banka

ČRa - České radiokomunikace

ČSÚ - Český statistický úřad

ČTÚ - Český telekomunikační úřad

DPPC - Dohledové poplachové přijímací centrum

ESSK - Evidenčně statistický systém kriminality

HZS - Hasičský záchranný sbor

IOS - integrované operační středisko

I&HAS - intrusion and hold-up alarm system

JTS - jednotná telefonní síť

KH - Kutná hora

KL - Kladno

KO - Kolín

KOTEC - konsolidované technologické centrum

KŘP - Krajské ředitelství Policie

KŘPS - Krajské ředitelství Policie Středočeského kraje

LTV - linka tísňového volání

MB - Mladá Boleslav

ME - Mělník

MV - Ministerstvo vnitra

NB - Nymburk

OPL - omamné psychotropní látky

OSZ - Okresní státní zastupitelství

OTO - Odbor technické ochrany

OZ - objektové zařízení

PB - Příbram

PCO - pult centralizované ochrany

PP - policejní prezidium

PVJ - Praha venkov jih

PVV - Praha venkov východ

PVZ - Praha venkov západ

PZTS - Poplachový zabezpečovací a tísňový systém

RA - Rakovník

ŘSD - Ředitelství silnic a dálnic

SCO - systém centralizované ochrany

SKPV - Služba kriminální policie a vyšetřování

ÚO - územní odbor

ZPPP - závazný pokyn policejního prezidenta

9 SEZNAM POUŽITÉ LITERATURY

1. **Policie České republiky.** *ZPPP č. 115/2009 o výstavbě a provozu systémů centralizované ochrany.* Praha : Policejní prezidium Policie České republiky, 2009.

2. **ČSN EN 50518-1 ED.2.** *Dohledová a poplachová přijímací centra - Část 1: Umístění a konstrukční požadavky.* Praha : Český normalizační institut, 2014.

3. **ČSN EN 50131-1 ED.2.** *Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 1: Systémové požadavky.* Praha : Český normalizační institut, 2007.

4. **Uhlář, Jan.** *Technická ochrana objektů II. díl Elektrické zabezpečovací systémy II 2. vydání.* Praha : Policejní akademie České republiky v Praze, 2009. ISBN 978-80-7251-313-0.

5. **Fides spol. s.r.o.** *FAUTOR II Návod k obsluze elektronického zabezpečovacího systému.* Brno : Fides spol. s.r.o., 1995.

6. **Fides spol. s.r.o**. *FAUTOR II Návod k obsluze objektového zařízení FA101a, b.* Brno : Fides spol. s.r.o., 1995.

7. **Trade Fides.** *LATIS Návod k obsluze programu SERVER.* Brno : Trade Fides a.s., 2000.

8. **Trade Fides**. *LATIS Návod k obsluze programu KLIENT.* Brno : Trade Fides a.s., 2000.

9. **Policie České republiky.** *Pokyn č. 8/2010 ředitele centrály informatiky a analytických procesů SKPV PP ČR kterým se upravuje postup příslušníků specializovaných pracovišť PČR při provozování SCO.* Praha : Policejní prezidium Policie České republiky, 2010.

10. *Zákon č. 273/2008 o Policii České republiky.* Praha : Česká republika, 2008.

11. **Lukáš, Luděk a kolektiv.** *Bezpečnostní technologie, systémy a management V.* Zlín : Radim Bačuvčík - VeRBuM, 2015. ISBN 978-80-87500-67-5.

12. **Říha, Milan, Sieger, Ladislav a Pikola, Pavel.** *Bezpečnostní systémy 2. díl.* Praha : TRIVIS, 2011. 978-80-87103-35-7.

13. **Říha, Milan a Sieger, Ladislav.** *Bezpečnostní systémy 1. díl.* Praha : TRIVIS, 2008. 978-80-87103-12-8.

14. **Kyncl, Jaromír a kolektiv.** *Bezpečnost objektu ve světle moderních technologií.* Praha : Komora podniků komerční bezpečnosti České republiky, 2014. 978-80-260-7115-0.

15. **Ivanka, Ján.** *Systemizace bezpečnostního průmyslu.* Zlín : Univerzita Tomáše Bati ve Zlíně, 2014. 978-80-7454-410-1 .

16. **Policie České republiky.** *ZPPP 16/2009 kterým se upravuje jednotný postup příslušníků Policie České republiky při vyžadování použití zabezpečovací techniky.* Praha : Policejní prezidium Policie České republiky, 2009.

17. **Policie České republiky**. *ZPPP 17/2009 kterým se upravuje postup specializovaných pracovišť při použití zabezpečovací techniky.* Praha : Policejní prezidium Policie České republiky, 2009.

18. **Policie České republiky**. *ROZKAZ PP 145 kterým se zřizuje pracovní skupina k zajištění realizace modernizace systému centralizované ochrany Policie České republiky* . Praha : Policejní prezidium Policie České republiky, 2017.

19. **ČSN EN 50136-1.** *Poplachové systémy - Polachové přenosové systémy a zařízení - Obecné požadavky na poplachové.* Praha : Český normalizační institut, 2012.

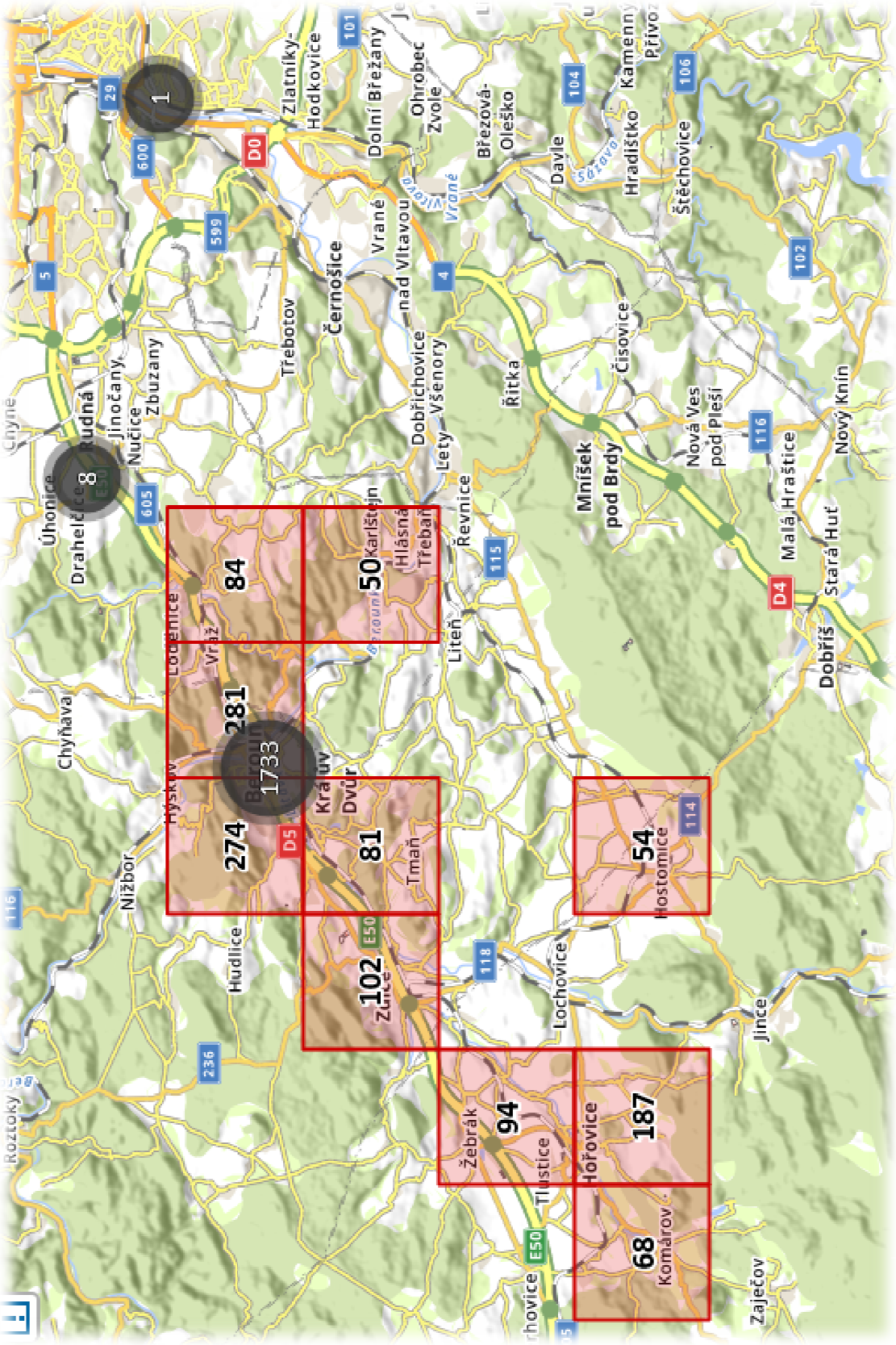
20. **ČSN EN 50518-1 ED.2.** *Dohledová a poplachová přijímací centra - Umístění a konstrukční požadavky.* Praha : Český normalizační institut, 2014.

