ČVUT

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Odolnost letectví proti podvrženým signálům GNSS a ADS-B

Jakub Hospodka

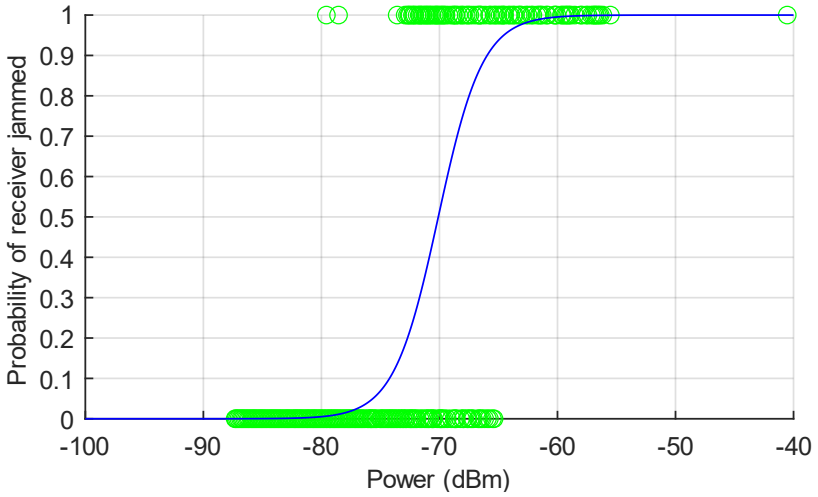
ČVUT v Praze – Katedra letecké dopravy

Související výzkum na Katedře letecké dopravy

- grant No. VI20172019090 – Výzkum ministerstva Vnitra – Detektor Jammingu GNSS – 2018-2020
- TAČR CK02000127 - Systém detekce rušení signálů družicové navigace pro oblast integrovaných bezpečnostních prvků v silniční dopravě 2022-2024
- **TAČR Doprava – Výzkum vlivu rušení GNSS signálu v oblasti letectví 2021 - 2024**
- **MV OPSEC - Odolnost letectví proti podvrženým signálům GNSS a ADS-B 2023-2025**

Výzkum vlivu rušení GNSS signálu v oblasti letectví
Projekt TAČR (program Doprava 2020+)

- **Metodika detekce nezákonného ovlivňování signálu GNSS prostřednictvím využití systému ADS-B** *(Zjištěn pravděpodobnostní popis úrovně rušícího signálu při které dochází ke ztrátě polohové informace na letadle a odezva v rámci parametrů kvality vysílaných v ADS-B zprávách.)*
- **Model pro fúzování zdrojů informací o nezákonném rušení** *(Slučování informací s cílem zlepšit odhad parametrů zdroje rušení, např. poloha, výkon, …)*

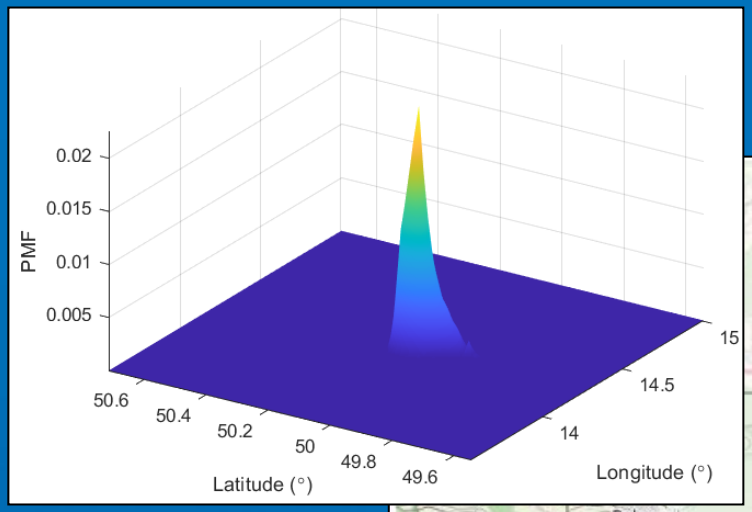


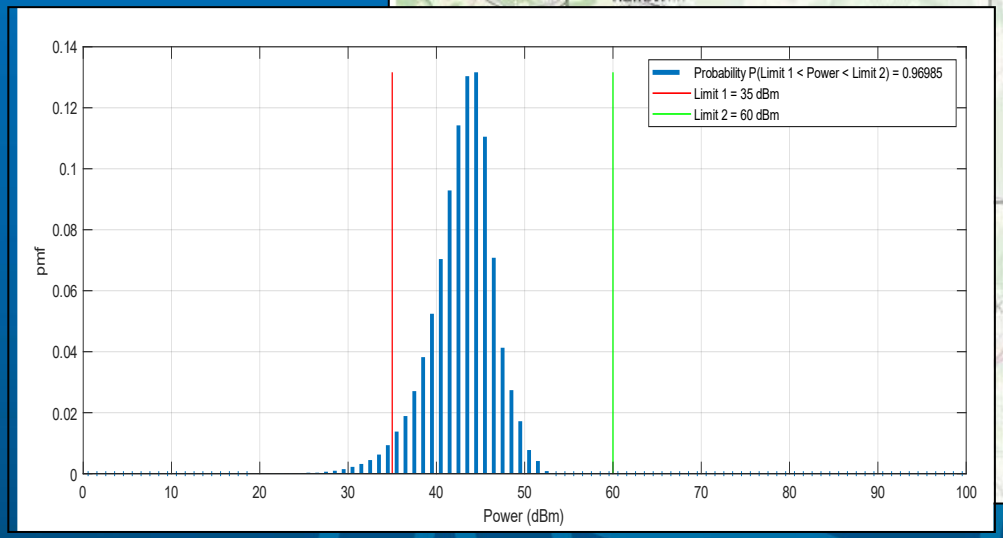
ČVUT

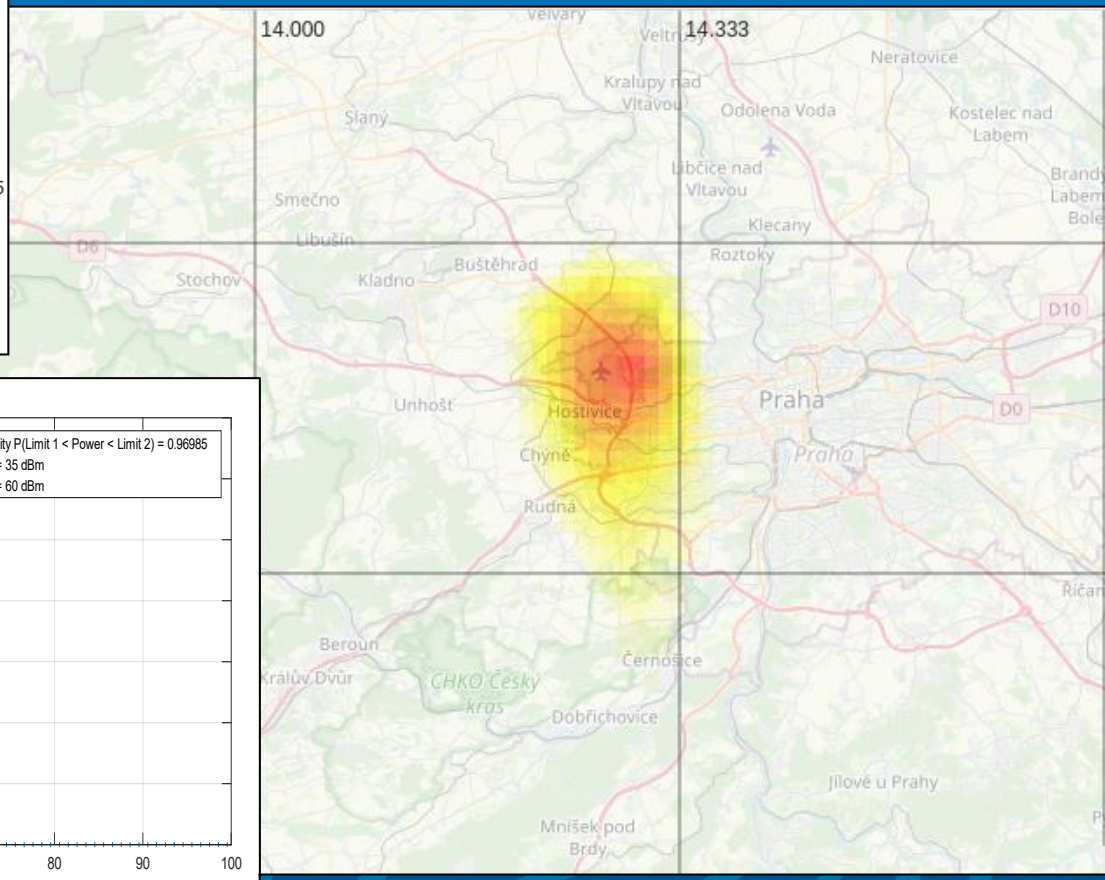
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

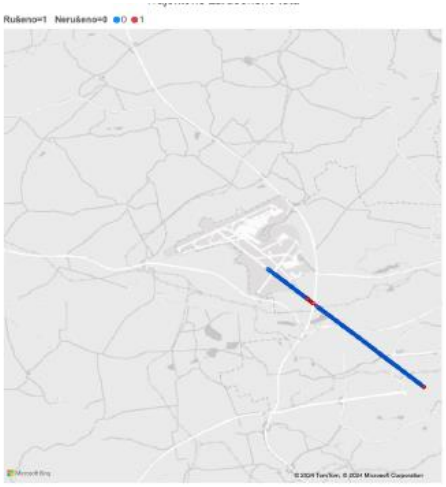
Odhad pozice a výkonu zdroje rušícího signálu

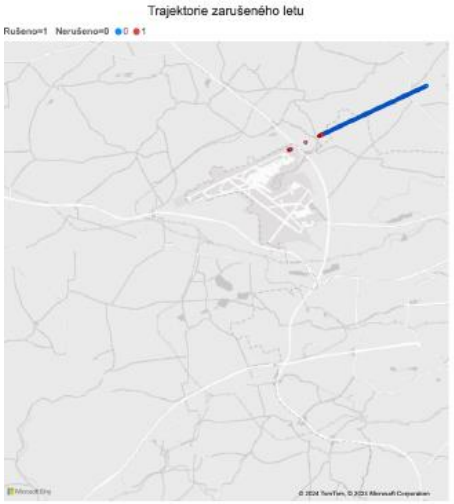
(Příklad simulace fúze informací z 12-ti senzorů Y/N)

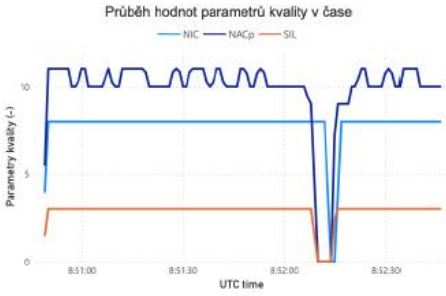


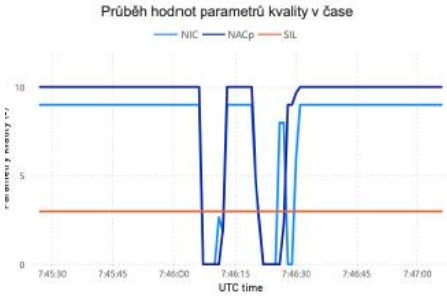


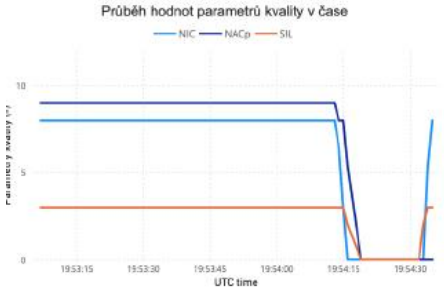








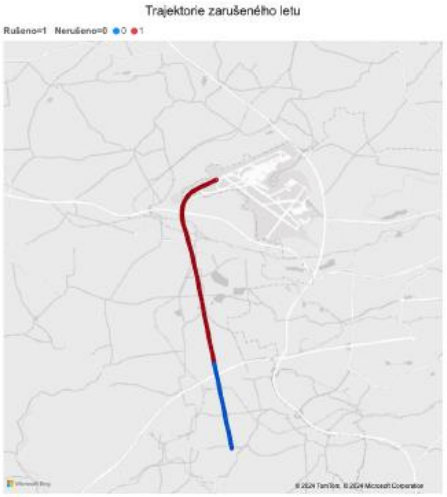


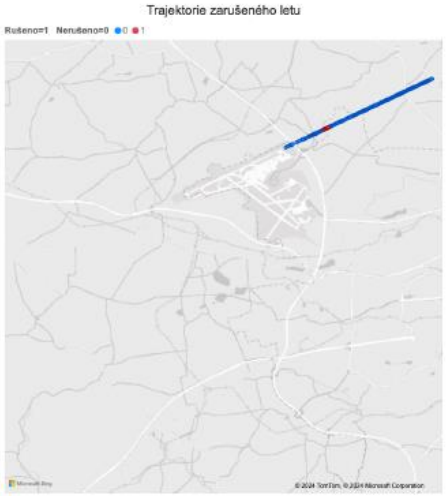


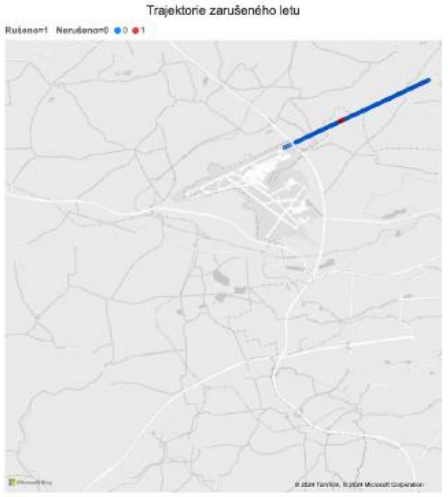
duben 2021 až březen 2022 – 71 500 pohybů

