
# ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

FAKULTA DOPRAVNÍ

Bc. Kristýna Vodičková


# Možnosti zavádění technologií na odhalování nezákonného rušení GNSS signálu v ČR

Diplomová práce

**2018**

**ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE**
**Fakulta dopravní**
**d ě k a n**
Konviktská 20, 110 00 Praha 1

**K621**..... **Ústav letecké dopravy**

# ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení studenta (včetně titulů):

**Bc. Kristýna Vodičková**

Kód studijního programu a studijní obor studenta:

**N 3710 – PL – Provoz a řízení letecké dopravy**

Název tématu (česky): **Možnosti zavádění technologií na odhalování nezákonného rušení GNSS signálu v ČR**

Název tématu (anglicky): Possibilities of deployment technologies for GNSS RFI mittigation in the CR

## Zásady pro vypracování

Při zpracování diplomové práce se řiďte osnovou uvedenou v následujících bodech:

- Technologie pro odhalování nezákonného rušení
- Identifikace zúčastněných subjektů (oblast vývoje, oblast zákazníků)
- Možnost a způsob testování nových technologií na odhalování rušení
- Návrh podkladů pro podporu zavádění technologií v ČR
- Shrnutí problematiky

ČVUT FD

Rozsah grafických prací: dle pokynů vedoucího diplomové práce

Rozsah průvodní zprávy: minimálně 55 stran textu (včetně obrázků, grafů a tabulek, které jsou součástí průvodní zprávy)

Seznam odborné literatury: ICAO. Doc 9849 : Global Navigation Satellite System (GNSS) Manual. Montreal

Calcagno R. An interference detection algorithm for COTS GNSS receivers, 2010

Vedoucí diplomové práce: **Ing. Jakub Kraus, Ph.D.**

**Ing. Roman Matyáš**

Datum zadání diplomové práce: **28. července 2017**
(datum prvního zadání této práce, které musí být nejpozději 10 měsíců před datem prvního předpokládaného odevzdání této práce vyplývajícího ze standardní doby studia)

Datum odevzdání diplomové práce: **29. května 2018**
a) datum prvního předpokládaného odevzdání práce vyplývající ze standardní doby studia a z doporučeného časového plánu studia
b) v případě odkladu odevzdání práce následující datum odevzdání práce vyplývající z doporučeného časového plánu studia

VYSOKÉ UČENÍ TECHNICKÉ V PRAZE Fakulta dopravní L. S.

Kraus

Ing. Jakub Kraus, Ph.D.
vedoucí
Ústavu letecké dopravy

prof. Dr. Ing. Miroslav Svítek, dr. h. c.
děkan fakulty

Potvrzuji převzetí zadání diplomové práce.

Vodičková

Bc. Kristýna Vodičková
jméno a podpis studenta

V Praze dne 28. července 2017

## Poděkování

Na tomto místě bych ráda poděkovala svému vedoucímu práce doc. Ing. Jakubovi Krausovi, Ph.D. a zejména Ing. Tomášovi Dušovi, Ph.D., který mi umožnil zpracování této práce a po celou dobu zpracování mě podporoval a poskytoval mi cenné rady a připomínky. Dále děkuji své rodině za podporu při mém studiu na Fakultě dopravní.

## Prohlášení

Prohlašuji, že jsem předloženou práci vypracovala samostatně a že jsem uvedla veškeré použité informační zdroje v souladu s Metodickým pokynem o dodržování etických principů při přípravě vysokoškolských závěrečných prací.

V Praze dne 28. května 2018

podpis autora

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
Fakulta dopravní

# MOŽNOSTI ZAVÁDĚNÍ TECHNOLOGIÍ NA ODHALOVÁNÍ NEZÁKONNÉHO RUŠENÍ GNSS SIGNÁLU V ČR

diplomová práce
květen 2018
Bc. Kristýna Vodičková

ABSTRAKT

Tato práce se zabývá problematikou nezákonného rušení GNSS signálu v prostředí kritické infrastruktury. V prvé řadě je věnována pozornost teorii rušení GNSS signálu, zahrnující typy rušení včetně interních a externích vlivů na kvalitu signálu. Dále jsou zmiňovány i způsoby detekce a reálné důsledky rušení GNSS signálu v prostředí kritické i nekritické infrastruktury. Kritické infrastruktuře a jejím relevantním sektorům se teoreticky věnuje následující kapitola. Praktická část se zabývá analýzou detekčních řešení a subjektů kritické infrastruktury, u nichž je vhodné se problematikou rušení GNSS signálu zabývat. Byla navržena základní metodika pro podporu zavádění detekčních řešení a informační materiály týkající se možností zabezpečení proti nezákonnému rušení GNSS signálu.

ABSTRACT

This thesis deals with the issue of unlawful interference of GNSS signal in the vicinity of critical infrastructure. The theory covers interference of GNSS signal and its types, including internal and external influence on GNSS signal quality, possibilities of interference detection and real consequences of interference in the environment of both critical and non-critical infrastructure. Critical infrastructure and its' relevant sectors are discussed in a subsequent chapter. The practical part of the thesis deals with an analysis of possible detection solutions and analysis of critical infrastructure entities where the issue of GNSS interference is relevant. Fundamental rules for the support of detection solutions implementation and information materials dealing with the possibilities of protection against the illegal interference of GNSS signal have been proposed in the last part of the thesis.

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
Fakulta dopravní

# MOŽNOSTI ZAVÁDĚNÍ TECHNOLOGIÍ NA ODHALOVÁNÍ NEZÁKONNÉHO RUŠENÍ GNSS SIGNÁLU V ČR

diplomová práce
květen 2018
Bc. Kristýna Vodičková

KLÍČOVÁ SLOVA

Kritická infrastruktura, GNSS, nezákonné rušení, detekce, Jamming, Spoofing, energetika, letecká doprava, mýtný systém

KEY WORDS

Critical infrastructure, GNSS, Unlawful interference, Detection, Jamming, Spoofing, Energy, Aviation, Toll system

**Seznam použitých zkratek** ..... **8**

**Úvod** **13**

**1 Rušení GNSS signálu** ..... **14**

1.1 Externí a vnitřní vlivy omezující kvalitu signálu GNSS ..... 16

1.1.1 Vnitřní vlivy na kvalitu GNSS signálu a funkčnost systému EGNOS ..... 17
1.1.2 Externí vlivy na kvalitu GNSS signálu ve formě vesmírného počasí a RFI ..... 18

1.2 Neúmyslné rušení ..... 19

1.3 Záměrné rušení a vysílání falešného signálu ..... 20

1.3.1 Vlivy rušení – dlouhodobý, krátkodobý vliv ..... 20
1.3.2 Dostupnost rušiček a zaznamenané případy rušení ..... 21
1.3.3 Jamming ..... 23
1.3.4 Spoofing ..... 25
1.3.5 Meaconing ..... 26

1.4 Detekce úmyslného rušení ..... 27

1.4.1 Detekce Jamming ..... 27
1.4.2 Detekce Spoofing ..... 28

**2 Kritická infrastruktura obecně** ..... **31**

2.1 Kritická infrastruktura v legislativě EU ..... 32

2.2 Kritická infrastruktura v legislativě ČR ..... 34

2.3 Využití GNSS v kritické infrastruktuře ..... 34

2.3.1 Elektronické komunikační sítě ..... 36
2.3.2 Servery burzovních systémů ..... 37
2.3.3 Energetické přenosová soustava a distribuční sítě ..... 38
2.3.4 Letecká doprava ..... 39
2.3.5 ANSP – Poskytovatelé leteckých navigačních služeb ..... 41
2.3.6 Pozemní infrastruktura ..... 41

**3 Průzkum aktuálně dostupných řešení pro detekci rušení Jamming a Spoofing a jejich dílčí charakteristiky** ..... **44**

3.1 Inovační a výzkumné projekty zabývající se problematikou ..... 44

3.1.1 GAARDIAN a SENTINEL ..... 44
3.1.2 Detector ..... 45
3.1.3 GMCA ..... 45
3.1.4 TIGER ..... 45
3.1.5 FENIX ..... 46

3.2 Komerční řešení zabývající se problematikou ..... 46

3.2.1 Produkty CTL3510 a CTL3520 + CTL8200 od Chronous Technology ..... 46
3.2.2 Produkt GNOME od společnosti IDS ..... 47
3.2.3 Produkt GISMO společnosti NSL ..... 47
3.2.4 Produkt BroadShield společnosti Spectaracom ..... 47

**4 Systém pro odhalování nezákonného rušení GNSS signálu v blízkosti strategické infrastruktury – charakteristika českého projektu Detektor** ..... **49**

4.1 Testování Řízením letového provozu ČR, ČVUT a Českým telekomunikačním úřadem 53

**5 Relevantní odvětví kritické infrastruktury dle dopadu úmyslného rušení GNSS signálu ..... 55**

5.1 Energetika 55

5.1.1 Přenosová/Distribuční soustava ..... 55

5.2 Doprava 58

5.2.1 Silniční doprava – Ředitelství silnic a dálnic ČR ..... 58
5.2.2 Letecká doprava – Řízení letového provozu ČR ..... 61
5.2.3 Letecká doprava – Provozovatelé lokálních letišť ..... 63

**6 Návrh obecné metodiky pro podporu zavádění systému pro detekci nezákonného rušení GNSS signálu v prostředí kritické infrastruktury ..... 66**

**7 Zpracování návrhu informačních materiálů týkajících se možnosti zabezpečení proti nezákonnému rušení GNSS v závislosti na konkrétním problému pro dílčí stupně managementu ..... 69**

7.1 Energetika – ČEPS ..... 69

7.1.1 Podklady k prvnímu jednání ..... 69
7.1.2 Návrh podkladů k druhému jednání ..... 71

7.2 Silniční doprava – Ředitelství silnic a dálnic ČR ..... 75

7.2.1 Podklady k prvnímu jednání ..... 75
7.2.2 Návrh podkladů k druhému jednání ..... 75

7.3 Letecká doprava – Provozovatelé lokálních letišť ..... 75

7.3.1 Podklady k prvnímu jednání ..... 75

**Závěr 76**

**Použitá literatura ..... 78**

**Seznam obrázků ..... 84**

**Seznam schémat ..... 85**

**Seznam tabulek ..... 86**

**Seznam příloh ..... 87**

# Seznam použitých zkratek

| | | |
|---|---|---|
| ABAS | Palubní referenční systém | Aircraft Based Augmentation Systems |
| ADC | Analogově digitální převodník | Analog to Digital Converter |
| ADF | Radiokompas | Automatic Direction Finding |
| AGC | Automatické řízení citlivosti | Automatic Gain Control |
| AIP | Letecká informační příručka | Aeronautical Information Publication |
| ANSP | Poskytovatel leteckých navigačních služeb | Air Navigation Service Providers |
| APV | Přiblížení s vertikálním vedením | Approach Procedures with Vertical Guidance |
| ATM | Uspořádání letového provozu | Air Traffic Management |
| BITS | Zdroj sekundárního taktu | Building Integrated Timing System |
| BTS | Základnová stanice mobilní sítě | Base Transceiver Station |
| C/No | Poměr mezi intenzitou signálu nosné vlny a intenzitou šumu | Carrier to Noise Density Ratio |
| CAA | Úřad pro civilní letectví | Civil Aviation Authority |
| CDMA | Kódový multiplex | Code Division Multiple Access |
| CFIT | Kontrolovaný let do terénu | Controlled Flight into Terrain |
| CI | Kritická infrastruktura | Critical Infrastructure |
| CIWIN | Výstražné informační sítě kritické infrastruktury | Critical Infrastructure Warning Information Network |
| COTS | Výrobky připravené k prodeji tak jak jsou | Component of the Shelf |
| ČEPS | Česká energetická přenosová soustava | |
| ČTÚ | Český telekomunikační úřad | |
| ČVUT | České vysoké učení technické | |
| DH | Výška rozhodnutí | Decision Height |
| DME | Měřič vzdálenosti | Distance Measuring Equipment |
| DRCC | Duální kros-korelační přijímač | Dual-receiver Cross-correlation |

| | | |
|---|---|---|
| DSRC | Komunikace na krátkou vzdálenost | Dedicated Short Range Communication |
| DVB-T | Digitální televizní vysílání | Digital Video Broadcasting - Terrestrial |
| E.ON | Distribuční společnost elektrické energie v ČR | |
| ECI | Evropská kritická infrastruktura | European Critical Infrastructure |
| EGNOS | Evropská podpůrná geostacionární navigační služba | European Geostationary Navigation Overlay Service |
| EGPWS | Varovný anti-kolizní systém | Enhanced Ground Proximity Warning System |
| EIRP | Efektivně vyzářený výkon | Equivalent Isotropically Radiated Power |
| ENU | Východ-Sever-Nahoru | East-North-Up |
| EPCIP | Evropská komise na ochranu kritické infrastruktury | European Critical Infrastructure Protection |
| EU | Evropská unie | |
| FAB CE | Funkční blok vzdušného prostoru – Střední Evropa | Functional Airspace Block Central Europe |
| FENIX | | Front-End GNSS Interference eXcisor |
| GAARDIAN | | GNSS Availability, Accuracy, Reliability anD Integrity Assessment for Timing and Navigation |
| GBAS | Systém pozemních referenčních stanic | Ground Based Augmentation Systems |
| GCE | GNSS Centrum Excellence | GNSS Centre of Excellence |
| GISMO | | GNSS Integrity and Signal Monitoring Observatory |
| GMCA | | Galileo Monitoring for Critical Applications |
| GNOME | | GNSS Operative Monitoring Equipment |
| GNSS | Globální družicový polohový systém | Global Navigation Satellite System |

| | | |
|---|---|---|
| GPCA | | GPS Monitoring for Critical Applications |
| GPS | Globální polohový systém | Global Positioning System |
| GSA | Evropská GNSS Agentura | European GNSS Agency |
| GSM | Globální Systém Mobilní komunikace | Global System for Mobile Communication |
| GUI | Uživatelské grafické zobrazení | Graphical User Interface |
| HDOP | Horizontální oslabení přesnosti | Horizontal Dilution of Precision |
| HPL | Horizontální úroveň ochrany | Horizontal Protection Level |
| HZSČR | Hasičský záchranný sbor ČR | |
| ICAO | Mezinárodní organizace pro civilní letectví | International Civil Aviation Organization |
| ICT | Informační a komunikační technologie | Information and Communication Technologies |
| ILS | Systém pro přesné přiblížení a přistání | Instrument Landing System |
| IMU | Inerční měřící jednotka | Inertial Measurement Unit |
| IZS | Integrovaný záchranný sbor | |
| LKCS | Letiště České Budějovice | |
| LKKB | Letiště Praha – Kbely | |
| LKKU | Letiště Kunovice | |
| LKKV | Letiště Karlovy Vary | |
| LKMH | Letiště Mnichovo Hradiště | |
| LKMT | Letiště Leoše Janáčka Ostrava | |
| LKPD | Letiště Pardubice | |
| LKPO | Letiště Přerov | |
| LKPR | Letiště Václava Havla Praha | |
| LKTB | Letiště Brno – Tuřany | |
| LKVO | Letiště Vodochody | |
| LNAV | Horizontální navigace | Lateral Navigation |
| LPV | Přiblížení s výškovým vedení podle GNSS | Localizer Performance with Vertical Guidance |

| | | |
|---|---|---|
| MCC | Řídící centrum systému EGNOS | Master Control Center |
| MLS | Mikrovlnný přistávací systém | Microwave Landing System |
| MSS | Mobilní satelitní spojení | |
| MVČR | Ministerstvo vnitra ČR | |
| NCI | Národní kritická infrastruktura | National Critical Infrastructure |
| NDB | Nesměrový radiomaják | Non-Directional Beacon |
| NGIS | | Northrop Grumman Information Systems |
| NMA | Autentizace navigační zprávy | Navigation Message Authentication |
| NOTAM | Oznámení pro pracovníky zabývající se letovým provozem | Notice to Airmen |
| OBU | Palubní jednotka | On Board Unit |
| OTH | Přes-horizontální radar | Over the Horizon Radar |
| PBN | Navigace založená na výkonnosti | Performance Based Navigation |
| PBN-RNAV | PBN-oblastní navigace | PBN - Area Navigation |
| PCCIP | Prezidentská komise na ochranu kritické infrastruktury | Presidential Commission for Critical Infrastructure Protection |
| PMU | Fázorová měřící jednotka | Phasor Measurement Unit |
| PNT | Poloha, Navigace, Čas | Position, Navigation, Timing |
| PPD | Prostředek pro zajištění soukromí | Personal Privacy Device |
| PRE | Pražská energetika, a.s. | |
| PRN | Pseudo-náhodný šum | Pseudo Random Noise |
| PVT | Poloha, Rychlost, Čas | Position, Velocity, Time |
| RAIM | Autonomní monitorování integrity přijímače | Receiver Autonomous Integrity Monitoring |
| RFI | Vysokofrekvenční rušení | Radio Frequency Interference |
| RIMS | Pozemní monitorovací stanice systému EGNOS | Ranging and Integrity Monitoring Stations |
| RNP | Požadovaná navigační výkonnost | Required Navigation Performance |
| RNSS | Radionavigační družicová služba | Radio Navigation Satellite Services |
| RWY | Dráha | Runway |
| ŘLP | Řízení letového provozu | |

| | | |
|---|---|---|
| ŘSD | Ředitelství silnic a dálnic | |
| SAR | Pátrání a záchrana | Search and Rescue |
| SARPS | Standardy a doporučené postupy ICAO | Standards and Recommended Practices |
| SBAS | Družicový referenční systém | Satellite Based Augmentation Systems |
| SDD | Dokument služby Galileo/EGNOS | Galileo/ EGNOS Service Definition Document |
| SDR | Softwarově definované rádio | Software Defined Radio |
| SENTINEL | | GNSS SErvices Needing Trust In Navigation, Electronics, Location & timing |
| SESAR | Projekt Jednotné evropské nebe | Single European Sky ATM Research |
| SID | Standardní přístrojový odlet | Standard Instrument Departure |
| SIM | SIM karta | Subscriber Identity Module |
| SPS | Standardní polohová služba | Standard Position Service |
| STAR | Standardní přístrojový přílet | Standard Terminal Arrival Route |
| TIGER | | Trusted GNSS Receiver |
| UT | | University of Texas |
| UTC | Koordinovaný světový čas | Universal Time Coordinated |
| VDOP | Vertikální oslabení přesnosti | Vertical Dilution of Precision |
| VFR | Pravidla pro let za viditelnosti | Visual flight rules |
| VNAV | Vertikální navigace | Vertical Navigation |
| VOR | VKV všesměrový radiomaják | VHF Omnidirectional Radio Range |
| VPL | Vertikální úroveň ochrany | Vertical Protection Level |
| WAAS | Plošný referenční systém | Wide Area Augmentation System |
| WACS | Systém plošné kontroly | Wide Area Control System |
| WAMS | Systém plošného monitorování přenosové soustavy | Wide Area Monitoring System |

# Úvod

Globální navigační satelitní systémy (GNSS) jsou dnes již běžnou součástí moderní civilizace a jsou využívány mnoha aplikacemi v civilním i armádním sektoru. GNSS signál poskytuje funkci navigace, přesného určení polohy a přesného určení času (PNT). Všechny tyto funkce nám usnadňují každodenní civilní život. Ovšem kromě běžného využití pro osobní potřebu je GNSS signál využíván po celém světě v aplikacích kritické infrastruktury, které jsou nezbytné pro zajištění bezpečnosti a funkčnosti státu a jeho kritické infrastruktury.

S rozvojem moderních technologií a především s rozvojem využití GNSS v mnoha odvětvích kritické i nekritické infrastruktury začaly pochopitelně postupně narůstat i případy rušení GNSS signálu ať už ve svůj vlastní prospěch nebo s cílem ochromit daný subjekt. Až teroristické útoky, které se odehrály v 90. letech 20. století v USA, daly podnět k zahájení diskuze ohledně ochrany kritické infrastruktury. Tato práce se konkrétně zabývá subjekty kritické infrastruktury, které využívají ve svých klíčových systémech GNSS signál, definováním možných typů rušení GNSS signálu, možnostmi detekce a vlivy rušení na infrastrukturu, včetně zaznamenaných případů rušení z minulosti.

Cílem této práce je analyzovat subjekty kritické infrastruktury, které využívají GNSS signál a jejich dílčí problémy z hlediska ochrany před nezákonným rušením GNSS signálu. Druhým cílem práce je uceleně zpracovat analýzu na trhu dostupných produktů pro detekci různých typů rušení a jejich charakteristik. Následně práce navazuje na projekt s názvem Systém pro odhalování nezákonného rušení GNSS signálu v blízkosti strategické infrastruktury alias Detektor a porovnává tento český produkt s ostatními dostupnými produkty. V poslední části, která je dílčím cílem práce, jsou zpracovány ucelené materiály pro vybrané subjekty kritické infrastruktury upozorňující na aktuální hrozbu v podobě rušení GNSS signálu a představující modulované řešení pro konkrétní subjekty. Navrhované materiály budou sloužit jako podklady pro zahájení jednání ohledně implementace Detektoru, v prvé řadě ve společnosti ČEPS a dále s Ředitelstvím silnic a dálnic ČR a s operátory lokálních letišť s publikovaným (zamýšlenou publikací) LPV postupů pro přiblížení na přistání. Materiály jsou dále přizpůsobitelné i pro jiné subjekty kritické i nekritické infrastruktury.

# 1 Rušení GNSS signálu

Následující kapitola se zabývá rozborem rušení GNSS signálu. V prvé řadě jsou zmíněny vnitřní a externí vlivy na jeho kvalitu, které jsou velmi těžko ovlivnitelné. Zahrnují působení kosmického počasí, nebo chyby vzniklé v interních subsystémech. Okrajově je popsáno neúmyslné rušení, způsobené rušením různých radiových systémů a vysokofrekvenčních radiových vysílačů. Převážná část kapitoly rozebírá jev záměrného (nezákonného) rušení, které je klíčovým elementem této práce. Jsou zde popsány základní typy rušení GNSS signálu – Jamming, Spoofing a Meaconing a dostupnost rušiček pro jednotlivé typy rušení. V návaznosti na to jsou uvedeny možné způsoby detekce Jamming a Spoofing podle použité metody a komplexity odhalení. Detekce Meaconing není detailně rozebírána, jelikož tento druh rušení GNSS signálu není zcela relevantní pro praktickou část práce.

Služby Position, Navigation, Timing (PNT), které jsou bezplatně (dostupné i ve zpoplatněné verzi) poskytovány přijímačem v rámci dostupnosti GNSS signálu, se díky své přístupnosti v rozvinutých státech staly součástí běžného života. Služby PNT zajišťují tři důležité funkce:

1) *POSITION – Přesné určení polohy* – schopnost přesně určit polohu a směr ve trojrozměrném prostoru ve standardním geodetickém systému (př. WGS84)
2) *NAVIGATION – Navigace* – schopnost určit současnou a požadovanou polohu (relativní nebo absolutní) a uplatnit případné směrové, orientační a rychlostní korekce, pro získání požadované polohy kdekoliv na zeměkouli a
3) *TIMING – Přesné určení času* – schopnost určit a udržet přesný standardní čas (koordinovaný univerzální čas, UTC) kdekoliv na zemi a současně zajistit uživateli definované parametry týkající se také časových přenosů.

S rozvojem využití GNSS signálu v mnoha aplikacích nejen v segmentu dopravy (navigace a přesné určení polohy), ale i v mnohých dalších segmentech jako je energetika (přesné určení času), bankovnictví (přesné určení času) nebo mobilní komunikační sítě (přesné určení času), dochází ke stále častějšímu výskytu rušení. V následujících odstavcích jsou vymezeny typy rušení a vlivy omezující kvalitu příjmu GNSS signálu.

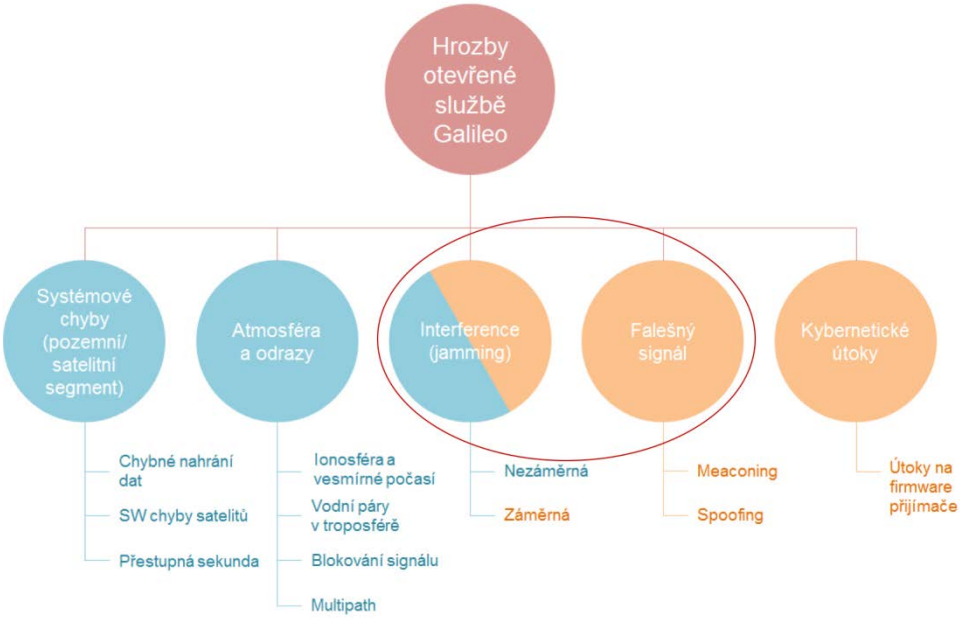



*Schéma 1: Hrozby otevřené službě Galileo, zdroj: [8], vlastní úprava*

Schéma 1 zobrazuje hrozby otevřené službě Galileo. Hrozby jsou graficky odděleny na záměrné a nezáměrné, tyrkysovou barvou jsou znázorněny chyby a hrozby, které vznikají nezáměrně vlivy kosmického počasí a systémovými chybami. Oranžová barva znázorňuje záměrné ovlivnění signálu prostřednictvím RFI nebo vysíláním falešného signálu. Samostatný segment tvoří kybernetické útoky na firmware přijímače. Červená elipsa naznačuje hrozby, které jsou dále v práci rozebírány a které lze aktivně ovlivnit.

Rušení GNSS signálu, tzv. Radio Frequency Interference (RFI), lze klasifikovat dle potřeb diplomové práce a v souvislosti s tvorbou materiálů v praktické části do následujících skupin:

I. Podle nosné frekvence
II. Úmyslné/neúmyslné rušení
III. Dle dopadu – krátkodobý vliv/dlouhodobý vliv rušení (dále pojednáváno v kapitole 1.3.1)
IV. Dle typu použité RFI techniky – Jamming, Spoofing, Meaconing (dále pojednáváno v kapitole 1.3.3, 1.3.4 a 1.3.5)

V případě rušení GNSS signálu, dle výše stanoveného rozdělení, se setkáváme se čtyřmi typy rušení. Prvním typem je klasifikace rušení dle nosné frekvence. Tím je myšleno, na jaké frekvenci je rušivý signál vysílán a jaké frekvenční pásmo rušení ovlivňuje (pro signál GPS to je nosná frekvence L1 1575,42 MHz, L2 1227,60 MHz). Druhým typem je neúmyslné nebo přirozené rušení. Do této kategorie lze zařadit systémové chyby pozemního nebo satelitního

segmentu způsobené chybným nahráváním dat nebo softwarovou chybou satelitů. Dalším způsobem neúmyslného rušení GNSS signálu jsou chyby způsobené průchodem signálu atmosférou a odrazy signálu. Zde působí značný vliv ionosféry (ionosférická chyba), troposféry a kosmického počasí. Může také dojít k intra/inter-systémovému rušení vysíláním signálu jiným satelitem nebo při rušení mezi službami GPS a Galileo (případně jinými konstelacemi). Takové rušení bereme jako přirozené. Úmyslnému rušení je věnována samostatná kapitola 1.3. Třetí formou klasifikace je rozdělení dle vlivu na dlouhodobé nebo krátkodobé ovlivnění příjmu GNSS signálu přijímačem, krátkodobé rušení je způsobeno osobními rušičkami GNSS signálu, dlouhodobé rušení je způsobeno sofistikovanými rušičkami s vyšším výkonem a delší výdrží baterie, dále je tomuto věnována kapitola 1.3.1. Posledním jmenovaným typem je pak členění dle použité techniky rušení na Jamming, Spoofing a Meaconing. Tyto jednotlivé skupiny jsou blíže popsány v nadcházejících kapitolách.

V souvislosti se zpracovávaným tématem, je nutné zmínit, že civilní aplikace služeb GNSS využívají pro přenos signálu dvě nosné frekvence 1575,42 MHz a 1227,60 MHz, pro GPS jsou frekvence označeny L1 a L2, označení Galileo frekvencí je L1, E5a a E5b, které jsou víceméně nechráněné. Signál vyslaný od vysílače k přijímači urazí přes 22 000 km. Při průchodu atmosférou na něj působí mnoho nepříznivých vlivů, a tak vznikají chyby z důvodu působení atmosférických vlivů a vlivů kosmického počasí. Dochází k blokování signálu a ke vzniku tzv. multipath (vícecestné šíření vznikající odrazem od překážky). Při dosažení přijímače je signál logicky v návaznosti na předchozí vlivy slabý, maximálně -125 dBm, a je tudíž snadno napadnutelný. [1, 56]

Pro účely této práce a pro zamezení nejasnostem bude nadále souhrnně používán pojem „rušení“, který bude zahrnovat rušení signálu Jamming a ovlivňování signálu Spoofing, termín RFI je používán pouze v souvislosti s rušením typu Jamming.

## 1.1 Externí a vnitřní vlivy omezující kvalitu signálu GNSS

V návaznosti na předchozí úvod to tématu je třeba zdůraznit, že vlivy na kvalitu a sílu GNSS signálu působí „*Interní (vnitřní) vlivy*“, týkající se selhání procesů subsystémů GNSS, tzn. GPS nebo EGNOS a „*Externí vlivy*“ za které můžeme považovat například působení kosmického počasí a RFI.