21. **Ivanka, Ján.** *Systemizace bezpečnostního průmyslu II.* Zlín : Univerzita Tomáše Bati ve Zlíně, 2009. 978-80-7318-863-4.

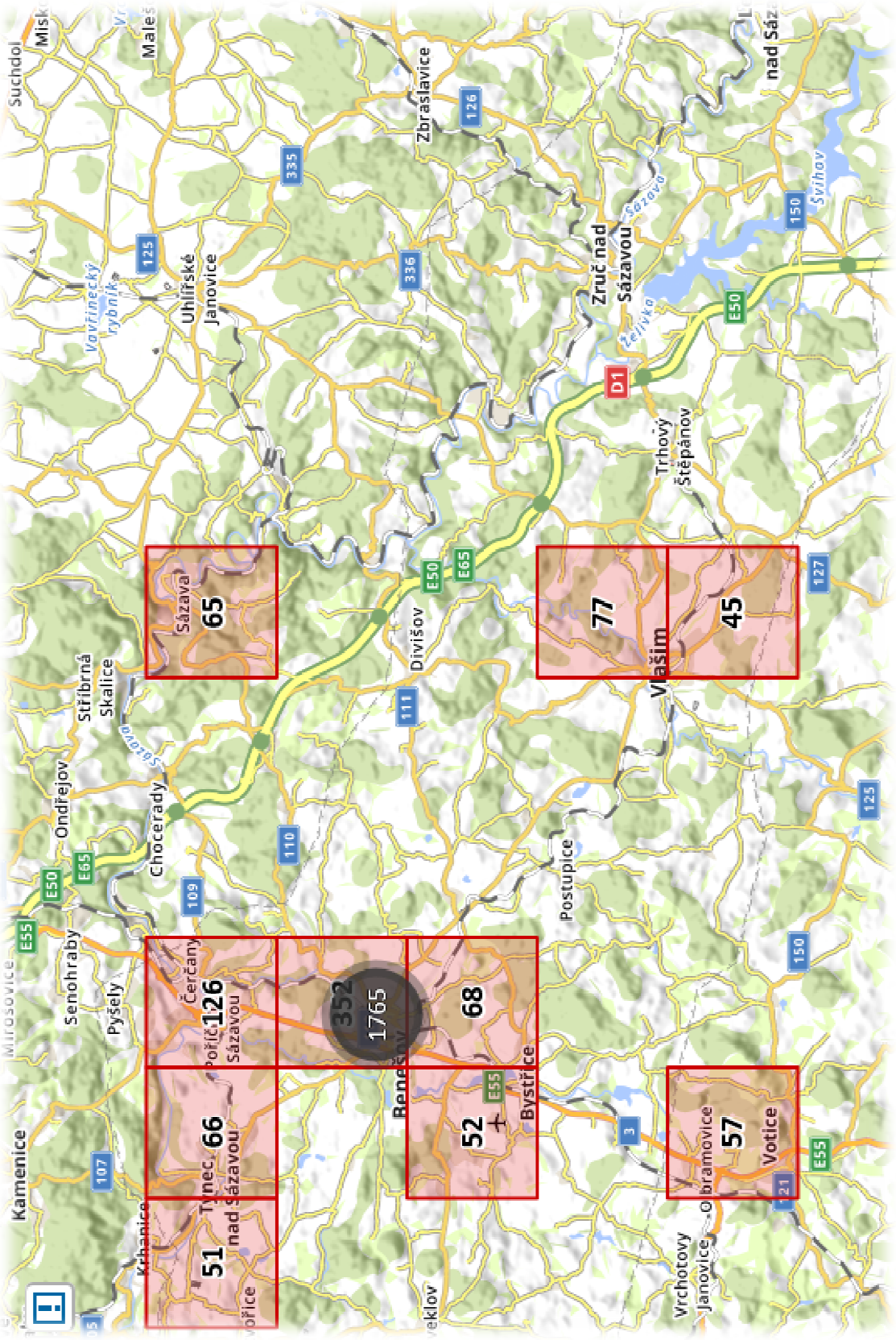
10 SEZNAM POUŽITÝCH OBRÁZKŮ

11 SEZNAMU POUŽITÝCH TABULEK

