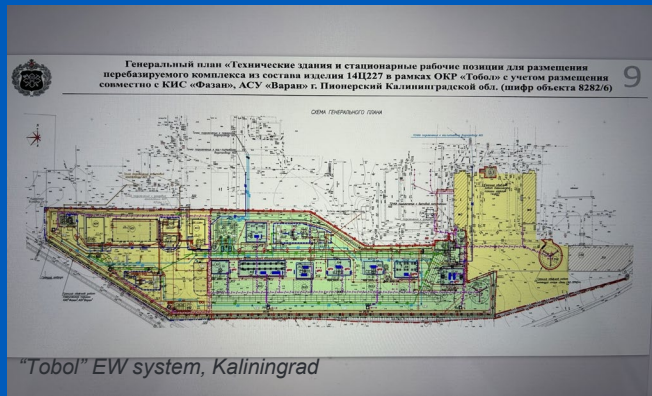


# GNSS störningar – Nya normala

Jamming - ökning 500% från 2022

Spoofing - ökning 400% från Q1 2024

Johan Westin, Sektionen för flygbolag

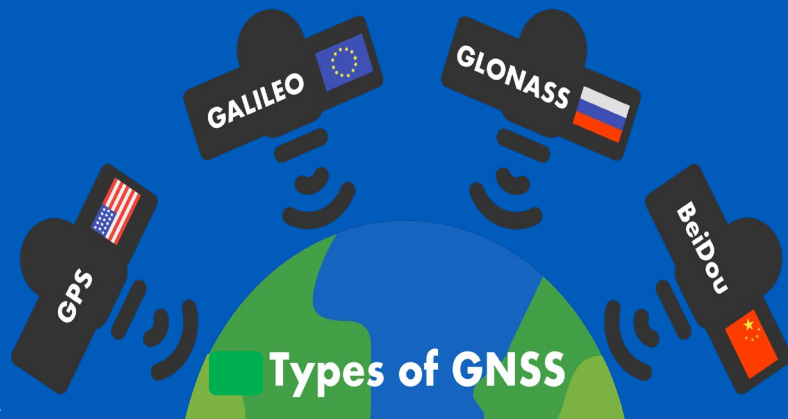




# Sårbarhet med GNSS

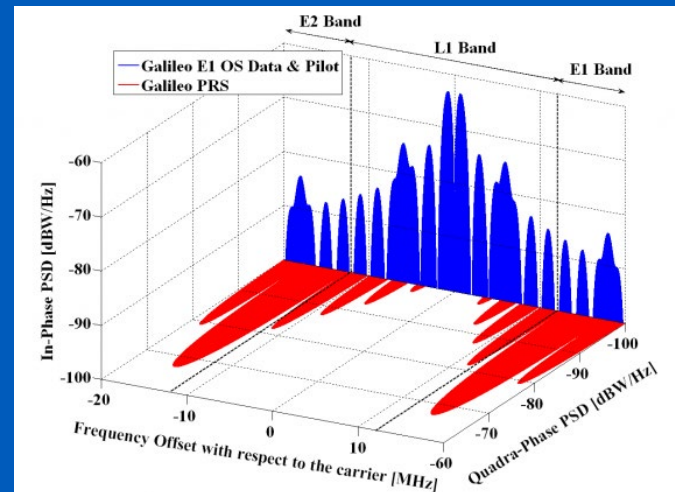
Problemet

- 80 tals teknik – inte byggt för dags cyberhotbild
- Civilt luftfart – icke krypterad svag signal L1



