Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Strategické řízení a přívětivý úřad Zlínského kraje
CZ.03.4.74/0.0/0.0/18_092/0014595

Zlínský kraj

# INTELIGENTNÍ ŘEŠENÍ ŘÍZENÍ DOPRAVY VE ZLÍNSKÉM KRAJI

# – AKČNÍ PLÁN –

## Příloha 5. k části 3.3.

## Metodika integrace telematických systémů ve veřejné dopravě do systému krizového řízení, komunikace z hlediska technické / technologické úrovně standardů

**ZLÍNSKÝ KRAJ**

**třída Tomáše Bati 21, 761 90 Zlín**

**Dodavatel: KPM CONSULT, a.s.**

**Kounicova 688/26, 602 00 Brno**

**Listopad. 2021**

## Autorský tým:

Ing. František Kopecký, Ph.D.

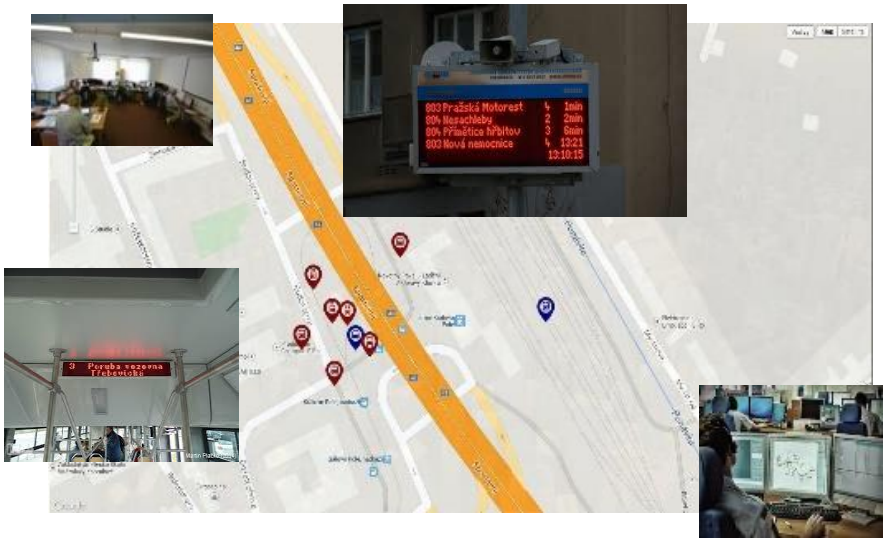
Ing. Arnošt Matlafus

Ing. Lubomír Malínek

Bc. Marek Večerka

# CERTIFIKOVANÁ METODIKA

## Metodika integrace telematických systémů ve veřejné dopravě do systému krizového řízení, komunikace z hlediska technické / technologické úrovně standardů



**Autoři:**

**Ing. František Kopecký Ph.D.**

**Ing. Arnošt Matlafus**

**Ing. Miloslav Věžník**

**Oponenti:**

**prof. Ing. Jan Kovanda, CSc.**

**Prof. Ing. Václav Cempírek, Ph.D.**

Metodika vznikla v rámci projektu *" Telematika ve veřejné dopravě v krizovém řízení"* podpořeného Ministerstvem vnitra České republiky pod číslem *VG20132015118. Další informace jsou dostupné na portálu www.its-knihovna.cz.*

# Obsah

# 1 Cíl metodiky

V dnešním světě neustále vzrůstá nebezpečí vzniku krizových situací, jako jsou například povodně, velké požáry, ale vzrůstá i nebezpečí teroristických útoků. Pokud ke krizové situaci dojde, je sanace důsledků spojena s velkým úsilím pro zajištění bezpečnostní situace a to zejména v městských, příměstských oblastech a regionech. Kritickým atributem pro zabezpečení klidu a bezpečnosti v oblastech výskytu krizových situací je zabezpečení informovanosti občanů. Jak prokázala zkušenost ze stávajících průběhů krizových situaci u nás i v zahraničí, jsou stávající informační kanály nedostatečné a v některých případech nespolehlivé. Je jasné, že vlastní síť prostředků krizového řízení nemůže pokrýt veškeré potřeby specifik území. Proto se standardně využívá i služeb operátorů mobilních sítí pro informování občanů v předmětné oblasti. Mobilní sítě zpravidla však v krizových oblastech kolabují, obtížně zabezpečují služby vlastnímu managementu krizového řízení, kapacita sítě již chybí. Je třeba hledat i jiné možnosti, které dnešní rozvoj ICT v městech a regionech poskytuje.

Plánování, organizování a řízení veřejné dopravy je složitým problémem. Mají-li být služby veřejné dopravy vyhledávané, musí vykazovat vysoký standard služeb. Veřejná doprava musí být spolehlivá, rychlá a bezpečná, jednotlivé subsystémy musí na sebe navazovat. Proto je dnes organizování a řízení veřejné dopravy silně podporováno aplikacemi, subsystémy a systémy dopravní telematiky na bázi komunikačních a informačních technologií. Postupně jsou realizované dispečinky dopravců, v městských aglomeracích dispečinky městské hromadné dopravy, ale nově se realizují dispečinky koordinátorů veřejné dopravy v regionech. Dispečink zná aktuální polohu všech dopravních prostředků veřejné dopravy v systému, poskytuje aktuální informace na různá informační media cestujícím do vozidel, na vybrané zastávky a přestupní uzly, do kulturních, obchodních center, ale i na webové stránky a všem dopravním zaměstnancům v systému. Informace mají charakter audio, video, psaný text. Na vybrané zastávky se umísťují inteligentní stojany, které cestují standardně formou textové zprávy, informují o příjezdech linek na zastávku, o možnostech přestupu, o mimořádnostech v systému, atd. Na přestupní uzly se umísťují velké a malé informační tabule, které kromě klasické textové zprávy umožní i produkci v kvalitě video například pro zobrazení map a podobně. Do společenských, kulturních a obchodních center se umísťují interaktivní informační stojany zpravidla s informační tabulí pro informační sdělení cestujícím. Stojan umožňuje i přímou komunikaci s dispečerem. Ve vozidlech veřejné dopravy dnes najdeme množinu informačních panelů. Kromě standardního panelu pro sdělování textových informací mohou být ve vozidle standardní LCD panely. Každé vozidlo zejména v městských aglomeracích umožňuje dispečerské audio vstupy. Podobná služba je možná i v informačních mediích předchozích typů. Nově se rozvíjí i různé multimodální služby s vyhledávači. I tato služba je důležitou možnosti oslovení cestujících v systému. Všechna popsaná informační média jsou rozmístěna všude tam kde, je silný pohyb občanů a to nejen cestujících a to prakticky na celém území řízené oblasti jako je město, příměstská oblast, ale i celé území kraje. Vlastní technické a technologické řešení telematiky ve veřejné dopravě zpravidla splňuje vysoký stupeň spolehlivosti, v době kritických situací zůstávají zpravidla v plném provozuschopném stavu.

Zásadním problémem dnešního stavu je, že jak systém krizového řízení, respektive systémy složek krizového řízení, byly budovány samostatně bez možnosti tvorby informačních vazeb na okolí. Dispečeři složek krizového řízení například nemají přehled o pohybu prostředků veřejné dopravy, i když tato informace by jim umožnila lépe řešit krizové a mimořádné situace. Také telematické systémy veřejné dopravy jsou budovány uzavřeně, i když dispečer veřejné dopravy by měl mít dnes kvalitnější zprávy o řešení mimořádných situací s center krizových řízení a tyto informace bezpečnostního a krizového charakteru přenést na popsaná informační media. Informační média telematiky ve veřejné dopravě tedy dnes nelze využít pro krizové řízení přímo, protože nejsou informačně otevřené komunikační kanály a komunikační rozhraní. Dnes vzájemná komunikace dispečerů se odehrává prostřednictvím linek operátorů telefonní sítí (pevné, mobilní) a výhradně fónický.

Metodika, vytvořená v rámci řešení projektu " Telematika ve veřejné dopravě v krizovém řízení" podpořeného Ministerstvem vnitra České republiky, je obrazem zjištěných skutečností. V řešeném projektu bylo cílem nalezení nejoptimálnějšího způsobu tvorby informačních vazeb mezi systémy organizací krizového řízení a dispečinky řízení veřejné dopravy pro zabezpečení sdílení informací, které zlepší řešení krizí a mimořádných událostí.

Cílem této metodiky je vytvořit základní definice technických a technologických rámců pro zabezpečení těchto informačních vazeb.

Metodika naplňuje cíle Akčního plánu rozvoje ITS ČR, a to rámcový specifický cíl č. 3.3: „Zvýšení informovanosti osobám nacházejících se uvnitř či přijíždějícím k oblasti živelné pohromy nebo jiné krizové situace". Doporučení metodiky rovněž naplňují cíl č. 3. 1. 11 „Nezbytnost využívání technických norem, standardů a systémových parametrů při zadávání veřejných zakázek".

# 2 Teoretická základna- definice pojmů

## 2.1 Aplikace

Zpravidla řeší jeden problém v systému IDS bez zohlednění následných informačních vazeb. Bouřlivý vývoj v dopravní telematice byl poznamenán právě masovým rozšířením aplikací v celém spektru dopravy. Například:

- byly a jsou rozvíjeny elektronické platební systému u jednotlivých dopravců,[1]
- práce s obrazem,[2]
- polohovací systémy dohledu (dispečink),[3]
- atd.

Hovoříme o ***aplikačním přístupu*** k telematice neboli také o ***nesystémovém přístupu***. Situaci zhoršuje i nejednotný přístup k informační bázi. Potom je velmi těžké budovat ucelený systém vedoucí k tvorbě znalostí[4].

## 2.2 Systém

Systém je zpravidla sestaven na základě „širších" požadavků, je tedy složen z množiny funkčních celků, můžeme říci z aplikací, s cílem poskytnutí množiny služeb uživatelům. V oblasti IDS se jedná například o:

- elektronické platební systémy - budou kompatibilní u všech dopravců v systému,
- dispečerské řízení procesů - budou v systému IDS propojitelné
- informační systémy pro cestující- budou pracovat v systému IDS na jednotné technické bázi,
- atd.

I systém, pokud je zadán bez širšího rozkladu informačních vazeb, může být vybudován izolovaně bez možnosti sdílení informací. Potom hovoříme opět o nesystémovém přístupu. Můžeme očekávat problémy v rozvoji dalších služeb.

---

[1] Zpravidla bez možnosti vzájemných vazeb.
[2] Bez možnosti sdílení obrazové informace.
[3] Bez možností sdílení dat se sousedy, nebo dalších služeb umožňující navazující vazby.
[4] Pokud jsou však, požadavky na aplikaci jsou zadávány z hlediska koncepčního přístupu, stává se i jednoúčelové řešení součástí systému, respektive architektury.

## 2.3 Architektura

Každá architektura ICT by měla mít svoji referenční podobu – svůj referenční model. Ten by měl popisovat, jak architektura vypadá ve své generické podobě. Referenční architektura však není ani konkrétní technologie nebo produkt ani norma nebo standard, ale obecný přístup jak aplikace budovat nebo integrovat. Referenční architektura je tedy generická, nepředepisující a obsahuje koncepce systému. Pojem architektura definuje také základní uspořádání systémů, subsystémů a aplikací do funkčních bloků. Jejím cílem je co největší přehlednost a srozumitelnost. Vše musí vést k zajištění propojitelnosti vedoucí ke sdílení informací uvnitř architektury s přesně definovanými vazbami na „okolí“. Protože dopravní systém má globální rysy, proto architekturu dopravní telematiky vnímáme v několika úrovních:

- **evropské** – pro zabezpečení výměny zboží, bezpečnosti, ale i informovanosti uživatelům dopravního systému,
- **národní** – pro zabezpečení propojitelnosti informací v národní úrovni s vazbou na evropskou,
- **regionální** – pro zabezpečení specifik regionů, respektive krajů
- **městskou** – i městská úroveň má svá specifika.

V této oblasti se potom obecné používají pojmy logická, respektive fyzická architektura.

### 2.3.1 Referenční architektura

Cílem definování referenční architektury je obecně poskytnout stručný referenční bod, který je jak vzdělávacím tak pracovním rámcem pro proces standardizace. Referenční architekturu použijí pracovní skupiny pro vývoj jejich vlastní logické a fyzické architektury uceleným a soudržným způsobem, resp. poskytnout základnu pro vypracování norem pro účely propojování systémů.

Otevřený systém podle tohoto modelu je abstraktním modelem reálného otevřeného systému. Jak bylo již výše uvedeno, nespecifikuje implementaci (realizaci) systémů, ale uvádí všeobecné principy sedmivrstvé síťové architektury - OSI. Popisuje vrstvy, jejich funkce a služby. Nejsou zde zařazeny žádné protokoly, které by vyžadovaly zbytečně mnoho detailů. Referenční model ISO/OSI vypracovala organizace ISO jako hlavní část snahy o standardizaci počítačových sítí nazvané OSI a v roce 1984 ho přijala jako mezinárodní normu ISO 7498.