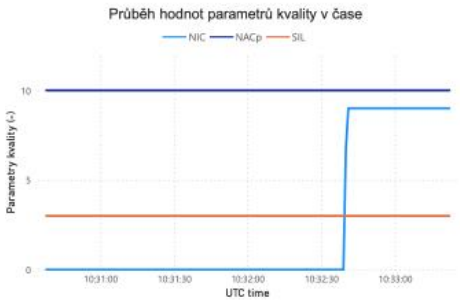
Cca 37 detekovaných eventů – zarušených letů

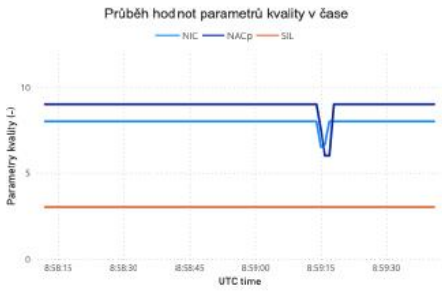
Počet detekovaných rušení na dálnicích – stovky hlášení za měsíc z jednoho detektoru;
„běžné“ rušičky v autech mohou ovlivnit leteckou dopravu – ale typicky jen v těsné blízkosti letiště kde jsou letouny blízko

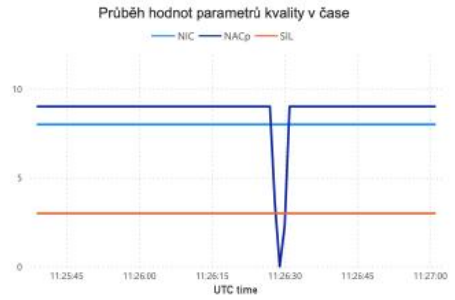










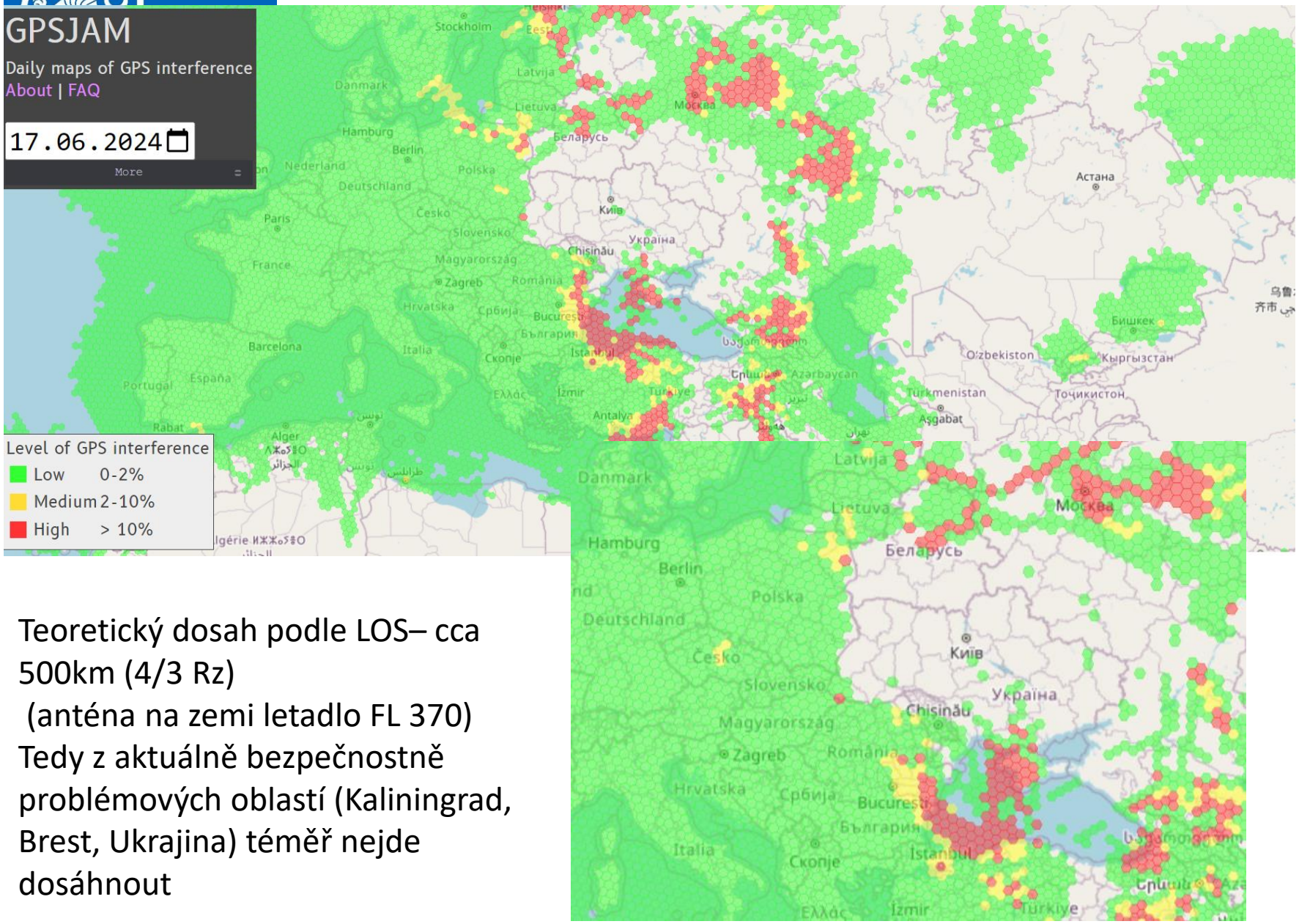


Není vždy zřejmé zda se jedná o jamming

Většina zmíněných letů nepodala žádné hlášení

Parametry kvality GNSS signálu jsou někdy kontaminovány letadly která vysílají nesprávné hodnoty

Rušení ze zahraničí



Teoretický dosah podle LOS– cca 500km (4/3 Rz)
(anténa na zemi letadlo FL 370)
Tedy z aktuálně bezpečnostně problémových oblastí (Kaliningrad, Brest, Ukrajina) téměř nejde dosáhnout

ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
FAKULTA DOPRAVNÍ
KATEDRA LETECKÉ DOPRAVY

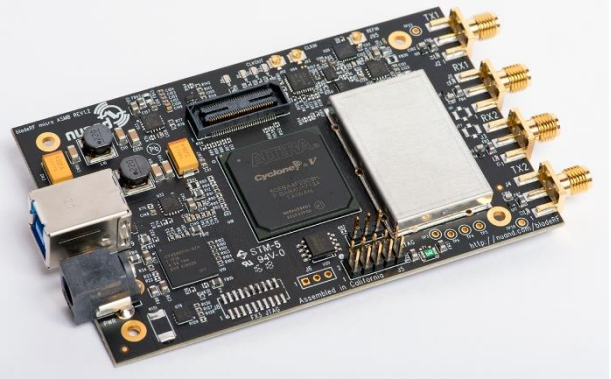
Odolnost letectví proti podvrženým signálům GNSS a ADS-B

- **Doba řešení: 2023-2025**
- **Sektorový Program MV ČR – OPSEC - Otevřené výzvy v bezpečnostním výzkumu 2023-2029**
- **ČVUT v Praze - Fakulta Dopravní a Fakulta Elektrotechnická**
- **Řízení letového provozu České republiky, státní podnik (ŘLP ČR, s.p.)**
- **Aplikační garant - NÚKIB**
- **Cílem je ohodnotit a zlepšit odolnost letecké infrastruktury v ČR proti spoofingu GNSS signálu.**
- **Testujeme různé metody spoofingu a vyhodnocujeme dopady spoofingu na systémy – původně jen ŘLP nyní částečně i letadla**

ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
FAKULTA DOPRAVNÍ
KATEDRA LETECKÉ DOPRAVY

Podvržení signálu – bez tzv. „smooth“ přechodu

- **SDR + Využití volně dostupného SW**
- **Levné a „snadné“**
- **Poloha bude pro všechny v zasažené oblasti stejná**
- **Různá odolnost zařízení**
  - Letadlo ne
  - Dron ano
  - Squid ne
  - e-Identifikace ano



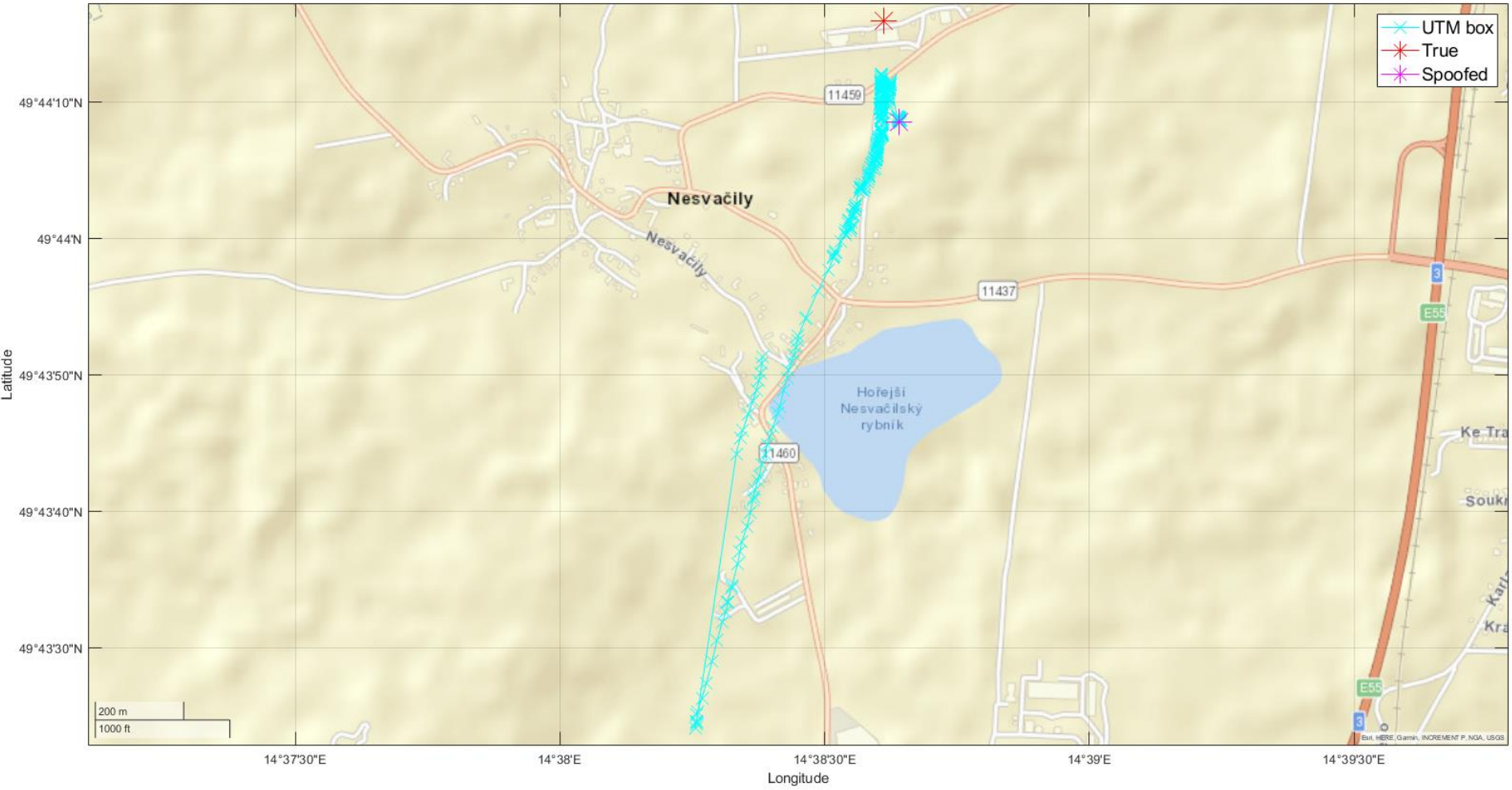
ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
FAKULTA DOPRAVNÍ
KATEDRA LETECKÉ DOPRAVY