### 1.1.1 Vnitřní vlivy na kvalitu GNSS signálu a funkčnost systému EGNOS

Výkonnost GNSS signálu lze měřit dle následujících parametrů, které jsou konkrétně specifikovány v dokumentu GPS Standard Positioning Service (SPS) Performance Standard[1] a dokumentu „ICAO SARPs – Standards and Recommended Practices – Global Navigation Satellite System (GNSS) Manual[2]:

a) Přesnost – polohová, časová, rozsah
b) Integrita
c) Dostupnost
d) Kontinuita
e) Pravděpodobnost selhání hlavní služby

I když jsou všechna specifika uvedená v předchozích dvou dokumentech nadmíru splněna, u kosmického segmentu na rozdíl od řídícího (pozemního) a uživatelského segmentu nelze výskyt chyb predikovat. U pozemního segmentu nelze výskyt chyb vyloučit, ovšem díky nezávislosti satelitů a zálohám pozemního segmentu jsou selhání minoritním problémem, které nezpůsobuje degradaci služby.

Interní vlivy, které mohou ovlivnit přesnost způsobuje více faktorů. Satelitní hodiny jsou vybaveny přesnými atomovými hodinami, které i tak každé 3 hodiny projeví odchylku v řádu $10^{-9}$ s ~ 30 cm. Řídící segment proto pomocí pozemních monitorovacích stanic Ranging and Integrity Monitoring Station (RIMS) vypočítává odchylky a následně vysílá zpět družici korekce. Chyba hodin přijímače způsobuje špatné určení vzdálenosti, pro určení polohy a času potřebujeme vidět minimálně čtyři družice, tuto chybu lze vypočítat pomocí rovnic o čtyřech neznámých, kde tři neznámé X, Y, Z reprezentují polohu a čtvrtá T chybu hodin přijímače. Další interní faktor, který působí na přesnost je efemeridická chyba neboli odchylka od dráhy družice. Dráhy družic jsou monitorovány pozemními monitorovacími stanicemi, které vypočítávají korekce, ty jsou následně vysílány k družici a následně zpět do pozemního GNSS přijímače. Tyto předpovědi mohou obsahovat odchylku, která může způsobit špatné určení polohy. [1]

[1] Odkaz na dokument GPS Standard Positioning Service (SPS) Performance Standard: GPS Standard Positioning Service (SPS) Performance Standard
[2] Odkaz na dokument Global Navigation Satellite System (GNSS) Manual: https://www.icao.int/Meetings/PBN-Symposium/Documents/9849_cons_en%5B1%5D.pdf

Aplikace kritické z hlediska bezpečnosti, pro které je důležité zachování integrity, využívají funkcí GNSS pouze v kombinaci s rozšiřujícími systémy (Augmentation systems) – Satelite Based Augmentation System (SBAS), Ground Based Augmentation System (GBAS) a Aircraft Based Augmentation System (ABAS). [56]

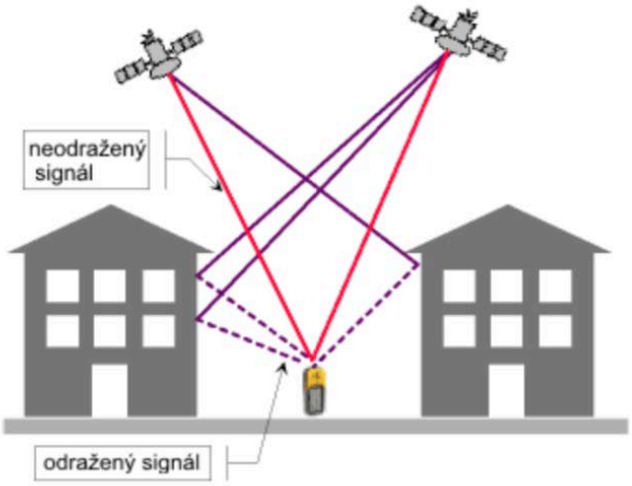
### 1.1.2 Externí vlivy na kvalitu GNSS signálu ve formě vesmírného počasí a RFI

Průchod GNSS signálu atmosférou ovlivňují její aktuální podmínky, které mění rychlost světla, dle které vypočítáme vzdálenost k družici. Vlivy atmosféry a kosmického počasí způsobují zkrácení pseudovzdálenosti při fázovém měření nebo naopak její prodloužení při kódovém měření. Nejvíce je signál ovlivněn právě při průchodu ionosférou a troposférou.

Troposféra je nejnižší část atmosféry, kde na GNSS signál působí vodní páry, nedochází zde k rozptylu vlnění až do frekvence 15GHz, přesnost signálu závisí také na aktuální hustotě, teplotě a vlhkosti vzduchu. Korekce pseudovzdálenosti jsou vypočítány dle troposférických modelů, tím je kompenzována chyba vzniklá zpožděním signálu při průchodu troposférou.

Ionosféra je nejvyšší část atmosféry, s výskytem velkého množství volných elektronů, díky nimž je tato část atmosféry ionizovaná a vodivá. Vodivost má negativní vliv na elektromagnetické vlnění, které při průchodu ztrácí na intenzitě. Vliv ionosféry závisí na denní době, ve dne je její vliv intenzivnější. Zároveň také závisí na vlnové délce tzn. působí rozdílně na nosné frekvence GNSS signálu. Ionosférické chyby jsou eliminovány pomocí korekcí pseudovzdálenosti z ionosférického modelu (dle obsahu elektronů v ionosféře) a zasláním v navigační zprávě, nebo výpočtem vlivu ionosféry na dvě nosné frekvence GPS signálu L1/L2 a Galileo L1/E5a,b.

V hustě zastavěných oblastech nebo v oblastech s velkou členitostí terénu vzniká vícecestné šíření neboli „Multipath“ odrazem od okolních budov nebo od vyšších terénních překážek, jak je znázorněno na obrázku 1 níže. Odražený signál urazí k přijímači delší dráhu, než kdyby bylo jeho šíření přímé. Multipath způsobuje nepravidelné kolísání GNSS signálu s odchylkou několika metrů. Tento negativní vliv na přesnost GNSS signálu může ohrozit například systémy pro výběr satelitního mýtného, pokud se počítá s jejich zavedením v zastavěných oblastech měst nebo u dálnic s převyšujícím terénem. Vlivy Multipath lze odstranit polarizací signálu. Současně vyráběné antény přijímačů dokáží vzniku tohoto efektu již spolehlivě zabránit. [1, 56]




*Obrázek 1: Multipath – odraz od okolních budov, zdroj: [1]*

## 1.2 Neúmyslné rušení

Signál GNSS je vysílán v radionavigačním frekvenčním spektru (RNSS), které je omezeno pouze pro vysílání tohoto signálu. Vzhledem k existenci a častému využívání jiných radiových systémů s vyšším výkonem v sousedním spektru RNSS, tento silnější signál současně zvyšuje i hladinu šumu ve spektru RNSS. Neúmyslné rušení může tedy být způsobeno rušením rozdílných radiových systémů a vysokofrekvenčních radiových vysílačů. Hladina šumu, způsobená vyšším harmonickým kmitočtem rušivého zařízení, při dosažení určité výšky negativně ovlivní i signál GNSS. Zdrojem takto rušivých signálů jsou nejčastěji úzkopásmové signály digitálních trunkových systémů nebo širokopásmové signály standardu digitálního televizního vysílání DVB-T. V případě uvažování o využití GNSS signálu v okolí letiště, mohou mít na GNSS signál negativní vliv i aplikace a systémy běžně používané v letištním provozu, mezi které patří radionavigační služby VOR, ILS a služby řízení letového provozu, tímto tématem se podrobně zabývá V. Loužil ve své diplomové práci s názvem Detekce a lokalizace rušení GNSS systémů. Mezi další známé RFI můžeme zařadit rušení radary, mobilní satelitní spojení (MSS) a Over the Horizon radary (OTH). [2, 3, 4]

Faktor neúmyslného rušení není pro tuto práci relevantní, proto nebude dále zmiňován a je o něm hovořeno pouze pro uvedení čtenáře do problematiky.

## 1.3 Záměrné rušení a vysílání falešného signálu

Úmyslné rušení nebo ovlivňování GNSS signálu se stává v současné době velmi rozšířené. Zapříčiněno je zejména vzrůstajícím využíváním prostředků pro zajištění soukromí – „Personal Privacy Device“ (PPD).

Kromě elementárního rozdělení rušení na úmyslné a neúmyslné, ho kategorizovat dle typu a použité technologie (dělení dle IV. jak bylu uvedeno v úvodu kapitoly 1). Zde rozlišujeme Jamming, Spoofing a Meaconing, kde je hlavním rozdílem úroveň složitosti použité technologie a současně komplexnost technologie potřebné pro zamezení typu rušení.

### 1.3.1 Vlivy rušení – dlouhodobý, krátkodobý vliv

Při zpracování podkladů pro jednotlivé subjekty kritické infrastruktury (CI) jsou pro účely této práce používány pojmy *Dlouhodobý a Krátkodobý vliv rušení*. Definování těchto pojmů tak, jak budou následně používány, je specifikováno v následujících odstavcích.

V prostředí kritické infrastruktury, pro jejíž subjekty je tato práce zpracovávána, můžeme detekovat rušení s dlouhodobým nebo krátkodobým vlivem na funkčnost systémů. Krátkodobé rušení může nastat například při využívání PPD řidiči automobilů na silnicích nebo na přilehlých komunikacích k subjektu kritické infrastruktury. V těchto případech jsou zaznamenávány pouze krátkodobá omezení příjmu signálu přijímačem. Vlivy krátkodobého rušení byly zaznamenány v USA na Newark Liberty International Airport (EWR), kde byly z dlouhodobého hlediska zaznamenány případy krátkodobých výpadků systému GBAS. Při šetření bylo zjištěno, že příchod rušivého signálu je z dálnice, která se nachází v blízkosti přistávací dráhy. Zdrojem rušení byla zjištěna rušička signálu GPS typu PPD, zabraňující dalším stranám lokalizaci vozidla, jejichž používání je v USA protizákonné. Z tohoto případu, kdy nebylo způsobeno závažné ohrožení, plyne, že je velmi snadné narušit příjem signálu GNSS, a způsobit tak závažné škody subjektům kritické infrastruktury. Zajímavě tyto incidenty z EWR rozebírá článek od autorů S. Pullen a G Xingxin Gao z roku 2012, GNSS Jamming in the Name of privacy: Potential Threat to GPS Aviation[3], kdy byl tento problém aktuální. Článek zajímavě rozebírá i různé typy a dopady používání PPD na zařízení GBAS a referenční stanice Wide Area Augmentation System (WAAS) v USA. [6]

Dlouhodobý vliv rušení se může projevit při využití silnějších rušiček s napájením z připojené baterie, které byly testovány viz kapitola 4.1. Takto upravené rušičky mohou být v provozu až

[3] Odkaz na článek GNSS Jamming in the Name of privacy: Potential Threat to GPS Aviation: http://insidegnss.com/wp-content/uploads/2018/01/marapr12-Pullen.pdf

několik dní, a tím závažně ohrozit veškeré funkce systémů využívajících GNSS (tzn. funkce určení přesné polohy „Position“, navigace „Navigation“ a přesného určení času „Timing“), jejichž záložní systémy jsou schopny synchronizace pouze po určitou omezenou dobu. Rušičky s delší výdrží jsou spíše používány k úmyslnému rušení s cílem ohrozit kritickou infrastrukturu. Dlouhodobý vliv rušení může způsobit následky v podobě finančních škod včetně závažného ohrožení infrastruktury.

### 1.3.2 Dostupnost rušiček a zaznamenané případy rušení

Nejčastěji užívaným způsobem rušení je úmyslný Jamming. V zásadě se jedná o ztrátu GNSS příjmu signálu v přijímači v důsledku jeho rušení pomocí rušičky „Jammeru“. Rušičky GNSS signálu lze jednoduše pořídit v internetových e-shopech v řádech desítek eur (viz příklady rušiček uvedené v tabulce 2 a tabulce 3). Dosah takového zařízení je až do stovek metrů (test dvou rušiček popisovaný v kapitole 4.1 prokázal, že rušička s uváděným dosahem 8 m a výkonem 33 dBm v manuálu měla při reálném měření dosah až cca 227 m, druhá rušička s uváděným dosahem 40 m a výkonem 35 dBm v manuálu měla při reálném měření dosah 550 m, přičemž prodejci rušiček deklarují, že zařízení má maximální dosah v řádu metrů, maximálně desítek metrů. [4, 5]

Kromě případu na letišti EWR jsou známy další případy, kdy docházelo k rušení družicového signálu v mnohem závažnější míře a za použití vysoce výkonných rušiček GPS. Konkrétním případem je hraniční oblast mezi Severní Koreou (KLDR) a Jižní Koreou a jejím hlavním městem Soul, které se nachází v bezprostřední vzdálenosti (50 km) od hranice a kde je zároveň nejvytíženější letiště této oblasti. RFI přicházející z KLDR je každoročně opakujícím se případem s trváním i několik týdnů. To znepříjemňuje život zejména řidičům z jihokorejském Soulu, kteří se pravidelně setkávají s výpadky navigačních služeb ve svých vozidlech. V případě letecké dopravy zatím nejsou známy žádné závažné problémy, jelikož využívá alternativní navigační prostředky. Avšak tyto případy RFI znemožňují plné využití navigačních prostředků na palubách letadel využívajících GNSS. [7]

*Tabulka 1: Zaznamenané případy Jamming od roku 2007 do roku 2017, zdroj: [59], doplněno autorkou*

| Rok | Motivace | Popis incidentu |
|---|---|---|
| ***2007*** | *testování* | *Americké námořnictvo **omylem** rušilo GPS signál v oblasti San Diega zhruba po dobu dvou hodin.* |
| ***2012*** | *osobní* | ***Kněz používal zařízení pro Jamming v kostele**, aby návštěvníci nerušili kázání používáním mobilních telefonů.* |
| ***2012*** | *osobní* | ***Cestujícímu vlakem** vadilo, že ostatní cestující v "tichém* |

| | | |
|---|---|---|
| | | *voze" telefonují. Situaci vyřešil tím, že každý den na své cestě do/z práce používal kombinovaný GPS/GSM Jammer.* |
| ***2012*** | *kriminální činnost* | *Zatčen **gang odpovědný za krádeže 150 vozů** Mercedes Sprinter během 8 měsíců z oblasti letiště Heathrow. Gang využíval zařízení pro jamming k rušení sledovacích zařízení umístěných ve vozidlech.* |
| ***2012*** | *vojenský konflikt* | ***U hranic Severní a Jižní Koreje** bylo v letech 2010 až 2012 zaznamenáno a ohlášeno velice silné rušení GPS signálu.* |
| | | *Výčet zasažených oblastí výpadkem GPS a délka trvání rušení:*<br>*- 2010 (4 dny): 181 věží mobilních operátorů, 15 letadel, 1 válečná loď,*<br>*- 2011 (11 dní): 145 věží mobilních operátorů, 106 letadel, 10 lodí,*<br>*- 2012 (16 dní): 1016 letadel, 254 lodí.* |
| ***2009-2012*** | *osobní* | ***Řidič dodávky** svým jammerem způsoboval problémy na letišti v Newarku. Provoz letiště byl opakovaně narušen pachatelem, využívajícím málo výkonný jammer, který cestoval rutinně po dálnici I95, která vede kolem **letiště**. Anténa systému GBAS (pozemní augmentační systém) přijímající signály GPS byla umístěna za plotem v blízkosti dálnice, kde byla interference velmi silná v momentě, kdy vozidlo projíždělo okolo.* |
| ***2013*** | *kriminální činnost* | *Desítky **taxikářů** v Melbourne přistiženi při používání zařízení pro Jamming, aby podváděli při jízdách.* |
| ***2014*** | *kriminální činnost* | *Dva Jammery pro rušení případného skrytého sledovacího zařízení nalezena v **ukradeném nákladním voze**.* [8] |
| **2015** | Kriminální činnost | Čtyři Jammery nalezeny v nákladních automobilech s farmaceutickým zbožím a v nákladních automobilech převážejících měď. |
| **2016** | Kriminální činnost | **Ukradené dva modely automobilů Tesla S** – potenciální příčinou krádeže bylo rušení GPS signálu, umožňující zlodějům zamezit sledování pohybu vozidla. |
| **2017** | osobní | **Zapomenutý a zapnutý GPS Jammer** v osobním automobilu způsobil problémy a zpoždění letů na letišti v Nantes Atlantis Airport. |

V tabulce výše jsou uvedeny zaznamenané případy rušení od roku 2007 do roku 2017, uvedena je pouze část případů, kde byla zjištěna příčina nebo byl odhalen viník. Incidenty v podobě rušení GNSS signálu neustále stoupají, jak uvádí i Dana Goward, v článku z listopadu 2016 GPS disruption is a growing problem for Aviation, reports show[4]. Ta došla analýzou databáze NASA k závěru, že mezi roky 2013 až 2016 bylo reportováno celkem 77 incidentů (autorka také zmiňuje, že databáze je dobrovolná, což nezaručuje, že obsahuje kompletní seznam zaznamenaných případů rušení) a meziroční počet incidentů neustále stoupá. [52]

V souvislosti s případy, které se odehrávaly na letišti EWR, byl orgánem Federal Aviation Administration (FAA) vydán dokument GPS Privacy Jammers and RFI at Newark – Navigation Team AJP-652 Results[5], který zaznamenává a zabývá se jednotlivými událostmi rušení GBAS na EWR mezi roky 2009 (první zaznamenaný případ) až do roku 2012, kdy byl problém vyřešen a uzavřen. Autoři upozorňují i na snadnou možnost pořízení PPD (velmi nízká cena – rozsah od cca USD 33 do USD 155) a jejich funkcionalitu. V závěru také shrnují možné způsoby zabránění RFI pomocí softwarových modifikací a konfigurací pozemního segmentu GBAS. [49]

Z tabulky zaznamenaných incidentů a jejich vážnosti i z článku zmíněného v předchozím odstavci vyplývá, že problém rušení GNSS signálu je velmi aktuální téma, které má přesah mezi jednotlivými sektory jak kritické, tak i nekritické infrastruktury. V nadcházejících třech kapitolách jsou formulovány jednotlivé typy rušení GNSS signálu – Jamming, Spoofing a Meaconing.

### 1.3.3 Jamming

Jamming se řadí k nejčastěji využívaným způsobům rušení GNSS signálu. Jedním z faktorů je jednoduchost systému a bezpochyby dostupnost RFI rušiček. Nejjednodušším způsobem je úzkopásmové rušení pomocí jednoduchého oscilátoru ve frekvenčním pásmu L1 nebo L2 připojeným k zesilovači a anténě. Takový typ RFI zařízení je velmi snadno dostupný na webu pod názvem PPD. Jak bylo již zmíněno, tato zařízení si většinou uživatelé pořizují pouze pro osobní potřebu, bez zájmu ohrožení subjektů kritické infrastruktury v domnění, že dosah takového PPD je v řádu jednotek metrů. Ve skutečnosti je ale rušený perimetr mnohem rozlehlejší.

[4] Odkaz na článek GPS disruption is a growing problem for Aviation, reports show: https://rntfnd.org/2016/11/07/gps-disruption-is-a-growing-problem-for-aviation-reports-show/
[5] Odkaz na dokument GPS Privacy Jammers and RFI at Newark – Navigation Team AJP-652 Results: http://laas.tc.faa.gov/documents/Misc/GBAS%20RFI%202011%20Public%20Version%20Final.pdf

*Obrázek 2: Jednoduché a snadno dostupné PPD*

Efektivnějším způsobem je širokopásmové rušení fungující na stejném principu jako GNSS. Tato metoda je technologicky náročnější a velmi drahá. Signál GNSS je složený z navigačních zpráv (bitová rychlost přenosu 50 kb/s), které jsou násobeny pseudonáhodným fázovým šumem (PRN) modulovaným na nosnou sinusovou frekvenci. Vysílaný signál je následně rozšířen do spektra, kde se sníží jeho výkon. Superponovaný signál má charakter pseudo šumu, ovšem v přijímači se pseoudo šum násobí stejným PRN jako ve vysílači. Díky tomu je signál spektrálně zúžený a úroveň přijímaného signálu zvýšena o systémový přírůstek. Tento způsob používaný u širokopásmových rušiček má mnohem větší dosah než úzkopásmové rušičky. Z důvodu jeho složitosti, vysokých nákladů a dosahu není na trhu běžně dostupný pro civilní účely, jeho využití je primárně pro armádní účely případně pro úmyslné rušení za účelem ochromení kritické infrastruktury. [4]

*Obrázek 3: Typy armádních Jammerů*

### 1.3.4 Spoofing

Další používanou technikou je Spoofing. Jedná se o metodu, kdy je rušičkou vysílán identický signál jako signál GNSS za účelem manipulace s časem nebo polohou uživatele. Jelikož se jedná o metodu vysílání falešného identického signálu, je velmi malá pravděpodobnost, že bude přijímačem rozeznán. Zatímco při rušení pomocí metody Jamming dochází k přerušení příjmu signálu v přijímači, na základě čehož není přijímač schopen vypočítat svou polohu nebo určit čas, uživatel je o chybě informován a toto zařízení nebude považovat za spolehlivé. Opak je tomu u Spoofing, kde falešný signál vysílaný spoofingovým zařízením přebere kontrolu nad pravým GNSS signálem, přijímač vypočítává chybnou polohu a čas, což lze jen velmi těžko odhalit.

V principu Spoofing funguje tak, že rušička vysílá falešný signál s nižším výkonem, než je autentický GNSS signál. Následně se signál vysílaný rušičkou zesiluje a snaží se napodobit autentický signál. Jakmile se falešný signál shoduje s autentickým, začne rušička svůj signál znovu zesilovat, až je původní autentický signál plně zachycený na ten falešný. V poslední fázi, kdy rušička plně imituje signál z GNSS vysílače, změní útočník polohu GNSS přijímače na falešnou, kterou GNSS přijímač považuje za svou skutečnou polohu.

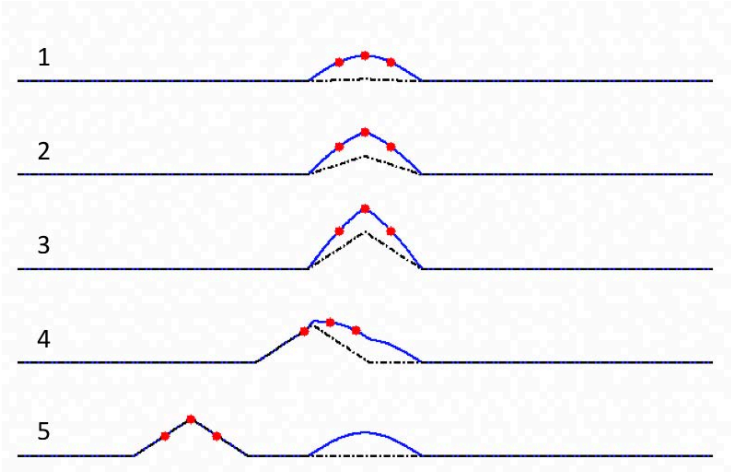



*Schéma 2: Znázornění procesu útoku Spoofing – tmavě modrá značí falešný signál, světle modrá značí autentický GNSS signál [9]*

Schéma výše znázorňuje proces spoofingového útoku. V první fázi je falešný signál slabý, následně dochází ke zvyšování jeho výkonu, až dosáhne úrovně autentického GNSS signálu. V poslední fázi je po zachycení falešného signálu přijímačem znovu zvýšen výkon a útočník již může pracovat s posouváním signálu v čase. [1, 58]

### 1.3.5 Meaconing

Poslední zmiňovanou metodou rušení je Meaconing, neboli znovu přehrání dříve nahraného signálu. Chybně může být tato metoda zaměňována za Spoofing, s kterým má shodná specifika. Principem Meaconing je generování dříve nahraného přijatého GNSS signálu a jeho následné přehrání se zpožděním a s vyšším výkonem, než má autentický GNSS signál. V případě Meaconing musí vysílač „falešného“ signálu současně fungovat jako přijímač. Opakovač signálu přijme GNSS signál, který následně nijak nemodifikovaný s časovým zpožděním znovu přehraje s vyšším výkonem, než má autentický GNSS signál. Tento opakovaný signál je díky vyššímu výkonu zpracovaný přijímačem GNSS signálu, který následně pracuje s chybnými informacemi o své poloze a čase.

Jedním ze specifik Meaconingu je odolnost vůči kryptografickým ochranným štítům, jejichž úkolem je zajištění ochrany integrity a autenticity přenášených zpráv, ovšem ochrana autenticity signálu je jimi opomíjena. V návaznosti na tuto mezeru v ochraně je tedy možná manipulace s funkcemi PNT přijímače pouhým znovu odvysíláním autentického signálu s časovým zpožděním. [10]

Vzhledem k tomu, že tyto útoky jsou prováděny vždy v závislosti na časovém posunu, je tedy možné rozpoznat začátek a konec takového útoku na základě porovnávání časové informace v přijímači. V případě útoku je totiž znatelná jasná nesouvislost mezi interním časem přijímače a časem GNSS.

Rozsáhlá publikace s názvem Understanding GPS Principles and Applications od autorů E. D. Kaplan a C. J. Hegarty na více než 700 stranách detailně popisuje systém GPS a možnosti jeho rušení. V úvodních kapitolách popisují základy družicové navigace a jednotlivé segmenty systému GPS. Navazují charakteristikami signálu včetně identifikace jednotlivých nosných pásem, dále se na téměř dvou set stranách věnují problému ovlivňování GPS signálu v důsledku vícecestného šíření signálu a šumu, působení ionosférických a troposférických vlivů včetně typů a zdrojů rušení a zdrojů chyb v měření času a polohy. V posledních kapitolách se kniha zmiňuje i o systému Galileo a dalších družicových navigačních systémech. [3]

Vzhledem k zaměření této práce na detekci rušení Jamming a Spoofing v prostředí kritické infrastruktury nebude v následující části práce již metoda Meaconing dále rozebírána. V následujícím textu, zabývajícím se detekcí rušení, jsou proto brány v úvahu pouze metody detekce Jamming a Spoofing. Rušením jsou nadále myšleny metody Jamming nebo Spoofing.

## 1.4 Detekce úmyslného rušení

Aby byla zajištěna správná funkčnost přijímače GNSS signálu a integrita přijímaného signálu, je nutno uvažovat i různé způsoby detekce chybného fungování způsobeného RFI nebo Spoofingem. Následně lze použít vhodné techniky pro eliminaci možných útoků a zvýšení ochrany proti možnému narušení, které jsou popsány v kapitole 1.3.

### 1.4.1 Detekce Jamming

V případě detekce rušení je Jamming jednoznačně nejjednodušší metodou na odhalení, jelikož dochází buď k úplným ztrátám příjmu GNSS signálu nebo jeho slábnutí na vstupu do přijímače a následnému zhoršení schopnosti určení polohy přijímače. Metody detekce jsou uvedeny v následujícím textu. Můžeme rozlišit šest metod, z nichž většina je založena na softwarovém přístupu:

- Detekce $C/N_0$ (Carrier to Noise Density Ratio),
- Detekce vyhodnocením odezvy Automatic Gain Control (AGC),
- Kontrola integrity Receiver Autonomous Integrity Monitoring (RAIM),
- Detekce vzájemné kros-korelace dvou přijímačů DRCC (Dual-receiver Cross-correlation),
- Ověření navigační zprávy NMA a
- Více prvková anténní konfigurace.

V souvislosti s rozsahem práce jsou dále blíže specifikovány pouze dvě metody detekce Jamming – detekce poměru $C/N_0$ a detekce vyhodnocením AGC.