### 2.3.2 Fyzická architektura

Fyzická architektura přiřazuje jednotlivým subsystémům a funkčním blokům konkrétní zařízení včetně jejich alokace. Komunikační architektura definuje konkrétní požadavky na přenos informací mezi jednotlivými fyzickými subsystémy (s respektováním požadavků na systémové parametry) z čehož je možno odvodit možnou technologii přenosu (GSM, GPRS, ATM, TETRA, atd.) případně i použitý protokol (různé stupně zabezpečení, atd.).

Organizační architektura přiřazuje jednotlivým funkcím humánní komponenty případně organizační zabezpečení jednotlivým funkcím. Návrh fyzické architektury musí respektovat legislativu ČR případně další národní konvence a odpovědnosti jednotlivých organizačních jednotek.

### 2.3.3 Logická architektura

Logická architektura zpracovává funkce, které budou poskytovat koncepční chování, a tím poskytne některé podrobnosti o modularitě. Fyzické architektury se dosáhne definováním skutečného rozmístění systémových modulů, ze kterého vyplývají důležité implikace pro komunikace.

## 2.4 Architektura ITS na bázi ICT ve veřejné dopravě

Controlling veřejné dopravy je nově rozvíjeným pojmem právě v souvislosti s rozvojem IDS. Je a bude přímou podporou fungujícího dopravního systému v regionu, a to podporou provázaností jednotlivých linek a spojů jednotlivých dopravců. Pro potřeby systémového rozvoje dopravní telematiky je nutno vnímat controlling ve třech základních úrovních:

- **Plánovací** – zpravidla je součástí rozvojových územních plánů. Ve vztahu k dopravní obslužnosti se jedná o plánování jednotlivých linek tak, aby byla propojena významná centra regionu, průmyslové zóny, společenská a turistická centra atd., důležitým požadavkem této úrovně je také optimalizace, modernizace a výstavby dopravní infrastruktury, dopravních terminálů a přestupních uzlů.
- **Organizační** – je podporou praktické realizace dopravy, můžeme ji přirovnat k osazení dopravních značek na silnicích. Ve vztahu k dopravní obslužnosti se jedná o podporu plánování jednotlivých spojů, linek různých dopravců a dopravních oborů, plán jízdních řádů (JŘ), respektive grafikonů. Jedná se také o organizaci plateb v IDS, organizaci rozpouštění dotačních prostředků, ale i o tvorbu smluv s dopravci a kontrolu plnění.
- **Operativní** – praktická realizace řízení dopravy v IDS. Ve vztahu k dopravní obslužnosti se jedná o sledování plnění grafikonu, respektive JŘ, obsazenosti jednotlivých spojů, tržeb, nákladů atd., ale i o poskytování aktuálních informací cestující veřejnosti. Typickým příkladem řešení „operativy" je řešení vlivů dopadů nepříznivých situací, jako jsou například kongesce, nesjízdnost silnic, nehody a další mimořádné situace ovlivňující plynulost dopravy.

Každá z těchto úrovní je dnes podporována aplikacemi dopravní telematiky. Z hlediska cílů této metodiky je důležitá „Operativní" úroveň controllingu veřejné dopravy.

## 2.5 Rozhraní v dopravně-telematických systémech

Problematika tvorby složitých systémů dopravní telematiky vedoucí k tvorbě znalostí o dopravně přepravním procesu, o tvorbě nástrojů aktivního řízení (i represe), vede k nutnosti informace vzájemně sdílet a předávat data. V praxi se postupně realizují složité architektury[5] vzájemně provázaných aplikací dopravní telematiky. Zkusme se na problematiku rozhraní v systémech podívat podrobněji. Na následujících obrázcích je zobrazen princip „rozhraní" v ICT z hlediska systémového inženýrství.

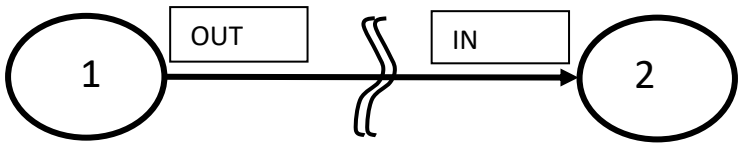
Rozhraní je technickým, technologickým a informačním integračním / homogenizačním článkem mezi aplikacemi, subsystémy a systémy. Lze na něm názorně demonstrovat způsoby práce se vstupními a výstupními informacemi v informatice, respektive v dopravní telematice. Informace (proměnná) na výstupu hraničního prvku 1 je vstupní proměnnou navazujícího prvku 2[6]. Má-li být rozhraní regulární, musí být příslušné proměnné výstupu a navazujícího vstupu shodné, musí mít společnou bázi, společné argumenty[7] a domény hodnot těchto argumentů shodné, nebo alespoň s podstatným průnikem[8].

[5] Architekturou ve smyslu systémového inženýrství rozumíme účelově identifikovaný systém na daném objektu nebo primárním systému s charakteristikami:(i.) umístění do relevantního prostoru, (ii.) podpory rozvoje primárního systému resp. objektu (iii.) návaznosti infrastruktury (iv.) podpory záměru (účinku) konceptora – architekta.

[6] Typicky přenos kmenových proměnných například ze senzorů dopravního prostředku či dopravní infrastruktury k zpracování v centru.

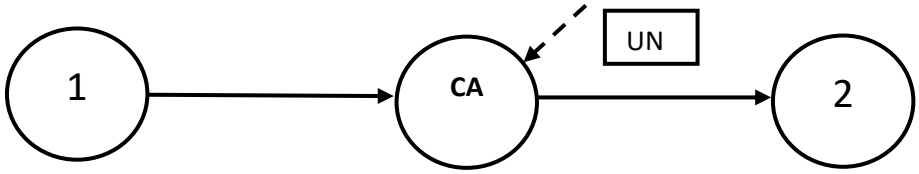
[7] Například IP protokol

[8] (v takovém případě zavádíme pojem přípustné degradace rozhraní)




*Obr. 1.: Základní schéma systémového rozhraní dvou prvků systému 1 a 2 na vazbě mezi těmito prvky.*

V dopravní telematice jsou klíčové objekty (aplikace), zabývající se řízením provozu, sběrem a distribucí dopravních informací. Problematika rozhraní respektive jeho regularita má kromě ryze technických[9] a technologických[10] i popisnou část. Tedy zabezpečení jednotného rozpoznání a interpretace přenášené proměnné na jednotné bázi[11] mezi jednotlivými aplikacemi, subsystémy a systémy. Problematika rozhraní má také výrazný váhový charakter spočívající ve splnění systémových požadavků uživatelů systému[12]. Snaha o zabezpečení jednotné báze proměnných při tvorbě nových složitých systémů[13] vede nutně k tvorbě takzvaných transformačních - konverzních HW a SW prvků, umístěných právě na rozhraních[14]. To při nevhodném návrhu či způsobu realizace silných procesů[15] může výrazně narušit stabilitu systému, časové charakteristiky procesů uvnitř systému a zvětšit spolehlivostní a bezpečnostní rizika. Systém se stává složitějším a obtížně "dozorovaným" subsystémy zajištění integrity. Proto bylo nutné definovat základní systémové parametry.




*Obr. 2.: Konverzní prvek CA zařazený do vazby pro regularizaci rozhraní*

## 2.6 Systémové parametry v ITS

V dopravní telematice hrají významnou roli tzv. systémové parametry (performance parameters), pomocí kterých je možno definovat systémové požadavky na telematickou aplikaci, subsystém a systém. Systémové parametry lze přiřadit jak k funkci, tak k telekomunikační vazbě, ale i k jednotlivým procesům v dopravně telematickém systému, ale také k jednotlivým parametrům např. k polohové informaci, přenosu informace, atd.

### 2.6.1 Definice systémových parametrů

Systémové parametry jsou definovány pravděpodobnostně pro jednotlivé parametry. V následujících definicích pro jednotlivé parametry je přiblížen základní teoretický aparát. Parametry jsou definovány obecně tak, aby je bylo možno použít pro celou škálu telematických aplikací, ale i jednotlivých jejich částí z hlediska jejich funkce.

---

[9] HW -zásuvky, zobrazení atd.
[10] Jednotná frekvence komunikačních kanálů, jednotný formát dat
[11] Zabezpečení tak zvané synchronizace informací v čase, prostoru a parametru.
[12] Bezpečnost, spolehlivost, dostupnost, integrita.
[13] Vedena systémovým požadavkem homogenizace
[14] Protože logicky pracují s již zavedenými aplikacemi, subsystémy a systémy
[15] tedy zejména těch procesů, které zajišťují provoz dané aplikace

#### 2.6.1.1 Přesnost

Je definována jako stupeň shody mezi měřenou a definovanou hodnotou parametru/procesu/funkce:

$$P\left(\left|p_i - p_{m,i}\right| \le \varepsilon_1\right) \ge \gamma_1 \qquad \textbf{(1)}$$

Rovnice (3) definuje, že rozdíl mezi požadovaným parametrem $p_i$ a měřeným parametrem $p_{m,i}$ nepřesáhne hodnotu $\varepsilon_1$ na hladině pravděpodobnosti $\gamma_1$, kde uvedený vztah platí i pro vektory parametrů.

Např. u systému monitorování pohyblivých objektů po pohybové ploše letiště je požadavek daný předpisem, že chyba polohové informace nesmí překročit v horizontální rovině 7.5 m na hladině pravděpodobnosti 99.9%.

#### 2.6.1.2 Spolehlivost

Je schopnost systému plnit požadované funkce bez přerušení během daného postupu v průběhu definovaného časového intervalu:

$$P\left(\left|\vec{v}_t - \vec{v}_{m,t}\right| \le \varepsilon_2\right) \ge \gamma_2, t \in \langle 0, T\rangle \qquad \textbf{(2)}$$

Rovnice (4) definuje, že rozdíl mezi požadovanými funkcemi/procesy reprezentovanými požadovanými parametry (vektory parametrů) $\vec{v}_t$ a měřenými (skutečnými) parametry nepřesáhne hodnotu $\varepsilon_2$ na hladině pravděpodobnosti $\gamma_2$ v každém čase t v intervalu $\langle 0, T\rangle$.

Např. u polohové informace spolehlivost reprezentuje poměr nedostupnosti lokalizační služby k času sledování - čas sledování se typicky určuje jako 1 rok pro hodnocení systémů GPS, 1 hodina pro hodnocení systémů na železnici a typicky 3 minuty pro hodnocení leteckých systémů. Pokud je požadavek 99% spolehlivosti systému na hladině pravděpodobnosti 99% v čase 1 hodina, znamená to, že 99% času z 1 hodiny je služba dostupná a opakujeme-li měření 100krát, pouze jedenkrát se stane, že služba měla spolehlivost horší než 99%.

#### 2.6.1.3 Dostupnost

Je schopnost systému plnit požadované funkce při inicializaci (spuštění) systému/procesu dle daného postupu:

$$P\left(\left|q_i - q_{m,i}\right| \le \varepsilon_3\right) \ge \gamma_3 \qquad \textbf{(3)}$$

Rovnice (5) definuje, že podíl požadovaného úspěšného spuštění i-té funkce/procesu $q_i$ a měřeného podílu $q_{m,i}$ nepřekročí hodnotu $\varepsilon_3$ na hladině pravděpodobnosti $\gamma_3$. Měřená hodnota podílu $q_{m,i}$ je definována:

$$q_{m,i} = \frac{Q_i}{Q} \qquad \textbf{(4)}$$

kde $Q_i$ je počet úspěšných experimentů spuštění funkce/procesu a Q je počet všech provedených experimentů spuštění funkce/procesu.

Dostupnost je spojena s inicializací funkce. Např. na příkladu lokalizačních informací lze demonstrovat, že při zapnutí GPS přijímače musí být služba dostupná během 30 sekund na hladině pravděpodobnosti 99% (u GPS lokalizace je tento čas známý jako TTF - time to first face, nebo-li čas spuštění služby). Tento požadavek znamená, že provedeme-li 100 náhodných spuštění lokalizační služby, pouze v jednom případě naběhnutí lokalizační služby trvá déle než 30s.

#### 2.6.1.4 Kontinuita (spojitost)

Je schopnost systému plnit požadované funkce/procesy bez (neplánovaného) přerušení (maximální povolená délka přerušení je předem definována) během daného postupu (nebo definovaného časového intervalu):

$$P\left(\left|r_i - r_{m,i}\right| \le \varepsilon_4\right) \ge \gamma_4 \qquad \textbf{(5)}$$

Rovnice (6) značí, že rozdíl mezi požadovaným podílem úspěšnosti činnosti funkce/procesu bez přerušení $r_i$ a měřené hodnoty $r_{m,i}$ tohoto podílu nepřesáhne hodnotu $\varepsilon_4$ na hladině pravděpodobnosti $\gamma_4$. Kontinuita má blízko ke spolehlivosti, ale hlavním rozdílem je sledování délky výpadku. Jde o rozložení výpadků - u spolehlivosti můžeme zaznamenat jeden dlouhý výpadek anebo, mnoho krátkodobých výpadků. Právě kontinuita dokáže mezi těmito dvěma případy rozlišit a definovat, jaká maximální délka výpadku je povolena.