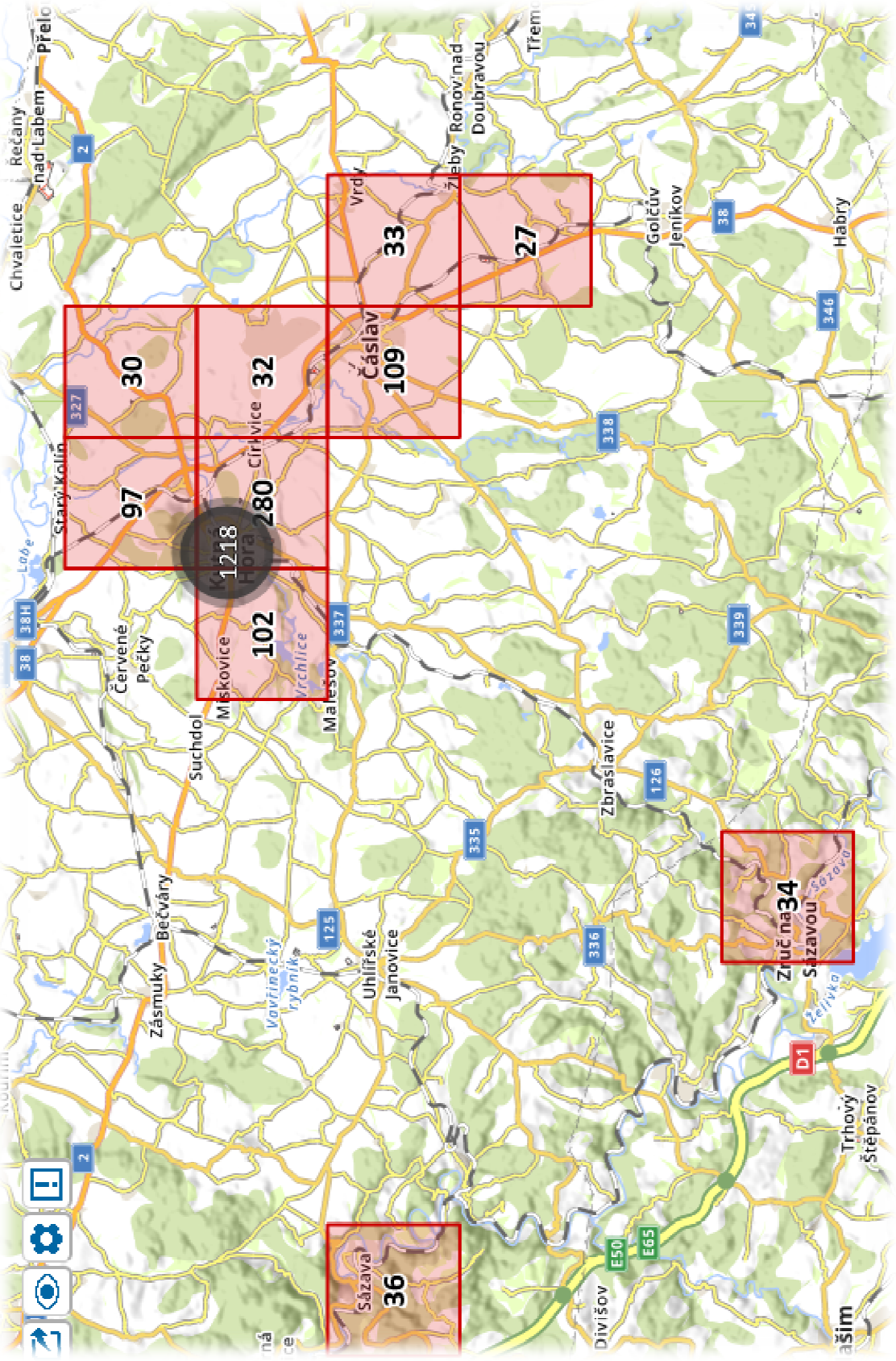
12 SEZNAM PŘÍLOH



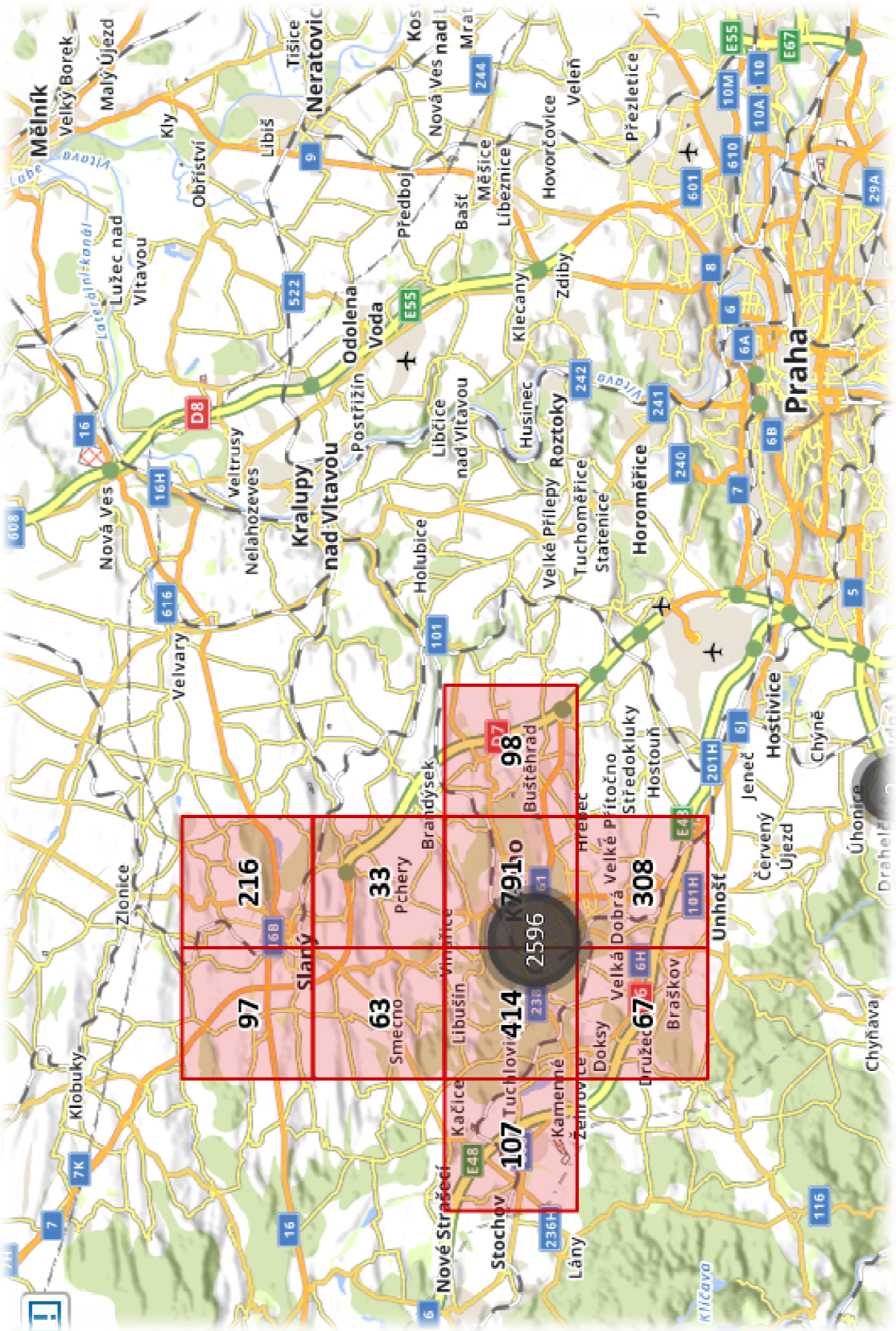
Příloha 1 Mapa rizikových oblastí TČ krádeže vloupáním - ÚO Beroun Zdroj: Mapa kriminality PČR