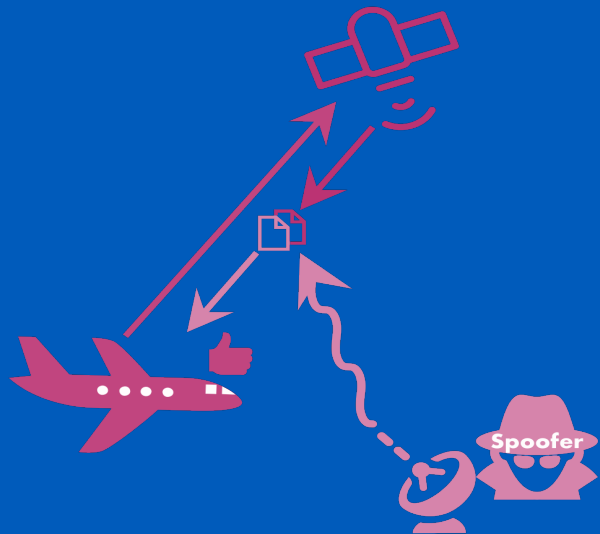
## Störkällor

- Fysiska hinder
- Atmosfäriska Störningar (Störningar - Jonosfären / Troposfären)
- Militära - säkerhetspolitiska störningar ( avsiktig – reglerad )
- Tekniska begränsningar ( svag, icke krypterad, flervägseffekt)



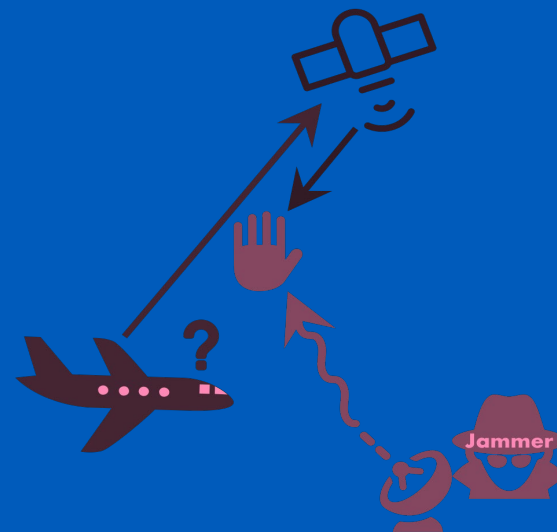
# GNSS Interference

Problemset



## Spoofing

- Function:** Spoofing involves broadcasting fake signals that mimic legitimate GPS or communication signals. These false signals can trick the receiver into thinking it is receiving correct data, when in fact it is using incorrect information.
- Purpose:** The goal is to manipulate the receiver into believing it is in a different location or receiving false instructions. Spoofing is more sophisticated than jamming because it tries to imitate and replace the legitimate signal.
- Example:** A GPS spoofer can send fake GPS data that makes an aircraft think it is in a different location than it actually is.



## Jamming

- Function:** Jamming involves sending a strong signal on the same frequency as the GPS or other wireless signals, which overwhelms the receiver. This makes it impossible for the receiver to read or interpret the legitimate signal.
- Purpose:** The goal is to completely block or interfere with the reception of signals, causing the system to lose its ability to navigate or communicate.
- Example:** A GPS jammer emits signals that prevent GPS receivers from capturing real satellite signals, causing location determination to fail.

# Lösningar GNSS mottagning



- Multipla frekvenser (L1,L2,L5)
- Multipla konstellationer (GPS, Galileo, GLONASS, BDS)
- Integration med tröghetsensor
- Bättre Oscillation
- Ökad förmåga hos mottagare (Detektion. Filter, via spektrum)
- Bättre antenn/antennerna (elevation < 15 grader) (CPRA - Grupp antenner, dvs flera 2-7st)

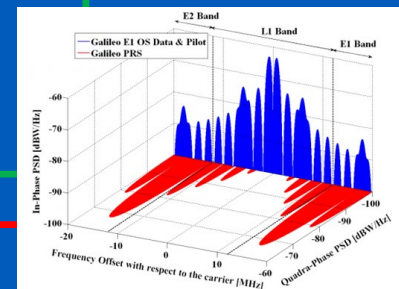


# Lösningar GNSS Galileo Satellit signal

Nya signaler ny möjligheter

OSNMA (Open Source Navigation Message Protokoll)

- Säkerställer att signalen kommer från rätt satelliter



PRS (Public Regulated Service) PRS Decision 1104/2011

- Krypterad tjänst för myndighetsbruk

- Militärt

EU/EC/EUSPA/ESA → PRSCA(SE MSB) → Civil användare



# Framtida navigations lösningar

ny möjligheter

eLoran,

Mobil 5G,6G - WIFI

**INS teknik**

Stjärn navigering

**Optiska system – Laser (Lidar)**

**Kvant teknik (dator)**

Jordens magnet fält

# Vårt problem

Flygplan - lång  
tid för  
uppgradering av  
system



GNSS - svag  
icke krypterad  
signal





# Info ang Eurocontrol B2B – tillgång till GNSS karta

## **If you are not familiar with NM B2B services:**

NM27.0 introduces a new NM B2B service *GNSSInterferenceMapListRequest*, which provides geographical areas affected by GNSS degradation.