Uveďme též příklad z lokalizačních služeb, kdy na letišti je požadavek maximální délky výpadku lokalizační služby 5 sekund na hladině pravděpodobnosti 99% v časovém intervalu 3 minuty. Znamená to, že v intervalu 3 minuty jsou možné výpadky pouze s maximální délkou 5 sekund. Provedeme-li 100 měření, pouze v jednom případě se stane, že v 3 minutovém intervalu nalezneme výpadek delší než 5 sekund. Kontinuita má velký vztah ke kritickým aplikacím pracujícím v reálném čase.

#### 2.6.1.5 Integrita

Je schopnost systému včasně a bezchybně informovat uživatele, že systém nemůže být použit pro operace daného postupu

$$P\left(\left|S_i - S_{m,i}\right| \le \varepsilon_5\right) \ge \gamma_5 \qquad \textbf{(6)}$$

Rovnice (8) říká, že rozdíl mezi požadovanou úspěšností hlášení poruch $S_i$ o překročení daného limitu (AL - Alert Limit), kdy porucha je nahlášena nejpozději do časového limitu (TTA - Time to Alert) a měřenou hodnotou úspěšnosti hlášení poruch $S_{m,i}$ nepřekročí hodnotu $\varepsilon_5$ na hladině pravděpodobnosti $\gamma_5$.

Integrita vyjadřuje schopnost diagnostického systému včas diagnostikovat překročení předdefinovaných parametrů a za požadovaný časový interval o této skutečnosti informovat uživatele/obsluhu.

V případě lokalizačních funkcí je požadavek, že pokud se přesnost určení polohy překročí hranici 10 metrů, uživatel musí být o této změně přesnosti informován do 5 sekund na hladině pravděpodobnosti 99%. Tento požadavek je typický pro kritické aplikace, kde provedeme-li 100 pokusů testu diagnostického systému, pouze v jednom případě se uživatel dozví později než 5 sekund, nebo nedozví vůbec o zhoršení přesnosti lokalizační funkce.

#### 2.6.1.6 Bezpečnost

Je schopnost systému, že v případě vzniku poruchy nedojde k poškození systému nebo k materiálním ztrátám či ztrátám na lidském životě (ztráty vycházejí z provedené analýzy a klasifikace rizik):

$$P\left(\left|W_i - W_{m,i}\right| \le \varepsilon_6\right) \ge \gamma_6 \qquad \textbf{(7)}$$

Rovnice (9) říká, že rozdíl mezi požadovanou rizikovou situací $W_i$ a skutečnou rizikovou situací $W_{m,i}$ nepřekročí hodnotu $\varepsilon_6$ na hladině pravděpodobnosti $\gamma_6$.

Bezpečnost, jako systémový parametr, rozděluje chyby/poruchy, které se vyvíjí bezpečným směrem, pak jde o výpadky, které jsou charakterizovány spolehlivostí, kontinuitou, integritou, atd. a chyby/poruchy, které se vyvíjí nebezpečným směrem. Zjištění bezpečných a nebezpečných stavů systému je součástí klasifikace a analýz rizik.

## 2.7 Systémové parametry v přenosu informace

Při tvorbě složitých systémů na bázi ICT má přenos informací důležitou a zpravidla rozhodující úlohu. Systémové parametry v telekomunikacích byly odvozeny od základních systémových parametrů s položením důrazu na specifikace komunikačního prostředí. Pro stanovení metodiky návrhu telekomunikačního subsystému vycházíme z definice provozních indikátorů systémů v oblasti monitorování polohy a stavu mobilních prostředků a předkládáme definice provozních indikátorů komunikačního řešení, které reflektují fakt, že komunikační subsystém je integrální součástí telematického řetězce. Definice komunikačních parametrů je koncipována ve snaze maximální možné kompatibility s telematickými indikátory.

### 2.7.1 Aktivační doba dostupnosti služby

$$P\left(\left|a_i - a_{m,i}\right| \le \varepsilon_1\right) \ge \gamma_1 \qquad \textbf{(8)}$$

tj., rozdíl požadovaného času úspěšného i-té aktivace systému $a_i$ a naměřeného aktivačního času $a_{m,i}$ nepřekročí hodnotu $\varepsilon_1$ na hladině pravděpodobnosti $\gamma_1$.

### 2.7.2 Dostupnost služby (např. virtuálního okruhu)

Je schopnost okruhu plnit požadované funkce bez přerušení během daného postupu v průběhu definovaného časového intervalu:

$$P\left(\left|ca_t - ca_{m,t}\right| \le \varepsilon_2\right) \ge \gamma_2, t \in \langle 0, T \rangle \qquad \textbf{(9)}$$

tj., rozdíl mezi požadovanými parametry $ca_t$ a měřenými (skutečnými) parametry $ca_{m,t}$ nepřesáhne hodnotu $\varepsilon_2$ na hladině pravděpodobnosti $\gamma_2$ v každém čase t v intervalu $\langle 0, \mathrm{T} \rangle$.

Dostupnost virtuálního okruhu je chápána jako podíl dostupnosti okruhu v daném čase sledování. V telekomunikacích se obvykle uvádí hodnotami dostupnosti služby v období 1 roku. Např. roční dostupnost 99,95% reprezentuje nedostupnost okruhu cca 4 hod. v průběhu jednoho roku s tím, že v 99 pokusech ze 100 pokusů je v 99 případech dostupnost splněna. S ohledem na paritní definici spolehlivosti telematických služeb je takto stanovená hodnota nesouměřitelná a je nutno ji kombinovat s veličinami MTBF a MTTR, jejichž definice následuje.

### 2.7.3 Střední doba mezi dvěma poruchami (Mean Time Between Failures, MTBF):

$$P\left(\left|f_i - f_{m,i}\right| \le \varepsilon_3\right) \ge \gamma_3, \qquad \textbf{(10)}$$

tj. i-tý rozdíl vzorku požadované doby mezi dvěma poruchami $f_i$ a skutečné hodnoty tohoto parametru $f_{m,i}$, který je menší než $\varepsilon_3$ na hladině pravděpodobnosti $\gamma_3$.

Pokud je interval MTBF na dané hladině pravděpodobnosti řádově větší, než je interval $\langle 0, \mathrm{T} \rangle$ definice **Chyba! Nenalezen zdroj odkazů.**, lze tento parametr, tj. dobu mezi dvěma poruchami, považovat n a dané hladině pravděpodobnosti za nevýznamný. Tento stav ale není dosažitelný zejména u mobilních komunikačních systémů aplikovaných v členitém terénu. Obdobně ale v těchto prostorách bude pro zachování služby nutné alternovat i polohovací metody GNSS např. inerciálními systémy (kap. **Chyba! N enalezen zdroj odkazů.**).

Je proto nezbytné v komplikovanějších aplikacích co nejpřesněji specifikovat území s různou úrovní (rozptylem) požadavků na provozní parametry, např.:

- místa s kritickým požadavkem (uzly a jejich okolí)
- místa s nekritickým požadavkem (širá trať, dálnice apod.)
- vozovny, depa apod.

### 2.7.4 Doba obnovení služby - MTTR (Mean Time to Restore):

$$P\left(\left|rc_i - rc_{m,i}\right| \le \varepsilon_4\right) \ge \gamma_4, \qquad \textbf{(11)}$$

tj. rozdíl požadované $rc_i$ a skutečné hodnoty $rc_{m,i}$ i-tého obnovení funkcionality po poruše sítě je menší než $\varepsilon_4$ na hladině pravděpodobnosti $\gamma_4$.

Tato hodnota je samozřejmě vázaná na redundantní síťová telekomunikační řešení s automatickou obnovou. Tato veličina je interpretovatelná jako (dominantní) součást parametru kontinuita (**Chyba! Nenalezen zdroj odkazů.**), tj. maximální doba výpadku služby v daném intervalu na dané hladině pravděpodobnosti.

S ohledem na možnost způsobení výpadku třetí stranou (poškození kabelu, úder blesku apod.) považujeme za vhodné s touto hodnotou vždy počítat – tedy alespoň při stanovování kritických časových prodlev způsobených kumulací zpoždění signálu komunikačním zařízením. Je ale třeba zmínit, že tyto hodnoty se liší i o několik řádů podle použitého síťového řešení (např. IP VPN/L2 versus MPLS/L3).

### 2.7.5 Zpoždění

$$P\left(\left|d_t - d_{t,m}\right| \le \varepsilon_5\right) \ge \gamma_5, t \in \langle 0.T \rangle, \qquad \textbf{(12)}$$

tj., rozdíl požadované hodnoty zpoždění $d_t$ a měřené hodnoty zpoždění $d_{t,m}$ nepřesáhne hodnotu $\varepsilon_5$ na hladině pravděpodobnosti $\gamma_5$. Zpoždění má akumulační charakter a je mj. ovlivněno

- přenosovou rychlostí rozhraní,
- velikostí paketu/rámce/buňky a
- zatížením každého z uzlů, kterými spojení prochází.

Zatímco přenosová rychlost rozhraní a velikost paketu jsou veličiny statické (za předpokladu konstantní délky paketu/rámce), je zatížení uzlu, jak již bylo uvedeno, veličinou pravděpodobností svou příslušností patřící do kategorie „měkkých“ systémů. Důvodem je skutečnost, že existují nástroje řízení sítě, které mohou snížit pravděpodobnost vlivu zatížení uzlů sítě zejména u nejvyšší třídy služby na hodnotu blízkou nule. Pokud není přetížení sítě způsobené třetí stranou, tj. jev z kategorie bezpečnosti sítě, je v možnostech správce sítě (je-li k tomu vůle z ekonomických důvodů využití sítě) udržet stupeň vytížení uzlů pod kritickou hodnotou především korektní konfigurací sítě, tj. jejích jednotlivých uzlů a příslušných rozhraní. V kompetenci řešitele telematického systému je volba spolehlivého poskytovatele služby a příslušné třídy služby, která obsahuje mj. i toleranční pásmo zpoždění přeneseného paketu každým uzlem a kumulativně celou sítí.

### 2.7.6 Ztráta paketů

$$P\left(\left(pl_{t,d} / pl_t\right) \ge \varepsilon_7\right) \ge \gamma_7, t \in \langle 0.T \rangle \qquad \textbf{(13)}$$

tj., podíl počtu dodaných paketů $pl_{t,d}$ a celkového počtu odeslaných paketů $pl_t$ je roven anebo větší než $\varepsilon_7$ na hladině pravděpodobnosti $\gamma_7$, pro každý čas t z intervalu $\langle 0, T \rangle$.

Problematika ztráty paketů souvisí, stejně jako v předešlém odstavci, na korektnosti konfigurace sítě a volbě odpovídající třídy služby. Významnou úlohu má i relevantně navržená aplikační vrstva, případně v kombinaci s TCP anebo RTP/UDP transportními protokoly.

Vysoké procento ztracených paketů ve svém důsledku vyvolává změnu průchodnosti sítě - v případě jednoduché aplikace protokolu TCP, může mít lokální přetížení sítě důsledek v možnosti až patologického nárůstu zpoždění přenosu paketů. Proto jsou často užívány např. pro multimediální aplikace právě kombinace protokolů RTP/UDP, které s ohledem na typ aplikace spíše tolerují ztrátu jednotlivého paketu, než narůstající zpoždění generované měnícími se časovými podmínkami odesílání paketů protokolem TCP. Opět i zde platí důležitost volby adekvátní třídy služby, která je svými parametry relevantní dané aplikaci.

### 2.7.7 Bezpečnost

je schopnost systému, že v případě vzniku poruchy nedojde k poškození vlastní funkcionality komunikačního systému:

$$P\left(\left|Wc_i - Wc_{m,i}\right| \le \varepsilon_6\right) \ge \gamma_6 \qquad \textbf{(24)}$$

tj., rozdíl mezi i-tou požadovanou hodnotou rizikové situace $Wc_i$ a skutečnou hodnotou rizikovou situací $Wc_{m,i}$ nepřekročí hodnotu $\varepsilon_6$ na hladině pravděpodobnosti $\gamma_6$.

Nebezpečným stavem je, pokud jsou třetí stranou poškozovány přenášené informace, tj. bezpečnostním rizikem je odstranění/modifikace anebo zaslání falešné informace jiným zdrojem, než je vlastní relevantní zdroj informace.

## 2.8 Posuzování shody komponentů a aplikací ITS na bázi ICT

Na základě definovaných cílů „Akčního plánu ITS ČR“ bude posuzování shody komponentů a aplikací na bázi ITS v ČR v krátkém časovém období zavedeno. Cílem zavedení posuzování shody jednotlivých komponentů v architektuře složitých systémů ICT je zabezpečení technických a technologických standardů, které zajistí nejen funkčnost, ale zejména další modulární rozšiřování systémů. Tímto přístupem budou moci být rozšiřovány systémy bez dodatečných finančních nároků na překonání technických bariér a dojde tak k zefektivnění vložených finančních prostředků. Zabezpečení shody pomohou řešit většině subjektů veřejného sektoru problémy nejen technického posouzení, ale také ekonomického hodnocení systémů a služeb systémů na bázi ICT navrhovaných k realizaci. Posuzování shody je v oblasti dopravní telematiky podporováno i evropskými iniciativami a bude se obvíjet ve dvou rovinách.