#### 1.4.1.1 Detekce $C/N_0$ (Carrier to Noise Density Ratio)

Poměr Carrier to Noise ($C/N_0$) slouží k vyjádření poměru mezi intenzitou signálu nosné vlny a intenzitou šumu vztažené na šířku měřeného pásma. V principu, čím vyšší je poměr, tím vyšší je kvalita GNSS signálu na vstupu do přijímače. Tato hodnota je ovlivňována parametry GNSS přijímače a zároveň dalšími vstupními parametry (rozdíl ve výkonu družic, ztráty ve volném prostoru, atmosférické chyby, vícecestné šíření, změna zisku antény v závislosti na směru příchodu signálu – poloha družice). Tato metoda je specifická svou jednoduchostí implementace, vývoje a měření i nízkými požadavky na výpočetní techniku a zároveň poskytuje rychlé výsledky. V současné době jsou všechny přijímače GNSS signálu schopny měření $C/N_0$, vzhledem k tomu, že SNR přepočítané z $C/N_0$ je jedním z parametrů GNSS RAW dat. Nevýhodou této analýzy je ovšem její přesnost pouze ve statických případech,

v dynamických případech nejsou výsledky akurátní, jelikož není schopna rozlišit mezi snížením hodnoty $C/N_0$ z důvodu snížení síly GNSS signálu a zvýšením hodnoty rušivého signálu. Pokud budeme uvažovat pouze statické případy, je možné tuto metodu zutilizovat na statických místech k ochraně dlouhodobého majetku, k ochraně perimetru, a to zejména v místech, kde je zvýšený výskyt RFI (blízkost frekventovaných komunikací, parkovišť atd.). [4, 11, 12, 57]

#### 1.4.1.2 Detekce vyhodnocením odezvy AGC

Detekovat rušení lze jednoduše prostřednictvím součásti GNSS přijímače – AGC. Při přenosu GNSS signálu je cílem zachování konstantní amplitudy signálu na vstupu do analogově digitálního převodníku (ADC). V případě výskytu rušivých elementů typu Jamming se však dynamický rozsah přijímaného signálu značně zvýší, což vede k poklesu analogového zisku přijímače. V přijímači slouží AGC k zesílení přijímaného signálu na vstupu do přijímače s ohledem na intenzitu okolního šumu a ke změně analogového vstupního napětí na optimální úroveň ADC a současně zajištění relativně konstantního výstupního výkonu. Vzhledem ke značné citlivosti AGC na jakékoliv výkyvy v širokopásmovém šumu a na rušení kontinuální vlnou, lze náhlým poklesem zisku, spojeným s nárůstem výkonu v pásmu GNSS určit možné rušení. [13, 14]

### 1.4.2 Detekce Spoofing

Oproti Jamming jsou útoky Spoofing mnohem více sofistikované, a tudíž i jejich detekce vyžaduje větší úsilí. Při spoofingovém útoku nedochází k výpadkům nebo ztrátám příjmu GNSS signálu, přijímač totiž stále přijímá signál, který ovšem může být falešný, což je mnohem hůře identifikovatelné než při pouhém přerušení příjmu. Možnosti, jak detekovat Spoofing jsou následující:

- Detekce náhlých výkyvů a zvýšení výkonu signálu
- sledování odchylky pozice přijímače a systémového času
- ověřování šifrováním
- sledování vzájemné geometrie

#### 1.4.2.1 Detekce náhlých výkyvů a zvýšení výkonu signálu

Přijímač GNSS signálu v průběhu správného fungování ukazuje téměř konstantní hodnoty klíčových veličin. Nejjednodušší metodou detekce Spoofing se tedy jeví být porovnávání výkonu přicházejícího signálu do přijímače v určitém časovém úseku. Podstatou je sledování

náhlých skokových nárůstků přijímané nosné amplitudy ($A_i$), fáze nosné vlny nebo nosné fáze kódu a porovnávání přijímaných hodnot $A_i$ a referenčních hodnot automatického vyrovnávání citlivosti. Jejich náhlé rychlé nárůstky oproti referenčním hodnotám značí začátek spoofingového útoku. Podstata spoofingové útoku (viz kapitola 1.3.4) je totiž ve zvyšování výkonu falešného signálu, dokud přijímač nezachytí falešný signál, který je mu podsunut a autentický signál je upozaděný, útočník pak může libovolně změnit polohu na falešnou, kterou přijímač bude považovat za autentickou. [9]

#### 1.4.2.2 Sledování odchylky pozice přijímače a systémového času

Tento druh detekce se zaměřuje na indikování neobvyklých odchylek v pozici přijímače a systémového času. V případě sledování chyby hodin přijímače se detekce zaměřuje na náhlé rychlé změny, kdy je rychlost posunu odchylky větší, než je specifikovaná standardní chyba pro danou třídu oscilátoru instalovaného v přijímači. Pokud nastane takový jev, je téměř jednoznačné, že dochází v daný moment ke spoofingovému útoku. Chyba hodin přijímače a zároveň i výše tolerované odchylky závisí na instalované třídě oscilátoru (krystalový, rubidiový, tepelně kompenzovaný, vodíkový oscilátor atd.). Kromě chyby hodin přijímače lze sledovat odchylky v pozici přijímače včetně rychlosti změny. K tomu lze využít Inerční měřící jednotku (IMU) nebo jiný pohybově citlivý senzor, který detekuje neúměrné změny rychlosti a pozice přijímače. [4, 9]

#### 1.4.2.3 Ověřování šifrováním

Mezi způsoby detekce lze zařadit i kryptografické ověřování (šifrování) pro zabezpečení GNSS signálu proti spoofingovým útokům. Při kryptografickém ověřování lze použít dva způsoby, buď symetrické nebo asymetrické šifrování. Symetrický způsob šifrování vytváří silnější ochranu proti útokům, jelikož zahrnuje šifrování celého vysílaného signálu. Vysílající družice a ověřený přijímač v sobě nesou kopii tohoto klíče, který ověřuje autenticitu přenášeného signálu. Elementárním principem tohoto způsobu ověřování je digitální podepisování vysílaných družicových zpráv, kdy přijímač kontroluje veškeré přijímané zprávy oproti svému digitálnímu podpisu, který sdílí s vysílající družicí. Zprávy, jejichž podpis není přijímač schopen rozšifrovat, jsou následně zamítnuty. [4, 9]

#### 1.4.2.4 Sledování vzájemné geometrie

Jedním ze způsobů detekce Spoofing je sledování směru příchodu signálu. U této metody detekce jsou k přijímači GNSS signálu připojeny tři nebo více antén s rozdílnými vzdálenostmi od přijímače vytvářející vzájemné pole. Díky tomu je možné v přijímači určit

směr příchodu rušení s odchylkou ~ 3° v případě vzdálenosti mezi přijímačem a anténou $\Delta d=0,1$ m. V případě normální funkčnosti jsou vektory směru příchodu signálu k přijímači rovnoměrné v závislosti na aktuální konstelaci družic. Typický systém detekce Spoofing na základě vzájemné geometrie měří, zda přijaté fáze nosné vlny $\phi_i$ na vícero anténách jsou konzistentní s rozdíly vektorů směru příchodu signálu (případ u autentického signálu) nebo naopak vykazují jednotnost směru, což je typické pro vysílače Spoofing s jednou anténou. [9]

# 2 Kritická infrastruktura obecně

V této kapitole práce definuji pojem kritická infrastruktura, který se následně bude prolínat do praktické části práce. V prvé řadě je teoreticky uvedeno, co se pod pojmem kritická infrastruktura skrývá, podněty pro úpravu tohoto odvětví a její vymezení v legislativě Evropské unie (EU) a České republiky (ČR). Navazující podkapitola již spojuje kritickou infrastrukturu s využíváním GNSS signálu, vymezuje sektory, které pro zajištění svých funkcí využívají GNSS a konkrétní sektory jsou spojené s jednotlivými službami PNT, které GNSS poskytuje. Z konkrétních sektorů využívajících GNSS jsou specificky popsány elektronické komunikační sítě, servery burzovních systémů, energetické distribuční sítě a energetické přenosové soustavy. Z dopravy jsou vybrány sektory letecké dopravy a pozemní infrastruktura.

Pojem kritická infrastruktura je vykládán v mnoha zdrojích poměrně obecně, ovšem jedná se o velmi rozvětvenou problematiku týkající se bezpečnosti mnoha odvětví. Obecně, dle zákona č. 240/2004 Sb., lze pojem CI definovat jako „*prvky nebo systémy (stavby, zařízení, prostředky nebo veřejná infrastruktura) a jejich provozovatelé, v jejichž případě by narušení jejich funkce mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu*“. [47]

S vývojem moderní společnosti postupně začaly přicházet podněty otevírající téma kritické infrastruktury a zejména její ochrany. Jednoznačným impulsem k započetí diskuse o potřebě ochrany kritické infrastruktury byly teroristické útoky v 90. letech 20. století (v New Yorku rok 1993 a v Oklahoma City rok 1995). Odezvou bylo Prezidentské rozhodnutí PDD-39 z června 1995 ustanovující skupinu oborníků CIWG, jejímž úkolem bylo zkoumat problematiku ochrany kritické infrastruktury. Na základě poznatků této skupiny byl v červenci 1996 prezidentem Clintonem vydán základní dokument upravující ochranu kritické infrastruktury (Executive order 13010) a rovněž zřizující Prezidentskou komisi na ochranu CI (PCCIP). Ta vydala v roce 1997 report (Critical Foundations) stanovující oblasti CI a zahrnující: energetické sítě, vodní hospodářství, potravinářství a zemědělství, plynárenský a ropný průmysl, dopravní systémy, komunikační a informační systémy, bankovní a finanční sektor, záchranné služby a veřejnou správu.

S postupem ve vývoji globálních družicových navigačních systémů GNSS (zejména GPS), došlo k jejich nedílnému zapojení a aktivnímu využívání v kritické infrastruktuře, kde se staly důležitým prvkem zajištění spolehlivosti a integrity. Služby PNT poskytované v rámci GNSS jsou v současnosti využívány mnoha sektory CI, zejména pro synchronizaci času systémů

CI. Funkce přesného časování je využívána například k časové synchronizaci přenosové a distribuční soustavy elektrické energie, u kterých v současné době roste decentralizace a zároveň se stávají složitější na synchronizaci. V případě informačních a komunikačních sítí je rovněž využívána synchronizace času prostřednictvím signálu GNSS u BTS stanic mobilních telefonních sítí. Další kritickou sítí se stává stále používanější systém eCall, celoevropský systém tísňového volání využívající družicové navigace. V případě letecké dopravy je jednou z klíčových fází letu přiblížení na přistání, kde je využíváno přiblížení na přistání pomocí GNSS a je nutné dodržet vysokou přesnost a spolehlivost přijímaného signálu a nejen to. Řízení letového provozu (ŘLP) využívá GNSS pro synchronizaci svých systémů, které poskytují veškeré řídící funkce. Pokud zůstaneme u dopravy, v současné době se přechází u výběru mýtného na pozemních komunikacích na systémy, které využívají k lokalizaci vozidla GNSS a tzv. virtuální mýtné stanice. Vozidlo má v takovém případě na palubě palubní jednotku, která prostřednictvím GSM předává data o své poloze přijatá z družic centrálnímu systému.

To ovšem vede ke skutečnosti, že případné narušení příjmu GNSS signálu může mít fatální následky. V případě energetické přenosové soustavy a distribučních sítí může v nejvážnějších situacích dojít black-outům, jak se již stalo v USA, což má za následek vysoké finanční ztráty. Rozbor příčin a následných doporučení v souvislosti s tímto black-outem jsou rozsáhle popsané ve vládním dokumentu Final Report on the August 14, 2003 Blackout in the United States and Canada[6], vydaném bezprostředně po této události, odkaz na dokument je uveden v poznámce po čarou. Pokud by došlo k narušení GNSS signálu u systému eCall, zvýšila by se tak jeho nespolehlivost a pro záchranné složky by to znamenalo značné ztížení komunikace. Pokud budeme mluvit o letecké dopravě, pak i zde má rušení GNSS signálu značný vliv na bezpečnost provozu. Zejména v konečných fázích přiblížení na přistání, což je jedna z nekritičtějších fází letu, kde by v případě rušení signálu mohlo dojít i k nehodě.

## 2.1 Kritická infrastruktura v legislativě EU

Otázkou CI se zabývá legislativa EU, která upravuje jednotlivá sdělení a směrnice pro členské státy. Zakotvení CI do legislativy EU je stále předmětem jednání. Prvním materiálem vydaným na území EU, bylo sdělení Komise Radě a Evropskému parlamentu Ochrana

[6] Odkaz na dokument Final Report on the August 14, 2003 Blackout in the United States and Canada: https://www3.epa.gov/region1/npdes/merrimackstation/pdfs/ar/AR-1165.pdf

kritické infrastruktury při boji proti terorismu[7] z roku 2004. Toto sdělení obsahuje specifikaci pojmů *Hrozba*, *Kritická infrastruktura*, dále vymezuje oblasti CI a faktory pro jejich určování a ochranu, poskytuje přehled současných opatření k tématu CI a navrhuje další možná opatření, která by vedla ke zvýšení účinnosti stávajících nástrojů. V souvislosti se zvyšováním bezpečnosti CI je v dokumentu podnět pro vytvoření Evropského programu na ochranu kritických infrastruktur (EPCIP) a Výstražné informační sítě kritické infrastruktury (CIWIN).

Na evropské půdě je pojem CI pevně zakotven v dokumentu COM/2005/0576, Zelená kniha o evropském programu na ochranu kritické infrastruktury[8], vydaném evropskou komisí. Tento dokument si klade za cíl zapojit velké množství subjektů a získat od nich konkrétní informace, které lze uplatnit při zvyšování účinnosti ochrany CI, a to na základě komunikace, koordinace a spolupráce na národní a evropské úrovni. Je zde uveden základní rámec EPCIP, definována evropská CI (ECI) a národní CI (NCI).

V prosinci 2006 vydala Komise Sdělení o Evropském programu na ochranu kritické infrastruktury. „*Sdělení stanovuje zásady, procesy a nástroje navržené pro provádění programu EPCIP. Ohrožení, na něž má program reagovat, se netýkají jen terorismu, ale patří sem také trestné činnosti, přírodní nebezpečí a další důvody nehod na principu stejného přístupu pro veškerá ohrožení.“* [15]

Následně bylo v prosinci 2008 Evropským parlamentem podáno usnesení o Návrhu Směrnice Rady EU o určování a označování evropské CI a o posouzení potřeby zvýšit její ochranu. Komise v období 2007-2012 financovala více než 100 různých projektů v rámci programu prevence, připravenosti a zvládání následků terorismu a dalších bezpečnostních rizik (CIPS). V roce 2013 přijala Komise návrh dokumentu 2013 Working Staff Document, který otevírá nový přístup k EPCIP. Představuje revidovanou a praktičtější implementaci činností v rámci tří hlavních pracovních postupů – prevence, připravenost a reakce. Nový přístup má za cíl vytvořit společné nástroje a společný přístup v EU k ochraně a odolnosti kritické infrastruktury, přičemž lépe zohlední vzájemnou závislost. [60]

[7] Odkaz na dokument Sdělení Komise Radě a Evropskému parlamentu Ochrana kritické infrastruktury při boji proti terorismu: http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:52004DC0702&from=EN

[8] Odkaz na dokument Zelená kniha o evropském programu na ochranu kritické infrastruktury: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:52005DC0576&from=CS

## 2.2 Kritická infrastruktura v legislativě ČR

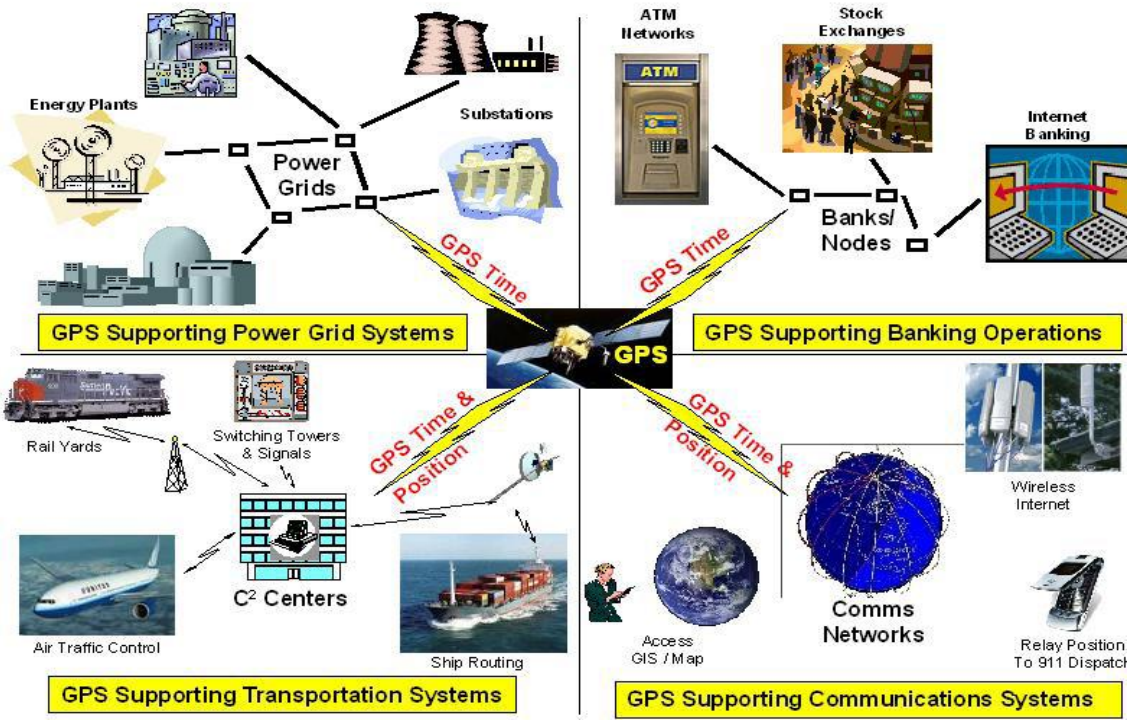
Na území ČR kritickou infrastrukturu vymezuje legislativa v Krizovém zákoně, zák. č. 240/2000 Sb., pozměněný zákonem č. 430/2010 Sb. Dále Nařízení vlády č. 432/2010 o kritériích pro určení prvku kritické infrastruktury, které definuje odvětvová kritéria CI ve specifických oblastech: energetika, vodní hospodářství, potravinářství a zemědělství, zdravotnictví, doprava, komunikační a informační systémy, finanční trh a měna, nouzové služby a veřejná správa, pozměno Nařízením vlády č. 315/2014. Mezi tato odvětvová kritéria spadá Letecká doprava, konkrétně Řízení letového provozu, a to přibližovací služba řízení a letištní služba řízení letiště určeného jako kritická infrastruktura nebo oblastní služba řízení poskytující letové provozní služby včetně ŘLP ve vzdušném prostoru České republiky. V souvislosti s ŘLP a zejména s touto diplomovou prací je třeba zmínit, že tato výše zmíněná příloha definuje i odvětví Komunikační a informační systémy, jejichž nedílnou součást tvoří část Technologické prvky pro družicovou komunikaci, což se týká z velké části této práce.

Problematice CI se také věnují prováděcí předpisy a metodiky[9] Hasičského záchranného sboru ČR (HZSČR), včetně různých směrnic a metodik vydaných Ministerstvem vnitra ČR (MVČR), například metodika MVČR k zpracování plánů krizové připravenosti subjektu CI podle nařízení vlády č. 462/2000 Sb. Podmínky pro řešení problematiky kritické infrastruktury na národní úrovni řeší zákon č. 118/2011 Sb. [16]

## 2.3 Využití GNSS v kritické infrastruktuře

Zabezpečení funkčnosti kritické infrastruktury je v mnoha ohledech závislé na příjmu GNSS signálu. Ten je v systémech CI využíván k časové synchronizaci systémů, navigaci i určení přesné pozice. Mezi subjekty kritické infrastruktury využívající funkci *synchronizace času* patří energetická přenosová soustava a distribuční sítě a bankovní operace. Funkci *synchronizace času* dohromady s *navigační funkcí* a *funkcí určení přesné pozice* aktivně využívají přepravní systémy v letecké, vlakové a lodní dopravě, dále tyto funkce využívají komunikační systémy a sítě, kam lze zařadit operátory mobilních sítí využívající funkce pro přenos bezdrátového internetu a systémy tísňového volání.

[9] Odkaz na prováděcí předpisy a metodiky HZSČR: http://www.hzscr.cz/clanek/dokumenty-ke-stazeni.aspx




*Obrázek 4: Využití GPS aplikací v civilním sektoru, zdroj: [17]*

Celkem 15 sektorů CI využívá funkci časové synchronizace podle GNSS, celkem pro 11 sektorů CI (komunikační služby, záchranná služba, ICT, bankovnictví a finance, zdravotnictví, elektrická energie, nukleární energie, přehrady/vodní elektrárny, chemický průmysl, kritická výroba, poštovní služby, doprava, vládní sektor, obrana a komerční sektor) je tato funkce klíčová k zajištění správné funkčnosti systémů. Mezi hlavní oblasti užití se řadí síťová a fázová synchronizace v drátovém i bezdrátovém přenosu v informačním a komunikačním sektoru, přesné generování frekvencí a jejich stabilizace pro jedno frekvenční bezdrátové sítě, fázová synchronizace v Energetickém sektoru, časové plánování, kontrola a synchronizace při zpracování ropy a zemního plynu a jejich následné distribuce, časové značení dat a transakcí u vysokofrekvenčního obchodování v Bankovním a Finančním sektoru.

Co se týká funkce navigace, ta nachází v CI hlavní využití v dopravním sektoru. V letecké dopravě GNSS umožňuje trojrozměrné stanovení polohy letadla ve všech fázích letu (vzlet, traťové vedení, přistání a následně vedení po letištních plochách), data z GNSS mimo jiné využívá palubní systém varování před srážkou se zemí Groung Proximity Warning System (EGPWS), redukující riziko kontrolovaného letu do terénu Controlled Fligth into Terrain (CFIT). Dalším dílčím uživatelem dopravního sektoru je železniční přeprava osob a nákladu, kde GNSS nachází uplatnění zejména při snižování počtu nehod, zpoždění a celkových nákladů dohromady se zvyšováním železniční kapacity. GNSS umožňuje sledování polohy

vlaků a jejich pohybu i v odlehlých oblastech, kde nejsou jiné sledovací systémy dostupné. Klíčové je i využití GNSS v lodní dopravě, kde slouží v prvé řadě jako systém *Search and Rescue* (SAR) pro lodě nacházející se v odlehlých oblastech oceánu. Dále slouží k mapování mořského dna a k lokalizaci navigačních nebezpečí a k řízení provozních operací v lodních přístavech. [17]

Kritickou součást nouzových systémů včasného varování tvoří GNSS lokalizace u subjektů poskytujících nouzové služby při zajišťování veřejné bezpečnosti a při zmírňování dopadů katastrof. Dochází k časovým úsporám při záchranných operacích díky přesné lokalizaci vozů a vzájemné komunikaci subjektů Integrovaného záchranného systému (IZS).

Moderní civilizace je do jisté míry závislá na komplexním propojeném systému komunikace, dopravní dostupnosti, přenosu elektrické energie, dostupnosti finančních zdrojů, a mnohých dalších, dohromady tvořících prvky kritické infrastruktury. Jednotlivé prvky kritické infrastruktury, využívající pro zachování své integrity, autenticity a dostupnosti signálu GNSS, jsou popsány níže.

### 2.3.1 Elektronické komunikační sítě

Signálu GNSS je hojně využíváno k časové synchronizaci informačních, telekomunikačních a komunikačních sítí včetně internetu.

Pevné telefonní sítě využívají GNSS jako zdroj časové informace. Digitální telekomunikační sítě jsou tvořeny datovými pakety, které jsou po sítí průběžně přenášeny konstantní rychlostí definovanou na základě šířky pásma dané sítě. Aby bylo zajištěno, že se konkrétní datový paket dostane do konkrétní lokace bez chyb, musí mít tyto stanice stejný referenční čas. K synchronizaci času je využíváno právě GNSS To umožňuje lokálním operátorům kalibrovat lokální časovací zařízení, což v porovnání s časem nastaveným dle atomových hodin přináší značné finanční úspory. V případě pevných telekomunikačních sítí jsou pro zajištění časové synchronizace využity celkem tři zdroje, aby byla zajištěna odolnost vůči náhlým výpadkům jednoho ze zdrojů. Pevné sítě jsou schopny udržet svou synchronizaci po značný časový úsek, v případě použití rubidiového oscilátoru je tato perioda až tři týdny. Po tuto dobu nemusí být výpadek příjmu GNSS signálu vůbec zaznamenán.

Na rozdíl od pevných telekomunikačních sítí je mnohem větší zranitelnost v případě rušení GNSS signálu u mobilních telekomunikačních sítí, které z velké části využívají GNSS k časové synchronizaci, konkrétně kódový multiplex CDMA. Každá z vysílacích stanic CDMA vysílá v rozdílném čase, proto je vyžadována velmi přesná synchronizace zajišťující

bezproblémové převzetí mezi jednotlivými mobilními zařízeními. V případě využití GNSS jsou základny synchronizovány s časovou přesností ≤ 1 μs, podmínkou je zachování synchronizace dobu 8–24 hodin s přesností ≤ 10 μs. [18]

Dalšími sítěmi využívajícími GNSS k časové synchronizaci jsou vysílací stanice digitálního televizního vysílání. V případě nedostupnosti GNSS signálu zůstávají sítě synchronní v řádech hodin podobně jako u mobilních telekomunikačních sítí. Delší výpadky příjmu signálu mají za následek zhoršení jak obrazového, tak zvukového záznamu. Dlouhodobé výpadky příjmu signálu vedou k celkové desynchronizaci a následnému rozladění sítě, což způsobuje, že každý vysílač se stává rušičkou „Jammer“ ostatních přijímačů v síti. [4]

### 2.3.2 Servery burzovních systémů

Množství uskutečněných finančních transakcí dosahuje denně závratných čísel. Obraty ve finančním sektoru jsou v řádech miliard USD za minutu, roční obrat burzovních operací je dle A. F. Bacha, hlavního architekta pro finanční služby ve společnosti Juniper Networks, v řádech desítek kvadrilionů USD. Takový objem finančních transakcí vyžaduje přesnou časovou synchronizaci. V současné době využívají finanční instituce systém Building Integrated Timing System (BITS), který využívá k synchronizaci informace o čase a datu z GNSS. BITS má ovšem i své vlastní atomové hodiny, které jsou schopny generovat časové informace nezávisle na sobě. Přesná synchronizace jednotlivých finančních organizací mezi sebou, se nyní stává více než dříve rozhodujícím faktorem. [25]

Finanční sektor vyžaduje časové značení transakcí, aby byla zajištěna převládající cena v momentě zaúčtování transakce. Přesná synchronizace mezi geograficky vzdálenými finančními platformami je nutná zejména u vysokofrekvenčního obchodování (přesná definice ve Směrnici Evropského Parlamentu a Rady 2014/65/EU). V této oblasti je synchronizace finančních transakcí pomocí GNSS již dlouho využívána. Tento trend by měl dle GNSS Market Report z 2017 pokračovat i s příchodem nových regulatorních opatření, která budou od finančních operátorů vyžadovat přesnou sledovatelnost transakcí vzhledem k času Universal Time Coordinated (UTC) pomocí časových značek v řádu mikrosekund. [26, 27]

Časové značení operací je u bank vyžadováno s přesností 1ms s ohledem k UTC, u vysokofrekvenčního obchodování je požadovaná přesnost 1μs. Vysokofrekvenční obchodování je krátkodobé obchodování ve velkém objemu, závislé na přesně počítačově stanovených algoritmech. Systémy využívané vysokofrekvenčními obchodníky jsou zejména sofistikované oscilátory, schopné zaručit pokračování obchodu i dlouho po ztrátě externího

zdroje časování. Stejný systém je využívaný i při obchodování na burzách cenných papírů. Množství uskutečněných transakcí vysokofrekvenčních obchodníků může být i v řádech tisíců za den, což je možné pouze díky velice přesnému časování. [18]

Rušení GNSS signálu pomocí Spoofing může mít v případě finančních operací závažné dopady. Záměrné ovlivnění časové synchronizace může zabránit vstupu akcií na trh, což se stalo v USA v roce 2010, kdy došlo ke kolapsu akciového trhu a ztrátě tržní hodnoty akcií v řádu jednoho bilionu USD. V druhém případě dochází pomocí Spoofing k neoprávněným výhodám při tržním obchodování, což je kvůli získání několika milisekundových výhod využíváno ve finančních kybernetických útocích. [4]

### 2.3.3 Energetické přenosová soustava a distribuční sítě

V energetice se funkcí GNSS využívá zejména k fázování energetické přenosové soustavy a distribučních sítí, k optimalizaci dodávek eklektické energie v závislosti na aktuální poptávce koncových uživatelů, k zajištění efektivní koordinace v elektrárnách, dále k identifikaci a přesné lokalizaci poruch a přerušení v síti. Zmíněné procesy převážně využívají funkci časové synchronizace, ovšem například při lokalizaci poruch v distribuční síti je využita i funkce přesné lokalizace.

S rozvojem chytrých sítí, které do své soustavy zapojují neprediktivní zdroje elektrické energie (obnovitelné zdroje energie – solární elektrárny, větrné elektrárny, vodní elektrárny), vychází najevo dosud opomíjený problém vypořádání s přebytečnou energií nebo naopak pokrytí poptávky ve špičce. Moderní energetika se přiklání k jisté míře decentralizace elektrických sítí, tzv. Smart Grid, která je specifická využitím digitálního sběru dat jak od koncových spotřebitelů, tak i od dodavatele elektrické energie v návaznosti na jeho aktuálním chování a aktuální spotřebě/dostupnosti. Díky sběru a vyhodnocování dat lze zautomatizovat a zvýšit efektivitu, spolehlivost a udržitelnost produkce a distribuce elektrické energie současně s minimalizováním ekonomických nákladů. Při zapojení autonomních prvků elektrické energie do energetické soustavy a její decentralizaci, musí fungovat vzájemná synchronizace, která je zajištěna právě pomocí služby přesné časové synchronizace podle GNSS. [4, 19]

Přenosová soustava využívá GNSS signál jako zdroj časové synchronizace rozvodných stanic a pro fázorové měření stavu přenosové soustavy. Využití fázorových měřících jednotek (PMU) umožňuje monitorování celé soustavy, včetně monitorování a ochrany monitorovacích systémů Wide Area Monitoring System (WAMS) a Wide Area Control System (WACS). Dostupnost GNSS signálu je pro přenosovou soustavu klíčová z hlediska

zajištění synchronního přenosu elektrické energie mezi jednotlivými rozvodnami a transformace z přenosové do distribuční sítě. [50, 51]

### 2.3.4 Letecká doprava

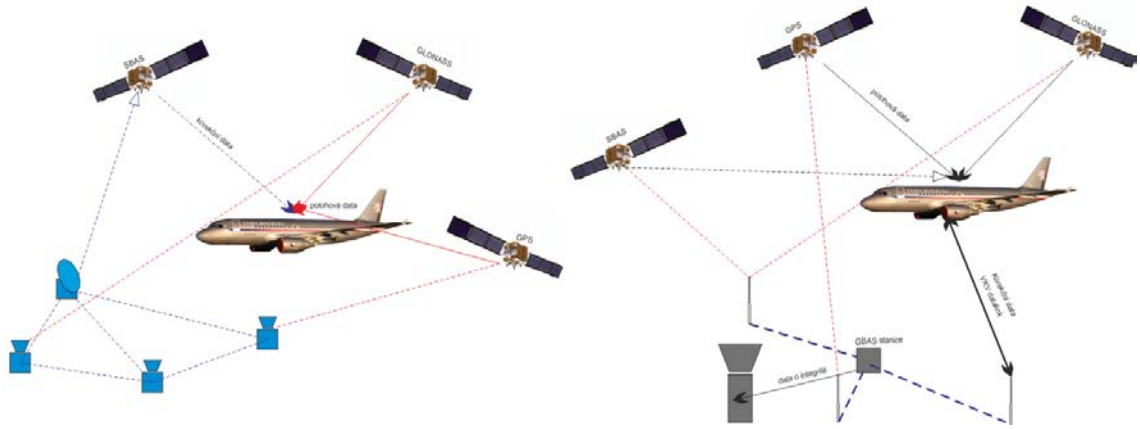
Letecká doprava je jedním ze subjektů kritické infrastruktury, pro který je využití GNSS velmi důležité. Při současném vývoji a zvyšující se hustotě leteckého provozu je potřeba doplnit současně využívané radionavigační prostředky tak, aby byla zajištěna dostatečná bezpečnost provozu. V posledních letech je pro leteckou navigaci stále více využíváno GNSS nahrazující tradiční radionavigační prostředky a pozemní a inerční systémy. To je způsobeno tím, že stále více provozovatelů se přiklání k pokročilým navigačním postupům Performance Based Navigation (PBN) a k družicovým navigačním technologiím, stále více využívaných Air Navigation Service Providers (ANSP). [20]

PBN – RNAV (Performance Based Navigation – Area Navigation) je prostorová navigace traťového vedení letadla po předem určené trati, založená na výkonnosti/přesnosti Required Navigation Performance (RNP). Pro RNP přiblížení je jako hlavní navigační prostředek využíváno GNSS, ovšem navigační výkonnost nemusí být vždy stoprocentní a systém sám o sobě není schopný zjistit nedostupnost GNSS signálu, proto jsou využívány zpřesňující systémy SBAS, GBAS a ABAS.