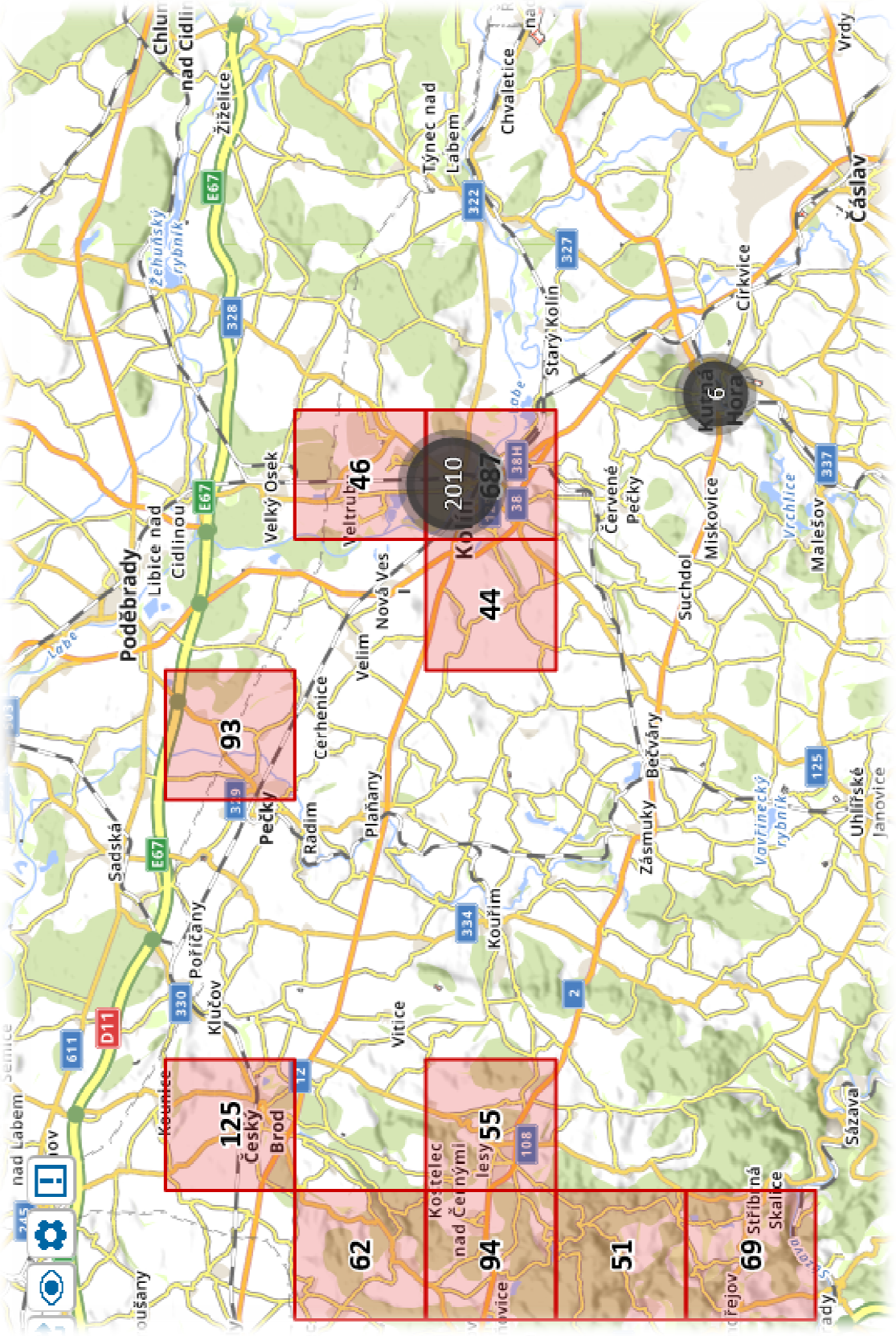
Příloha 2 Mapa rizikových oblastí TČ krádeže vloupáním - ÚO Benešov Zdroj: Mapa kriminality PČR



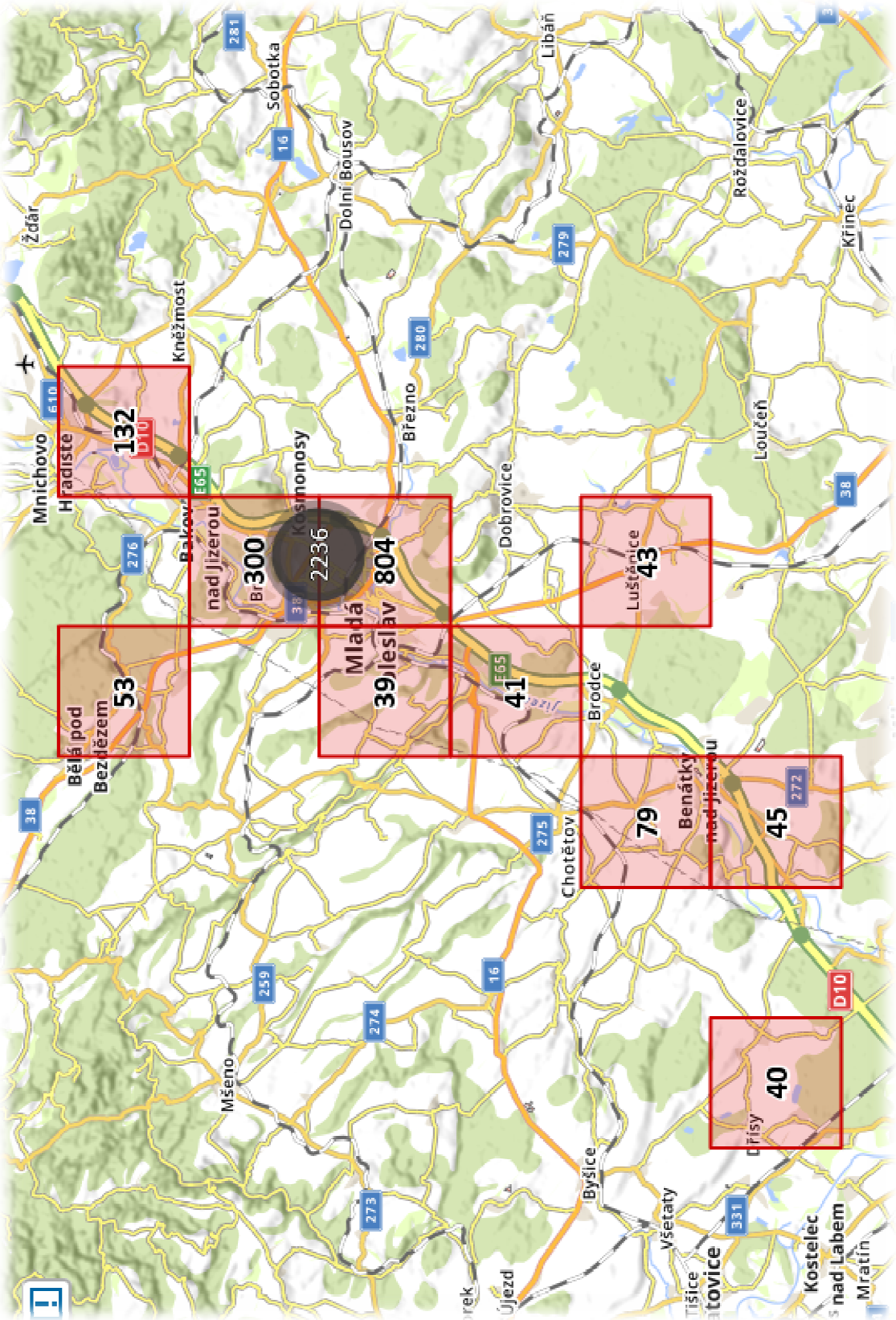
Příloha 3 Mapa rizikových oblastí TČ krádeže vloupáním - ÚO Kutná Hora Zdroj: Mapa kriminality PČR