Meaconing

- Zpoždění signálu se odvíjí od délky „kabelu“
- Spoofovaná poloha bude neměnná v místě přijímací antény
- Využití reálného signálu = větší riziko úspěšného útoku

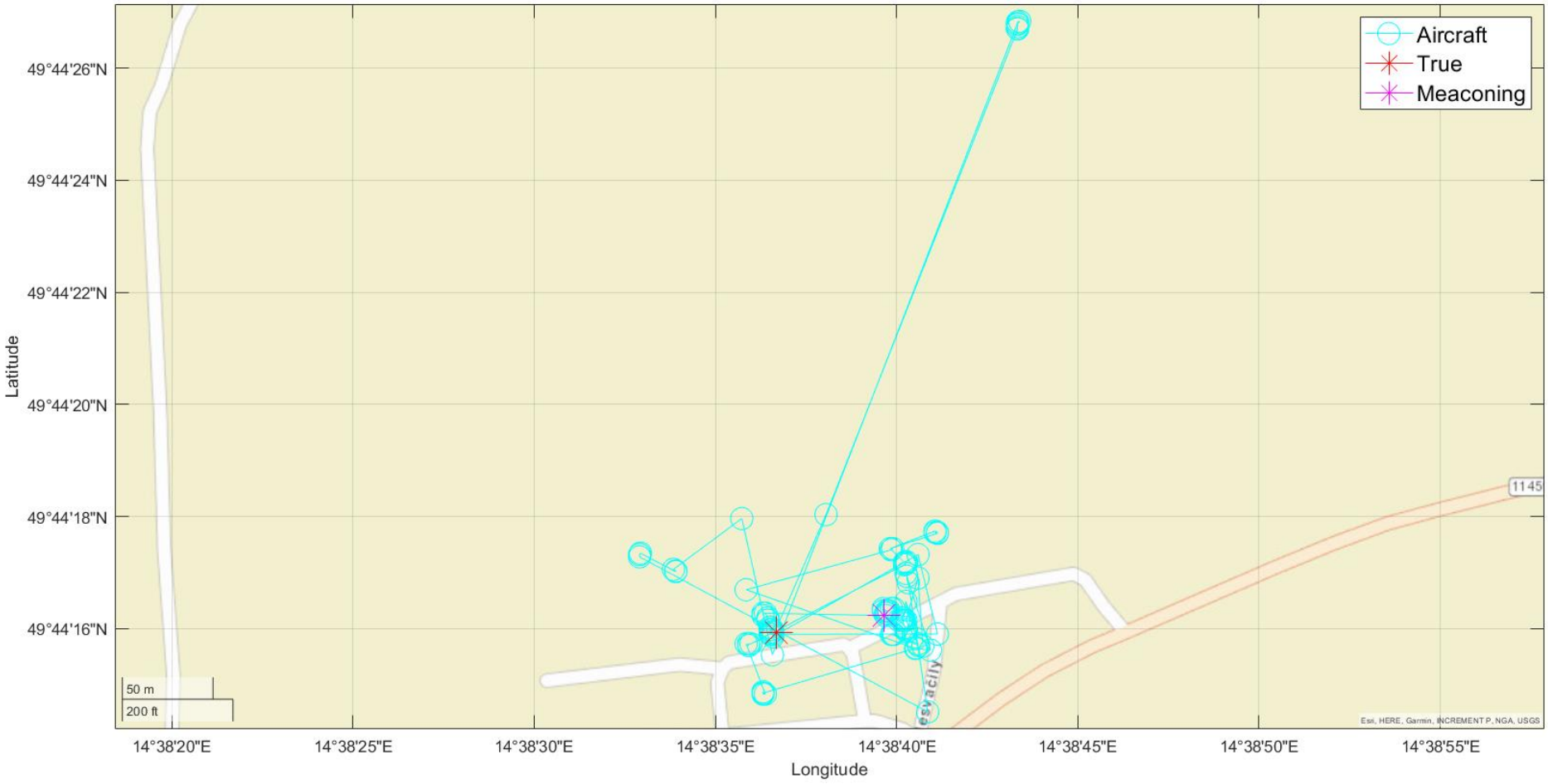
ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
FAKULTA DOPRAVNÍ
KATEDRA LETECKÉ DOPRAVY

Spoofing eID



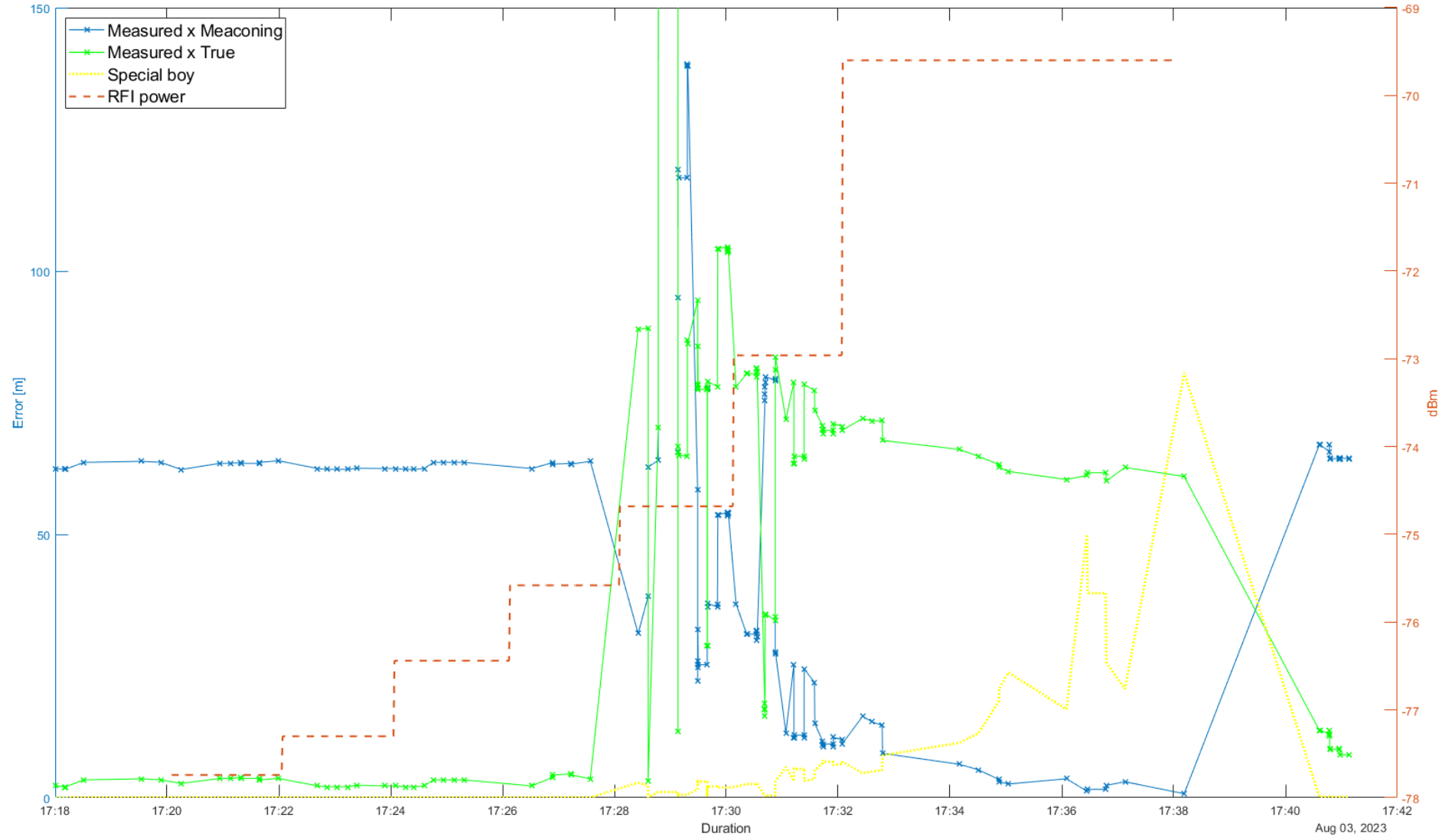
ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
FAKULTA DOPRAVNÍ
KATEDRA LETECKÉ DOPRAVY

Meaconing letounu



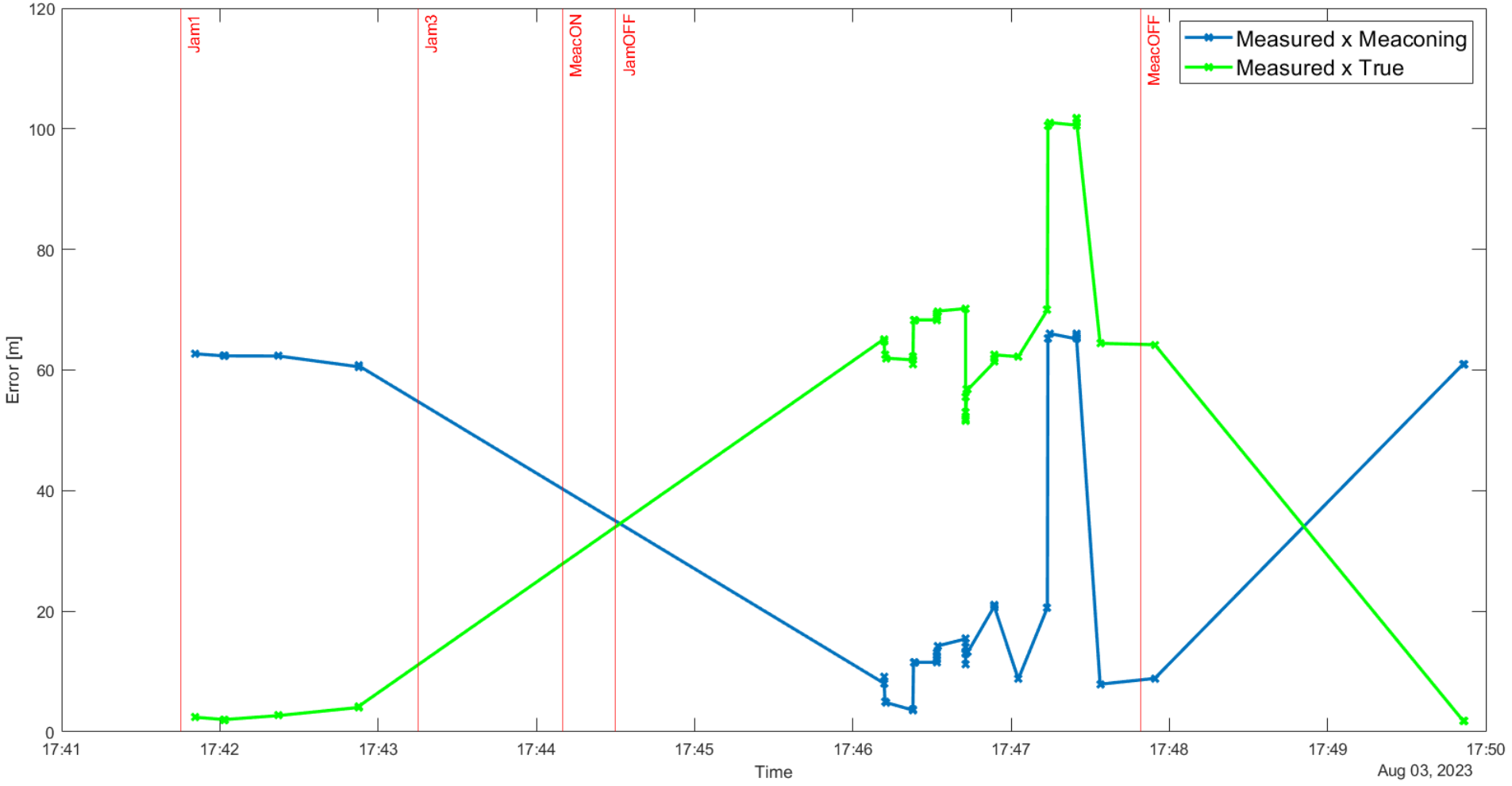
ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
FAKULTA DOPRAVNÍ
KATEDRA LETECKÉ DOPRAVY