### 2.8.1 Posuzování shody prostřednictvím tzv. prohlášení o shodě

Cílem této činnosti bude získat souhrn doporučených praktik a postupů, pokrývajících posouzení shody nebo vhodnosti pro použití součástí, aplikací a služeb ITS na bázi ICT zjednodušeným způsobem, tedy prostřednictvím předložením prohlášení.

#### *2.8.1.1 Základní přiblížení*

Prohlášení o shodě je písemné ujištění výrobce nebo dovozce o tom, že výrobek splňuje požadavky technických předpisů platných v ČR a že byl dodržen stanovený postup při posouzení shody.Při uvádění

výrobku na trh v první řadě záleží na skutečnosti, zda tento výrobek spadá do regulované sféry, nebo se jedná o výrobek ze sféry neregulované.

Do neregulované sféry spadají výrobky, které nepředstavují zvýšenou míru ohrožení oprávněného zájmu. Tyto výrobky nepodléhají posuzování shody podle zákona č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů. Pro tyto výrobky nejsou stanoveny zvláštní technické požadavky pro uvádění na trh. Takové výrobky musí splnit pouze obecné požadavky bezpečnosti.

Do regulované sféry jsou naopak řazeny tzv. stanovené výrobky ve smyslu § 12 zákona 22/1997 Sb. Jedná se o výrobky představující zvýšenou míru ohrožení oprávněného zájmu. Tyto výrobky a požadavky na ně jsou určeny prostřednictvím jednotlivých nařízení vlády k provedení zákona o technických požadavcích na výrobky. U těchto výrobků musí být před jejich uvedením na trh posouzena shoda.

Vzhledem k členství České republiky v Evropském společenství je v rámci regulované sféry třeba rozlišovat ještě oblast harmonizovanou a neharmonizovanou. V harmonizované oblasti jsou technické požadavky na výrobky při uvádění na trh stanoveny jednotně pro všechny členské státy sekundárními právními předpisy Evropského společenství (splnění těchto předpisů osvědčuje ES prohlášení o shodě). Tím se zároveň odstraňují překážky ve volném pohybu výrobků v rámci vnitřního trhu v podobě rozdílných technických požadavků v jednotlivých členských státech.

Z hlediska posuzování shody mají zásadní význam zejména následující právní normy:

**Zákon č. 102/2001 Sb., o obecné bezpečnosti výrobků**, stanoví obecný standard, kterému musí všechny výrobky vyhovět z hlediska bezpečnosti a ochrany zdraví pro spotřebitele. Tento zákon např. ukládá povinnost poskytnout spotřebiteli informace o potenciální nebezpečnosti daného výrobku a dále upravuje otázku průvodní dokumentace a označování výrobku.

**Zákon č. 634/1992 Sb., o ochraně spotřebitele**, stanoví povinnost prodávat výrobky v předepsané nebo schválené jakosti, v souladu s cenovými předpisy a ceny při prodeji výrobků správně účtovat. Tento zákon se dále věnuje informační povinnosti prodávajícího, která spočívá zejména v povinnost informovat spotřebitele o vlastnostech prodávaných výrobků a v povinnosti výrobek viditelně a srozumitelně označit. V této souvislosti je třeba pamatovat na to, že veškeré informace včetně návodu musí být v českém jazyce.

**Zákon č. 22/1997 Sb., o technických požadavcích na výrobky**, upravuje stanovování technických požadavků na výrobky, které by mohly ve zvýšené míře ohrozit zdraví nebo bezpečnost osob, majetek nebo životní prostředí, popřípadě jiný veřejný ("oprávněný") zájem. Tento zákon vysvětluje a právně definuje důležité pojmy, jako je výrobek, uvedení výrobku na trh, uvedení výrobku do provozu, výrobce, distributor, technické předpisy a normy, harmonizované technické normy apod. Hlava III tohoto zákona se věnuje státnímu zkušebnictví, certifikaci a činnosti autorizovaných osob. Je zde popsán systém posuzování shody a vysvětleno ke kterým výrobkům musím být vystaveno prohlášení o shodě (osvědčení, že výrobek splňuje požadavky příslušných právních předpisů). V důležitém § 13b tohoto zákona je také obecně zakotvena zásada vzájemného uznávání neharmonizovaných výrobků.

### 2.8.2 Posuzování shody v případě bezpečnostně kritických nebo bezpečnostně relevantních systémů

Posuzování shody v případě bezpečnostně kritických nebo bezpečnostně relevantních aplikací, subsystémů a systémů ITS bude zajištěno činností certifikované laboratoře.

#### *2.8.2.1 Základní přiblížení*

Procesem posuzování shody musí „projít“:

- V případě bezpečnostně kritických nebo bezpečnostně relevantních systémů a aplikací je nutné zajistit jejich spolehlivost, protože chybná funkce systému by mohla mít za následek ohrožení nebo dokonce i zmaření lidských životů.
- V případě aplikací ICT, při nichž chyba ve fungování systému neznamená ohrožení života osob nebo podstatné ohrožení majetku, se předpokládá posouzení shody zjednodušeným způsobem, tedy předložením prohlášení o tom, že jsou splněny stanovené požadavky v příslušném nařízení EK[16]. Tato prohlášení bude posuzovat nestranný a nezávislý vnitrostátní subjekt, který bude určen ze strany státu.

Cílem této části připravovaného procesu je podpořit zřizování nezávislé „Certifikační laboratoře pro ověření shody a pro certifikaci bezpečnostně kritických systémů a aplikací ITS“, která by jako notifikovaná osoba pro posuzování shody s požadavky evropských směrnic a delegovaných aktů:

a) před zahájením projektu na realizaci systému nebo aplikace ICT v dopravě posoudila jeho shodu se stanovenými specifikacemi podle směrnice EU č. 40/2010 a dále s platnými národními a mezinárodními standardy;
b) prostřednictvím této laboratoře garantovala požadovanou úroveň systému nebo aplikace ITS či služby s ohledem na mezinárodní propojitelnost, kvalitu služby a garanci technických parametrů.

Posuzování shody v případě bezpečnostně kritických nebo bezpečnostně relevantních aplikací, subsystémů a systémů ITS činností certifikované laboratoře bude řešeno ve dvou oblastech:

- Zabezpečení informačních vazeb.
- Garance spolehlivosti v celé struktuře aplikace.

[16] Pokud bude podporována evropskou normou

# 3 Vlastní popis předmětu metodiky

Metodika integrace telematických systémů ve veřejné dopravě do systémů organizaci krizového řízení vychází z poznatků řešeného projektu. Přístup k řešení tvorby budoucích informačních vazeb vycházel ze základních teoretických atributů pro tvorbu složitých architektur informačních systémů s položeným důrazem na principy tvorby architektur dopravní telematiky ve veřejné dopravě.

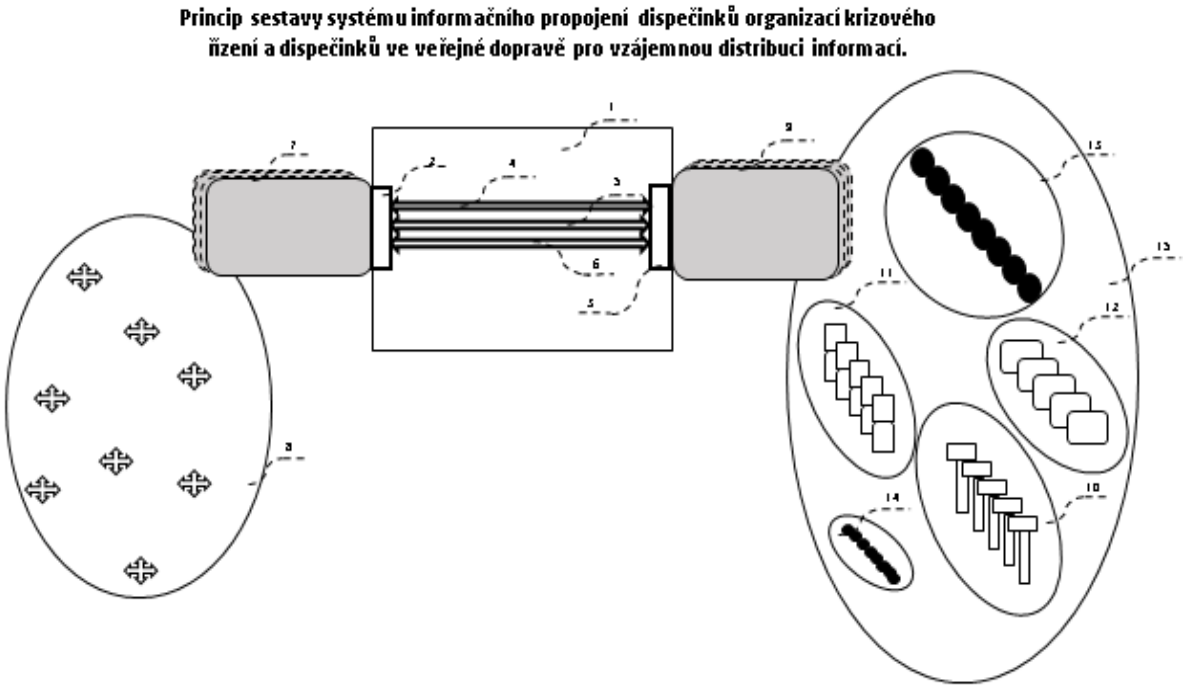
Nosným aspektem ke stanovení obsahu vlastní metodiky je i strategický materiál MD ČR ve vztahu k rozvoji ITS s názvem Akční plán rozvoje inteligentních dopravních systémů (ITS) v ČR do roku 2020 (s výhledem do roku 2050). Důležitým zjištěním je, že vlastní realizaci informačních vazeb nelze uskutečnit přímo bez vložení SW HW prostředků na rozhraní obou systémů. Příčinou je rozdílnost řešení jednotlivých subsystémů zejména v oblasti informační báze, formátů zobrazení, formátů dat apod., jsou však technicky a technologicky řešitelná[17] při dodržení základních zásad.

## 3.1 Fyzická architektura informační vazby

Technické řešení je tvořeno standardizovaným systémem informačního propojení dispečinků organizací krizového řízení a dispečinků ve veřejné dopravě pro vzájemnou přímou distribuci informací zobrazovaných na informačních médiích v systémech pro zabezpečení vyšší bezpečnosti občanů při vzniku krizových situací.

Princip řešení je zobrazen na obr. 3.

Vlastní technické řešení informačního propojení je na obrázku označeno 1.




*Obr. 3.: Schéma sestavy systému informačního propojení dispečinků IZS a dispečinků řízení veřejné dopravy.*

[17] Bylo ověřeno v rámci řešení projektu.

**Popis schématu:**

1. Systém vlastního informačního propojení dispečinků krizového řízení a dispečinků ve veřejné dopravě pro vzájemnou distribuci informací
2. Modul rozhraní informačních vazeb dispečinků organizací krizového řízení
3. Modul rozhraní informačních vazeb dispečinků ve veřejné dopravě
4. Informační obousměrná vazba mezi dispečinky krizového řízení a dispečinky veřejné dopravy pro sdílení dopravních informací krizovými dispečinky
5. Audio informační přímá obousměrná informační vazba mezi dispečinky krizového řízení a veřejné dopravy
6. Obousměrná informační vazba organizování a prezentace textových a audio zpráv bezpečnostního a krizového charakteru na informačních médiích telematiky ve veřejné dopravě
7. Dispečink organizací krizového řízení
8. Systém informačních medií krizového řízení
9. Dispečink organizací ve veřejné dopravě
10. Množina inteligentních zastávkových stojanu s aktivními informačními médii v systému
11. Množina interaktivních informačních stojanů s aktivními informačními médii v systému
12. Množina samostatných informačních tabulí na přestupních uzlech v systému
13. Množina informačních medií v dopravních prostředcích veřejné dopravy v systému
14. Množina ostatních informačních medií v systému
15. Telekomunikační prostředí v systému dispečinků veřejné dopravy

Systém vlastního informačního propojení dispečinků krizového řízení a dispečinků ve veřejné dopravě se tedy vyznačuje tvorbou rozhraní s vloženou inteligencí obou systémů pro zabezpečení vybudování vzájemných informačních vazeb. Tyto vazby zabezpečující informační a technickou interoperabilitu pro vzájemnou distribuci informací na zobrazovací media v obou systémech pomocí vybraných komunikačních prostředků. Uvedené dále v textu pro zjednodušení popisu bude označeno jako „Jádro propojení systémů“.

Uvedené řešení překonává současný stav tím, že doplňuje **stávající systémy** SW a HW prostředky, které vytváří základní informační vazby, přenosové kanály, mezi technologiemi dispečinků, prostřednictvím rozhraní s vloženou inteligencí.

## 3.2 Popis jednotlivých komponent řešení

„Jádro propojení systémů“ zabezpečuje technickou, komunikační a informační propojitelnost systémů organizací krizového řízení a dispečinků ve veřejné dopravě pro zabezpečení vzájemné distribuce informací ve třech rovinách:

I. Informace o aktuální poloze prostředku veřejné dopravy na jednotlivých linkách na informačních mediích organizací dispečinků krizového řízení.

