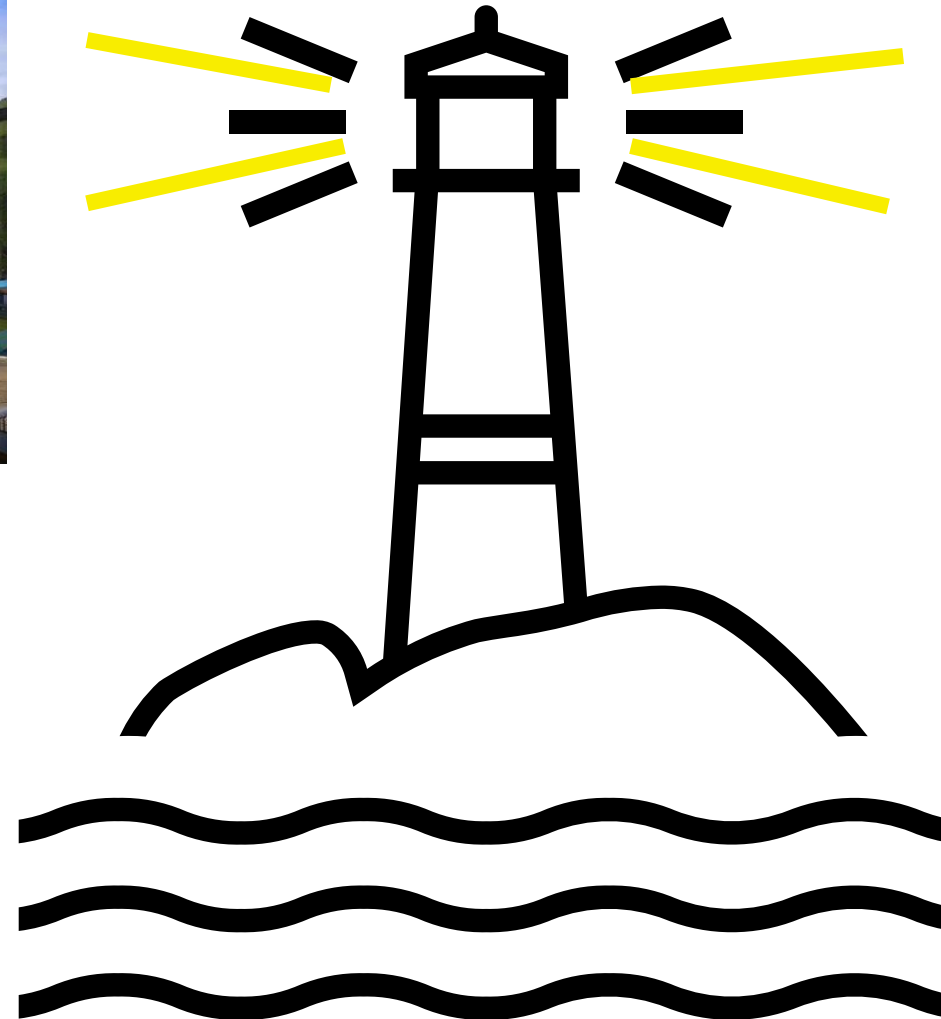


Falsche Koordinaten, echte Gefahr - GNSS Jamming und Spoofing

*Prof. ZHAW Dr.-Ing. Michael Felux
Benoit Figuet, Raphael Monstein, Valentin Fischer,
Zürcher Hochschule für Angewandte Wissenschaften (ZHAW)*





1000W +

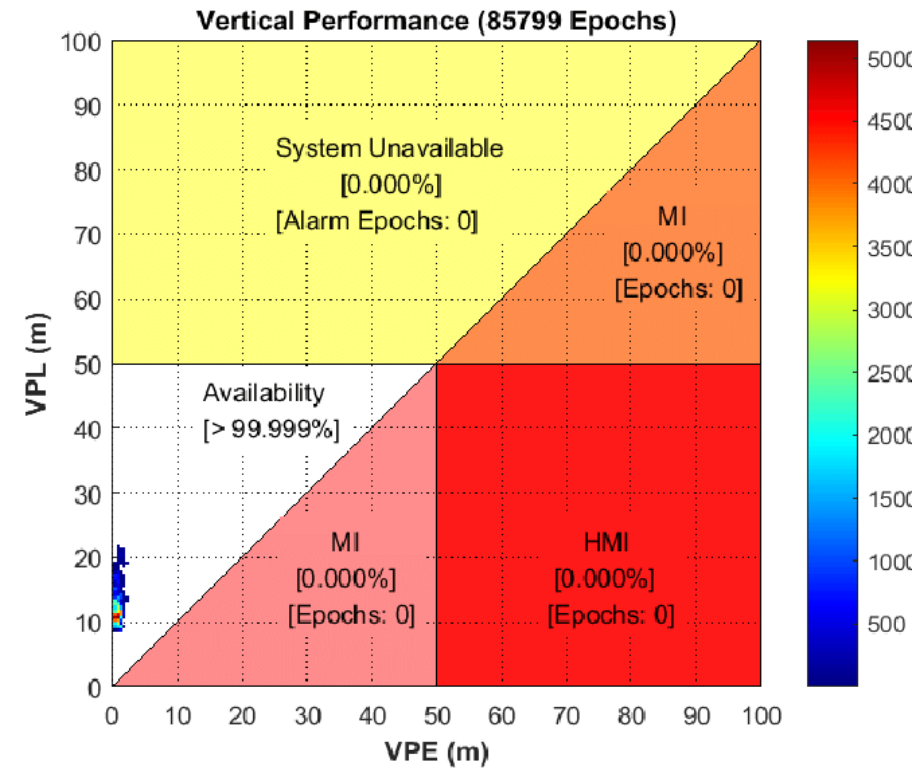
Wie weit sieht man Leuchtturm?