Vývoj v navigačních prostředcích určuje zvyšující se hustota provozu. Na základě toho byl v Evropě uveden program Single European Sky Air Traffic Management Research (SESAR), který směřuje k modernizaci systému řízení letového provozu v Evropě. Mezi hlavní trendy se řadí posun k družicové navigaci se zachováním pozemní zálohy, ale i bez ní je například na nařízených letištích poskytováno vertikálního vedení letadel po trati a implementace PBN. Tento směr ve vývoji navigace v letectví může být zajištěn kombinací GNSS navigace, samostatných navigačních systémů a konvenčních navigačních prostředků. Přechod k GNSS navigaci umožní vyřazení některých navigačních prostředků jako je VOR a NDB/ADF čímž dojde k uvolnění radiového spektra pro nově vznikající letecké služby. [21, 56]

Kromě traťového vedení je GNSS využíváno k přesnému přiblížení na přistání, které je jednou z nejrizikovějších částí letu a současně je také nejvíce dostupné úmyslnému rušení Jamming. Z tohoto důvodu provozovatelé letišť nadále zachovávají zálohování v podobě DME, ILS (MLS). Pro zlepšení přesnosti GNSS zařízení se využívají zpřesňující systémy ABAS, GBAS a SBAS. ABAS je systém integrovaný v GNSS přijímači, který slouží pro samostatnou kontrolu integrity přijímaného signálu pomocí automatického příjmu signálu

z více družic zároveň, což mu umožňuje určit družice vysílající špatný signál. Systém ABAS je vyžadován pro jakoukoliv RNAV navigaci na SID a STAR a přiblížení s využitím GNSS. GBAS je systém fungující na principu permanentních pozemních stanic se známou polohou (souřadnice letiště), stanice konstantně přijímají signál a měří rozdíly mezi známou a naměřenou hodnotou, na základě těchto hodnot určují korekce, které jsou následně odesílány radiovým signálem palubnímu přijímači. Znám je již případ, kdy docházelo k pravidelným výpadkům systému GBAS na letišti EWR, které byly způsobeny projíždějícím nákladním vozidlem po dálnici v bezprostřední blízkosti letiště, využívajícím PPD, viz kapitola 1.3.2. Třetí systém zajišťující integritu a přesnost přijímaného signálu je SBAS. Tento systém využívá k zpřesňování polohy sítě geostacionárních družic a sítě pozemních korekčních stanic rozmístěných v případě evropského systému EGNOS po celé Evropě. SBAS funguje na podobném principu pozemních stanic jako GBAS, avšak čítá mnohem více stanic. Ty měří nepřesnosti v oblasti svého umístění a vysílají je na geostacionární družice, které následně vypočítají a odešlou korekce do příslušného palubního zařízení. [22, 23]




*Obrázek 5: Princip systému SBAS (vlevo) a systému GBAS (vpravo) s využitím pozemních stanic, zdroj: airnav.eu*

Evropský systém SBAS se nazývá EGNOS a čítá celkem 40 pozemních referenčních monitorovacích stanic RIMS. Data z těchto stanic jsou odesílána do čtyř kontrolních center Master Control Center (MCC), které vyhodnocují nepřesnosti družic a data s korekcí jsou pomocí vysílacích stanic pak odeslána zpět družici, která následně data předává palubnímu přijímači (ten uplatňuje korekce na signál přijatý od družice). Podobně jako pro oblast EU funguje EGNOS, v USA je systém nazývaný WAAS. [24]

EGNOS poskytuje následující služby:

1) *základní služba (Open Service – OS)*
2) *služba "kritická" z hlediska bezpečnosti (Safety of Life service – SoL)*
3) *komerční služba "EGNOS Data Access Server" (EDAS)* [48]

### 2.3.5 ANSP – Poskytovatelé leteckých navigačních služeb

Poskytovatelé leteckých navigačních služeb a jimi využívané systémy jsou klíčovými uživateli GNSS v letectví, poskytování služeb na standardní úrovni je závislé na časové synchronizaci systémů prostřednictvím GNSS. Většina systémů vyžaduje přesné časování. Mezi tyto systémy se řadí časová synchronizace serverů pro zajištění časové synchronizace celé systémové sítě, záložní radarové systémy využívající multilateraci nebo systémy datových převodů. Všechny tyto systémy využívající k synchronizaci příjmu GNSS signálu jsou bezpečné i v kritických situacích. Vzhledem k tomu že vykazují zálohy buď systému jako celku i jednotlivých subsystémů, zvládají výpadky příjmu GNSS signálu v řádech desítek minut až dní. Odolnost systému tzn. čas, po který nejsou zaznamenány negativní vlivy z důvodu rušení signálu, je samozřejmě závislý na typu použitého oscilátoru. Vysoce kvalitní oscilátory jsou použity u klíčových systémů pro synchronizaci serverů. Ty jsou rozmístěny v různých místech poskytovatele služeb řízení letového provozu a mezi sebou propojeny do sítě, což ještě více zvyšuje jejich odolnost proti externímu rušení. I když se díky těmto obranným mechanismům prakticky eliminuje vliv rušení GNSS signálu, je třeba tento problém neodsouvat a brát v úvahu jeho vliv i na ostatní letištní systémy například pro přiblížení na přistání. [2]

### 2.3.6 Pozemní infrastruktura

#### 2.3.6.1 Družicový výběr mýtného

Výběr mýtného na silnicích pro vozidla nad 3,5 t přináší značný finanční přínos pro státní pokladnu a umožňuje monitorovat kvantitu nákladního provozu na silnicích. Stavba jakéhokoliv mýtného systému se řídí Směrnicí Evropského Parlamentu a Rady 2004/52/ES o interoperabilitě elektronických systémů pro výběr mýtného ve Společenství. V současné době existují tři možnosti výběru mýtného. První je mikrovlnná komunikace v mikrovlnném pásmu radiových kmitočtů na frekvenci 5,8 GHz s použitím technologie komunikace na krátké vzdálenosti (DSRC), která je využívaná pro výběr mýtného v USA, Japonsku a převládá ve státech EU. V principu výběr mýtného funguje tak, že palubní jednotka (OBU) umístěná na palubě vozidla odešle informaci mýtné bráně ve své bezprostřední blízkosti a je tak určena konkrétní poloha vozidla vzhledem k poloze mýtné brány. Data jsou následně z mýtné brány odesílána do centrálního systému vypočítávajícího mýtnou povinnost vozidla. Mikrovlnný mýtný systém je vhodné využít pro frekventované páteřní sítě (dálniční sítě), kde je kvůli velkému množství projíždějících vozidel potřeba i velké množství levných OBU. [28]

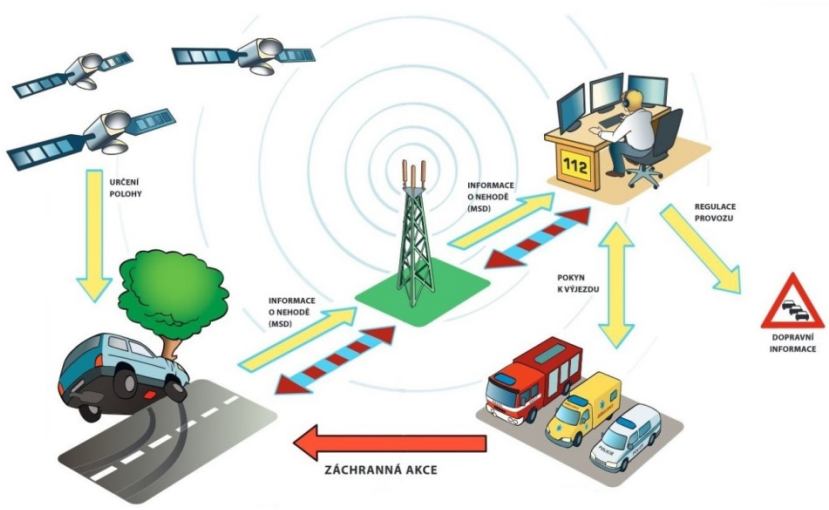
Druhá možnost výběru mýtného uvažuje o využití družicového systému. Tyto systémy využívají k lokalizaci vozidla navigační systémy GNSS. Palubní přijímač zároveň přijímá GNSS signál, prostřednictvím kterého určuje svou polohu a průběžně odesílá tyto informace o své aktuální poloze do centrálního elektronického mýtného systému. K odesílání dat o své poloze je využíváno mobilní sítě (GSM). Na rozdíl od mikrovlnného výběru mýta není potřeba stavět fyzické mýtné brány, které při průjezdu vozidla zaznamenají jeho polohu, jelikož jednotlivé mýtné brány jsou pouze virtuálně zaneseny v mapových datech palubní jednotky. Při průjezdu virtuální mýtnou branou je zaregistrován její průjezd a následně vypočítána výše mýtného. Výhodou oproti stanovení mikrovlnného mýtného je jeho vypočítání přímo palubní jednotkou OBU, což značně snižuje nároky na komunikaci mezi jednotkami. Naproti tomu jsou zde vyšší nároky na vybavení vozidel zahrnující komplexnější software a hardware palubních jednotek. Výběr mýtného pomocí družicového systému je vhodné použít pro plošné zpoplatnění komunikací, kde by bylo značně nereálné provádět nákladnou výstavbu fyzických bran mikrovlnného výběru mýtného. Tento způsob je v současnosti plně implementovaný v Německu a na Slovensku, kde využívá signálu GPS.

Třetí možností výběru je tzv. hybridní mýtný systém, který spojuje mikrovlnný systém a družicový systém do jednoho. Data o pohybu vozidel mohou být centrálním systémem zpracována jak z přenosu z fyzických mýtných bran, tak i z družicových palubních jednotek. Je zde taktéž využíváno mobilní sítě GSM pro odesílání polohových informací vozidla do centrálního systému. [29]

Výběr mýtného pomocí družicových technologií může být jednoduchým terčem útoků Jamming a Spoofing, jak již bylo zmíněno výše v kapitole 1.3.2. Řidiči nákladních vozidel totiž často využívají rušiček PPD, které brání třetí straně lokalizovat vozidlo. Tímto způsobem může být omezena schopnost virtuálních mýtných bran přesně určit polohu daného vozidla a není tudíž správně uplatněna mýtná povinnost. Mimo jiné tento způsob rušení může mít fatální vliv i na jiné subjekty kritické infrastruktury v případě pohybu vozidla vybaveného PPD v jejich bezprostřední blízkosti.

#### 2.3.6.2 Systém eCall

Novinkou zavedenou u pozemní infrastruktury je povinnost pro nová silniční vozidla (osobní a nákladní vozidla do 3,5 t) využívat systém automatického tísňového volání eCall. Účelem zavedení tohoto systému je zmírnění dopadu dopravních nehod a zvýšení celkové bezpečnosti silničního provozu v členských státech EU. eCall je veřejná služba spojující tři základní složky: palubní jednotku eCall integrovanou výrobcem ve vozidle, sítě mobilních operátorů a složky integrovaného záchranného sboru 112.




*Obrázek 6: Princip fungování systému eCall, zdroj: czechspaceportal.cz*

Princip systému je založen na automatickém sestavení tísňového hovoru na linku 112, kde jsou pracovníci okamžitě informování o času nehody, přesné poloze vozidla, typu vozidla a počtu cestujících prostřednictvím mezinárodně kompatibilní zprávy. Existují dvě možnosti sestavení tísňového volání, buďto automatické (například při nárazu vozidla), kdy jsou pracovníkovi linky 112 automaticky sděleny informace o nehodě, anebo je další možností manuální stisknutí tísňového tlačítka, kdy je posádka ve vozidle je následně spojena k telefonickému hovoru. Informace o nehodě jsou operátorovi tísňové linky dostupné v časovém rozmezí 14-17 minut bezprostředně po události. V systému je použita „spící“ SIM, která se aktivuje pouze v případě aktivace palubní jednotky (tzn. při nehodě). Následně je pak umožněno zavolat zpět do vozidla. K určení polohových dat využívá GNSS, jednotka zároveň ukládá poslední tři pozice vozidla. Je tedy samozřejmé, že pokud by vozidlo využívalo jakýchkoliv PPD se snahou zamezit třetím stranám určení své polohy, může tak ohrozit život nejen sobě, ale i vozidlům, které tento systém využívají a nacházejí se v dosahu rušivého signálu. [30, 31]

# 3 Průzkum aktuálně dostupných řešení pro detekci rušení Jamming a Spoofing a jejich dílčí charakteristiky

Na následujících stranách jsou popsány produkty a projekty zabývající se problematikou detekce rušení GNSS signálu. V prvé části byla provedena analýza vědecko-výzkumných projektů, které vznikly za spolupráce akademické sféry v zahraničí. Patří sem projekty GAARDIAN, SENTINEL, Detector, GMCA, TIGER a FENIX. Druhá část analyzuje charakteristiky komerčních produktů aktuálně dostupných na trhu. Sem patří produkty CTL3510 a CTL3520 + CTL8200 společnosti Chronous Technology, produkt GNOME od společnosti IDS, produkt GISMO společnosti NSL a produkt BroadShield společnosti Spectaracom. Tato analýza je důležitým prvkem této práce, jelikož její výsledky souvisejí s budoucí možností uplatnění produktu Detektor, vyvinutého v rámci ČVUT, na který současně práce navazuje. V kapitole 1.4 jsou uvedené různé způsoby detekce rušení typu Jamming a Spoofing, v návaznosti na to jsou v této kapitole uvedeny projekty a produkty, které využívají těchto detekčních metod.

## 3.1 Inovační a výzkumné projekty zabývající se problematikou

Inovačními a výzkumnými projekty jsou myšleny projekty a jejich produkty, které vznikly na základě spolupráce akademické a podnikové sféry, případně na ně bylo poskytnuto financování v rámci vládních výzev.

### 3.1.1 GAARDIAN a SENTINEL

Projekt GAARDIAN (GNSS Availability, Accuracy, Reliability and Integrity Assessment for Timing and Navigation), britskou vládou financovaný projekt, byl realizován ve spolupráci University of Bath a společností Chronous Technology Ltd. za účelem vyvinutí systému pro účinnou detekci RFI způsobující odchylky PNT (detekce pro signál GPS/eLoran) u aplikací kritické infrastruktury. Projekt je koncipován tak, že vytváří síť senzorů pro detekci a zabránění negativního vlivu RFI rozmístěných v sensitivní oblasti kritické infrastruktury a aplikacích využívajících GNSS signál pro funkce PNT. Senzory monitorují integritu, kontinuitu, spolehlivost a přesnost lokálně přijímaného GNSS signálu, měří prvky navigační zprávy, poměr výkonu nosné vlny k šumu ($C/N_o$), posun frekvencí na základě Dopplerova jevu, fázi nosné vlny, pseudovzdálenosti a celkové množství elektronů v Ionosféře prostřednictvím sítě detekčních alarmů přirozeného i úmyslného rušení.

Navazující projekt SENTINEL (GNSS Services Needing Trust In Navigation, Electronics, Location & timing) rozšiřuje stávající GAARDIAN o schopnost detekce a lokalizování směru příchodu úmyslného/neúmyslného rušení. Technická data ohledně prototypu nebyla prostřednictvím volně dostupných zdrojů dostupná. [33, 32]

### 3.1.2 Detector[10]

Projekt Detector (Detection, Evaluation and Characteriyation of Threats to Road Applications) představuje řešení pro detekci výpadků v automobilových nebo železničních systémech, využívajících pro určení své polohy družicových systémů, způsobených zařízením pro Jamming. Výsledkem projektu je funkční prototyp pro detekci Jamming dostupný při nízkých nákladech a nasazený v aplikacích pozemních komunikačních sítí (dálniční a železniční sítě). Klíčovým prvkem je přesná detekce běžně dostupných rušiček PPD a evaluace jejich dopadu na sítě kritické pozemní infrastruktury využívající GNSS v rámci EU. Momentálně je prototyp Detectoru nasazen ve Velké Británii, Francii a na Slovensku. [34]

### 3.1.3 GMCA

Galileo Monitoring for Critical Applications, je projekt financovaný programem Horizon2020, který rozšiřuje stávající monitorovací systém pro GPS (GPCA) o senzory pro detekci Jamming a Spoofing signálů Galileo. Prototyp vycházející z tohoto projektu je oproti předchozímu GPCA schopný monitorovat a nahrávat GNSS signál a zároveň slouží k detekci Jamming a Spoofing v oblasti letecké dopravy (ANSP, CAA a provozovatelé letišť). [35]

### 3.1.4 TIGER

Projekt TIGER (Trusted GNSS Receiver) je dalším projektem podpořeným European GNSS Agency (GSA) v rámci výzvy programu RP7. Výsledkem je funkční prototyp nepřenosného GNSS přijímače, který zajišťuje integritu PVT (Position, Velocity, Time) a je schopný detekovat jak Spoofingové, tak i Jamming útoky a vydat potvrzení o stavu přijímaného signálu. V prvé řadě je toto řešení vyvinuto pro detekci a zajištění odolnosti proti útokům na systémy využívající časové synchronizace podle GNSS. Technologie využité v projektu TIGER, včetně způsobů detekce rušení, jsou detailně popsány v článku z roku 2011, Tamper Resistance[11] od autorů O. Pozzobon, Ch. Wullems a M. Detratti, kteří se na projektu podíleli. Autoři současně hodnotí zranitelnost bezpečnostních funkcí (šíření kódového

[10] Nezaměňovat projekt Detector za český projekt Detektor s „k“
[11] Odkaz na článek Tamper Resistance: http://gpsworld.com/transportationtamper-resistance-11403/

šifrování/ověřování na úrovni navigačních dat) a posuzují návrhy možných řešení pro předcházení útokům Spoofing. [36]

### 3.1.5 FENIX

Produkt FENIX (Front-End GNSS Interference eXcisor) je vyvinutý ve spolupráci se španělskou Universitat Politècnica de Catalunia. Jedná se o technologii pro detekci rušení typu Jamming kombinující statistickou detekci RFI a multi-rezoluční algoritmy časového kmitočtu v GNSS přijímačích. Více informací o této problematice a produktu FENIX je rozebráno v článku od autorů Jorge Querol a Adriano Camps Real-time Pre-correlation Anti-jamming System for Civilian GNSS Receivers[12]. FENIX cílí na GNSS aplikace, které vyžadují zajištění vysoké míry spolehlivosti a integrity přijímaného signálu pomocí eliminace a filtrování rušivého signálu z autentického signálu ve snaze tak zvýšit jeho výkon. Zařízení je umístěno mezi GNSS anténu a přijímač a je tedy využitelné pro různé aplikace. Využití je možné v aplikacích letecké, námořní, silniční a železniční dopravy. FENIX dokáže přijímat a zpracovat i signály na nových konstelacích Galileo, Beidou a s novou verzí Glonass. [40, 41]

## 3.2 Komerční řešení zabývající se problematikou

Komerčními řešeními jsou míněny produkty, které vznikly v podnicích, nebo jako akademický výzkum s následným zajištěním komercializace a přepracování do komerčního produktu.

### 3.2.1 Produkty CTL3510 a CTL3520 + CTL8200 od Chronous Technology

Společnost Chronous Technology nabízí dva produkty pro detekci Jamming CTL3510 a CTL3520. První produkt CTL3510 je cenově dostupné řešení. Zařízení je schopno detekovat RFI v pásmu civilního signálu GNSS L1/E5a, E5b a zároveň umožnuje záznam událostí v případě opakovaného rušení. Druhé zařízení CTL3520 je schopno detekovat Jamming v pásmu L1/E5a, E5b a současně určit směr příchodu RFI (azimut) u nejsilnějšího zdroje vysílání. Oba tyto produkty jsou sensitivní do – 100 dBm v pásmu 20 MHz v blízkosti pásma GNSS signálu L1/E5a, E5b (1575,42 MHz). Primárně byly vyvinuty pro účely operátorů vozových parků, pro celní správu a pro operátor CI v UK. [37, 38]

[12] Odkaz na článek Real-time Pre-correlation Anti-jamming System for Civilian GNSS Receivers: https://www.ion.org/publications/abstract.cfm?articleID=15304

Třetím produktem Chronous Technology je CTL8200, který byl vyvinut pro monitorování rozsáhlých ploch pomocí sítě senzorů. Senzory nepřetržitě monitorují integritu, kontinuitu, přesnost a spolehlivost signálu GPS a eLoran v konkrétním místě. Využití produktu je v letecké dopravě. [39]

Datasheety k produktům jsou volně dostupné na stránce společnosti Chronous Technology, popisují základní vlastnosti produktu, možnosti použití, technické specifikace a další operativní data.

### 3.2.2 Produkt GNOME od společnosti IDS

Produkt GNOME (GNSS Operative Monitoring Equipment) od italské společnosti IDS je zařízení skládající se z komplexní sítě vzdálených detekčních a lokalizačních prvků Jamming a Spoofing pro monitorování integrity, kontinuity, přesnosti a spolehlivosti GNSS signálu, zejména v blízkosti letišť. Zařízení funguje na bázi softwarově definovaného radia (SDR) se zahrnutím možnosti RAIM pro generování návrhů GNSS NOTAM a tvorby brífinků pro piloty. Sleduje celý proces zpracování GNSS signálu od fyzické vrstvy (fyzické zpracování/zkoumání signálu) až po navigační doménu (zkoumání správného určení polohy) v reálném čase. Obsažena je i funkce nahrávání v souladu s ICAO Anex 10. [42]

### 3.2.3 Produkt GISMO společnosti NSL

GISMO (GNSS Integrity and Signal Monitoring Observatory) je softwarová služba pro komplexní monitorování a analýzu signálu GNSS využívaného v aplikacích v letectví. Systém je schopný monitorovat značnou část charakteristik přijímaného GNSS signálu včetně funkce nahrávání, ovšem nelze s určitostí říci, že je schopný detekovat jakoukoli formu RFI, jelikož na webové stránce společnosti dosud nebyly tyto informace zveřejněny. [43]

### 3.2.4 Produkt BroadShield společnosti Spectaracom

Systém BroadShield vyvinutý týmem Talen-X, je plně integrovaným prvkem produktu SecureSync (Time and Frequency Synchronization Platform) od společnosti Spectracom pro GNSS synchronizaci času a frekvence. BroadShield se skládá z balíku 75 softwarových algoritmů pro detekci Jamming a Spoofing včetně neúmyslného rušení GNSS signálu v reálném čase fungujících v pásmu GPS L1/L2 a Galileo L1/E5a, E5b. V případě detekce dysfunkcí je automaticky přerušena synchronizace systémů využívajících GNSS a systém

využívá pro synchronizaci jiné dostupné vstupní reference nebo přesný integrovaný oscilátor. BroadShield je dostupný pouze jako součást platformy SecureSync. [44]

*Tabulka 2: Charakteristiky aktuálně dostupných detekčních řešení Jamming a Spoofing, zdroj: vlastní*

| | Jamming | Spoofing | Azimut | Galileo frekvence | Nahrávání | Oblasti CI |
|---|---|---|---|---|---|---|
| **GAARDIAN & SENTINEL** | ✓ | - | částečně | - | - | Doprava – letecký a pozemní segment Energetika |
| **DETECTOR** | ✓ | - | - | ✓ | - | Doprava – pozemní segment (silnice a železnice) |
| **GMCA** | ✓ | ✓ | - | ✓ | ✓ | Doprava – letecký segment |
| **TIGER** | ✓ | ✓ | - | ✓ | - | |
| **Chronous Technology** | ✓ | - | CTL3520 | - | - | Doprava – letecký (CTL8200) a pozemní segment |
| **Fenix** | ✓ | - | - | ✓ | - | Doprava – letecký, pozemní a námořní segment (železnice, lodní doprava, silnice) |
| **GNOME** | ✓ | ✓ | ✓ | ✓ | ✓ | Doprava – letecký segment |
| **GISMO** | - | - | - | - | ✓ | Doprava – letecký segment |
| **BroadShield** | ✓ | ✓ | - | - | - | |

Z analýzy výše uvedených řešení vyplývá, že dosud není na trhu komplexní řešení, které by kombinovalo veškeré uvedené charakteristiky (detekce Jamming, detekce Spoofing, určení azimutu, určení přesné lokace rušení, řešení pro frekvence Galileo, nahrávání dat). Taktéž není dosud dostupné řešení, které by bylo implementovatelné pro různé subjekty infrastruktury zároveň. Veškerá výše uvedená řešení kombinují pouze dílčí segmenty CI. Projekt GAARDIAN a rozšiřující SENTINEL integrují dopravní segment a energetický segment, ovšem nedisponují funkcí detekce Spoofing a možností nahrávání. Jediným produktem kombinujícím všechny požadované charakteristiky je produkt GNOME od italské společnosti IDS, který je ovšem omezen pouze pro segment letecké dopravy, tudíž ho nelze modulovat pro jiné segmenty CI.

# 4 Systém pro odhalování nezákonného rušení GNSS signálu v blízkosti strategické infrastruktury – charakteristika českého projektu Detektor[13]

Projekt Detektor, celým názvem Systém pro odhalování nezákonného rušení GNSS signálu v blízkosti strategické infrastruktury. Vznikl na základě analýzy zranitelnosti kritické infrastruktury využívající funkcí GNSS a dostupných produktů vhodných k předcházení hrozbám Jamming a Spoofing v okolí (viz. kapitola 3).

Detektor na rozdíl od výše zmíněných produktů, kombinuje všechny funkce (detekce Jamming a Spoofing, kompatibilita na Galileo frekvencích, určení azimutu a přesné lokace zdroje rušení a možnost integrace pro různé subjekty kritické infrastruktury), které by byly dosaženy pouze implementací více produktů.

Struktura produktu sestává z 1 až 3 měřících stanovišť, která jsou připojena na centrální zpracovatelský server pomocí optické kabeláže. Vzdálenost jednotlivých měřících stanic od zpracovatelského serveru je definována současnými technickými parametry zvolených komponent – *cca 1,7 km* mezi měřícím stanovištěm a serverem. Tato hodnota není hraniční, jelikož s vývojem kvality a snížením pořizovací ceny dalších komponent pro ICT a při zachování dosavadních finančních nákladů lze dosáhnout i vyšší vzdálenosti.

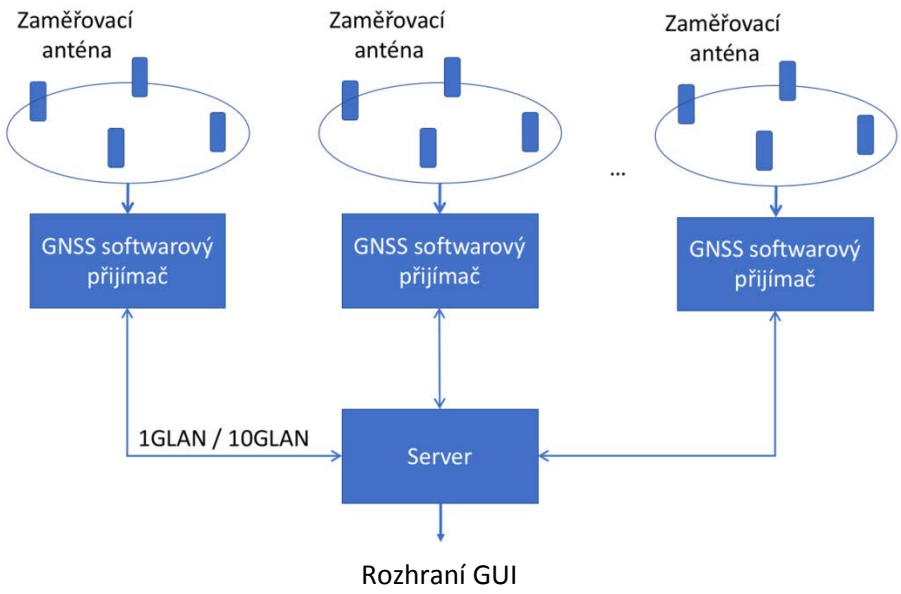



*Schéma 3: Blokové schéma systému – rozmístění anténních zářičů a propojení měřících stanovišť s centrálním serverem a přenesení do GUI, zdroj: Detektor ruseni – prezentace*

[13] Nezaměňovat český projekt Detektor s „K“ za britský projekt Detector, zmíněný v kapitole 3.1.2

Měřící stanoviště pracují na principu SDR a používají anténní blok skládající se ze 4 segmentů (čtyř samostatných anténních zářičů v provedení J-Pole „Jéčko“ tvořících tzv. antenna array). Výhodou anténního zářiče J-Pole je lepší vyzařovací charakteristika do prostoru, anténa se nemusí natáčet a vytváří prstenec rovnoběžný s povrchem země, což je z hlediska detekce rušiček GNSS signálu na Zemi relevantní. Plochá anténní pole (planární antény), i když jsou jednoduše dostupné jako Component of the Shelf (COTS) (tzn. je jednoduchá instalace a interoperabilita s existujícím systémem), mají všesměrovou vyzařovací charakteristiku ve tvaru polokoule od roviny antény, která není vhodná pro detekci rušení ze země a nelze vyzařovací charakteristiku přizpůsobit jako v případě J-Pole zářiče.