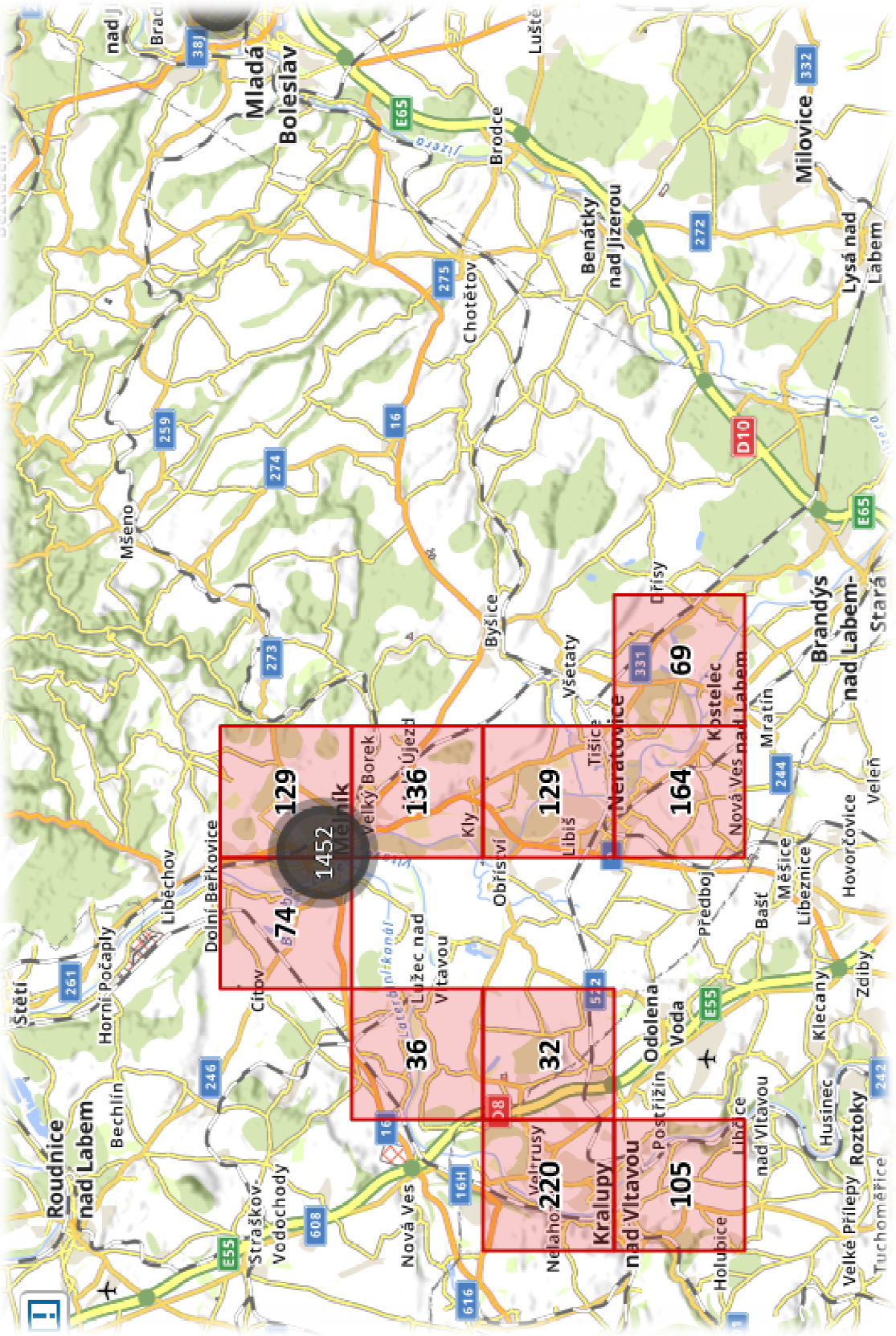
Příloha 4 Mapa rizikových oblastí TČ krádeže vloupáním - ÚO Kladno Zdroj: Mapa kriminality PČR



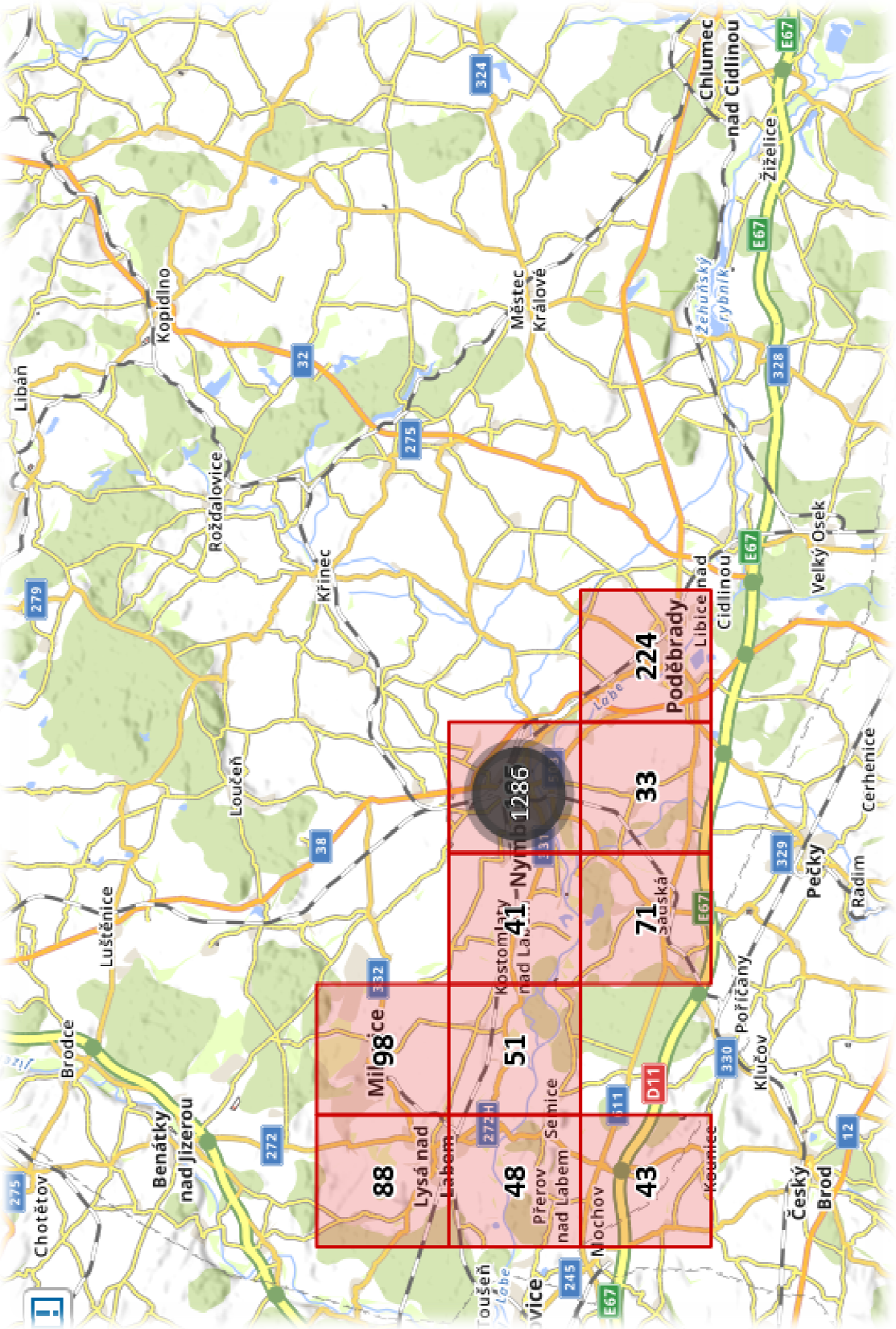
Příloha 5 Mapa rizikových oblastí TČ krádeže vloupáním - ÚO Kolín Zdroj: Mapa kriminality PČR