- ~20.000 km Entfernung
- ~100 W Sendeleistung
- Empfangsleistung:
ca. -150dBW



- GNSS Rückgrat der Navigation
- Flugzeug, Schiff, Auto, UAV, Handy..
- Aber auch genauestes und global verfügbares System zur Zeitsynchronisation



D. Kim et al., 2016, A Study of SBAS Position Domain Analysis Method: WAAS and EGNOS Performance Evaluation

Ist das eine gute Idee?

Aviation these days

Testflug zu Spoofing bereits im Februar 2020



- Denial of Service
- Aussenden eines Störsignals auf der/den GNSS Frequenz(en)
- GNSS Signale nicht mehr empfangbar

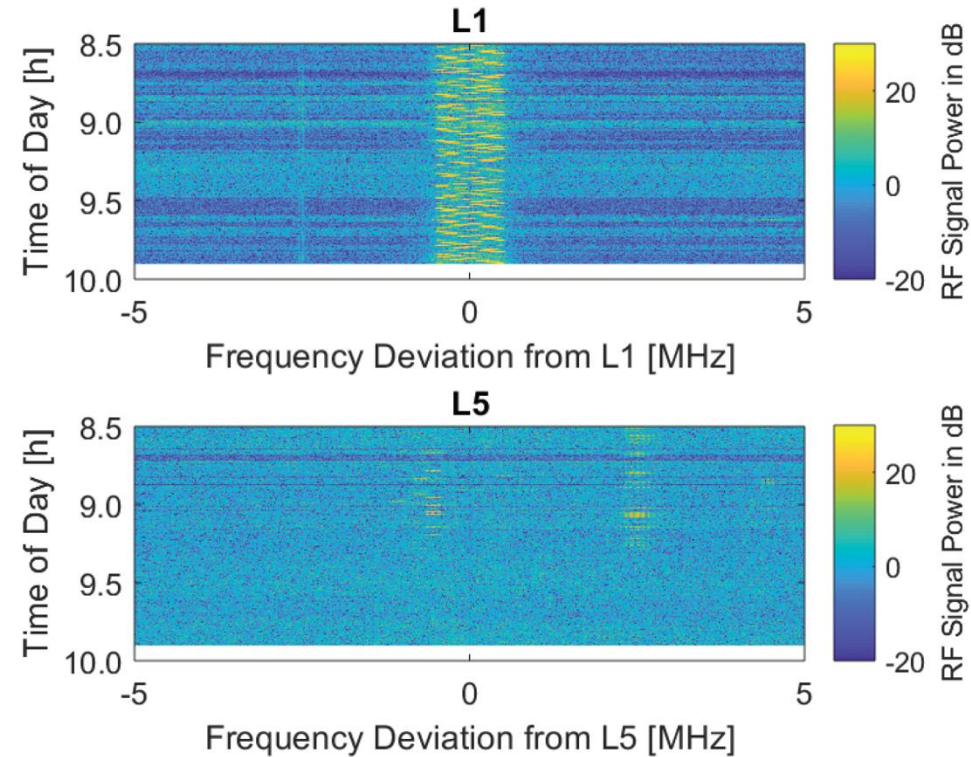


Image: O. Osechas et al., 2022, Impact of GNSS-Band Radio Interference on Operational Avionics, Navigation