Meaconing letounu



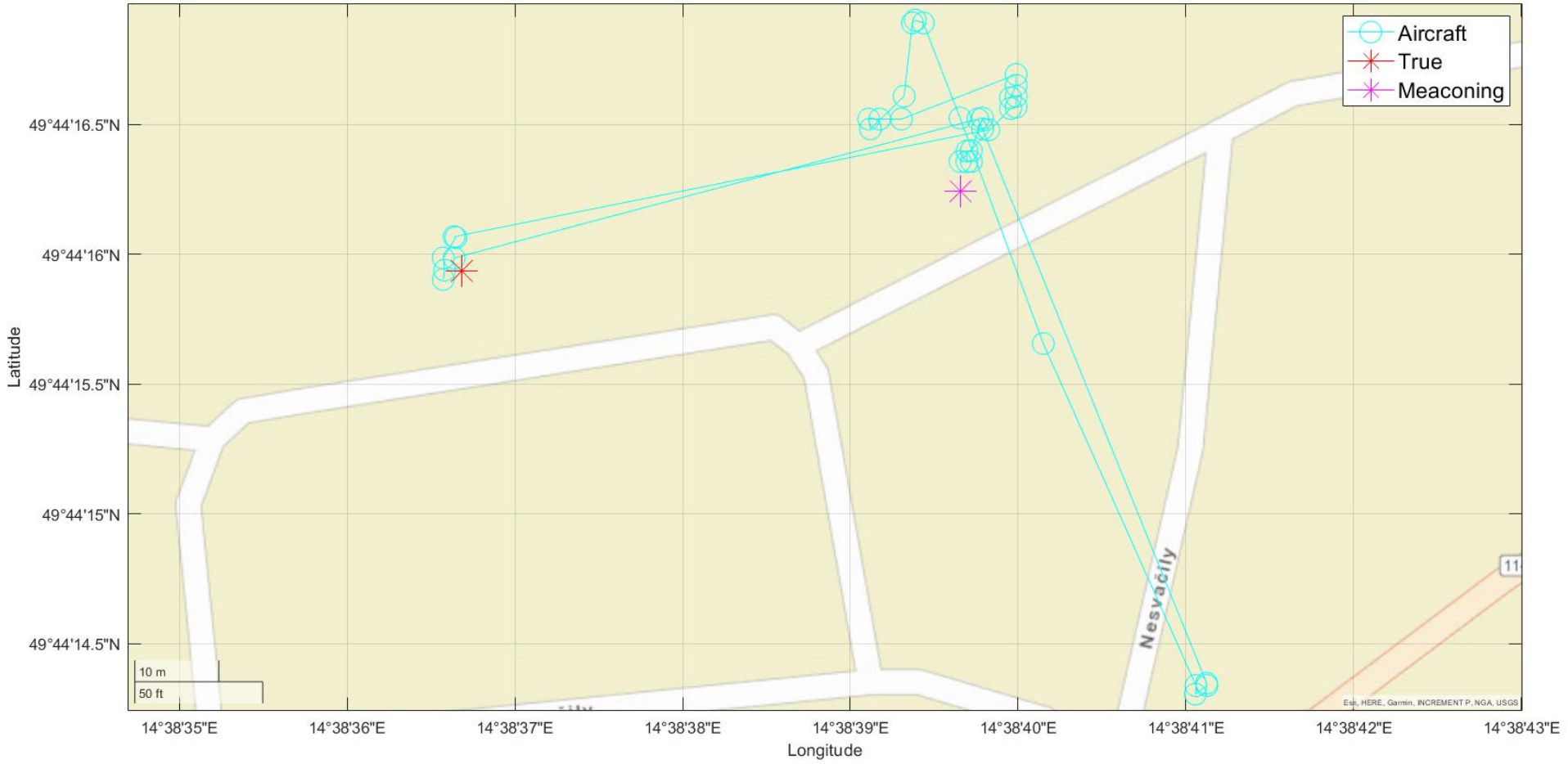
ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
FAKULTA DOPRAVNÍ
KATEDRA LETECKÉ DOPRAVY

Jamming & Meaconing letounu



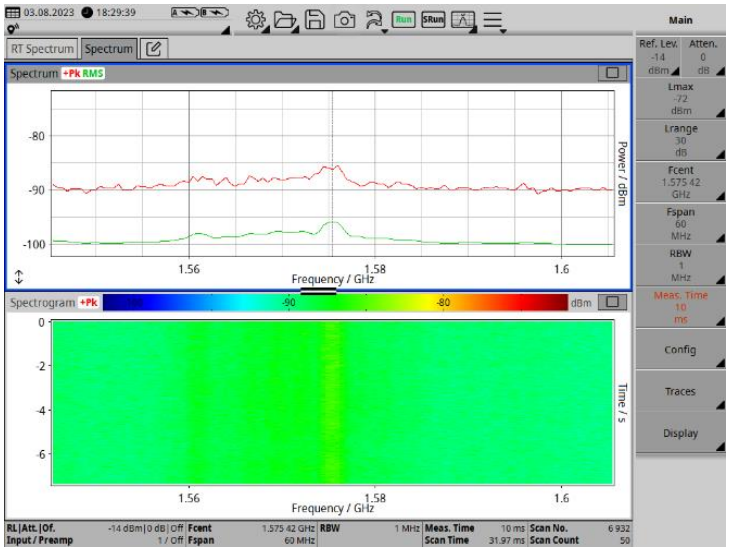
ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
FAKULTA DOPRAVNÍ
KATEDRA LETECKÉ DOPRAVY

Jamming & Meaconing letounu



Prvotní poznatky

- **Nebezpečnější je varianta jamming + spoofing**
- **I „dostupné“ metody fungují (byť ne na vše)**
- **Nebezpečím je, že systém nepozná, že je spoofován**
- **Různé systémy reagují různě – závisí na konkrétním výrobci čipu**
- **„Snadné“ metody nejsou schopné spoofovat „pod šumem“ – tedy minimální síla spoof signálu -76 dbm**



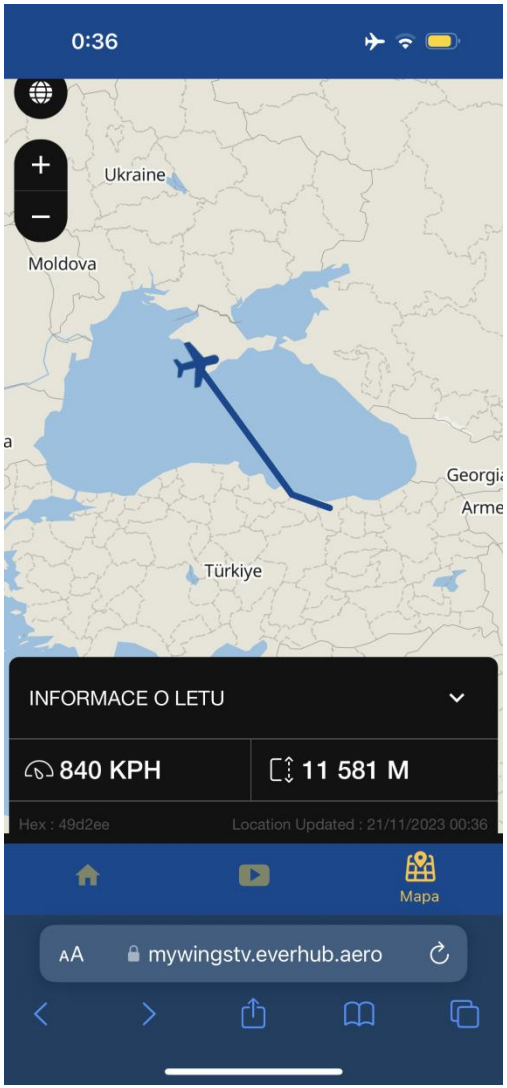
ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
FAKULTA DOPRAVNÍ
KATEDRA LETECKÉ DOPRAVY

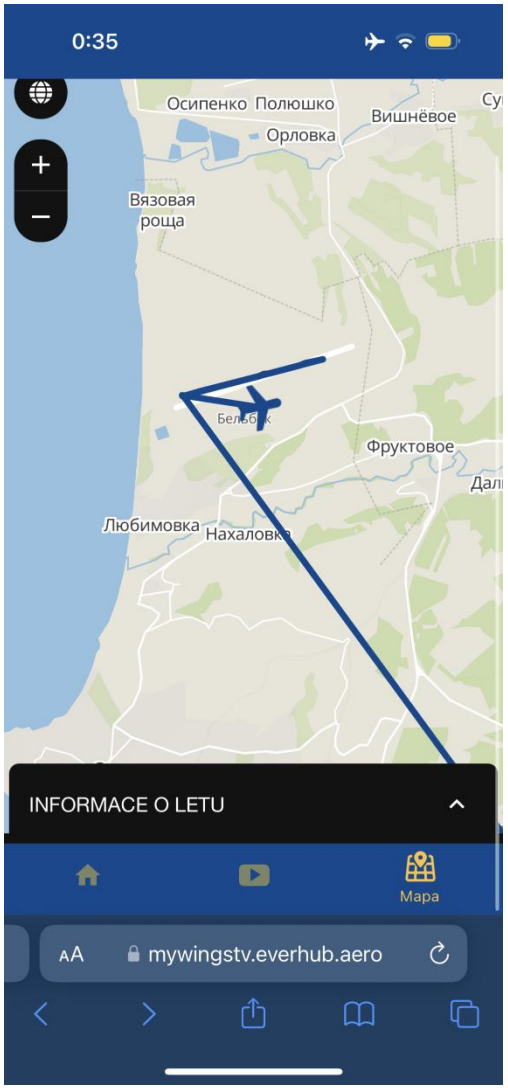
Útoky na letadla (změna projektu od 2024)

- **Identifikovali jsem více desítky případů letů které byly ovlivněny spoofingem GNSS**
- **V oblastech se složitou bezpečnostní situací – Černé Moře, Izrael, Irán**
  - Jamming se děl v těchto oblastech už cca 10 let
  - Spoofing je ale nový fenomén od 2023
- **Zdá se, že metody jsou zatím poměrně hrubé – ale i tak letadlo ovlivnit mohou**
- **Zjevně se používají různé metody spoofingu**
- **Dopad na různé systémy – GPWS, meteoradar, RAAS, EFB, infotainment**