II. Distribuce textových zpráv z dispečinků organizací krizového řízení na informační media ve veřejné dopravě.

III. Zabezpečení přímé hlasové komunikace mezi dispečery organizací krizového řízení a organizací ve veřejné dopravě.

### 3.2.1 Popis informační vazby I. – aktuální poloha

Jedná se o základní informační vazbu. Ta zabezpečuje distribuci informací o aktuální poloze dopravního prostředku linek veřejné dopravy v systému veřejné dopravy na obrazovky organizací krizového řízení. A to prostřednictvím obou rozhraní s vloženou inteligencí. Přičemž informační vazba musí umožnit dispečerům krizového řízení:

- výběr lokalit,
- způsob zobrazení,
- vyslání pokynů pro distribuci takové informace z dispečinku dopravců,

Informační vazba je obousměrná, přičemž vlastní realizace informační vazby prostřednictvím bloků obou modulů rozhraní, může být zabezpečeno prostřednictvím komunikačního kanálu například v privátním komunikačním prostředí prostřednictvím pevné a rádiové sítě, v prostředí magistrátní telekomunikační sítě, pronajatým okruhem nebo vlastním technickým řešením atd. s minimálním požadavkem na kapacitu přenosového kanálu 2Mbit/s, rozvojově 10mbit/s.

### 3.2.2 Popis informační vazby II. – distribuce textových zpráv

Druhá informační vazba zabezpečuje distribuci bezpečnostních a krizových informací v textové podobě z dispečinků organizací krizového řízení. Tyto informace jsou určeny pro zobrazování na informačních médiích telematických prostředků ve veřejné dopravě, jako jsou například:

- inteligentní zastávkové stojany,
- interaktivní informační stojany,
- informační tabule přestupových uzlů,
- informační media ve vozidlech a moderní multimodální aplikace.

Informační vazba je obousměrná, přizpůsobení je realizováno prostřednictvím vložené inteligence obou rozhraní, které musí umožnit potvrzení příjmu zprávy dispečery ve veřejné dopravy a geografický výběr zobrazovacích medií v oblasti, šifrování zpráv a archivaci dat na obou rozhraních., přičemž vlastní realizace komunikačního kanálu může být realizována například v privátním komunikačním prostředí prostřednictvím pevné a rádiové sítě, v prostředí magistrátní telekomunikační sítě, pronajatým okruhem atd. s minimálním požadavkem na kapacitu přenosového kanálu 64kbit/s.

### 3.2.3 Popis informační vazby III. – přímé komunikační propojení dispečinků

Třetí informační vazba zabezpečí přímý komunikační kanál mezi dispečinky organizací krizového řízení a dispečinky ve veřejné dopravě pro přímou fónickou komunikaci prostřednictví rozhraní obou systémů s vloženou inteligencí zabezpečující přizpůsobení na technologie fónické komunikace dispečinků s možností archivace a šifrování komunikace, přičemž vlastní realizace komunikačního kanálu může být realizována například v privátním komunikačním prostředí prostřednictvím pevné a rádiové sítě, v prostředí magistrátní telekomunikační sítě, pronajatým okruhem atd. s minimálním požadavkem na kapacitu přenosového kanálu 64kbit/s.

## 3.3 Provozní cíle „jádra propojení systémů“

Pro stanovení postupů pro projektování, které však také budou nosné pro zabezpečení prokázání shody systému, je nutno definovat obecně „rozvojový“ potenciál řešení. Nadřazené cíle definují výkonnostní charakteristiky, kde "jádro propojení systémů" musí prokázat tyto základní vlastnosti:

- Flexibilnost: Návrh "jádra propojení systémů“ musí být schopen přizpůsobit se vnějším změnám bez nutnosti přepracování návrhu.
- Rozšiřitelnost: Implementace "jádra propojení systémů" musí brát v potaz budoucí růst. Rozšíření mohou být dosažena přidáním nových funkcí nebo změnou funkce, které existuje v době, kdy je rozšíření potřebné.
- Škálovatelnost: "jádro propojení systémů" musí být schopno zvládnout rostoucí množství práce pohodlným způsobem, nebo být rozšířen tak, aby zvládnul rostoucí množství práce, aniž by bylo nutné systém přepracovat.
- Udržovatelnost: "jádro propojení systémů" musí být udržovatelné takovým způsobem, aby se minimalizoval čas potřebný na údržbu, s nejnižšími náklady a použití podpůrných prostředků. Přesněji řečeno, představy opatření, které je třeba definovat, jsou:
    - Pravděpodobnost, že daná položka v rámci "jádra propojení systémů" bude obnovena do provozního stavu v daném časovém období, kdy se údržba provádí, jak bylo navrženo.
    - Pravděpodobnost, že údržba není zapotřebí více než na dané množství časů v daném období, kdy je provozován systém, jak byl navržen.
    - Pravděpodobnost, že náklady na údržbu na systém nesmí překročit určenou hodnotu, když je systém provozován a udržován, jak bylo navrženo.
- Rozmístitelnost: "jádro propojení systémů" musí být schopno nasazení v existujících prostředích jak veřejné dopravy, tak IZS, bez nutnosti výměny stávajících systémů, s cílem poskytnout měřitelné zlepšení.

## 3.4 Specifikace systémových parametrů systému

Systémové požadavky, respektive systémové parametry, v případě tvorby složitých systémů ICT s nutnosti tvorby nových rozhraní zabezpečující transformaci rozdílných standardů propojovaných informačních prostředí, jsou důležitým prostředkem pro zabezpečení funkčnosti systému. Hodnoty systémových parametru jednoduše a transparentně vyjadřují požadavky na systém a to v celé struktuře. Projektantovi jasně definují požadavky na technické řešení. Informační vazba mezi dispečinky organizací krizového řízení a dispečinky ve veřejné dopravě bude předmětem procesu prokazování shody. I v této oblasti sehrávají systémové parametry rozhodující roli[18]. Základní teoretické rámce v této oblasti byly definovány v části 2 této metodiky, v této části bude provedeno vlastní stanovení hodnot systémových parametrů.

### 3.4.1 Atributy stanovení hodnot

Stanovení vlastních hodnot systémových parametrů předchází rozklad uživatelských požadavků.

[18] Dnes je to již v letecké a železniční dopravě.

#### 3.4.1.1 Definice požadavku

Požadavkem je schopnost, která je identifikována pro dosažení určeného cíle nebo vyřešení daného problému, zvláště v tomto případě, musí být podporováno "jádro propojení systémů". Popisuje, co je požadováno, a zároveň se vyhýbá implementačním specifikům, nebo způsobu provedení.

Každý požadavek je třeba identifikovat jednoznačně; obsahuje popis a odůvodnění. Odůvodnění mohou obsahovat příklady toho, jak mohou být schopnosti systému vykonávány.

Pro „jádro propojení systémů“ jsou určeny dva typy požadavků:

- Požadavky uživatelů, které popisují schopnost požadovanou uživatelem, aby pro daného uživatele vedly k dosažení cíle,
- Systémové požadavky, které popisují schopnost „jádra propojení systémů“ splnit požadované požadavky uživatelů.

Všechny typické požadavky, uvedené níže, jsou popsány z pohledu "jádra propojení systémů".

#### 3.4.1.2 Proces identifikace požadavků na „jádro propojení systémů“

Každý proces implementace bude muset spolupracovat a diskutovat konkrétní požadavky na "jádro propojení systémů", které má být realizováno, nebo revidováno. Požadavky a koncepční cíle samosprávy nebo entity zavádějící "jádro propojení systémů" budou prioritní úvahou, ale je třeba se všemi zúčastněnými aktéry konzultovat, a je třeba, aby se konečné navrhované řešení rozložilo do jednotlivých řešení. Doporučuje se formální proces s formální zpětnou vazbou a hodnocením.

Tato část uvádí typické požadavky, které formulují definici "jádra propojení systémů", včetně názvu, popisu a zdůvodnění každého požadavku.

Všechny požadavky "jádra propojení systémů" jsou zaměřeny na poskytování služeb, které se v určitém okamžiku použijí na podporu aplikací.

Následující požadavky jsou typické a je třeba je vzít v úvahu při rozvoji koncepce pro konkretizaci všech funkcí "jádra propojení systémů" (i když může v jednotlivých případech uplatňovat různé způsoby naplnění dané potřeby, zakotvené v požadavku). Pro každý z těchto požadavků, budou uživatelé muset zadat:

- Cíl
- Kritéria
- Specifikace prostředků pro naplnění požadavku
- Prostředky pro měření úspěchu / selhání
- Postupy v případě selhání.

#### 3.4.1.3 Seznam požadavků

Sekvence seznamu, který následuje, neznamená stanovení priorit, které se mohou lišit případ od případu:

##### 3.4.1.3.1 Požadavek: Navázání důvěry s jádrem propojení systémů

"Jádro propojení systémů" potřebuje proces navázání důvěry s uživateli systému. Takové vztahy důvěryhodnosti jsou nutné, aby "jádro propojení systémů" zajistilo, že uživatelé systému jsou těmi, za které je systém pokládá, a proto důvěřuje zdroji dat i datům, které z nich obdrží. Formulujte cíle "navázání důvěry", kritéria, prostředky k jejich dosažení, prostředky k měření úspěchu / neúspěchu a postupy v případě selhání.

#### 3.4.1.3.2 Požadavek: Zrušení důvěry s jádrem propojení systémů

"Jádro propojení systémů" musí být v případě potřeby schopno zrušit vztah důvěryhodnosti, který má se svými uživateli systému. Důvěryhodný uživatel může v systému pracovat takovým způsobem, který naznačuje, že by již neměl být důvěryhodný, a v tomto případě musí "jádro propojení systémů" mít způsob, jak tuto důvěru zrušit. Určete cíle "zrušení důvěry“, kritéria prostředky k jejich dosažení, prostředky k měření úspěchu / neúspěchu a postupy v případě selhání.

#### 3.4.1.3.3 Požadavek: Důvěra uživatele systému

"Jádro propojení systémů" také potřebuje zajistit proces nastolení důvěry mezi uživateli systému. Takové vztahy důvěryhodnosti jsou nutné, aby uživatelé systému si mohli být jisti, že ostatní uživatelé systému jsou těmi, za které se vydávají, a uživatel tak může důvěřovat zdroji dat a datům z nich přijatých. Formulujte cíle "důvěry uživatelů systému“, kritéria, prostředky k jejich dosažení, prostředky k měření úspěchu / neúspěchu a postupy v případě selhání. Subsystém řízení důvěry uživatelů řídí důvěru mezi uživateli systému a mezi nimi a jádrem propojení systémů tím, že poskytuje digitální certifikáty, které mohou uživatelé systému použít k prokázání, že jsou legitimní uživatelé systému. Poskytuje digitální certifikáty kvalifikovaných uživatelům a přijímá oznámení o špatném chování uživatelů z managementu chování a ruší certifikáty špatně se chovajícím uživatelům. Také udržuje seznam zrušených certifikátů.

#### 3.4.1.3.4 Požadavek: zrušení důvěry uživatele systému

"Jádro propojení systémů" musí poskytovat možnost zrušení těchto vztahů důvěryhodnosti mezi uživateli, pokud je to třeba. Důvěryhodný uživatel může v systému pracovat takovým způsobem, který naznačuje, že by již neměl být důvěryhodný, v tomto případě "jádro propojení systémů" musí mít způsob, jak provede zrušení důvěry mezi uživateli systému. Formulujte cíle "zrušení důvěry uživatelů systému“, kritéria, prostředky k jejich dosažení, prostředky k měření úspěchu / neúspěchu a postupy v případě selhání.

#### 3.4.1.3.5 Požadavek: Společný časový základ a synchronizace

"Jádro propojení systémů" a uživatelé systému potřebují pracovat ve společném časovém základu. Koordinace času mezi vnitřními systémy, které provozují "jádro propojení systémů", zabraňuje chybám vnitřní synchronizace a umožňuje časově citlivé interakce s uživateli systému. Formulujte cíle "časové synchronizace“, kritéria, prostředky k jejich dosažení, prostředky k měření úspěchu / neúspěchu a postupy v případě selhání.

#### 3.4.1.3.6 Požadavek: Žádost o data

"Jádro propojení systémů" musí poskytnout mechanismus pro konzumenty dat, aby mohli požadovat data, která jsou vytvářena poskytovateli dat. Jedná se o jednu žádost o předplatné (subskripci) na určitý typ dat, a následnou změnu požadavku na změnu datových typů nebo parametrů předplatného. Parametry zahrnují frekvenci poskytování dat, typ dat a místo, ve kterém byla data vytvořena. To umožňuje distribuci anonymně poskytovaných údajů zúčastněným konzumentům dat, aniž by musely vstoupit do vztahu s poskytovateli dat. Formáty žádosti o data musí umožnit konzumentům dat, aby byli schopni rozlišovat a přijímat pouze takové typy dat, které sami požadovali. Například to zahrnuje typ dat, geografický rozsah, frekvenci a rozsah dat.