Bild links: Septentrio

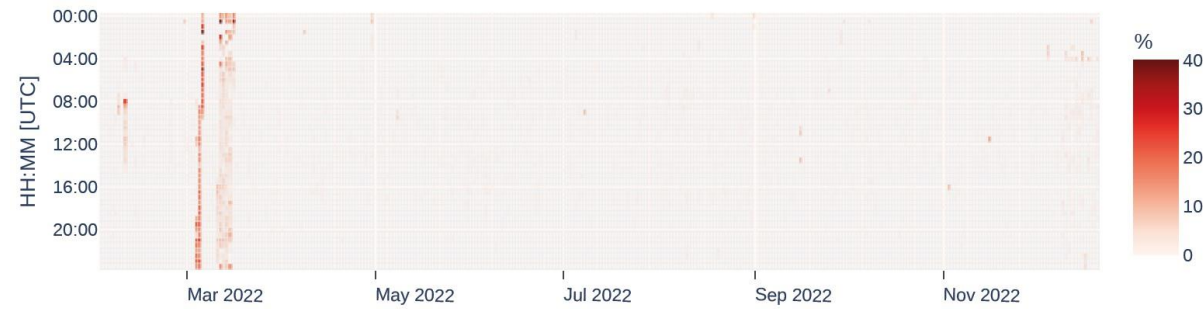
Bild rechts: Wikipedia

Zivile Luftfahrt in aller Regel Kollateralschaden

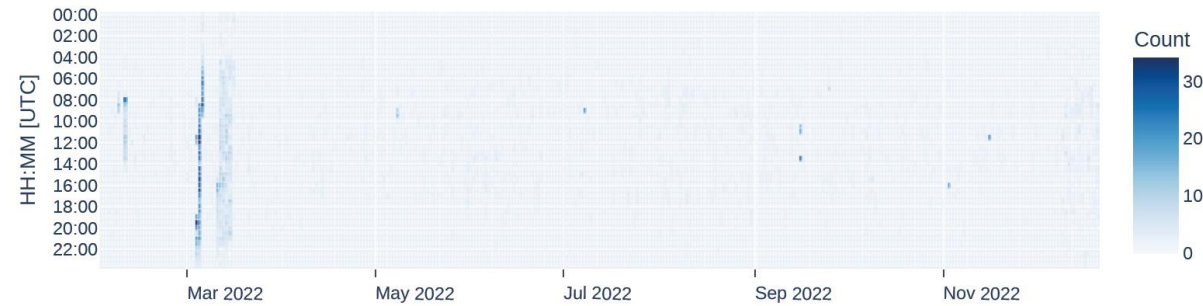
Betroffener Flugverkehr

Im Jahr 2022

Baltikum

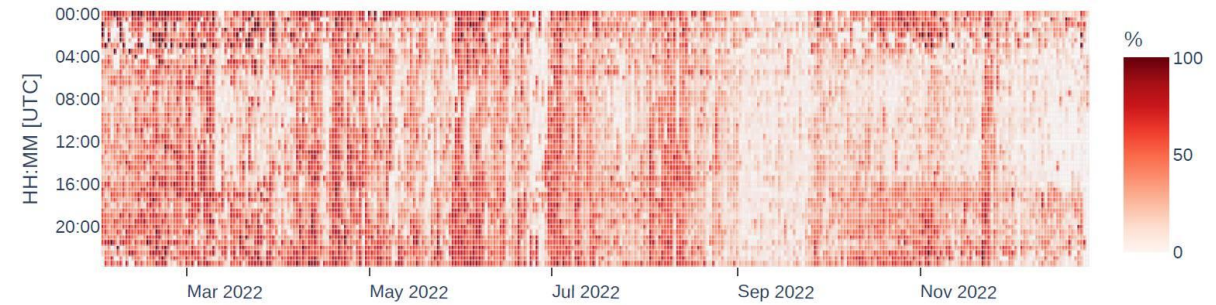


(a) Relative share of aircraft being subject to RFI.

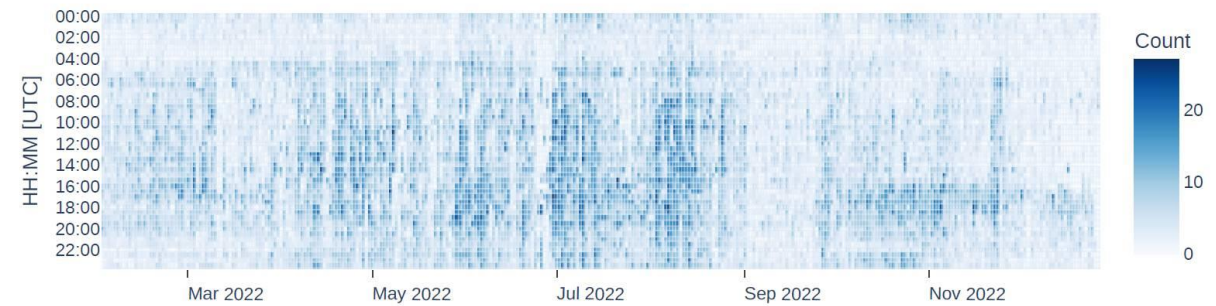


(b) Absolute number of aircraft being subject to RFI.

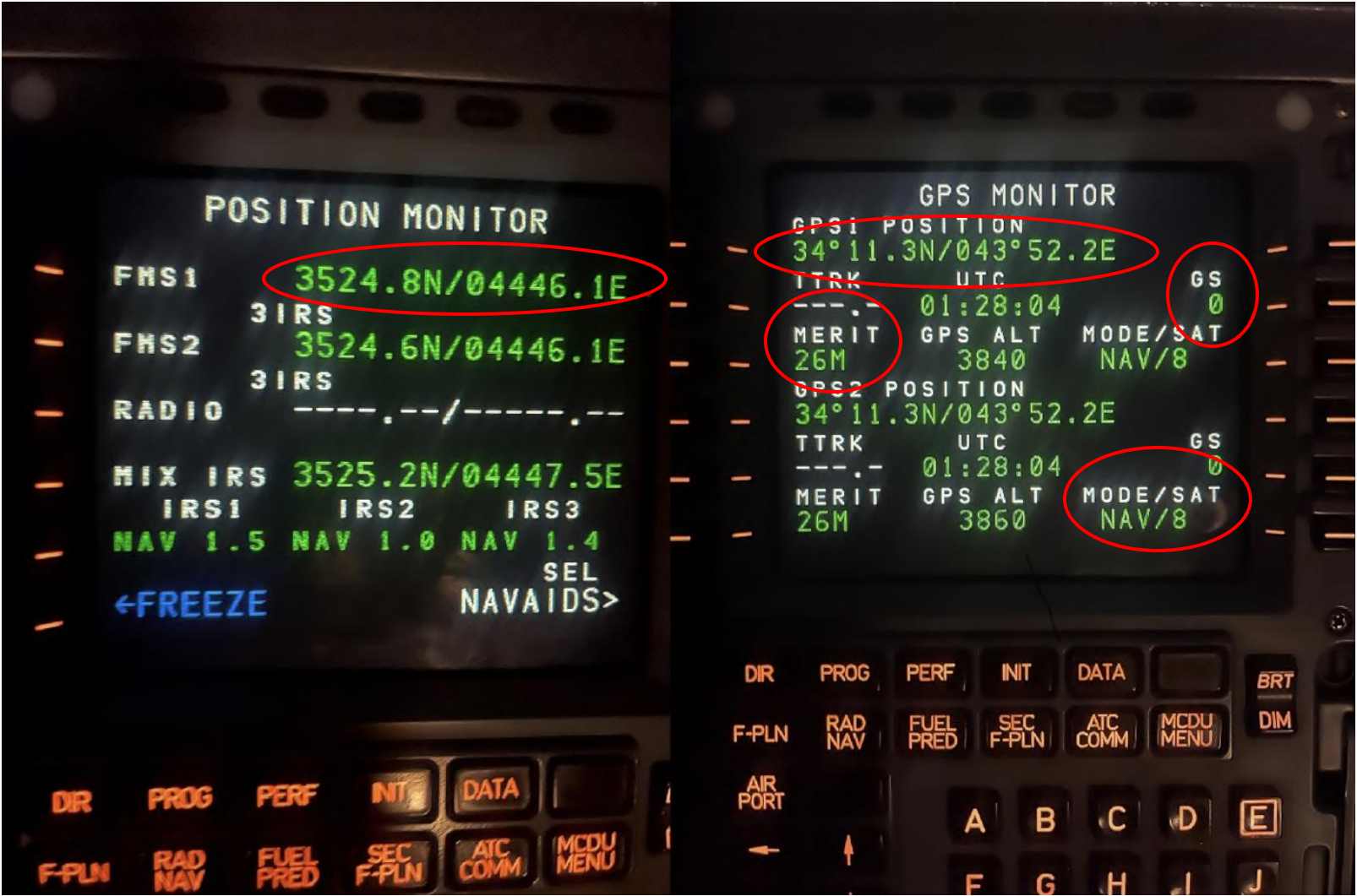
Östliches Mittelmeer



(a) Relative share of aircraft being subject to RFI.