You may consult [Network Manager business-to-business web services \(NM B2B\) | EUROCONTROL](#) for the general introduction to the NM B2B services. To join the B2B, the first step is filling out the [Access request form | EUROCONTROL](#) for obtaining the B2B PREOPS certificate. Once your PREOPS certificate is properly set you may start with the internal testing and enter the validation process at your convenience. In order to use *GNSSInterferenceMapListRequest* via B2B in OPS, you must pass the NM B2B validation.

## **If you are aware of other services proposed by NM B2B:**

NM27.0 introduces a new B2B READ service *GNSSInterferenceMapListRequest* which provides geographical areas affected by GNSS degradation.

Details about the introduction of this new service can be found in the NM Release Notes: [eurocontrol-nm-maint-2-release-notes-ed-1.pdf](#)

Please contact NM B2B Office for properly adjust the access rights for your PREOPS certificate. Once your PREOPS certificate is properly set you may start with internal testing and enter the validation process per your convenience.

Please be aware that in order to use *GNSSInterferenceMapListRequest* in OPS, you must successfully complete the B2B validation.

All documentation, announcements, contact details, requests for support and validation are available at our page [NM B2B Services - Home \(sharepoint.com\)](#) and for more details please do not hesitate to contact NM B2B Office ([NM\\_B2B\\_Office@eurocontrol.int](mailto:NM_B2B_Office@eurocontrol.int)).

# Best Practices

EASA - Global Navigation Satellite System (GNSS) Outages and Alterations



Global Navigation Satellite System  
GNSS Radio Frequency Interference  
Safety Risk Assessment

Version 4 September 2024



Safety Information Bulletin  
Operations – ATM/ANS – Airworthiness

SIB No.: 2022-02R3

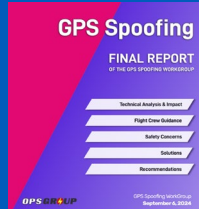
Issued: 05 July 2024

**Subject:** Global Navigation Satellite System Outage and Alterations  
Leading to Communication / Navigation / Surveillance  
Degradation



24002

**SAFO**  
Safety Alert for Operators  
SAFO 24002  
DATE: 01/25/24  
Flight Standards Service  
Washington, DC



## GNSS jamming specific recommendations for Air operators:

- o Ensure that flight crews and relevant flight operations personnel:
  - are aware of possible GNSS jamming;
  - verify the aircraft position by non-GNSS means, when flights are operated in proximity to the affected areas;
  - check that the navigation aids essential to the operation for the intended route and approach are available;
  - remain prepared to revert to a non-GNSS procedure where appropriate; and
  - report (AIREP) any observed irregularities to air traffic services.