#### 3.4.1.3.7 Požadavek: Poskytování / distribuce dat

"Jádro propojení systémů" musí poskytovat informace poskytovatelům dat, které jim umožní přenášet data cílovým konzumentům. Minimálně musí charakteristiky dat zahrnovat typ, četnost a místo, kde byla data generována, takže uživatelé, kteří mají požadovaná data (viz požadavek: žádost o data) mohou rozlišovat mezi dostupnými daty. Tento požadavek umožňuje poskytovatelům dat nasměrovat data, která vytváří, konzumentům dat, a slouží jako poskytovatel dat na základě žádosti o dodávku dat. To může

podporovat širokou škálu aplikací, včetně těch, které se zaměřují na poskytování dat uživatelům. Formulujte cíle "poskytování dat“, kritéria, prostředky k jejich dosažení, prostředky k měření úspěchu / neúspěchu a postupy v případě selhání. Subsystém distribuce dat má centralizované a decentralizované komponenty. Udržuje záznamy v centrálním registru, který obsluhuje každé zařízení, které se k odběru dat přihlásilo. Každé zařízení pak může posílat data do vozidel ve svém komunikačním rozsahu abonentům. A takto podporuje mechanismy distribuce dat více směry (multiple-distribution), včetně zdroj-cíl a publish-subscribe. To znamená, že musí řídit anonymizaci a být schopen zabalit (přebalit) data, která obdrží od poskytovatelů dat, odstraňovat informace o hlavičce zdroje při zachování obsahu zprávy. Potom odešle přebalený vlastní obsah zprávy jejím abonentům.

#### 3.4.1.3.8 Požadavky: Předávání dat

"Jádro propojení systémů" musí poskytnout mechanismus pro distribuci dat, která se vytváří uživatelem systému působícím jako poskytovatel dat a je požadovaná jiným uživatelem systému. "Jádro propojení systémů" musí poskytovat spíše tento distribuční mechanismus, než se spoléhat na jednotlivé vztahy poskytovatel-odběratel, protože více odběratelů může chtít mít přístup ke stejným údajům. Například tím, že "jádro propojení systémů" data distribuuje, jsou uživatelé systému osvobozeni od požadavku na vícenásobný přenos dat. Dále, některé údaje, které mohou být důležité pro správné fungování povinných aplikací, jako jsou údaje, které podporují geo-polohu vozidel veřejné dopravy, data o čase, z nichž všechny budou pravděpodobně ve většině případů pocházet z jediného zdroje a budou muset být rozděleny velkému počtu uživatelů systému. Kromě toho mohou uživatelé systému komunikovat přes omezené zdroje komunikačních spojení, takže redistribuce dat "jádrem propojení systémů" fakticky snižuje potenciální zátěž na těchto spojeních. Formulujte cíle "předávání dat“, kritéria, prostředky k jejich dosažení, prostředky k měření úspěchu / neúspěchu a postupy v případě selhání.

#### 3.4.1.3.9 Požadavky: Síťová konektivita

"Jádro propojení systémů" potřebuje připojení k Internetu. To umožňuje "jádru propojení systémů" poskytovat služby pro všechny uživatele systému, kteří jsou schopni připojit se k internetu. Formulujte cíle "síťová konektivita“, kritéria, prostředky k jejich dosažení, prostředky k měření úspěchu / neúspěchu a postupy v případě selhání.

#### 3.4.1.3.10 Požadavek: Ochrana dat "jádra propojení systémů"

"Jádro propojení systémů" musí chránit data, která spravuje, před neoprávněným přístupem. Tím je zajištěno, že informace, které má "jádro propojení systémů" k dispozici, mohou obsahovat citlivá data o uživatelích systému, a taková jsou přístupná pouze oprávněným uživatelům. Formulujte cíle "ochrana dat jádra propojení systémů“, kritéria, prostředky k jejich dosažení, prostředky k měření úspěchu / neúspěchu a postupy v případě selhání.

#### 3.4.1.3.11 . Požadavek: Ochrana dat

"Jádro propojení systémů" musí být schopno chránit data, která zpracovává, před neoprávněným přístupem. Tento požadavek je nutný pro podporu aplikací, které si vyměňují citlivé informace, jako jsou identifikace osob či finanční informace, které, pokud porušena, by mohly ohrozit soukromí nebo finanční záznamy uživatele. Formulujte cíle "ochranu údajů“, kritéria, prostředky k jejich dosažení, prostředky k měření úspěchu / neúspěchu a postupy v případě selhání.

#### 3.4.1.3.12 . Požadavek: Zachování anonymity

"Jádro propojení systémů" musí být navrženo tak, aby cílilo na zachování anonymity uživatelů systému, kteří využívají jeho služeb, jako svůj normativní provozní modus operandi, a odchýlit se od toho konceptu lze jen se souhlasem uživatele (obvykle výměnou za ztrátu anonymity je uživatel schopen získat další výhody, a za těchto okolností dostává silnou ochranu soukromí). To zajišťuje, že uživatelé systému komunikující s "jádrem propojení systémů", kteří si přejí zůstat v anonymitě, nebudou mít porušenu svou anonymitu v důsledku komunikace s "jádrem propojení systémů". Formulujte cíle "zachování anonymity“,

kritéria, prostředky k jejich dosažení, prostředky k měření úspěchu / neúspěchu a postupy v případě selhání.

#### 3.4.1.3.13 . Požadavek: Síťové služby

Subsystém síťové služby poskytuje management pro komunikační vrstvy zdrojů. Subsystém síťové služby je také zodpovědný za ochranu systému před počítačovými hrozbami.

#### 3.4.1.3.14 . Požadavek: Připojení k privátní síti

"Jádro propojení systémů 'musí být schopno se připojit k příslušným privátním sítím. To umožňuje "jádru propojení systémů" poskytovat služby všem oprávněným uživatelům systému, kteří poskytují připojení k privátní síti do "jádra propojení systémů". Určení toho, jaké sítě jsou "vhodné", bude důležitým úkolem při vývoji jakýchkoliv specifikací a provozních pokynů "jádra propojení systémů". Formulujte cíle "připojení k privátní síti“, kritéria, prostředky k jejich dosažení, prostředky k měření úspěchu / neúspěchu a postupy v případě selhání.

#### 3.4.1.3.15 . Požadavek: Směrování privátní sítě

"Jádro propojení systémů" může potřebovat směrovat komunikaci mezi ostatními "základními systémy" a uživateli systému, kdy jeden nebo oba ze zúčastněných stran při komunikaci je připojen do "jádra propojení systémů" prostřednictvím privátní sítě. To umožňuje uživatelům systému spojených privátní sítí komunikovat s aplikacemi provozovanými centrem, a také usnadňuje operace zálohování mezi "základními systémy". Formulujte cíle "směrování privátní sítě“, kritéria, prostředky k jejich dosažení, prostředky k měření úspěchu / neúspěchu a postupy v případě selhání.

#### 3.4.1.3.16 Požadavek: Správa a management autorizace uživatelských oprávnění

"Jádro propojení systémů" je třeba řídit autorizačními mechanismy pro definování rolí, odpovědností a oprávnění pro uživatele systému. To umožňuje "jádru propojení systémů" stanovit provozní prostředí, kde mohou různí uživatelé systému mít různé možnosti, pokud jde o přístup k službám jádra propojení systémů a interakci s druhými uživateli. Stanovte cíle "managementu autorizace“, kritéria, prostředky k jejich dosažení, prostředky k měření úspěchu / neúspěchu a postupy v případě selhání.Tento subsystém ověřuje, zda je uživatel systému oprávněn provést opatření požadované v obsahu zprávy. Proto udržuje status uživatelů a provozovatelů systémů, udržuje jejich povolené chování (publikování, přihlášení, akce povoleny na vyžádání, administrátor, atd.).

#### 3.4.1.3.17 Požadavek: Ověření autorizace

Kde je potřeba, "jádro propojení systémů" musí být schopno ověřit, že uživatelé systému (a provozní pracovníci "jádra propojení systémů") jsou oprávněni provádět danou operaci. To umožňuje "jádru propojení systémů" omezit operace na ty uživatele, jimž je povoleno tyto operace používat. Formulujte cíle "ověření autorizace“, kritéria, prostředky k jejich dosažení, prostředky k měření úspěchu / neúspěchu a postupy v případě selhání.

#### 3.4.1.3.18 Požadavek: Řízení nevhodného chování (vedení přečinů)

"Jádro propojení systémů" musí být schopno identifikovat uživatele systému, kteří se nechovají v souladu s pravidly. Nevhodní aktéři nemusí mít nutně zlé úmysly; může se jednat o vadné zařízení, které se může rušit s jiným systémem uživatelů. Identifikace nevhodných aktérů umožňuje provedení následných kroků k ochraně integrity všech uživatelů sdílejících oblast dopravy. Formulujte cíle "řízení nevhodného chování“, kritéria, prostředky k jejich dosažení, prostředky k měření úspěchu / neúspěchu a postupy v případě selhání. Subsystém řízení nevhodného chování analyzuje zprávy v každém zařízení a odešle podezřelé zprávy na centrální BackOffice, který pak může identifikovat, zda uživatelé pracují mimo svá přidělená oprávnění. Identifikuje podezřelé požadavky a udržuje záznam o uživatelích, kteří poskytují

nepravdivé nebo zavádějící údaje, brání ostatním uživatelům, nebo pracují mimo rozsah svého oprávnění. Subsystém určí, kdy má dojít ke zrušení svěřených práv takovým hlášeným uživatelům.

#### 3.4.1.3.19 Požadavek: Geografické vysílání (geovysílání)

"Jádro propojení systémů" musí poskytovat informace nezbytné pro uživatele systému, kteří chtějí komunikovat se skupinami uživatelů systému v určitém místě. Tato funkce umožňuje uživatelům systému zaměřit se na ty uživatele, nacházející se v určité oblasti, pro předání informací, které chtějí distribuovat, aniž by museli posílat jednotlivé zprávy každému příjemci.

#### 3.4.1.3.20 Požadavek: Monitorování statutu služby "jádra propojení systémů"

"Jádro propojení systémů" musí být schopno monitorovat stav služeb "jádra propojení systémů" a poskytovat přesné informace o stavu uživatelům systému. "Jádro propojení systémů“ pak může informovat provozní personál "jádra propojení systémů", kdy služba funguje v abnormálním nebo omezeném módu. Kromě toho nemusejí uživatelé systému mít přístup k službám "jádra propojení systémů" a mohou chtít vědět, kde a kdy by mohli očekávat, že služba bude opět zpřístupněna. Stanovte cíle "monitorování statutu služby "jádra propojení systémů"“, kritéria, prostředky k jejich dosažení, prostředky k měření úspěchu / neúspěchu a postupy v případě selhání.

Subsystém monitorovací služby monitoruje stav základních funkcí, rozhraní a komunikačních sítí. Monitoring pravděpodobně bude mít decentralizované i centralizované komponenty.

#### 3.4.1.3.21 Požadavek: Monitorování provozního výkonu systému

„Jádro propojení systémů" bude muset mít organizovaný a měřitelný systém pro sledování jeho výkonu. To bude pravděpodobně zahrnovat stav rozhraní a služeb a metriky pro poptávku po službách a řešení těchto požadavků. Sledování výkonu služeb a rozhraní "jádra propojení systémů" musí poznat, kdy systém pracuje správně, a odhadnout, kdy se výkon systému blíží své kapacitě, a tak může učinit opatření, aby se zabránilo systému ze stavu neposkytování služby, např. stanovením maximálního počtu transakcí za sekundu, nebo omezením šířky pásma interní komunikace, a dát tak uživatelům důvěru v celý systém. Stanovte cíle "monitorování provozního výkonu systému", kritéria, prostředky k jejich dosažení, prostředky k měření úspěchu / neúspěchu a postupy v případě selhání.

#### 3.4.1.3.22 Požadavek: nezávislost "jádra propojení systémů"

"Jádro propojení systémů" musí být strukturováno, nasazeno, spravováno a provozováno způsobem, který poskytuje služby "jádra propojení systémů" všem uživatelům systému v rámci jeho provozního rozsahu, a to způsobem, který je vidět, že je fér. Toho lze nejčastěji dosáhnout, pokud "jádro propojení systémů" běží samostatně. Nicméně, v některých případech může samospráva potřebovat nebo chtít kontrolovat a případně i ovládat "jádro propojení systémů". V tomto případě je třeba mít jasně definované a veřejně známé cíle, a otevřený systém "auditu" s pravidelným auditem a podáváním zpráv jak tvůrcům, tak i uživatelům systému. Stanovte cíle "nezávislost jádra propojení systémů", kritéria, prostředky k jejich dosažení, prostředky k měření úspěchu / neúspěchu a postupy v případě selhání.