(b) Absolute number of aircraft being subject to RFI.



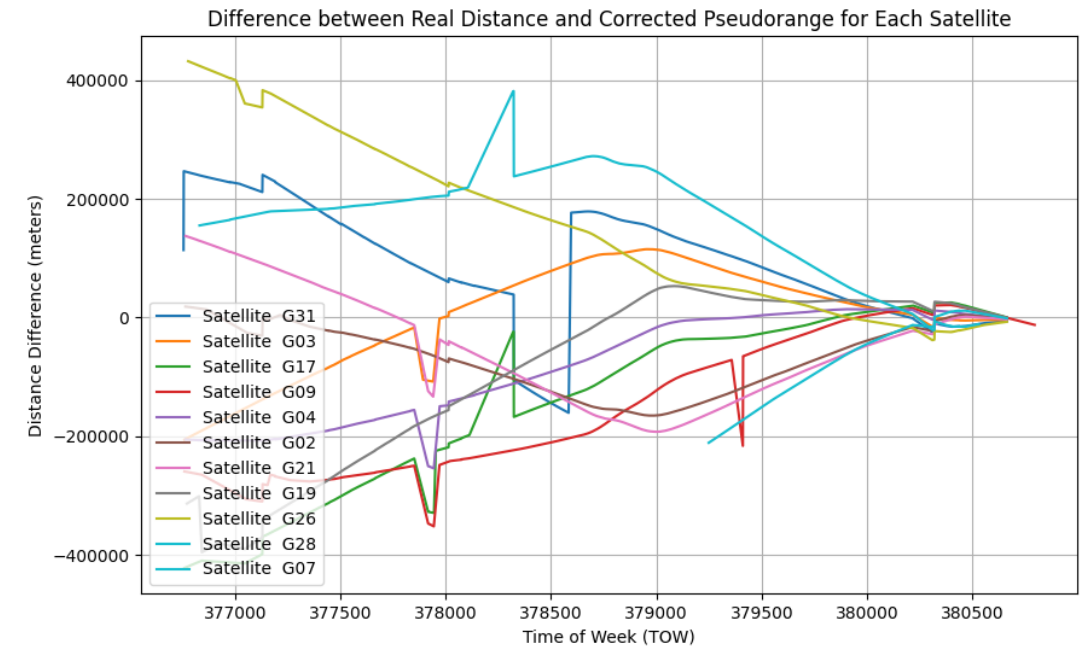
Source:

OpsGroup Report on
GPS Spoofing
<https://ops.group/blog/gps-spoofing-final-report/>

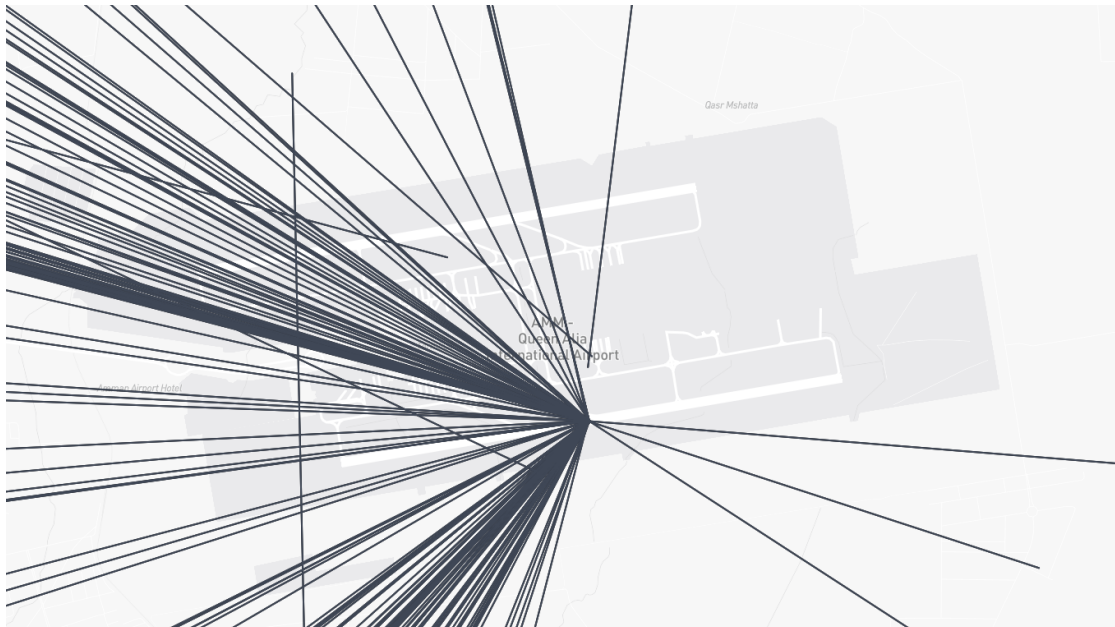
Spoofing

Wie funktioniert das?