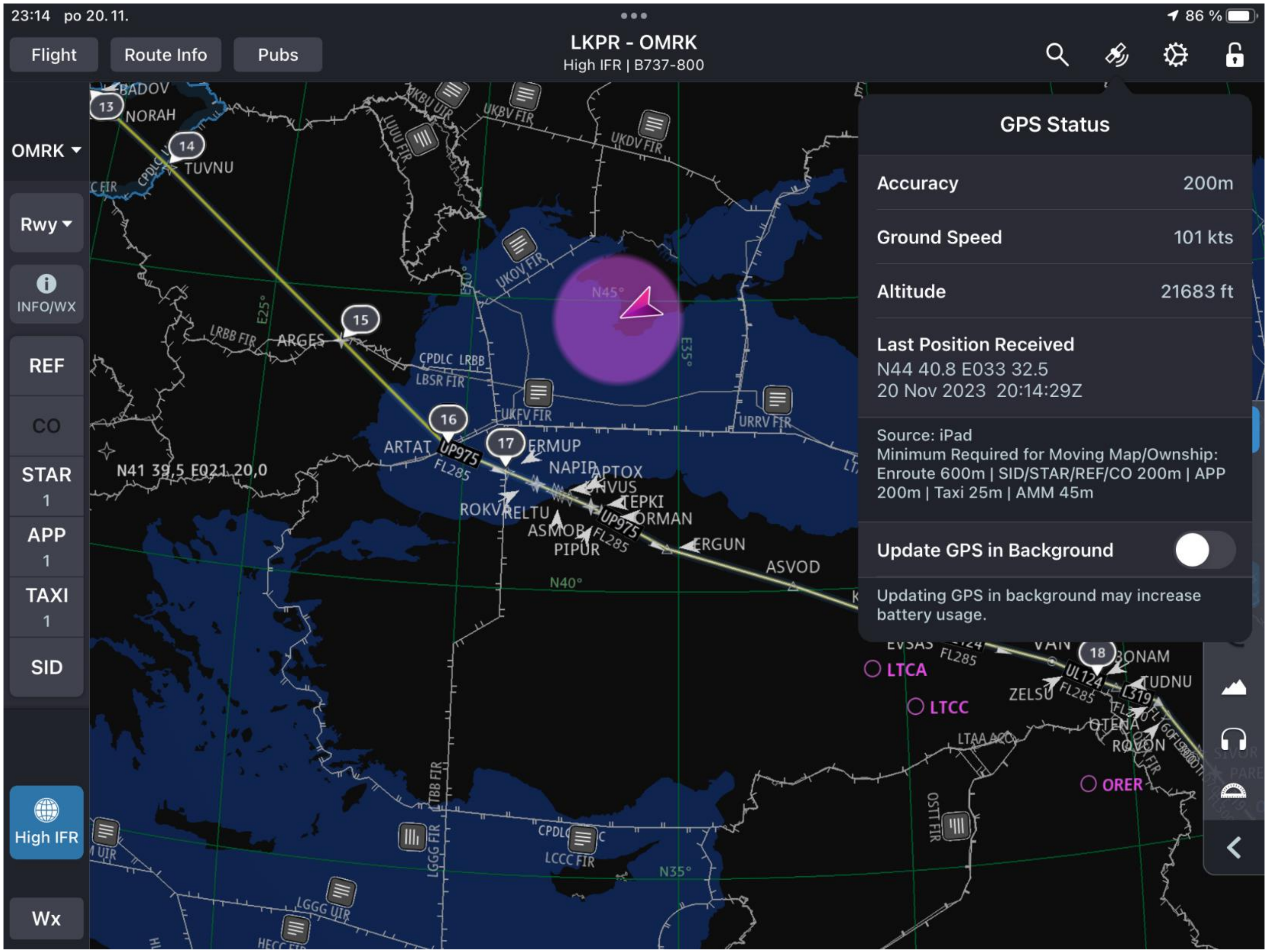
ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
FAKULTA DOPRAVNÍ
KATEDRA LETECKÉ DOPRAVY

ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
FAKULTA DOPRAVNÍ
KATEDRA LETECKÉ DOPRAVY





ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
FAKULTA DOPRAVNÍ
KATEDRA LETECKÉ DOPRAVY

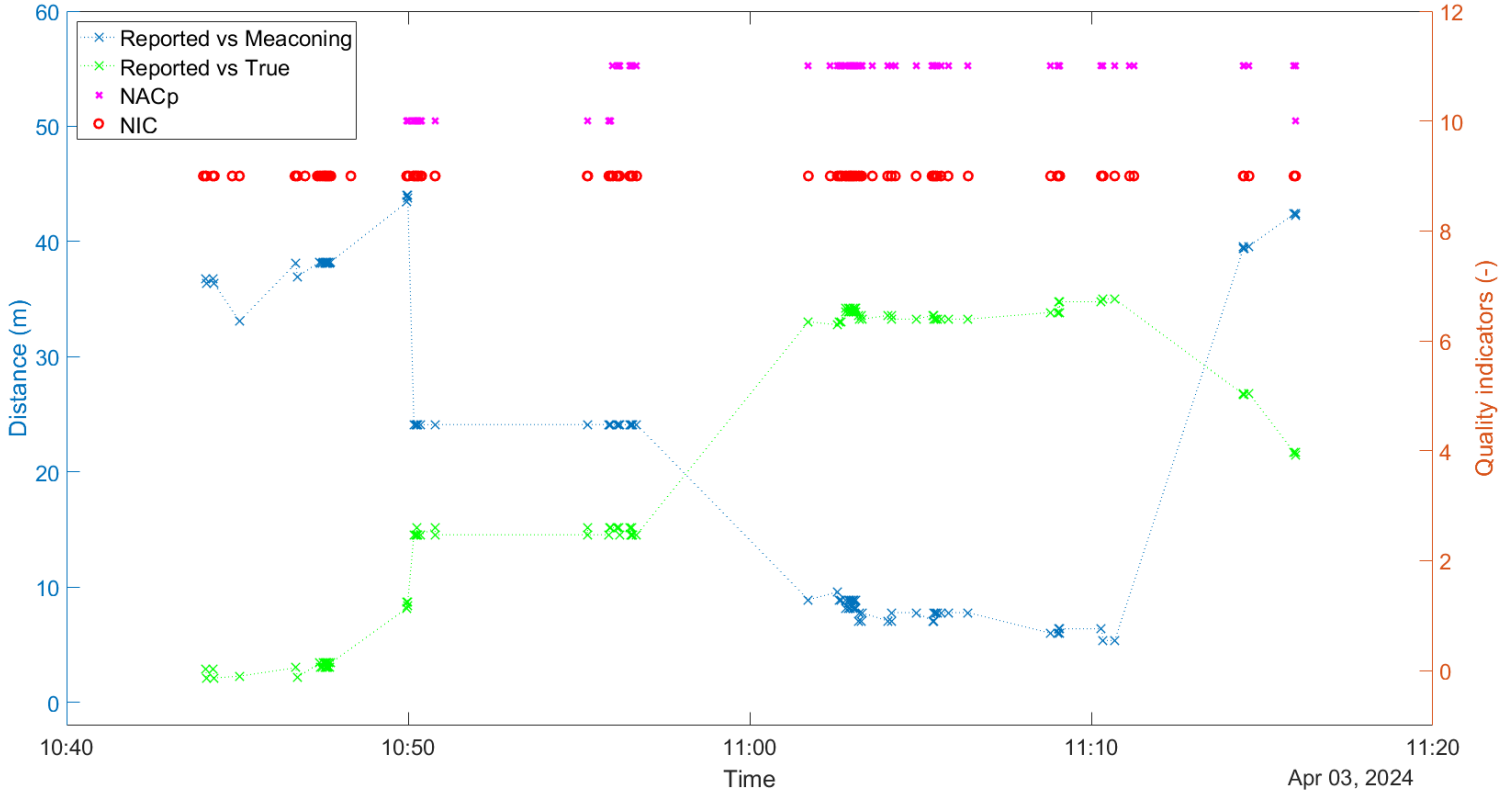

23:14 po 20.11.
86 %
Flight
Route Info
Pubs
LKPR - OMRK
High IFR | B737-800
OMRK
Rwy
INFO/WX
REF
CO
STAR 1
APP 1
TAXI 1
SID
High IFR
Wx
N41 39,5 E021 20,0
GPS Status
Accuracy 200m
Ground Speed 101 kts
Altitude 21683 ft
Last Position Received
N44 40.8 E033 32.5
20 Nov 2023 20:14:29Z
Source: iPad
Minimum Required for Moving Map/Ownship: Enroute 600m | SID/STAR/REF/CO 200m | APP 200m | Taxi 25m | AMM 45m
Update GPS in Background
Updating GPS in background may increase battery usage.


LRCV
80
LBPL
10
10
LBGO
0.0
FMC R
RNP 2.00
ANP 0.17
POS SHIFT 3/3
FMC-L FMC-R
<111°/0.0NM 119°/0.0NM>
GPS-L GPS( ) GPS-R
<165°/ 36NM 165°/ 36NM>
IRS-L IRS(2) IRS-R
<305°/0.5NM 043°/0.7NM>
RNP/ACTUAL RADIO
2.00/0.17NM 107°/0.0NM>
NAV STATUS>
<INDEX
GND PROX
SYS TEST
RUNWAY
FLAP INHIBIT
GEAR INHIBIT
NORM
A
B
C
D
E

ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
FAKULTA DOPRAVNÍ
KATEDRA LETECKÉ DOPRAVY

Útoky na letadla – 2024 – sofistikovanější

Spoofing nelze snadno identifikovat pomocí indikátorů kvality



ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
FAKULTA DOPRAVNÍ
KATEDRA LETECKÉ DOPRAVY

Další plánované činnosti v projektu

- Ověření chování některých systémů ŘLP při spoofingu pomocí meaconing a SDR
- Nový typ spooferu který by měl být na podobném pricipu jako SDR ale dají se nastavovat další prvky a předpokládáme že bude účinnější
- Testování dopravního letadla na Ruzyni
- Testování různých systémů pomocí nového spooferu
- Testování systému ADS-B
- Meaconing signálu PRS ne frekvenci E6 (kvůli službě PRS)
- Sběr dat od dopravců, ŘLP a ÚZPLN k identifikaci spoofingu
- Ověření podezření na spoofing v ČR

ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

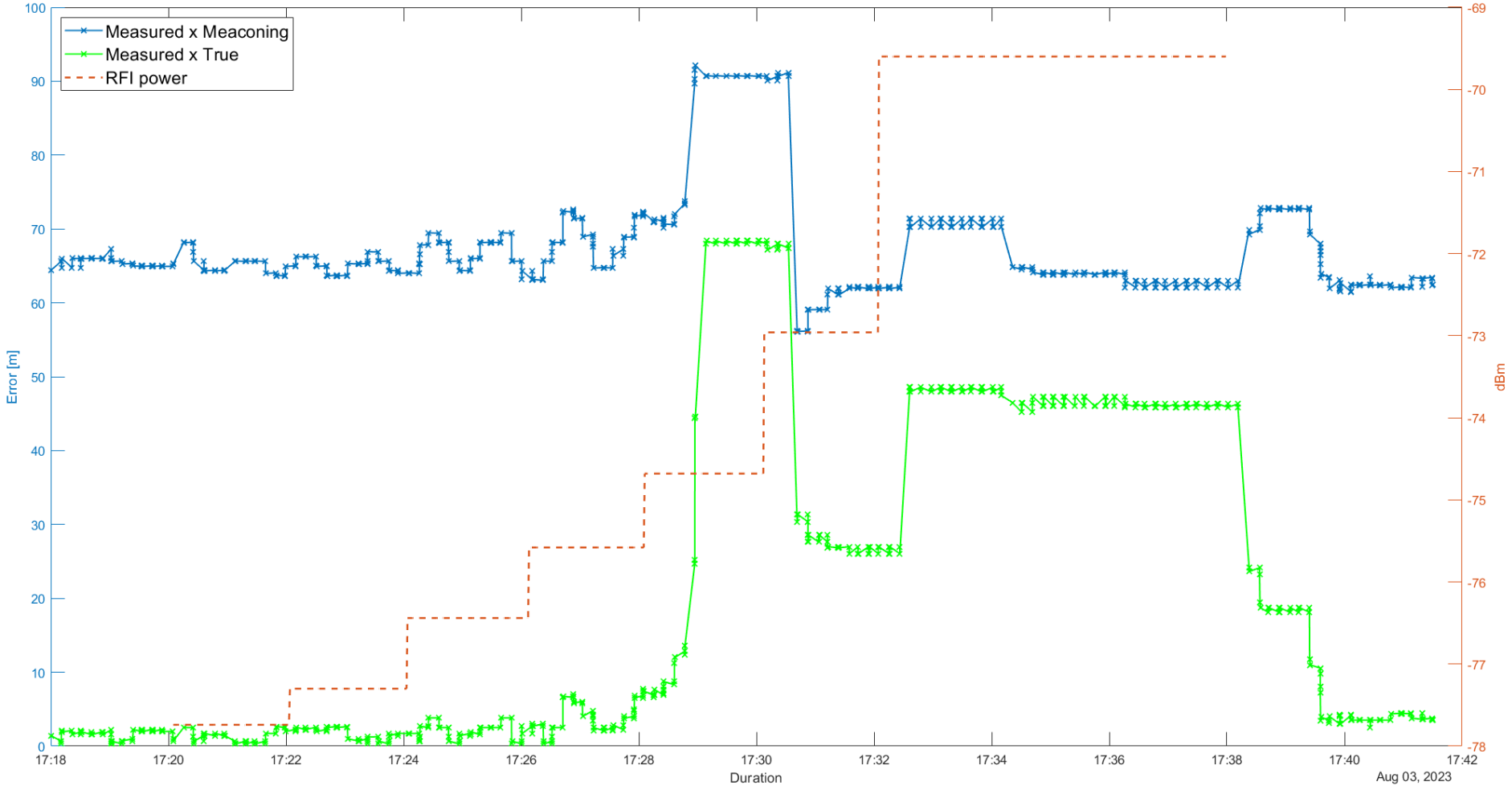
Děkuji za pozornost

Katedra letecké dopravy ČVUT v Praze

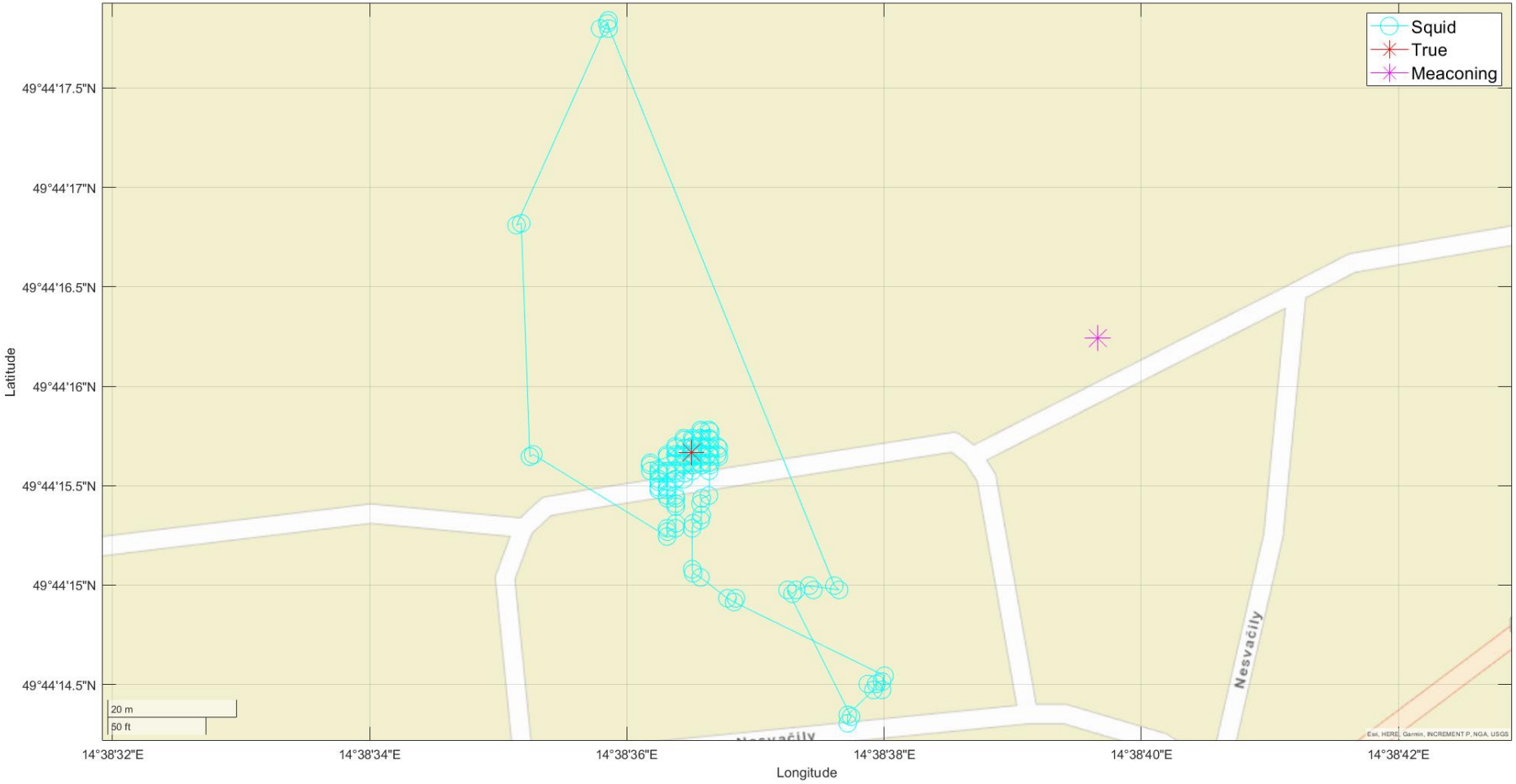
Jakub Hospodka – hospodka@fd.cvut.cz

Back-up snímky

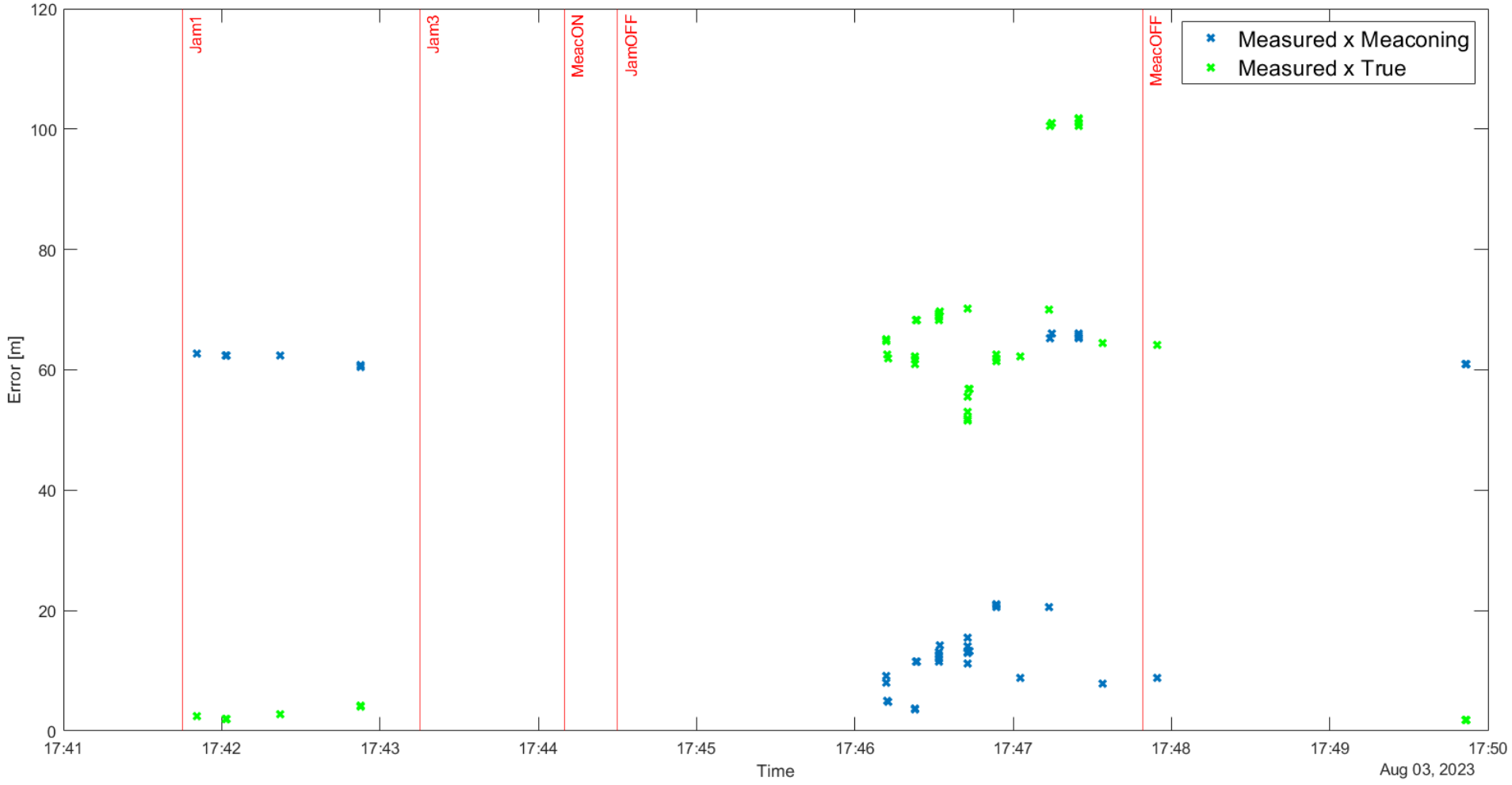
Meaconing Squidu



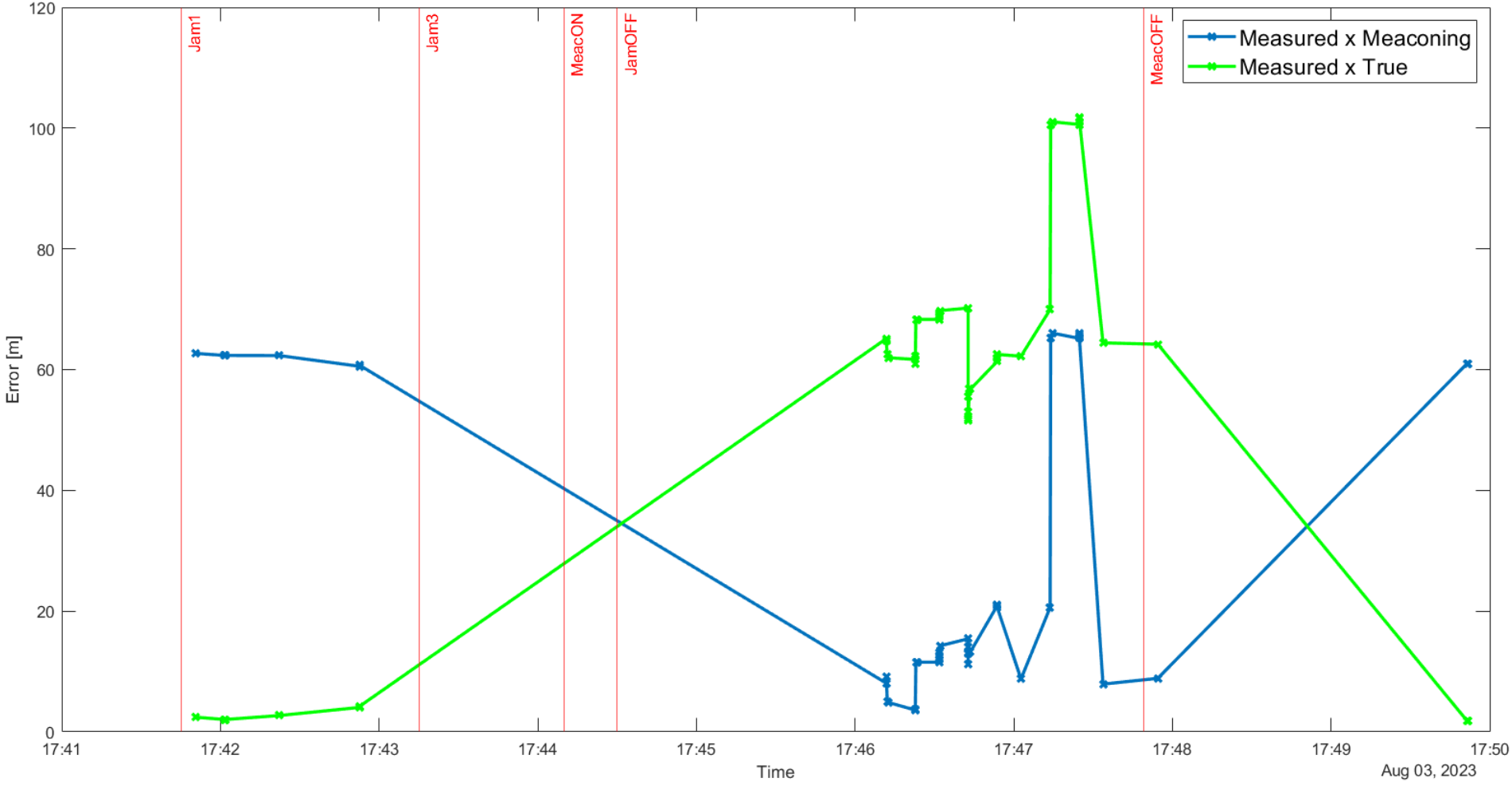
Meaconing Squidu



Jam&Meacoing Tecnam

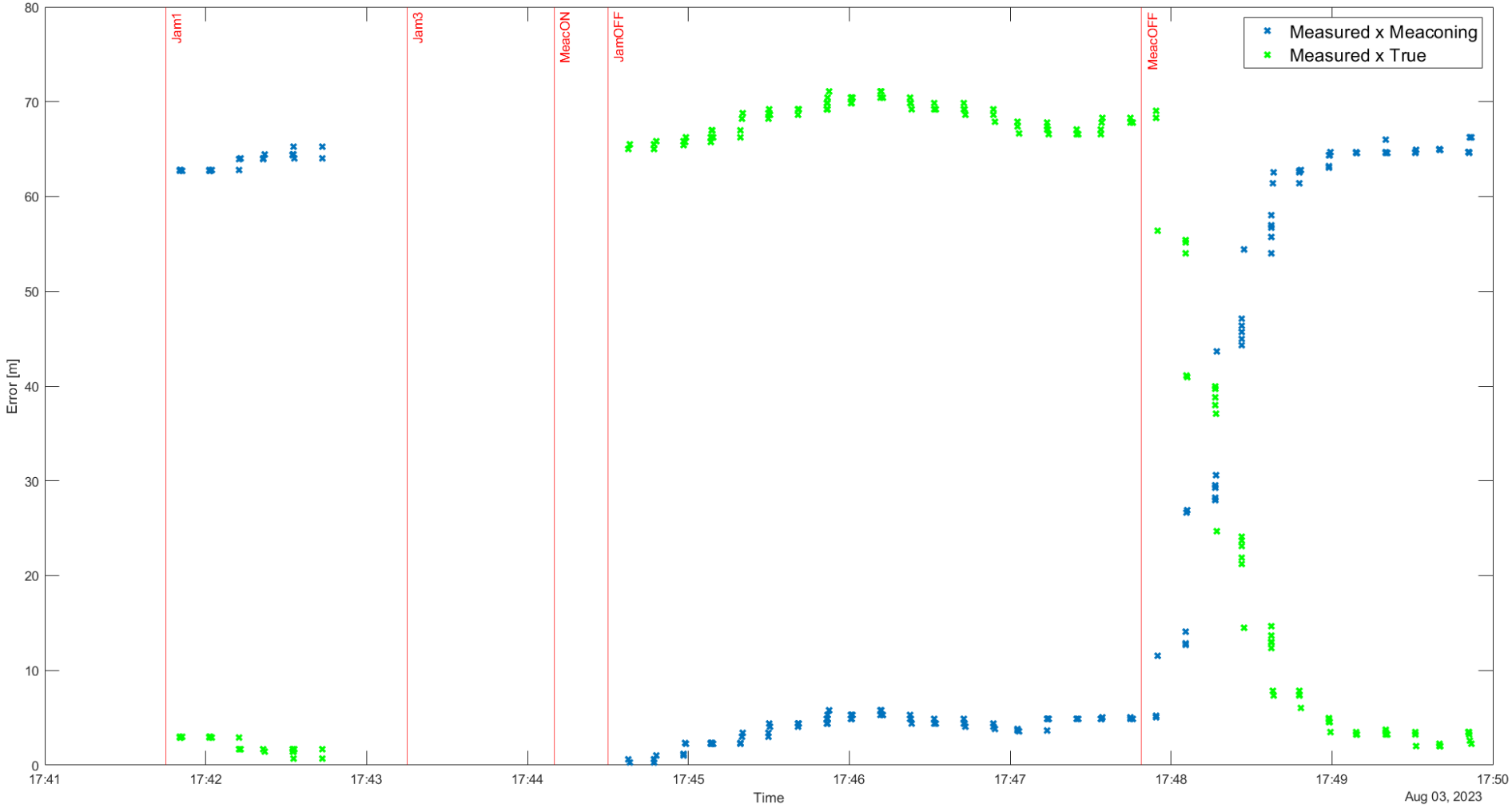


Jam&Meacoing Tecnam

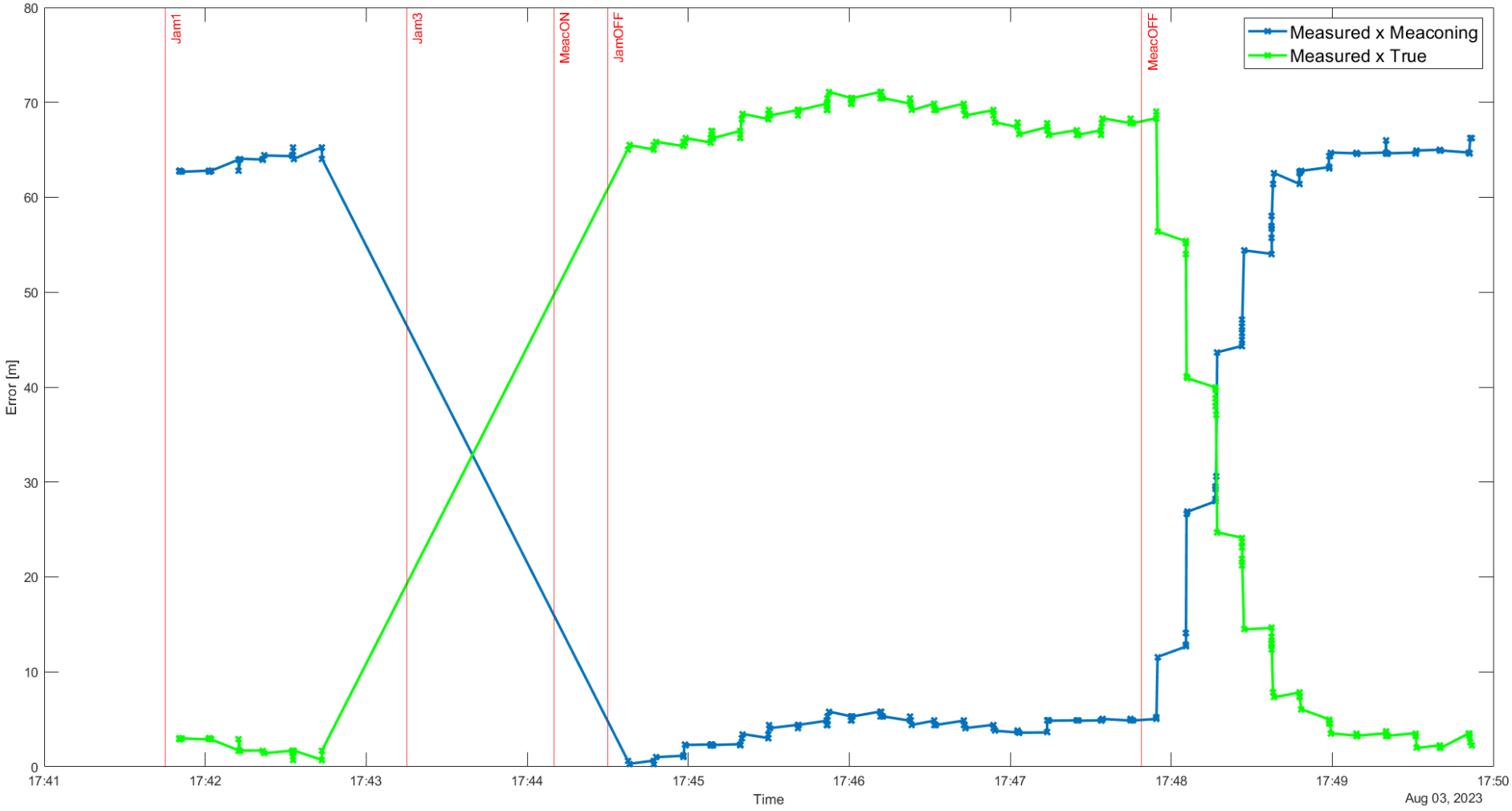


Jam&Meacoing Tecnam

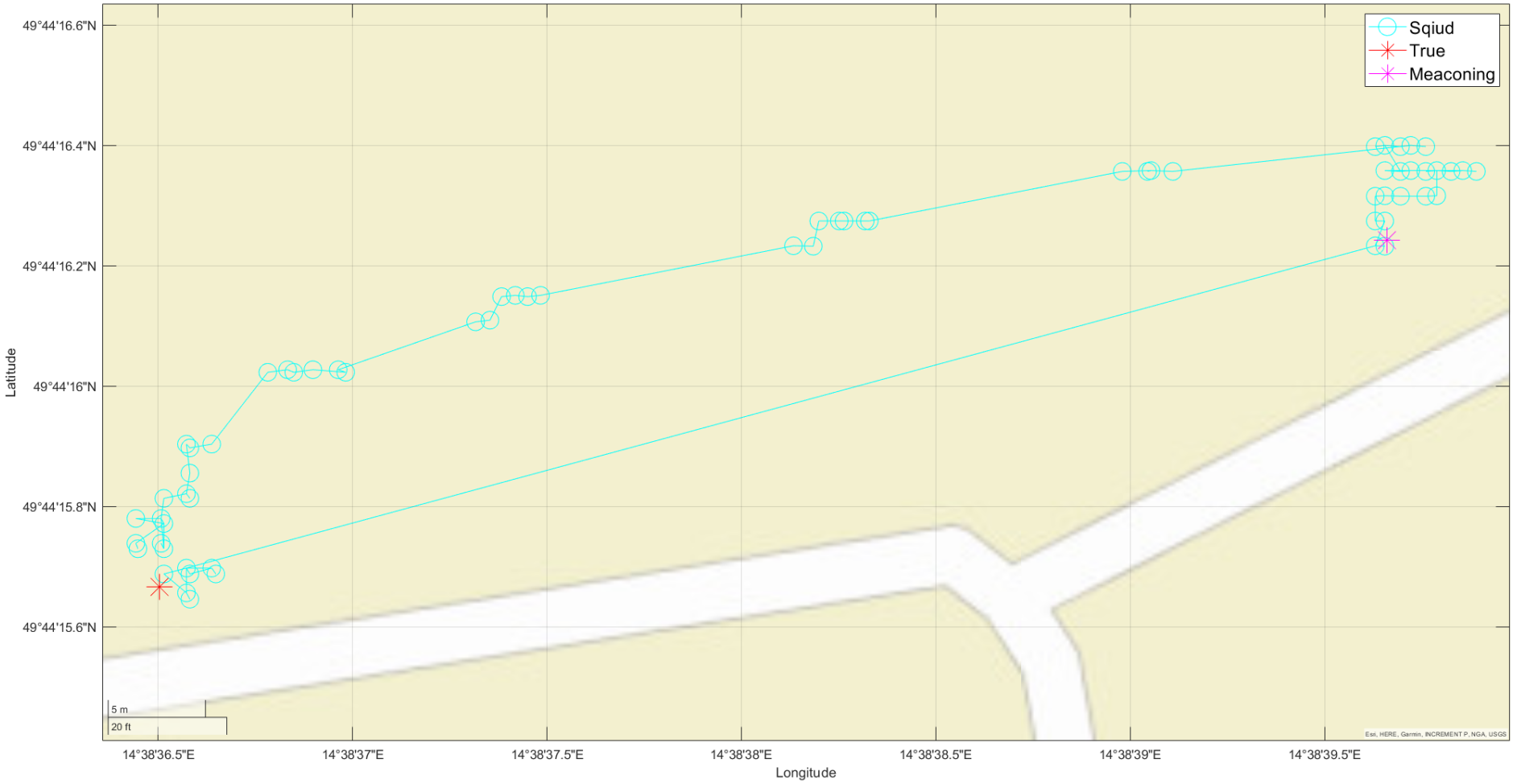
Jam&Meacoing Squidu



Jam&Meacoing Squidu



Jam&Meacoing Squidu



Doplňující materiály

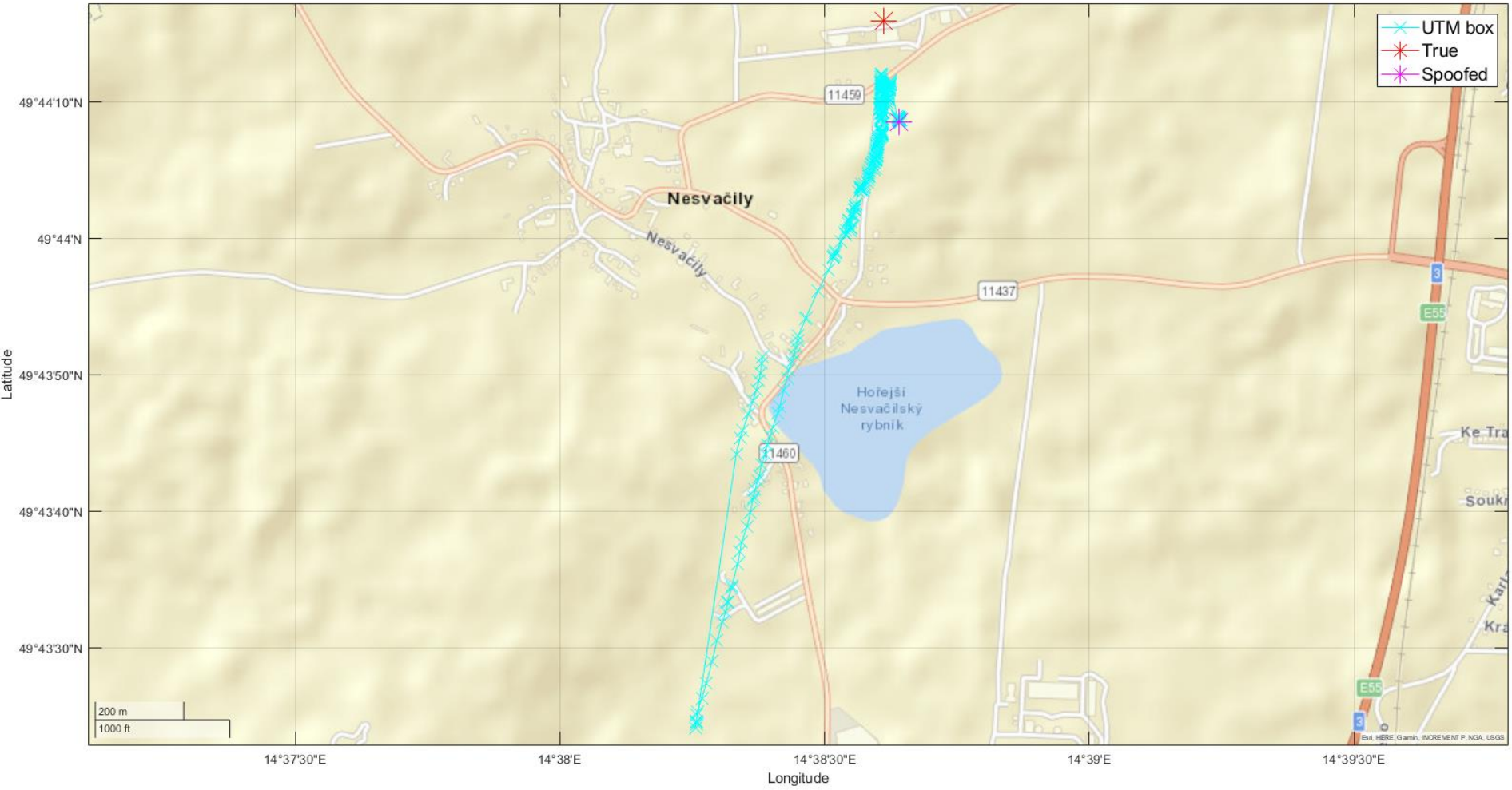
- The satellites have an orbit altitude of 20200 km (90 degrees elevation) from earth. It's transmit power is 44.8 Watt at 1575.43 MHz and the antenna gain is 12 dBi.