## GNSS spoofing specific recommendations for Air operators:

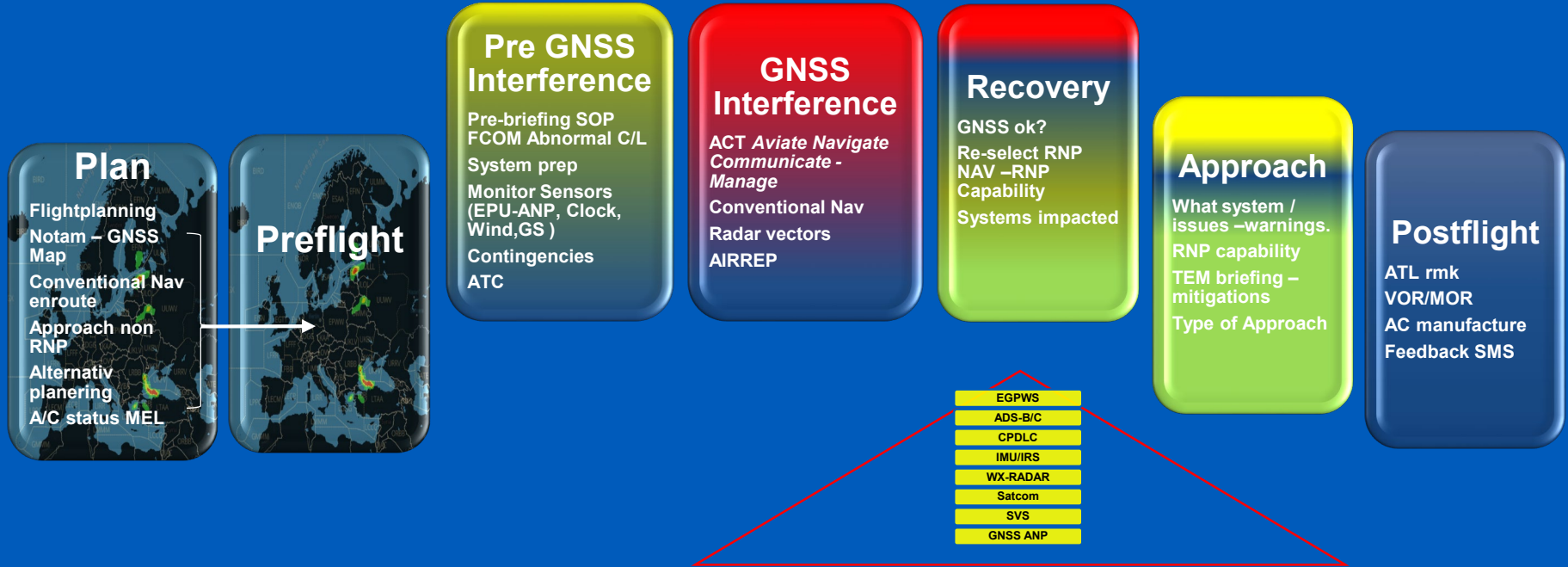
- o Ensure that flight crews and relevant flight operations personnel:
  - are aware of possible GNSS spoofing;
  - when possible monitor aircraft position using non-GNSS nav aids and all available automatic navigation accuracy calculations, including the Estimated Position Uncertainty (EPU) figure;
  - monitor the GNSS time versus non-GNSS time sources;
  - closely monitor the ATC frequencies in the vicinity of spoofing area;
  - apply the manufacturer's instructions and guidance for the aircraft type on detecting and dealing with suspected spoofing;

Prepare  
Initiate  
Act

Finns en etablerad process - SOP för att proaktivt planera, genomföra och avsluta en flygning där GNSS störningar kan förekomma

# SRA – GNSS Interference

## GNSS Process - SOP





## Technological disruptions *external factors*



Möjlig "high level" grundorsak

- Systemfel EBF
- Solstorm
- Mobil 5G störning på avionik
- RTC/RAATS avbrott i funktion
- **Brist kontinuitet satellitnavigering**



### • **Förväntas i tillsyn:**

- Dokumenterade åtgärder enligt EASA SIB 2022-02R3
- Kontroll på MEL Training Programme AMC1 ORO.GEN.110(e)
- MEL visar tydligt hur "inoperative item" på verkar NAV/COM/Surv.
- **Piloter/OP/OCC personal uppföljning och utbildning**
- **Finns en etablerad process - SOP för att proaktivt planera, genomföra och avsluta en flygning där GNSS störningar kan förekomma.**

### • **Information:**

- **EASA SIB No: 2011-24R1**
- **EASA SIB 2022-02R3**
- **[AOC infobrev](#): 2021-06-21, 2023-03-22, 2023-10-11**
- Eurocontrol **[European GNSS Contingency/Reversion Handbook for PBN Operations Rev 6](#)**
- **[Spoofing Report - Ops-Group](#)**
- **[IATA - GNSS Safety Risk Assessment](#)**

### • **TS (CAA)**

- Vidareutveckla nationellt RCZ-system
- Vidareutbilda inspektörer (GNSS, MEL)





# SLUT?