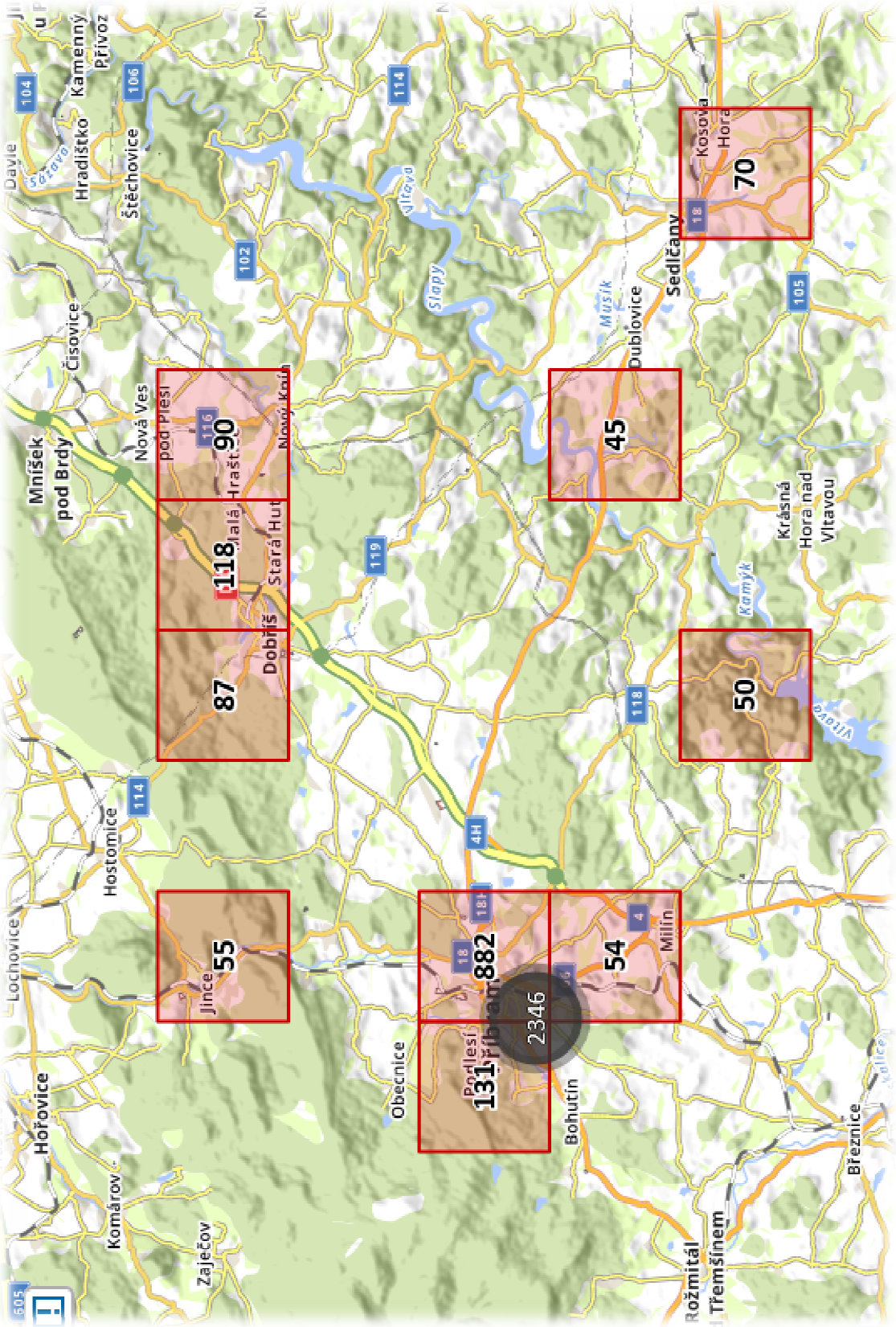
Příloha 6 Mapa rizikových oblastí TČ krádeže vloupáním - ÚO Mladá Boleslav Zdroj: Mapa kriminality PČR



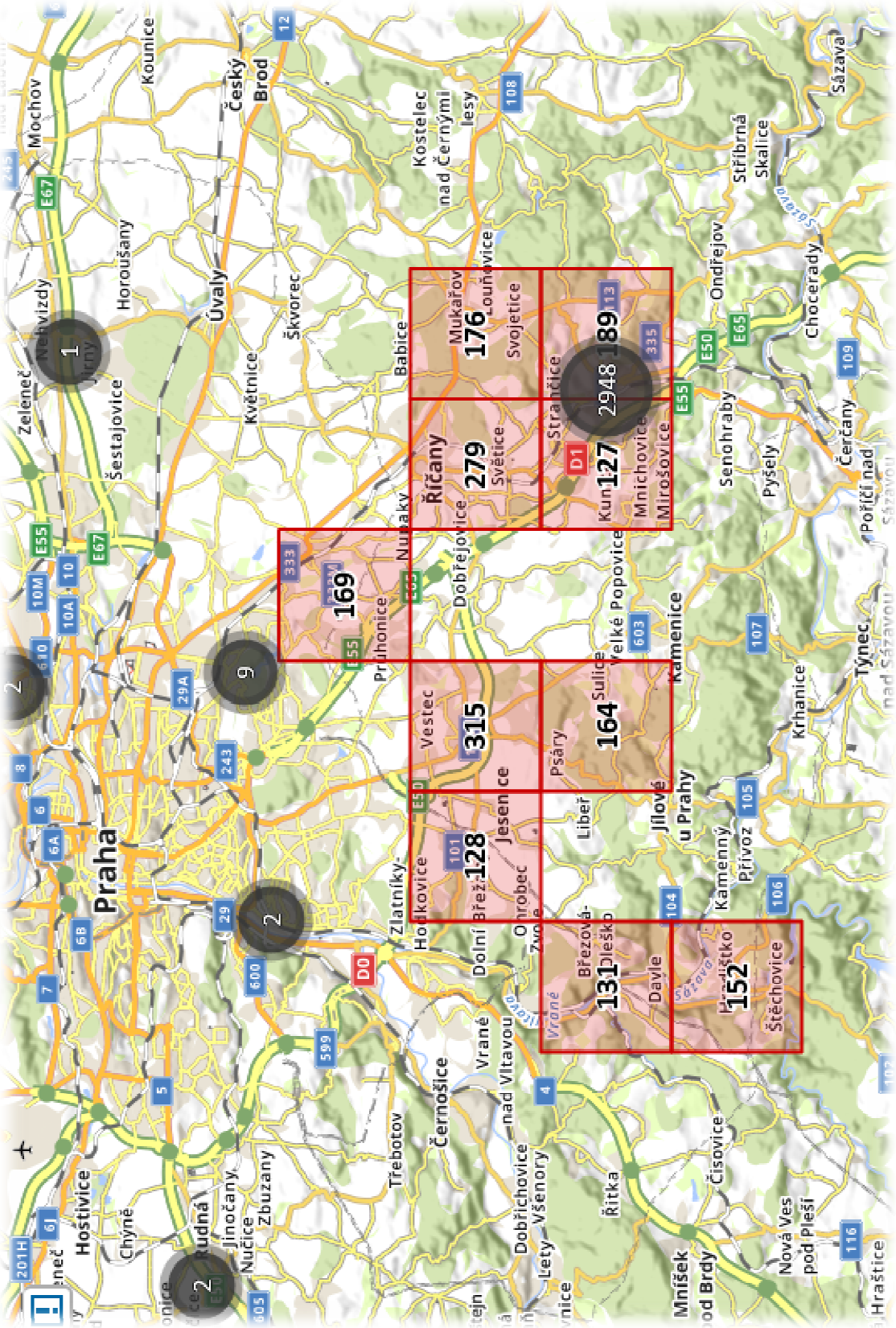
Příloha 7 Mapa rizikových oblastí TČ krádeže vloupáním - ÚO Mělník Zdroj: Mapa kriminality PČR



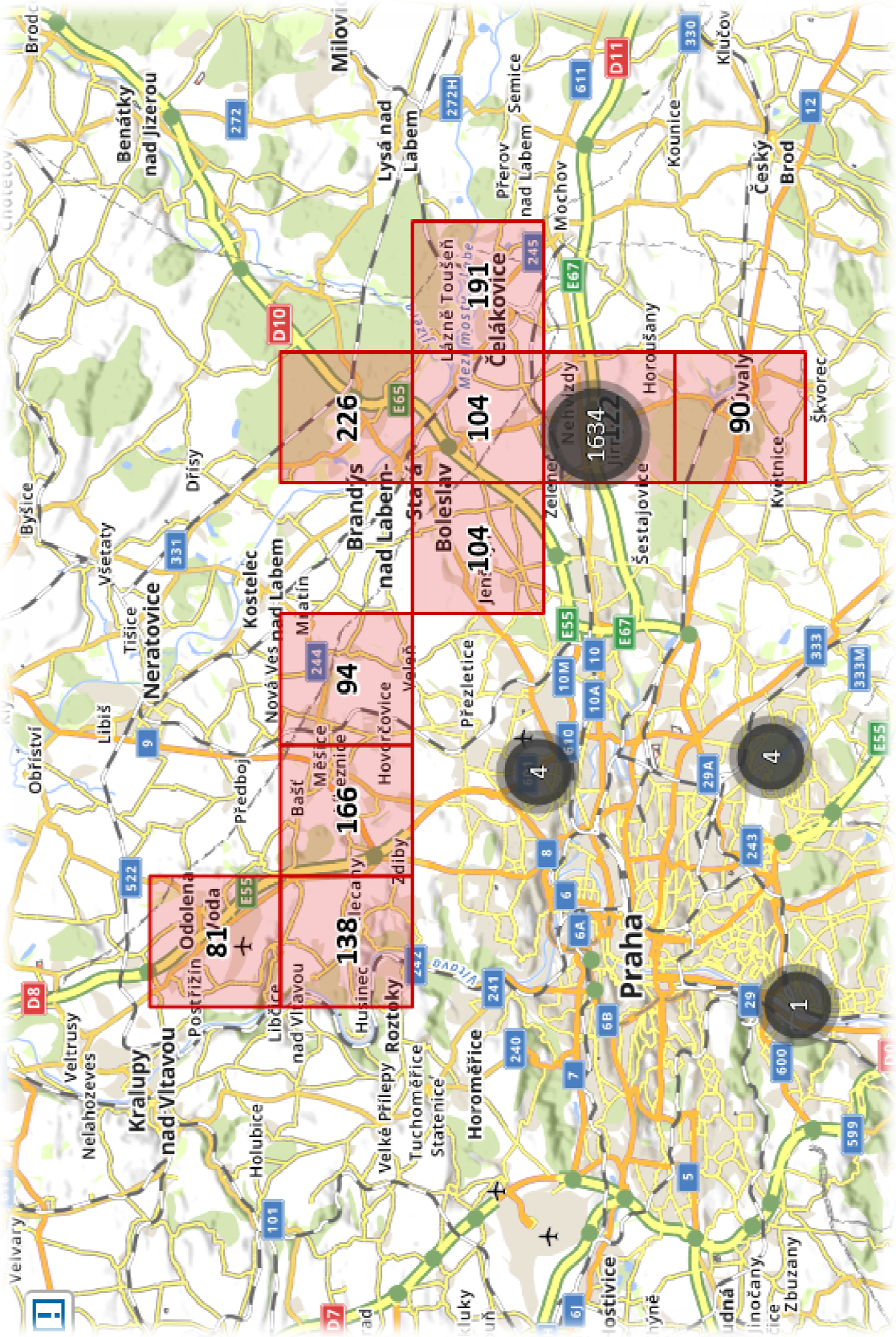
Příloha 8 Mapa rizikových oblastí TČ krádeže vloupáním - ÚO Nymburk Zdroj: Mapa kriminality PČR



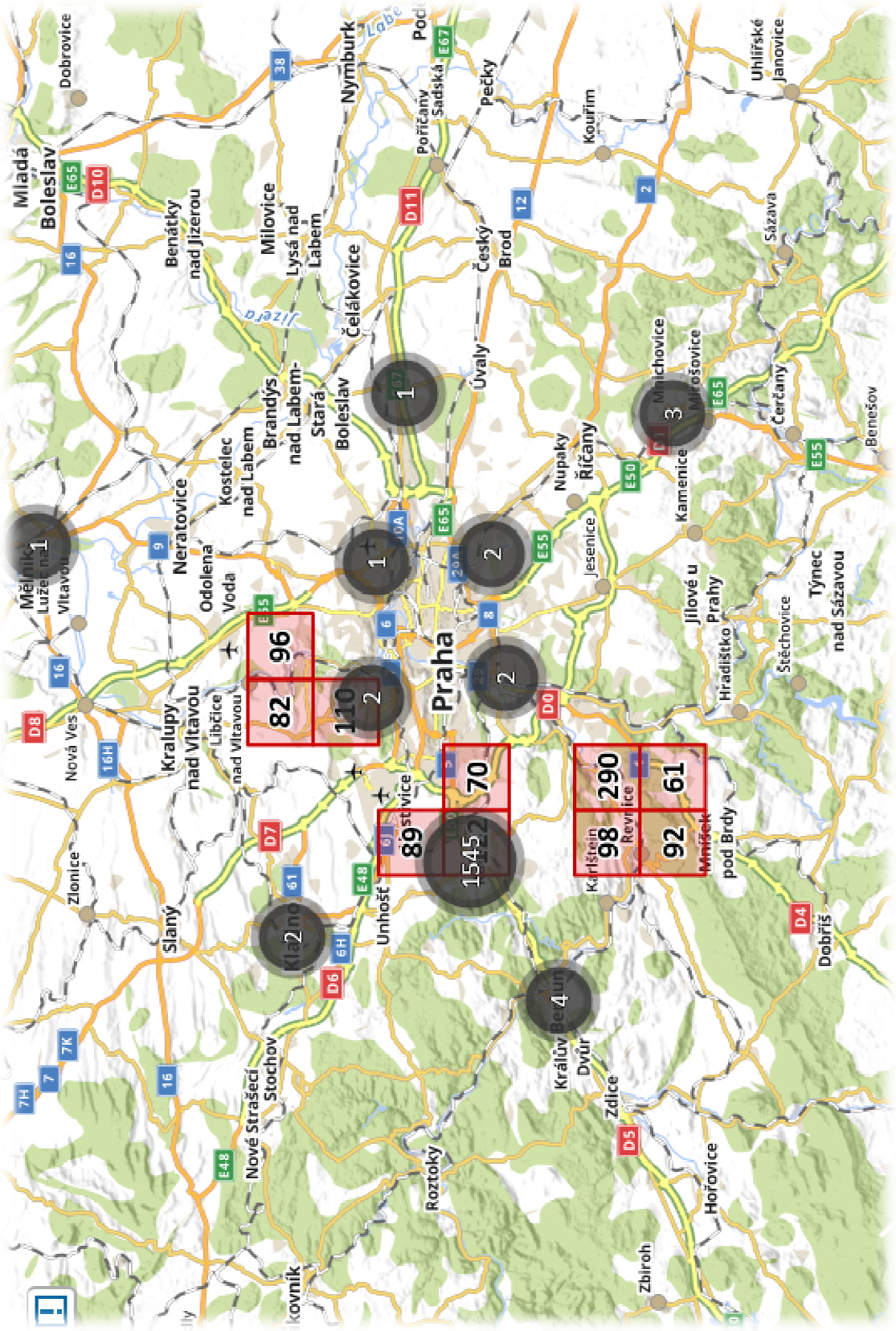
Příloha 9 Mapa rizikových oblastí TČ krádeže vloupáním - ÚO Příbram Zdroj: Mapa kriminality PČR



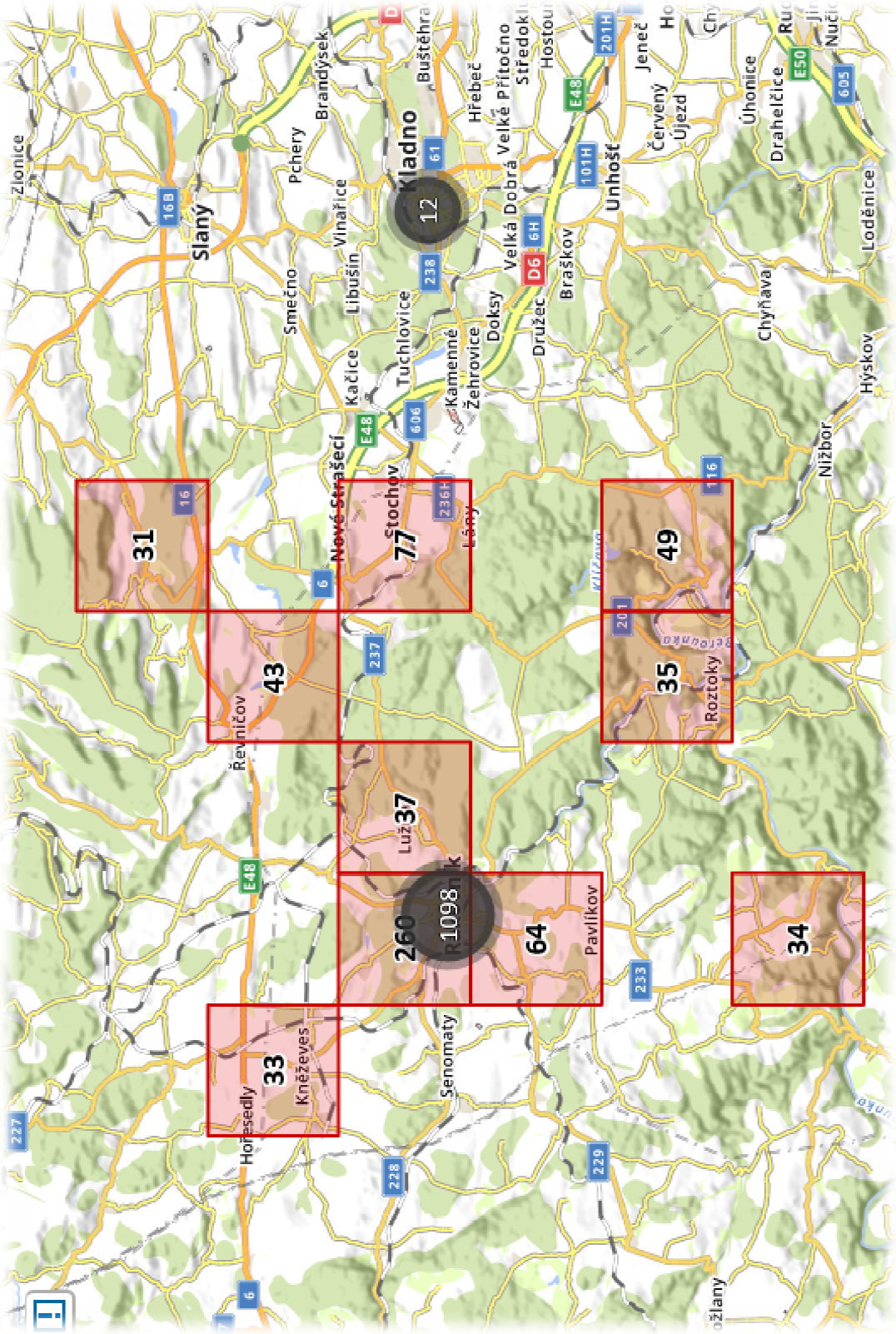
Příloha 10 Mapa rizikových oblastí TČ krádeže vloupáním - ÚO Praha venkov jih Zdroj: Mapa kriminality PČR



Příloha 11 Mapa rizikových oblastí TČ krádeže vloupáním - ÚO Praha venkov východ Zdroj: Mapa kriminality PČR



Příloha 12 Mapa rizikových oblastí TČ krádeže vloupáním - ÚO Praha venkov západ Zdroj: Mapa kriminality PČR



Příloha 13Mapa rizikových oblastí TČ krádeže vloupáním - ÚO Rakovník Zdroj: Mapa kriminality PČR