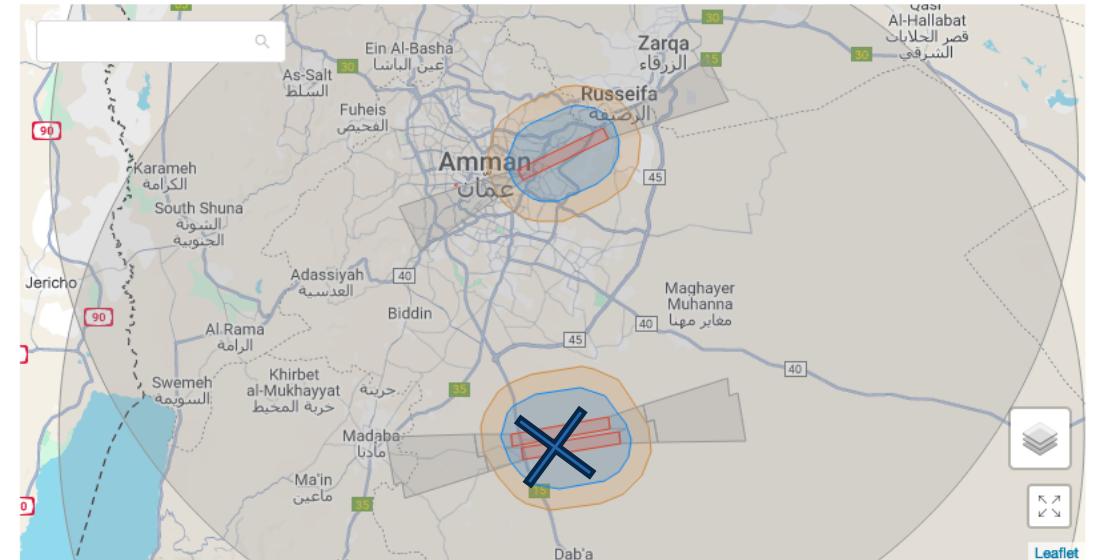
- GNSS Signalstruktur öffentlich (zivile Signale)
- Signale für beliebige Nutzerposition können einfach generiert werden
- Signale werden mit hoher Leistung gesendet
- Authentische Signale werden dadurch unterdrückt



- Electronische Kriegsführung
- Drohnenabwehr



GEO Zone Map



Report Incorrect Data

* In compliance with the relevant laws, policies, and regulations, some Restricted Zones will not appear on this web map. Please refer to the DJI app for more GEO Zones in effect. Be noted that as it consumes too much time for mass data loading, all GEO Zones will be hidden when zoomed out to a certain extent.

DJI GEO Zones

[Learn More](#)

Restricted Zones

Restricted Zones: In these Zones, which appear in red on the map, users will be prompted with a warning **and flight is prevented**. If you believe you have the authorization to operate in a Restricted Zone, please contact flysafedji.com or request for Online Unlocking.

DJI Flysafe Website

- Mögliche Probleme Navigation
- GPS speist viele Systeme im Flugzeug
 - Uhr/Datum
 - Terrain Warnung
 - ADS-B
- Größerer Einfluss auf Sicherheit als Jamming