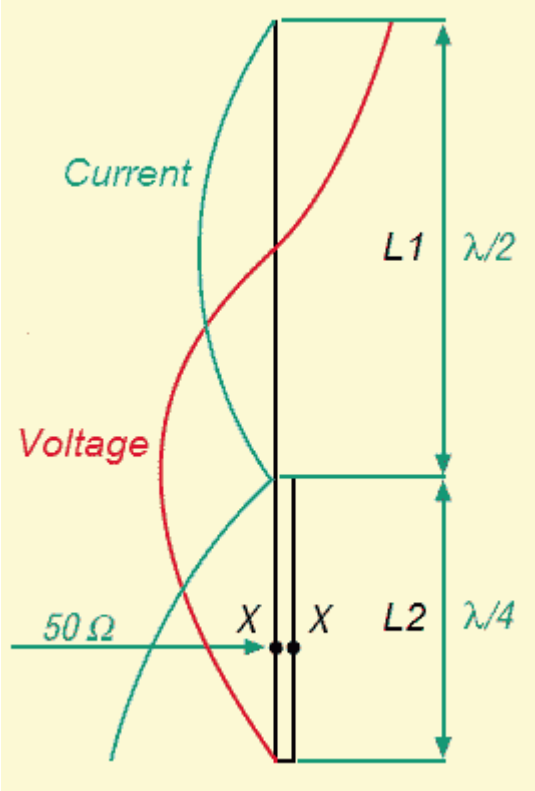



*Schéma 4: Schéma antény J-Pole s kruhovou vyzařovací charakteristikou v rovině rovnoběžné s povrchem Země, zdroj: interní dokumenty k projektu*

Citlivost detekce měřící antény na úrovni šumu, je stanovena dle ICAO limitu –120 dBm, úroveň síly GNSS signálu přijímaná uživatelem při příchodu na Zem je -158,5 dBW (-128,5 dBm) pro C/A kód na L1, a -160 dBW (-130 dBm) pro P(Y) kód na L2 dle Galileo/EGNOS Service Definition Document (SDD). Při odfiltrování šumu a rušivého signálu je pak přijímač schopný zvýšit intenzitu autentického signálu. Detektor detekuje přítomnost rušivého signálu i pod úrovní -120 dBm, což znamená že je schopný detekovat rušení i pod úrovní šumu u signálu s velmi nízkým výkonem, citlivost přijímače ale zatím není stanovena.

Rozlišovací schopnost v měření azimutu je +- 5°, což ve zjednodušeném případě udává šířku detekčního louče 10°. To znamená celkem 36 detekčních poloh v kružnici, umožňující triangulační zaměření zdroje rušivého signálu – míra přesnosti určení se samozřejmě s rostoucí vzdáleností snižuje.

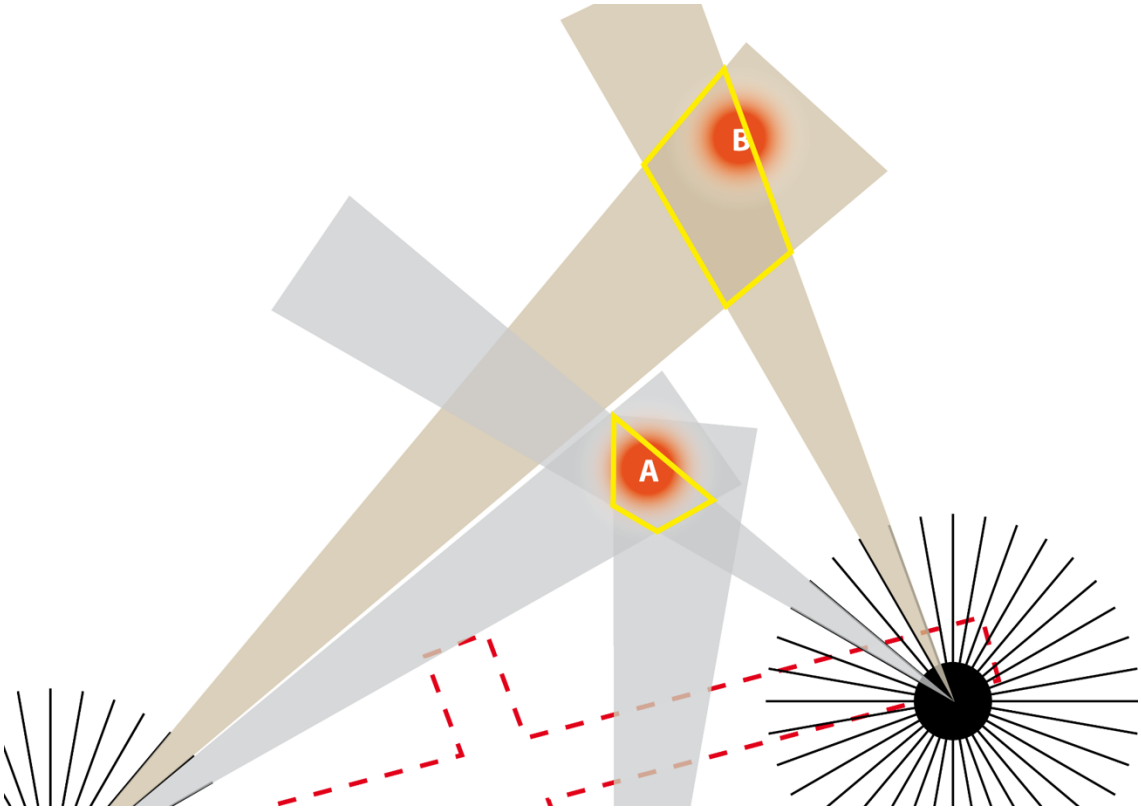
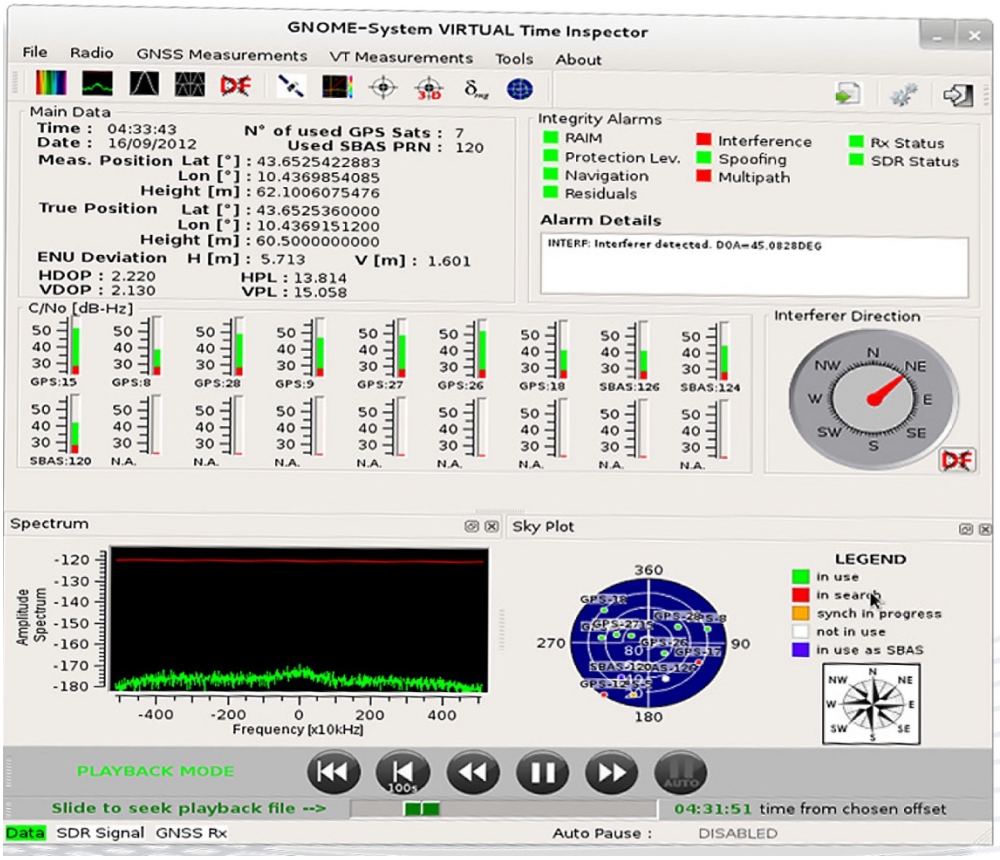



*Schéma 5: Schéma detekce zdroje rušení pomocí triangulační metody zaměření, zdroj: interní podkladky projektu*

Principem systému je kontinuální sběr signálu ze všech tří měřících stanovišť, který je po optické datové síti posílán do zpracovatelského serveru. To znamená, že ve zpracovatelském serveru pracujeme se signály ze 4 x n stanovišť (n=počet stanovišť 1 až 3), což umožňuje matematické a fyzikální výpočty mezi signály z jednotlivých antén. Tento princip se dosud neobjevil u žádného z konkurenčních řešení (ostatní srovnávaná řešení zpracovávají pouze jeden signál, který jde z anténního celku čtyř antén, čímž ztrácíme možnost porovnání signálů mezi sebou).




*Obrázek 7: GUI produktu GNOME, zdroj: interní podklady projektu*

Obrázek výše znázorňuje grafické rozhraní (GUI) produktu GNOME (viz. kapitola 3.2.2). Grafické rozhraní Detektoru zvažuje podobnou grafickou úpravu, včetně zobrazení obdobných parametrů. V levém horním rohu je kromě aktuálního času a data zobrazena přesná pozice fixního přijímače vypočtená pomocí GNSS signálu. ENU Deviation zobrazuje odchylku v souřadnicovém systému East-North-Up. Horizontal/Vertical Dilution of Precision (HDOP/VDOP) jsou parametry nepřesnosti v horizontální a vertikální rovině. Horizontal Protection Level (HPL) poskytuje vazbu na horizontální chybu polohy s pravděpodobností odvozenou z požadavku integrity. Podobně vertikální úroveň ochrany (VPL) poskytuje vazbu ve svislé poloze. V pravém horním rohu je zobrazen blok s kontrolkami pro dílčí typy alarmů a detail spuštěného alarmu. Vidíme, že je detekovaná RFI a její Direction of Arrival 45°, což je vidět na vykreslené růžici (Interference Direction), která zobrazuje radiál k rušiči. Ke všem družicím, které jsou v dosahu je v prostředním bloku zobrazen parametr $C/N_0$ včetně jejich PRN uvedeným pod grafem. Rozmístění družic na sféře vidíme na detailu Sky Plot. Blok v levém dolním rohu Spectrum (Power Spectral Density) znázorňuje naměřené intenzity signálu a jeho rozmístění ve spektru. 0 na horizontální ose je nosná frekvence. Vidíme, že filtr na RF Frontend je nastavený na +-5 MHz, což znamená, že pokud je frekvence detektoru nastavená na pásmo L1/E5a, E5b (1575,42 MHz), detektor vnímá frekvenční

spektrum 1570,42 – 1580,42 MHz, ostatní frekvence přesahující toto spektrum není schopný detekovat.

Grafické rozhraní lze upravit dle požadavků pro jednotlivé uživatele segmentů CI. Přesné potřeby jsou následně doladěny na základě konzultací s jednotlivými uživateli a nastaveny na základní rozložení GUI.

## 4.1 Testování Řízením letového provozu ČR, ČVUT a Českým telekomunikačním úřadem

ŘLP s aktivní účastí Českého telekomunikačního úřadu (ČTÚ) a ČVUT provedli testování vlivu rušení RFI prostřednictvím vybraných typů rušiček na sledované systémy v areálu IATCC Jeneč. Pro testování byl využit policejní vrtulník EC-135 s palubním zařízením Garmin Area 795 a Freeflight (Trimble) 2101 Approach Plus. Celkem byly provedeny dva typy testů:

1) Závislost rušení GNSS signálu na šikmé vzdálenosti 2 typů rušiček při maximálním konstantním výkonu a
2) Závislost rušení GNSS signálu na šikmé vzdálenosti výkonné rušičky při různých konstantních výkonech (TG-5CA).

V průběhu testování byl analyzován vliv rušení na sledované systémy s rušičkami rozmístěnými na různých místech areálu IATCC Jeneč.

Pro testování byl použit typ rušičky TG-5CA (Tangreat) s uváděným dosahem až 40 m a možností regulace výkonu na jednotlivých kanálech, které lze jednotlivě zapínat a vypínat. Takovou regulací lze u tohoto typu rušičky dosáhnout maximálního výkonu momentálně používaného kanálu, který mnohonásobně převyšuje výkon jiných rušiček. Maximální dosah rušičky dle testování byl stanoven na 550 m.

Dalším testovaným zařízením byla rušička PPD s uváděným dosahem 8 m, napájená ze 12 V zásuvky cigaretového zapalovače v automobilu. Uváděný výkon rušičky je 200 mW. U této jednoduché rušičky byl na základě měření stanoven dosah 227 m. Testováním dostupných rušiček se ve své disertační práci blíže zabývá Tomáš Duša v kapitole 4 „Evaluation and Testing“. [4]

*Tabulka 3: Rušičky testované v rámci testování ČTÚ, ČVUT a ŘLP, zdroj: vlastní*

| | Frekvence | Dosah | Cena | Popis | Obrázek |
|---|---|---|---|---|---|
| **TG-5CA** | GPS L1/L2 | 10-40 m | 120 USD | Rušička s výkonem až 12 W, napájení AC 220 V. Možnost úpravy výkonu, každé pásmo lze ovládat samostatně, možná konfigurace na 5 různých frekvencí |  |
| **PPD** | GPS L1/L2, | 8 m | 1390 Kč | Rušička pro připojení do 12 V zásuvky cigaretového zapalovače v automobilu, ruší veškerá GPS sledovací zařízení v automobilu. |  |

Z testování vyplynulo, že minimální vzdálenost GNSS přijímače od rušičky TG-5CA s efektivně vyzářeným výkonem EIRP 5 W je 200 m. Pod 200 m už dochází k chybám, které nelze ovlivnit a nelze zvýšit výkon autentického signálu (z testování vyplývá, že ve vzdálenosti rušičky 200 – 550 m od přijímače lze ještě autentický signál ovlivnit a zvýšit jeho výkon nad úroveň výkonu rušivého signálu). Ovšem pro zjištění konkrétní minimální bezpečné vzdálenosti je vhodné provést test rušení na konkrétním zařízení a následně případné úpravy vyzařovacích charakteristik GNSS antény.

# 5 Relevantní odvětví kritické infrastruktury dle dopadu úmyslného rušení GNSS signálu

Pro uplatnění výše uvedené metodiky detekce a eliminace byly vybrány dvě odvětví kritické infrastruktury v ČR a jejich konkrétní subjekty, pro které je hrozba nezákonného rušení GNSS signálu relevantní a v případě, že nebude tato hrozba brána v úvahu nelze zajistit bezpečnost a odolnost těchto subjektů jako součásti kritické infrastruktury.

V návaznosti na testování dostupných rušiček z kapitoly 4.1, jsou pro účely následujících kapitol používány pojmy „PPD“ – jednoduché rušičky s dosahem cca 227 m a sofistikované rušičky – s možností regulace výkonu a s dosahem cca 550 m.

## 5.1 Energetika

### 5.1.1 Přenosová/Distribuční soustava

Relevantním subjektem pro oblast energetiky byla vybrána akciová společnost ČEPS. Společnost působí na českém trhu jako výhradní provozovatel energetické přenosové soustavy Pod její správu spadá provoz celkem 42 rozvoden s 75 transformátory (některé slouží pro převod elektrické energie z přenosové do distribuční soustavy) a dále provozuje trasy vedení s napěťovou hladinou 400 kV a 220 kV s celkovou délkou 5633 km na území ČR. ČEPS mimo jiné poskytuje přenosové služby a služby pro zajištění rovnováhy mezi výrobou a spotřebou elektrické energie v reálném čase.

Provozovateli distribuční soustavy v ČR jsou společnosti ČEZ Distribuce a.s., PRE Distribuce a.s. a E.ON Distribuce a.s., Problém nezákonného rušení je relevantní i pro tyto společnosti. Pro účely této práce byl ovšem jako výhradní subjekt vybrána společnost ČEPS.

#### 5.1.1.1 Vymezení problému

Konkrétní využívané služby GNSS: Timing

Společnost ČEPS využívá GNSS signál pro časovou synchronizaci rozvoden přenosové soustavy a při fázorových měřeních stavu přenosové soustavy. Integrita a dostupnost GNSS signálu je proto klíčovým prvkem pro zajištění synchronního přenosu mezi jednotlivými rozvodnami, z nichž některé slouží i pro transformaci elektrické energie do distribuční sítě.

Fázorové měřící jednotky (PMU) přijímají signál GNSS, který je využíván jako zdroj časové synchronizace pro monitorování sítě. PMU poskytují automatickou havarijní ochranu monitorovacích systémů WAMS, Wide Area Control Systém (WACS) nebo jejich kombinace. Rozdíly ve fázových úhlech sítě indikují aktuální stav sítě, změny rozdílů v čase indikují potenciální chyby v síti, které mohou vést až k jejímu rozdělení na tzv. ostrovy nebo dokonce ke kompletnímu zhroucení sítě, tzv. black-outu. Ke krajnímu případu v podobě black-outu došlo například v roce 2003 v oblasti států Ohio a Michigan v USA. V ČR dosud takový kolaps elektrizační soustavy nenastal, ovšem k podobnému kolapsu jako v USA se přiblížil přelom roku 2011/2012 a srpen 2012, jak je uvedeno na webové stránce společnosti ČEPS v sekci často kladené otázky. Další země, kde k black-outu z důvod desynchronizace elektrizační soustavy již došlo, je Itálie, Brazílie a Indie. Na webové stránce společnosti ČEPS[14] jsou zodpovězeny otázky týkající se přenosové soustavy ČR včetně problematiky týkající se možné krizové situace v podobě black-outu.

V současnosti ČEPS využívá systém WAMS pro 39 distribučních bodů v ČR. WAMS má pouze funkci monitorování soustavy a částečné eliminace rušení RFI, ovšem o výskytu rušení není schopen podávat žádné informace do řídícího centra. Z toho plyne, že systém WAMS nelze použít jako systém zásadně důležitý pro zachování provozní bezpečnosti. V případě výskytu rušení GNSS signálu je systém schopný uchovat svou časovou synchronizaci po dobu jedné hodiny s maximální odchylkou +/- 5 μs. [4]

Rušení GNSS signálu v podobě Jamming a Spoofing musí být současně řešeno tak, aby rozvodný systém splňoval požadavky zásadně důležité pro bezpečnost z hlediska využívání GNSS jako hlavního zdroje synchronizace.

Z hlediska rušení typu Jamming je energetická distribuční síť vystavena především rušení s dlouhodobým vlivem na infrastrukturu, tedy rušení pomocí sofistikovanějších rušiček typu použitého při testování ČTÚ, ŘLP a ČVUT, které mají vyšší výkon s výdrží baterie v řádech dní. Krátkodobé rušení pomocí PPD v tomto případě není zcela relevantní, neboť jeho přítomnost po dobu průjezdu vozidla využívajícího toto zařízení je v řádu maximálně několika minut, což není dostačující pro ovlivnění časové synchronizace distribuční sítě.

Hrozba v podobě Spoofing, vysílání falešného signálu, je v oblasti energetiky aktuální. Tento typ rušení je schopný způsobit časový posun signálu při časové synchronizaci PMU při fázorových měřeních. I když jsou jednotky PMU rozmístěny po celé síti a díky centrálnímu monitorování dochází k pravidelné verifikaci, testy provedené Northrop Grumman

[14] Odkaz na webovou stránku ČEPS: http://www.ceps.cz/cs/casto-kladene-otazky

Information Systems (NGIS) a University of Texas (UT) prokázaly, že útok v podobě Spoofing po dobu 11 minut, může zvýšit maximální povolenou časovou chybu (max. 1μs odpovídající při síťovém kmitočtu 50 Hz chybě úhlu fázoru 0,018°) dle standardu IEEE C37.118. Podrobně se tímto zabývá článek od autorů D. P. Sheparda, T. E. Humphreys, and A. A. Fanslera Going Up Against Time: The Power Grid's Vulnerability to GPS Spoofing Attacks[15], kde autoři provedli testování spoofingových útoků na jednotky PMU a demonstrovali tak hrozbu pro integritu synchrofázorových měření.

Dalším zajímavým zdrojem informací k problematice odolnosti PMU proti rušení Spoofing je článek Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks[16] od autorů zmiňovaných výše. Autoři v článku navazujícím na výše zmíněný prezentují výsledky testů Spoofing na PMU, které dokázaly jejich zranitelnost. Upozorňují i na to, že útok trvající jen několik minut může způsobit vyšší fázovou chybu, než je maximální povolená standardem.

V aktuálním článku z roku 2017 Multi-Receiver GPS-Based Direct Time Estimation for PMU´s[17] v časopise InsideGNSS popisují autorky S. Bhamipidati, Y. Ng a G. Xingxin Gao z University of Illinois, algoritmus využívající vícenásobné použití přijímačů GPS signálu (multi-receiver direct time estimation - MRDTE) s cílem maximální eliminace rušících vlivů na jednotky PMU způsobených rušením typu Jamming a Meaconing. Obdobný postup též popisuje článek A Multi-Layered, Multi-Receiver Architecture, Reliable GPS – Based Timing for Power Systems[18] autorů L. Heng, D. Chou and G. Xingxing Gao ze stejné univerzity, uveřejněný v roce 2014 v časopise InsideGNSS.

Analytické funkce systému pro synchronní měření fázorů napětí a proudu pomocí jednotek PMU z rozsáhlého území propojených přenosových soustav v prostředí společnosti ČEPS rozebírají autoři v článku WAMS systémy pro monitoring elektrizační soustavy[19]. Článek popisuje architekturu WAMS, jednotlivé součásti a jejich funkce, zabývá se také implementací projektu WAMS do přenosové soustavy v ČR, která probíhá od roku 2013.

[15] Odkaz na článek Going Up Against Time: The Power Grid's Vulnerability to GPS Spoofing Attacks: http://gpsworld.com/wirelessinfrastructuregoing-against-time-13278/
[16] Odkaz na článek Eva luation of the vulnerability of phasor measurement units to GPS Spoofing attacks: https://www.sciencedirect.com/science/article/pii/S1874548212000480
[17] Odkaz na článek Multi-Receiver GPS-Based Direct Time Estimation for PMU´s: http://insidegnss.com/multi-receiver-gps-based-direct-time-estimation/
[18] Odkaz na článek A Multi-Layered, Multi-Receiver Architecture, Reliable GPS – Based Timing for Power Systems: http://insidegnss.com/reliable-gps-based-timing-for-power-systems/
[19] Odkaz na článek WAMS systémy pro monitoring elektrizační soustavy: http://www.allforpower.cz/UserFiles/files/2011/wams_alstom.pdf

ČEPS na svých stránkách uvádí následující „*Elektřina je pro dnešní běžný život nepostradatelná. Pokud by došlo k masívnímu a dlouhodobému výpadku elektřiny, může dojít k omezení nebo úplnému zastavení dodávek vody, plynu, ropy, ale i zásobování a základní zdravotní péče.“.* [45]

## 5.2 Doprava

Dalším relevantním odvětvím pro účely této práce je *Doprava*, kam dle Nařízení vlády č. 432/2010 Sb. patří konkrétně silniční doprava, letecká doprava a řízení letového provozu. V teoretické části této práce byly již konkrétně zmíněny aktuální hrozby a možné dopady pro tyto tři prvky CI.

### 5.2.1 Silniční doprava – Ředitelství silnic a dálnic ČR

V rámci silniční dopravy bylo jako relevantní subjekt vybráno Ředitelství silnic a dálnic ČR (ŘSD), které je státní příspěvkovou organizací spadající pod Ministerstvo vnitra ČR. Základní činností vykonávanou ŘSD je výkon vlastnických práv státu k nemovitostem tvořícím dálnice a silnice I. třídy, zabezpečení správy, údržby a oprav dálnic a silnic I. třídy a zabezpečení výstavby a modernizace dálnic a silnic I. třídy. ŘSD dále zajišťuje provoz mýta a výběr mýtných poplatků.

V průběhu dubna 2018 byl vyhlášen vítěz tendru na provoz mýtného systému v ČR, kterým se stala společnost CzechToll. Ta je partnerskou společností slovenské SkyToll. Společnost SkyToll na Slovensku od roku 2012 provozuje elektronický družicový mýtný systém, který pokrývá v EU nejrozsáhlejší silniční síť (celkem 17 736 km úseků dálnic, rychlostních silnic, silnic I., II. A III. třídy). Od roku 2015 společnost SkyToll zavedla pro Slovensko systém elektronické dálniční známky pro vozidla do 3,5t.

#### 5.2.1.1 Vymezení problému

Konkrétní využívané služby GNSS: Position, Navigation

Pro zajištění spolehlivého výběru mýtných poplatků od uživatelů silniční sítě je třeba se zaměřit na kontinuitu a dostupnost systému, který výběr mýta v ČR prostřednictvím družicové technologie zajišťuje. Sledování a dodržování mýtné povinnosti bylo dosud u mikrovlnného mýtného systému prováděno přímo detekcí při průjezdu mýtnou branou nebo mobilními jednotkami při kontrole na zpoplatněných komunikacích.

Se zavedením družicového výběru mýtných poplatků vzniká problém s úmyslným rušením GNSS signálu, a jak detekovat mýtnou povinnost při průjezdu virtuální mýtnicí. V současné době se rozšiřuje využívání osobních rušiček PPD, které jsou dostupné velmi levně.

V tabulce níže jsou uvedeny příklady dostupných rušiček pro osobní potřebu. Prodejci na svých stánkách často uvádějí, že použití těchto zařízení může být v zemích EU protizákonné. Dosah je uváděn průměrně v okruhu 10 m od vozidla, což je plně dostačující pro vyrušení příjmu GNSS signálu v dosahu mýtné brány. Na základě testování základních typů rušiček PPD (kapitola 4.1) bylo určeno, že tyto typy rušiček s uvedeným dosahem cca 10 m v manuálu mají dosah až 227 m (dle měření v disertační práci Tomáše Duši *Zvýšení bezpečnosti kritických GNSS aplikací využitím nástrojů fuze dat* [4]).

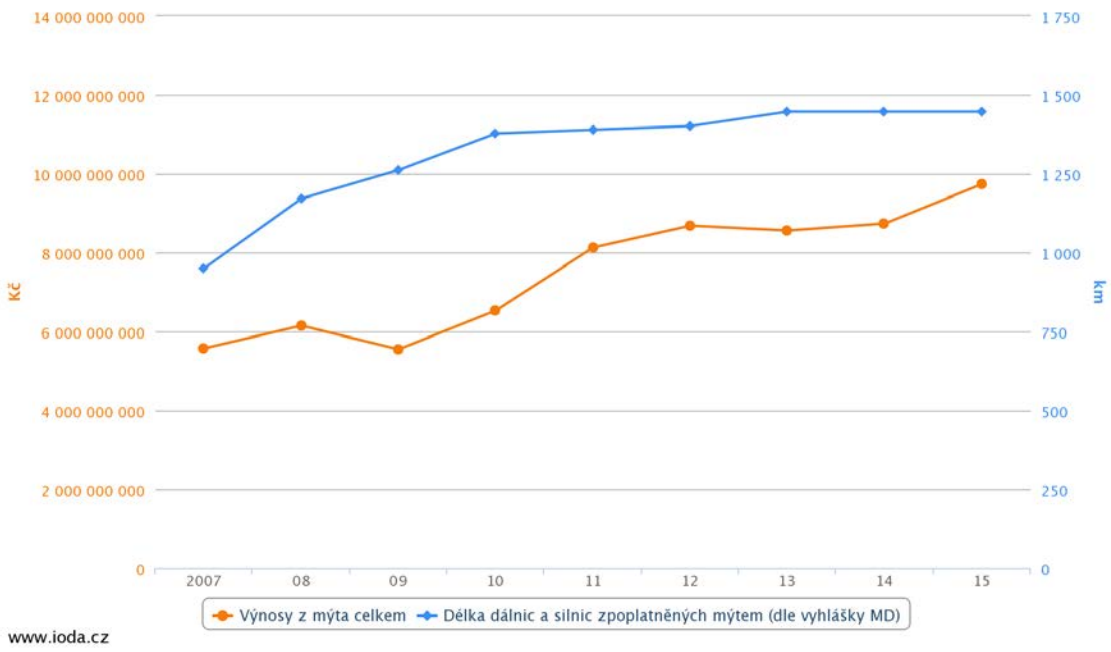
*Tabulka 4: Porovnání dostupných PPD v závislosti na uváděném dosahu a ceně, zdroj: vlastní*

| | Frekvence | Dosah | Cena | Popis | Obrázek |
|---|---|---|---|---|---|
| ***Mini rušička GPS signálu*** | 1575,42 MHz: GPS L1 | 10 m | 1 390 Kč | Rušička pro připojení do automobilového zapalování, ruší veškerá GPS sledovací zařízení v automobilu. Vhodné pro použití ve firemních automobilech. |  |
| ***Mini rušička GSM a GPS signálu*** | 1575,42 MHz: GPS L1<br>925–960 MHz: GSM 900<br>1805-1880 MHz: GSM 1800 | 10 m | 2 154 Kč | Díky současnému rušení GPS a GSM je schopná zamezit lokátoru ve sledování polohy pomocí GPS a současně vyřadí funkci nouzového sledování polohy dle nejbližšího BTS operátora pomocí sítě GSM. |  |
| ***GPS anti-lokátor*** | GPS L1/L2 | 15 m | 6 892 Kč | Ochrana před sledováním pomocí GPS lokalizačních jednotek – rušička zabrání přenosu dat z jednotky na server, a tím pádem je sledování v reálném čase nemožné. |  |

Sofistikovanějším problémem je využívání metody Spoofing, která v reálném čase simuluje GNSS signál (převezme kontrolu nad původním autentickým signálem) s falešnou polohou či falešným časem. Mobilní kontrolní jednotky, které jsou využívány úřadem ke kontrole dodržování mýtné povinnosti, nejsou dostatečně pro tento účel nezákonného rušení vybaveny. Jsou schopny detekovat pouze klasické RFI, tzn. když dojde k oslabení nebo ztrátě příjmu GNSS signálu přijímačem, simulovaný signál s falešnou polohou nejsou schopny rozeznat.

Rozvoj dopravní infrastruktury zvyšuje i množství zpoplatněných úseků komunikací. V roce 2017 dosahovala délka zpoplatněné sítě dálnic a rychlostních silnic 1231,9 km. Zpoplatnění podléhají také některé úseky silnic první třídy. Celková délka zpoplatněných úseků dosahovala dle dat z roku 2016 z ŘSD 1446,2 km.

V roce 2017 bylo dle údajů ŘSD, dostupných na http://www.vyrocenky.cz, vozidly podléhajícími mýtné povinnosti projeto celkem 2 661 348 909 km silničních komunikací s mýtnou povinností. Celková suma vybraného mýta činí za uvedený rok 10 406 381 590 Kč. Tato částka se meziročně neustále zvyšuje, jak je patrné i z grafu níže.




*Obrázek 8: Nárůst výnosů z mýtného meziročně od roku 2007 do 2015, zdroj:ioda.cz [53]*

Nejen v důsledku zvyšujících se výnosů z mýtných poplatků, ale zejména také z důvodu zavedení nové technologie výběru mýtného pomocí družicových technologií, je potřeba se

věnovat problému rušení GNSS signálu s následkem obcházení mýtné povinnosti souvisejícího snížení výnosů. [53, 54]

### 5.2.2 Letecká doprava – Řízení letového provozu ČR

Subjektem pro leteckou dopravu bylo vybráno Řízení letového provozu ČR, s.p. ŘLP se podílí na zajištění bezpečných, nákladově efektivních a dlouhodobě udržitelných letových služeb. Klíčovou aktivitou je poskytování a rozvoj letových provozních služeb ve vzdušném prostoru nad územím ČR. ŘLP dále zajišťuje rozvoj ATM infrastruktury a její maximální kompatibilitu s Functional Airspace Block Central Europe (FAB CE). Cílem je i zapojení do mezinárodních projektů pro zajištění evropské integrace. Díky členství v EU se ŘLP aktivně podílí na vytváření projektu SESAR a naplňování Evropské legislativy.

#### 5.2.2.1 Vymezení problému

Konkrétní využívané služby GNSS: Position, Navigation, Timing

ŘLP ve spolupráci s ČTÚ provedlo testování v okolí letiště, při kterém byla odhalena přítomnost rušení GNSS signálu u pozemních zařízení pro přiblížení na přistání. Mimo jiné byly testovány různé typy rušiček a jejich vliv na infrastrukturu ANSP (viz. kapitola 4.1).

*Časová synchronizace systémů ANSP*

Primární problém pro zachování služeb/provozu systému ANSP může vyvstat při využití sofistikovanějších typů rušiček s delším dosahem a vyšší výdrží baterie. Využití sofistikovanějších typů rušiček lze přiřadit k úmyslnému rušení s cílem ohrozit systémy kritické infrastruktury, a tak způsobit finanční ztráty, případně ohrozit životy lidí.

Systémy ANSP vyžadují pro svou synchronizaci funkci přesného určení času podle GNSS. Patří sem časová synchronizace serverů, které jsou klíčovým prvkem pro zajištění celkové časové synchronizace systémové sítě. Záložní radarové systémy využívající multilateraci nebo systémy datových převodů. I v případě výskytu kritických situací (nedostupnost signálu GNSS) jsou systémy ANSP bezpečné z důvodu využití oscilátorů, jak je uvedeno v kapitole 2.3.5.

I když systémy ANSP nevykazují přímou míru ohrožení v důsledku rušení GNSS signálu, v současné době zvyšujícího se výskytu teroristických útoků je potřeba chránit CI i za předpokladů, že hrozba není aktuální. Dále je potřeba se zaměřit i na ostatní letištní systémy, na které má rušení GNSS signálu vliv.

*Systémy pro přiblížení na přistání*

Při přiblížení na přistání jsou tradiční radionavigační prostředky a pozemní a inerční systémy nahrazovány systémy, které využívají GNSS. Na LKPR, vzhledem k těsné blízkosti přistávací/vzletové dráhy RWY 12/30 dráhy a frekventované komunikace dálnice D6 spojující Karlovarský kraj s Prahou a následně dálnice D7 spojující Ústecký kraj s Prahou v těsné blízkosti RWY 06/24, vyvstává problém s rušením GNSS signálu pomocí osobních rušiček PPD. Tyto rušičky mají mnohem vyšší dosah, než je uváděno v dokumentaci (porovnání rušiček viz tabulka č. 3 v kapitole 5.2.1, což bylo ověřeno v průběhu testování základních typů rušiček PPD. Výsledky dle měření v kapitole 4.1 stanovily dosah, který stačí pro ovlivnění pozemních systémů pro přiblížení na přistání s využitím GNSS. Pozemními systémy pro přiblížení na přistání je myšlen systém GBAS, viz. kapitola 2.3.4.


*Schéma 6: Dráhy LKPR a přilehlé komunikace D6 a D7, zdroj: vlastní*

Zkušenosti jsou i ze zahraniční. Příkladem je letiště EWR, viz. kapitola 1.3.2. Pro zlepšení přesnosti GNSS při přesném přiblížení na přistání jsou využívány korekční systémy ABAS, GBAS a SBAS. Palubní zařízení využívají korekční systémy (ABAS) sledující integritu a dostupnost GNSS signálu během letu, tudíž zde není téma rušení Jamming a Spoofing relevantní a není dále u těchto systémů diskutováno.

Stávající radionavigační, pozemní a inerční zařízení pro navádění letadel při přiblížení vyžadují pravidelnou údržbu a obnovu, s čímž se pojí pravidelné vysoké náklady. Je proto

logické jít s vývojem moderních technologií kupředu, což se týká využívání GNSS, a zajistit integritu a dostupnost všech systémů.

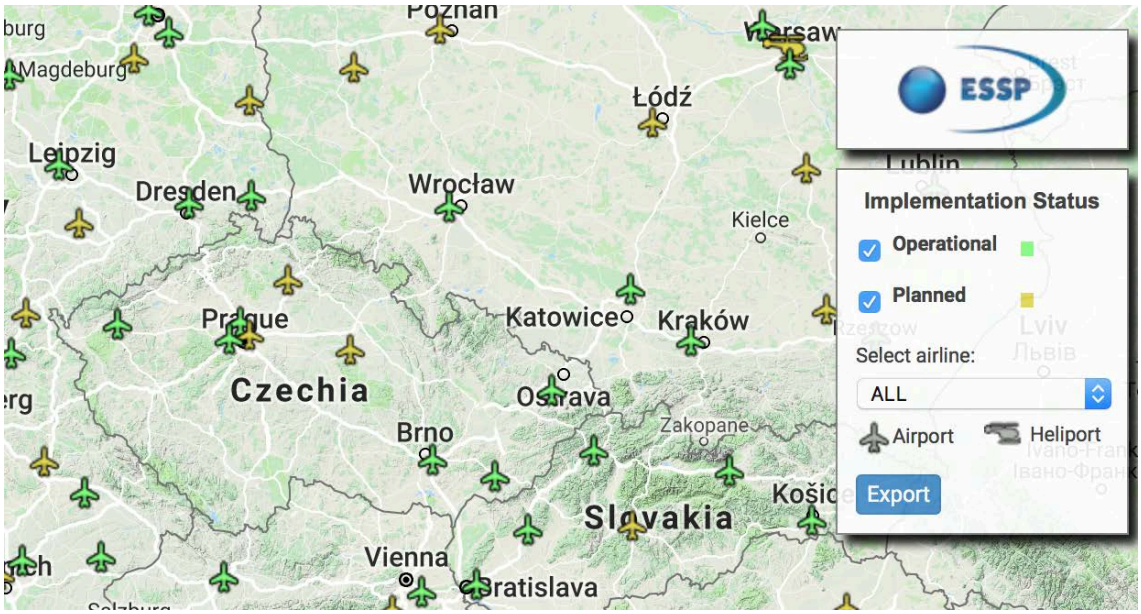
### 5.2.3 Letecká doprava – Provozovatelé lokálních letišť

V oblasti letectví jsou za relevantní subjekty považováni i provozovatelé lokálních letišť. S rozvojem GNSS technologií je trendem zavádění LPV (Localizer Performance with Vertical Guidance) přiblížení bez zálohy jiných radionavigačních systémů. LPV spočívá v přiblížení s výškovým vedením Approach with Vertical Guidance (APV) zabezpečovaného pomocí GNSS. Systém přiblížení LNAV/VNAV umožňuje vertikální vedení na základě barometrické výšky. Touto problematikou se zabývá již řada diplomových prací, například práce RNP přiblížení od Martina Mašáta (ČVUT) nebo práce Porovnání zavádění SBAS sestupů na neřízených letištích mezi USA a Evropou od Miloslava Krcha (ČVUT).

LPV letišti se pro účely této práce rozumí letiště s publikovanými postupy LPV, která využívají GNSS přiblížení se zálohou nebo bez zálohy jiných tradičních radionavigačních systémů. Předpisy jsou minima pro LPV přiblížení stanovena hodnotou Decision Height (DH) = 250 ft a více pro nezdařené přiblížení, následně lze pokračovat už jen dle vizuální reference a pilot se již nemůže spoléhat na palubní systém. S přiblížením LPV-200 je cílem snížit DH na 200 ft, což odpovídám minimům pro ILS Cat1.

Výhodou LPV přiblížení je možnost jeho publikace z obou směrů. Zatímco klasické radionavigační systémy fungují pouze z toho směru, kde jsou nainstalovány, odpadají tím náklady na vybudování infrastruktury a následnou údržbu zařízení VOR/DME a ILS. Letiště zavádějící pro přiblížení pouze LPV bez jiných záložních systémů jsou v Evropě momentálně trendem a jejich počet se neustále zvyšuje. Dle údajů z GSA k datu 30. 4. 2018 je v Evropské unii celkem 243 letišť s publikovaným LPV přiblížením, viz. mapa na webové stránce EGNOS User Support[20]. V ČR je momentálně celkem 6 letišť s publikovaným LPV přiblížením v AIP (LKKV, LKVO, LKTB, LKKU a LKMT). V procesu návrhu a implementace je LPV dále na třech letištích (LKKB, LKMH, LKPD a LKPR) a zájem o implementaci mají i letiště LKCS a LKPO. Na zavádění postupů v ČR se podílí asociace GNSS Centre of Excellence.

[20] Odkaz na web EGNOS User Support: https://egnos-user-support.essp-sas.eu/new_egnos_ops/resources-tools/lpv-procedures-map




*Obrázek 9: Publikace LPV v ČR (letiště s publikovaným LPV jsou vyznačena zeleně, plánovaná publikace LPV je označena žlutě), zdroj: EGNOS User Support [55]*

Výhody implementace LPV popisuje článek od společnosti Honeywell The Benefits of LPV Approach Operations for The Airline Operator[21], kde autoři vymezují přínosy zejména pro regionální a nízkonákladové společnosti, které často využívají menších letišť s méně rozvinutou pozemní infrastrukturou pro přesné přiblížení. LPV umožňuje stabilní a téměř přesné přiblížení s nejnižšími minimy vzhledem k jiným postupům nepřesného přiblížení v případech, kdy na letišti není k dispozici jiná možnost přesného přiblížení, například ILS. Autoři mimo jiné popisují i zvýšení bezpečnosti v souvislosti se zavedením LPV a zároveň snížení nákladů pro letecké společnosti z důvodu minimalizace nezdařeného přiblížení plynoucí ze snížení minim. [46]

#### 5.2.3.1 Vymezení problému

Konkrétní využívané služby GNSS: Position, Navigation

Stejně jako u systémů pro přiblížení na přistání využívaných na mezinárodních letištích jako je LKPR, je hrozba nezákonného rušení typu Jamming a Spoofing relevantní. Letiště využívající pro přiblížení pouze LPV, bez zavedení radionavigačních prostředků VOR/DME a ILS, jsou závislá na správné funkčnosti GNSS. V případě narušení GNSS signálu nelze provést přesné přiblížení ani jiný druh přiblížení podle GNSS (tzn. RNAV). Pilot tudíž musí provést vizuální přiblížení, pro které jsou stanovena vyšší minima (1500 ft základna

[21] Odkaz na článek Honeywell The Benefits of LPV Approach Operations for The Airline Operator: https://aerospace.honeywell.com/en/~/media/aerospace/files/white-paper/c61-1631-000-000-the-benefits-of-lpv-approach-operations-for-the-airline-operator-wp.pdf

oblačnosti nad letištěm a 5 km dohlednost), nebo v případě horších meteorologických podmínek musí divergovat let na jiné letiště.

Rušení u lokálních letišť je stejného původu jako u větších letišť. Buďto se jedná o rušení pomocí PPD, tzn. je vykazován pouze krátkodobý vliv rušení, nebo naopak se jedná o rušení pomocí sofistikovaných rušiček s výdrží baterie až několik dní. To může mít za následek vyřazení systému pro přiblížení podle GNSS z provozu a letiště je tak po určitou dobu degradováno na provoz VFR.

*Rušení pomocí PPD z přilehlých komunikací*

Při zaměření na letiště s plánovanou publikací LPV, je z mapy patrné, že letiště se nacházejí vždy v blízkosti frekventovaných komunikací. Práh dráhy u LKPD je vzdálený cca 750 m od silnice I/37, LKMH má práh dráhy vzdálený cca 750 m od silnice E65. Ze závěrů testování ČTÚ a ŘLP byla bezpečná vzdálenost GNSS přijímače od rušičky stanovena minimálně 200 m. Tato letiště by tedy neměla být ovlivněna PPD (v případě dosahu cca 227 m dle testování v disertační práci Tomáše Duši, *Zvýšení bezpečnosti kritických GNSS aplikací využitím nástrojů fuze dat.* [4]

V případě využití GNSS pro přiblížení na přistání na jiných letištích je vždy třeba brát v úvahu vzdálenost přilehlých komunikací a pohybujících se vozidel, která mohou být zdrojem rušení.

Hrozba plynoucí z využití sofistikovaných, výkonnějších rušiček je také v tomto případě reálná. Stejně jako u jiných subjektů kritické infrastruktury, mohou být tyto rušičky použity s úmyslem ochromit subjekt, v tomto případě zamezit možnosti využití GNSS signálu pro přesné přiblížení na přistání.

# 6 Návrh obecné metodiky pro podporu zavádění systému pro detekci nezákonného rušení GNSS signálu v prostředí kritické infrastruktury

Výše definované problémy u vybraných subjektů kritické infrastruktury v České republice umožňují zahájit testování systému na odhalování nezákonného rušení GNSS signálu v reálném prostředí konkrétního subjektu. Jedním z cílů této práce je příprava vhodných podkladů (informačních materiálů) k zahájení diskuze na téma nezákonného rušení, možností testování nového produktu a přizpůsobení produktu pro potřeby konkrétního subjektu. Důležitým krokem je stanovení obecné metodiky postupu pro podporu zavádění systému pro detekci nezákonného rušení GNSS signálu do praxe. Následující text bude sloužit jako návrh této obecné metodiky.

**Základní pravidla pro podporu zavádění Systému pro odhalování nezákonného rušení GNSS signálu v blízkosti strategické infrastruktury (dále jen „Detektor“)**

1) **Určení subjektu** kritické/nekritické infrastruktury. V prvním kroku je definován konkrétní subjekt, který využívá pro své kritické (ale i nekritické) aplikace GNSS signál. Definování, zda pro subjekt může být rušení GNSS signálu problémem.
2) **Konkrétně využívané funkce GNSS**, které subjekt pro své aplikace využívá (Positioning, Navigation, Timing) a u kterých by rušení mohlo být klíčovým problémem.
3) **Vymezení problému** konkrétního subjektu. Tento krok zahrnuje rešerši v oblasti systémů využívajících GNSS, specifikování možných ohrožení systémů z hlediska rušení (přítomnost pozemních komunikací v bezprostřední blízkosti subjektu, možné úmyslné napadaní s cílem indisponovat subjekt). Vlivy rušení u subjektu – krátkodobý/dlouhodobý vliv rušení na subjekt. Současně využívané zabezpečení proti nezákonnému rušení GNSS signálu.
4) **Zpracování materiálů pro první jednání**, přizpůsobené pro konkrétní subjekt a jeho problém vymezený v bodě 3). Obsah materiálů, s rozsahem jedné strany A4, by měl být následující:
    - Stručné představení projektu Systém pro odhalování nezákonného rušení GNSS signálu v blízkosti strategické infrastruktury, včetně zpracovatelů,
    - Současný stav problému – jeden odstavec shrnující informace z bodu 3), včetně možných následků v případě ignorování problému,

- Popis navrhovaného řešení – jeden odstavec, který stručně popisuje produkt Detektor (neobsahuje konkrétní technické specifikace),
- Uvedení důvodu pro navázání spolupráce se subjektem,
- Přínosy pro subjekt – v bodech vymezené krátkodobé/dlouhodobé přínosy pro subjekt, které plynou z implementace a mají být přesvědčující pro zahájení spolupráce
- Způsob zapojení subjektu – v bodech vymezené požadavky na subjekt pro zahájení dalších jednání.

5) **Zpracování materiálů pro druhé jednání**, přizpůsobené pro konkrétní subjekt, vycházející z materiálů připravených v bodě 4). Obsah materiálů je detailněji rozpracován a zahrnuje již faktické informace o produktu Detektor. Rozsah je cca dvě strany A4:
    - Stručné představení projektu Systém pro odhalování nezákonného rušení GNSS signálu v blízkosti strategické infrastruktury, včetně zpracovatelů,
    - Současný stav problému – jeden odstavec shrnující informace z bodu 3), včetně možných následků v případě ignorování problému,
    - Vlivy rušení typu Jamming a vlivy rušení typu Spoofing na systémy využívající GNSS v subjektu,
    - Parametry produktu Detektor a možný způsob implementace u subjektu – použité technologie, komunikace se serverem, metoda měření, vyhodnocování dat atd.,
    - Základní informace o testování přizpůsobeného prototypu v prostředí subjektu
    - Možnosti reportování událostí – možnosti nastavení podle konkrétních požadavků subjektu
    - Přínosy pro subjekt – v bodech vymezené přínosy, včetně přínosu testování a přizpůsobení produktu na základě výsledků testování
    - Způsob zapojení subjektu – požadavek na sestavení pracovní skupiny podílející se na vývoji a implementaci produktu.
6) **Zahájení společné diskuze** mezi členy pracovní skupiny ze strany subjektu, GNSS Centre of Excellence a vývojovým týmem Detektoru – vymezení požadavků a návrhů na přizpůsobení produktu
7) **Příprava testování ve spolupráci s ČTÚ** – rozhodnutí o verzi testování – v reálném prostředí/laboratorní testování/ve stíněné komoře

8) **Testování Detektoru** přizpůsobeného v závislosti na předchozí diskuzi a technických možnostech
    - Provedení prvotního účelového testu s reálnou rušičkou ve spolupráci s ČVUT a ČTÚ
9) **Dlouhodobý sběr dat** – dlouhodobý sběr reálných dat po dobu 6 až 12 měsíců
10) **Evaluace dat** získaných z průběhu testování
11) **Návrhy na požadované parametry** produktu a definování kritických míst na základě vyhodnocených dat.

Dle postupu podle mnou navržené metodiky jsou v nadcházející kapitole 7 zpracovány materiály pro první jednání s energetickými společnostmi ČEPS a ČEZ Distribuce, a.s., V oblasti energetiky lze identické materiály v minoritně upravené formě použít i pro jednání s distribučními společnostmi PRE Distribuce a.s. a E.ON Distribuce a.s. (finální podoba materiálů pro společnosti ČEPS a ČEZ Distribuce, a.s. je uvedena v příloze č. [4, 5]). Dále byly zpracovány materiály pro první jednání s Ředitelstvím silnic a dálnic ČR v souvislosti se zaváděním družicového mýtného systému v ČR a zobecněné materiály pro provozovatele lokálních letišť s publikovaným LPV (případně se zamýšlenou publikací LPV). Návrh materiálů pro druhé jednání byl zatím zpracován pro Ředitelství silnic a dálnic. Důvodem je aktuální situace ve výběru nového provozovatele mýtného systému v ČR. Dále byly materiály vypracovány pro společnost ČEPS z důvodu aktuální situace v oblasti energetiky a již dříve proběhlých jednání mezi zástupci ČEPS a GNSS Centre of Excellence jakožto účastníka projektu.

# 7 Zpracování návrhu informačních materiálů týkajících se možnosti zabezpečení proti nezákonnému rušení GNSS v závislosti na konkrétním problému pro dílčí stupně managementu

Následující kapitoly představují návrh obsahu materiálů zpracovaných na základě zanalyzování vhodných subjektů kritické infrastruktury, které využívají pro své kritické i nekritické aplikace GNSS signál. Pro zahájení diskuze ohledně navrhovaného řešení a zapojení subjektu do spolupráce na budoucím projektu, testování a především sběru dat v reálném provozu konkrétního subjektu, byly vypracovány materiály v kapitole 7.1.1. Materiály k druhému jednání, uvedené v kapitole 7.1.2, slouží pro prezentaci dílčích charakteristik nabízeného produktu Detektor v detailnějším zpracování, představení možného způsobu implementace a možných hrozeb vyplívajících z nedostatečného zabezpečení systémů využívajících GNSS. Smyslem je uvést do problematiky pracovníky zapojovaných subjektů a zahájit s nimi spolupráci na jednotlivých krocích projektu.

## 7.1 Energetika – ČEPS

### 7.1.1 Podklady k prvnímu jednání

Projekt: Systém pro odhalování nezákonného rušení GNSS signálu v blízkosti strategické infrastruktury

Projekt s názvem *Systém pro odhalování nezákonného rušení GNSS signálu v blízkosti strategické infrastruktury*, s pracovním názvem *Detektor* je zpracováván v rámci Programu bezpečnostního výzkumu České republiky 2015-2020, vyhlášeným Ministerstvem Vnitra ČR. Na realizaci projektu spolupracuje ČVUT Fakulta elektrotechnická a Fakulta dopravní a GNSS Centre of Excellence. Cílem projektu je zvýšení ochrany kritické infrastruktury (nejen té kritické) využívající pro své klíčové funkce signálu GNSS před nezákonným rušením signálu prostřednictvím Jamming a Spoofing.

Výstupem projektu je funkční systém schopný detekce a přesné lokalizace zdroje rušení typu Jamming a Spoofing a zabraňující ovlivňování funkčnosti (kritických) aplikací využívajících signálu GNSS z pohledu časové synchronizace nebo funkce určení přesné pozice.

**Současný stav problému**

S rozmachem využití GNSS dochází i k častějšímu výskytu nezákonného rušení signálu ať už úmyslně (způsobení finančních škod nebo ochromení infrastruktury) nebo neúmyslně využíváním osobních rušiček k jinému účelu, ovšem ovlivňujících i jiné subjekty. Společnost ČEPS, a.s. využívající GNSS signál k časové synchronizaci systému pro zjišťování fázových poměrů mezi uzly přenosové soustavy, se může lehce stát terčem útoku rušením GNSS. Pro zamezení vzniku finančních škod a nehod, které už v zahraničí vedly až k black-outu, je třeba dostatečné ochrany proti těmto rozrůstajícím se typům rušení.

**Popis navrhovaného řešení**

Detektor přichází s inovačním řešením kombinujícím schopnost detekce rušení typu Jamming a Spoofing, určení azimutu a přesné lokace zdroje rušení. Takový produkt dosud na trhu není dostupný, ale z pohledu ochrany (kritické) infrastruktury je zcela žádoucí. Detektor je již od prvního návrhu vyvíjen modulárně, a tudíž umožňuje přizpůsobení specifickým požadavkům pro různé subjekty (kritické) infrastruktury. Zařízení je postaveno jako distribuovaný systém skládající se z 1 až 3 měřících stanovišť pracujících na principu Software Defined Radio (SDR) z důvodu velké flexibility umožňující aplikaci nových metodik detekce rušení. Použitý anténní blok se skládá ze 4 samostatných anténních zářičů.

**Systém umožňuje:**

- Monitorování, detekci a rozpoznání typu rušení GNSS signálu
- Okamžité informování uživatele o případné nespolehlivosti nebo nedostupnosti GNSS signálu
- Určení směru a přesné polohy zdroje rušení

Rádi bychom Vás požádali o spolupráci při řešení projektu, zejména s ohledem na definování technických požadavků a potřeb ze strany ČEPS. A to především z důvodu posílení ochrany subjektu proti hrozbám způsobujícím snížení provozuschopnosti s možným dopadem nejen na ČEPS, ale i společnost jako celek. První funkční vzorek bude dostupný začátkem léta 2018. S tím přichází i možnost aktivního testování v reálném provozu. Reálným testováním v prostředí společnosti ČEPS, resp. na vybraném místě uzlu přenosové soustavy, získáme data pro navržení optimálního rozmístění měřících stanic, lze vytvářet různé potenciální scénáře rušení a následně po analýze a vzájemné konzultaci výsledků, modulovat produkt přesně podle potřeb společnosti.

**Co bude přínosem pro ČEPS:**

- Plně spolehlivý systém využívající výhod GNSS signálu, který splňuje všechny bezpečnostní prvky bez možnosti úmyslného ohrožení
- Možnost reálného testování, odhalující kritická místa a návrhy na rozmístění měřících stanovišť
- Modulovaný produkt podle specifických požadavků ČEPS

ČEPS tímto získá produkt, přesně podle svých specifických požadavků, který plně vyhovuje podmínkám pro nasazení do ostrého provozu.

**O co chceme požádat ze strany ČEPS:**

- Určení skupiny pracovníků pro součinnost při implementaci produktu do testovacího provozu
    - Definování možných kritických míst
    - Specifikování požadavků na produkt
    - Monitorování průběhu testovacího provozu a podíl na vyhodnocování výsledků
    - Specifikování následných požadavků na úpravu produktu
- Projekt máme financovaný ze strany Ministerstva vnitra, takže nyní máme zájem o spolupráci s ohledem na výše uvedenou součinnost – tedy není nutné vkládat žádné finanční prostředky ze strany ČEPS (vyjma nákladů spojených s činností vašich vlastních pracovníků)

Chtěli bychom Vás tímto požádat o možnost setkání, kde rádi odpovíme na případné technické dotazy.

### 7.1.2 Návrh podkladů k druhému jednání

Projekt: Systém pro odhalování nezákonného rušení GNSS signálu v blízkosti strategické infrastruktury

Projekt s názvem *Systém pro odhalování nezákonného rušení GNSS signálu v blízkosti strategické infrastruktury*, s pracovním názvem *Detektor* je zpracováván v rámci Programu bezpečnostního výzkumu České republiky 2015-2020, vyhlášeným Ministerstvem Vnitra ČR. Na realizaci projektu spolupracuje ČVUT Fakulta elektrotechnická a Fakulta dopravní a GNSS Centre of Excellence. Cílem projektu je zvýšení ochrany kritické infrastruktury

(nejen té kritické) využívající pro své klíčové funkce signálu GNSS před nezákonným rušením signálu prostřednictvím Jamming a Spoofing.

Výstupem projektu je funkční systém schopný detekce a přesné lokalizace zdroje rušení typu Jamming a Spoofing a zabraňující ovlivňování funkčnosti kritických aplikací využívajících signálu GNSS z pohledu časové synchronizace, nebo funkce určení přesné pozice.

## Současný stav problému ve společnosti ČEPS

Nezákonné rušení GNSS signálu se v moderní společnosti stává běžným prvkem ohrožujícím subjekty kritické infrastruktury. Společnost ČEPS jako výhradní provozovatel energetické přenosové soustavy v ČR spadá dle Nařízení vlády č. 432/2010 do prvků kritické infrastruktury. ČEPS distribuce, disponující moderní energetickou soustavou využívá v rámci zajištění provozu GNSS signál, konkrétně funkce časové synchronizace a časových značek. Synchronizace systému pro zajišťování fázových poměrů mezi uzly přenosové soustavy je závislá na funkci přesného časování podle GNSS a může se lehce stát terčem útoku rušením GNSS. GNSS signál využívaný pro tyto účely je při příchodu do přijímače oslaben průchodem atmosférou, což umožňuje snadné útoky rušení GNSS metodami Jamming a Spoofing, které jsou v současnosti na vzestupu.

### Rušení typu Jamming a vliv na systémy ČEPS

Typ rušení Jamming je elementární způsob rušení. Ovlivnění se projevuje oslabením nebo ztrátou GNSS signálu při příjmu koncovým přijímačem. Zdrojem Jamming jsou v první řadě jednoduché osobní rušičky PPD, v druhé řadě sofistikovanější rušičky s možností řízení výkonu a s napájením z akumulátoru, tzn. výdrží až několik dní. Druhý typ rušiček může skýtat pro ČEPS značný problém, jelikož systémy (WAMS) monitorující soustavu jsou schopny uchovat svou časovou synchronizaci s max. odchylkou +/- 5 μs po dobu jedné hodiny. Jamming je pomocí tohoto systému eliminován pouze částečně a neposkytuje informace operátorům řídícího centra.

## Rušení typu Spoofing a vliv na systémy ČEPS

Typ rušení Spoofing je sofistikovaným a hůře detekovatelným způsobem rušení. GNSS signál je v tomto případě kontinuálně přijímán přijímačem. Rušičkou je vysílán identický signál k autentickému GNSS signálu, který je postupně zesilován do momentu plného zachycení GNSS přijímačem. Jelikož nedochází k přerušení příjmu GNSS signálu, je Spoofing obtížně detekovatelný. Při Spoofingovém útoku trvajícím 11 minut může dojít při

časové synchronizaci jednotek PMU k časové chybě vyšší, než je povolená chyba dle standardu.

Následky rušení se mohou projevit způsobením finančních škod nebo ochromením infrastruktury, v krajních situacích až black-outem, jak tomu již bylo v zahraničí (USA – Ohio/Michigan 2003).

**Parametry produktu Detektor a možný způsob implementace u ČEPS**

*Monitorování – Detekce – Rozpoznání typu rušení – Informování uživatele – Azimut – Poloha*

Detektor je inovativní modulární produkt, který kombinuje funkce detekce rušení typu Jamming a Spoofing, určení azimutu a přesné lokace zdroje rušení. Modularita umožňuje přizpůsobení produktu včetně HW a SW podle specifik konkrétního uživatele.

Produkt je tvořen 1 až 3 měřícími stanovišti pracujícími na principu Software Defined Radio (SDR) s anténním blokem 4 samostatných zářičů typu J-Pole umožňujících přizpůsobení vyzařovací charakteristiky. Citlivost měřící antény je stanovena dle ICAO limitu na –120dBm. V případě Spoofing je při odfiltrování šumu a rušivého signálu přijímač schopen zvýšit výkon autentického signálu nad úroveň falešného. Měřící stanoviště jsou propojena pomocí optické kabeláže s centrálním zpracovatelským serverem, u prototypu je počítáno se vzdáleností cca 1,7 km, kterou lze prodloužit použitím jiného druhu kabeláže při zachování kvality i finančních nákladů. Detektor využívá triangulační metody zaměření zdroje rušivého signálu s rozlišovací schopností měření azimutu +- 5° odpovídající šířce detekčního louče 10° celkem s 36 detekčními polohami v kružnici. Sběr signálu ze všech měřících stanovišť probíhá kontinuálně, data jsou přenášena do zpracovatelského serveru, kde jsou vyhodnocovány signály 4 x 3 stanovišť, což umožňuje matematické a fyzikální porovnání signálů z jednotlivých antén mezi sebou. Grafické uživatelské rozhraní (GUI) lze upravit na základě požadavků společnosti ČEPS a doplnit základní nastavení o zobrazení požadovaných parametrů.

**Testování na konkrétní rozvodně přenosové soustavy**

Na základě stanovení konkrétních požadavků na produkt společností ČEPS, bude připraven prototyp pro reálné testování v provozu na vybrané rozvodně přenosové soustavy. Sběr dat bude probíhat po dobu 6–12 měsíců, současně bude probíhat evaluace. Na základě výsledků je možná následná úprava konečného produktu a jeho budoucí nasazení do reálného provozu. V rámci testování bude ve spolupráci s ČVUT a ČTÚ proveden prvotní

účelový test s reálnou rušičkou, který bude probíhat dle přesně stanovené osnovy. V průběhu testování bude měřeno chování systémů při vlivech rušení a chování Detektoru při probíhajícím rušení. Na základě výsledků lze následně definovat konkrétní kritická místa a požadované parametry produktu.

Výsledkem bude produkt spojující reálné technické parametry a požadavky konečného uživatele.

**Standard reportingu událostí**

Detektor kontinuálně provádí sběr dat, která předává do zpracovatelského serveru. Data jsou vyhodnocována na základě stanovených algoritmů a prostřednictvím reportu předávána uživateli.

Návrh standardu reportingu v čase může být následující:

1) V reálném čase
2) Periodicky – podle definovaných intervalů
3) 1 x za měsíc

Obsah reportu může být následující:

1) Povinný – ID události, typ události, typ zařízení, frekvenční pásmo rušení (GPS/Galileo), azimut, lokalita rušením, datum a čas události v UTC,
2) Nepovinný – začátek události, trvání, ztráta signálu GNSS (ano; ne), rozsah rušícího signálu, přístup k surovým datům, referenční hodnota šumu pro snímač, maximální intenzita v dB nad minimální prahovou hodnotou zařízení.

**Co bude přínosem pro ČEPS:**

- Plně spolehlivý systém využívající výhod GNSS signálu, který splňuje všechny bezpečnostní prvky bez možnosti úmyslného ohrožení
- Možnost reálného testování odhalujícího kritická místa a návrhy na rozmístění měřících stanovišť
- Modulovaný produkt podle specifických požadavků ČEPS

ČEPS tímto získá produkt, přesně podle svých specifických požadavků, který plně odpovídá podmínkám pro nasazení do ostrého provozu.

**O co chceme požádat ze strany ČEPS**

- Určení pracovní skupiny zapojující se do vývoje produktu a implementace do testovacího provozu
    - Předdefinování aktuálních kritických míst v systémech využívajících GNSS
    - Zahájení diskuze pro specifikování požadavků na produkt, včetně HW/SW + GUI
    - Monitorování v průběhu testování a vyhodnocování výsledků – stanovení konečných požadavků ve spolupráci s vývojovým týmem

Chtěli bychom Vás tímto požádat o možnost setkání, kde rádi odpovíme na konkrétní technické dotazy a detailně prodiskutujeme strukturu produktu.

## 7.2 Silniční doprava – Ředitelství silnic a dálnic ČR

### 7.2.1 Podklady k prvnímu jednání

Návrh tohoto podkladu je po obsahové stránce velmi podobný s tím, uvedeným v kapitole 7.1.1 s drobnými změnami pro konkrétního partnera. Kompletní text tohoto podkladu je uvedený v příloze číslo 1.

### 7.2.2 Návrh podkladů k druhému jednání

Návrh tohoto podkladu je po obsahové stránce velmi podobný s tím, uvedeným v kapitole 7.1.2 s drobnými změnami pro konkrétního partnera. Kompletní text tohoto podkladu je uvedený v příloze číslo 2.

## 7.3 Letecká doprava – Provozovatelé lokálních letišť

### 7.3.1 Podklady k prvnímu jednání

Návrh tohoto podkladu je po obsahové stránce velmi podobný s tím, uvedeným v kapitole 7.1.1 s drobnými změnami pro konkrétního partnera. Kompletní text tohoto podkladu je uvedený v příloze číslo 3.

# Závěr

Obsah této diplomové práce rozebírá problematiku rušení GNSS signálu při jeho využití v kritické infrastruktuře. V úvodu teoretické části jsou uvedeny hlavní pojmy vztahující se k problematice rušení GNSS signálu. Vysvětleny jsou zde externí a interní vlivy na kvalitu GNSS signálu, které způsobují, že při dosažení přijímače je signál již velmi slabý. V návaznosti na to je možné GNSS signál velmi jednoduše ovlivnit pomocí typů rušení Jamming, Spoofing a Meaconing. V souvislosti s tématem a aktuální situací v prostředí kritické infrastruktury jsou blíže rozebírány pouze typy rušení Jamming a Spoofing. Technologická náročnost těchto dvou typů rušení není vysoká, a proto jsou i na trhu velmi jednoduše dostupné různé typy rušiček, které lze pořídit v průměru za 1000,- Kč. Prodej včetně distribuce rušiček GNSS signálu je v zemích EU protizákonný, tudíž jsou označovány jako PPD (Prostředky zajištění osobního soukromí), které mají sloužit jako ochrana před nevyžádaným sledováním subjektu třetí stranou. Kromě těchto jednoduchých typů lze využít sofistikované typy rušiček s delším dosahem a výdrží baterie až několik dní. Tyto rušičky mohou závažně poškodit subjekty kritické infrastruktury.

Závislost na GNSS signálu s rozvojem moderní společnosti a technologií stoupá, GNSS signál je využíván v kritické infrastruktuře celkem v 15 sektorech, z nichž pro 11 sektorů je klíčový k zajištění správné funkčnosti systémů. Rušení GNSS signálu v těchto sektorech může zapříčinit vážné finanční škody a ohrozit bezpečnost občanů země. Pokud se zaměříme na Českou republiku, GNSS signál je využíván ve všech 11 sektorech. Práce se zaměřuje na jeho využití v systémových aplikacích v sektoru energetiky, pozemní dopravy a letecké dopravy a elektronických komunikačních sítí.

Tato diplomová práce si klade jako hlavní cíl rozšířit povědomí o nezákonném rušení GNSS signálu v prostředí kritické infrastruktury. Za tímto účelem je zpracována teoretická část práce, která se věnuje problematice rušení GNSS signálu v blízkosti kritické infrastruktury v teoretické rovině. Analýza dostupných produktů prokázala, že na trhu není dostupné řešení, které by kombinovalo funkce kontinuálního monitorování, detekce a rozpoznání typu rušení (Jamming/Spoofing), určení azimutu a přesné polohy zdroje rušení. Práce proto navazuje na projekt s názvem Systém pro odhalování nezákonného rušení GNSS signálu v blízkosti strategické infrastruktury, který byl vyvinutý ve spolupráci s ČVUT a umožňuje kombinaci zmíněných funkcí včetně modulace pro různé subjekty kritické i nekritické infrastruktury.

Z tohoto teoretické úvodu, rozboru dostupných produktů a z následné analýzy prostředí kritické infrastruktury vznikly informační materiály pro navázání diskuze ohledně implementace vhodného řešení za účelem minimalizace dopadů nezákonného rušení. Rozšířené materiály vznikly za účelem blíže seznámit pracovníky vybraných subjektů s problematikou a zahájit s nimi spolupráci na jednotlivých krocích projektu. Tyto materiály spolu s teoretickou rovinou a navrženou metodikou pro podporu zavádění systému detekce nezákonného rušení GNSS signálu v prostředí kritické infrastruktury slouží jako ucelený materiál ke zvýšení informovanosti o aktuální hrozbě a možnostech se jí bránit.

Práce slouží jako celkový vhled do problematiky nezákonného rušení GNSS signálu v prostředí kritické i nekritické infrastruktury a současně poukazuje na hrozby, které plynou zejména z rušení prostřednictvím PPD a sofistikovaných typů rušiček.

Na základě navržené metodiky a materiálů lze dále pokračovat v rozšiřování tohoto tématu nejen v České republice u dalších subjektů kritické i nekritické infrastruktury. Obecnou metodiku a materiály lze použít k rozšiřování povědomí o nezákonném rušení GNSS signálu v blízkosti kritické infrastruktury i mimo hranice České republiky a zaměřit se na analýzu potřeb subjektů například v dalších zemích střední a východní Evropy.

# Použitá literatura


[1] ČÁBELKA, Miroslav. Úvod do GPS [online]. 2008 [cit. 2018-04-09]. Dostupné z: https://www.natur.cuni.cz/geografie/geoinformatika-kartografie/ke-stazeni/vyuka/gps/skriptum-uvod-do-gps/

[2] LOUŽIL, Viktor. Detekce a lokalizace rušení GNSS systémů [online]. Praha, 2017 [cit. 2018-04-09]. Diplomová práce. ČVUT. Dostupné z: https://dspace.cvut.cz/bitstream/handle/10467/68391/F3-DP-2017-Louzil-Viktor-Detekce_a_lokalizace_ruseni_GNSS_systemu.pdf?sequence=-1&isAllowed=y

[3] KAPLAN, Elliott D. a C. HEGARTY. Understanding GPS: principles and applications [online]. 2nd ed. Boston: Artech House, c2006 [cit. 2018-04-09]. GNSS technology and applications series. ISBN 15-805-3894-0.

[4] DUŠA, Tomáš. Zvýšení bezpečnosti kritických GNSS aplikací využitím nástrojů fuze dat. Praha, 2017. Disertace. ČVUT.

[5] DUŠA, Tomáš. Odhaľovanie nezákonného rušenia signálov GNSS: Security konference 2016 [prezentace]. Praha, 2016.

[6] PULLEN, Sam a Grace XINGXIN GAO. GNSS Jamming in the Name of privacy: Potential Threat to GPS Aviation [online]. 03/2012 [cit. 2018-03-07]. Dostupné z: http://www.insidegnss.com/auto/marapr12-Pullen.pdf

[7] Massive GPS Jamming Attack by North Korea [online]. 2012 [cit. 2018-03-08]. Dostupné z: http://gpsworld.com/massive-gps-jamming-attack-by-north-korea/

[8] NOVÁK, Jiří, Adéla JELÍNKOVÁ a Lukáš ŽUBRIETOVSKÝ. Rušení GNSS (nejen) v aplikacích pro kritickou infrastrukturu [prezentace]. CGI Group Inc., 2016.

[9] PSIAKI, Mark L. a Todd E. HUMPHREYS. GNSS Spoofing and Detection. Proceedings of the IEEE [online]. 2016, 104(6), 1258-1270 [cit. 2018-05-10]. DOI: 10.1109/JPROC.2016.2526658. ISSN 0018-9219. Dostupné z: http://ieeexplore.ieee.org/document/7445815/

[10] MARNACH, Daniel, Sjouke MAUW, Miguel MARTINS a Carlo HARPES. Detecting Meaconing Attacks by Analysing the Clock Bias of GNSS Receivers. Artificial Satellites [online]. 2013 [cit. 2018-03-14]. DOI: 10.2478/arsa-2013-0006.

[11] CALCAGNO, R., S. FAZIO, S. SAVASTA a F. DOVIS. An interference detection algorithm for COTS GNSS receivers. 2010 5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC) [online]. IEEE, 2010, 2010, , 1-8 [cit. 2018-05-10]. DOI:

10.1109/NAVITEC.2010.5708008. ISBN 978-1-4244-8740-0. Dostupné z: http://ieeexplore.ieee.org/document/5708008/

[12] BARTL, Sascha, Philipp BERGLEZ a Bernhard HOFMANN-WELLENHOF. GNSS interference detection, classification and localization using Software-Defined Radio. 2017 European Navigation Conference (ENC) [online]. IEEE, 2017, 2017, , 159-169 [cit. 2018-05-10]. DOI: 10.1109/EURONAV.2017.7954205. ISBN 978-1-5090-5922-5. Dostupné z: http://ieeexplore.ieee.org/document/7954205/

[13] YANG, Jeong Hwan, Chang Ho KANG, Sun Young KIM a Chan Gook PARK. Intentional GNSS Interference Detection and Characterization Algorithm Using AGC and Adaptive IIR Notch Filter. International Journal of Aeronautical and Space Sciences [online]. 2012, 13(4), 491-498 [cit. 2018-05-10]. DOI: 10.5139/IJASS.2012.13.4.491. ISSN 2093-274X. Dostupné z: http://koreascience.or.kr/journal/view.jsp?kj=HGJHC0&py=2012&vnc=v13n4&sp=491

[14] DAI, Xinzhi, Junwei NIE, Baiyu LI, Zukun LU a Gang OU. Performance of GNSS receivers with AGC in noise pulse interference. In: 2016 5th International Conference on Computer Science and Network Technology (ICCSNT) [online]. IEEE, 2016, 2016, s. 735-740 [cit. 2018-05-10]. DOI: 10.1109/ICCSNT.2016.8070255. ISBN 978-1-5090-2129-1. Dostupné z: http://ieeexplore.ieee.org/document/8070255/

[15] Evropský program na ochranu kritické infrastruktury. 2007. Dostupné také z: http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=LEGISSUM:l33260&from=CS

[16] MINÁŘ, Alexander. Kritická infrastruktura EU a ČR [online prezentace]. [cit. 2018-05-10]. Dostupné z: https://www.google.cz/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwiboM7bornZAhVBmbQKHacjCG8QFggoMAA&url=http%3A%2F%2Fpvvc.cz%2Fckfinder%2Fuserfiles%2Ffiles%2FPrezentace%2520%2520.ppt&usg=AOvVaw3FAKhLy5Kh_Aq-ERyS6uVV

[17] GRAHAM, Monty. GPS Use in U.S. Critical Infrastructure and Emergency Communications[online]. [cit. 2018-03-21]. Dostupné z: https://www.gps.gov/multimedia/presentations/2012/10/USTTI/graham.pdf

[18] SADLIER, Greg, Rasmus FLYTKJÆR, Farooq SABRI a Daniel HERR. The economic impact on the UK of a disruption to GNSS [online]. In: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/619544/17.3254_Economic_impact_to_UK_of_a_disruption_to_GNSS_-_Full_Report.pdf

[19] PLCHÚT, Martin. Co je Smart Grid? [online]. 13. 4. 2015 [cit. 2018-03-22]. Dostupné z: https://elektro.tzb-info.cz/12544-co-je-smart-grid

[20] WOODROW, Bellamy. Are GPS Jamming Incidents a Growing Problem for Aviation?. Avionics[online]. 31.1.2017 [cit. 2018-04-04]. Dostupné z: http://www.aviationtoday.com/2017/01/31/are-gps-jamming-incidents-a-growing-problem-for-aviation/

[21] Navigation developments in SESAR [online]. [cit. 2018-04-04]. Dostupné z: http://www.eurocontrol.int/articles/navigation-sesar

[22] NOVOTNÝ, Radek. GNSS se stává běžnou součástí infrastruktury. Ekonom [online]. 2015, (06) [cit. 2018-04-04]. Dostupné z: https://www.gsa.europa.eu/sites/default/files/08-12_priloha_LoEk.pdf

[23] BRODSKÝ, Pavel. RNAV přiblížení [online]. [cit. 2018-04-04]. Dostupné z: https://wiki.vacc-cz.org/index.php?title=RNAV_přibl%C3%ADžen%C3%AD

[24] Technický popis systému EGNOS [online]. [cit. 2018-04-04]. Dostupné z: http://www.czechspaceportal.cz/3-sekce/gnss-systemy/egnos/technicky-popis-systemu-egnos/

[25] DIVIS, Dee Ann. Financial Networks Shifting to GPS-Stamped Precise Time [online]. 2014 [cit. 2018-04-01]. Dostupné z: http://www.insidegnss.com/node/4355

[26] SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY 2014/65/EU ze dne 15. května 2014 o trzích finančních nástrojů a o změně směrnic 2002/92/ES a 2011/61/EU. 2014. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32014L0065&from=EN

[27] GNSS Market Report [online]. 2017, (5) [cit. 2018-04-01]. Dostupné z: https://www.gsa.europa.eu/system/files/reports/gnss_mr_2017.pdf

[28] ČTK. Kapsch zvažuje nabídnout státu satelitní systém na výběr mýta [online]. 25.5.2017 [cit. 2018-04-02]. Dostupné z: http://zpravy.e15.cz/byznys/doprava-a-logistika/kapsch-zvazuje-nabidnout-statu-satelitni-system-na-vyber-myta-1332865

[29] Pracovní skupina elektronické mýtné [online]. 2013 [cit. 2018-04-02]. Dostupné z: http://www.elektronickemytne.cz

[30] Zařízení automatického tísňového volání ve všech nových typech aut od jara 2018 [online]. 28.4.2015 [cit. 2018-04-03]. Dostupné z: http://www.europarl.europa.eu/news/cs/press-room/20150424IPR45714/zarizeni-automatickeho-tisnoveho-volani-ve-vsech-novych-typech-aut-od-jara-2018

[31] Automatické tísňové volání (eCall) [online]. [cit. 2018-04-03]. Dostupné z: http://www.czechspaceportal.cz/3-sekce/its---inteligentni-dopravni-systemy/oblasti-rozvoje-its/automaticke-tisnove-volani-ecall/

[32] CURRY, Charles. GAARDIAN GPS Interference Detection & Mitigation [online prezentace]. 2010 [cit. 2018-05-10]. Dostupné z: http://www.npl.co.uk/upload/pdf/20091208_t%2Bf_curry.pdf

[33] Detecting GPS Jamming and Interference [online]. [cit. 2018-05-10]. Dostupné z: http://www.chronos.co.uk/index.php/en/resources/sentinel

[34] PÖLÖSKEY, Martin a Carsten HOELPER. DETECTION OF DYSFUNCTION OF SATNAV-BASED AUTOMOTIVE SYSTEMS BY GPS- OR GALILEO-JAMMERS [prezentace]. 2014.

[35] WILDE, John. GNSS Monitoring for Critical Applications (GMCA) - Overview [online]. [cit. 2018-05-12]. Dostupné z: https://www.gps.gov/cgsic/meetings/2015/wilde2.pdf

[36] TIGER: Trusted GNSS Receiver [online]. [cit. 2018-05-12]. Dostupné z: https://www.gsa.europa.eu/trusted-gnss-receiver-0

[37] CTL3510 GNSS Interference Detector and Logger: Datasheet [online]. [cit. 2018-05-12]. Dostupné z: http://www.chronos.co.uk/files/pdfs/ctl/ctl3510.pdf

[38] CTL3520 GNSS Interference Locator: Datasheet [online]. [cit. 2018-05-12]. Dostupné z: http://www.chronos.co.uk/files/pdfs/ctl/ctl3520.pdf

[39] CTL8200 eLoran GPS UTC Timing Receiver: Datasheet [online]. [cit. 2018-05-12]. Dostupné z: http://www.chronos.co.uk/files/pdfs/ctl/CTL8200.pdf

[40] QUEROL, Jorge a Adriano CAMPS. Real-time Pre-correlation Anti-jamming System for Civilian GNSS Receivers. Proceedings of the 30th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2017) [online]. Portland, Oregon, 1267 - 1288 [cit. 2018-05-12]. Dostupné z: https://www.ion.org/publications/abstract.cfm?articleID=15304

[41] Fenix – Front-End GNSS Interference eXcisor: Technology [online]. [cit. 2018-05-12]. Dostupné z: http://www.fenix-gnss.com/index.php/tech

[42] GNOME. IDS [online]. [cit. 2018-05-12]. Dostupné z: https://www.idscorporation.com/pf/gnome/#1481041686269-67220069-0138b704-28e4da12-5a30

[43] GNSS INTEGRITY AND SIGNAL MONITORING OBSERVATORY. Nottingham Scientific Ltd [online]. [cit. 2018-05-12]. Dostupné z: http://www.nsl.eu.com/nsl-jcms/gnss-environment/gnss-performance-monitor

[44] SecureSync BroadShield Option: GPS Jamming and Spoofing Detection [online]. [cit. 2018-05-12]. Dostupné z: https://spectracom.com/sites/default/files/document-files/SecureSync_BroadShield_Option_revA.pdf

[45] CO JE TO BLACKOUT? OPRAVDU NĚCO TAKOVÉHO MŮŽE POSTIHNOUT STŘEDNÍ EVROPU? [online]. [cit. 2018-05-12]. Dostupné z: http://www.ceps.cz/cs/casto-kladene-otazky

[46] HONEYWELL. THE BENEFITS OF LPV APPROACH OPERATIONS FOR THE AIRLINE OPERATOR[online]. [cit. 2018-05-12]. Dostupné z: https://aerospace.honeywell.com/en/~/media/aerospace/files/white-paper/c61-1631-000-000-the-benefits-of-lpv-approach-operations-for-the-airline-operator-wp.pdf

[47] Zákon o krizovém řízení a o změně některých zákonů (krizový zákon). 2001. Dostupné také z: https://www.zakonyprolidi.cz/cs/2000-240

[48] EGNOS - Evropská „podpůrná“ geostacionární navigační služba [online]. 2017 [cit. 2018-05-15]. Dostupné z: http://www.czechspaceportal.cz/3-sekce/gnss-systemy/egnos/

[49] WARBURTON, John a Carmen TEDESCHI. GPS Privacy Jammers and RFI at Newark – Navigation Team AJP-652 Results [online]. 2011 [cit. 2018-05-16]. Dostupné z: http://laas.tc.faa.gov/documents/Misc/GBAS%20RFI%202011%20Public%20Version%20Final.pdf

[50] GALETKA, Martin. Přenosová soustava elektrické energie [online]. In: . 11.1.2016 [cit. 2018-05-16]. Dostupné z: https://energetika.tzb-info.cz/elektroenergetika/13676-prenosova-soustava-elektricke-energie

[51] ŠÍMA, Jan, Stanislav VLČEK, Bohumil SADECKÝ a Marek HAVRDA. WAMS systémy pro monitoring elektrizační soustavy [online]. [cit. 2018-05-16]. Dostupné z: http://www.allforpower.cz/UserFiles/files/2011/wams_alstom.pdf

[52] GOWARD, Dana. GPS disruption is a growing problem for Aviation, reports show [online]. 7. 11. 2016 [cit. 2018-05-19]. Dostupné z: https://rntfnd.org/2016/11/07/gps-disruption-is-a-growing-problem-for-aviation-reports-show/

[53] ANALÝZA VÝVOJE VÝBĚRU MÝTA NA ZPOPLATNĚNÝCH POZEMNÍCH KOMUNIKACÍCH V ČR[online]. 2016 [cit. 2018-05-21]. Dostupné z: http://www.ioda.cz/_publikace/pub/2015_IODA_analyza_myto.pdf

[54] Projeté kilometry a projeté mýto - leden až prosinec 2017 [online]. 2018 [cit. 2018-05-21]. Dostupné z: http://www.vyrocenky.cz/dokument?f=1c925b708e5d2934cf004e660aef4795

[55] LPV Procedure Map [online]. [cit. 2018-05-21]. Dostupné z: https://egnos-user-support.essp-sas.eu/new_egnos_ops/resources-tools/lpv-procedures-map

[56] *ICAO. Doc 9849: Global Navigation Satellite System (GNSS) Manual*. Montreal, 2012. Dostupné také z: https://www.icao.int/Meetings/anconf12/Documents/Doc.%209849.pdf

[57] CALCAGNO, R., S. FAZIO, S. SAVASTA a F. DOVIS. An interference detection algorithm for COTS GNSS receivers. *2010 5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)* [online]. IEEE, 2010, 1-8 [cit. 2018-05-21]. DOI: 10.1109/NAVITEC.2010.5708008. ISBN 978-1-4244-8740-0. Dostupné z: http://ieeexplore.ieee.org/document/5708008/

[58] SHEPARD, Daniel P., Todd E. HUMPHREYS a Aaron A. FANSLER. Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks. *International Journal of Critical Infrastructure Protection* [online]. 2012, **5**(3-4), 146-153 [cit. 2018-05-25]. DOI: 10.1016/j.ijcip.2012.09.003. ISSN 18745482. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S1874548212000480

[59] NOVÁK, Jiří, Adéla JELÍNKOVÁ a Lukáš ŽUBRIETOVSKÝ. *Rušení GNSS (nejen) v aplikacích pro kritickou infrastrukturu*.

[60] *Critical infrastructure* [online]. [cit. 2018-05-25]. Dostupné z: https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en

# Seznam obrázků

Obrázek 1: Multipath – odraz od okolních budov, zdroj: [1] ..... 19
Obrázek 2: Jednoduché a snadno dostupné PPD ..... 24
Obrázek 3: Typy armádních Jammerů ..... 24
Obrázek 4: Využití GPS aplikací v civilním sektoru, zdroj: [17] ..... 35
Obrázek 5: Princip systému SBAS (vlevo) a systému GBAS (vpravo) s využitím pozemních stanic, zdroj: airnav.eu ..... 40
Obrázek 6: Princip fungování systému eCall, zdroj: czechspaceportal.cz ..... 43
Obrázek 7: GUI produktu GNOME, zdroj: interní podklady projektu ..... 52
Obrázek 8: Nárůst výnosů z mýtného meziročně od roku 2007 do 2015, zdroj:ioda.cz [53] . 60
Obrázek 9: Publikace LPV v ČR (letiště s publikovaným LPV jsou vyznačena zeleně, plánovaná publikace LPV je označena žlutě), zdroj: EGNOS User Support [55] ..... 64

# Seznam schémat

Schéma 1: Hrozby otevřené službě Galileo, zdroj: [8], vlastní úprava ..... 15
Schéma 2: Znázornění procesu útoku Spoofing – tmavě modrá značí falešný signál, světle modrá značí autentický GNSS signál [9] ..... 25
Schéma 3: Blokové schéma systému – rozmístění anténních zářičů a propojení měřících stanovišť s centrálním serverem a přenesení do GUI, zdroj: Detektor ruseni – prezentace.. 49
Schéma 4: Schéma antény J-Pole s kruhovou vyzařovací charakteristikou v rovině rovnoběžné s povrchem Země, zdroj: interní dokumenty k projektu ..... 50
Schéma 5: Schéma detekce zdroje rušení pomocí triangulační metody zaměření, zdroj: interní podkladky projektu ..... 51
Schéma 6: Dráhy LKPR a přilehlé komunikace D6 a D7, zdroj: vlastní ..... 62

# Seznam tabulek

Tabulka 1: Zaznamenané případy Jamming od roku 2007 do roku 2017, zdroj: [59], doplněno autorkou ..... 21
Tabulka 2: Charakteristiky aktuálně dostupných detekčních řešení Jamming a Spoofing, zdroj: vlastní ..... 48
Tabulka 3: Rušičky testované v rámci testování ČTÚ, ČVUT a ŘLP, zdroj: vlastní ..... 54
Tabulka 4: Porovnání dostupných PPD v závislosti na uváděném dosahu a ceně, zdroj: vlastní ..... 59

# Seznam příloh

Příloha 1 ..... 88
Příloha 2 ..... 91
Příloha 3 ..... 95
Příloha 4 ..... 98
Příloha 5 ..... 100

# Příloha 1

# Podklady k prvnímu jednání ŘSD

Projekt: Systém pro odhalování nezákonného rušení GNSS signálu v blízkosti strategické infrastruktury

Projekt s názvem *Systém pro odhalování nezákonného rušení GNSS signálu v blízkosti strategické infrastruktury*, s pracovním názvem *Detektor,* je zpracováván v rámci Programu bezpečnostního výzkumu České republiky 2015-2020, vyhlášeným Ministerstvem Vnitra ČR. Na realizaci projektu spolupracuje ČVUT Fakulta elektrotechnická a Fakulta dopravní a GNSS Centre of Excellence. Cílem projektu je zvýšení ochrany kritické infrastruktury (nejen té kritické) využívající pro své klíčové funkce signálu GNSS před nezákonným rušením signálu prostřednictvím Jamming a Spoofing.

Výstupem projektu je funkční systém schopný detekce a přesné lokalizace zdroje rušení typu Jamming a Spoofing a zabraňující ovlivňování funkčnosti kritických aplikací využívajících signálu GNSS z pohledu časové synchronizace nebo funkce určení přesné pozice.