LKBE experimenty

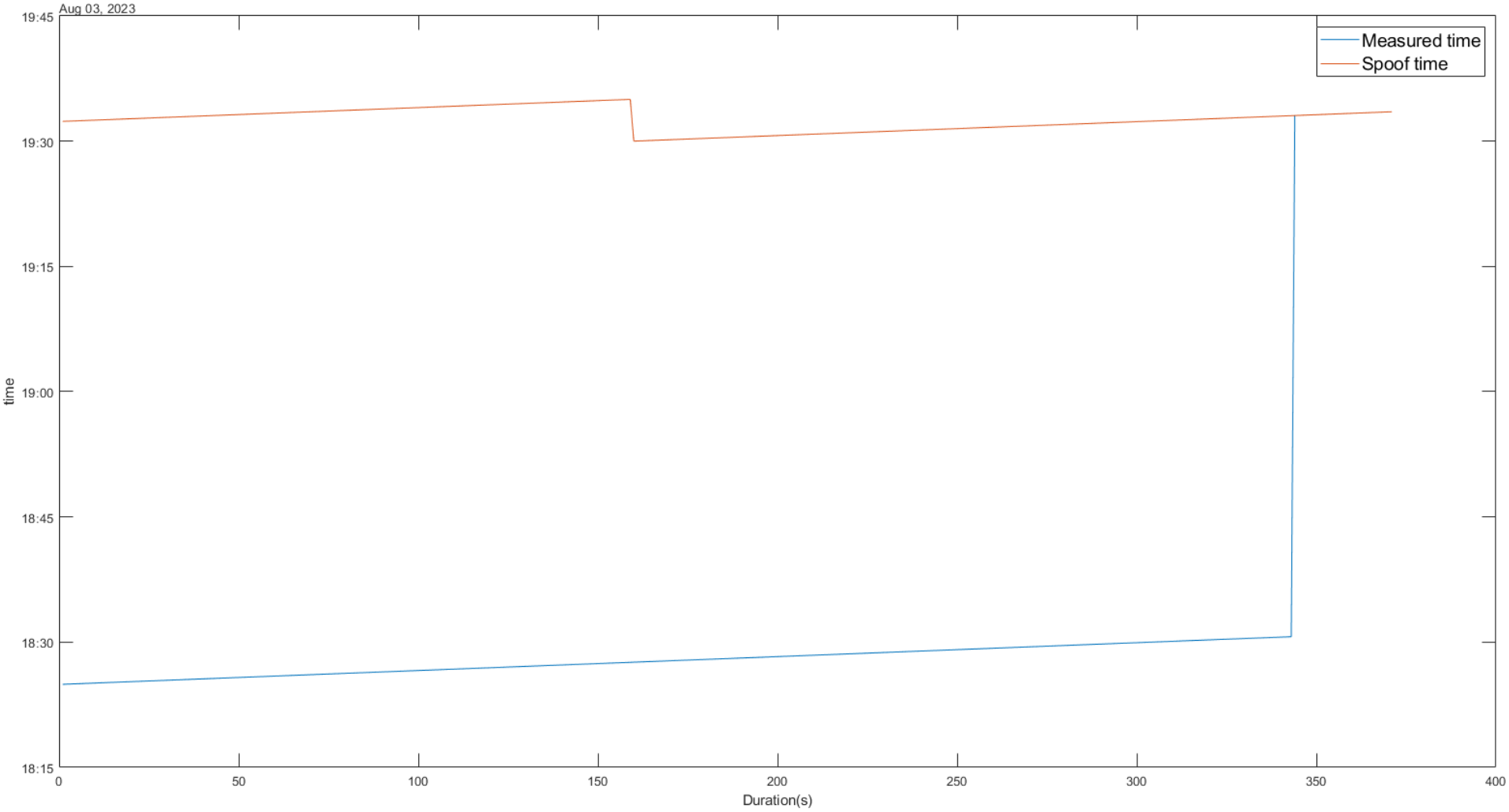
- ScC – Spoofing vs eID dronu

- HackRF spoofing + gps-sdr-sim
- 200m od letiště
- 1h časový posun
- Výkon: 75 dBµV/m

Spoofing eID



Spoofing eID



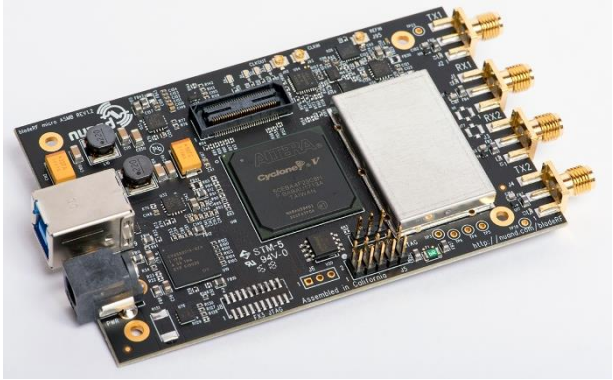
Možnosti HackRF

- Vzorkování: 8 bit, 20 MSPS
- Half-duplex
- Nadstavba Mayhem

- GPS-SDR-SIM → GPS L1
  - Nastavení polohy, času
  - Dynamic mode, max 5min
  - Static mode, max 24h

Možnosti BladeRF

- Vzorkování: 12 bit, 40 MSPS
- Full-duplex



- GPS-SDR-SIM
- Galileo-SDR-SIM
  - Ve vývoji
  - Gal E1

FEL: Meaconer

- GPS L1 C/A signál
- Zpoždění signálu se odvíjí od délky kabelu
- Nastavitelný vysílací výkon (0-30 dBm)

FEL: Tester spoofingu

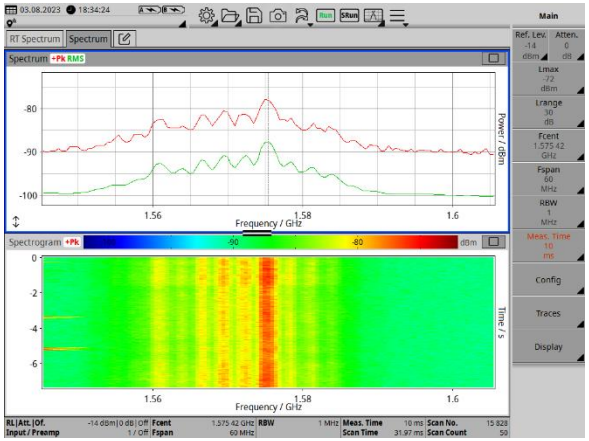
- Generování 2 signálů – repliky autentického a podvrženého
- GPS L1 C/A signál
  - Nastavitelný vzorkovací kmitočet