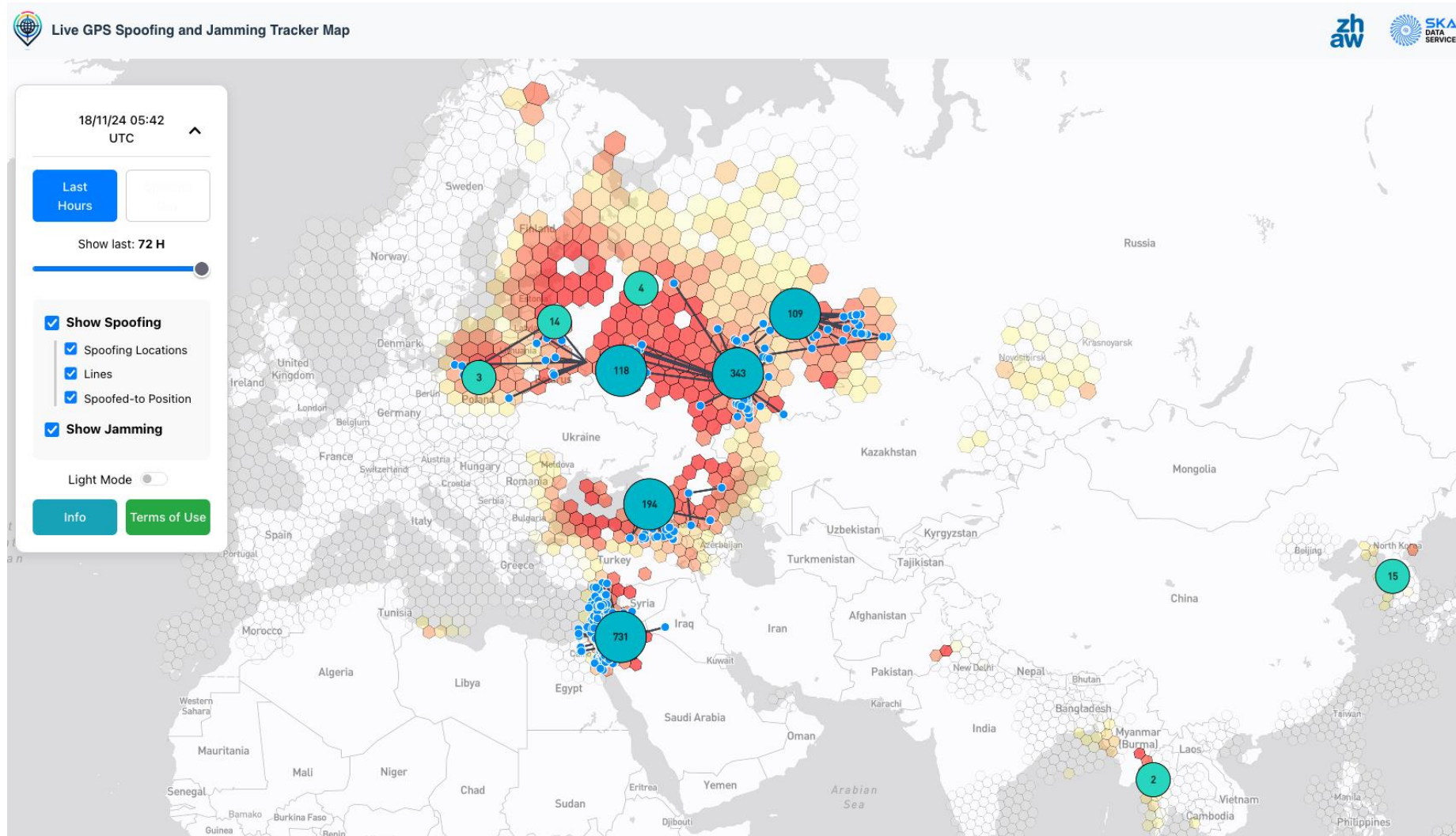


Quelle:

OpsGroup Report on GPS Spoofing

<https://ops.group/blog/gps-spoofing-final-report/>

Überblick Jamming/Spoofing aktuell

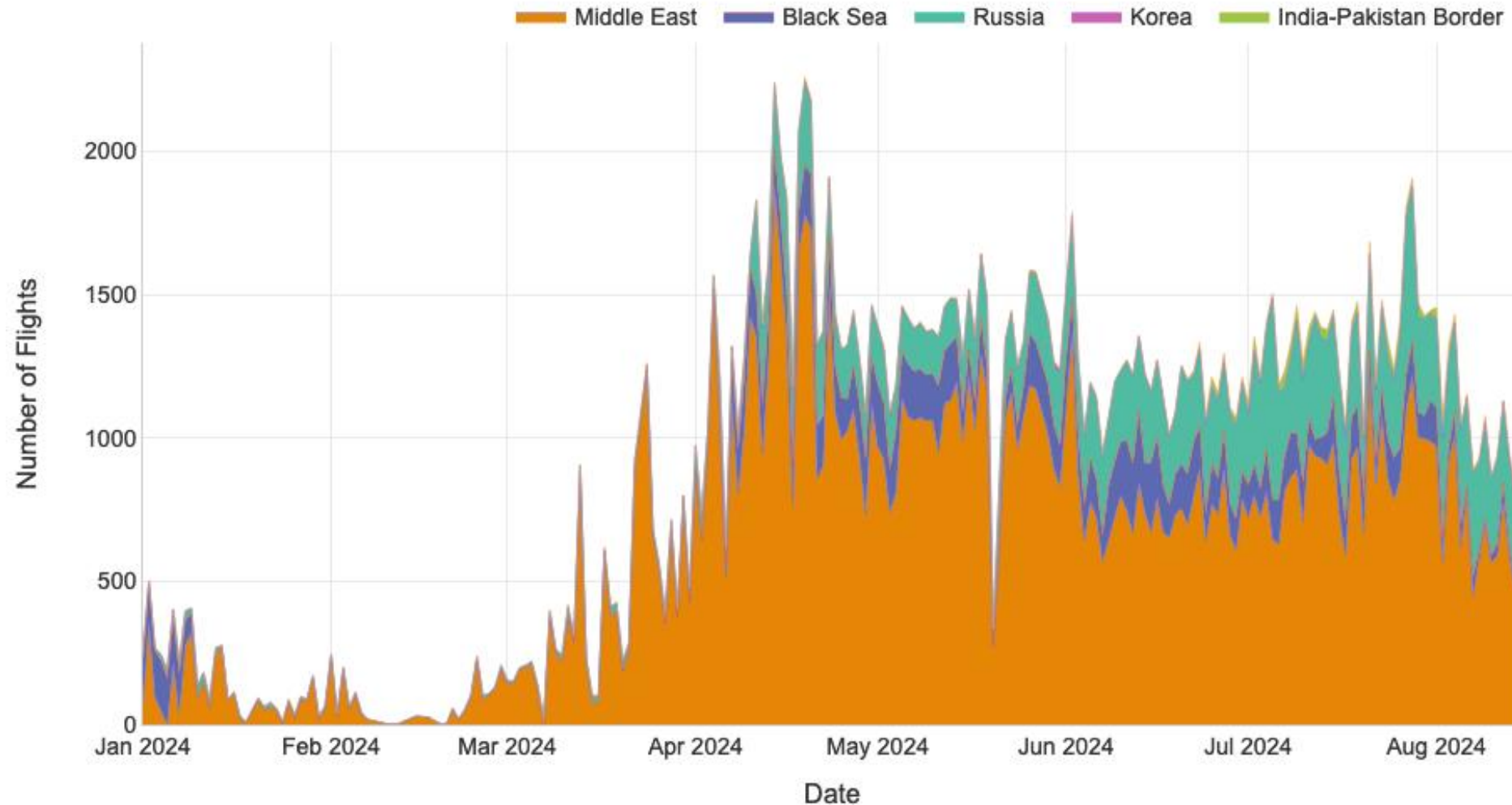


<https://spoofing.skai-data-services.com/>

Überblick Jamming/Spoofing aktuell

ca. 1000 Flüge täglich betroffen

Daily Estimated Number of Flights Affected by GPS Spoofing by Spoofed-to Region



Wie findet man Interferenz?

- ADS-B Daten als Indikator
- AIS Daten von Schiffen
- Direkte Messungen aus Referenzempfängern
- GNSS Empfänger im All
- ..

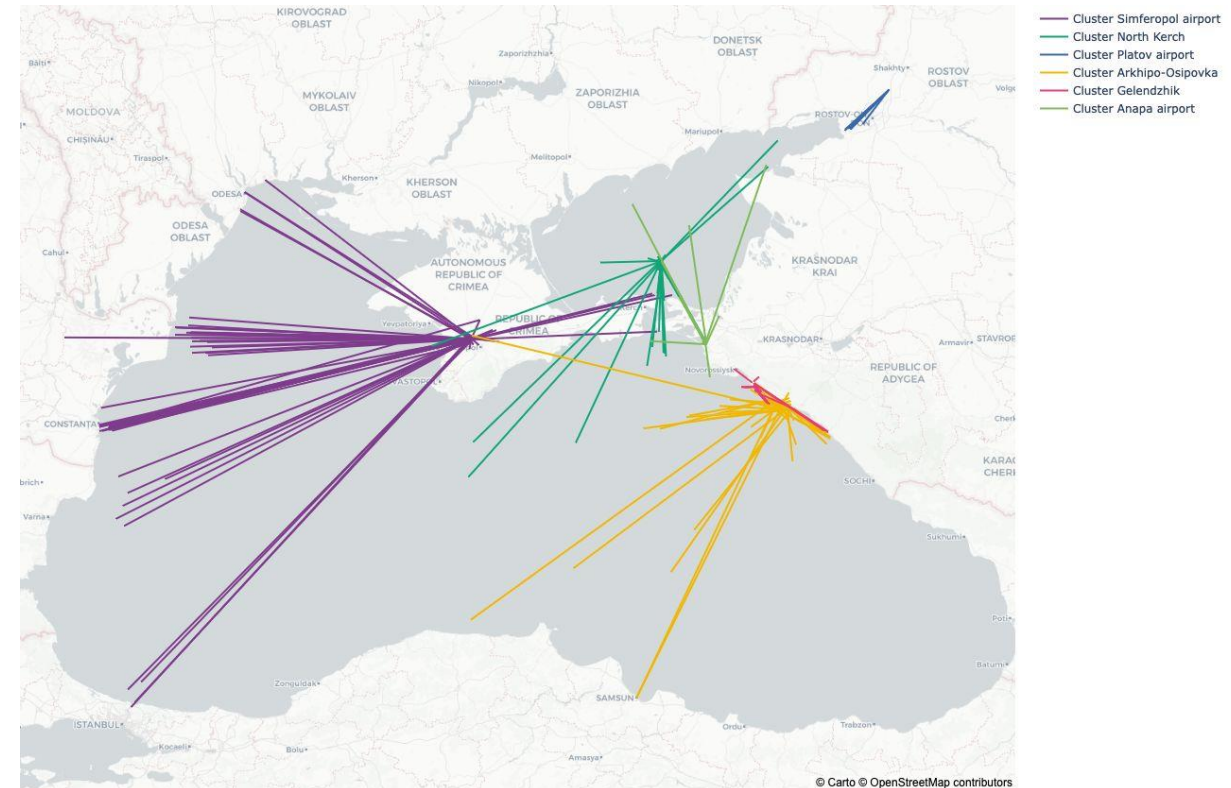


Quelle: Screenshot <https://www.marinetraffic.com/>
vom 24.08.2024

- Jamming: NAC_p
 - Navigation Accuracy Category for position (NAC_p)
 - NAC_p = 0 cumulatively for more than one minute
 - NAC_p > 7 cumulatively for more than one minute
- Spoofing:
 - Vergleich baro/GPS Höhe
 - Mehrere Flugzeuge an gleicher Position
 - Sprünge von Flugzeugen

NAC _p	EPU
11	< 0.00162 NM
10	< 0.0054 NM
9	< 0.0162 NM
8	< 0.05 NM
7	< 0.1 NM
6	< 0.3 NM
5	< 0.5 NM
4	< 1 NM
3	< 2 NM
2	< 4 NM
1	< 10 NM
0	> 10 NM or unknown

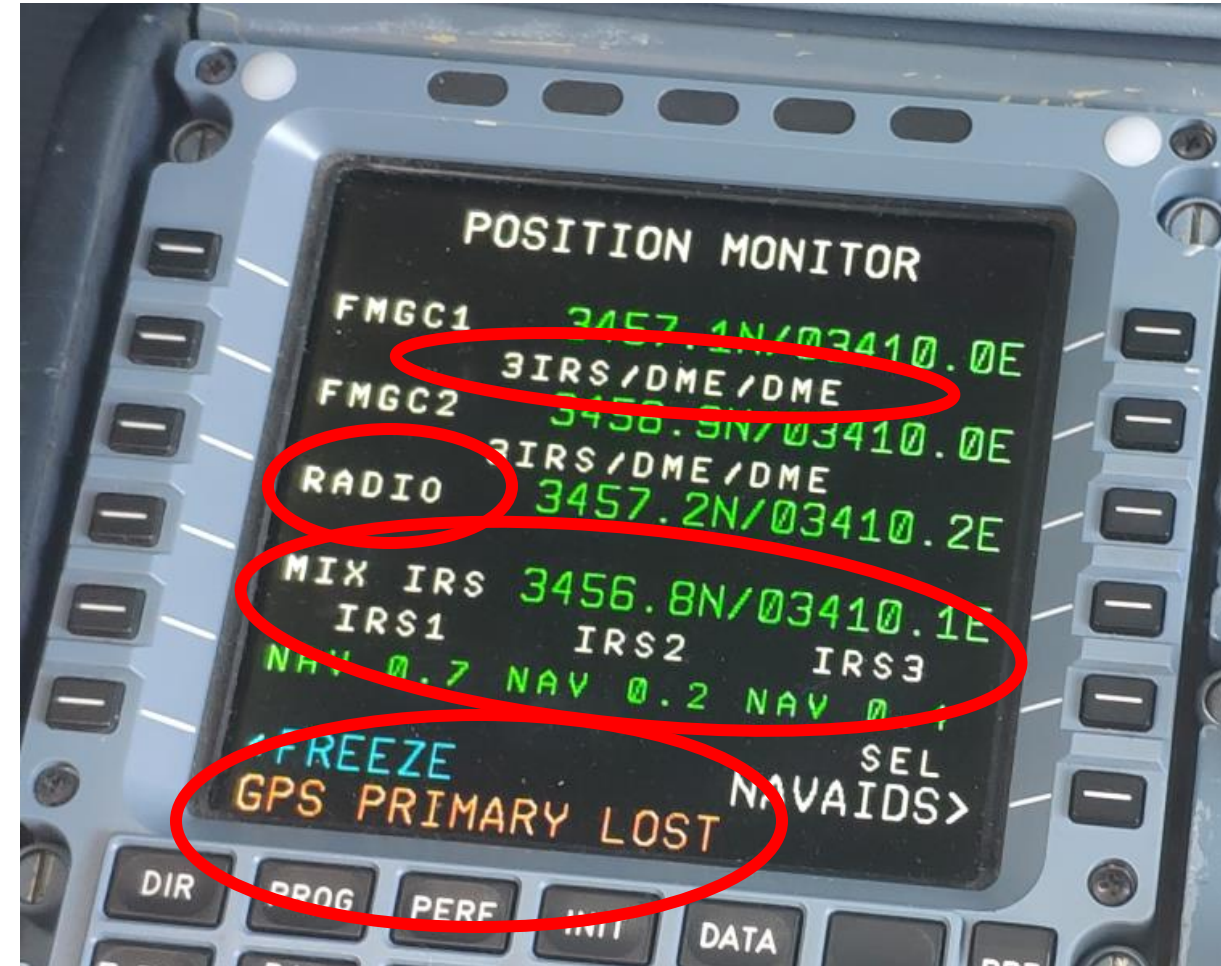
- Analyse AIS Daten Mai / Juni 2024 aus dem Schwarzen Meer
- Ca. 5000 Fälle von Spoofing in 2 Monaten
- 1534 der 7912 Schiffe im Datensatz betroffen von Spoofing
- Im Juni bis zu 250 Schiffe pro Tag betroffen



[Link zum Post](#)

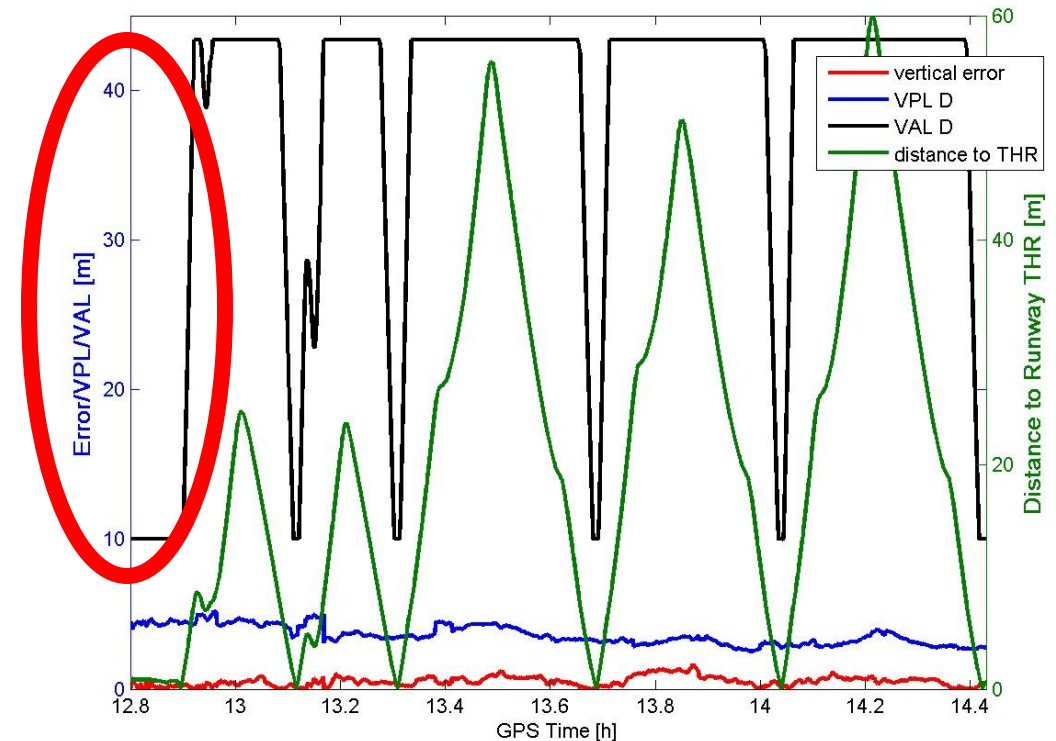
Warum kaum Probleme trotz Jamming und Spoofing?

- Redundante Navigationssysteme
- 3-fach redundante Trägheitssensoren
- Konventionelle Funknavigation
 - DME
 - VOR
 - NDB
- Aufwendige Fusionierung
- Radar als weitere unabhängige Technologie
- Generell: Viel Redundanz im System



- Standardisierte hohe Sicherheitsanforderungen (TLS 10^{-5} bis 10^{-9})
- Anforderungen richten sich nach konkretem Anwendungsfall
- Spezifikationen sind technologie-unabhängig

Spacing between tracks	A/C performance requirements
93km (50NM)	RNAV10, RNP4, RNP2
42.6km (23NM)	RNP4, RNP2, RCP240, RSP180



- GNSS Jamming und Spoofing an der Tagesordnung
- Sehr große Anzahl von Nutzern betroffen
- Notwendigkeit komplementärer Systeme
- Notwendigkeit für neue Technologien zum besseren Schutz der Verkehrsinfrastruktur