#### 3.4.1.3.23 Požadavek: interoperabilita "jádra propojení systémů"

V ideálním případě musí "jádro propojení systémů" poskytovat služby takovým způsobem, že když se mobilní uživatel přesune do oblasti jiného "jádra propojení systémů", jejich rozhraní do původního "jádra propojení systémů" stále funguje. To je důležité v situaci, kdy existuje několik "klíčových systémů" v rámci jedné samosprávy nebo skupiny samospráv v Takové nastavení pomáhá zvládat očekávání uživatelů a pomáhá zajistit, že když se mobilní uživatel přihlásí ke službě nebo si nainstaluje aplikaci, je uživatelská zkušenost konzistentní napříč několika "jader propojení systémů". Stanovte cíle "interoperabilita jádra propojení systémů", kritéria, prostředky k jejich dosažení, prostředky k měření úspěchu / neúspěchu a postupy v případě selhání.

#### 3.4.1.3.24 Požadavek: vzájemná závislost "jader propojení systémů"

"Jádro propojení systémů" musí být schopno pracovat v koordinaci s dalšími "jádry systému". Tím je zajištěno, že základní systémové služby poskytují informace, které jsou v souladu s informacemi dodanými jinými "jádry systému", které pomohou vyhnout se rozporům a nesouladu mezi klíčovými systémy a mezi systémovými uživateli interagujícími s několika "jádry systému". To bude do značné míry dosaženo vývojem a dodržováním mezinárodních norem. Stanovte cíle "vzájemné závislosti jader systému", kritéria, prostředky k jejich dosažení, prostředky k měření úspěchu / neúspěchu a postupy v případě selhání.

### 3.4.2 Kvantifikace hodnot systémových parametrů

Kvantifikace hodnot systémových parametrů vychází z výše uvedeného rozkladu uživatelských požadavků. Uživatelské požadavky jsou obrazem konkrétního prostředí. Při stanovení hodnot systémových parametrů je důležité si uvědomit přímé vazby hodnot systémových parametrů s ekonomikou řešení. Vysoká hodnota ovlivní výrazně cenu řešení v investiční i provozní oblasti. Na druhé straně nízké hodnoty „degradují informaci jako takovou a naruší garanci služby systému. Práce se systémovými parametry má tedy také významný ekonomický rozměr. Čím vyšší požadavek, tím vyšší náklady na dopravně-telematický systém a naopak. Problematiku ekonomické úrovně výstavby systému je třeba sledovat již ve vývoji a v návrhu, protože v této oblasti se dělají největší chyby, které ve své podstatě vedou k plýtvání veřejnými prostředky. Například - zbytečně je kladen důraz na kvalitu pořízení informace v mobilním prostředku, na bráně mýtného systému atd., kterou potom přenášíme do centra naprosto nevhodným komunikačním prostředím. Informace nedorazí včas, je zkreslená atd., nedá se již dále využít. Stanovení hodnot systémových parametrů musí zohlednit tato konstatování.

Vlastní stanovení hodnot systémových parametrů je provedeno odborným odhadem. Pro odborný odhad byly použity následující atributy získané v průběhu řešení projektu:

- Hodnocení uživatelských potřeb prostředí[19] - dle výše uvedených zásad
- Analýza stávající úrovně technického řešení:
  - Telematických systémů ve veřejné dopravě
  - Informačních systémů organizací krizového řízení
  - Vše ve vazbě na hodnoty systémových parametrů
- Ekonomických atributů – s orientací na minimalizaci vstupních pořizovacích nákladů a jednoduchý provozní servis.
- Minimalizace zásahů do stávajícího technického řešení[20]

#### *3.4.2.1 Informační vazba I*

**SW a blok HW rozhraní – krizové řízení, veřejná doprava**

- kontinuita = 99,95%,
- Integrita = 2s,
- spolehlivost = 99,95%.

**Přenos informací, komunikační prostředí**

- Aktivační doba dostupnosti služby = 2s
- Dostupnost služby (např. virtuálního okruhu) = 99,95%

[19] Konkrétně Brno a JMK, ověřeno prakticky na celém území ČR
[20] Ekonomický a legislativní atribut

- Doba obnovení služby - MTTR (Mean Time to Restore) = 5s
- Zpoždění = 1s
- Ztráta paketů = 99,95%

#### 3.4.2.2 Informační vazba II.

**SW a blok HW rozhraní – krizové řízení, veřejná doprava**

- kontinuita = 99,95%,
- Integrita = 2s,
- spolehlivost = 99,95%.

**Přenos informací, komunikační prostředí**

- Aktivační doba dostupnosti služby = 2s
- Dostupnost služby (např. virtuálního okruhu) = 99,95%
- Doba obnovení služby - MTTR (Mean Time to Restore) = 5s
- Zpoždění = 1s
- Ztráta paketů = 99,95%

#### 3.4.2.3 Informační vazba III.

**SW a blok HW rozhraní – krizové řízení, veřejná doprava**

- kontinuita = 99,55%,
- Integrita = 2s,
- spolehlivost = 99,55%.

**Přenos informací, komunikační prostředí**

- Aktivační doba dostupnosti služby = 5s
- Dostupnost služby (např. virtuálního okruhu) = 99,5%
- Doba obnovení služby - MTTR (Mean Time to Restore) = 5s
- Zpoždění = 2s

#### 3.4.2.4 Požadavky na bezpečnost dat a ochrana systému

- ochrana vstupů heslem,
- ochrana dat v databázích,
- šifrování bezpečnostních sdělení - pokud bude využívána:
  - webovská aplikace
  - veřejné komunikační prostředí
  - rádiové komunikační prostředí – i vlastní

## 3.5 Posouzení shody

Systém informačního propojení dispečinků organizací krizového řízení a dispečinků ve veřejné dopravě pro vzájemnou přímou distribuci informací zobrazovaných na informačních médiích v systémech pro zabezpečení vyšší bezpečnosti občanů při vzniku krizových situací je v souladu s předpokládaným rozvojem ICT v ČR. Je v souladu s cíli „Akčního plánu ITS“, ale s principy tvorby národní architektury ITS. Organizace krizového řízení v souladu s těmito principy a cíli jsou z množiny definovaných organizací s „okolí“ architektury ITS v dopravě.

Citovaná informační vazba bude tedy součástí architektury dopravně telematických systémů v příslušné městské, příměstské a regionální oblasti. „Akční plán“ zejména pro garanci rozvojového potenciálu v souladu s evropskými iniciativami definuje nutnost zabezpečení procesů spojenou s garancí služeb. Posouzení shody je již zavedeným procesem pro různé výrobky či produkty dle jednotlivého oboru. Specifikace pro oblast dopravy, respektive dopravní telematiku nebyla určena.

V kapitole 2 byl popsán předpokládaný vývoj. Ten se bude ubírat dvěma směry:

A. Posuzování shody prostřednictvím tak zvaného „prohlášení o shodě“.
B. Posuzování shody v případě bezpečnostně kritických nebo bezpečnostně relevantních systémů

V této kapitole budou popsány procesy pro jednotlivé směry posuzování shody ve vztahu k systému informačního propojení dispečinků organizací krizového řízení a dispečinků ve veřejné dopravě.

### 3.5.1 Posuzování shody prostřednictvím tzv. prohlášení o shodě

Posuzování shody nebo vhodnosti pro použití součástí, aplikací a služeb ITS na bázi ICT se provádí zjednodušeným způsobem, tedy prostřednictvím předložením prohlášení. Základní Obsah „prohlášení o shodě je dán příslušnými zákonnými normami. Do regulované sféry jsou naopak řazeny tzv. stanovené výrobky ve smyslu § 12 zákona 22/1997 Sb. Jedná se o výrobky představující zvýšenou míru ohrožení oprávněného zájmu. Tyto výrobky a požadavky na ně jsou určeny prostřednictvím jednotlivých nařízení vlády k provedení zákona o technických požadavcích na výrobky. U těchto výrobků musí být před jejich uvedením na trh posouzena shoda. Základní zákonné normy:

- **Zákon č. 102/2001 Sb., o obecné bezpečnosti výrobků**
- **Zákon č. 634/1992 Sb., o ochraně spotřebitele**
- **Zákon č. 22/1997 Sb., o technických požadavcích na výrobky**

#### *3.5.1.1 Specifikace obsahu dokumentu*

Kromě základních údajů plynoucí ze zákonných norem bude dokument obsahovat specifika oborové. Ve vztahu k navrhovanému systému informačního propojení se jedná o potvrzení základních funkcí vazeb a jejich garancí. Dokument musí obsahovat rozklad v následujících oblastech[21]:

**1. Požadavek: Navázání důvěry s jádrem propojení systémů**
**2. Požadavek: Zrušení důvěry s jádrem propojení systémů**
**3. Požadavek: Důvěra uživatele systému**
**4. Požadavek: zrušení důvěry uživatele systému**
**5. Požadavek: Společný časový základ a synchronizace**
**6. Požadavek: Žádost o data**
**7. Požadavek: Poskytování / distribuce dat**
**8. Požadavky: Předávání dat**
**9. Požadavky: Síťová konektivita**
**10. Požadavek: Ochrana dat "jádra propojení systémů"**
**11. Požadavek: Ochrana dat**
**12. Požadavek: Zachování anonymity**
**13. Požadavek: Síťové služby**

[21] Blíže popsáno v kapitole 3.4.1.3

**14. Požadavek: Připojení k privátní síti**

**15 Požadavek: Směrování privátní sítě**

**16 Požadavek: Správa a management autorizace uživatelských oprávnění**

**17. Požadavek: Ověření autorizace**

**18. Požadavek: Řízení nevhodného chování (vedení přečinů)**

**19. Požadavek: Geografické vysílání (geovysílání)**

**20. Požadavek: Monitorování statutu služby "jádra propojení systémů"**

**21. Požadavek: Monitorování provozního výkonu systému**

**22. Požadavek: nezávislost "jádra propojení systémů"**

**23. Požadavek: interoperabilita "jádra propojení systémů"**

**24. Požadavek: vzájemná závislost "jader propojení systémů"**

### *3.5.1.2 Systémové parametry v „prohlášení o shodě“.*

Pokud budou určeny hodnoty systémových parametrů v příslušné architektuře ITS řešené oblasti, musí dokument obsahovat i rozklad splnění těchto hodnot navrhovaným řešením. Základem pro rozklad je teorie spolehlivosti. Možný přístup:

Základ teorie vychází z teorie pravděpodobnosti. Posouzení, že výběr je správný, pokud události jsou naprosto náhodné, nemají historickou paměť. Stejně tak počet závad za časovou jednotku je konstantní.

Pokud označíme:
R(t) – je spolehlivost
F(t) - je pravděpodobnost, že systém bude mít závadu v době t, potom tedy platí:

- F(t) = nespolehlivost systému)

Můžeme matematicky vyjádřit:

$R(t) = e^{-\lambda t}$ , t≥0 (16)

$F(t)= 1 – R(t) = 1 - e^{-\lambda t}$ , t≥0 (17)

Kde:

$\boldsymbol{\lambda}$ = Četnost závad (měla by být konstantní), představuje průměrný počet závad za jednotku času;

**Příklad:**

*Hodnota MTBF kterou poskytl dodavatel = 60 000 hodin. Dosadíme do vzorců.*

$$\boldsymbol{\lambda} = \frac{1}{MTBF} = 1{,}667e - 5$$

$\boldsymbol{R_{display}}$**(t)** = $e^{-\lambda t} = e^{-(1{,}667e-5)\,t}$ *u(t)*

$\boldsymbol{F_{display}}$**(t)** = $1 - R_{palina}(t)$ =

$= (1 - e^{-(1{,}667e-5)\,t})$ u(t)

Uvedený postup můžeme uplatnit pro posouzení spolehlivosti všech prvků v systému. Potom vychází pravděpodobnost, že alespoň (n-k) prvků v systému pracuje správně, se vyjádří dle následujícího vzorce:

$$\boldsymbol{R_{displays\ k,n}}\textbf{(t)} = \sum_{i=0}^{k} \binom{n}{i} p^i * (1-p)^{n-i} = \sum_{i=0}^{k} p(i) \qquad (18)$$

Rozklad spolehlivosti systému dle systémového parametru spolehlivosti je použitelný i pro rozklad dalších parametru například kontinuity systému.

### 3.5.2 Posuzování shody v případě bezpečnostně kritických nebo bezpečnostně relevantních systémů

Pokud bude systém informačního propojení dispečinků organizací krizového řízení a dispečinků ve veřejné dopravě pro vzájemnou přímou distribuci informací zobrazovaných na informačních médiích v systémech pro zabezpečení vyšší bezpečnosti občanů při vzniku krizových situací bude zařazen do působení následujících definic:

- V případě bezpečnostně kritických nebo bezpečnostně relevantních systémů a aplikací je nutné zajistit jejich spolehlivost, protože **chybná funkce systému by mohla mít za následek ohrožení nebo dokonce i zmaření lidských životů.**
- V případě aplikací ICT, při nichž chyba ve fungování systému neznamená ohrožení života osob nebo podstatné ohrožení majetku, se předpokládá posouzení shody zjednodušeným způsobem, tedy předložením prohlášení o tom, že jsou splněny stanovené požadavky v příslušném nařízení EK. Tato prohlášení bude posuzovat nestranný a nezávislý vnitrostátní subjekt, který bude určen ze strany státu.