- Podpora statického a pohyblivého uživatele; Vzorkovací kmitočet polohy 10 Hz
- Volba délky a času simulace, max. délka 60 min.
- Možnost modifikace navigační zprávy a generování chyb při přenosu
- Generování podvržených signálů (spoofingu) –
  - stejná nebo modifikovaná navigační zpráva
  - Nastavování výkonu signálu a podvrženého signálu
  - Kladné a záporné zpoždění podvrženého signálu od 0 s po několik let

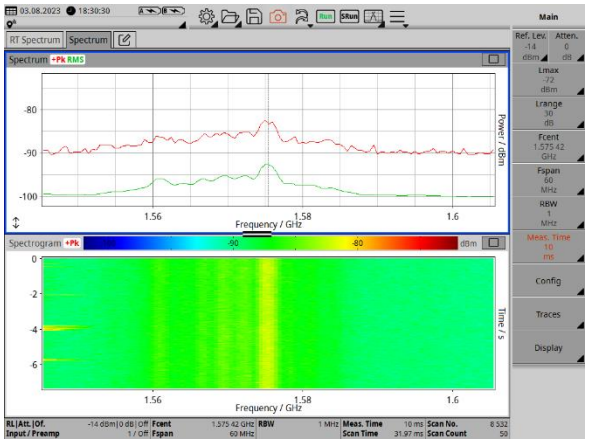
FEL: Tester spoofingu

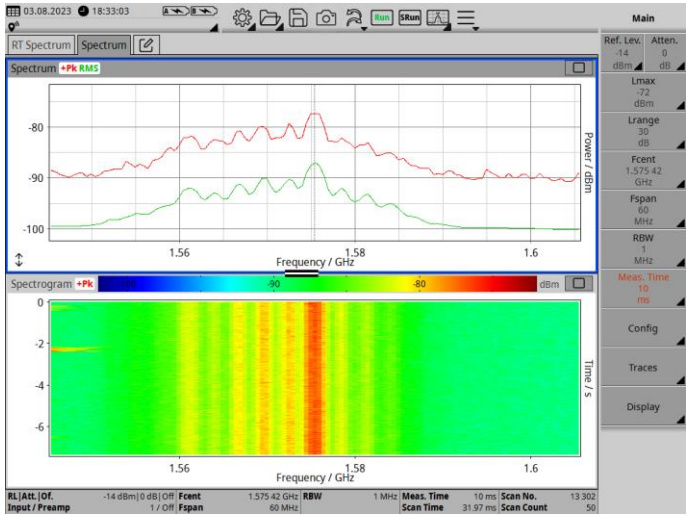
- Modelování vyzařovacího diagramu přijímací antény
- Možnost modelování zastiňování antény
- Zavádění ionosférického a troposférického zpoždění
- Mnohocestné šíření – paprskový model, přímý signál + dva odražené

ČVUT

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE







ČVUT

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE