MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

CGI

Experience the commitment®

Certifikovaná metodika

Metodika testování GNSS přijímačů proti jammingu

Evidenční číslo projektu: VH20162017007

Název projektu: Kategorizace hrozeb otevřené službě systému Galileo a opatření k jejich zmírnění

Zpracovatel: CGI IT Czech Republic s.r.o.

Metodika testování GNSS přijímačů proti jammingu

Vypracováno dle smlouvy

o poskytnutí účelové podpory na řešení projektu výzkumu, vývoje a inovací s názvem

Kategorizace hrozeb otevřené službě systému Galileo a opatření k jejich zmírnění

kód projektu VH20162017007

uzavřené mezi smluvními stranami

Česká republika – Ministerstvo vnitra

IČ: 00007064

se sídlem Nad Štolou 936/3, 170 34 Praha 7

zastoupená ředitelem odboru bezpečnostního výzkumu a vzdělávání

JUDr. Petrem Novákem, Ph.D.

dále jen „Objednatel“

a

CGI IT Czech Republic s.r.o.

IČ: 62412388

se sídlem Laurinova 2800/4, Praha 5 – Stodůlky, 155 00

zastoupená statutárním zástupcem Ing. Pavlem Malínkem

dále jen „Zpracovatel“.

Obsah

Zkratky

Zkratka	Význam
p.a.	Per annum, ročně
BeiDou	Čínský GNSS
BW	Bandwidth, šířka pásma
C/A	Coarse Acquisition, jeden ze signálů systému GPS
CDDS	Commercial Data Distribution System,Komerční systém pro distribuci dat
CDMA	Code division multiple access, metoda využívaná komunikačními systémy
CN0	Carrier to Noise Density, poměr mezi sílou signálu z družice (na nosné vlně) a hladinou šumu v daném frekvenčním pásmu (hustota šumu)
CPA	Competent PRS Authority, kompetentní autorita PRS
CPF	Central Processing Facility, centrální zařízení pro zpracování naměřených dat
CRPA	Controlled Radiation Pattern Antenna, vyvíjená anténa s ochranou proti jammingu
CSAC	Chip Scale Atomic Clocks, atomové hodiny
ČTÚ	Český telekomunikační úřad
DDC	Delay, Diversion and Cancellation, zpoždění, odklon a zrušení letu
DGPS	Differential Global Positioning System, diferenciální GPS
DHS	Department of Homeland Security, americké ministerstvo vnitřní bezpečnosti
DOP	Dilution Of Precision, parametr přesnosti udávající vliv geometrie prostorového uspořádání družic GNSS a přijímače v konkrétní epoše na přesnost určení polohy
EDAS	EGNOS Data Access Server, komerční služba šířící data EGNOS
EGNOS	European Geostationary Navigation Overlay Service, evropský SBAS
EK	Evropská komise
ESA	European Space Agency, Evropská kosmická agentura
EU	Evropská unie
FDD	Frequency Division Duplex, rozdělení komunikačních linků na frekvenční sloty
GAGAN	GPS and GEO Augmentation Navigation, indický SBAS
Galileo	Evropský GNSS
GBAS	Ground Based Augmentation System, pozemní augmentační systém
GIMOS	GNSS Interference Monitoring System, systém pro monitoring interference GNSS
GLONASS	Ruský GNSS
GNSS	Global Navigation Satellite System, globální satelitní navigační systém

GPS	Global Positioning Service, americký GNSS
GSA	European GNSS Agency, Evropská agentura pro GNSS
GSM	Global System for Mobile Communications, mobilní síť
HDP	Hrubý domácí produkt
HW	Hardware
I/Q	Způsob reprezentace signálu v ICT
ICAO	International Civil Aviation Organization, Mezinárodní organizace pro civilní letectví
ICT	Information and communications technology, informační a komunikační technologie
IMU/IMS	Inertial Measurement Unit / System, inerciální měřící jednotka/systém
ITS	Intelligent Transportation System, inteligentní dopravní systém
J/N	Jamming-to-Noise, metoda pro sledování síly interference
JLOC	Jammer Detection and Location System, systém pro detekci a lokalizaci rušiček
KI	Kritická infrastruktura
KPI	Key Performance Indicators, klíčové ukazovatele výkonnosti
L1	Signál systému Galileo na frekvenci 1575,42 MHz
LBS	Location Based Services
LTE	Long Term Evolution, standard pro vysokorychlostní bezdrátovou komunikaci
MSAS	Multi-functional Satellite Augmentation System, japonská SBAS
NMEA	National Marine Electronics Association, Národní sdružení pro lodní elektroniku
NTP	Network Time Protocol, protokol pro synchronizaci vnitřních hodin počítačů
OBU	On-Board Unit, palubní jednotka
OCXO	Temperature Controlled Crystal Oscillator, oscilátor
OS	Open Service, otevřená služba
PP	Power Profile, profil síly signálu
PNT	Positioning, Navigation, Timing, poloha, rychlost (navigace), čas
PPD	Personal Privacy Device, zařízení pro ochranu soukromí (rušička / jammer)
PRN	Pseudo Random Noise, pseudonáhodný šum
PRS	Public Regulated Service, veřejná regulovaná služba
PTP	Precision Time Protocol, protokol pro synchronizaci času
RAIM	Receiver Autonomous Integrity Monitoring, autonomní monitorování integrity

RF	Radio-frequency, radiofrekvenční
RFI	Radio-frequency Interference, radiofrekvenční interference
RIMS	Ranging Integrity Monitoring Stations, pozemní stanice systému EGNOS
RFCS	Radio Frequency Constellation Simulator, simulátor radiofrekvenčních konstelací
RTK	Real Time Kinematics, metoda měření pomocí GNSS
SACCSA	Sulución de Augmentación para Caribe, Centro y Sudamérica, SBAS států střední a jižní Ameriky
SATCOM	Satellite Communication, satelitní komunikace
SBAS	Satellite-Based Augmentation System, satelitní augmentační systém
SDCM	System for Differential Corrections and Monitoring, ruský SBAS
SDD	Service Definition Document, dokument týkající se systému pro podporu SoL aplikací na bázi EGNOS
SDR	Software Defined Radio, softwarové rádio
SNAS	Satellite Navigation Augmentation System, čínský SBAS
SNR	Signal To Noise Ratio, poměr signálu a šumu na pozadí
SoL	Safety of Life Service, služba kritická z hlediska bezpečnosti
SPS	Standard Positioning Service, standardní (otevřená) služba GPS
SV	Space Vehicle, družice
SVN	Satellite Vehicle Number, zkratka využívaná pro označení satelitů GPS
SW	Software
QZSS	Quasi-Zenith Satellite System, japonský regionální satelitní navigační systém
T&S	Timing and Synchronisation, časování a synchronizace
TDD	Time Division Duplex, rozdělení komunikačních linků na časové sloty
TTFF	The Time to First Fix, čas od spuštění přijímače do prvního určení polohy
USA	United States of America, Spojené státy americké
VSG	Vector Signal Generator, generátor signálů vektoru
WAAS	Wide Area Augmentation System, americký SBAS
WADGS	Wide Area Differential Global Positioning System, jihokorejský SBAS
WWVB	Rádio stanice pro synchronizaci času (Colorado, USA)

Seznam obrázků

Seznam tabulek

1 Úvod

Globální navigační satelitní systémy (GNSS) mají v současnosti prioritní postavení v mnohých oblastech lidské činnosti. Postupem času nahradily a v některých oblastech úplně vytlačily původní technologie, přičemž uplatnění GNSS se neustále rozšiřuje do nových oblastí společnosti a v těch stávajících posiluje svoje uplatnění.

GNSS je infrastruktura, která umožňuje uživatelům s kompatibilním zařízením zjišťovat jejich pozici, rychlost a přesný čas (Positioning, Navigation, Timing – PNT) pomocí zpracování signálů ze satelitů na oběžné dráze Země. Signály GNSS jsou poskytovány různými satelitními navigačními systémy včetně globálních konstelací a satelitních augmentačních systémů (Satellite-Based Augmentation Systems – SBAS) [1].

GNSS jsou používány mnoha typy aplikací, pokrývajícími masový trh včetně profesionálních a bezpečnostně-kritických aplikací, z nichž každá vyžaduje různou úroveň služeb. Mezi **důležité aspekty služeb GNSS všeobecně patří** (v závislosti na potřebách uživatelů):

- **dostupnost** – procento času, kdy je viditelný minimální počet satelitů potřebný pro získání informace o poloze, rychlosti nebo času,
- **přesnost** – rozdíl mezi skutečnou a vypočítanou pozicí (absolutní polohování),
- **spojitost** – schopnost poskytovat požadované výkony v průběhu operací bez výpadků od započetí operace,
- **integrita** – další informace pro uživatele o spolehlivosti signálu v rámci provozních požadavků,
- **odolnost** vůči spoofingu a jammingu – autentizační informace poskytované uživatelům pro ujištění, že signál přichází ze satelitů na oběžné dráze,
- **penetrace** do vnitřních prostor – schopnost signálu proniknout dovnitř budov [1].

Dostupnost technologie GNSS stále narůstá a spolu s tím roste i počet aplikací, které tuto technologii využívají. GNSS se staly dominantní technologií v oblasti určování polohy a času, používají se ve všech druzích dopravy a hrají rozhodující úlohu v oblasti telekomunikací, zeměměřičství, financí a energetiky. Přitom velká část těchto aplikací nemá žádné záložní řešení pro případ, kdy se GNSS stane nedostupné nebo nedůvěryhodné, ať už v důsledku zamýšleného útoku nebo nezáměrně škodlivým vlivem vnějšího prostředí. Z tohoto důvodu je třeba věnovat pozornost hrozbám, které mohou tento systém narušit, a vypracovat záložní řešení.

Signály GNSS jsou velmi slabé, a tím i náchylné na rušení. Přítomnost rušení může způsobit potíže při sledování družic, určování polohy a v nejhorším případě úplný výpadek služby.

Existuje mnoho potenciálních zdrojů rušení. Jejich základní dělení je na rušení neúmyslné a úmyslné.

Neúmyslným rušením se rozumí nechtěný zásah do signálů GNSS, který přesto způsobuje problémy a snižuje nebo úplně znemožňuje schopnost přijímat signály GNSS. Může sem patřit rušení způsobené přirozenými jevy (např. průchodem signálu atmosférou) nebo člověkem (např. chybné nebo nesprávně nastavení elektrického zařízení).

Úmyslné rušení má za cíl vědomé a cílené zhoršování nebo přerušení činnosti konkrétního GNSS přijímače nebo celé infrastruktury v určité oblasti. Zařazujeme sem jamming, spoofing a meaconing, přičemž je třeba poznamenat, že záměrné rušení proti konkrétnímu cíli může mít následky i na jiných zařízeních v okolí, která využívají signály GNSS.

Uživatel signálů GNSS může být ovlivněn různými způsoby rušení v závislosti na povaze rušení a jeho síle. Na úrovni přijímače může dojít k nárůstu polohové a časové nepřesnosti snížením počtu viditelných družic nebo zhoršením kvality přijímaného signálu. Na úrovni služeb může být dopad rušení, v závislosti na charakteru dané aplikace, velmi rozdílný – od malého vlivu na provoz dané služby až po ohrožení kritické infrastruktury a bezpečnosti.

Pozornost je nutné věnovat především **kritické infrastruktuře**. V jednotlivých státech se přesné definice kritické infrastruktury liší, i když oblasti, které definice zahrnují, se překrývají. Mezi prvky kritické infrastruktury se zpravidla zařazuje elektronická komunikace, energetika, doprava, zásobování vodou či finanční sektor. Mnohé prvky kritické infrastruktury jsou částečně a některé plně závislé na GNSS, což v případě nedostupnosti této služby představuje významnou hrozbu. Míra závažnosti dopadů je potom závislá na existujících záložních řešeních při ztrátě GNSS.

Americká vláda, konkrétně Ministerstvo vnitřní bezpečnosti uvádí, že 13 z 16 oblastí kritické infrastruktury v USA je kriticky závislých na PNT, jehož zdrojem je GPS, a další tři mají určitou míru závislosti. Konstelace GPS však sama o sobě není považována za kritickou infrastrukturu.

Evropská komise odhadla, že 6 – 7 % HDP západních zemí, což představuje 800 miliard € v EU, je již závislých na satelitní radiové navigaci. Takové rozšíření používání dat odvozených od GNSS v rámci našich ekonomik znamená, že bezpečné poskytování PNT dat je nyní otázkou národní bezpečnosti, stejně jako hlavním ekonomickým aktivem [2].

Otevřené služby (např. Galileo Open Service, GPS SPS a další) poskytují volně dostupné signály, které v současné době nejsou chráněné šifrováním. Avšak ani šifrování neochrání signály před rušením, pokud se jedná o silný zdroj rušení, může ale zabránit manipulací se signály. V konečném důsledku jsou aplikace, které tyto signály využívají, stále náchylnější ke zneužití. Přičemž počet evidovaných hrozeb neustále narůstá.

Přestože systém Galileo ještě není plně využíván, můžeme čerpat z analogií a zkušeností s používáním systému GPS. Signály obou těchto otevřených služeb GNSS jsou si velmi podobné a dopad hrozeb bude tím pádem prakticky shodný. S nárůstem aplikací využívajících systémy GNSS, které na ně spoléhají bez implementace záložního řešení, se hrozby stávají o to závažnější.

V současné době **neexistuje dostatečná informovanost v oblasti hrozeb GNSS** a dalo by se říci, že jejich znalost je jak na straně uživatelů, tak na straně autorit, stále relativně nízká. Zároveň **neexistuje žádný společný postup pro monitoring a vedení databáze incidentů a především jejich dopadů**.

Pro zabezpečení GNSS je třeba vytvořit společný standard pro monitorování a ohlašování hrozeb GNSS a **standard pro hodnocení výkonnosti GNSS přijímačů a aplikací vůči hrozbám**, jako je např. rušení signálu. Právě druhému kroku se věnuje tato metodika.

Hodnocení výkonnosti přijímačů je prováděno pomocí **testování**, kdy jsou nasimulované nebo zachycené hrozby přehrány přijímači v laboratorním prostředí a sleduje se jeho reakce. Nad to je také možné pomocí testování vyhodnotit závažnost jednotlivých hrozeb. Testování by proto mělo být jedno ze základních opatření proti hrozbám GNSS systémů, aby uživatelé znali svá rizika a mohli implementovat případná další opatření a záložní systémy.

V ideálním případě by měli testování zařídit již samotní výrobci zařízení, nicméně v praxi si často testování objednávají až koncoví uživatelé nebo provozovatelé jejich systémů. Díky tomu je možné otestovat také konkrétní instalaci zařízení, integraci s dalšími systémy od různých výrobců a současně zohlednit další potřeby konkrétního uživatele, např. scénáře, ve kterých se zařízení nejčastěji používá.

2 Předmět metodiky

2.1 Obecné

2.1.1 Dedikace

Tato metodika byla vypracována v rámci smlouvy o poskytnutí účelové podpory na řešení projektu výzkumu, vývoje a inovací s názvem *Kategorizace hrozeb otevřené službě systému Galileo a opatření k jejich zmírnění (kód projektu VH20162017007).*

2.1.2 Oponentura

Tato metodika byla oponována 2 odborníky z akademické a státní sféry.

2.2 Vlastní předmět metodiky

Metodika je zaměřená na specifikaci předpokladů a podmínek, které je nutné zajistit při testování přijímačů GNSS pod vlivem záměrně škodlivé radiofrekvenční interference. Toto rušení se nejčastěji označuje jako jamming. Metodika obsahuje jak všeobecný popis prvků architektury, tak i návrh parametrů, metod testování a výběru hrozeb.

Metodika se věnuje zejména následujícím klíčovým oblastem:

- cíl a podstata metodiky,
- srovnání novosti postupů,
- popis uplatnění certifikované metodiky,
- **vlastní popis metodiky,**
- ekonomické aspekty,
- seznam použité související literatury a studií.

Vlastní popis metodiky se skládá z několika částí, a to:

- architektury testů, popisu parametrů a prvků testování,
- testovacích metod,
- výběru hrozeb,
- analýzy výsledků testování.

Součástí vlastního popisu je také analýza hrozeb a dalších opatření pro zamezení jammingu.

3 Cíl metodiky

V současnosti neexistuje v České republice ani na mezinárodní úrovni metodika popisující testování přijímačů GNSS. Sice vznikly ze strany EK a ESA nebo jednotlivých států různé iniciativy se zaměřením na jamming, avšak byly zaměřeny především na monitorování a detekci případů interference. Proto v současnosti není dostupná široce akceptovaná metodika testování přijímačů, která by byla využívána praxi.

V posledních letech se objevuje stále více aplikací, které využívají informaci o poloze nebo času odvozené ze systémů GNSS, čímž vzniká stále větší závislost na těchto systémech. Mezi tyto aplikace se také řadí aplikace zajišťující chod kritické infrastruktury. Zároveň u většiny aplikací neexistuje záložní řešení pro případ, že dojde k výpadku služby GNSS. Dnes nejčastějším důvodem pro ztrátu příjmu signálu GNSS je škodlivá interference neboli jamming. Uživatelé často neznají dopady jammingu na své systémy a přijímače, které tyto systémy využívají. Znalost závislosti vlastních systémů na GNSS a jejich schopnosti vypořádat se s rušením signálu GNSS je pro zajištění provozu těchto systémů kritická. Proto je důležité vědět, jak tyto přijímače otestovat a tím stanovit míru dopadu na chod konkrétní aplikace.

V současné době chybí mezi uživateli a správci systémů GNSS obecné povědomí o:

- hrozbách a přítomnosti škodlivé interference,
- míře závislosti systémů a služeb na signálech GNSS,
- ekonomických dopadech výpadku GNSS,
- schopnostech vlastních systémů,
- metodice testování přijímačů,
- možných legislativních a technických opatřeních.

Tato metodika se bude věnovat alespoň ve stručnosti všem těmto tématům, nicméně hlavní pozornost je věnována samotné metodice testování.

Hlavním cílem tohoto dokumentu je popsat principy testování přijímačů pod vlivem jammingu. Metodika testování poskytne uživatelům systémů GNSS doporučený postup nastavení architektury a zvolení jednotlivých parametrů testování, sestavení testovacích scénářů, výběru hrozeb, výběru veličin pro sledování výkonu přijímače a analýzy výsledků.

Metodika je primárně určena orgánům státní správy, především Ministerstvu dopravy, Ministerstvu vnitra, Národnímu bezpečnostnímu úřadu resp. Národnímu úřadu pro kybernetickou a informační bezpečnost. Dále je předpokládáno využití metodiky správci systémů využívajících GNSS, včetně správců kritické infrastruktury.

V metodice se neuvádí detailní postup nastavení a provedení konkrétních testovacích scénářů s konkrétními přístroji, protože vzhledem k rozličnosti uživatelských potřeb, specifik aplikací a přístrojů samotných by nebylo možné v rámci jedné metodiky vše obsáhnout. Metodiku je možné použít jako univerzální seznam aktivit a doporučení. Dále je nutné, aby uživatelé přizpůsobili navrhované postupy vlastním potřebám a vybavení a řídili se mj. také dokumentací od výrobců.

4 Srovnání novosti postupů

Jak již bylo zmíněno v předešlých kapitolách, v současné době v českém prostředí ani na mezinárodní úrovni neexistuje metodika, která by se věnovala zkoumání vlivu radiofrekvenční interference na přijímače GNSS.

Hlubší studium hrozeb GNSS včetně například monitorování příslušného spektra je relativně mladý obor, ve které zatím nebyly ustáleny postupy testování a vytvořeny příslušné metodiky a standardy.

Na evropské úrovni se této problematice začal v roce 2016 věnovat projekt STRIKE3. Jedná se o tříletý projekt podporovaný z výzkumného programu Horizont 2020, který se zabývá detekcí interference GNSS na evropské úrovni. Součástí prací je také testování a hodnocení výkonosti přijímačů a vybudování databáze RF podpisů z posbíraných dat.

Vzhledem ke společným cílům projektu STRIKE3 a projektu *Kategorizace hrozeb otevřené službě systému Galileo a opatření k jejich zmírnění* probíhají diskuze obou řešitelských týmů, aby výsledné postupy byly navzájem v souladu a zároveň odrážely nejnovější poznatky v dotčených oblastech.

Vzhledem k narůstající závislosti na GNSS a současně rostoucí frekvenci výskytu hrozeb GNSS lze předpokládat, že v budoucnu budou nasazena opatření, která se věnují monitorování interference GNSS a následnému testování přijímačů a uživatelských systémů. Potřeba takových opatření je rozpracovaná i v **Akčním plánu rozvoje ITS**:

„8.3.5.6 Rámcový specifický cíl č. 5.6: Rozvoj kosmických technologií

...

Na otevřené službě systému Galileo (OS) bude v blízké době záviset mnoho aplikací z různých hospodářských odvětví, pravděpodobně nejvíce však z oblasti dopravy, jež je v současnosti největším uživatelem dat z globálních družicových navigačních systémů GNSS (zejména současného GPS). Budovaný systém Galileo a jeho služby, ostatně jako jakékoli jiný systém, nejsou plně odolné proti záměrnému rušení signálu (tzv. jamming) a z toho vyplývajícího znemožnění jeho příjmu přijímačem, anebo vytváření replik signálu (tzv. spoofing), se záměrem ovlivnit výslednou polohu kterou přijímač určí. Problém jammingu by do určité míry mohla odstranit tzv. autentifikace, o jejíž implementaci se u OS reálně uvažuje na úrovni celého systému Galileo, avšak vždy půjde o neustálý závod s těmi, kdo se snaží GNSS aplikace/signály zneužívat a ovlivňovat. Pozornost proto bude zaměřena na mitigační opatření proti hrozbám jammingu a spoofingu s cílem získat, udržovat a rozvíjet schopnosti potřebné pro zajištění správného fungování aplikací GNSS.“ [3]

Jedním z prvních kroků vedoucí ke zvýšené ochraně uživatelů a jejich (kritických) aplikací před záměrnou i nezáměrnou interferencí je zavedení této obecné metodiky, která zvýší povědomí o možnostech tohoto druhu opatření (testování) a uživatele lépe připraví pro sestavení konkrétní testovací specifikace, která bude jednotlivé kroky uvedené v této metodice doplňovat a zpřesňovat.

Metodika se věnuje všeobecným aspektům a parametrům testování i návrhu testovacích metod. Taktéž obsahuje proces výběru hrozeb a způsob měření výkonu testovaného zařízení na základě zvolených veličin. Cílem metodiky je vytvoření testovací architektury, která je komplexní a zároveň

co nejuniverzálnější a opakovatelná. Uživatelům poskytne informace o minimálních požadavcích na testování a hodnocení přijímače.

Testováním uživatelé získají důležité informace o chování svých zařízení a systémů v přítomnosti interference a budou tak lépe připraveni na provoz v reálném prostředí. Metodika testování proto představuje jeden ze základních prvků zabezpečení (kritických) systémů využívajících signál GNSS.

5 Uplatnění certifikované metodiky

Tato metodika definuje postup pro přípravu a průběh testování přijímačů GNSS vůči škodlivému rušení – jammingu. Součástí metodiky je taktéž popis hrozeb otevřené služby Galileo a dalších možných opatření. Je nutné zdůraznit, že testování přijímačů je jen jedním článkem komplexního procesu opatření proti jammingu, které je potřeba vykonávat, přičemž jednotlivé články jsou navzájem propojené (Obrázek 1). Aby bylo testování přijímačů efektivní a poskytlo vypovídající informace o výkonu testovaného zařízení, je nutné podrobit přijímač reálným hrozbám sesbíraným v reálném prostředí, a to prostřednictvím monitorování a detekce interference. Sesbírané hrozby je následně nutné sdílet s vybranými koncovými uživateli. Do celého zmíněného cyklu opatření vůči jammingu mohou být začleněné státní organizace, stejně jako i správci infrastruktury a soukromí uživatelé.

Obrázek 1: Procesní řetěz opatření pro zamezení škodlivé interferenci

Státní správa a samospráva může zastávat řídící roli, například se může podílet na vytvoření a provozu monitorovací sítě pro detekci škodlivé interference, vytvoření národní databáze detekovaných hrozeb a rovněž může využívat sesbíraná data pro testování vlastních zařízení a systémů. Jednou z úloh státu je i zvýšení povědomí uživatelů o hrozbách pro systém Galileo a tím i pro zařízení a systémy, které tuto službu využívají. Důležitou součástí celého procesu jsou správci infrastruktury, především kritické, na kterou by měl být kladen důraz při zavádění jednotlivých opatření.

Hlavním uživatelem na úrovni státní správy může být Ministerstvo dopravy (MD ČR), do jehož gesce spadá program Galileo a současně je správcem rozsáhlé dopravní infrastruktury. Role MD ČR může být jednak monitorování a detekce škodlivé interference na dopravní infrastruktuře, ale i přímo využití metodiky pro testování přijímačů vůči jednotlivým hrozbám. Mezi další uživatele můžou patřit Ministerstvo vnitra, Národní bezpečnostní úřad resp. Národní úřad pro kybernetickou a informační bezpečnost, jako instituce s bezpečnostní agendou státu.

Možné role státu:

- provozovatel vybraných systémů:
  - monitorovací systém a detekce škodlivé interference,
  - databáze detekovaných hrozeb,
  - databáze koncových uživatelů (především kritická infrastruktura),
- **správce systémů využívajících GNSS (testovaní zařízení a systémů),**
- provozovatel zařízení na dopravní infrastruktuře (ŘSD ČR, kraje a města, letiště),
- provozovatel zařízení na vybraných vozidlech státní správy (např. sypače, údržbové vozy atd.),
- zpracovatel dat z vozidel a infrastruktury,

- poskytovatel dopravních dat z dopravní infrastruktury,
- **definovaní požadavků na testování pro jednotlivé uživatele,**
- správce pravidel pro implementaci (udělovat licence pro provoz atd.),
- **autorita ověření správné implementace (certifikace, supervize atd.).**

Role koncových uživatelů je především v přímém využití předkládané metodiky testování:

- sestavení požadavků na konkrétní aplikaci,
- testování přijímačů a systémů,
- posílení vlastních systémů,
- zavedení záložních řešení.

Zavedení této metodiky by mělo přinést zvýšení povědomí o hrozbách otevřené službě Galileo a závislosti jednotlivých systémů na této službě, přičemž hlavní uplatnění metodiky je v zavedení všeobecných postupů pro sestavování testů, výběr metod a sledovaných parametrů i výběr hrozeb, vůči kterým budou přijímače testovány. Jedná se tedy o univerzální seznam aktivit a doporučení, přičemž uživatelé musí testování přizpůsobit vlastním potřebám a jednotlivým aplikacím.

6 Předchozí publikace a studie

S postupným zaváděním systému Galileo do provozu začaly vznikat různé iniciativy, především ze strany EK a ESA, ale i na úrovni jednotlivých členských států, na ochranu před hrozbami. **Nejčastějším tématem těchto projektů byl právě jamming**, avšak jednotlivé projekty byly zaměřeny především na monitorování a detekci jammingu, **než na samotné testování přijímačů GNSS vůči této hrozbě**.

Monitorování, detekce a zaznamenávání signálů rušení je důležité i při samotném testování přijímačů, protože umožňuje testování vůči reálným hrozbám a získání informací o výkonu přijímače v reálném prostředí. Níže je uveden popis vybraných projektů týkajících se hrozeb GNSS.

Největší prostor je zde věnován projektu STRIKE3, který se zaměřuje také na tvorbu metodiky testování přijímačů. Jeho poznatky zohledňuje také tato metodika.

DETECTOR

Výsledkem projektu DETECTOR byla nízkonákladová **služba pro detekci radiofrekvenční interference GNSS** pro použití v silniční dopravě a kritické infrastruktuře. Sondy, umístěné u vozovek a propojené s back-office, detekují interferenci pomocí technik využívajících softwarové přijímače. Schopnost analýzy interference na úrovni digitálních vzorků umožňuje spolehlivější detekci a **charakterizaci interferenčních signálů** a pomáhá rozlišit neúmyslné zdroje interference od záměrného rušení.

Veškerý software a hardware projektu DETECTOR byl testován jak v laboratoři, tak během polních testů a využíval specializované senzory a data dostupná z existujících referenčních sítí GNSS. Ve všech případech byla řešení schopná detekovat a charakterizovat řadu typických rušiček a posoudit jejich potencionální dopad na služby založené na GNSS. Z projektu vznikl stejnojmenný produkt pro nepřetržitý monitoring interference v cílových lokalitách.

PROTECTOR

Studie PROTECTOR (Protection, Evaluation and Characterisation of Threats Originating from Radio-sources) zkoumala potřeby ochrany evropských systémů a služeb GNSS proti zdrojům radiové interference za účelem **ochrany proti výpadkům**. Studie definovala a specifikovala operační službu pro zajištění ochrany a **kontinuity evropské infrastruktury a služeb GNSS**. Ta principiálně zahrnuje monitoring a ochranu sítí EGNOS a Galileo. Vize studie zahrnovala také využití pokročilejších technologií přijímačů se zaměřením na PRS.

Součástí studie bylo také zkoumání existence a integrace zařízení a schopností členských států bránit se výpadkům systémů a služeb GNSS se zjištěním, že většina států má detekční vybavení, které dokáže identifikovat přítomnost zdrojů radiofrekvenční interference.

ESA Interference Monitoring System

Cílem studie bylo vyvinout a demonstrovat použití **systému monitoringu interference** (Interference Monitoring System – IMS), který by měl poskytovat informace o interferenci v měřících stanicích téměř v reálném čase. Tyto stanice zahrnují zařízení Galileo Sensor Station a EGNOS RIMS (Ranging Integrity Monitoring Stations). IMS sestává z objektu pro zpracování (Processing

Facility – PF) a několika lokálních prvků (Local Elements – LEs). PF obsahují pracovní stanici pro příjem dat z LE a zprostředkovávají dále informace a data. LE jsou zařízení schopná monitorovat relevantní spektrum a poskytovat výsledky v digitální formě.

GAARDIAN

Projekt předcházející SENTINELu byl součástí programu „Gathering Data in Complex Environments“. Jeho úkolem bylo vytvořit systém, který by sbíral data a bylo by možné ho umístit v blízkosti objektů s **klíčovými** nebo **pro bezpečnost kritickými** aktivitami, kde by **ověřoval přesnost a spolehlivost PNT zdrojů**, konkrétně signálů GNSS. Technickou výzvou programu GAARDIAN byl sběr a nepřetržité filtrování velkého objemu dat z rozptýlených míst.

SENTINEL

Úkolem programu SENTINEL bylo určit spolehlivost signálů GNSS a eLoran PNT. Síť sond SENTINEL může být nasazena pro 24x7 monitoring klíčových parametrů a může **detekovat, kvantifikovat a lokalizovat přirozenou a umělou interferenci**.

Veřejná zpráva z projektu [4] obsahuje výstupy z měření interference v roce 2013 na různých lokalitách (v blízkosti letiště, v centru Londýna nebo poblíž frekventované dálnice). Kromě celkových počtů detekovaných incidentů jsou k dispozici také přehledy časového rozdělení v rámci týdne nebo dne a průměrná doba trvání nejvyšší intenzity rušení.

Řešení programu SENTINEL bylo použito i v rámci systému Excelis Sentry 1000 jako součást pro systém lokalizace rušiček.

GEMNet

V rámci britského projektu GEMNet vznikla studie [5]. Projekt se zabývá **zkoumáním interference GNSS, jejího rozsahu a povahy**. Za tímto účelem byly v UK vybudovány monitorovací stanice ve čtyřech vybraných lokalitách (zpravidla blízko kritické infrastruktury), jejichž hlavními úkoly jsou:

- monitorovat radiové spektrum GNSS ve vybraných lokalitách v UK, aby bylo možné kvantifikovat přítomnost rušiček,
- zachytit různé radiofrekvenční podpisy jednotlivých rušiček,
- vyhodnotit dopad rušiček a dalších zdrojů interference na práci přijímačů GNSS,
- posoudit vliv rušiček v závislosti na jejich vlastnostech (např. slabší vs. silnější rušička) nebo na prostředí (např. vzdálenost zdroje rušení od přijímače).

Senzory sítě GEMNet jsou umístěné v blízkosti přijímačů GNSS pro kritickou infrastrukturu, přibližně 100 až 150 m od dopravních komunikací, na kterých se předpokládá přítomnost většiny zdrojů interference.

Systém pro odhalování nezákonného rušení GNSS signálu v blízkosti strategické infrastruktury

Cílem projektu je výzkum a vývoj systému schopného odhalovat rušení „jamming“ a „spoofing“. Systém poskytne uživateli informaci o nespolehlivosti GNSS signálu a má za cíl zamezit případným nehodám či hrozbám vedoucím ke snížení bezpečnosti provozu. Výsledkem projektu má být:

- funkční systém umožňující detekci ilegálního rušení (RFI) GNSS signálu,
- dlouhodobé testování v reálných podmínkách,
- analýza vlivu rušení na strategickou infrastrukturu,
- certifikovaná metodika užití takovéhoto systému pro minimalizaci vlivu tohoto počínání na provozuschopnost strategické infrastruktury v ČR.

STRIKE3

Projekt STRIKE3 je tříletý projekt probíhající od února 2016 do ledna 2019 podporovaný z výzkumného programu Horizont 2020, který se zabývá **detekcí interference GNSS na evropské úrovni**. Součástí prací je také **testování přijímačů a vybudování databáze RF podpisů** z posbíraných dat.[6]

Dlouhodobým záměrem projektu je vytvořit globální **standardizované prostředí** pro:

- monitorování a reportování interference (vytvořením mezinárodních standardů),
- testování a hodnocení výkonosti přijímačů a aplikací GNSS, které na GNSS závisí (vytvořením testovacích standardů).

Cílem STRIKE3 v oblasti monitorování a reportování je návrh architektury systému a návrh standardů pro sdílení hlášení o zaznamenaných případech interference. Tím bude umožněno, aby se výsledky z různých typů detekčních zařízení a monitorovacích sítí zpracovávaly a zobrazovaly ve společném formátu a tím byla zabezpečena porovnatelnost a následná analýza výsledků.

Uvedený systém by mohl být velmi cenný pro monitorování úrovně hrozby způsobené rušením GNSS ve velkých oblastech a pro zjišťování, jak se mění hrozby v daných oblastech i v systému jako celku v závislosti na čase. Jedná se o systém skládající se z navzájem kompatibilních systémů různých správců umístěných v různých zemích.

Jedním ze stěžejních kroků k naplnění těchto cílů je **vytvoření a rozmístění sítě monitorovacích stanic** na různých místech světa. V současné době jsou monitorovací stanice umístěné v UK, České republice, Slovensku, Slovinsku, Polsku, Německu, Francii, Finsku, Švédsku a Indii. V plánu je síť dále rozšířit o monitorovací stanice v USA, Kanadě, Austrálii, Vietnamu, Jižní Koreji, Španělsku, Norsku, Belgii a Nizozemí.

Navrhovaný systém monitorování a hlášení hrozeb tvoří dva hlavní prvky:

- senzory (na detekci rušení a události hlášení),
- centralizovaný server (na shromažďování zpráv z různých snímačů v centralizované databázi a poskytnutí přístupu k výsledkům pro koncové uživatele) [6].

V tomto konceptu jsou senzory provozně nezávislé na centralizovaném serveru, tj. není potřeba nasazovat specifické monitorovací sítě nebo konkrétní typ detekčního zařízení na podporu centralizované databáze událostí. Cílem je, aby se na monitorování rušivých vlivů mohla používat zařízení od různých výrobců a do centralizované databáze mohly přispívat již nasazené senzory a monitorovací sítě i nové instalace.

V oblasti testování přijímačů je celkovým záměrem STRIKE3 poskytnout standardizovanou metodiku pro testování přijímačů proti skutečným interferenčním signálům sesbíraným v terénu. Zkušební orgány, výrobci a uživatelé potom mohou tyto standardy použít pro testování konkrétních aplikací/zařízení s vhodnými prahovými hodnotami intenzity rušení nebo zvolením jiných parametrů pro testování schopností přijímače. Výstupy projektu z oblasti testování by měly být architektura testů, metodologie testů, definování měřitelných veličin výkonu přijímače, kritéria a proces výběru hrozeb. Tyto výstupy by měly být veřejně dostupné v roce 2018 a budou obecným doporučením pro testování přijímačů GNSS vůči jammingu. Uvedené poznatky zohledňuje i tato metodika.

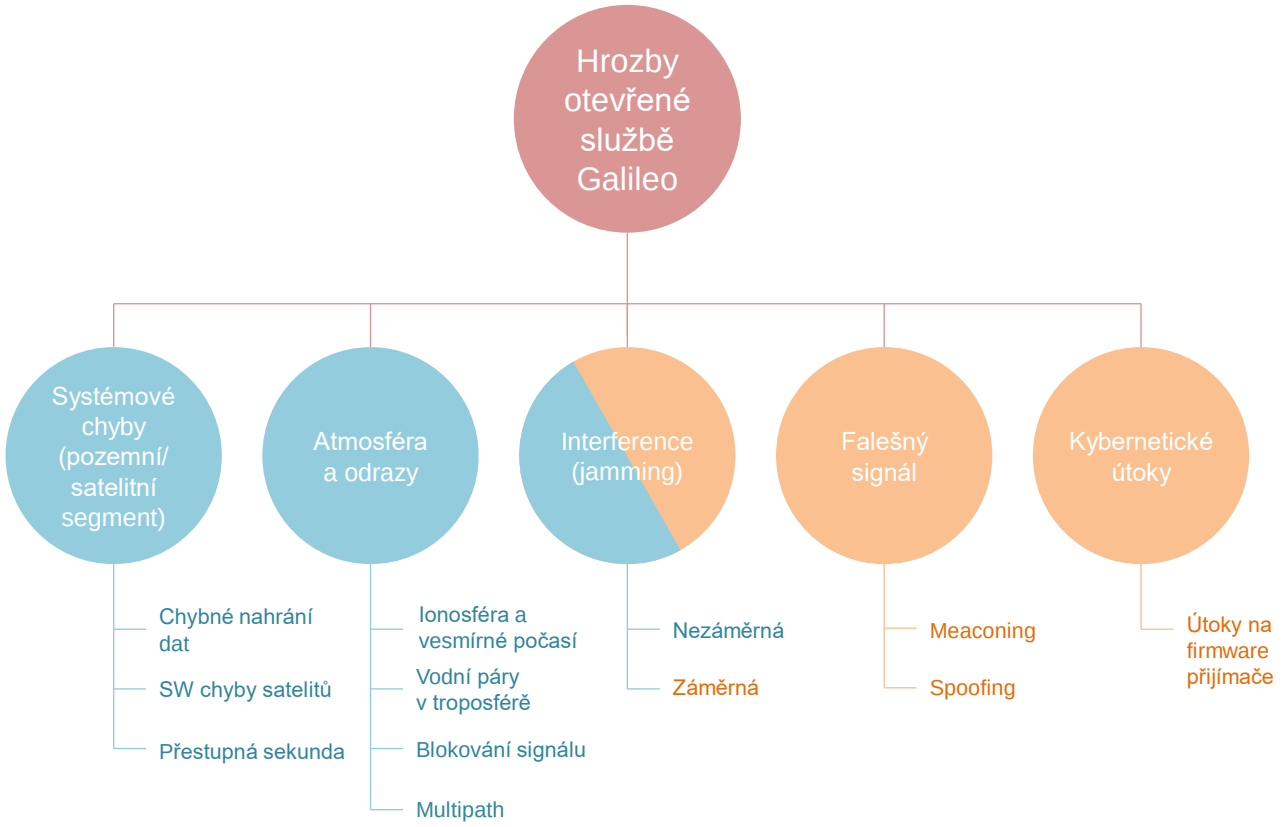
7 Hrozby GNSS a kritická infrastruktura

Signály vysílané GNSS satelity jsou obecně **velmi slabé**. Otevřená služba (např. Galileo Open Service, GPS SPS a další) poskytuje volně dostupné signály, které v současné době **nejsou chráněné šifrováním**. Vlivem těchto faktorů je snadné tyto signály rušit, blokovat či s nimi manipulovat. Aplikace, které tyto signály využívají, jsou následně citlivé na stále rostoucí množství hrozeb a to včetně kritické infrastruktury. Následující kapitola se věnuje jednotlivým hrozbám a popisu prvků kritické infrastruktury.

7.1 Hrozby GNSS

Za hrozbu považujeme takovou událost, která způsobí degradaci nebo nedostupnost služby nebo jiným způsobem poskytne uživateli nesprávnou informaci.

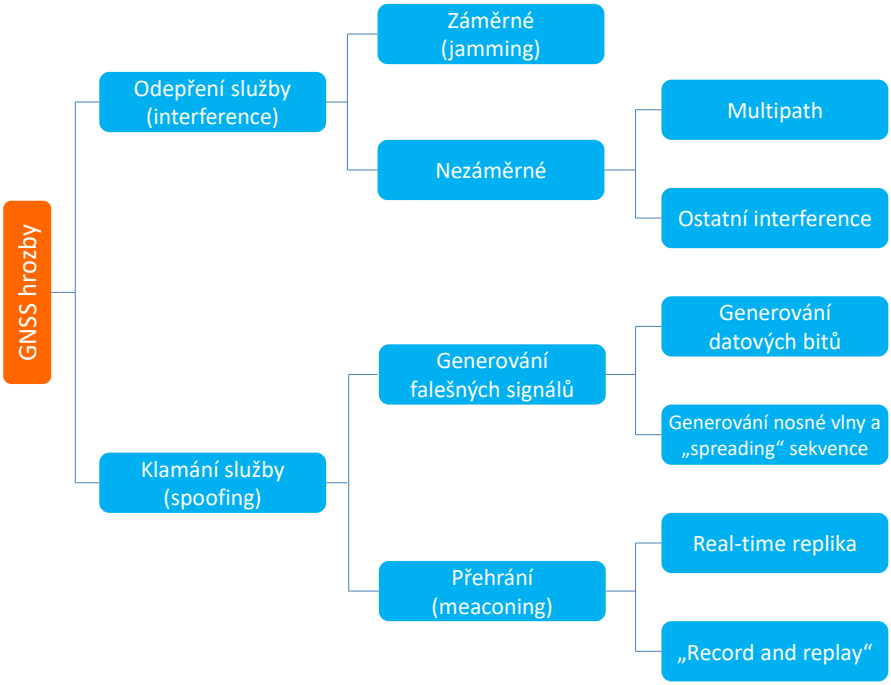
Hrozby můžeme rozdělit na záměrné a nezáměrné:



Obrázek 2: Kategorizace hrozeb otevřené službě Galileo

Hrozby jsou barevně odlišeny podle toho, zda se jedná o **záměrné napadení uživatele nebo jiný záměrný útok** (oranžově označené hrozby), či nikoliv (modře označené hrozby). V prvním případě se jedná o známé a zdokumentované případy úmyslného škození a tato studie se ve své poslední části bude věnovat opatřením na zmírnění jejich dopadu. V druhém případě jde o **chyby a slabá místa systému GNSS**, které se nedají do velké míry předvídat – vzniknou například při údržbě systému. Dále se může jednat o plánované události, jako je například přestupná sekunda a očekávané události, které se **běžně odehrávají při šíření signálu** (vliv atmosféry, odraz a další). Tento druh slabých míst GNSS je v dnešní době řešen především na úrovni zpracování signálu v přijímači a zavedením příslušných korekcí a opatření.

Pro doplnění uvádíme také oficiální rozdělení vydané agenturou GSA [7], které se věnuje pouze uměle (tj. člověkem) vytvořeným hrozbám.



Obrázek 3: Rozdělení uměle vytvořených hrozeb podle [7]

Následující kapitoly se věnují popisu jednotlivých hrozeb podle rozdělení uvedeného výše, avšak důraz certifikované metodiky je kladen na záměrné hrozby, především jamming, které jsou popsané detailněji.

7.1.1 Systémové chyby v pozemním a satelitním segmentu

Systémy pozemního a satelitního segmentu jsou navrženy tak, aby byly velice spolehlivé a zároveň odolné vůči různým druhům hrozeb (včetně například fyzického útoku v době válečných konfliktů). I přesto však existuje několik zdokumentovaných případů, kdy došlo k narušení služby GNSS vlivem chyby v pozemním nebo satelitním segmentu. Tyto případy, ač velice ojedinělé (často označované pojmem anomálie), měly mj. dopad na funkci kritické infrastruktury a proto je důležité tuto hrozbu zmínit. Mezi systémové chyby patří:

- chybné nahrání dat,
- softwarové chyby satelitů,
- přestupná sekunda.

7.1.2 Atmosféra a odrazy

Signál GNSS na cestě od satelitu k přijímači prochází atmosférou, kde je ovlivňován nabitými částicemi v ionosféře a vodními parami v troposféře, čímž vznikají určité chyby ovlivňující přesnost určení PNT. Vliv na šíření signálu má také extrémní vesmírné počasí (solární bouře) a bezprostřední okolí přijímače, ve kterém může dojít k odrazům nebo blokaci signálu. Řadíme sem:

- vliv ionosféry a vesmírného počasí,
- vodní páry v troposféře,
- blokování signálu,
- multipath (vícenásobný odraz).

7.1.3 Interference – jamming

Zdroj elektromagnetického záření může rušit slabý signál GNSS a tím způsobit pokles kvality výsledné informace o PNT, kterou uživatel ve výsledku získá. Kromě **přírodní interference**, ke které dochází například šířením signálu napříč atmosférou, existuje také interference nepřírodního původu – tedy vycházející z okolních elektronických zařízení. Nejedná se pouze o vysílače, ale o elektroniku jakéhokoliv druhu. V případě **záměrné interference** se používají speciální zařízení (rušičky, jammery) vysílající energii v pásmech odpovídajících frekvenčním pásmům GNSS.

Interference je obecně označovaná pojmem **jamming**. V současné době se s tímto spojením však spíše setkáme ve smyslu záměrné interference, tedy úmyslného škození.

7.1.3.1 Nezáměrná interference

K nezáměrnému rušení dochází v případě vysílání **radiofrekvenčního hluku** (šumu), který interferuje s frekvencí GNSS. Tento jev je celkem běžný a je možné jej pozorovat **v přítomnosti různých elektronických zařízení**. Také šum ze samotného přijímače může mít negativní vliv na kvalitu získané informace. Ve většině případů nemá okolní šum na správnou funkci přijímače GNSS významný vliv, protože je slabý, nicméně pokud by síla šumu přerostla určité meze, došlo by ke zhoršení nebo úplné ztrátě služby, stejně jako je tomu v případě záměrného rušení.

Zdrojem nezáměrného rušení z okolí mohou být vysílače nebo porouchané antény, ale v zásadě může být zdrojem rušivé interference jakékoliv jiné zařízení v blízkosti přijímače. Jedním takovým případem byl například rušivý signál vycházející z kamery umístěné uvnitř automobilu. K významnému narušení příjmu GNSS došlo v roce 2002, kdy bezpečnostní kamera blokovala GPS signál v přibližně kilometrovém okolí.

V případě nezáměrného rušení vycházející přímo z antény přijímače GNSS jde o jev zvaný **rebroadcasting antenna**, který byl popsán například v [4]. Jedná se o případy, kdy se starší

antény mohou porouchat a začít vysílat zpět zesílený signál GNSS, který přijaly. Zdokumentováno je například rušivé vysílání antény, která tímto znemožňovala práci jiné anténě umístěné přibližně o 30 m dále. Vzhledem k tomu, že rušivý signál z antény může být shodný se strukturou signálu GNSS, považuje se tento jev také za spoofing.

7.1.3.2 Záměrná interference

Záměrná interference, jamming, je **úmyslné rušení** už tak slabého GNSS signálu takovým způsobem, že přijímač není nadále schopný vyhodnotit správné PNT. V horším případně dojde k celkové ztrátě signálu.

Jednou ze záludností jammingu je fakt, že **uživatel ho jako takový nedovede identifikovat**. Jeho přijímač sice začne podávat nepřesnou informaci (nebo přestane zcela fungovat), ale není možné s jistotou říci, že se jedná právě o vliv rušiček. To dovede s určitou mírou spolehlivosti prokázat až sofistikovaný detektor a následná analýza zachyceného RF spektra.

Jakmile jamming ustane, většina přijímačů je schopna se okamžitě vzpamatovat a znovu fungovat správně. V případě využití přijímače pro kritickou aplikaci je však vhodné přijímač řádně otestovat a to jak pro případ jammingu samotného, tak pro chování přijímače poté, co jamming ustane.

7.1.4 Falešný signál

7.1.4.1 Meaconing

Meaconing (výraz pochází ze spojení anglických slov mislead a beacon) je **znovu přehrání dříve nahraného signálu GNSS za účelem zmatení uživatele**. Zaznamenané signály jsou znovu vysílány na stejné frekvenci a zpravidla s vyšší silou. V důsledku meaconingu získá přijímač nesprávné měření PNT, což může způsobit problémy především v automatizovaných aplikacích, kdy přijímač není schopen rozpoznat útok. Meaconing je někdy uváděn jako forma (podmnožina) spoofingu.

Existují spekulace, že meaconing stál například za některými leteckými haváriemi, nicméně zdokumentované případy z důvěryhodných zdrojů nejsou dostupné. Důvodů může být několik – například to, že meaconing nebyl rozpoznán a potvrzen, ale také předpoklad, že útočníci pro tento typ útoku, jakým je užití falešných GNSS signálů, spíše zvolí více sofistikovaný spoofing.

7.1.4.2 Spoofing

Spoofing je **vysílání falešných signálů GNSS za účelem manipulace s informací o poloze nebo přesném čase**. Dříve byl spoofing považován za téměř hypotetickou hrozbu s velmi malým počtem reálných případů. Nicméně s rozvojem **softwarového rádia (Software Defined Radio – SDR)**, nižší cenou HW komponent a dostupností open source kódu se spoofing stal velice hmatatelnou hrozbou a **lze očekávat nárůst výskytu této hrozby**.

Na rozdíl od jammingu, kdy přijímač pod útokem zpravidla přestane fungovat nebo je patrné, že došlo ke zhoršení přesnosti v poloze nebo čase, **nemusí být spoofing přijímačem vůbec**

rozpoznán. Útočník, použije-li dostatečně sofistikovaný útok, může poté zcela **převzít kontrolu nad daným zařízením**, což může mít kritické následky.

7.1.5 Kybernetické útoky

Za kybernetický útok se dá považovat výše zmíněné generování falešného signálu. Některé zdroje označují jamming také jako formu kybernetického útoku. Nicméně existují i případy, kdy docházelo k **manipulaci se softwarem nebo daty uvnitř zařízení**. Je nutné zdůraznit, že přijímač jako takový tento zásah nemusí poznat, stejně jako tomu je například v případě napadení počítačového systému virem.

Chybná informace o poloze nebo čase je velmi nebezpečná hlavně v případě automatizovaných aplikací nebo autonomních zařízení. Ty budou v blízké budoucnosti stále více přítomné v každodenním životě spolu s nástupem trendů, jako jsou například internet věcí nebo autonomně řízená vozidla.

Tento druh útoku se někdy shodně označuje jako (location) spoofing, ale nejedná se o stejný útok jako GNSS spoofing zmíněný v předešlé kapitole. Pojem spoofing původně pochází právě ze světa počítačových technologií. Jedná se například o zásahy, kdy uživatelé manipulují s IP adresou za účelem dostat se k obsahu, který je nepřístupný v místě, kde se nachází.

Oblast těchto kybernetických útoků za účelem manipulace s PNT informací ještě není zcela objevena, nicméně **v blízké budoucnosti může představovat další velice významnou hrozbu spojenou s užíváním GNSS systémů**. Je potřeba ale zdůraznit, že se již nejedná o hrozbu způsobenou zranitelností otevřené služby GNSS jako takové, ale o slabé místo zařízení, které informace z GNSS využívá.

7.2 GNSS a kritická infrastruktura

Speciální pozornost v metodice je věnována kritické infrastruktuře a aplikacím, u nichž mají hrozby GNSS kritický dopad. Kritická infrastruktura je v českém prostředí definovaná **zákonem č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)** [8]. V §2 tohoto zákona jsou vymezené pojmy a to následovně:

„Pro účely tohoto zákona se rozumí
...
*g) **kritickou infrastrukturou** prvek kritické infrastruktury nebo systém prvků kritické infrastruktury, narušení jehož funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu,*
*h) **evropskou kritickou infrastrukturou** kritická infrastruktura na území České republiky, jejíž narušení by mělo závažný dopad i na další členský stát Evropské unie,*
*i) **prvkem kritické infrastruktury** zejména stavba, zařízení, prostředek nebo veřejná infrastruktura, určené podle průřezových a odvětvových kritérií; je-li prvek kritické infrastruktury součástí evropské kritické infrastruktury, považuje se za prvek evropské kritické infrastruktury,…“*

Dále jsou v **Nařízení vlády č. 432/2010 Sb. o kritériích pro určení prvku kritické infrastruktury** [9] v §1 uvedena průřezová kritéria:

„Průřezovým kritériem pro určení prvku kritické infrastruktury je hledisko

*a) obětí s mezní hodnotou **více než 250 mrtvých nebo více než 2 500 osob s následnou hospitalizací** po dobu delší než 24 hodin,*
*b) ekonomického dopadu s mezní hodnotou **hospodářské ztráty státu vyšší než 0,5 % hrubého domácího produktu**, nebo*
*c) dopadu na veřejnost s mezní **hodnotou rozsáhlého omezení poskytování nezbytných služeb** nebo jiného **závažného zásahu do každodenního života postihujícího více než 125 000 osob**.“*

Národní centrum kybernetické bezpečnosti poskytlo přehledné schéma sloužící při procesu určování prvků kritické informační infrastruktury (KII) [10], které vychází ze zákona č. 240/2000 Sb. a nařízení vlády č. 432/2010 Sb. Nicméně o určení prvků KII se rozhoduje až na základě jednání mezi potenciálními povinnými subjekty (správci prvků KII) a zástupci NBÚ/NCKB.

Na evropské úrovni se kritickou infrastrukturou zabývá především **směrnice Rady 2008/114/ES ze dne 8. prosince 2008 o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu**. Pro zajímavost uvádíme, že tato směrnice explicitně neodkazuje na sektor komunikačních sítí a bankovnictví, ale za kritické považuje především energetiku a dopravu. Dále je zde uvedeno, že v případě potřeby může být tato směrnice použita i v ostatních sektorech s prioritou pro oblast ICT.

V jednotlivých členských státech EU je definice kritické infrastruktury závislá na národních předpisech, nicméně ve velké většině oblastí je společná. Mezi prvky kritické infrastruktury se zpravidla řadí:

- elektronická komunikace,
  - pevná telekomunikační správa sítě,
  - mobilní telekomunikační služby,
  - rádiové spojení a navigace,
  - satelitní spojení,
  - rozhlasové vysílání,
  - internetový přístup,
  - poštovní a kurýrní služby,
  - bankovnictví,
- energetika,
  - elektrická energie,
  - ropa,
  - plyn,
- zásobování vodou a odpadní voda,
- doprava,
- satelitní infrastruktura.

V českém prostředí není závislost sektorů kritické infrastruktury na GNSS ještě zcela zmapována, nicméně průzkum Ministerstva dopravy identifikoval následující uživatele přesného družicového času:

- Česká národní banka,
- Generální ředitelství cel ČR,
- Generální ředitelství hasičského záchranného sboru ČR,
- Správa železniční dopravní cesty,
- Státní plavební správa,
- Povodí Ohře,
- Policie ČR (Řízení, provoz a vývoj ICT),
- Řízení letového provozu České republiky.

Jednotlivé sektory **kritické infrastruktury jsou navzájem úzce propojené a závislé jeden na druhém**. Z toho důvodu je důležité při vyhodnocování rizik a dopadů při přerušení dodávky GNSS uvažovat nejen přímý dopad na daný sektor, ale mít na paměti také tyto závislosti. Ztráta GNSS může poté způsobit kaskádový efekt, kdy budou postupně ovlivňovány další kritické sektory, které jsou závislé na správném chodu napadeného sektoru.

8 Ekonomické aspekty

Tato část metodiky je zaměřena na obecný popis využití a přínosu GNSS, jakož i na analýzu ekonomického vlivu výpadku služby na jednotlivé sektory trhu, včetně dopadů na kritickou infrastrukturu. Součástí kapitoly jsou i ekonomické aspekty spojené s využitím této certifikované metodiky.

8.1 Ekonomické aspekty spojené s využitím této certifikované metodiky

Vzhledem k tomu, že v současné době není k dispozici podobný dokument, který by definoval metodiku testování přijímačů vůči jammingu, dají se ekonomické přínosy pouze odhadnout nastavením tzv. vstupních parametrů. Těmito parametry se rozumí základní výhody, nevýhody, příležitosti a rizika použití této certifikované metodiky. Přestože je obtížné kvantifikovat ekonomické aspekty metodiky, lze vyčíslit přínosy nepřerušeného provozu GNSS i dopady jeho přerušení. Testování je jedním z opatření, které výpadku GNSS mohou do jisté míry zamezit, případně minimalizovat jeho dopady. V této části jsou v přehledu uvedeny základní vstupní parametry, detailnější ekonomický dopad výpadku GNSS, jakož i nefinanční důsledky, jsou detailně rozepsány v následujících kapitolách.

Výhody	Nevýhody
Metodika poskytuje postupy a doporučení pro správné provedení testování přijímačů vůči jammingu. Podává přehled o hrozbách a dalších možných opatřeních.	Metodika neuvádí detailní postup nastavení a provedení konkrétních testovacích scénářů, ale definuje univerzální seznam nastavení, aktivit a doporučení.
Metodika shrnuje všechny studie, které se doposud tématu hrozeb GNSS věnovaly, a přináší komplexní pohled na tuto problematiku.	Metodika nemůže být použita samostatně, je nutné ji doplnit o konkrétní technické specifikace při testování jednotlivých přijímačů.
Příležitosti	**Rizika**
Metodika přináší přehled možných opatření, která mohou minimálně na národní úrovni pomoci nastavit pravidla a prostředí tak, aby se co nejvíce zamezilo následkům ohrožení signálu GNSS.	Nevyužití doporučení uvedených v metodice může vést k nedostatečnému testování přijímačů, které nebude splňovat základní podmínky a neposkytne vypovídající hodnocení výkonu přijímačů v přítomnosti jammingu.
Zvýšení povědomí o hrozbách systémů závislých na GNSS mezi uživateli a správci infrastruktury.	Navzdory vysokým rizikům není možné nařídit testování přijímačů a systémů závislých na GNSS na úrovni uživatelů/správců systémů. Může být založeno jen na dobrovolnosti.

Tabulka 1: SWOT analýza ekonomických aspektů

8.2 Revize existujících studií

Většina studií, které se věnují dopadu výpadku GNSS na existující tržní segmenty, je silně orientována na trh USA, případně na trh velké Británie. Zároveň s tím existuje pouze omezené množství studií rozebírajících ekonomický dopad. Pokud existují, jsou většinou pouze rámcově zaměřené na specifickou oblast průmyslu.

Pro tuto certifikovanou metodiku jsou proto níže uvedené výsledky brány orientačně pro přehled o rozsahu škod, který by nastal při výpadku GNSS v České republice.

Při srovnání ročního přínosu a krátkodobého výpadku je zřejmý značný rozdíl mezi ziskem a ztrátou. Z uvedených čísel je patrné, že krátkodobá nedostupnost GNSS by způsobila natolik komplikované situace pro sektory GNSS využívající, nebo na GNSS závislé, že celkový negativní dopad by mnohonásobně převýšil ekonomický přínos rozpočítaný na stejné období. Ve zdrojové studii je uvažován výpadek na období 5 dnů, stejný příměr je pro ilustraci uveden i v této metodice.

8.2.1 Využití a přínos GNSS

V roce 2014 využívalo GNSS na 3,6 miliardy zařízení. Toto číslo podle odhadů dosáhne 7 miliard do roku 2019 [1]. Z tohoto počtu tvoří největší podíl smartphony využívající polohové služby. Podle studie společnosti Oxera Consulting [11] z roku 2013 je odhadovaná hrubá přidaná hodnota služeb poskytujících polohové služby ve spojitosti s mapami 113 miliard USD. Zároveň s tím studie odhaduje úsporu 1,1 miliardy hodin ročně v oblasti navigace, kdy v opačném případě by tento čas byl strávený v obtížných situacích při cestování (ztráta orientace, atp.).

8.2.2 Ekonomický dopad

V případě analýzy ekonomického dosahu výpadku GNSS je třeba zvážit částečnou a plnou penetraci trhu. V případě částečné penetrace (60% využití v relevantních oblastech) by výpadek znamenal ztrátu ve výši 67,6 miliard amerických dolarů. V případě plné penetrace (100% využití ve všech relevantních oblastech) by se ekonomická ztráta pohybovala ve výši 87,2 miliardy USD. V případě připočtení ztráty způsobené výrobcům GPS zařízení dosahuje celková hodnota ekonomické ztráty 96 miliard USD, což se rovná 0,7 % HDP USA.

8.2.3 Současné využití a přínos GNSS

GNSS Market Report [1] udává, že v současné době existuje pro GNSS osm tržních segmentů:

- Location-Based Services (LBS),
- silniční doprava,
- letectví,
- železniční doprava,
- lodní doprava,
- zemědělství,
- zeměměřičství,
- čas a synchronizace (T&S).

Roční ekonomický přínos pro Velkou Británii, jakožto zemi geograficky a politicky nejbližší České republice, pro kterou zároveň existuje vypracovaná relevantní studie ekonomického dopadu, je rozebraný v rámci těchto segmentů. Ty se dotýkají i klíčové národní infrastruktury, např. energetiky nebo telekomunikací.

Location-Based Services (LBS)

Odhadovaný celkový roční přínos ekonomice v souvislosti s GNSS je 204,8 milionů GBP. LBS je primárně využívána skrze smartphony a tablety, spolu s výrazně menším počtem dedikovaných

zařízení pro snímání polohy (zavazadla, fitness elektronika, atp.). Jen v případě pěší navigace byl přínos LBS v mobilních zařízeních odhadnutý na 137,6 milionu GBP. V případě osobní automobilové dopravy je přidaná hodnota odhadována na 57,4 milionů GBP ročně. Toto v sobě nezahrnuje odhad přínosu GNSS profesionálním řidičům, pro které je přidaná hodnota LBS měřena samostatně.

Silniční doprava

Přínos GNSS silniční dopravě v UK je oceněný na 1 217,4 milionů GBP. Toto číslo agreguje roční úsporu času stráveného za volantem, úsporu paliva a s tím spojenou redukci emisí a skleníkových plynů. Je vhodné zmínit, že i v této oblasti jsou často využívaným zařízením smartphony, které nahradily zařízení přímo určená pro navigaci.

Letectví

V oblasti letectví je hrubá přidaná hodnota GNSS 0,5 milionu GBP. Další přínosy spojené s GNSS byly vyčísleny na 2 miliony GBP ročně. Hlavní přínos GNSS v letecké dopravě je v redukci zpoždění, odklonů a zrušení letů (DDC, Delay, Diversion and Cancellation), a v asistenci při přistávání ve zhoršených podmínkách. Dále se počítá s úsporou paliva a tím i snížením množství emisí
a množství asistenčních technologií pro piloty.

Železniční doprava

Odhadovaná roční hrubá přidaná hodnota GNSS železniční dopravě je 10,9 milionů GBP. Největším přínosem železniční dopravě v UK jsou tzv. „driver advisory systems“, asistenční systémy pro strojvůdce, plně implementované ve vysokorychlostních a nákladních vlacích. Tyto systémy snižují energetickou náročnost železniční dopravy a opotřebení brzdných systémů. Zároveň umožňují vyšší utilizaci vlaků, tedy přepravu většího množství zboží bez nutnosti rozšířit existující infrastrukturu. Samotný ekonomický přínos GNSS pro vysokorychlostní a nákladní železniční dopravu je oceněn na 10,9 milionů GBP ročně.

Lodní doprava

Hrubá přidaná hodnota využití GNSS v lodní dopravě je odhadována na 420 milionů GBP ročně, plus 8,8 milionů dalších odhadovaných přínosů. Přínos GNSS systémů pro lodní dopravu v UK samozřejmě nebude proporcionální přínosu GNSS v lodní dopravě v České republice.

Kromě navigačních systémů používaných v lodní dopravě je významnou přidanou hodnotou využití GNSS v oblasti záchrany lidského života a dalších bezpečnostních systémech.

Zemědělství

Odhadovaná roční hrubá přidaná hodnota v zemědělství je 132,5 milionu GBP, spolu s dalšími výhodami oceněnými na 151,9 milionu GBP ročně. V oblasti zemědělství má GNSS dvě hlavní oblasti využití – precizní navigaci stroje, kdy jsou řidiči poskytovány informace pro okamžitou úpravu trasy, a automatické zatáčení, tedy systém, který autonomně řídí techniku. GNSS tím umožňuje efektivnější využití lidských zdrojů i samotné mechanizace.

Zeměměřičství

Hrubá přidaná hodnota GNSS v zeměměřičství je vyčíslena na 13,9 milionu GBP ročně. Toto číslo je tvořené čtyřmi kategoriemi:

- tvorba map,
- důlní práce,
- námořní geodetické práce,
- stavebnictví.

V případě vytváření map je přínos GNSS oceněn na 1 milion GBP ročně, pro oblast důlních prací je to méně než 1 milion GBP ročně, pro námořní geodetické práce 1,4 milion GBP (v případě České republiky lze očekávat výrazně nižší hodnoty), a pro oblast stavebnictví je celková hodnota využití satelitních systémů vyčíslena na 7,5 milionu GBP ročně. Zde se GNSS využívá zejména pro precizní kontrolu strojů, podobně jako v zemědělství. Hlavním přínosem je zejména zpřesnění práce, která by bez GNSS nebyla možná. To znamená především úsporu využitého materiálu, snížení chybovosti a snazší plánování návaznosti komunikací. V této oblasti se GNSS využívá hlavně při projektování pozemních komunikací a stavby železnice.

Čas a synchronizace (T&S)

Přesné vyčíslení přidané hodnoty GNSS v této oblasti je obtížné. Precizní čas a synchronizace jsou klíčové pro oblast telekomunikace, národní obrany, energetiky, finančních služeb ad. Kvůli obtížně definovatelnému předělu mezi samotným odvětvím a přínosem precizního měření času a synchronizace zůstává tato oblast bez přesně vyčíslené hodnoty.

8.2.4 Analýza dopadu pětidenního výpadku GNSS

Pětidenní výpadek GNSS by drasticky poznamenal všech osm diskutovaných tržních segmentů. Před samotným vyčíslením je třeba stanovit rozdíl mezi ekonomickým dopadem výpadku GNSS a mezi hodnotou ekonomické aktivity podporované GNSS.

Ekonomický dopad výpadku GNSS v rámci této analýzy řeší pouze pětidenní výpadek v UK a omezuje se na přímý dopad výpadku a v konkrétních ekonomických aktivitách.

Hodnota ekonomických aktivit podporovaných GNSS se v první řade zabývá ročním přínosem a nebere v potaz faktory jako je spolehlivost, odolnost, nebo technologické alternativy k GNSS.

Location-Based Services (LBS)

Ekonomická ztráta v oblasti LBS využívající GNSS je během pětidenního výpadku odhadována na 0,8 milionu GBP. V osobní oblasti LBS je ztráta přístupu k GNSS do značné míry nahraditelná přístupem k jiným způsobům navigace. V urbanistických oblastech se lze navigovat pomocí dostupných schémat veřejné dopravy, atp. Je ovšem nutné vzít v potaz ztrátu přínosů popsaných v sekci 8.2.3, jako jsou ztráta úspory času stráveného na cestě do cílové lokace, ztráta zavazadel a nemožnost využívání různých služeb závislých na přesné poloze.

Silniční doprava

Ztráta v silniční dopravě je odhadována na 1 869,7 milionů GBP. Náhlá nedostupnost GNSS by značně zkomplikovala silniční dopravu, kdy by docházelo ve velké míře ke ztrátě orientace a schopnosti řidičů optimalizovat svoji trasu. S tím by se pojily vzniklé dopravní zácpy a další návazné komplikace, jejichž cenový dopad je odhadovaný na 1 853 milionů GBP, z toho 1 668 milionů GBP za čas a 185 milionů GBP za palivo ztracené v dopravních zácpách.

Letectví

Celková ekonomická ztráta v letectví je odhadována na souhrnnou částku 0,4 milionu GBP. Díky vybavení letadel redundantními systémy pro takové případy, by se ztráta GNSS neprojevila tak drasticky jako v jiných odvětvích.

Železniční doprava

Ztráta hrubé přidané hodnoty během pětidenního výpadku GNSS je v železniční dopravě odhadována na 94,9 milionů GBP; ztráta dalších přínosů byla vyčíslena na 15,5 milionů GBP. Za největší oblast ztrátovosti lze označit nemožnost dopravy pracujících do jejich zaměstnání kvůli zrušeným spojům. Výpadek GNSS by se dotkl i oblastí přepravy nákladů, volnočasového cestování a znamenal ztrátu potenciálních zákazníků.

Lodní doprava

Celková ztráta způsobená pětidenním výpadkem je pro UK odhadována na 12 milionů GBP. Tato částka zahrnuje lodní nákladní dopravu, rybářské lodě, výdaje spojené s cestováním ad.

Opět lze předpokládat, že v případě České republiky by byla způsobená ztráta výrazně nižší.

Zemědělství

Ztráta hrubé přidané hodnoty během pětidenního výpadku pro oblast zemědělství je vyčíslena na 151,6 milionů GBP, spolu se ztrátou dalších přínosů ve výši 4,2 milionů GBP. Výnos z precizního používání zemědělských strojů závisí na velikosti pole a na zaseté plodině. Je odhadováno, že pětidenní výpadek GNSS by způsobil pokles v celkové úrodě o 13 % [12], což by se samo o sobě rovnalo ekonomické ztrátě 125,7 milionů GBP. Značnou ztrátu by také zaznamenaly následné sektory závislé na produkci místního zemědělství.

Vytížení zemědělství se přirozeně mění podle ročního období, tudíž je možné, že by krátkodobý výpadek GNSS mohl způsobit výrazně menší ztrátu.

Zeměměřičství

Odhadovaná ztráta pro sektor zeměměřičství při nedostupnosti GNSS je 344,8 milionů GBP. Za nejvíce zasaženou oblast lze jednoznačně považovat oblast stavebního inženýrství [13]. Zde by došlo k zastavení prací, navýšení stavebních cen a následné akumulaci penalizací. Spolu se stavebním inženýrstvím by byly zasaženy také geodetické práce, průzkumy půdy a další. Škodu by zaznamenal i ropný průmysl, zejména kvůli ztrátě funkčnosti průzkumných plavidel a dalších zařízení.

Čas a synchronizace (T&S)

Jak bylo zmíněno v kapitole 8.2.3 – kvůli široké škále odvětví, které přesné časování a synchronizaci z GNSS využívají, nelze ztrátu způsobenou jeho výpadkem přesně vyčíslit.

8.3 Dopady výpadku GNSS na kritickou infrastrukturu

Jak bylo uvedeno v kapitole 7.2, v dnešní době je většina kritické infrastruktury závislá na GNSS, které systémům dodává informaci o přesné poloze, rychlosti a především času. GNSS je často primárním zdrojem této informace, mnohé segmenty kritické infrastruktury jsou tak přímo závislé na GNSS, což představuje určitou hrozbu v případě nedostupnosti této služby. Míra závažnosti dopadů je poté závislá na přítomnosti záložních řešení při ztrátě GNSS.

Podle studie SENTINEL [4] existuje několik oblastí **kritické infrastruktury nebo dalších kritických aplikací**, které mohou být jammingem vážně ohroženy. Tabulka 2 podává přehled o těchto a několika dalších oblastech a možném dopadu při rušení GNSS.

Oblast	Možný dopad při rušení GNSS
GBAS, SBAS a letecké přistávací systémy	Jednou z prvních aplikací, která přiznala zranitelnost GPS jammingem, byl přistávací systém na Mezinárodním letišti v Newarku v USA, který využívá technologii GBAS. Rozhovory s leteckými organizacemi, které využívají GNSS technologie (včetně SBAS) pro přistávací systémy, potvrdily, že jsou znepokojeni GPS jammingem. Také se obávají zranitelnosti systémů SBAS, které hrají klíčovou roli při zajištění integrity v leteckých navigačních systémech založených na GNSS.
Drátové telekomunikační sítě	Drátové telekomunikační sítě využívají GPS signály jako zdroj přesného času od roku 1996. Během ztráty GPS signálu udržují synchronizaci automatickým přepnutím na vnitřní zdroj času, který zajišťují vysoce stabilní OCXO oscilátory nebo rubidiové atomové hodiny. Díky této a dalším zálohám jsou drátové telekomunikační sítě, pokud jsou vhodně navržené, odolné proti výpadku GPS signálu.
Bezdrátové telekomunikační sítě	V současné době vyžaduje rozdělení komunikačních linků na frekvenční sloty (Frequency Division Duplex, FDD) bezdrátových telekomunikačních sítí relativně nízkou přesnost, krátkodobá ztráta GPS signálu tak chod sítě neovlivní. Nicméně nastupující 4G sítě používají tzv. techniky rozdělení komunikačních linků na časové sloty (Time Division Duplex, TDD), které vyžadují sub-mikrosekundovou přesnost času. Zranitelnost vůči ztrátě GPS se ukázala během jammingových útoků Severní Koreji na Jižní Koreu – četné CDMA mobilní telefonní sítě ztratily časování a selhaly.
Výroba a distribuce elektřiny	Odvětví výroby a distribuce elektrické energie vyžaduje zdroje časování s přesností lepší než 1 nanosekunda pro sledování chyb a vyrovnávání fází. Stále častěji jsou pro tento účel využívány GPS přijímače. Tyto systémy mají mnohem menší odolnost, než je tomu u telekomunikačních sítí a GPS zařízení. Toto odvětví připouští, že má zranitelná místa, ale zatím je vynakládáno jen málo úsilí k jejich zmírnění nebo odstranění, protože žádné problémy doposud nebyly přičítány přímo GPS jammingu.
Finanční obchodování, bankovnictví	Vzhledem k vyžadované přesnosti potřebné k synchronizaci těchto systémů (méně než 1 mikrosekunda) doporučila britská vláda používání GPS a Evropská komise zvažuje nařízení používání systému Galileo. V návaznosti na využití GPS či jiných GNSS bude potřeba se zaměřit na robustnost těchto systémů a možné následky spojené s jammingem.
Telematika pro pojišťovnictví	Telematika je v oblasti pojištění relativně nový termín, ale současně jde o rychle rostoucí novou formu pojištění. Ukazuje se, že je účinnou formou snižování nákladů na pojištění pro nové řidiče. Vozidla vozí telematické jednotky, které sledují cesty a styl jízdy řidiče a na základě těchto údajů je řidičům přiřazována prémie z pojištění. Palubní jednotky také poskytují detailní údaje v případě nehody. Tato technologie je plně závislá na GPS a tím se předpokládá její zranitelnost vůči jammingu.

Sledování majetku, vozidel a osob	Sledovací řešení založená na GPS jsou již dostupná po mnoho let. Mnohé z těchto systémů nemají žádnou ochranu proti GPS jammingu. Jiná využívají hybridní řešení, které používají akcelerometry či jiné senzory nezávislé na GPS, čímž zajišťují kontinuitu, i když jen po omezenou dobu a vzdálenost. V současné době již existují jasné důkazy, že rušičky GPS jsou používány při krádežích cenného majetku.
Zpoplatnění vozovek	Vybírání poplatků za využívání vozovek na základě GPS je dnes běžné v mnoha zemích. Existují jasné důkazy o využívání rušiček GPS v případech, kdy tyto systémy byly nasazeny.
Autonomní vozidla	Autonomní vozidla jsou blízkou budoucností a zatím neexistují zdokumentované případy dopadu jammingu na tyto systémy. S uvedením autonomních vozů do běžného provozu však bude nutné mít jistotu, že záložní systémy (zpravidla další senzory ve vozech) poskytují dostatečně robustní řešení. Lze totiž očekávat, že tato vozidla přijdou na silnicích do těsné přítomnosti rušiček GNSS.
Nad rámec studie SENTINEL zde uvádíme ještě několik dalších aplikací, kde může mít jamming GNSS závažné dopady.	
Bezpečnostní aplikace (Safety of life service)	Některé bezpečnostní aplikace (například pro integrovaný záchranný systém) využívají otevřené signály GNSS. Jejich operativa může být jammingem narušena, i když se nepředpokládá, že by v tomto případě došlo ke kritickému narušení výkonu práce těchto složek (v případě krátkodobého jammingu).
Řízení dopravy	Kromě leteckých řídicích systémů spoléhají na GNSS do určité míry také systémy jiných módů dopravy – železniční, silniční a říční. Chod těchto systémů může být jammingem taktéž narušen a je potřeba na tuto skutečnost brát ohled při návrhu systémů. Vzhledem k výskytu dnešních případů jammingu je nejvyšší pravděpodobnost jammingu u systémů silniční dopravy.

Tabulka 2: Jamming jako hrozba pro kritickou infrastrukturu a kritické aplikace

V kritické infrastruktuře se GNSS využívá především jako **globální zdroj velmi přesného času**. V případě nedostupnosti GNSS se o udržení synchronizace nebo přesného systémového času starají **oscilátory**. Existuje několik druhů oscilátorů, které se liší zejména v tom, jak kvalitně (a dlouho) jsou schopné udržet požadovaný přesný čas nebo synchronizaci. V závislosti na tom mají také různé pořizovací ceny (Tabulka 3). V poslední době se začínají objevovat tzv. **chip scale atomic clocks (CSAC)**. Jejich přesnost je srovnatelná nebo lepší než u rubidiových oscilátorů, navíc jsou tato zařízení výrazně menší a spotřebují mnohem méně energie.

	Temperature Controlled Crystal Oscillator (TCXO)	Oven Controlled Crystal Oscillator (OCXO)	Rubidium Oscillator
Čas pro udržení 1 µs	10 minut až 1 hodina	1 až 8 hodin	8 hodin až 3 dny
Cenové rozpětí (odhad přepočten na Kč)	125 až 625 Kč	1 250 až 3 750 Kč	12 500 až 37 500 Kč

Tabulka 3: Druhy oscilátorů a jejich schopnost udržet 1 µs (zdroj: [14])

V [15] je dále uveden podrobnější přehled vybraných odvětví kritické infrastruktury a jejich zranitelnosti v případě **dlouhodobějšího výpadku GNSS** (Tabulka 4). Tento výpadek může být způsoben jammingem, ale také například vlivem vesmírného počasí nebo systémovou chybou, jako tomu bylo v případě vyřazení satelitu SVN23.

Sektor KI	Požadavky na přesnost	Využívané oscilátory			Min. robustní oscilátor	Holdover [hod]	Vliv na provoz	
		TCXO	OCXO	Rb			Nezáměrná interference 8 hod	Záměrný jamming více dní
Komunikace	v řádu ns		X	X	OCXO	24+	ne	ano
Krizové řízení	v řádu ns		X		OCXO	24+	ne	ano
IT	20 až 100 ns		X		OCXO	1	ano	ano
Bankovnictví	v řádu ms až μs	X	X	X	TCXO	< 1,7	ano	ano
Energetika	v řádu μs		X		OCXO	1	ano	ano
Doprava	v řádu ns		X	X	OCXO	24+	ne	ano

Tabulka 4: Oscilátory ve vybraných sektorech kritické infrastruktury (zdroj: [15])

Je třeba zdůraznit, že kritická infrastruktura je zranitelná v případě **dlouhodobého (stacionárního) jammingu**. V případě slabších mobilních rušiček, jejichž výskyt je dnes pravděpodobně nejběžnější, dochází většinou pouze ke **krátkodobé interferenci** v řádu jednotek až desítek vteřin, která zpravidla chod kritické infrastruktury nijak neovlivní. Nicméně v případě záměrného útoku s vyšší rušivou silou a delší dobou trvání, může být kritická infrastruktura vážně ohrožena s možnou řetězovou reakcí a dopadem do více systémů.

8.4 Dílčí závěry

V této kapitole byla ukázána závislost jednotlivých sektorů na systému GNSS a uskutečněna analýza finančních i nefinančních důsledků jeho výpadku, včetně dopadu na prvky kritické infrastruktury. Na základě analýzy je zjevná vysoká závislost velké části aplikací na kontinuálním provozu systémů GNSS, přičemž mnohé z nich nemají žádné náhradní řešení. Ekonomický dopad na všechny sektory byl ve Velké Británii vyčíslen na 5,2 miliard GBP, v USA v případě částečné penetrace (60% využití v relevantních oblastech) by výpadek znamenal ztrátu ve výši 67,6 miliard USD.

Kromě vysokých finančních ztrát byla také ukázána závislost kritické infrastruktury na systémech GNSS i provázání jednotlivých prvků kritické infrastruktury navzájem, čímž dochází k ohrožení provozu systémů nevyhnutelných pro chod společnosti. Tím se výpadek GNSS systémů stává strategickým ohrožením a je nutné podniknout opatření na různých úrovních, která budou schopná v co největší míře zabránit výpadku, respektive budou minimalizovat jeho dopady. V současnosti dochází k aktivitám na úrovni jednotlivých zemí i nadnárodních institucí, které mají za cíl prozkoumat opatření a jejich zavedení do praxe.

Jednotlivá opatření dokáží zamezit výpadku nebo minimalizovat následky v různé míře. Jedním z elementárních opatření je testování přijímačů, které uživatelům poskytuje informace o vlastnostech jejich zařízení či systému při působení rušení, čímž jim umožňuje připravit aplikace na takovouto hrozbu. Avšak kvantifikace přínosu konkrétního opatření je velmi obtížná, možná proto by se spíše mělo vycházet z ekonomických či neekonomických dopadů výpadku a tím vyhodnotit důležitost jednotlivých opatření.

Následující kapitola detailněji popisuje možná opatření, jedním z opatření je testování přijímačů. Samotná metodika testování je rozpracována v oddělené kapitole.

9 Opatření

V minulé kapitole byla představena rozsáhlá škála hrozeb systémů GNSS se zaměřením na otevřenou službu. V návaznosti na to jsou v této kapitole představena známá opatření proti těmto hrozbám.

Je zřejmé, že **výskyt hrozeb neustále narůstá, přičemž** nejvíce hrozeb přibývá v oblasti záměrných útoků. Hrozby jsou relativně snadno realizovatelné a také jsou stále sofistikovanější. Vznik nových aplikací závislých na GNSS a technologický vývoj jako takový s sebou může nést riziko vzniku nových hrozeb.

S ohledem na tuto skutečnost je třeba věnovat zvýšenou pozornost možným **opatřením,** a to ideálně již **při návrhu systému**, který je na GNSS závislý. Je nezbytné **neustále sledovat měnící se vývoj hrozeb**, protože reakční doba na implementaci nových opatření do stávajících systémů je zpravidla výrazně delší, než tempo jakým mohou nové hrozby vznikat.

Je nutné zdůraznit, že **pro kritické aplikace by mělo být preferováno použití šifrovaného signálu** (např. PRS), avšak jak bylo zmíněno, při silném zdroji rušení nedokáže šifrování ochránit signál před tímto rušením, dokáže ale poskytnout ochranu před manipulací signálu. Pokud tomu tak není a aplikace využívá otevřený signál, je nezbytné využít robustní přijímače a spolehlivé záložní systémy.

9.1 Úroveň implementace opatření

Opatření mohou být implementována na **několika úrovních**:

- **nadnárodní,**
  - Jedná se především o zabezpečení pozemního a vesmírného segmentu, ochranu a modernizaci signal-in-space, zavedení právních předpisů a standardů pro:
    - monitoring a reporting rušení GNSS,
    - **testování přijímačů a dalších zařízení**,
    - ochranu systémů kritické infrastruktury.
  - K těmto opatřením se řadí také investice do uživatelského segmentu ve smyslu (finanční) podpory:
    - výrobců s cílem vytvořit robustnější přijímače, chipsety a antény,
    - uživatelů formou studií a akcí na zvyšování povědomí o této problematice,
    - zavádění aplikací využívajících GNSS na trh, například pomocí pilotních projektů.
- **národní.**
  - Jednotlivé státy implementují vlastní opatření na národní úrovni. Často se tak děje v souvislosti s ochranou národní kritické infrastruktury a kritických aplikací, případně obecněji s ochranou RF spektra na území daného státu. Jedná se především o **monitoring a reporting rušení GNSS nebo vydání právních předpisů a standardů**. Dále mezi národní iniciativy mohou patřit výše zmíněná opatření spojená s podporou uživatelského

segmentu. Navíc mají jednotlivé státy prostřednictvím CPA přístup ke službě PRS, čímž mohou ochránit určité kritické aplikace před vybranými hrozbami.

- **výrobní (GNSS zařízení),**
  - Samotní výrobci implementují hardwarová a softwarová opatření na úrovni chipsetů, přijímačů a antén. Mezi nejzákladnější opatření, které používají přijímače, patří využití filtrů při přijímání a zpracování signálů, tyto filtry se liší v závislosti od výrobce a zařízení (opatření proti jammingu uvádí např. výrobce zařízení u-blox v [47]). Mimo to se vytváří zařízení obsahující inerciální senzory, které slouží jako další vrstva opatření. Zařízení jsou často vytvářena na míru konkrétním případům užití a požadavkům ze strany uživatele. Na straně výrobce také dochází k certifikaci zařízení (například certifikace zařízení pro systém eCall). Výrobci také nechávají svá zařízení testovat, aby ověřili dopady „reálného“ náporu vybraných GNSS hrozeb na konkrétní typ zařízení.
- **uživatelská,**
  - V rámci zabezpečení svých systémů si uživatelé objednávají testování ušité na míru jejich provozním potřebám a implementují doplňkové a záložní systémy. V případě nákupu nového zařízení hledají uživatelé vhodný poměr mezi bezpečností (tj. mírou ochrany před známými hrozbami) a pořizovací cenou, přičemž zařízení musí splňovat řadu dalších požadavků (přesnost, velikost, výdrž baterie a další).

9.2 Druhy opatření

V současnosti existuje mnoho druhů opatření, přičemž některá z nich zmírňují dopady několika hrozeb najednou, zatímco jiná se zabývají jednou konkrétní hrozbou. Tabulka 5 se věnuje **přehledu dnes existujících možností** a obsahuje taky možné záložní systémy.

Kategorie	Popis opatření
Signal-in-space	• Nové signály a více dostupných frekvencí v rámci OS • Využití více konstelací • Autentifikace a šifrování signálu
RF spektrum	• Zákonná ochrana RF spektra proti jammingu a spoofingu • Prostředky na dopadení a potrestání pachatelů (enforcement a právní úprava) • Standardy pro monitorování a reportování interference • Monitorování a detekce RF interference ve spektrech GNSS • Lokalizace zdrojů interference
Přijímače	• Vylepšené robustní přijímače, chipsety a antény (HW i SW) • Hybridní přijímače (využití některých doplňkových systémů, např. inerciální nebo pozemní systémy) • Autonomní monitorování integrity (Receiver Autonomous Integrity Monitoring – RAIM) • Standardy a certifikace pro přijímače, chipsety, antény a další zařízení • Testování přijímačů • Standardy pro testování zařízení • Patentovaná řešení jednotlivých výrobců • Vhodné umístění antény (pro stacionární aplikace)
Pozemní segment	• Fyzická ochrana a informační bezpečnost • Redundantní geograficky vzdálené lokality • Záložní (HW i SW) řešení

Doplňkové systémy	• Inerciální senzory • Určení polohy s využitím Wifi nebo mobilních dat • SBAS a další augmentační systémy • Pseudolity • Pozemní systémy pro DGPS a RTK • Oscilátory pro aplikace využívající přesný čas a synchronizaci
Záložní systémy	• eLoran • Oscilátory a atomové hodiny pro aplikace využívající přesný čas a synchronizaci • PNT cloud
Kritická infrastruktura	• Zákonem definovat kritickou infrastrukturu • Nastavení požadavků na systémy KI – možnost zachovat provoz po určitou dobu (s využitím záložních systémů), požadavky na přesnost, definice dalších ukazatelů výkonnosti a monitorování jejich účinnosti • Plány a strategie pro případ výpadku GNSS nebo útoku na systém GNSS (nastavení procesů)
Uživatelé	• Rozšíření povědomí o hrozbách, slabých místech, dopadech a možnostech monitorování a reportování • Vytvoření národní databáze kritických uživatelů používajících OS GNSS • Nastavení rolí a zodpovědných autorit • Nastavení požadavků na systém například formou KPI • Pravidelný audit zařízení a systémů
Rámcové programy a R&D	• Studie • Vývoj nových technologií a inovace • Ověřovací pilotní projekty

Tabulka 5: Přehled opatření

Některá vybraná opatření jsou více rozepsána v následujících podkapitolách. Jedná se o:

- právní opatření a opatření na politické úrovni,
- rámcové programy a R&D,
- opatření proti interferenci,
- využití více konstelací GNSS,
- využití více frekvencí GNSS,
- augmentační satelitní systémy,
- záložní pozemní systém eLoran,
- monitorování a detekce RF interference,
- testování.

9.2.1 Právní opatření a opatření na politické úrovni

Právní opatření musí odpovídat aktuálnímu vývoji hrozeb a musí zabezpečit ochranu signálu GNSS s důrazem na kritickou infrastrukturu. Počet případů interference neustále narůstá a jejich uskutečnění je stále jednodušší. Současně dochází k nárůstu dostupných informací o závislosti kritické infrastruktury na systémech GNSS v jednotlivých zemích. Proto je nutné předpokládat, že v budoucnosti dojde k útokům na signál GNSS s cílem přerušit provoz kritické infrastruktury. Jednotlivé státy a nadnárodní organizace by měly mít **dostupné plány a strategie pro případ výpadku GNSS** nebo útoku na systém GNSS.

Mezi základní opatření patří zákonné definování kritické infrastruktury, identifikace jejích nedostatků z hlediska přijímání signálů GNSS a návrh záložních řešení. Taktéž by mělo dojít k **vytvoření národní databáze kritických uživatelů používajících OS GNSS** a k nastavení rolí a zodpovědných autorit. Cílovým stavem je poznání všech prvků a uživatelů kritické infrastruktury závislých na signálech GNSS a vytvoření záložních řešení.

Těmto procesům se již delší dobu věnuje americká vláda (Department of Homeland Security, DHS), která nejprve vypracovala studii nesoucí název ,,National Risk Estimate: Risk to U. S. Critical Infrastructure from Global Positioning System Disruptions“ [16] (volně přeloženo se jedná o rizika americké kritické infrastruktury plynoucí z přerušení služby GPS) a v současnosti přijala zákon ,,National Defense Authorization Act (NDAA) for 2018“, ve kterém ukládá povinnost pro Ministerstvo obrany, dopravy a vnitřní bezpečnosti vytvořit technologickou demonstraci záložního systému pro GPS. Také žádá o začlenění signálů evropského Galilea a japonského QZSS do přijímačů Ministerstva obrany.

S budováním systému Galileo a jeho uvedením do provozu se evropští politici začali intenzivněji věnovat problematice využití vesmírných navigačních technologií. V následujícím textu je uveden přehled právních a politických dokumentů, které se dotýkají oblasti Galilea a kritické infrastruktury. U vybraných dokumentů je uvedena také citace.

- Nařízení Evropského parlamentu a Rady 1285/2013/EU ze dne 11. prosince 2013 o **zřízení evropských systémů družicové navigace a jejich využití** a o zrušení nařízení Rady (ES) č. 876/2002 a nařízení Evropského parlamentu a Rady (ES) č. 683/2008 [17],
- Směrnice Rady 2008/114/EU ze dne 8. prosince 2008 o **určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu** [18],
- Pracovní dokument SWD(2013)318 o novém přístupu k programu ochrany evropské kritické infrastruktury (a new approach to the European Programme for Critical Infrastructure Protection – Making European Critical Infrastructure more secure) [19],
- Směrnice Evropského parlamentu a Rady 2016/1148/EU ze dne 6. července 2016 o **opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii** [20],
- 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 Směrnice 2014/65/EU o trzích a finančních nástrojích [21]: Článek 50 – Synchronizace obchodních hodin,
- Společné sdělení Evropskému parlamentu a Radě – **Společný rámec pro boj proti hybridním hrozbám**, 6.4.2016 [22]:

  *„Opatření č. 8: V kontextu nové kosmické strategie a evropského obranného akčního plánu navrhne Komise **posílit odolnost vesmírných infrastruktur proti hybridním hrozbám**, zejména případným rozšířením působnosti pozorování a sledování vesmíru tak, aby do ní byly zahrnuty hybridní hrozby, dále přípravu příští generace GovSatCom na evropské úrovni a **použití systému Galileo u kritických infrastruktur, jež jsou závislé na časové synchronizaci**.“,*

- Usnesení Evropského parlamentu ze dne 8. června 2016 o **vesmírných kapacitách evropské bezpečnosti a obrany** (2015/2276(INI)) [23].

Nad rámec těchto opatření, která se týkají hrozeb spíše na obecné úrovni, se právo zaměřuje také na boj proti konkrétním hrozbám. Tabulka 6 podává přehled například o tom, jak se různé státy a EU staví k problematice rušiček

Rušičky	USA	Rusko	Čína	EU
Výroba	ilegální	ilegální	ilegální	různé, dle států
Prodej	ilegální	ilegální	ilegální	ilegální
Export	ilegální	ilegální	ilegální	různé, dle států
Nákup	nedefinováno (spotřebitelský import ilegální)	ilegální	ilegální	ilegální
Vlastnictví	legální	nedefinováno	nedefinováno	ilegální
Používání	ilegální	ilegální	ilegální	ilegální

Tabulka 6: Zákaz rušiček v jednotlivých regionech světa (zdroj: [24])

Jednotlivé evropské státy přistupují v rámci své legislativy k jammerům různě, v některých státech je ilegální už jejich vlastnictví, v jiných je ilegální jejich používání, avšak vlastnictví je povoleno. Na základě průzkumu Electronic Communications Committee (ECC CEPT) [46] je vlastnictví povoleno např. v Maďarsku, Srbsku, Estonsku, Černé hoře nebo Švýcarsku. Tato zpráva se také věnuje prodeji jammerů v jednotlivých státech a zjišťuje kdo je v jednotlivých zemích odpovědný za ochranu rádiového spektra a monitoring rušení. V České republice se této oblasti věnuje ČTÚ, který má na svých webových stránkách následující vyjádření:

„Používání zařízení pro zabránění komunikace GSM a GPS (rušiček) v České republice

Zařízení pro zabránění komunikace GSM a GPS (rušičky – „jammery“) nelze v České republice provozovat ani uvádět na trh. Jakékoli vysílání za účelem zabránění komunikace je v rozporu s ustanovením § 100 odst. 1 zákona č. 127/2005 Sb., o elektronických komunikacích, v rozporu s požadavky na efektivní využívání rádiového spektra, na ochranu výkonu práv oprávněných provozovatelů veřejné telekomunikační sítě, jakož i na ochranu uživatelů veřejné telekomunikační služby, a proto je provoz takového zařízení v ČR nepřípustný. Za využívání kmitočtů, pro jejichž využívání je třeba oprávnění k využívání rádiových kmitočtů podle § 17 odst. 1 zákona o elektronických komunikacích, bez tohoto oprávnění, uloží Český telekomunikační úřad (dále jen „Úřad“) právnické nebo podnikající fyzické osobě pokutu do 20 000 000 Kč, fyzické osobě pak pokutu do výše 100 000 Kč. Podle ustanovení § 74 odst. 3 zákona o elektronických komunikacích dá Úřad podnět orgánu, v jehož kompetenci je dozor nad uváděním přístrojů na trh (Česká obchodní inspekce), aby zakázal nebo omezil uvádění na trh nebo stáhl z trhu rádiová zařízení, která způsobují škodlivou interferenci existujících služeb elektronických komunikací nebo by způsobovala škodlivou interferenci plánovaných služeb elektronických komunikací v kmitočtových pásmech využívaných na území České republiky.“

Kromě zákonné ochrany RF spektra proti jammingu je nutné vytvoření prostředků na identifikaci a potrestání pachatelů způsobujících interferenci. Monitorování a detekci interferencí signálu GNSS se věnuje kapitola 9.2.8.

V oblasti časování a synchronizace je vhodné zmínit také dokument „Best Practices for Improved Robustness of Time and Frequency Sources in Fixed Locations“ vydaný americkým DHS [25]. Jedná se o doporučení určená především firmám, které instalují a spravují T&S systémy. V dokumentu je zmíněno, že systémy, které mají nastaveny přísné limity pro přesnost určení času a frekvence, často využívají právě GPS časové přijímače. Jednotlivé kapitoly tohoto doporučení se věnují například situacím co dělat, když dojde k výpadku GPS nebo přijímač hlásí alarm, a také pojednávají o umístění antény a doporučují vhodné typy antén a kabelů. Dále je věnována pozornost také dalším zdrojům času, například NTP a atomové hodiny.

Dalším dokumentem věnujícím se časování a synchronizaci je „Time Distribution Alternatives for the Smart Grid“ vydaný americkým National Institute of Standards and Technology (NIST) [26], který rozpracovává alternativy GPS pro zabezpečení časové synchronizace v elektrických sítích a stanovuje budoucí požadavky a žádané parametry těchto systémů. Mezi příklady alternativ patří Enhanced Loran (eLoran), Enhanced WWVB, Wide Area Precision Time Protocol (PTP) a jiné.

9.2.2 Rámcové programy a R&D

Ze strany EK probíhá a v nedávné minulosti probíhala řada inciativ na budování opatření:

- Tabulka 7 – významné evropské projekty týkající se různých opatření zmírňujících zranitelnost aplikací využívajících GNSS,
- Tabulka 8 – projekty s tématem kritické infrastruktury a časování a synchronizace.

Projekt	Program	Popis
Standardisation of GNSS Threat reporting and Receiver testing through International Knowledge Exchange, Experimentation and Exploitation (STRIKE3)	Horizont 2020	Projekt STRIKE3 si klade za cíl standardizaci systémů, procesů a rozhraní pro reporting rušení GNSS a testování přijímačů. V rámci projektu proběhne řada vývojových prací, které mají vést k pokročilým demonstrátorům a prototypům. Projekt začal v únoru 2016 a potrvá 36 měsíců.
Detection, Evaluation and Characterization of Threats to Road Applications (DETECTOR)	FP7	Projekt DETECTOR měl za cíl vytvořit prototyp levného řešení pro detekci a charakterizaci rádio-frekvenční interference a zvýšit využívání GNSS v kritických dopravních aplikacích. Software a hardware byl testován v laboratořích i polních podmínkách a ve všech případech byl schopen spolehlivě detekovat a charakterizovat celou řadu typických rušiček a posoudit jejich možný dopad na služby GNSS. Projekt probíhal od ledna 2012 do září 2013.
Trusted multi-application receiver for trucks (TACOT)	FP7	Program TACOT vyvinul důvěryhodný modul GNSS pro dodávání informací o PNT včetně indikace důvěryhodnosti. Modul měří a analyzuje konzistenci informací. Projekt probíhal od září 2012 do září 2014.
Authenticated Time and Location for Location Based Application and Services (ATLAS)	FP7	V rámci projektu ATLAS bylo vyvinuto několik inovací pro speciální servery a přijímače GNSS pro autentizované aplikace integrující nové koncepty, robustní polohovací algoritmy a bezpečnostní protokoly. Projekt probíhal od února 2010 do srpna 2011.

Precise and secUre autoMative trAcking (PUMA)	FP7	Hlavním výstupem projektu PUMA byl prototyp palubní jednotky (OBU), který má implementované anti-spoofingové opatření. V případě jammingového nebo spoofingového útoku je OBU schopná rekonstruovat pravou cestu vozidla a upozornit na tuto událost kontrolní centrum. Projekt probíhal od prosince 2009 do června 2011.
Application of Turbo Techniques to GNSS Receivers (TGR)	FP6	Projekt se zaměřoval na navrhování inovativních algoritmů inspirovaných z partnerských znalostí turbo technik pro řešení úlohy "time to first fix" (TTFF) a přesnosti určování polohy v prostředí s velkým množstvím odražených signálů (multipath). Projekt probíhal od února 2006 do května 2007.
Quantification of the potential threat to Galileo from man-made Noise sources (QGN)	FP6	Tento projekt učinil přesné měření radiového hluku v řadě prostředí a tato data byla zpracována do volně dostupných zpráv. Jsou to například Zpráva o vlastnostech rušení, Zpráva popisující očekávané umělé zdroje hluku, které by mohly mít vliv na přijímače Galileo, Výsledky měření či Zpráva o charakteristikách umělého hluku Galileo. Projekt probíhal od dubna 2006 do srpna 2007.
Management of Galileo Interferences and Counter Measures (MAGIC)	FP6	Cílem projektu MAGIC bylo definovat a ověřit technické řešení, které umožní provozovatelům služby Galileo nabízet systém bez interferencí. Zaměřoval se na tři témata: detekce, izolace a zmírňování, která byla definována, prostudována a hodnocena prostřednictvím teoretického přístupu, softwarových simulací a reálnými zkouškami. Projekt probíhal od srpna 2005 do listopadu 2007.

Tabulka 7: Rámcové a vědeckovýzkumné programy zabývající se opatřeními proti hrozbám GNSS

Projekt	Program	Popis
Robust EGNSS Timing Services	Horizont 2020	Výstupem je kompletní definice robustní časové služby ověřené testováním, včetně využití skutečných signálů Galileo. V rámci projektu byl vybudován plán pro standardizaci v oblasti robustních časových služeb. Výsledný systém je založen na synchronizaci zařízení s využitím systémového času Galileo bez potřeby signal-in-space.
DEMonstrator of EGNSS services based on Time Reference Architecture (DEMETRA)	Horizont 2020	Projekt měl za cíl definovat a navrhnout provozní architekturu, nastavit provozní prostředí pro pilotní aplikace, vyhodnotit dopady na infrastrukturu Galileo a podpořit poskytování časových služeb Galileo. V rámci projektu byly vyvinuty tzv. demonstrátory využívající čas kosmických technologií.
Prototype timing receiver for critical infrastructure	Fundamental Elements (GSA)	Cílem projektu bude vytvořit levný časový přijímač využívající systém Galileo, který bude schopný určit čas na velmi přesné úrovni a bude mít implementovaná opatření proti jammingu. ITT bude vyhlášen.
PRS Added Value for Timing & Synchronisation	Specifická smlouva (DG-GROW)	Výsledkem projektu má být vyhodnocení výkonnosti služeb Galileo a testování odolnosti s využitím služby PRS.

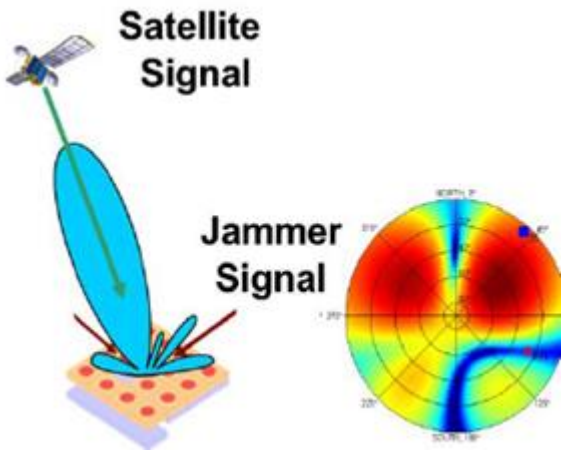
Tabulka 8: Rámcové a vědeckovýzkumné programy pro téma kritické infrastruktury a přesného času a synchronizace

9.2.3 Opatření proti jammingu

Existuje několik druhů opatření proti jammingu a další rušivé interferenci. Úspěšnost jednotlivých opatření závisí mimo jiné na síle interference. **V extrémních případech** (např. teroristický, vojenský či jiný silný jamming) **většina opatření ztrácí na účinnosti**. Uživateli poté zpravidla nezbývá nic jiného, než využít jiný zdroj získání PNT, než je GNSS.

K existujícím opatřením proti jammingu patří:

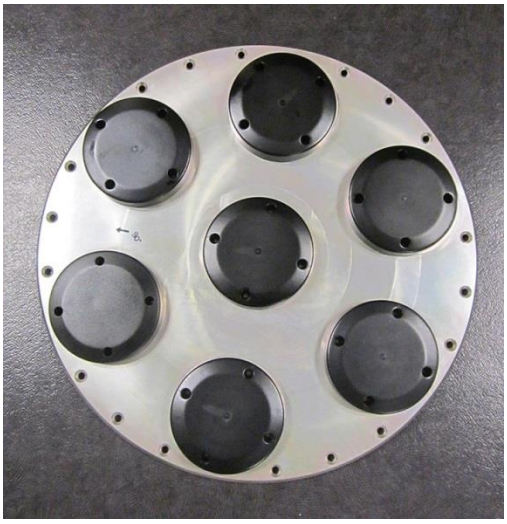
- **odstranění interference v přijímači:,**
  - detekce, např. pomocí Jammer-to-noise power ratio (J/N),
  - filtrování na front-endu,
  - metoda Code/Carrier Tracking Loop,
  - pokročilé metody zpracování signálu,
- **využití hybridních přijímačů**, např. inerciální senzory,
- **odstranění/zmírnění interference pomocí antény**, např.:
  - tzv. beamforming techniky – vynulování interferujícího signálu pomocí tzv. nulling antény (označováno také jako null-steering antény, popřípadě směrové antény, Obrázek 4),
  - metoda CRPA (Controlled Radiated Pattern Antenna, Obrázek 5),
- **využití více frekvencí** (nicméně rušení ve více frekvencích způsobí výpadek přijímaní informací PNT, více viz samostatná podkapitola Využití více frekvencí GNSS),
- **enforcement** – monitorování spektra, detekce a lokalizace pachatelů nebo zdroje rušení (více viz samostatná podkapitola Lokalizace rušení).



Obrázek 4: Schéma zamítnutí nežádoucí interference (zdroj: Technische Universität Braunschweig)

Speciální **antény jsou dnes asi nejspolehlivějším opatřením proti jammingu**, nicméně náklady na jejich pořízení bývají vysoké (až stovky tisíc korun) a zároveň využití těchto speciálních antén není schůdné pro každou aplikaci. V případě kritických aplikací, kde je možnost anténu použít, může posloužit jako účinné **opatření nejen proti jammingu, ale také proti vybraným případům spoofingu a pro zamítnutí odražených signálů**.

V případě T&S aplikací vyžadujících velice přesnou časovou informaci **se využití některých speciálních antén (např. CRPA) nedoporučuje** vzhledem k tomu, že technologie těchto antén jsou stále ve vývoji a zpracování signálu by mohlo mít negativní vliv na přesnost určení času (může například docházet k proměnlivému zpoždění signálu).



Obrázek 5: CRPA anténa (zdroj: [27])

Vzhledem k neúčinnost jakýchkoli opatření při extrémních případech rušení je vhodné věnovat pozornost také záložním systémům, které by měly být zdrojem PNT při výpadku GNSS. Mezi záložní systémy patří např. systém eLoran (kapitola 9.2.7).

9.2.4 Využití více konstelací GNSS

V blízké době bude možné **přijímat signál z více než 120 dostupných satelitů GNSS**. Uživatelé tak budou potenciálně moci přijímat signály z 50 družic najednou. Viditelnost tolika družic přináší řadu výhod, jakými je například **odmítnutí nekvalitních měření** (neexistující přímá viditelnost, odražené signály, nízká elevace apod.).

Pro výrobce produktů GNSS, poskytovatele služeb i uživatele samotné přináší multi-GNSS benefity v podobě **dostupnosti více satelitů, zvýšené přesnosti a robustnosti trackingu** (především v náročných prostředích, jako je městská zástavba nebo hustá vegetace) **a zmírnění určitých hrozeb**.

Na druhou stranu existují určité **pochybnosti, například interference jednotlivých signálů a přílišné navýšení prahu radiofrekvenčního hluku**, což může být pro určité přijímače problematické. Pro výrobce přijímačů GNSS to rovněž přináší nutnost implementovat strategie výběru (odmítnutí) družic.

9.2.5 Využití více frekvencí GNSS

Pro méně až středně přesná měření je dostačující využití jedné frekvence. U přesných měření bývá často nutné využití více frekvencí. Používání více frekvencí GNSS je totiž nejefektivnějším způsobem pro **odstranění ionosférických chyb** při výpočtu polohy, čímž dojde k výraznému zpřesnění měření. Ionosférická chyba ovlivňuje různé frekvence signálu GNSS odlišně, takže porovnáním zpoždění dvou signálů, například L1 a L2, může přijímač opravit dopady ionosférické chyby.

Významnou vlastností využití více frekvencí je **zvýšená imunita vůči interferenci**. Například pokud se vyskytuje interference v pásmu L2, multifrekvenční přijímač stále sleduje signály v pásmech L1 a L5 pro zajištění aktuální pozice.

Při použití více frekvencí je také možné **rychleji a spolehlivěji vyřešit ambiguity**.

Mezi další přínosy **nově zaváděného signálu L5** patří skutečnost, že bude využíván všemi systémy GNSS a SBAS, je vzdálenější od L1 a L2, a tudíž dojde ke zmírnění rizika jammingu, poskytuje lepší korekci ionosférické chyby, spolehlivější odstranění chyby z odrazu a nabízí vyšší sílu přijatého signálu.

Pro kritické aplikace, kde je vyžadována redundance a odolnost vůči jammingu, je využití multifrekvenčních přijímačů bezpochyby vhodnou volbou. Nicméně při silném zdroji rušení ve více frekvencích tohle opatření ztrácí účinek.

9.2.6 Augmentační satelitní systémy

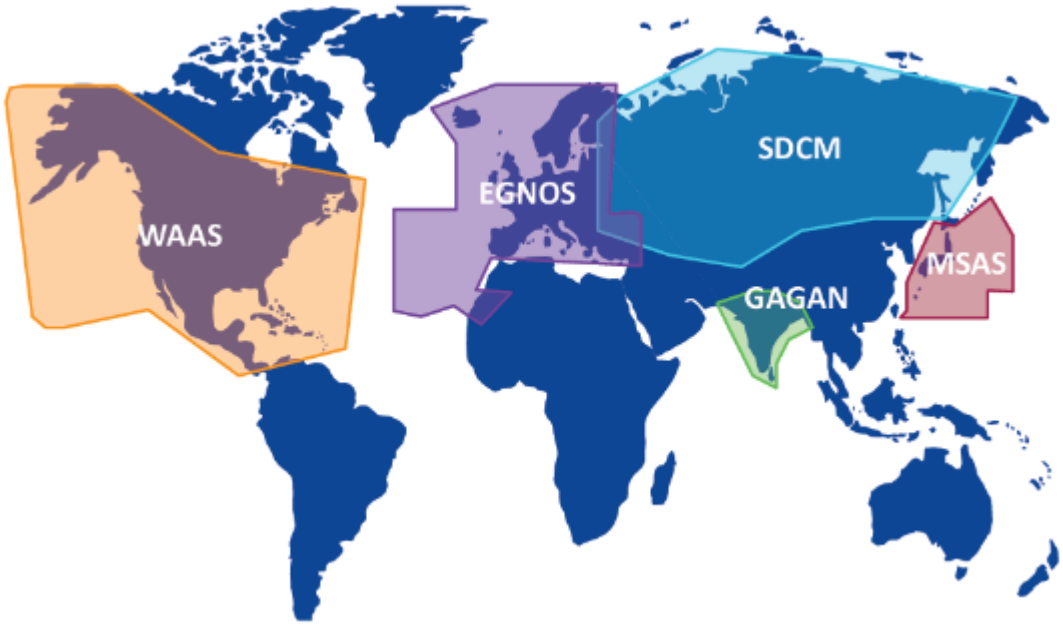
Augmentace globálních navigačních systémů (GNSS) je metodou vylepšování výkonosti navigačních systémů, například **integrity, kontinuity, přesnosti nebo dostupnosti, s využitím externích informací**.

Satelitní augmentační systémy (Satellite Based Augmentation System, SBAS) slouží pro podporu kontinentální či regionální augmentace pomocí geostacionárních družic, které vysílají augmentační informace. Hlavním cílem SBAS je zajištění integrity, ale zároveň zlepšení přesnosti určení PNT.

Pozemní infrastruktura zahrnuje přesně zaměřené senzorové stanice, které přijímají signály z primárních družic GNSS a Central Processing Facility (CPF), kde se počítají integrační, opravná a tzv. GEO ranging data tvořící signál SBAS. Geostacionární družice SBAS následně přenášejí signál k uživatelům.

Augmentační informace obsahují korekce a integritu pro pozici satelitů, chybu satelitních hodin a chyby způsobené zpožděním signálů při průchodu ionosférou. Pro chyby způsobené troposférou využívají uživatelé model troposférického zpoždění.

Několik států zavedlo svoje vlastní satelitní augmentační systémy (Obrázek 6). Území Evropy a severní Afriky pokrývá evropský systém **EGNOS** (European Geostationary Navigation Overlay Service). USA mají vlastní systém **WAAS** (Wide Area Augmentation System). Japonsko je pokryto systémem **MSAS** (Multi-functional Satellite Augmentation System) a Indie spustila svůj SBAS program **GAGAN** (GPS and GEO Augmentation Navigation), který pokrývá indický subkontinent. Další programy jsou ve vývoji, např. ruský systém **SDCM** (System for Differential Corrections and Monitoring), čínský **SNAS** (Satellite Navigation Augmentation System), **WADGS** (Wide Area Differential Global Positioning System) Jižní Koreji a státy jižní a střední Ameriky pracují na systému **SACCSA** (Solución de Augmentación para Caribe, Centro y Sudamérica).



Obrázek 6: Geografická působnost systémů SBAS (zdroj: GSA)

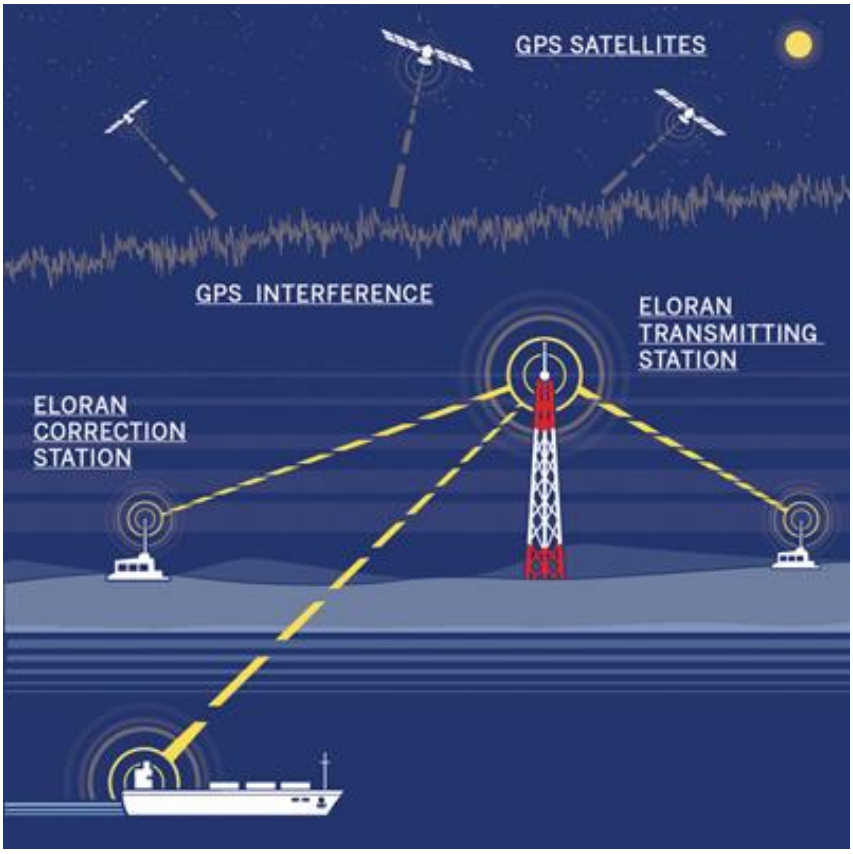
Služby poskytované systémem EGNOS

- **Základní služba** (Open Service – OS) – základní signál, poskytován zdarma, služba spuštěna 1. října 2009. Volně dostupná služba pro podporu všeobecně volně rozšířených aplikací GNSS.
- **Služba "kritická" z hlediska bezpečnosti** (Safety of Life service – SoL) – rozšířený signál zahrnující informaci o integritě, která během několika vteřin oznámí uživateli snížení kvality signálu pod určitou mez. Tato služba byla certifikována 2. března 2011 a oficiálně zpřístupněna pro využití při navigaci především v letecké dopravě. Je certifikována z hlediska mezinárodních standardů Mezinárodní organizace pro civilní letectví (ICAO) a pravidel Otevřeného nebe (Open Sky Regulations) a byl k ní vydán Service Definition Document (SDD). Tento dokument popisuje očekávaný výkon a schopnosti systému pro podporu aplikací SoL na bázi EGNOS.
- **Komerční služba** "EGNOS Data Access Server" (**EDAS**) – služba EDAS šíří data EGNOS v reálném čase prostřednictvím internetu a rozšiřuje tak možnosti pro šíření signálu EGNOS. EDAS by měl být součástí komplexního systému CDDS (Commercial Data Distribution System) [28].

9.2.7 Záložní pozemní systém eLoran

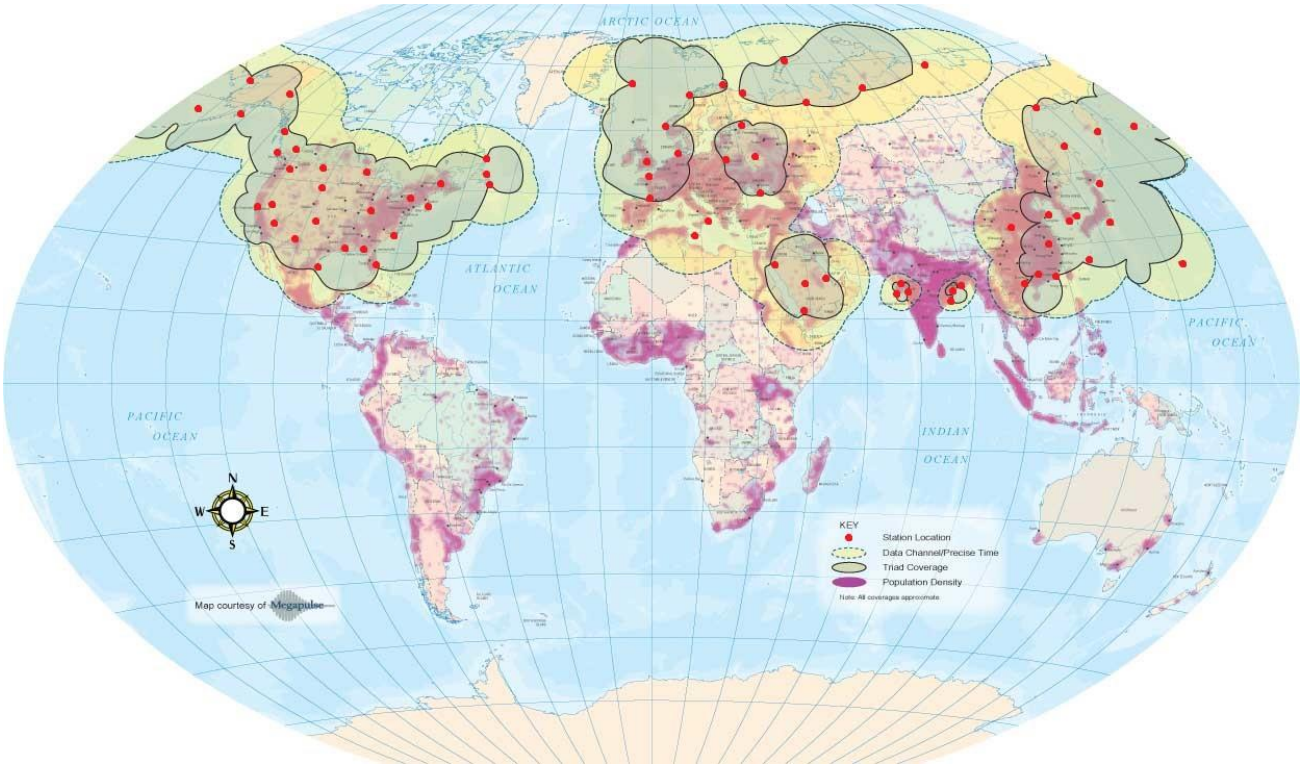
Loran je pozemní navigační systém původně vybudovaný během 2. světové války. Systém je založený na vysílání velice silného signálu (přibližně tisíckrát silnějšího než signál GPS) o nízké frekvenci (přibližně deset tisíckrát menší než signál GPS), který počítal i s autentifikací signálu, tedy opatřením proti spoofingu.

Základ infrastruktury tvoří vysílací věže, které mohou být rozmístěny až stovky kilometrů od sebe (Obrázek 7).



Obrázek 7: eLoran jako záloha GPS (zdroj: [30])

V současné době se buduje a testuje obnovená verze nazvaná **eLoran** (enhanced Loran). eLoran je hlavní technickou modernizací systému Loran-C, ale může být poskytovaný stejnými vysílacími věžemi používanými pro Loran-C. Systém eLoran funguje podobně jako GPS nebo jiné družicové systémy, jedná se však o doplňkový a nezávislý pozemní systém. Důležité je, že funguje při výrazně vyšších úrovních výkonu než družicové systémy, a proto je výrazně těžší ho rušit nebo spoofovat. Signály rušení musí mít větší sílu než signály, které se pokoušejí rušit, a vysílání velmi silného výkonu při nízkých frekvencích a dlouhých vlnových délkách eLoranu by vyžadovalo velmi vysoké věže. eLoran dosahuje polohové přesnosti v horizontální rovině v řádech jednotek až desítek metrů (předpokládaná polohová přesnost eLoran na základě údajů UrsaNav je při inicializační fázi pod 100 m a při plné operační fázi pod 10 m). Chybí mu ale možnost určení vertikální polohy. eLoran může sloužit také jako zdroj velice přesného času (předpokládaná časová přesnost eLoran na základě údajů UrsaNav je při inicializační fázi +/- 500 ns a při plné operační fázi +/- 50 ns).



Obrázek 8: Rozmístění stanic eLoran (zdroj: [32])

O nasazení systému se stále vedou politické debaty. Na jeho zavedení pracuje například Jižní Korea, která se potýká s jammingem ze strany Severní Koreji, a řada iniciativ na podporu eLoran vychází také z Velké Británie. Vzhledem k hrozbám výpadku GPS nařídila v roce 2017 americká vláda Ministerstvu dopravy vybudování funkčního systému eLoran, přestože v roce 2010 označila systém Loran-C za nadbytečný a zpomalila jeho vývoj.

9.2.8 Monitorování a detekce interference

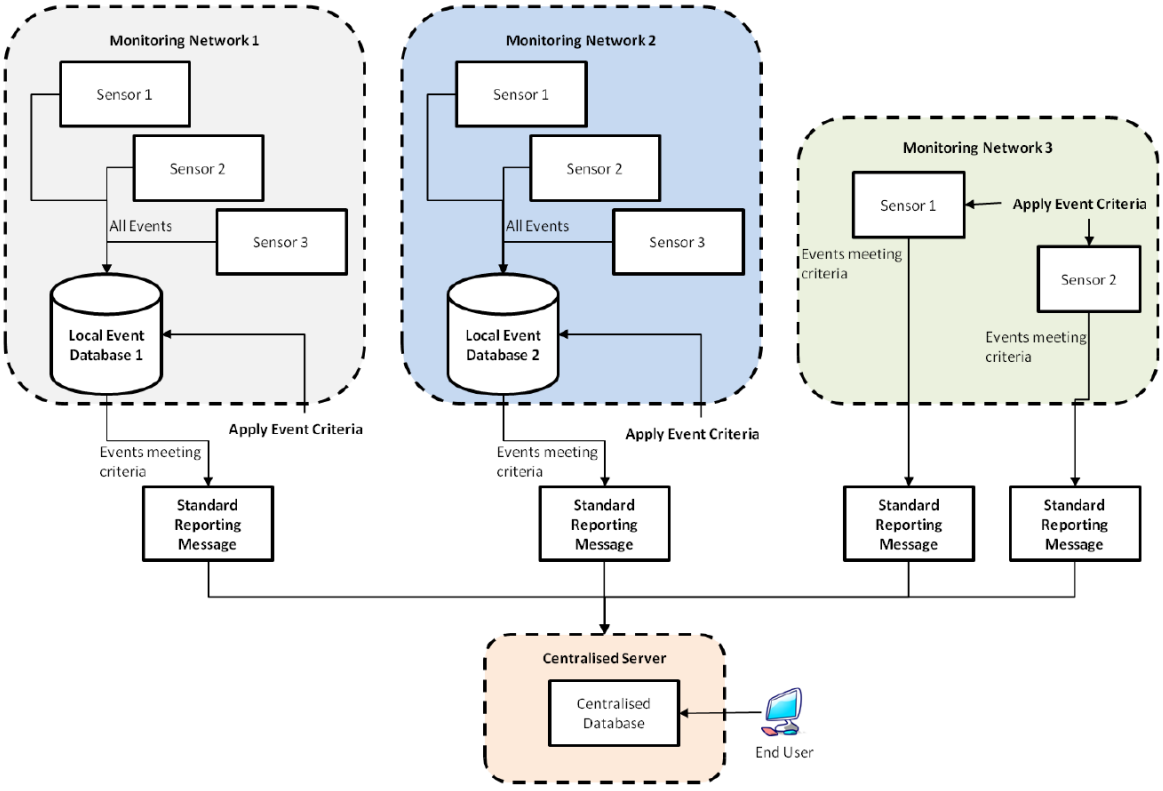
Pro pochopení úrovně hrozby v reálném prostředí a vyvinutí účinných opatření proti interferenci je žádoucí systematicky monitorovat případy interference a sdílet výsledky se zúčastněnými stranami. Existuje několik různých typů detekčních zařízení, které je možné použít pro detekci interference a vytvořit z nich komplexnější systémy. V současnosti už proběhly nebo ještě probíhají projekty a monitorovací kampaně, jejichž cílem je monitorování případů interference a jejich následná analýza.

Přestože tyto typy lokálního monitorování mohou být efektivní při sledování a ochraně konkrétní lokality nebo větší oblasti, schopnost zkombinovat výsledky různých detekčních zařízení a monitorovacích sítí a získat širší pochopení úrovně ohrožení je omezené z několika důvodů. Za prvé různá detekční zařízení a monitorovací sítě vykazují různé hodnoty a statistiky o událostech rušení, a proto není vždy jednoduché kombinovat výsledky. Za druhé různé typy detekčních zařízení mají odlišné detekční algoritmy a prahové hodnoty, protože jsou navržené pro různé účely a různé typy detekčních zařízení instalované na stejném místě mohou hlásit zcela odlišné počty

událostí. Proto je potřeba **vytvořit standardy monitorování a detekce případů interference**, aby byla zajištěna kompatibilita měření a **umožnit analýzy zjištěných případů interference**. Standardizaci monitorování a sdílení výsledků se věnuje probíhající evropský projekt STRIKE3 [6].**Vytvoření standardů je prvním krokem pro komplexní monitorování a detekci případů interference**.

Na základě detekovaných případů interference je možné zjistit reálné ohrožení aplikací využívajících signály GNSS v konkrétních oblastech, resp. typech oblastí (zařízení u letišť, dálnic, elektráren, atd.) a přijmout opatření na jejich ochranu a zabezpečení. Detekované signály interference je také vhodné využít při testování přijímačů, díky čemuž uživatel získá důležité poznatky o chování zařízení v reálných podmínkách.

Vytvoření monitorujícího systému by mělo být jedním z hlavních opatření, přičemž jak bylo již několikrát zdůrazněno, při výběru lokalit by **měly být upřednostňovány lokality s kritickou infrastrukturou**, jejichž výpadek by měl na chod společnosti největší dopad. Takový systém by odhalil reálné hrozby pro systémy kritické infrastruktury a umožnil jednotlivé systémy na ně připravit.



Obrázek 9: Návrh systému monitorovaní a sdílení případů interference (zdroj: [6])

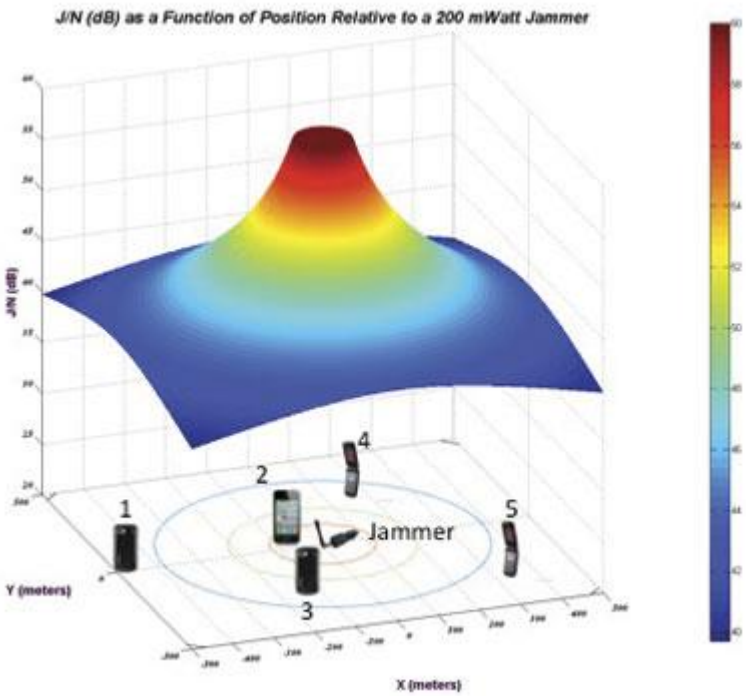
9.2.8.1 Lokalizace rušení

Jedna z možností, jak bojovat proti rušení, je jeho **lokalizace**. Vzhledem k faktu, že rušičky vysílají relativně silný signál, může být snadné rušení zaznamenat, nicméně lokalizace takového přístroje je náročnější úlohou. Existuje několik metod, jakými je možné lokalizaci provést.

Základní metodou lokalizace zdroje rušení je využití **ručních přístrojů**. Tyto přístroje, např. CTL3520 od společnosti Chronos (Obrázek 10), umožňují pomocí indikačních diod určit směr, odkud rušící signál přichází. Tato metoda je bohužel omezena pouze na určení směru, nikoliv polohy rušičky [33].

Obrázek 10: Ruční detektor a lokalizátor rušení (zdroj: [34])

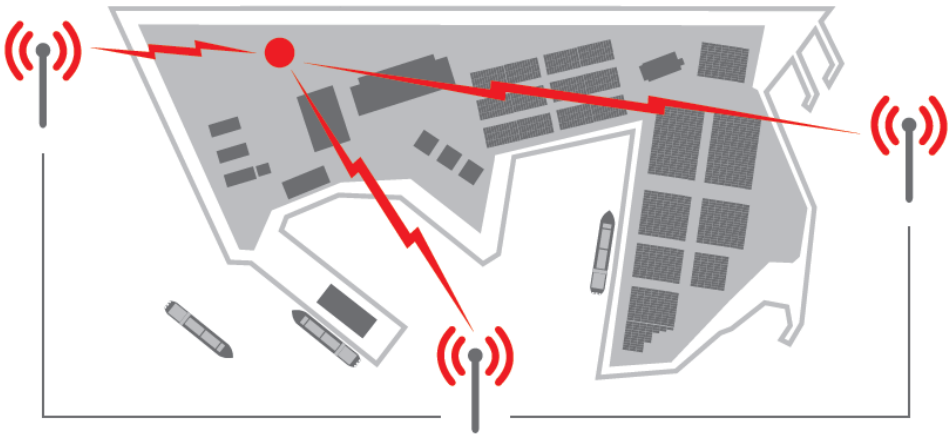
Prozatím ve fázi konceptu je druhá metoda, **crowdsourcingový projekt detekce a lokalizace rušení za pomocí mobilních telefonů a uživatelů J911** (Obrázek 11). Na základě online dat o síle rušícího signálu, která budou sbírána uživateli pomocí mobilních telefonů, by bylo možné přesně určit polohu rušičky. Během workshopu, který proběhl v roce 2015, bylo ale mimo jiné shledáno, že v úvodní provozní fázi projektu by bylo výhodnější využít pro sběr dat vysílače mobilních operátorů namísto mobilních telefonů [35].



Obrázek 11: Detekce a lokalizace rušení za pomoci mobilních telefonů (zdroj: [66])

Třetí metoda pro lokalizaci rušiček je výstavba **komplexních systémů**, které budou neustále sbírat data a v centrálním objektu určovat polohu rušičky. V nejjednodušším případě takové systémy

mohou využívat pouze **stacionární senzory** (Obrázek 12), například řešení Signal Sentry 1000 od společnosti Exelis [36].



Obrázek 12: Zjednodušený princip lokalizace rušení pomocí stacionárních senzorů (zdroj: [37])

V jiném případě je kromě využití stacionárních senzorů možné využít i **mobilní senzory**, které mohou být instalované například v automobilech. Takovýmto systémem je například systém GIMOS, který provozuje společnost pro řízení letového provozu v Německu (DFS – Deutsche Flugsicherung GmbH). Americký systém JLOC využívá kombinaci stacionárních senzorů a přenosných měřících zařízení, ale do budoucna počítá i s využitím **senzorů umístěných na bezpilotních letadlech** a jiných mobilních prostředcích [38].

V českým prostředí probíhá projekt **Systém pro odhalování nezákonného rušení GNSS signálu v blízkosti strategické infrastruktury,** jehož cílem je vývoj systému schopného odhalovat rušení „jamming“ a „spoofing“.

Mezi základní charakteristiky systému navrhovaného v rámci zmíněného projektu patří:

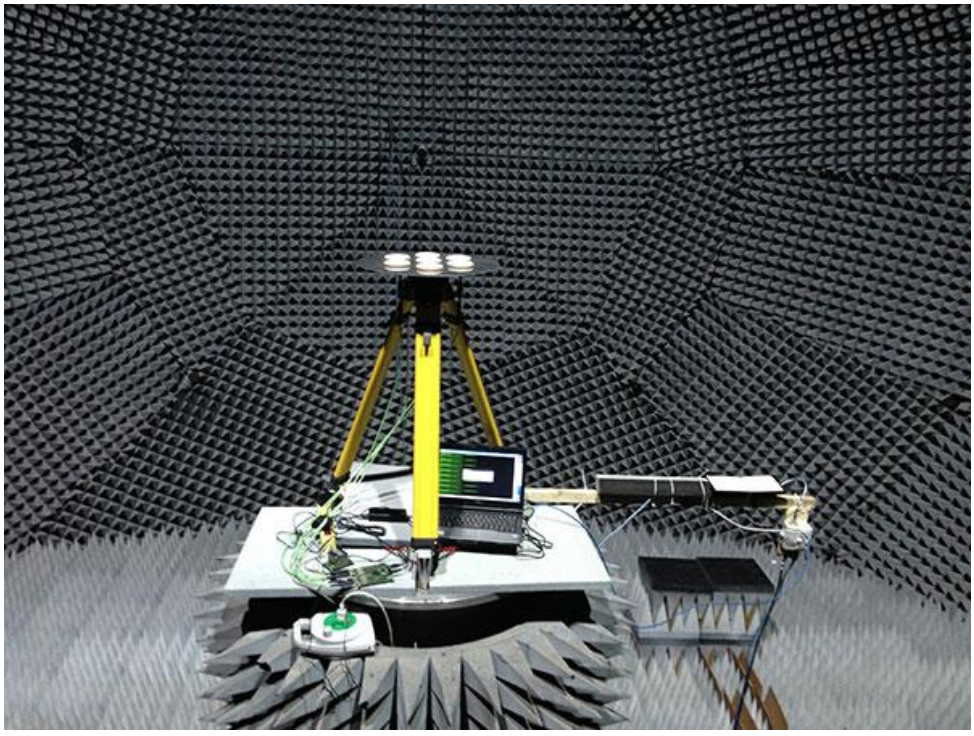
- Systém má využívat technologii softwarového rádia (SDR) z důvodu velké flexibility, která umožní snáze aplikovat nové metody detekce a lokalizace zdrojů rušení, tj. update i upgrade systému dle požadavků klientů a změn požadavků na funkce v průběhu nasazení.
- Systém má podporovat dva principy zaměřování rušení, a to metodu měření doby příchodu signálu ToA (Time of Arrival), případně rozdílu doby příchodu signálu DToA (Difference in Time of Arrival) a směrové zaměřování založené na interferometrickém principu.
- Systému má být v první fázi realizován pro kmitočtové pásmo GPS L1 a Galileo E1 s tím, že hardware má být navržen univerzálně tak, aby byl jednoduše modifikovatelný i pro další GNSS kmitočty.
- Systém má pokrývat kmitočtové pásmo s jistou rezervou tak, aby bylo možné detekovat signály i v tzv. přechodovém pásmu GNSS přijímače.
- Systém umožní klasifikaci rušivých signálů do kategorií: i) úzkopásmové nekorelované rušení (úzkopásmový jamming), ii) širokopásmové nekorelované rušení (širokopásmový jamming), iii) korelované rušení (semi-spoofing), iv) inteligentní rušení (spoofing).
- Systém umožní stanovovat míru rizika, s jakou rušivé signály mohou ovlivňovat funkci GNSS přijímačů.

9.2.9 Testování

Jedním ze základních opatření proti většině hrozeb je **znalost vlastních systémů a zařízení**, především přijímačů GNSS, do té míry, aby bylo možné ohodnotit rizika plynoucí z jednotlivých hrozeb a odolnost vlastních systémů proti těmto hrozbám.

Každá hrozba je svým způsobem unikátní. Je tomu jak u hrozeb přírodních, nezáměrných, tak u těch záměrných, jako jsou například jamming a spoofing. Každá rušička vydává rušení s „vlastním“ RF podpisem. Zároveň každý přijímač zvládá přítomnost rušení jinak v závislosti na implementovaných opatřeních a aktuálních podmínkách vnějšího prostředí, například na počtu viditelných družic.

I tak je ale možné poměrně věrohodně **nasimulovat útoky vybraných hrozeb** na konkrétních přijímačích. Hrozby, jako je rušení, je možné posbírat **monitorováním spektra GNSS** například v blízkosti zařízení kritické infrastruktury, na vytížených dopravních tazích nebo na dalších místech, kde se očekává přítomnost zdrojů rušení. Následnou analýzou RF vzorků vzniknou tzv. I/Q soubory reprezentující jednotlivé incidenty rušení. Ty je poté možné v laboratoři, např. v **anechoické komoře** (Obrázek 13), přehrát a sledovat, jak testované zařízení reaguje.



Obrázek 13: Anténní soustava během testování v anechoické komoře (zdroj: [39])

V současné době se při testování přijímačů příliš nebere v potaz účinek směrových antén (dnes jedno z nejúčinnějších opatření proti jammingu) – na otestování se totiž jedná o složitou úlohu. Je potřeba teprve vyvinout nové testovací metody, které spolehlivě nasimulují schopnosti směrových antén a následně je implementovat do standardizovaného testování.

Pomocí testování je možné vyhodnotit závažnost jednotlivých hrozeb na provoz přijímačů a systémů závislých na GNSS. **Testování by proto mělo být jedno ze základních opatření proti**

hrozbám systémů GNSS, aby uživatelé znali svá rizika a mohli implementovat případná další opatření a záložní systémy. Na základě testování přijímačů bude také možné shromáždit podklady pro vytvoření standardu pro robustní přijímače. Metodice testování přijímačů se podrobně věnuje následující kapitola.

10 Testování GNSS přijímačů proti jammingu

Testování přijímačů a komplexní vyhodnocení výsledků je zásadní pro poznání vlastností zařízení a jeho schopností odolat různým druhům interference. Na základě výsledků je možné rozpoznat hrozby pro konkrétní přijímač a aplikaci a následně přijmout adekvátní kroky pro zabezpečení cílového systému.

V ideálním případě by měli testování zařídit již samotní výrobci zařízení, nicméně často si testování objednávají až koncoví uživatelé nebo provozovatelé jejich systémů. Výhodou testování na straně koncového uživatele je možnost otestovat konkrétní zařízení a jeho integraci s dalšími systémy různých výrobců. Koncový uživatel může zohlednit konkrétní aplikaci systému a vybrat scénáře testování, které nejlépe vystihnou reálný provoz a hrozby, které se v něm vyskytují.

Některé aplikace vyžadují krátký Time-to-first-fix (TTFF), jiné potřebují pracovat se slabými signály v obtížném prostředí, zatímco další mají vyšší nároky na absolutní přesnost výsledné polohy.

Jednou z nejdůležitějších součástí návrhu testovacího prostředí systému GNSS je tedy co možná nejpřesnější definice parametrů, které mají hlavní vliv na správné fungování zařízení v praxi.

10.1 Specifikace testování

Tato kapitola obsahuje specifikace testování, ve které jsou uvedeny typy testovaných jednotek, parametry testů, typy interferujících signálů a popis testovacích scénářů. Metodika zohledňuje poznatky vycházející z evropského projektu STRIKE3 [6], jehož cílem je vytvoření základů pro integrované a harmonizované monitorování hrozeb na nadnárodní úrovni a také zavedení metodiky testování přijímačů vůči zaznamenaným hrozbám.

10.1.1 Testované typy přijímačů

Testování, jeho nastavení a parametry úzce souvisí s testovaným typem přijímače. Jednotlivé typy přijímačů jsou určené pro různorodé aplikace a mají tedy odlišné vlastnosti a parametry. Avšak metodika testování by měla být co nejuniverzálnější, aby bylo možné testovat široké spektrum přijímačů. Z tohoto důvodu jsou přijímače na základě jejich vlastností rozdělené do dvou hlavních skupin, pro které metodika uvádí testovací scénáře:

- profesionální přijímač GNSS,
- běžný spotřebitelský přijímač.

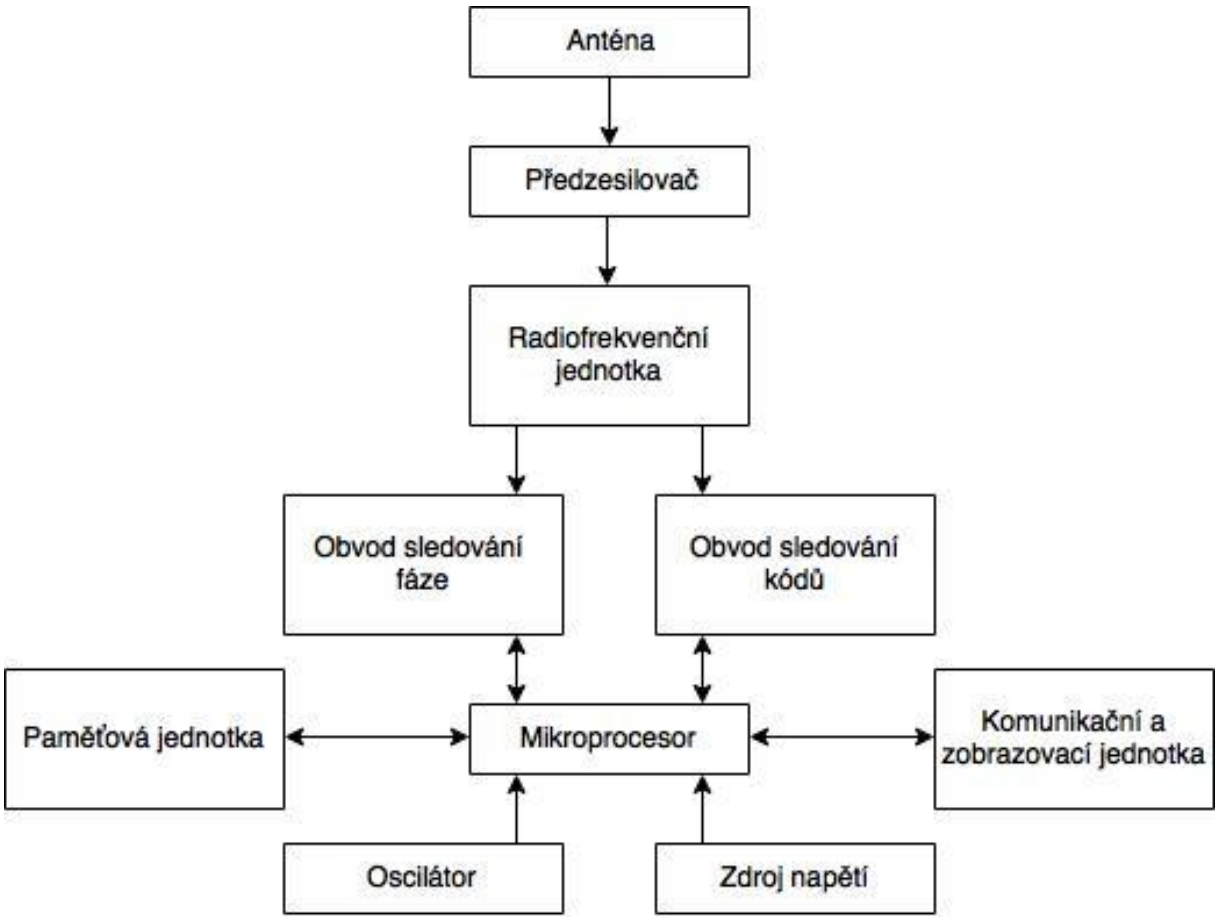
Profesionální přijímače jsou obvykle dostupné za vyšší náklady, jsou optimalizované pro přesná měření a určování polohy a často dokáží pracovat s několika různými frekvencemi (L1&E1, E5a&L5) a konstelacemi (GPS, Galileo, GLONASS, BDS). Jsou využívané především v geodetických aplikacích, kde je potřebná vysoká přesnost určení polohy.

Běžné spotřebitelské přijímače jsou obvykle dostupné za nižší náklady, s nižší spotřebou energie a jsou optimalizované pro dostupnost signálu odpovídající jejich provoznímu prostředí – např. přijímače využívané v automobilových navigacích jsou optimalizované pro pohyb v náročném městském prostředí a dokáží poskytnout informaci o poloze i za ztížených podmínek (byť na úkor

kvality této informace). Obvykle využívají jednu frekvenci (L1), i když jsou dostupná i zařízení s vícero konstelacemi. Tento typ je dnes hojně využívaný v různých odvětvích, například v automobilovém průmyslu nebo na trhu pro řízení strojů.

Mezi další rozšířené typy přijímačů se řadí přijímače integrované do jiných zařízení (např. jako součást mobilního telefonu) a přijímače přesného času, které jsou určené pro speciální aplikace využívající přesný čas systémů GNSS. Tyto dva typy přijímačů zpravidla využívají celou řadu dalších senzorů (např. akcelerometr, gyroskop), záložních komponent (např. oscilátor) či jiných zdrojů pro určení polohy nebo času (wifi, protokoly PTP a NTP). Použití těchto typů přijímačů a jejich případné testování je natolik specifické, že v této certifikované metodice nebyly zvažovány. Typy přijímačů zvolené pro tuto metodiku, tj. běžný spotřebitelský a profesionální, můžeme považovat za reprezentativní, pokud je potřebné vyhodnotit a porovnat vliv vybraných hrozeb (konkrétně vliv radiofrekvenční interference – RFI) na vybranou kategorii uživatelského zařízení.

Základními bloky přijímače GNSS jsou anténa s předzesilovačem, radiofrekvenční jednotka, moduly sledování signálu, komunikační a zobrazovací jednotka, frekvenční oscilátor a zdroj napětí. Hlavní moduly profesionálního, geodetického přijímače a jejich vzájemné vazby jsou znázorněny na Obrázek 14.



Obrázek 14: Schéma přijímače GNSS (zdroj: [40])

Doporučuje se detailně nastudovat technickou dokumentaci testovaného přijímače, která je důležitým zdrojem informací o jeho jednotlivých funkcích, parametrech a výkonu. Dokumentace by měla obsahovat jak technický popis přijímače, tak specifikaci protokolu. Na základě dokumentace je možné zjistit účel přijímače, vhodné provozní prostředí, provozní režimy, hardwarové a softwarové opatření proti rušení (implementace různých typů filtrů), podporované konstelace a frekvence, formát výstupních dat, popis protokolu a jiné.

10.1.2 Signály GNSS

Při testování přijímačů je nutné rozhodnout, jakým způsobem bude signál GNSS poskytnut. Jednou z možností je přehrání reálně nahraného signálu. Tento přístup se může jevit jako výhodnější, protože přijímač bude přijímat signál nahraný v reálném prostředí, avšak má mnoho nedostatků. U nahraného signálu GNSS hrozí, že bude znehodnocený rušením nebo vícenásobným odrazem a nebude mít dostatečnou kvalitu; tím by bylo do testování vnášené rušení, které neumíme kontrolovat a ovlivnilo by konečné výsledky. Velkou nevýhodou je také nemožnost testování budoucích signálů a konstelací (např. plná konstelace Galilea). Pokud je žádoucí použít reálně nahraný signál GNSS, je potřeba tento signál očistit od vlivů prostředí, jakými jsou vícenásobný odraz či možné rušení.

Druhou možností je využití simulátoru konstelací GNSS. Tento simulátor poskytuje efektivní způsob testování přijímačů a systémů, které jsou na nich závislé. Simulátor GNSS vytváří dynamické prostředí modelováním pohybu družic a přijímače, vlastností signálu, atmosférických a jiných efektů, čímž simuluje reálné prostředí. Přijímač zpracovává tyto generované signály stejným způsobem, jakým by přijímal reálné signály GNSS. Simulátor GNSS umožňuje následující [41]:

- Generuje signál konstelací GNSS pro jakoukoliv polohu a čas. Scénáře pro různé oblasti s rozdílným časem v minulosti, současnosti nebo budoucnosti mohou být testovány bez nutnosti opuštění laboratoře.
- Modelování pohybu vozidla obsahujícího přijímače GNSS, jako jsou letadla, lodě a pozemní vozidla. Scénáře pohybu vozidel pro různé trajektorie a v různých oblastech mohou být testovány bez reálné potřeby pohybu testovaného přijímače.
- Modelování různých efektů ovlivňujících výkon přijímače, jako jsou atmosférické podmínky, vícenásobný odraz, blokování signálu, vlastnosti antény a interferujících signálů. Možnost testování více kombinací a úrovní těchto efektů.

Hlavní výhodou simulátoru GNSS je možnost opakování testování. Pokud jsou použité signály nahrané v reálném prostředí, nedokážeme ovládat všechny parametry a dynamicky je měnit podle potřeby. Využití nahrávacího a přehrávacího zařízení je vhodný doplněk k simulátoru GNSS a je zásadní v případech, kdy není důležitá úplná znalost testovacího signálu, ale spíše podmínky reálného prostředí. Přehrávací zařízení je ideální pro testování v komplexním prostředí, kde je kladen důraz na různé efekty ovlivňující signál GNSS.

V případě simulátoru GNSS je generovaný signál vždy identický, a čímž umožňuje konzistenci, opakovatelnost a porovnatelnost naměřených výsledků. Avšak je nutné mít na paměti, že navzdory simulacím, které se co nejvíce snaží přiblížit signálům v běžném prostředí, se nejedná o signály reálného prostředí.

10.1.3 Frekvence / Konstelace

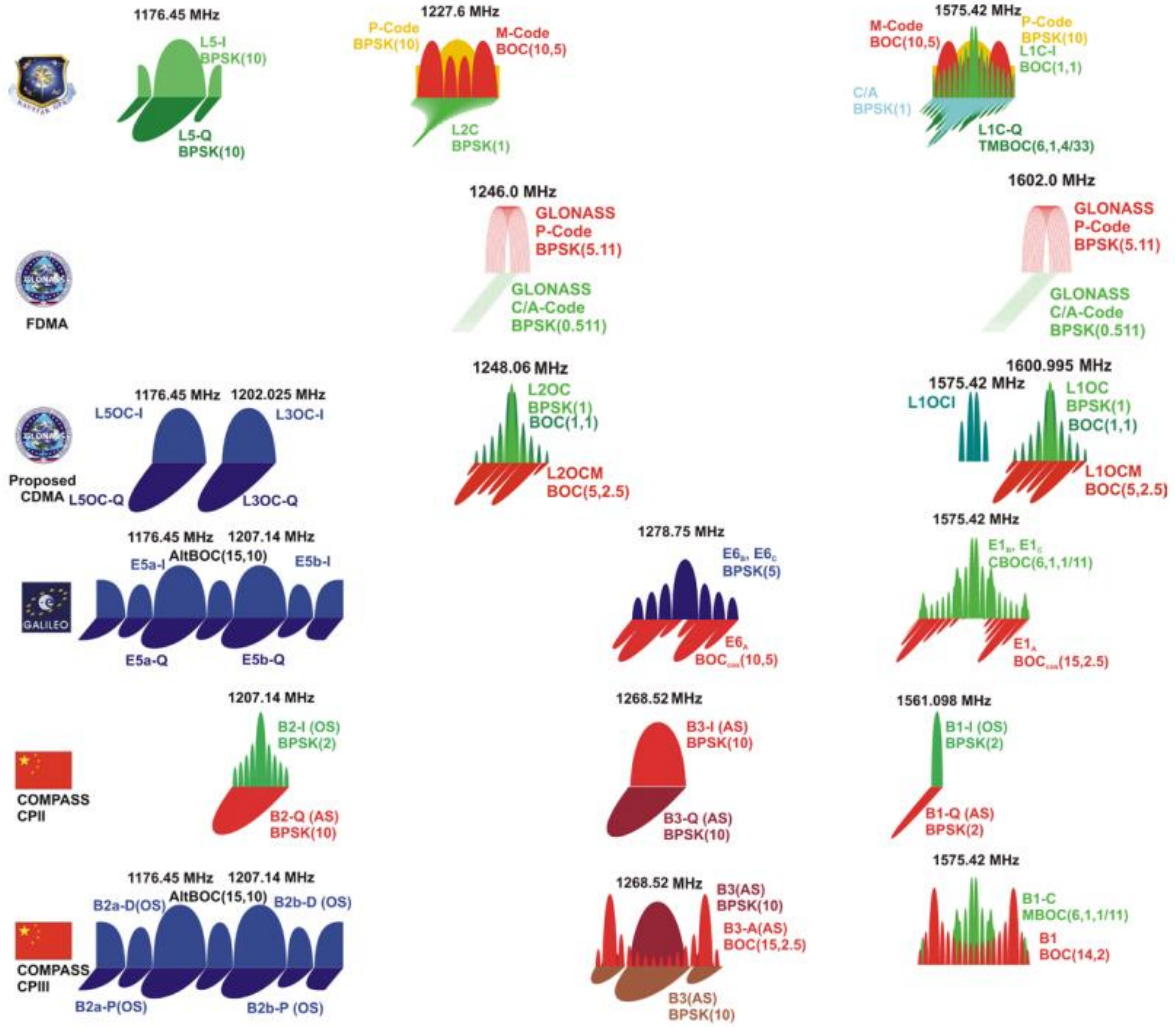
Hlavním doporučením pro přijímače se schopností pracovat s více konfiguracemi a frekvencemi je testování, které plně pokryje schopnosti daného přístroje. Testování v každém případě musí pokrýt kanál L1, který je u mnoha přijímačů jediným kanálem, avšak u mnohých přijímačů, především profesionálních, jsou podporované i jiné konstelace a frekvence. Minimálně by měla být testována každá frekvence samostatně, doporučené je ale komplexnější testování na všech frekvencích zároveň, které ukáže celistvý obraz o chování přijímače a může odhalit závislost zpracování jedné frekvence na jiné.

Tabulka 9 a Obrázek 15 níže zobrazují frekvenční pásma používaná v každé konstelaci spolu s centrální frekvencí a úrovní výkonu každého signálu, které se musí dosáhnout při vstupu do přijímače po dobu testu.

Konstelace	Střed frekvence (MHZ)	Min. síla (dBm)
GPS L1, L1C	1575,42	-128,5 (C/A) -127 (L1C)
GPS L2, L2C	1227,6	-134,5 -> 131,5[1]
GPS L5	1176,45	-127,9
GLONASS L1	1598,0625 – 1605,375	-131
GLONASS L2	1242,9375 – 1248,625	-137
GLONASS L3	1202.025	-128
GALILEO E1 (OS)	1575,42	-127
GALILEO E5a	1191,795	-125
GALILEO E5b	1176,45	-125
GALILEO E6 (CS)	1278,75	-125
QZSS L1	1575,42	-128,5 (C/A) -127 (L1C) -131 (SAIF)
QZSS L2	1227,6	-130
QZSS LEX	1278,75	-125,7
QZSS L5	1176,45	-127,9
BEIDOU B1	1575,42	-133
BEIDOU B2	1207,14	-133
BEIDOU B3	1268,52	-133

Tabulka 9: Základní vlastnosti konstelací (zdroj: [6])

[1] Zvýšení výkonu s novějšími družicemi



Obrázek 15: Frekvenční pásma GNSS (zdroj: [42])

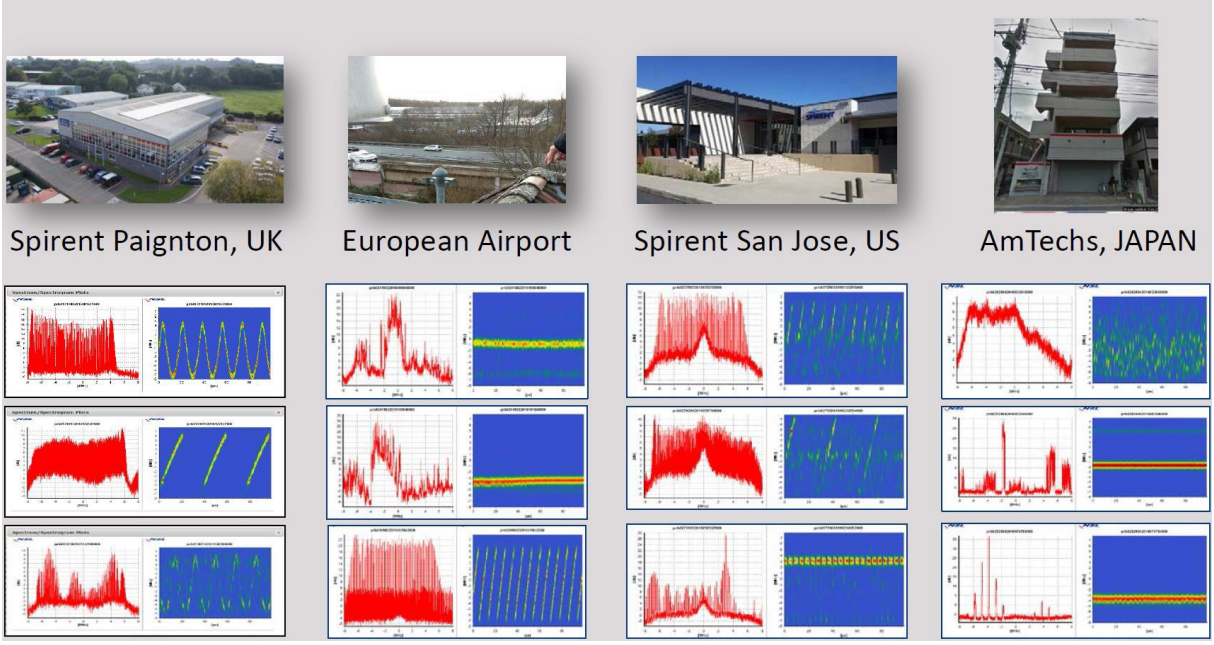
10.1.4 Typy interference

Zdroj elektromagnetického záření může rušit slabý signál GNSS a tým způsobit pokles kvality výsledné informace o PNT, kterou uživatel ve výsledku získá. Kromě **přírodní interference**, ke které dochází například šířením signálu napříč atmosférou, existuje také interference **nepřírodního původu** – tedy vycházející z okolních elektronických zařízení. Nejedná se pouze o vysílače, ale o elektroniku jakéhokoliv druhu**.** V případě **záměrné interference** se používají speciální zařízení (rušičky) vysílající energii v pásmech odpovídajících frekvenčním pásmům GNSS.

K interferenci signálů obvykle dojde tehdy, když přijímač přijímá současně dva signály, které se jen minimálně liší svou frekvencí, respektive fází. Obvyklým výsledkem interference je neschopnost přijímače zpracovat užitečný signál. Interference představuje pro komunikační a navigační systémy velký problém [43].

Jednou ze záludností jammingu je fakt, že uživatel ho jako takový nedovede identifikovat. Jeho přijímač sice začne podávat nepřesnou informaci (nebo přestane zcela fungovat), ale není možné

s jistotou říci, že se jedná právě o vliv rušičky. To dovede s určitou mírou spolehlivosti prokázat až sofistikovaný detektor a následná analýza zachyceného RF spektra (viz obr. níže).



Obrázek 16: Příklady zachycených incidentů interference, nalevo RF podpis v zasaženém frekvenčním spektru, napravo spektrogram znázorňující závislost frekvence na času (zdroj: Spirent)

Zařízení pro jamming, obecně označované jako jammery, rušičky nebo také tzv. Personal Privacy Device (PPD), jsou dnes na trhu snadno dostupné a jejich cena je relativně nízká.

K nejběžnějším zařízením patří rušičky s napájením z cigaretového adaptéru (rušící zpravidla pouze jednu frekvenci), a multifrekvenční, které ruší více frekvencí. V případě vícefrekvenčních rušiček jde ale zřídkakdy o rušení více frekvencí GNSS, ale jedná se spíše o rušení na jiných frekvencích – nejčastěji GSM, 3G, LTE, wifi. Co se týče rušení GNSS, většina dostupných rušiček ruší pouze frekvenci GPS L1. Pouze výjimečně je rušička schopna rušit i ostatní frekvence GPS. Tato situace odráží skutečnost, že většina aplikací GNSS, proti kterým jsou rušičky namířené, využívá právě GPS L1. S nástupem vícefrekvenčních GNSS přijímačů v těchto aplikacích se dá očekávat nástup odpovídajících rušiček. Přidat další frekvenci pro rušičku není po technologické stránce žádná překážka.

Obrázek 17: „Základní“ rušičky nižší cenové kategorie (zdroj: www.signalprofi.cz)

Uživatelé, často motivováni přínosem ve prospěch jich samotných, si nejsou vědomi, že použitím rušičky ruší nejen například „své“ sledovací zařízení, ale všechna zařízení v provozním dosahu rušičky. Neuvědomují si tak plně následky svého konání.

Obecně je ale celkem obtížné stanovit a kvantifikovat různé případy **motivace k jammingu**, protože pachatel není znám. Stejně tak není známa ani technologie, kterou pro jamming použil.

Obecně se dá říci, že se jedná o následující kategorie:

- obrana státu, terorismus a vojenské konflikty,
- testování (záměrně vyvolaný jamming vedoucí k nezáměrné interferenci),
- kriminální činnost,
- ochrana soukromí a další osobní důvody.

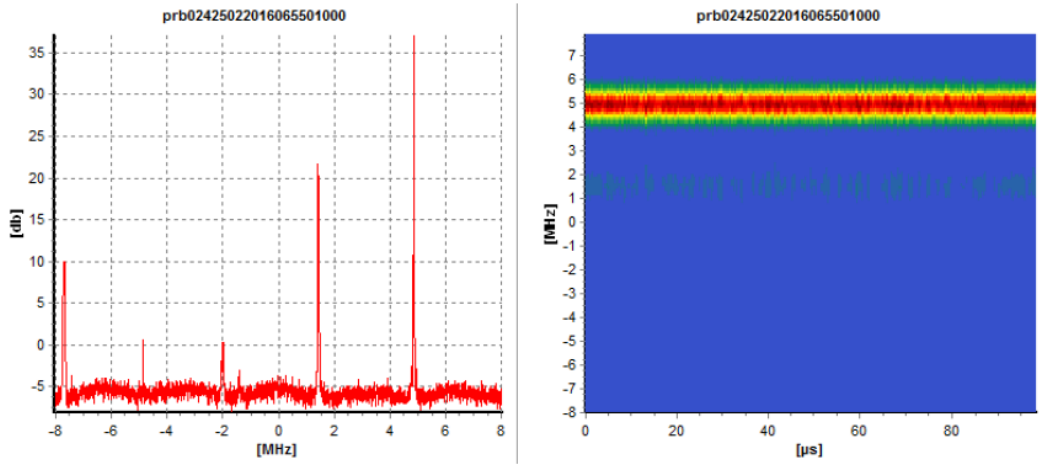
10.1.5 Typy interferujících signálů

Kromě výkonu a počtu frekvenčních pásem se také rušičky klasifikují **podle metody, kterou k interferenci přistupují**. Popis těchto metod je nad rámec této studie, nicméně v základním rozdělení se jedná o úzkopásmové (narrow band) a širokopásmové (wide band). Nejčastěji je u rušiček používaná metoda **chirp**. Pokud detekovaná interference prokazuje známky typické pro tento druh signálu, dá se prakticky s jistotou říci, že se jedná o záměrnou interferenci.

Detailně se rozboru signálů záměrné interference věnuje technický článek [44]. Uvádíme zde **rozdělení rušivých signálů** převzaté z tohoto článku:

- **Narrowband Continuous Wave Interference** – frekvence signálu je neměnná (Obrázek 18),
- **Chirp Interference** – frekvence opakovaně přejíždí přes definované frekvenční pásmo (na spektrogramu se tato vlastnost projevuje periodicky se opakující intenzitou signálu na dané frekvenci, Obrázek 19); tento signál je nejvíce typický pro běžně dostupné rušičky,
- **Gaussian Noise Jammers** – jedná se o širokopásmové rušení napříč celým frekvenčním pásmem vybraného systému GNSS; rušení založené na tomto signálu není možné v přijímači odstranit.

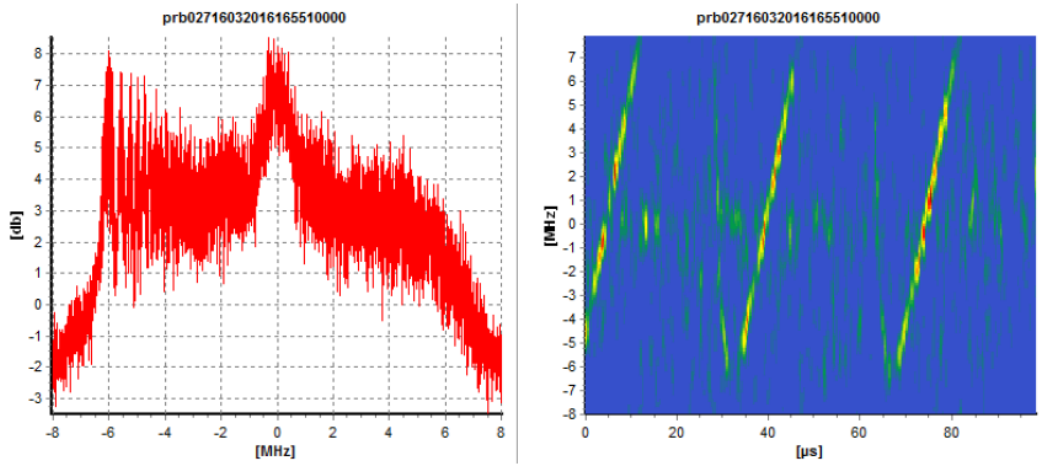
Location	Time	Duration (sec)
Near a small airport in Germany	06:55, 22 Feb. 2016	36



Classification	Potential RFI Source
Narrow band	Out-of-band, AM-modulated signal

Obrázek 18: Jeden z možných případů Narrowband Continuous Wave interference (zdroj: Spirent)

Location	Time	Duration (sec)
Near a motorway in CA, USA	16:55, 16 Mar. 2016	20



Classification	Potential Source
Pulsed Chirp Saw Tooth Up	Intentional Jammer

Obrázek 19: Jeden z možných případů chirp interference (zdroj: Spirent)

10.1.6 Proces a kritéria výběru hrozeb

Při testování přijímačů se většinou berou do úvahy interference, které používají různé typy syntetického signálu na monitorování chování přijímače a berou ohled na dopad takových hrozeb na jeho schopnost určit polohu nebo čas. Výhoda tohoto přístupu spočívá v tom, že různé přijímače mohou být na posouzení jejich odolnosti testované standardizovaným způsobem s využitím konkrétního vektoru hrozeb a je zabezpečeno kvantitativní vyhodnocení odolnosti. Nedostatkem takovýchto přístupů je, že nemusí být přímo spojené s reálnými hrozbami, které se vyskytují v provozním RF prostředí. Proto je vhodné využití zaznamenaných reálných ohrožení, které jsou doporučené i v metodice testování projektu STRIKE3. Je třeba zdůraznit, že využití syntetických i zaznamenaných hrozeb má své výhody a nevýhody a při zkoušce by měl být zvolen ten variant, který poskytne komplexnější testování GNSS přijímače vzhledem k jeho provozování v reálných podmínkách. V této kapitole zohledňujeme výstupy projektu STRIKE3 a věnujeme větší rozsah použití reálných hrozeb.

10.1.6.1 Použití reálných hrozeb

Účelem použití reálných hrozeb je otestovat přijímače proti rušivým signálům, se kterými se mohou reálně potkat během provozu. Takové testování má větší vypovídací hodnotu než testování proti syntetickému signálu, který bude mít významný vliv na výkon přijímače, ale bude generovaný pouze v laboratorním prostředí.

Nevýhodou však je, že detekce konkrétní události rušení – a charakteristik spojených s touto událostí (úrovně intenzity, trvání, atd.) – závisí na zařízení detekujícím interferenci, prahových hodnotách a poloze vzhledem ke zdroji rušení. Pokud je to možné, měly by se z tohoto procesu odstranit specifické aspekty místa / senzoru; tj. je to signál rušení, který je využitý na testování, a ne vlastnosti samotné události [6].

Z praktického hlediska to znamená, že:

- Musí být možné opakovat signál s vlastnostmi, které byly zjištěné v reálném prostředí (z hlediska centrální frekvence, frekvenční variace, rychlosti opakování impulzů, atd.).
- Musí být možné upravit úroveň výkonu interferenčního signálu, tj. opakovat signál testované hrozby při nižší nebo vyšší intenzitě, než jakou měl signál zjištěný v reálném prostředí.
- Musí být možné modifikovat trvání rušivého signálu, tj. opakování signálu testované hrozby s krátkým nebo delším trváním, než měla událost zjištěná v reálném prostředí.
- Musí být možné reprodukovat jen testovací signál rušení, tj. ignorovat samotný stav signálů GNSS (např. jaké signály se sledují, s jakou úrovní intenzity se signály sledují, výskyt vícenásobných odrazů nebo jiných chyb, atd.) v čase skutečné události.

Na splnění těchto cílů existují dva alternativní přístupy – parametrizace hrozeb a opětovné zpracování údajů ze souhrnných vzorků.

10.1.6.2 Parametrizace hrozeb

První možností používání skutečných hrozeb při testování je **parametrizace hrozeb**. V tomto přístupu se analyzuje skutečný podpis ohrožení a vybírají se parametry podpisu ohrožení (např.

centrální frekvence, frekvenční rozsah, časová změna frekvence, trvání impulzu, atd.). Parametry se potom používají na řízení generátoru signálů vektoru (VSG) v průběhu testování přijímače, tj. signál generovaný VSG je založený na parametrech reálných hrozeb [6].

Výhoda tohoto přístupu spočívá v tom, že typ signálu a charakteristiky interferenčních událostí (např. úroveň intenzity, trvání) mohou být dobře řízené pomocí VSG a může se vytvořit čistý opakovatelný signál na smíšení se signály GNSS. Avšak jelikož jde o syntetický signál, který je nějakým způsobem idealizovaný, nemusí správně reprezentovat nuance reálných interferenčních signálů – i když parametry na generování signálu testovací hrozby jsou založené na skutečných údajích.

10.1.6.3 Přehrání nahraných vzorků signálů rušení

Alternativním přístupem k parametrizaci signálu a přehrávání prostřednictvím VSG je **opětovné přehrání samotných vzorových dat**. Podpis digitalizované hrozby se načítá do zařízení, které je schopné přehrát vzorek a opakovaně spouštět nahrané vzorky. Amplitudové profily definované pro různé testy se potom aplikují na signál.

Výhodou tohoto přístupu je, že při komplexnějších hrozbách by mohl potenciálně poskytnout přesnější rekonstrukci detekované hrozby. Avšak aby bylo možné reprodukovat nahrané údaje a splnit požadavky na test, je potřeba zvážit několik faktorů. Za prvé údaje o surových vzorcích musí být zachycené s příslušnými charakteristikami, jinak nebude možné přesně replikovat signál interference.

Za druhé nahraný vzorek bude mít jen krátkou dobu trvání a vzorek se musí neustále opakovat, aby se umožnilo opakované přehrávání.

Za třetí údaje o nahraných vzorcích budou obsahovat satelitní informace (kódy PRN), stejně tak jako informace o interferenčním signálu, a proto se tyto informace musí odfiltrovat před přehráváním signálu tak, aby interferující signál neobsahoval satelitní informace GNSS.

10.1.6.4 Výběr hrozeb

Je nepraktické testovat přijímače na všechny zjištěné hrozby, kterých jsou monitorovací sítí detekovány tisíce. Proto je nutné vybrat ty hrozby, které jsou pro testování přijímačů relevantní.

Existuje několik možných přístupů při výběru hrozeb pro další testování, včetně výběru signálů s nejvyšším výkonem, nejběžnějších signálů, neobvyklých signálů, nebo těch, které mají největší vliv na GNSS.

Jednou z možných metod výběru hrozeb při testování přijímače je výběr takových, které jsou detekované s nejvyšší úrovní intenzity. Hlavní výhoda tohoto přístupu je v tom, že signály s vysokou intenzitou budou mít pravděpodobně velký vliv na schopnost přijímače určit polohu.

Avšak tento přístup má několik nevýhod. Za prvé přijatá úroveň intenzity interference závisí na mnoha faktorech, včetně charakteristik detekčního zařízení, vysílací intenzitě zdroje rušení, vzdálenosti interferujícího zařízení od detekčního a charakteru lokálního prostředí v detekčním zařízení. Proto nemůžeme provést výběr jen na základě intenzity interference, avšak je vhodné

zkombinovat tento přístup s jiným přístupem, který bude sloužit jako prvotní filtr pro snížení celkového počtu signálů, neboť vyřadí příliš slabé signály.

Další možnou metodou výběru hrozeb pro testování přijímače je výběr signálů, které se vyskytují nejčastěji. Tento přístup by musel zahrnovat nějaký druh parametrizace signálů a následné porovnání vlastností na identifikaci nejběžnějších typů – např. 5 nejběžnějších signálů různých kategorií (např. úzkopásmový, širokopásmový, chirp, atd.), nebo výběr signálů, které se nejčastěji vyskytují na rozdílných typech monitorovacích oblastí (např. letiště, dálnice, atd.) [6].

Je však třeba poznamenat, že nejčastější hrozby nejsou nutně ty, které budou mít největší vliv na určování polohy přijímačem. Kromě toho testování jen proti nejčastějším hrozbám nepomůže ochránit přijímač před nově vznikajícími hrozbami, dokud se nestanou rozšířené a do určité míry by mohly ovlivnit operace pro uživatele GNSS.

Navzdory svým nevýhodám by se tento přístup mohl ukázat jako užitečný pro testování proti těm hrozbám, se kterými se přijímač s největší pravděpodobností setká v reálném prostředí.

Poslední metodou výběru, o které se píše v této části, je výběr hrozeb založených na dopadu na výkon přijímače. Jsou zvolené ty signály interference, které mají největší dopad na schopnost přijímače určovat polohu. Výhodou je testování limitů přijímače.

Tuto metodu však komplikuje několik faktorů. Není vždy lehké a priori na základě charakteristiky signálu určit, jestli bude mít daný signál velký dopad na výkon přijímače, a proto identifikace signálů, které budou mít největší vliv (na stejnou přijatou úroveň intenzity), není snadná.

10.2 Architektura testů

Cílem této části je vytvořit **testovací architekturu** potřebnou na testování přijímačů v přítomnosti rušení RF, která je komplexní, opakovatelná a pokrývá hlavní typy přijímačů.

Navrhnutí dostatečně robustního testovacího prostředí je založené na **pěti hlavních faktorech** [45]:

- **Kontrola** – úplná a přesná kontrola všech důležitých parametrů signálu GNSS, interference a zařízení, např. postupné zeslabování intenzity signálu pro přesné nalezení hraniční hodnoty přijímače, při které ještě dokáže sledovat družice a určovat polohu.
- **Opakovatelnost** – bez ohledu na testovací scénář je potřeba zabezpečit opakovatelnost testování za stejných, předem definovaných podmínek. To znamená, že celé prostředí musí být totožné (ne jen geometrie družic, ale i atmosférické podmínky a interference), jinak není možné zabezpečit konzistenci výsledků měření výkonu přijímače a jejich porovnatelnost.
- **Flexibilita** – možnost vytvářet různé testovací scénáře s různými parametry, které otestují hranice výkonu přijímače a dokáží vytvořit podmínky, za kterých přijímač selže.
- **Pokrytí testy** – čím více jsou testovací prostředí a testovací scénáře reprezentativnější, tím větší jsou šance na správné fungování přijímače v prostředí, pro které je určený. Testování by mělo pokrývat všechny schopnosti přijímače.

- **Účinnost a efektivita** – i u jednoduchého přijímače je počet testovacích scénářů vysoký, a proto je třeba celý proces automatizovat. Tím se ušetří čas, náklady a zabezpečí se tím konzistence a porovnatelnost výsledků.

Na základě zmíněných požadavků jsou **hlavní prvky nastavení testů následující**:

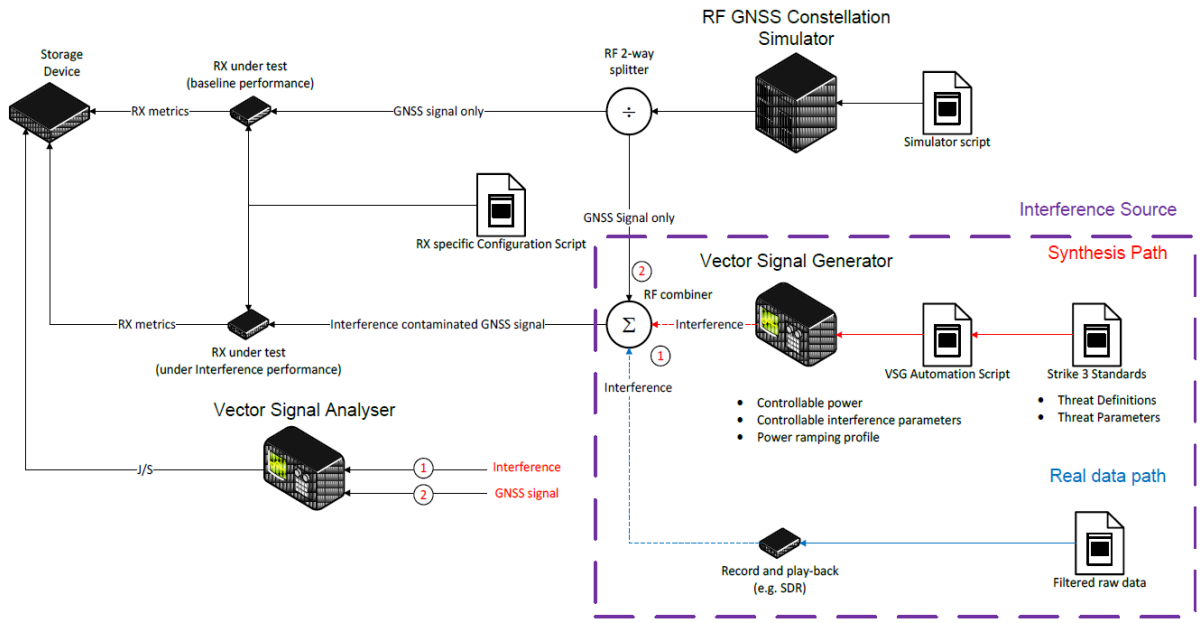
- Je vhodnější využít simulátor konstelací. Druhou možností je přehrání nahraných signálů GNSS přímo z oběžné dráhy; u tohoto postupu ale hrozí, že signály budou ovlivněné rušením nebo vícenásobným odrazem a nebudou pro testování dostatečně kvalitní.
- Pro testování přijímače se využívají signály rušení z reálných detekovaných událostí. Tato nahraná rušení mohou být implementována jako parametrizované reprezentace, které jsou naprogramované do generátoru signálů, nebo přehráváním zaznamenané interference.
- Simulátor GNSS, signály interference a konfigurace přijímače by měly být skriptované tak, aby se zabezpečila opakovatelnost testování.
- Všechny vybrané a sledované veličiny hodnotící výkon přijímače by měly být zaznamenané pro pozdější analýzu vůči použitým signálům GNSS a interference.
- Automatizace testování je žádoucí.

Nejdůležitější částí navrhování testovacího prostředí a scénářů je výběr parametrů, které mají největší vliv na výkon přijímače v reálném provozu. Některé aplikace potřebují co nejrychlejší určení polohy, přičemž na přesnost se neklade důraz, jiné naopak vyžadují co nejvyšší přesnost, zatímco další musí pracovat v prostředí s nízkou intenzitou GNSS signálů a vysokým šumem. Proto je nutné přesně definovat, pro jakou aplikaci bude přijímač určený a v jakém prostředí bude v provozu.

10.2.1 Testování běžného spotřebitelského přijímače

V testovacím prostředí, znázorněném na Obrázek 20, je signál GNSS generovaný prostřednictvím simulátoru GNSS. Výstup z generátoru je rozdvojený, aby bylo možné porovnat měření přijímače přijímajícího čisté nerušené signály GNSS s výsledky měření při přijímání signálu, do kterého bylo kontrolovaně přidáno rušení. Měření na základě čistého signálu představuje základ, vůči kterému jsou porovnávána měření signálu znehodnoceného interferencí. Tímto je dosažena porovnatelnost výsledků, protože do obou měření vstupuje stejně generovaný signál ve stejném čase [6].

Je možné vyměnit simulátor konstelací GNSS se záznamovým a přehrávacím zařízením pro signály GNSS, pokud simulátor není k dispozici. Uživatel ale musí zajistit, aby nahrávka byla kvalitní a nebyla znehodnocena rušením, vícenásobným odrazem apod.



Obrázek 20: Nastavení testů pro běžný spotřebitelský přijímač (zdroj: [6])

Protože signál je generovaný z RF simulátoru a je tedy opakovatelný, zkoušky s rušením i bez rušení mohou být vykonávány sériově nebo paralelně. Výhodou vykonání testu v sérii je potřeba jen jednoho přijímače, přičemž rozbočovač není potřebný. Zatímco při paralelním testu se šetří čas, neboť test je spuštěn jen jednou.

V této konfiguraci jsou **dvě možnosti přidání interference**:

- První jsou **syntetické signály**, při kterých generátor vektorových signálů generuje předem definované syntetické signály interference na základě parametrů odvozených z vybraných hrozeb, které jsou detekované monitorovacími stanicemi.
- Druhou možností je **přehrání nahraných signálů interference**. Signál GNSS je nejprve odfiltrován ze surového signálu a následně přehráván prostřednictvím záznamového a přehrávacího zařízení jako je softwarové rádio (SDR).

Po sestavení testovacího systému musí být systém kalibrovaný, aby se zabezpečilo, že simulovaný signál GNSS bude na vstupu do přijímače na úrovni -130 dBm. Kalibrace signálu interference je vzhledem ke své proměnlivosti méně důležitá. Musí však být možně měřit a zaznamenávat intenzity interference na vstupu do přijímače, a to v průběhu celého testu.

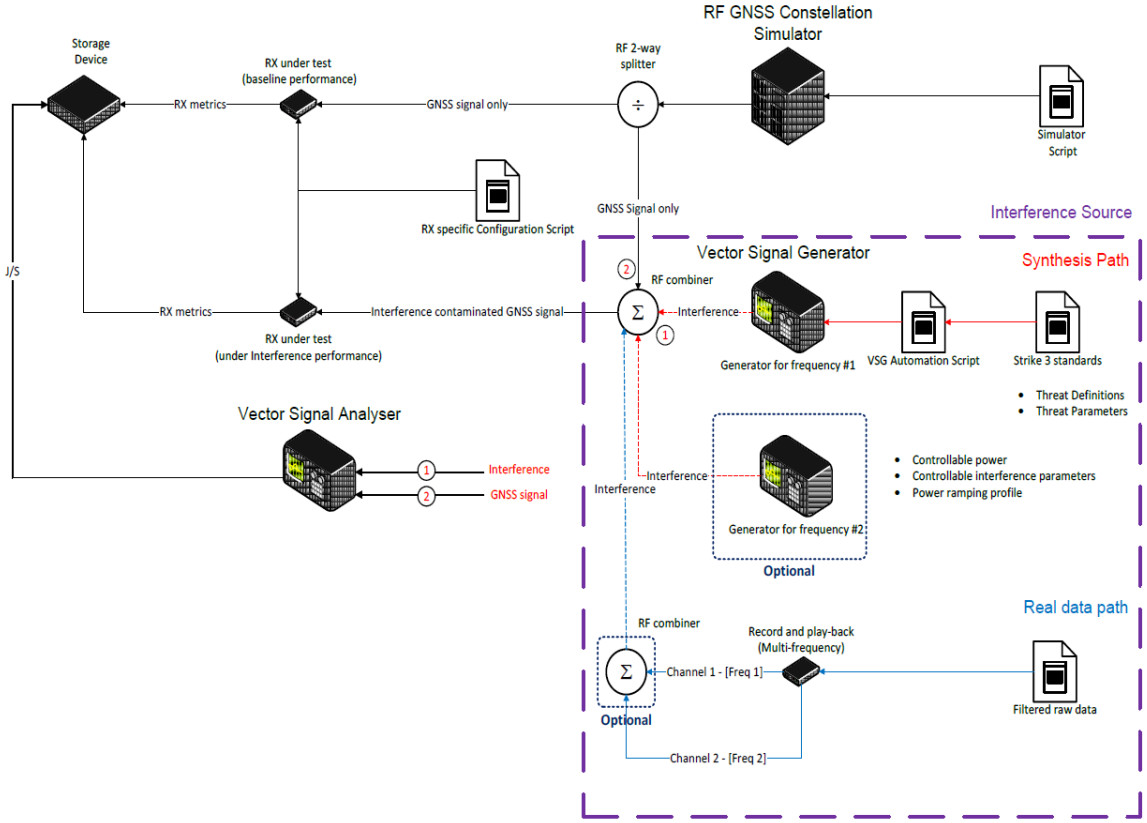
10.2.2 Multi-konstelační testování profesionálního přijímače

Základní nastavení prostředí při testování profesionálních přijímačů je stejné jako pro běžné spotřebitelské přijímače. Hlavním rozdílem je vyšší komplexnost testování vzhledem k pokročilým vlastnostem profesionálního přijímače, mezi které patří příjem signálu na více frekvencích i z více konstelací. Při testování tohoto typu přijímačů je důležité, aby byly testovány všechny možnosti daného přijímače.

Přijímač pracující se dvěma frekvencemi by měl být testovaný na rušení na obou frekvencích, a to buď jednotlivě nebo současně. Doporučené je současné testování rušení na všech frekvencích, aby mohla být odhalena možná závislost zpracování jedné frekvence na jiné. Pro uživatele je znalost těchto vztahů nutná.

Stejně tak přijímač, který umožňuje příjem signálu GNSS z různých konstelací, by měl být testovaný na rušení na všech konstelacích, a to jednotlivě nebo současně.

Při testování profesionálního přijímače se jako minimum doporučuje testování všech frekvencí a konstelací jednotlivě. Uživatelé mohou zadat vykonání simultánních testů podle potřeby.



Obrázek 21: Nastavení testů pro profesionální přijímač (zdroj: [6])

10.2.3 Testovací metody

V této kapitole jsou popsané dvě metody testování a jejich klíčové parametry:

- Time To First Fix (TTFF),
- testování citlivosti pro příjem a sledování signálu.

10.2.3.1 Time To First Fix

TTFF je v podstatě čas, který uplyne od spuštění přijímače až do prvního určení polohy přijímače. Tento čas je silně závislý na údajích, které má přijímač k dispozici. Pokud přijímač provede cílené vyhledání družic a je schopen prakticky hned použít signál, jedná se o **horký start** a čas nezbytný

pro start přijímače je velice krátký. Přijímače pro serióznější aplikace přesto i v těchto případech provedou kontrolní příjem alespoň části navigační zprávy, aby prověřily stav družic (mohl se změnit od posledního vypnutí přijímače).

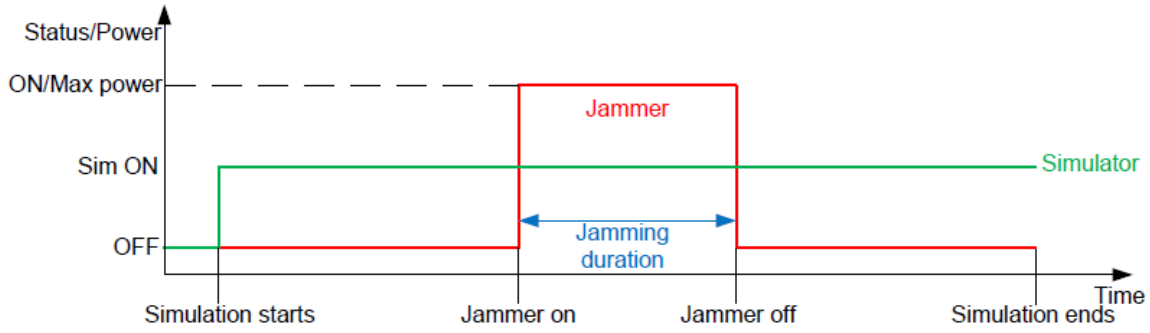
Při **teplém startu** má přijímač dostatek informací k tomu, aby mohl cíleně vyhledávat signál družic, které se nachází v příznivé poloze pro příjem. Pro použití signálu k určení polohy je ale třeba ještě načíst efemeridy.

Pokud přijímač nemá dostatek informací, musí začít náhodně procházet přijímací pásmo a tento proces může trvat relativně dlouho.

Tento test se používá na měření času potřebného na zotavení přijímače okamžitě po skončení silného rušení. Použitím měření času od počátku testování a času, který byl potřebný na určení polohy v nominálních podmínkách, může být hodnoceno chování přijímače hned po rušivé události. Parametry požadované pro tuto testovací metodu znázorňuje Obrázek 22.

Pro vykonání testu jsou potřebné následující kroky [6]:

1. Nastavení testovacího přijímače a potřebného zařízení s ohledem na typ přijímače podle příslušného popisu architektury testování (kapitola 10.1 a 10.2).
2. Příprava pro zaznamenání příslušné sady měřených veličin z přijímače.
3. Zvolení hodnot parametrů, jako např. doba trvání rušení nebo maximální síla interference.
4. Zaznamenání času začátku simulace.
5. Spuštění simulace při zapnutém simulátoru GNSS a bez zdroje rušení, dokud přijímač neuskuteční první určení polohy, a zaznamenání času potřebného na první určení polohy přijímače od spuštění simulace.
6. Spuštění zdroje interference při definované maximální síle výkonu a zaznamenání času spuštění interference.
7. Vypnutí zdroje rušení na konci zvoleného trvání interference.
8. Simulátor GNSS je neustále zapnutý, zaznamenání času potřebného na to, aby přijímač získal fixaci polohy po vypnutí zdrojů interference.



Obrázek 22: Profil TTFF testu (zdroj: [6])

Jak je znázorněno na Obrázek 22, testovaný přijímač určí polohu ze simulátoru GNSS a zaznamená se TTFF. Následně se zapne zdroj interference na stanovenou dobu s takovou

intenzitou, aby přijímač ztratil schopnost určení polohy. Po stanovené době rušení je zdroj interferencí vypnutý, zatímco simulátor GNSS je zapnutý, dokud přijímač nezíská polohovou fixaci. Čas mezi vypnutím zdroje interference a první polohovou fixací se zaznamená jako TTFF po rušení a porovná se s TTFF v nominálních podmínkách.

10.2.3.2 Testování citlivosti pro příjem a sledování signálu

Při testování schopnosti přijímače přijímat signál z družice a určovat polohu může být použita:

- **Konstantní síla interferujícího signálu**: Tento profil je typický pro statické zdroje interference (relativně vzhledem k přijímači) a síla vysílaného signálu se nemění. Jeden příklad takové interference byl detekován při měření v Praze (příklad – Obrázek 23).
- **Proměnná síla interferujícího signálu**: Tento případ reprezentuje stoupající a klesající intenzita interference. To nastane ve chvíli, kdy se zdroj interference a přijímač navzájem vůči sobě pohybují, nebo když je síla vysílané interference proměnná (příklad – Obrázek 24).

Testování konstantní silou interferujícího signálu je základní formou testování, při které je možné vidět dopad interferujícího signálu s definovanou intenzitou na výkon přijímače. Může se jednat o testování proti známým statickým zdrojům interference.

Testovací profil s **konstantní intenzitou interferujícího signálu** má následující postup [6]:

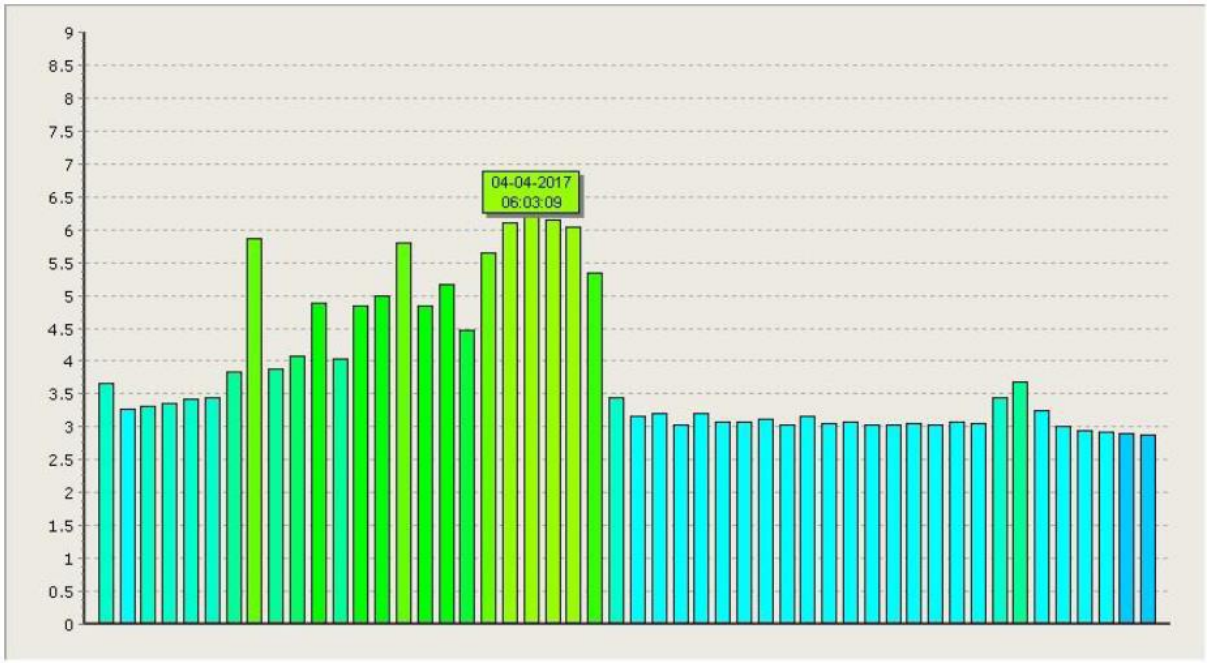
1. Nastavení testovaného přijímače a potřebného zařízení vzhledem k typu přijímače podle příslušného popisu architektury testování (kapitola 10.1 a 10.2).
2. Příprava pro zaznamenávání příslušné sady měřených veličin z přijímače.
3. Zvolení hodnot parametrů – intenzita interference a její trvání.
4. Zaznamenání času začátku simulace.
5. Spuštění simulace při zapnutém simulátoru GNSS a bez zdroje interference, dokud přijímač neuskuteční první určení polohy, zaznamenání času potřebného na první určení polohy přijímače od spuštění simulace.
6. Zapnutí zdrojů signálů interference s definovaným trváním a intenzitou.
7. Zaznamenání sledovaných veličin pro monitorování vlivu interference na kvalitu přijímaného signálu GNSS.
8. Vypnutí zdroje interference a zaznamenání sledovaných veličin pro monitorování chování přijímače pro vypnutí interference.

Kroky spuštění konstantního profilu intenzity interference:

1. interference vypnuta,
2. interference začne vysílat na úrovni P_{jam},
3. po daném čase, T_{jam}, je interference opět vypnuta.

Obrázek 23: Příklad konstantní intenzity pro dlouhodobou interferenci detekovanou v Praze

Druhou variantou je testování s měnící se intenzitou interferujícího signálu. Takové testování je důležité pro zjištění, jak přijímač reaguje na různé profily síly rušení. Tím je možné určit bod, ve kterém testovaný přijímač už nedokáže sledovat dostatek družic na určení polohy (citlivost sledování) a bod, ve kterém testovaný přijímač začne opětovně sledovat dostatečný počet družic. Umožňuje také studování jakéhokoliv nežádoucího chování za těchto podmínek, např. generování chybných údajů.



Obrázek 24: Proměnlivá intenzita interferujícího signálu detekovaného v Praze

Pokud intenzita interferujícího signálu narůstá, dochází k poklesu hodnot SNR a zároveň k poklesu počtu použitých družic pro určování polohy ve stejném okamžiku. Pokud se počet použitých družic zmenší na 3, 3D určení polohy se změní na 2D určení polohy a dojde ke zvýšení chyby v poloze. Když se počet družic zmenší na 2, dochází ke ztrátě schopnosti určit polohu. Parametry požadované pro tuto testovací metodu znázorňuje Obrázek 25.

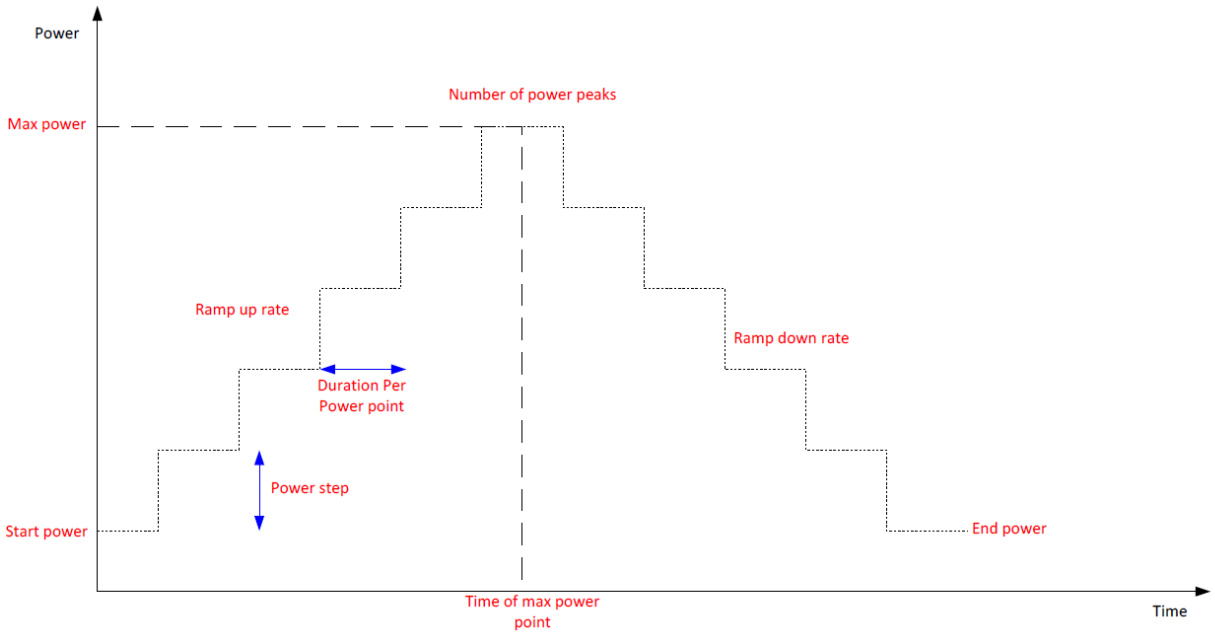
Testovací profil s **dynamicky se měnící intenzitou interferujícího signálu** má následující postup [6]:

1. Nastavení testovaného přijímače a potřebného zařízení s ohledem na typ přijímače podle příslušného popisu architektury testování (kapitola 10.1 a 10.2).
2. Příprava pro zaznamenání příslušné sady měřených veličin z přijímače.
3. Zvolení hodnot parametrů, např. maximální intenzity interference, kroku velikosti změny a trvání úrovně intenzity.
4. Zaznamenání času začátku simulace.
5. Spuštění simulace při zapnutém simulátoru GNSS a bez zdroje interference, dokud přijímač neuskuteční první určení polohy, zaznamenání času potřebného na první určení polohy přijímače od spuštění simulace.
6. Zapnutí zdrojů signálů interference s definovaným trváním pro každou úroveň intenzity, zvyšování úrovně intenzity definovaným krokem změny.
7. Zaznamenání úrovně intenzity (dBm) interference, při které přijímač už není schopný určit polohu. Pokračování ve zvyšování síly až do dosáhnutí definovaného maxima na potvrzení úplné ztráty polohy.
8. Postupné snižování úrovně intenzity definovaným krokem s definovaným trváním kroku a zaznamenání času, kdy přijímač znovu začne sledovat družice a dokáže určit polohu, zaznamenání úrovně intenzity (dBm), kdy k jednotlivým událostem došlo.

Kroky spuštění dynamického profilu intenzity interference:

1. interference vypnuta,
2. úroveň interference je nastavena na P_{low},
3. interference roste po kroku G_{step} každých T_{step} vteřin,
4. až Interference dosáhne P_{high}, setrvá v tomto stavu po dobu T_{jam},
5. interference klesá po kroku G_{step} každých T_{step} vteřin,
6. až Interference dosáhne P_{low}, je vypnuta.

Obrázek 25 zobrazuje doporučený testovací profil a klíčové parametry. Tyto parametry by měly být naprogramované v generátoru interferujícího signálu.



Obrázek 25: Profil dynamicky se měnícího rušení s jedním vrcholem (zdroj: [6])

10.2.4 Testovací scénáře

Na základě informací uvedených výše je nutné zvážit a konfigurovat následující parametry:

- typ přijímače,
- zdroj signálu GNSS (simulátor GNSS nebo přehrávací zařízení),
- použití syntetických vektorů hrozeb nebo nahrávek rušení,
- testovací metoda.

Po specifikování testovacího prostředí, přijímače a jednotlivých parametrů je každý scénář definovaný specifickou kombinací:

- poskytnutého GNSS signálu (zvolené konstelace a frekvence) (SIG-xx),
- profilu intenzity interferujícího signálu (PP-xx),
- typu interferujícího signálu (RFI-xx).

Při testování přijímače je nutné aplikovat vícero testovacích scénářů s různými kombinacemi typu interferujícího signálu a profilu intenzity daného signálu, aby bylo testování dostatečně vypovídající a pokrylo všechny schopnosti daného přijímače i variabilitu interference, ke které dochází v reálném prostředí. Při testování dvou nebo více přijímačů by měl být každý scénář aplikovaný na každý testovaný přijímač, aby testování poskytlo úplné porovnání.

Během každého testu, před spuštěním interference, je **přijímač ve stavu stabilního příjmu signálů** z družic. Tímto jsou simulovány případy, kdy je přijímač před samotnou přítomností hrozby již v provozu. Z pohledu uživatelské aplikace jsou toto ty nejčastější případy a zároveň působí nejvíce problémů, protože je obtížné zjistit příčinu rušení.

Existuje další kategorie případů, ve kterých je interference dlouhodobě přítomna během doby, kdy se přijímač snaží přijmout signály z družic bez znalosti potřebných vstupních hodnot (někdy je tato fáze provozu přijímače označována jako studený start). Nicméně přijímače GNSS pracují v tomto stavu pouze po krátkou dobu a v této fázi je snadné detekovat příčinu/přítomnost rušení, čímž je dopad na uživatele méně závažný. Z tohoto důvodu je v této metodice věnována pozornost prvnímu zmíněnému případu.

Příklad vytvoření testovacích scénářů se nachází v Tabulka 10.

Testovací scénář	Signál GNSS	Profil síly	Interference
TC-01	SIG-01	PP-01	RFI-01
TC-02		PP-02	RFI-01
TC-03			RFI-02
TC-04			RFI-03
TC-05			RFI-04
TC-06	SIG-02	PP-01	RFI-04
TC-07		PP-02	RFI-05

Tabulka 10: Testovací scénáře pro jamming

Každý přijímač je schopen v průběhu testování zaznamenávat data ve formátu NMEA a dále proprietární data v závislosti na daném typu a výrobci. Pro každý testovací scénář jsou tato data sbírána ve formě zpráv na výstupu z přijímače. Zprávy jsou poté analyzovány s pozorností věnovanou příjmu signálu (vč. počtu viditelných družic a SNR) a kvalitě řešení polohy (DOP a přesnost polohy). Jednotlivým měřeným veličinám při testování se věnuje následující kapitola.

10.3 Analýza výsledků testování

Tato část se věnuje monitorování přijímače, měření a výstupům, které mohou být použity na hodnocení výkonu přijímače v přítomnosti rušení. Jednotlivé přijímače se liší pouze o výstupní veličiny, proto metodika navrhuje využít nejčastěji dostupné veličiny na hodnocení přijímačů.

Hodnocení výkonu přijímače může být vykonané prostřednictvím veličin, které jsou rutinně dostupné z přijímače:

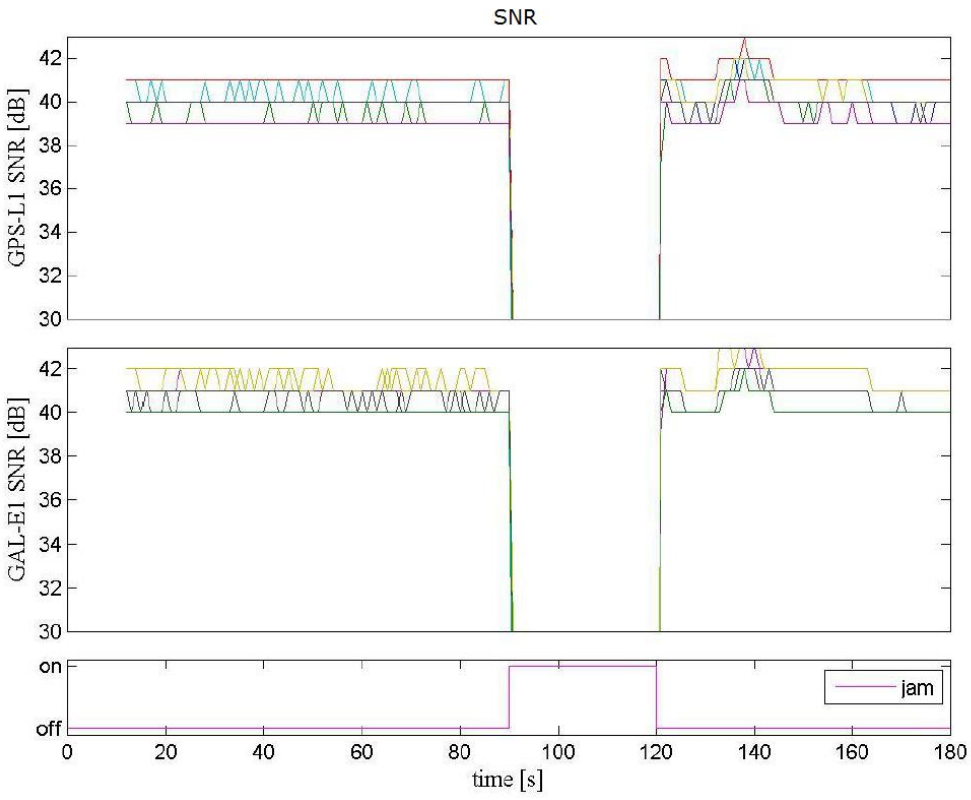
- **hodnota SNR,**
  - SNR je měřítkem kvality signálu. Hodnota SNR není konstantní, liší se většinou podle velikosti elevačního úhlu družice, který se mění v průběhu dne. SNR je rovněž ovlivněno náhodnými elementy (šum na pozadí).
  - SNR se sníží v případě, kdy se síla šumu (a současně jammingu) zvýší. Když je hodnota SNR satelitního signálu nevyhovující, dojde ke ztrátě signálu a přijímač již nebude schopný poskytovat údaje o poloze.
- **počet družic** (s nenulovým SNR),
  - Počet družic podává informaci o počtu hlášených nenulových hodnot SNR. To může být užitečné pro demonstraci zjištění, kolik družic je rušičkami "vyřazeno" ze sledování. Tato skutečnost může být na druhou stranu zavádějící, protože přijímače mají během jammingu

tendenci falešně získávat satelitní signály a hodnoty SNR by mohly činit přibližně 15 dB, což je indikátor falešné akvizice satelitního signálu.

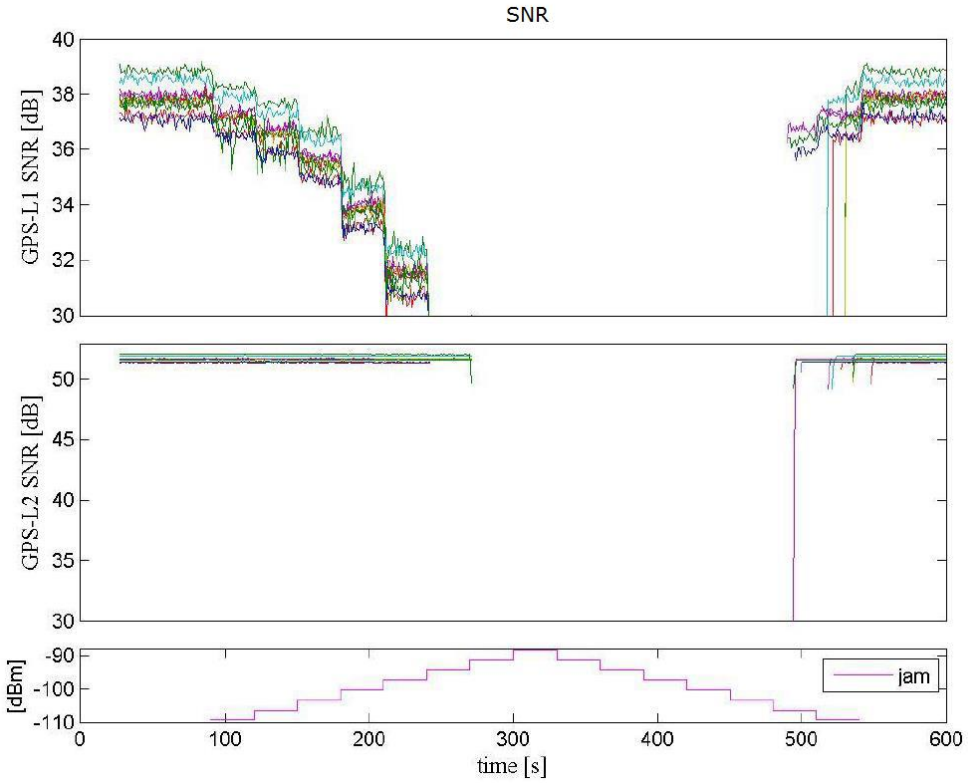
- **2D a 3D chyba v poloze,**
  - Chyba v poloze znázorňuje vzdálenost (v metrech) mezi skutečnou polohou (v případě testování je skutečná poloha nastavená v simulátoru) a polohou odhadnutou přijímačem. 2D je horizontální chyba v poloze, zatímco 3D přihlíží také k chybě ve vertikální poloze. Tyto údaje podávají informaci o tom, zda konečný výstup přijímače (obvykle přesnost v poloze) byl ovlivněn jammingem.
- **hodnota DOP ve třech rovinách** (poloha, horizontální, vertikální),
  - V případě jammingu očekáváme, že signál družic s nízkými elevačními úhly (slabší signál) bude jako první ztracen, čímž dojde ke zvýšení hodnoty DOP.

Příklady výstupů zobrazují následující obrázky.

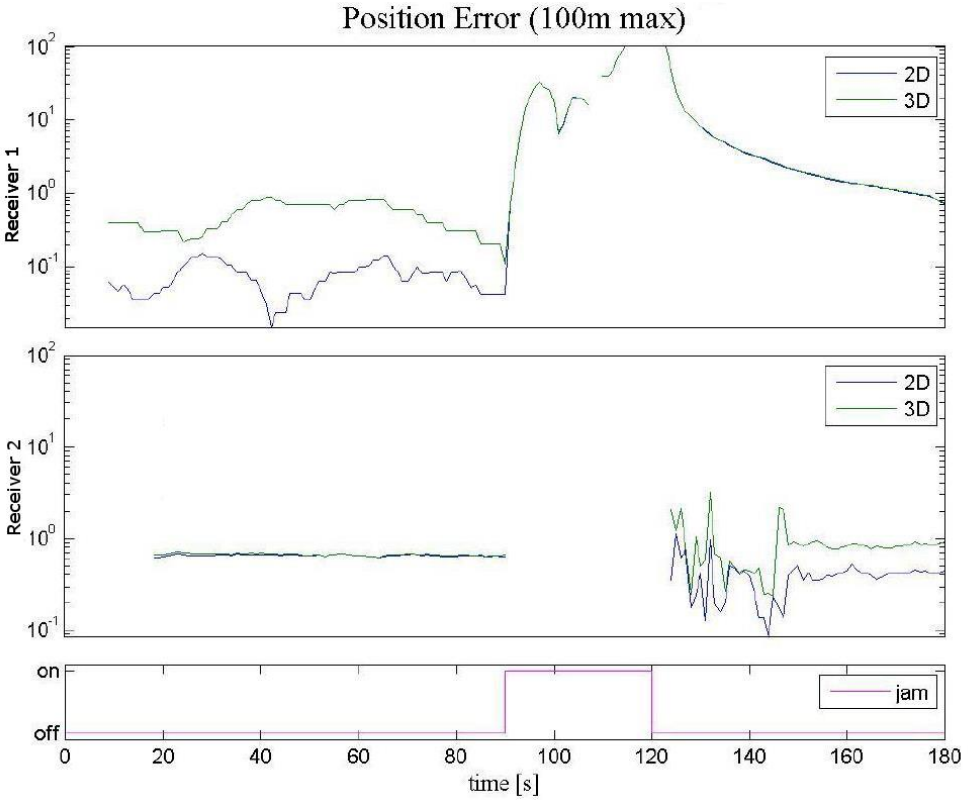
Obrázek 26 zobrazuje hodnoty SNR pro jeden přijímač a dvě konstelace (GPS-L1 a Galileo-E1) při konstantní intenzitě interference, která je zobrazená v nejspodnější části grafu. Z grafu je zřejmé, že po zapnutí interference dochází k zablokování signálů z obou konstelací a tedy úspěšnému jammingu. V Obrázek 27 jsou zobrazené hodnoty SNR pro dvě frekvence GPS (L1 a L2) a je použitá proměnná intenzita interference. S nárůstem hodnoty intenzity interference dochází postupně k poklesu hodnot SNR až k úplné ztrátě signálu. Obrázek 28 zobrazuje chybu určení polohy pro dva testované přijímače. U prvního přijímače dochází po zapnutí zdroje interference k nástupu chyby určení polohy, u druhého k úplné ztrátě signálu.



Obrázek 26: Hodnoty SNR pro frekvence GPS-L1 a Galileo-E1 při konstantní intenzitě interference



Obrázek 27: Hodnoty SNR pro frekvence GPS-L1 a GPS-L2 při proměnné intenzitě interference



Obrázek 28: Chyby v poloze u dvou testovaných přijímačů při konstantní síle interference

10.4 Aplikace navržené metodiky testování

Tato část vysvětluje, jak by se měla testovací metodika použít při hodnocení výkonu přijímače GNSS:

1. Výběr přijímače na testování.
2. Zjištění výrobců a modelu přijímače.
3. Zjištění typu přijímače (profesionální / běžný spotřebitelský). Typ přijímače ovlivní architekturu testů, parametry a metodologii.
4. Výběr metody generování signálů interference, použití generátoru signálů nebo zařízení na přehrání signálu interference.
5. Výběr testu na základě potřeb pro specifickou aplikaci (statický / dynamický / TTFF).
6. Sestavení konfigurace testu na základě informací uvedených výše (v kapitolách 10.1 a 10.2).
7. Konfigurace jednotlivých zařízení tvořících testovací prostředí. Tento krok by měl být ve formě skriptů:
    - Pro testovaný přijímač:
        - konfigurace parametrů v souladu s aplikací přijímače, spolu s parametry specifickými pro požadované testy, např. konstelace / frekvence a měřené veličiny.
    - Pro simulátor konstelací GNSS:
        - konfigurace parametrů pro vykonání specifického testu,
        - zabezpečení, aby úroveň výkonu GNSS na vstupu do přijímače byla v souladu se specifickou konstelací GNSS a testovanou frekvencí.
    - Pro generátor rušení:
        - výběr hrozby, vůči které bude přijímač testovaný,
        - výběr signálů interference,
        - konfigurace generátoru signálů interference nebo zařízení na přehrávání nahraných signálů interference.
8. Konfigurace parametrů testování specifických pro daný test, které ještě nejsou nakonfigurované.
9. Zapnutí zařízení na zaznamenávání měřených veličin.
10. Vykonání specifického testu(ů).
11. Analýza výsledků a jejich porovnání vůči požadovanému výkonu.

11 Doporučení

V rámci metodiky testování byla uvedena doporučení na sestavení architektury testování, výběr metod testování i výběr hrozeb, vůči kterým je vhodné přijímače testovat. Také byly uvedeny měřené veličiny, na základě kterých je možné hodnotit výkon přijímače v testovaných podmínkách. Uvedené postupy nemají za cíl představit detailní popis nastavení a průběhu testování, nakolik se jednotlivé typy přijímačů liší v zaměření, parametrech či výkonu a také se různí potřeby uživatelů a jejich systémů. Jedná se o univerzální seznam aktivit a doporučení, které je vhodné při testování jednotlivých zařízení dodržet, aby byla zabezpečena správnost, integrita a porovnatelnost výsledků testování, a aby testování podalo vypovídající a komplexní hodnocení výkonu přijímače.

Mezi hlavní zásady při testování přijímače patří:

- Nastudování technické dokumentace testovaného přijímače, která je nejdůležitějším zdrojem informací o jednotlivých parametrech přijímače a jeho výkonu, podporovaných konstelacích a frekvencích. Obsahuje technický popis přístroje, specifikaci protokolu a i účel jeho využití a vhodné provozní prostředí. Na základě dokumentace je také možné zjistit použitá opatření proti rušení (implementace různých typů filtrů). Výběr správného přijímače pro konkrétní aplikaci a prostředí je základním opatřením na minimalizaci rizik v provozním prostředí.
- Testování by mělo pokrýt všechny schopnosti přijímače – konstelace a frekvence. Minimálním požadavkem je testování každé frekvence samostatně, doporučené je ale komplexní testování na všech frekvencích zároveň, které odhalí závislost zpracování jedné frekvence na jiné. Navzdory tomu, že výrobci na trh uvádějí přijímače označené jako multikanálové, které mají zvýšit robustnost řešení, ne vždy všechna tato zařízení skutečně poskytují zvýšenou ochranu. Testováním zařízení bylo zjištěno, že v mnohých multikanálových přijímačích je zpracování jedné frekvence závislé na jiné, respektive jedné konstelace na jiné a při rušení jedné frekvence/konstelace dojde k rušení ostatních a tím k výpadku provozu zařízení. Proto je pro uživatele nutné, aby poznali tyto závislosti a mohli podniknout konkrétní opatření.
- Při testování by měly být použity reálné nahrávky interference z provozního prostředí. Při využití reálných nahrávek existují dva přístupy – parametrizace hrozeb a opakované zpracování ze souhrnných vzorků. Uživatel by si měl zvolit přístup na základě cílů, které mají být testováním dosaženy. Výhodou přehrání nahraných vzorků signálu je, že při komplexnějších hrozbách by mohlo poskytnout přesnější rekonstrukci hrozby. Výhodou parametrizování nahrávek je větší kontrola nad parametry signálu rušení a tím větší variabilita testování.
- Při sestavování architektury testování a testovacích scénářů je nutné dbát na základní zásady – testování by mělo být v co největší míře automatizované, je nutné mít kontrolu nad všemi důležitými parametry signálu GNSS, bez ohledu na scénář je potřeba zabezpečit opakovatelnost testování za stejných podmínek a pokrytí testy musí být reprezentativní.

Testování přijímačů patří mezi základní opatření, avšak je jen jedním článkem v komplexním procesu ochrany před škodlivým rušením. Aby bylo testování přijímačů efektivní a poskytlo vypovídající informace o výkonu testovaného zařízení, je nutné podrobit přijímač reálným hrozbám sesbíraným v reálném prostředí. Testování je proto vhodné doplnit dalšími opatřeními a vytvořit komplexní systém ochrany před rušením. **Mezi navrhovaná opatření patří:**

- **Zřízení testovacího místa (laboratoře)** pro ověřování odolnosti přijímačů GNSS proti záměrnému rušení (jammingu). Oficiální testovací pracoviště by zaručilo objektivní, kvantifikované a komparativní testování jednotlivých typů přijímačů. Zřízení takového pracoviště má opodstatnění především pro potřeby aplikací GNSS ve státní službě. Státní orgány tak dostanou relevantní a komplexní hodnocení používaných přijímačů GNSS.
- **Vytvoření monitorujícího systému**, který bude systematicky a kontinuálně monitorovat RF spektrum za účelem detekce interference. Zvolením vhodných detekčních zařízení a parametrů selekce případů interference je možné identifikovat případy škodlivé nezákonné interference. Monitorovací systém by měl být kompatibilní s vytvářenými celoevropskými standardy, což umožní sdílení detekovaných hrozeb na nadnárodní úrovni. Získané informace přispějí k pochopení úrovně hrozby v reálném prostředí a bude možné vyvinout účinná opatření na zamezení, respektive minimalizaci vlivu interference na chod systémů. Zaznamenané hrozby bude možné využít při testování přijímačů a tím vyhodnotit jejich výkon v reálném prostředí.
- **Vytvoření národní databáze kritických uživatelů závislých na GNSS** a nastavení rolí a zodpovědných autorit. Státní orgány by měly mít znalost o kritických infrastrukturách využívajících GNSS systém pro svůj provoz, jejich závislosti a záložních řešeních. Taková databáze poskytne kontrolu připravenosti kritické infrastruktury vůči hrozbám GNSS. Cílovým stavem je poznání všech prvků a uživatelů kritické infrastruktury závislých na GNSS signálech a jejich připravenost na výpadek GNSS.
- **Analýza a příprava možných záložních systémů**. V případě dlouhodobějšího výpadku GNSS by mělo význam mít připravené technologické alternativy, jak z hlediska navigace, tak i určení polohy a/nebo času. Doporučuje se identifikace možných substitučních řešení a systémů, spolu s analýzou finanční náročnosti realizace jednotlivých alternativ. Žádné z opatření proti rušení nedokáže zabránit výpadku při velmi silném rušení, a proto je nutné mít k dispozici záložní systémy, které budou schopné, v případě dlouhodobějšího výpadku GNSS, zabezpečit provoz především kritické infrastruktury.
- **Zvýšení povědomí o existujících hrozbách** mezi správci systémů a koncovými uživateli, kteří jsou závislí na systému GNSS. Zvýšení povědomí o hrozbách pro GNSS, ať už organizováním akcí příslušnými státními orgány nebo jiným způsobem, by pomohlo jednotlivým uživatelům identifikovat potenciální hrozby pro jejich aplikace a systémy a následně vyvinout účinná opatření či záložní systémy. Zvýšení povědomí o hrozbách patří mezi základní opatření, kterým mohou státní orgány zvýšit ochranu a zabezpečení systémů a minimalizovat dopady škodlivého rušení.

12 Reference

[1] GNSS Market Report, Issue 4, GSA, 2015

[2] Global Navigation Space Systems: Reliance and Vulnerabilities, The Royal Academy of Engineering, 2011

[3] Akční plán rozvoje inteligentních dopravních systémů (ITS) v ČR do roku 2020 (s výhledem do roku 2050), Ministerstvo Dopravy ČR, 2015

[4] SENTINEL Project: GNSS Vulnerabilities, Chronos, 2014

[5] Technology Study: GNSS Threat Quantification in the United Kingdom in 2015 (GemNET project), Catapult

[6] Standardisation of GNSS Threat reporting and Receiver testing through International Knowledge Exchange, Experimentation and Exploitation, STRIKE3 Consortium, 2017

[7] GNSS User Technology Report, Issue 1, GSA, 2016

[8] Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)

[9] Nařízení vlády č. 432/2010 Sb. o kritériích pro určení prvku kritické infrastruktury

[10] Proces určování kritické informační infrastruktury, Národní centrum kybernetické bezpečnosti

[11] Oxera Consulting, What is the economic impact of Geo services ?, 2013

[12] Low end of the 9%-35% range in Ingenia Online (2015) Precision farming. 2015

[13] Office for National Statistics, Annual Business Survey for 2015, 2015

[14] GPS Vulnerability in Mobile Network, NIST, 2013

[15] GPS Critical Infrastructure: Usage/Loss Impacts/Backups/Mitigation, DHS, 2011

[16] National Risk Estimate: Risks to U.S. Critical Infrastructure from Global Positioning System Disruption, DHS, 2011

[17] Nařízení Evropského parlamentu a Rady 1285/2013/EU ze dne 11. prosince 2013 o zřízení evropských systémů družicové navigace a jejich využití a o zrušení nařízení Rady (ES) č. 876/2002 a nařízení Evropského parlamentu a Rady (ES) č. 683/2008

[18] Směrnice Rady 2008/114/EU ze dne 8. prosince 2008 o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu

[19] Pracovní dokument SWD(2013)318 o novém přístupu k programu ochrany evropské kritické infrastruktury

[20] Směrnice Evropského parlamentu a Rady 2016/1148/EU ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii

[21] 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 Směrnice 2014/65/EU o trzích a finančních nástrojích
[22] Společné sdělení Evropskému parlamentu a Radě – Společný rámec pro boj proti hybridním hrozbám, 6.4.2016
[23] Usnesení Evropského parlamentu ze dne 8. června 2016 o vesmírných kapacitách evropské bezpečnosti a obrany (2015/2276(INI))
[24] Interference Detection and Mitigation and GNSS Jammers, U.S. Coast Guard Navigation Center, 2015
[25] Best Practices for Improved Robustness of Time and Frequency Sources in Fixed Locations, DHS, 2015
[26] National Institute of Standards and Technology (NIST), Time Distribution Alternatives for the Smart Grid, 2017
[27] Anti/Jam Protection by Antenna, GPS World, 2013
[28] EGNOS - Evropská „podpůrná“ geostacionární navigační služba, Český kosmický portál
[29] GNSS/GPS Radio Hacking, Tomáš Rosa, 2016
[30] GPS can be jammed and 'spoofed'-just how vulnerable is it?, Marine Electronics, 2016
[31] European eLoran Forum, eLoran: Securing Positioning, Navigation and Timing for Europe’s Future, 2008
[32] International Loran Association, 2015
[33] CTL3520, GPS Jammer Detector & Locator, Chronos
[34] CTL3520 Handheld Directional GPS Jammer Detector and Locator
[35] J911: Fast Jammer Detection and Location Using Cell-Phone Crowd-Sourcings, GPS World, 2010
[36] Signal Sentry 1000, Exelis
[37] Signal Sentry 1000, Harris
[38] In-Car GNSS Jammer Localization Using Vehicular Ad-Hoc Networks, Inside GNSS, 2013
[39] Innovation: Null-steering antennas, GPS World, 2016
[40] Žilinská univerzita v Žiline, Globálne navigačné systémy, 2005
[41] Spirent, Spirent White Paper: Why Simulate ?, 2010
[42] GNSS Data Processing Volume I: Fundamentals and Algorithms, ESA, 2013
[43] Vysoká Škola Báňská – Technická univerzita Ostrava, Družicové polohové systémy, 2002
[44] Listening for RF Noise, InsideGNSS, 2016
[45] Spirent, How to Construct a GPS/GNSS Test Plan, 2016

[46] European Conference of Postal and Telecommunications Administrations, Electronic Communications Committee, GNSS jamming investigation, 2018

[47] Ublox, Anti-Jamming techniques in u-blox GPS receivers, 2009