**Současný stav problému**

S rozmachem využití GNSS dochází i k častějšímu výskytu nezákonného rušení signálu, ať už úmyslně (způsobení finančních škod nebo ochromení infrastruktury) nebo neúmyslně využíváním osobních rušiček k jinému účelu, ovšem ovlivňujících i jiné subjekty. ŘSD je organizací zajišťující provoz a výběr mýtných poplatků v ČR. Rok 2018 je v ČR s příchodem nového provozovatele mýtného systému, společnosti CzechToll, milníkem na cestě k zavedení systému družicového výběru mýtného. S družicovým výběrem mýtného vzniká problém s úmyslným rušením GNSS signálu pomocí levně dostupných osobních rušiček PPD na palubách automobilů podléhajících mýtné povinnosti. Mobilní jednotky využívané pro kontrolu dodržování mýtné povinnosti nejsou dostatečně vybaveny pro detekci všech aktuálních typů rušení GNSS signálu, a proto je v současné době jednoduché obejít platební povinnost a způsobit tak značné finanční škody.

**Popis navrhovaného řešení**

Detektor přichází s inovačním řešením kombinujícím schopnost detekce rušení typu Jamming a Spoofing, určení azimutu a přesné lokace zdroje rušení. Takový produkt dosud na trhu není dostupný, ale z pohledu ochrany (kritické) infrastruktury je zcela žádoucí.

Detektor je již od prvního návrhu vyvíjen modulárně, a tudíž umožňuje přizpůsobení specifickým požadavkům pro různé subjekty (kritické) infrastruktury. Zařízení je postaveno jako distribuovaný systém skládající se z 1 až 3 měřících stanovišť pracujících na principu Software Defined Radio (SDR) z důvodu velké flexibility umožňující aplikaci nových metodik detekce rušení. Použitý anténní blok se skládá ze 4 samostatných anténních zářičů.

**Systém umožňuje:**

- Monitorování, detekci a rozpoznání typu rušení GNSS signálu
- Okamžité informování uživatele o případně nespolehlivosti nebo nedostupnosti GNSS signálu
- Určení směru a přesné polohy zdroje rušení

Rádi bychom Vás požádali o spolupráci při řešení projektu, zejména s ohledem na definování technických požadavků a potřeb ze strany ŘSD. A to z důvodu zvýšení schopnosti detekovat a eliminovat obcházení mýtné povinnosti na komunikacích v ČR, tím zajistit kontrolu nad příjmy plynoucími z mýtných poplatků a umožnit organizaci následné jednodušší vymáhání poplatků. První funkční vzorek bude dostupný začátkem léta 2018. S tím přichází i možnost aktivního testování v reálném provozu. Reálné testování na zpoplatněných úsecích komunikací umožní sběr dat pro navržení optimálního rozmístění měřících stanovišť. Zařízení je z pohledu využití pro detekci rušení družicového mýtného systému vhodné umístit podél komunikace, v každém směru jedna detekční stanice. Současně bude nutné systém doplnit kamerovým systémem, který bude synchronně s detekováním pořizovat obrazové záznamy vozidel a jejich poznávacích značek. Na základě testování v reálném provozu na placených úsecích získáme jak vstupní data o množství vozidel vyhýbajících se mýtné povinnosti, tak i data pro následné modulování produktu podle potřeb ŘSD.

**Co bude přínosem pro ŘSD:**

- *Krátkodobý (momentální) přínos*:
    - V současné době ještě systém výběru mýtného funguje na mikrovlnné technologii, ale máme již možnost začít testovat rozsah problému na hranicích států, kde je družicový systém výběru mýtného implementován
    - Možnost aktuálního testování na hranici se Slovenskem na dálnici D2 a silnici E50.

- *Dlouhodobý přínos*:
    - Dovyvinutí systému ve spolupráci s ŘSD s promítnutím výsledků z testování na komunikacích D2/E50
    - Nasazení upraveného systému současně s přechodem na družicový výběr mýtného
- Plně spolehlivý systém využívající výhod GNSS signálu, který splňuje všechny bezpečností prvky pro spolehlivý výběr mýtných poplatků
- Možnost reálného testování pro odhalení aktuální situace v oblasti rušení GNSS signálu a návrh na rozmístění měřících stanovišť
- Modulovaný produkt podle specifických požadavků ŘSD

ŘSD tímto získá produkt, přesně podle svých specifických požadavků, který plně odpovídá podmínkám pro nasazení do ostrého provozu.

**O co chceme požádat ze strany ŘSD:**

- Určení skupiny pracovníků pro součinnost při implementaci produktu do testovacího provozu
    - Definování nejfrekventovanějších komunikací s největším množstvím projíždějících vozidel nad 3,5 t
    - Specifikování požadavků na produkt
    - Monitorování průběhu testovacího provozu a podíl na vyhodnocování výsledků
    - Specifikování následných požadavků na úpravu produktu
- Projekt máme financovaný ze strany Ministerstva vnitra, takže nyní máme zájem o spolupráci s ohledem na výše uvedenou součinnost – tedy není nutné vkládat žádné finanční prostředky ze strany ŘSD (vyjma nákladů spojených s činností vašich vlastních pracovníků)

Chtěli bychom Vás tímto požádat o možnost setkání, kde rádi odpovíme na případné technické dotazy.

# Příloha 2

# Návrh podkladů k druhému jednání ŘSD

Projekt: Systém pro odhalování nezákonného rušení GNSS signálu v blízkosti strategické infrastruktury

Projekt s názvem *Systém pro odhalování nezákonného rušení GNSS signálu v blízkosti strategické infrastruktury*, s pracovním názvem *Detektor,* je zpracováván v rámci Programu bezpečnostního výzkumu České republiky 2015-2020, vyhlášeným Ministerstvem Vnitra ČR. Na realizaci projektu spolupracuje ČVUT Fakulta elektrotechnická a Fakulta dopravní a GNSS Centre of Excellence. Cílem projektu je zvýšení ochrany kritické infrastruktury (nejen té kritické) využívající pro své klíčové funkce signálu GNSS před nezákonným rušením signálu prostřednictvím Jamming a Spoofing.

Výstupem projektu je funkční systém schopný detekce a přesné lokalizace zdroje rušení typu Jamming a Spoofing a zabraňující ovlivňování funkčnosti kritických aplikací využívajících signálu GNSS z pohledu časové synchronizace nebo funkce určení přesné pozice.

**Současný stav problému v ŘSD**

Nezákonné rušení GNSS signálu se v moderní společnosti stává běžným prvkem, ohrožujícím subjekty kritické infrastruktury. ŘSD jakožto organizace zajišťující provoz a výběr mýtných poplatků v ČR je nyní vystavena nové výzvě v podobě implementace nového systému výběru mýtného založeného na GNSS. Společnost CzechToll, která vyhrála tendr na provozovatele mýtného systému, přichází s technologií družicového mýtného systému, který bude v ČR implementován v kombinaci s mikrovlnnou technologií. S družicovým výběrem mýtného vzniká problém s úmyslným rušením GNSS signálu pomocí levně dostupných osobních rušiček PPD na palubách automobilů podléhajících mýtné povinnosti. Využití PPD je v současné době na vzestupu, jak dokazují i data získaná ze zahraničí. Mobilní jednotky využívané pro kontrolu dodržování mýtné povinnosti nejsou dostatečně vybaveny pro detekci všech aktuálních typů rušení GNSS signálu, a proto je v současné době jednoduché obejít platební povinnost a způsobit tak značné finanční škody.

**Rušení typu Jamming a vliv na systémy družicového výběru mýtného**

Typ rušení Jamming je elementární způsob rušení. Ovlivnění se projevuje oslabením nebo ztrátou GNSS signálu při příjmu koncovým přijímačem. Zdrojem Jamming jsou v první řadě

jednoduché osobní rušičky PPD, v druhé řadě sofistikovanější rušičky s možností řízení výkonu a s napájením z akumulátoru, tzn. výdrží až několik dní. Pro ŘSD se jako primární problém jeví zejména PPD, které jsou využívány řidiči automobilů. Při průjezdu virtuální mýtnou bránou rušička generuje šum na stejné frekvenci jako je vysílaný GNSS signál, palubní přijímač tak není schopen přijmout signál z družice a současně nevysílá ani informace o své poloze. Z toho plyne, že nelze ověřit a stanovit výši mýtného pro takto vybavené vozidlo. Mobilní jednotky využívané pro kontrolu dodržování mýtné povinnosti nejsou dostatečně vybaveny pro detekci všech aktuálních typů rušení GNSS signálu, a proto je v současné době jednoduché obejít platební povinnost a způsobit tak značné finanční škody.

**Parametry produktu Detektor a možný způsob implementace u ŘSD**

*Monitorování – Detekce – Rozpoznání typu rušení – Informování uživatele – Azimut – Poloha*

Detektor je inovativní modulární produkt, který kombinuje funkce detekce rušení typu Jamming a Spoofing, určení azimutu a přesné lokace zdroje rušení. Modularita umožňuje přizpůsobení produktu včetně HW a SW podle specifik konkrétního uživatele.

Pro potřeby ŘSD je navrhovaný produkt tvořen 2 měřícími stanovišti pracujícími na principu Software Defined Radio (SDR) s anténním blokem 4 samostatných zářičů typu J-Pole, umožňujících přizpůsobení vyzařovací charakteristiky. Navrhované rozmístění měřících stanovišť je 1x v každém směru, aby byla zajištěna obousměrná detekce na komunikace a umožněna schopnost detekovat azimut příchodu rušení. Citlivost měřící antény je stanovena dle ICAO limitu na – 120dBm. Měřící stanoviště jsou propojena pomocí optické kabeláže s centrálním zpracovatelským serverem, u prototypu je počítáno se vzdáleností cca 1,7 km, tuto vzdálenost lze prodloužit použitím jiného druhu kabeláže při zachování kvality i finančních nákladů. Detektor využívá triangulační metody zaměření zdroje rušivého signálu, s rozlišovací schopností měření azimutu +- 5° odpovídající šířce detekčního louče 10° celkem s 36 detekčními polohami v kružnici. Sběr signálu ze všech měřících stanovišť probíhá kontinuálně, data jsou přenášena do zpracovatelského serveru, kde jsou vyhodnocovány signály 4 x 2 stanovišť, což umožňuje matematické a fyzikální porovnání signálů z jednotlivých antén mezi sebou. Grafické uživatelské rozhraní (GUI) lze upravit na základě požadavků ŘSD a doplnit základní nastavení o zobrazení požadovaných parametrů.

**Testování na konkrétním úseku zpoplatněné komunikace**

Na základě stanovení konkrétních požadavků na produkt ze strany ŘSD bude připraven prototyp pro reálné testování v provozu na vybraném úseku komunikace. Pro tento účel se jeví jako vhodné lokace úseky dálnice D2 a silnice E50 při Slovenské hranici. Dlouhodobý sběr dat bude probíhat po dobu 6–12 měsíců, současně bude probíhat evaluace. Na základě výsledků je možná následná úprava konečného produktu a jeho budoucí nasazení do reálného provozu. Jelikož v současné době funguje výběr mýtného na mikrovlnné technologii, máme zatím možnost výše zmíněného testování na hranici se Slovenskem, kde je družicový výběr mýtného již implementován. Na základě výsledků získáme data pro další možné modifikace dle aktuální situace, při reálném přechodu na družicovou technologii bude již nasazen upravený systém.

Výsledkem bude produkt spojující reálné technické parametry a požadavky konečného uživatele.

**Standard reportingu událostí**

Detektor kontinuálně provádí sběr dat, která předává do zpracovatelského serveru. Data jsou vyhodnocována na základě stanovených algoritmů a prostřednictvím reportu předávána uživateli.

Návrh standardu reportingu v čase může být následující:

1) V reálném čase
2) Periodicky – podle definovaných intervalů
3) 1 x za měsíc

Obsah reportu může být následující:

1) Povinný – ID události, typ události, typ zařízení, frekvenční pásmo rušení (GPS/Galileo), azimut, lokalita rušením, datum a čas události v UTC,
2) Nepovinný – začátek události, trvání, ztráta signálu GNSS (ano; ne), rozsah rušícího signálu, přístup k surovým datům, referenční hodnota šumu pro snímač, maximální intenzita v dB nad minimální prahovou hodnotou zařízení.

**Co bude přínosem pro ŘSD:**

- *Krátkodobý (momentální) přínos:*
    - Možnost aktuálního testování na hranici se Slovenskem na dálnici D2 a silnici E50.
- *Dlouhodobý přínos:*
    - Dovyvinutí systému ve spolupráci s ŘSD s promítnutím výsledků z testování na komunikacích D2/E50
    - Nasazení upraveného systému současně s přechodem na družicový výběr mýtného
- Plně spolehlivý systém využívající výhod GNSS signálu, který splňuje všechny bezpečností prvky pro spolehlivý výběr mýtných poplatků
- Možnost reálného testování pro odhalení aktuální situace v oblasti rušení GNSS signálu a návrh na rozmístění měřících stanovišť
- Modulovaný produkt podle specifických požadavků ŘSD

**O co chceme požádat ze strany ŘSD**

- Určení pracovní skupiny, zapojující se do vývoje produktu a testovacího provozu
    - Zahájení diskuze pro specifikování požadavků na produkt, včetně HW/SW + GUI
    - Definování nejfrekventovanějších komunikací s největším množstvím projíždějících vozidel nad 3,5 t a určení testované komunikace
    - Monitorování v průběhu testování a vyhodnocování výsledků – stanovení konečných požadavků ve spolupráci s vývojovým týmem

Chtěli bychom Vás tímto požádat o možnost setkání, kde rádi odpovíme na konkrétní technické dotazy a detailně prodiskutujeme strukturu produktu.

# Příloha 3

# Podklady k prvnímu jednání Provozovatelé lokálních letišť

Projekt: Systém pro odhalování nezákonného rušení GNSS signálu v blízkosti strategické infrastruktury

Projekt s názvem *Systém pro odhalování nezákonného rušení GNSS signálu v blízkosti strategické infrastruktury*, s pracovním názvem *Detektor,* je zpracováván v rámci Programu bezpečnostního výzkumu České republiky 2015-2020, vyhlášeným Ministerstvem Vnitra ČR. Na realizaci projektu spolupracuje ČVUT Fakulta elektrotechnická a Fakulta dopravní a GNSS Centre of Excellence. Cílem projektu je zvýšení ochrany kritické infrastruktury (nejen té kritické) využívající pro své klíčové funkce signálu GNSS před nezákonným rušením signálu prostřednictvím Jamming a Spoofing.

Výstupem projektu je funkční systém schopný detekce a přesné lokalizace zdroje rušení typu Jamming a Spoofing a zabraňující ovlivňování funkčnosti kritických aplikací využívajících signálu GNSS z pohledu časové synchronizace, nebo funkce určení přesné pozice.

**Současný stav problému**

S rozmachem využití GNSS dochází i k častějšímu výskytu nezákonného rušení signálu, ať už úmyslně (způsobení finančních škod nebo ochromení infrastruktury) nebo neúmyslně využíváním osobních rušiček k jinému účelu, ovšem ovlivňujících i jiné subjekty. Trendem v rozvoji letišť je publikace LPV postupů, bez zálohy tradičních radionavigačních zařízení, které skýtají vysoké náklady na vybudování infrastruktury a následnou údržbu. Publikace LPV umožňuje snížení minimální výšky rozhodnutí DH na 250 ft, publikace LPV-200 až na 200 ft, odpovídající ILS Cat 1. LPV letiště se mohou snadno stát terčem útoku v podobě úmyslného rušení s cílem dlouhodobě degradovat provoz na provoz dle postupů VFR nebo pomocí osobních rušiček PPD dočasně ovlivnit integritu a dostupnost GNSS signálu.

**Popis navrhovaného řešení**

Detektor přichází s inovačním řešením kombinujícím schopnost detekce rušení typu Jamming a Spoofing, určení azimutu a přesné lokace zdroje rušení. Takový produkt dosud na trhu není dostupný, ale z pohledu ochrany (kritické) infrastruktury je zcela žádoucí.

Detektor je již od prvního návrhu vyvíjen modulárně, a tudíž umožňuje přizpůsobení specifickým požadavkům pro různé subjekty (kritické) infrastruktury. Zařízení je postaveno jako distribuovaný systém skládající se z 1 až 3 měřících stanovišť pracujících na principu Software Defined Radio (SDR) z důvodu velké flexibility umožňující aplikaci nových metodik detekce rušení. Použitý anténní blok se skládá ze 4 samostatných anténních zářičů.

**Systém umožňuje:**

- Monitorování, detekci a rozpoznání typu rušení GNSS signálu
- Okamžité informování uživatele o případné nespolehlivosti nebo nedostupnosti GNSS signálu
- Určení směru a přesné polohy zdroje rušení

Rádi bychom Vás požádali o spolupráci při řešení projektu, zejména s ohledem na definování technických požadavků a potřeb ze strany provozovatelů letišť. A to zejména z důvodu posílení ochrany subjektu proti hrozbám způsobujícím snížení provozuschopnosti a bezpečnosti leteckého provozu s vlivem nejen na provozovatele letiště, ale především jeho uživatele. První funkční vzorek bude dostupný začátkem léta 2018, s tím přichází i možnost aktivního testování v reálném provozu. Reálným testováním v leteckém provozu získáme data pro navržení optimálního rozmístění měřících stanic na daném letišti, také v závislosti na rozmístění pozemní infrastruktury, kde mohou být projíždějící vozidla zdrojem rušení. V průběhu testování lze vytvářet různé potenciální scénáře rušení a následně po analýze a vzájemné konzultaci výsledků je možné produkt přizpůsobit přesně podle potřeb daného letiště.

**Co bude přínosem pro provozovatele letiště:**

- Plně spolehlivý systém využívající GNSS signál, který splňuje všechny bezpečností prvky bez možnosti úmyslného ohrožení
- Možnost reálného testování odhalujícího kritická místa a návrhy na rozmístění měřících stanovišť
- Modulovaný produkt podle specifických požadavků v závislosti na situaci letiště

Provozovatel letiště tímto získá produkt, přesně podle svých specifických požadavků, plně splňující podmínky pro nasazení do ostrého provozu.

**O co chceme požádat ze strany provozovatele letiště:**

- Určení skupiny pracovníků pro součinnost při implementaci produktu do testovacího provozu
    - Definování možných kritických míst (přilehlé silnice atd.)
    - Specifikování požadavků na produkt
    - Monitorování průběhu testovacího provozu a podíl na vyhodnocování výsledků
    - Specifikování následných požadavků na úpravu produktu
- Projekt máme financovaný ze strany Ministerstva vnitra, takže nyní máme zájem o spolupráci s ohledem na výše uvedenou součinnost – tedy není nutné vkládat žádné finanční prostředky ze strany ČEPS (vyjma nákladů spojených s činnostní vašich vlastních pracovníků)

Chtěli bychom Vás tímto požádat o možnost setkání, kde rádi odpovíme na případné technické dotazy.

# Příloha 4

# Podklady k prvnímu jednání ČEPS


## Projekt: Systém pro odhalování nezákonného rušení GNSS signálu v blízkosti strategické infrastruktury

Projekt s názvem *Systém pro odhalování nezákonného rušení GNSS signálu v blízkosti strategické infrastruktury*, s pracovním názvem *Detektor* je zpracováván v rámci Programu bezpečnostního výzkumu České republiky 2015-2020, vyhlášeným Ministerstvem Vnitra ČR. NA realizaci projektu spolupracuje ČVUT Fakulta elektrotechnická a Fakulta dopravní a GNSS Centre of Excellence. Cílem projektu je zvýšení ochrany infrastruktury (nejen té kritické) využívající pro své klíčové funkce signálu GNSS před nezákonným rušením signálu prostřednictvím Jamming a Spoofing.

Výstupem projektu je funkční systém schopný detekce a přesné lokalizace zdroje rušení typu Jamming a Spoofing a zabraňující ovlivňování funkčnosti (kritických) aplikací využívajících signálu GNSS z pohledu časové synchronizace nebo funkce určení přesné pozice.

### Současný stav problému

S rozmachem využití GNSS dochází i k častějšímu výskytu nezákonného rušení signálu ať už úmyslně (způsobení finančních škod nebo ochromení infrastruktury) nebo neúmyslně využíváním osobních rušiček k jinému účelu, ovšem ovlivňujících i jiné subjekty. Společnost ČEPS, a.s. využívající GNSS signál k časové synchronizaci systému pro zjišťování fázových poměrů mezi uzly přenosové soustavy se může lehce stát terčem útoku rušením GNSS. Pro zamezení vzniku finančních škod a nehod, které už v zahraničí vedly až k black-outu, je třeba dostatečné ochrany proti těmto rozrůstajícím se typům rušení.

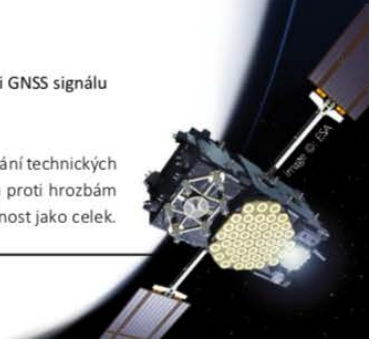
### Popis navrhovaného řešení

Detektor přichází s inovačním řešením kombinujícím schopnost detekce rušení typu Jamming a Spoofing, určení azimutu a přesné lokace zdroje rušení. Takový produkt dosud na trhu není dostupný, ale z pohledu ochrany (kritické) infrastruktury je zcela žádoucí. Detektor je již od prvního návrhu vyvíjen modulárně, a tudíž umožňuje přizpůsobení specifickým požadavkům pro různé subjekty (kritické) infrastruktury. Zařízení je postaveno jako distribuovaný systém skládající se z 1 až 3 měřících stanovišť pracujících na principu Software Defined Radio (SDR) z důvodu velké flexibility umožňující aplikaci nových metodik detekce rušení. Použitý anténní blok se skládá ze 4 samostatných anténních zářičů.

### Systém umožňuje:

- **Monitorování, detekci a rozpoznání typu rušení GNSS signálu**
- **Okamžité informování uživatele o případné nespolehlivosti nebo nedostupnosti GNSS signálu**
- **Určení směru a přesné polohy zdroje rušení**

Rádi bychom Vás požádali o spolupráci při řešení projektu, zejména s ohledem na definování technických požadavků a potřeb ze strany ČEPS. A to především z důvodu posílení ochrany subjektu proti hrozbám způsobujícím snížení provozuschopnosti s možným dopadem nejen na ČEPS, ale i společnost jako celek.




GNSS Centre of Excellence z.s.p.o.
Navigační 787, 252 61 Jeneč, Česká republika; IČO: 01269313
e-mail: info@gnss-centre.cz; WEB: www.gnss-centre.cz

První funkční vzorek bude dostupný začátkem léta 2018. S tím přichází i možnost aktivního testování v reálném provozu. Reálným testováním v prostředí společnosti ČEPS, resp. na vybraném místě uzlu distribuční soustavy, získáme data pro navržení optimálního rozmístění měřících stanic. Lze vytvářet různé potenciální scénáře rušení a následně po analýze a vzájemné konzultaci výsledků, modulovat produkt přesně podle potřeb společnosti.

## Co bude přínosem pro ČEPS:

- Plně spolehlivý systém využívající výhod GNSS signálu, který splňuje všechny bezpečnostní prvky bez možnosti úmyslného ohrožení
- Možnost reálného testování, odhalující kritická místa a návrhy na rozmístění měřících stanovišť
- Modulovaný produkt podle specifických požadavků ČEPS

ČEPS tímto získá produkt, přesně podle svých specifických požadavků, který plně vyhovuje podmínkám pro nasazení do ostrého provozu.

## O co chceme požádat ze strany ČEPS:

- Určení skupiny pracovníků pro součinnost při implementaci produktu do testovacího provozu
  - Definování možných kritických míst
  - Specifikování požadavků na produkt
  - Monitorování průběhu testovacího provozu a podíl na vyhodnocování výsledků
  - Specifikování následných požadavků na úpravu produktu
- Projekt máme financován ze strany Ministerstva vnitra, takže není máme zájem o spolupráce s ohledem na výše uvedenou součinnost – tedy není nutné vkládat žádané finanční prostředky ze strany ČEPS (vyjma nákladů spojených s činností vašich vlastních pracovníků)

Chtěl bych Vás tímto požádat o možnost setkání, kde rádi odpovíme na případné technické dotazy.

Předem děkuji a s pozdravem,

[redacted]

Web: www.gnss-centre.cz

GNSS Centre of Excellence z.s.p.o.
Navigační 787, 252 61 Jeneč, Česká republika; IČO: 01269313
e-mail: info@gnss-centre.cz; WEB: www.gnss-centre.cz

# Příloha 5

# Podklady k prvnímu jednání ČEZ


## Projekt: Systém pro odhalování nezákonného rušení GNSS signálu v blízkosti strategické infrastruktury

Projekt s názvem *Systém pro odhalování nezákonného rušení GNSS signálu v blízkosti strategické infrastruktury*, s pracovním názvem *Detektor* je zpracováván v rámci Programu bezpečnostního výzkumu České republiky 2015-2020, vyhlášeným Ministerstvem Vnitra ČR. NA realizaci projektu spolupracuje ČVUT Fakulta elektrotechnická a Fakulta dopravní a GNSS Centre of Excellence. Cílem projektu je zvýšení ochrany infrastruktury (nejen té kritické) využívající pro své klíčové funkce signálu GNSS před nezákonným rušením signálu prostřednictvím Jamming a Spoofing.

Výstupem projektu je funkční systém schopný detekce a přesné lokalizace zdroje rušení typu Jamming a Spoofing a zabraňující ovlivňování funkčnosti (kritických) aplikací využívajících signálu GNSS z pohledu časové synchronizace nebo funkce určení přesné pozice.

### Současný stav problému

S rozmachem využití GNSS dochází i k častějšímu výskytu nezákonného rušení signálu ať už úmyslně (způsobení finančních škod nebo ochromení infrastruktury) nebo neúmyslně využíváním osobních rušiček k jinému účelu, ovšem ovlivňujících i jiné subjekty. Společnost ČEZ distribuce využívající GNSS signál k časové synchronizaci systému pro zjišťování fázových poměrů mezi uzly distribuční sítě, se může lehce stát terčem útoku rušením GNSS. Pro zamezení vzniku finančních škod a nehod, které už v zahraničí vedly až k black-outu, je třeba dostatečné ochrany proti těmto rozrůstajícím se typům rušení.

### Popis navrhovaného řešení

Detektor přichází s inovačním řešením kombinujícím schopnost detekce rušení typu Jamming a Spoofing, určení azimutu a přesné lokace zdroje rušení. Takový produkt dosud na trhu není dostupný, ale z pohledu ochrany (kritické) infrastruktury je zcela žádoucí. Detektor je již od prvního návrhu vyvíjen modulárně, a tudíž umožňuje přizpůsobení specifickým požadavkům pro různé subjekty (kritické) infrastruktury. Zařízení je postaveno jako distribuovaný systém skládající se z 1 až 3 měřících stanovišť pracujících na principu Software Defined Radio (SDR) z důvodu velké flexibility umožňující aplikaci nových metodik detekce rušení. Použitý anténní blok se skládá ze 4 samostatných anténních zářičů.

### Systém umožňuje:

- **Monitorování, detekci a rozpoznání typu rušení GNSS signálu**
- **Okamžité informování uživatele o případné nespolehlivosti nebo nedostupnosti GNSS signálu**
- **Určení směru a přesné polohy zdroje rušení**

Rádi bychom Vás požádali o spolupráci při řešení projektu, zejména s ohledem na definování technických požadavků a potřeb ze strany ČEZ distribuce. A to především z důvodu posílení ochrany subjektu proti hrozbám způsobujícím snížení provozuschopnosti s možným dopadem nejen na ČEZ, ale i společnost jako

GNSS Centre of Excellence z.s.p.o.
Navigační 787, 252 61 Jeneč, Česká republika; IČO: 01269313
e-mail: info@gnss-centre.cz; WEB: www.gnss-centre.cz

celek. První funkční vzorek bude dostupný začátkem léta 2018. S tím přichází i možnost aktivního testování v reálném provozu. Reálným testováním v prostředí společností ČEZ, resp. na vybraném místě uzlu distribuční soustavy, získáme data pro navržení optimálního rozmístění měřících stanic. Lze vytvářet různé potenciální scénáře rušení a následně po analýze a vzájemné konzultaci výsledků, modulovat produkt přesně podle potřeb společnosti.

## Co bude přínosem pro ČEZ:

- Plně spolehlivý systém využívající výhod GNSS signálu, který splňuje všechny bezpečnostní prvky bez možnosti úmyslného ohrožení
- Možnost reálného testování, odhalující kritická místa a návrhy na rozmístění měřících stanovišť
- Modulovaný produkt podle specifických požadavků ČEZ

ČEZ tímto získá produkt, přesně podle svých specifických požadavků, který plně vyhovuje podmínkám pro nasazení do ostrého provozu.

## O co chceme požádat ze strany ČEZ:

- Určení skupiny pracovníků pro součinnost při implementaci produktu do testovacího provozu
  - Definování možných kritických míst
  - Specifikování požadavků na produkt
  - Monitorování průběhu testovacího provozu a podíl na vyhodnocování výsledků
  - Specifikování následných požadavků na úpravu produktu
- Projekt máme financován ze strany Ministerstva vnitra, takže není máme zájem o spolupráce s ohledem na výše uvedenou součinnost – tedy není nutné vkládat žádané finanční prostředky ze strany ČEZ distribuce (vyjma nákladů spojených s činností vašich vlastních pracovníků)

Chtěl bych Vás tímto požádat o možnost setkání, kde rádi odpovíme na případné technické dotazy.

Předem děkuji a s pozdravem,

[redacted]

Web: www.gnss-centre.cz

GNSS Centre of Excellence z.s.p.o.
Navigační 787, 252 61 Jeneč, Česká republika; IČO: 01269313
e-mail: info@gnss-centre.cz; WEB: www.gnss-centre.cz