Posuzování shody v tomto případě bude zajišťováno činností certifikované laboratoře. Posuzování shody se předpokládá ve dvou oblastech:

- Zabezpečení informačních vazeb.
- Garance spolehlivosti v celé struktuře aplikace.

Certifikační laboratoře pro ověření shody a pro certifikaci bezpečnostně kritických systémů a aplikací ITS“, která by jako notifikovaná osoba pro posuzování shody s požadavky evropských směrnic a delegovaných aktů:

- před zahájením projektu na realizaci systému nebo aplikace ICT v dopravě posoudila jeho shodu se stanovenými specifikacemi podle směrnice EU č. 40/2010 a dále s platnými národními a mezinárodními standardy;
- prostřednictvím této laboratoře garantovala požadovanou úroveň systému nebo aplikace ITS či služby s ohledem na mezinárodní propojitelnost, kvalitu služby a garanci technických parametrů.

#### *3.5.2.1 Přístup k procesu posuzování shody*

Ve vztahu k systému informačního propojení dispečinků organizací krizového řízení a dispečinků ve veřejné dopravě pro vzájemnou přímou distribuci informací budou formulovány předpokládané postupy a to ve dvou oblastech:

- Posouzením shody prostřednictvím „prohlášení o shodě“
- Ověření spolehlivosti rozhodujících technických řešení

##### 3.5.2.1.1 Posouzení shody prostřednictvím „prohlášení o shodě“

Prohlášení o shodě vydává či potvrzuje „Certifikační laboratoř“.

Možný postup:

- Prohlášení o shodě vypracuje dodavatel výrobku či služby dle postupu uvedeného v kapitole 3.5.1 této metodiky. Následně „Certifikační laboratoř“ ověří hodnověrnost dokumentu.
- Prohlášení o shodě vypracuje „Certifikační laboratoř“ dle postupu uvedeného v kapitole 3.5.1. této metodiky.

#### 3.5.2.1.2 Ověření spolehlivosti rozhodujících technických řešení

Ověřování shody v této oblasti je vztaženo k systémovým parametrům. Hodnoty systémových parametrů pro systém informačního propojení dispečinků organizací krizového řízení a dispečinků ve veřejné dopravě pro vzájemnou přímou distribuci informací, byly určeny:

**Informační vazba I**

**SW a blok HW rozhraní – krizové řízení, veřejná doprava**

- kontinuita = 99,95%,
- Integrita = 2s,
- spolehlivost = 99,95%.

**Přenos informací, komunikační prostředí**

- Aktivační doba dostupnosti služby = 2s
- Dostupnost služby (např. virtuálního okruhu) = 99,95%
- Doba obnovení služby - MTTR (Mean Time to Restore) = 5s
- Zpoždění = 1s
- Ztráta paketů = 99,95%

**Informační vazba II.**

**SW a blok HW rozhraní – krizové řízení, veřejná doprava**

- kontinuita = 99,95%,
- Integrita = 2s,
- spolehlivost = 99,95%.

**Přenos informací, komunikační prostředí**

- Aktivační doba dostupnosti služby = 2s
- Dostupnost služby (např. virtuálního okruhu) = 99,95%
- Doba obnovení služby - MTTR (Mean Time to Restore) = 5s
- Zpoždění = 1s
- Ztráta paketů = 99,95%

**Informační vazba III.**

**SW a blok HW rozhraní – krizové řízení, veřejná doprava**

- kontinuita = 99,55%,
- Integrita = 2s,
- spolehlivost = 99,55%.

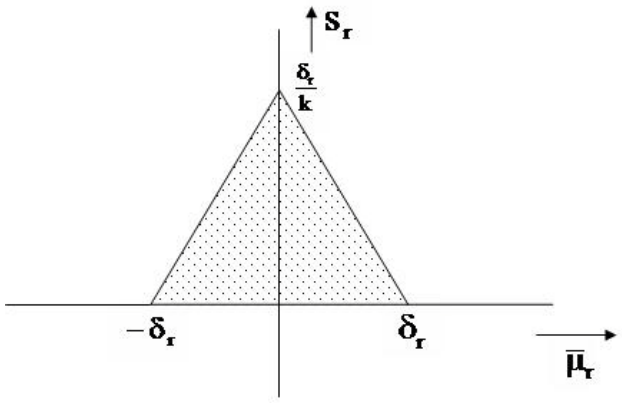
**Přenos informací, komunikační prostředí**

- Aktivační doba dostupnosti služby = 5s
- Dostupnost služby (např. virtuálního okruhu) = 99,5%
- Doba obnovení služby - MTTR (Mean Time to Restore) = 5s
- Zpoždění = 2s

Ověřování se bude odvíjet na základě algoritmů testů. Pro přiblížení problematiky je následně uveden princip.

Testovací algoritmus systémových parametrů se skládá z následujících kroků:

1. Definice počtu vzorků n.
2. Výpočet střední hodnoty μr a směrodatné odchylky sr z měřeného souboru n dat.
3. Definice požadované spolehlivosti (1−α) a závislosti měření β dle telematické aplikace.
4. Výpočet parametru k dle aproximačních vzorců a dle požadované spolehlivosti (1−α) a závislosti měření β dle telematické aplikace.
5. Stanovení požadované přesnosti systémových parametrů δr dané telematické aplikace na hladině spolehlivosti (1−α) a závislosti β.
6. Vynesení střední hodnoty $\mu_r$ a směrodatné odchylky $s_r$ do grafu na obrázku 4.




*Obr. 4.:Odhad testování systémových parametrů*

1. Pokud vynesený bod padne do trojúhelníku, systém splňuje předdefinované systémové parametry, pokud ne, systém je nesplňuje.

## 3.6 Management bezpečnosti

Vychází s dodatečných požadavků uvedených v kapitole „systémových parametrů“:

- ochrana vstupů heslem,
- ochrana dat v databázích,
- šifrování bezpečnostních sdělení - pokud bude využívána:
  - webovská aplikace
  - veřejné komunikační prostředí
  - rádiové komunikační prostředí – i vlastní

Správa digitálních certifikátů, potřebných pro komunikaci, bude muset zajistit interoperabilitu v rámci územní samosprávy, státu, nebo v některých případech i mezinárodní interoperabilitu. Některý subjekt nebo subjekty, pověřené autority danou samosprávou a uznávané vlastníky a provozovateli zařízení uživatelů systému, budou muset tyto digitální certifikáty spravovat. Konkrétní provozní pokyn pro dané „jádro propojení systémů“ bude muset definovat a specifikovat tyto aspekty. Identifikace špatného chování uživatelů bude vyžadovat komunikaci mezi každým "jádrem propojení systémů", nebo alespoň Proxy komunikaci s každým "jádrem propojení systémů“, které komunikuje se stejným subjektem, spravujícím certifikáty.

Je nutné jasné vymezit tyto aspekty, aby přilehlé / spolupracující "jádra propojení systémů" porovnala a sladila své režimy a podmínky, nebo stanovila pravidla pro řešení problémů tam, kde se provozní podmínky liší.

# 4 Srovnání „novosti“ postupů

Metodika stanovení požadavků na techniku, informační vazby a pokyny pro projektování integrálního využití v obou systémech přináší koncepční způsob návrhu fyzické a komunikační architektury. Nejrůznější systémy jsou v praxi často používány jednoúčelově, často bez možnosti využití jejich výstupů jinými aplikacemi. Metodika popisuje postup návrhu varovného zařízení od zjišťování požadavků po test v reálném provozu.

Metodiku lze využít pro dosažení následujících druhů výstupů:

- Návrh hardwarové části zařízení
- Návrh grafického rozhraní
- Stanovení podmínek testů
- Test v simulačním provozu
- Test v reálném provozu
- Definování nutného technického vybavení.
- Možnost průběžného doplňování nových technologických možností, či dalších vyvíjených (nebo teprve zamýšlených) technologií s možností posouzení jejich efektivity.

# 5 Popis uplatnění metodiky

Metodika poskytuje podklady pro využití stávajících a definování základních požadavků na nově pořizované technologie. Předpokládanými uživateli metodiky mohou být orgány státní správy, které mají na starost koncepční řešení dispečinků IZS a další subjekty. Metodika je vhodná i pro ty subjekty, které se zabývají problematikou integrace a řízení veřejné dopravy. Možnými uživateli metodiky tak mohou být například Ministerstvo vnitra i dopravy, Policie ČR, Hasičský záchranný sbor, projektanti dispečerských systémů a další. Uplatněna bude zejména v následujících materiálech:

- Koncepční materiály rozvoje architektur dopravní telematiky v městských, příměstských a regionálních oblastech.
- Podklad pro přípravu a realizaci procesu potvrzování shody.
- Vývoj nových technologií v oblasti rozvoje ICT v řízení veřejné dopravy.

Důležitým bodem pro koordinované zavádění je vytyčení hlavních služeb evropských inteligentních dopravních systémů, které budou poskytovány a stanovení rámce pro zavádění těchto služeb.

# 6 Seznam použité literatury


[1] Zákon o krizovém řízení, č. 240/2000 Sb.,

[2] Zákon o kybernetické bezpečnosti, č.181/2014 Sb.

[3] European Commission, "Communication from the Commission. Action Plan for the Deployment of Intelligent Transport Systems in Europe," European Commission, Tech. Rep.,2008.

[4] Směrnice Evropského Parlamentu a Rady č. 2010/40/EU ze dne 7. 7. 2010 o rámci pro zavedení inteligentních dopravních systémů v oblasti silniční dopravy a pro rozhraní s jinými druhy dopravy.

[5] Návrh Nařízení EK v přenesené pravomoci (EU) č. C(2014) 9672 final z 18. 12. 2014, kterým se doplňuje směrnice Evropského parlamentu Rady 2010/40/EU, pokud jde o poskytování informačních služeb o dopravním provozu v reálném čase v celé EU

[6] ČSN EN ISO/IEC 17065:2013 Posuzování shody – Požadavky na orgány certifikující produkty, procesy a služby.

[7] ROZHODNUTÍ EVROPSKÉHO PARLAMENTU A RADY č. 768/2008/ES ze dne 9. července 2008 o společném rámci pro uvádění výrobků na trh

[8] Projekt POSSE – „Promoting Open Specifications and Standards in Europe" (http://posse.intens.cz/).

[9] Akční plánu rozvoje inteligentních dopravních systémů (ITS) v ČR do roku 2020 (s výhledem do roku 2050)

[10] Projekt č. 1F54E/058/520, „Telematický nástroj podpory udržitelnému rozvoji dopravy v regionech.", Technické metodiky telematiky veřejné dopravy regionů.

[11] Projekt č. 1F54E/058/520, „Telematický nástroj podpory udržitelnému rozvoji dopravy v regionech.", Metodika systémových parametrů-přenos informací v dopravní telematice.

[12] Projekt č. 1F54E/058/520, „Telematický nástroj podpory udržitelnému rozvoji dopravy v regionech.", Metodika jednotných požadavků na SW a HW provozního dispečinku.

[13] Projekt č. 1F54E/058/520, „Telematický nástroj podpory udržitelnému rozvoji dopravy v regionech.", Metodika organizačních aspektů informačních systémů pro cestující ve veřejné dopravě.

[14] Projekt č. 1F54E/058/520, „Telematický nástroj podpory udržitelnému rozvoji dopravy v regionech.", Metodika následné kontroly systémových parametrů v dopravní telematice.

[15] Test of normality [http://www.caspur.it/risorse/softappl/doc/sas_docs/qc/chap1/sect19.htm]

[16] Novovicova J.: Probability and mathematical statistics, textbook, Faculty of transportation sciences, CTU Prague, 1999.

[17] Jilek M.: Statistical confidence intervals, Teoreticka kniznice inzenyra, SNTL, Prague, 1988.

[18] Howe W.G.:Two-sided tolerance limits for normal populations, JASA, 64, 1969.

[19] Bowker A.H.: Computation of factors for tolerance limits on a normal distribution when sample is large, AMS 17, 1946.

[20] Ghosh D.T.: A note on computation of factor for tolerance limits for a normal distribution, Sankhya B42, 1980.

[21] COST 323, European Specification on Weigh-In-Motion of Road Vehicles. Draft 3.0, EUCO-COST/323/x/99, June 1999.

[22] Jacob, B., Assessment of the Accuracy and Classification of Weigh-In-Motion Systems, Part 1 - Statistical Background. March 1997.

[23] Lieshout, R.A. van, Zoutenbier, M.H.H., Weigh-In-Motion of Road Vehicles. WIM-VID/IMP1, nr 6800.0770, E1655-01, CQM. May 1998.

[24] Lieshout, R.A. van, Zoutenbier, M.H.H., Weigh-In-Motion of Road Vehicles. WIM-VID/IMP1, nr 68000.0821-Studying Measurement Accuracy-, E1657-01, CQM. Sept 1999.

[25] Owen, D.B., Handbook of Statistical Tables. Reading, Mass, 1962.

[26] Stig Danielson: Accuracy in WIM systems - An examination of different methods for determining precision, Report, Linkoping University, Department of Mathematics Statistics.

[27] Projekt č. 802/210/108, „Inteligentní dopravní systémy v podmínkách dopravně-telekomunikačního prostředí České republiky", Výzkumné zprávy 2001-2005