Christina Clausnitzer  
Management and Program Analyst  
Office of Safety Standards  
and  
Ken Alexander  
Chief Scientist and Technical Advisor for  
Satellite Navigation Systems  
Office of Senior Technical Experts
Goals

- Assess safety threats
- Develop mitigation strategies
- Unified European Aviation PNT strategy

Discussion

- Risk identification
- Collaborative Assessment
- Short-Term Solutions
- Long-Term Solutions
EASA/IATA PNT Resiliency Workshop
Jan 25, 2024

Participants
- Airlines
- Manufacturers
- System Suppliers
- Air Navigation Service Providers
- Institutions
Why is civil GNSS vulnerable?

- Signals are extremely weak and easily overpowered
- Public GNSS signals have no security protocols
  - Unencrypted and unauthenticated digital data messages
- Easily imitated (open public standards)
- Most devices “blindly” trust signals they receive
- Unlike computers/routers, GNSS has no firewall or virus protection
- Spoofing, tactics & techniques-widely available on the internet
- Low-cost devices have large area effect

**GNSS can be trusted, but how do you know what you’re using is from GNSS?**
Aircraft and ATC GNSS Dependencies

- **Comm**: Datacom, SATCOM, Networks
- **Nav**: RNAV, RNP & LPV
- **Surveillance**: ADS–B and ADS–C
- **Safety**: GNSS enables Terrain Awareness and Warning System (TAWS) forward-looking function
- **Automation & Aircraft Specific Functions**
- **Support Equipment**: Elec Flt Bag, Survey, etc.
- **FAA ATC & Industry Infrastructure**

*May not be able to identify or “deselect” erroneous GNSS signal inputs*
False Alerts & Warnings

Two fundamental principles:

1. Trust Your Instruments
2. Follow Standard Operating Procedures

Pilot must either:

1. Ignore alerts/warnings; or
2. Follow required checklists & execute mandatory evasive maneuvers

Spoofing can result in repeating TAWS alerts and other alerts
- Aural Warnings cannot be muted or turned down

Representative Audio:

Increased pilot workload and desensitization can contribute to, or directly result in an accident
FAA Jamming / Spoofing Activities

- SAFO (25 Jan 24) provides information and guidance to operators and manufacturers for operations in a disrupted environment
- Performance Based Navigation (PBN) Aviation Rulemaking Committee (PARC) GPS/GNSS Disruption Action Team coordinating with stakeholders to ensure safe and efficient continuity and recovery of aircraft
- Leveraging industry and international partners and RTCA to identify and implement both operational & technical mitigations
- Developing integrated FAA/Industry “Playbooks” for future events
- FAA working with RTCA to improve DME PBN Navigation capability
- Evaluating situational awareness tools for display and decision making
- FAA researching jam and spoof resistant antennas for civil aircraft
Federal Aviation Administration

ICAO Europe/North Atlantic/Middle East Radio Navigation Symposium (February 6-8, 2024)

• Theme “Towards Safe, Reliable and Resilient Air Navigation”
  – Included experts from States, Organizations & Aviation industry

Symposium Objectives Included:

• Provide updates on ICAO activities and plans at Regional and Global levels as well as guidance on rationalization of conventional Navigation aids and their evolving solutions

• Provide updates on GNSS and augmentations, identify & address emerging challenges including GNSS vulnerabilities a

• Discuss GNSS vulnerabilities management plan & possible GNSS jamming/spoofing monitoring solutions
Complementary Positioning: Architecture Change?

• Many of TODAY’s Aircraft, FMS NAV Integration is an “availability switch”
  
  • IF GPS/GNSS is available, THEN use GPS
  
  • IF GPS/GNSS is not available, THEN use INS or RADIONAV
    
    – Unless forced through an outage, RADIONAV position gets ignored
    
    – Systems today are trimmed to deliver high availability / continuity
  
• TOMORROW’s Aircraft Flight Management System NAV Integration: “improved consideration of all sources”

  • (Operators are) Not interested in carrying another aircraft system just in case the other one does not work

  • Service provision: Need to push for DME network to provide GNSS-like navigation service
EUROCONTROL Voluntary Pilot/ATC Incident Reporting (EVAIR)
(Events per 10,000 flights - 2016 to 2020)

2018 GPS Jamming & Spoofing Safety Reports (Green)
~ Three times all other categories combined

1st two months of 2024 are 3 times 2023
From June 2022-June 2023: 209 Airlines recorded ~150,000 Loss of GPS Events n ~5 million flight operations
GNSS outage (ECR data), mitigations

The annual rate for GNSS outages/alterations has a steep, increasing trend!

Continued increase in GNSS jamming and cases of spoofing resulted in EASA SIB 2022-02R2 being issued in November 2023

Rates are per 1,000,000 flights
Spoofing Reports in ECR

- Turkey, Black Sea, Romania
- Iraq, Egypt, Bulgaria, Cyprus
- Iran, Georgia, Israel

Rates are per 1,000,000 flights

1-4th Qtr 2023
Spoofing and jamming
1st public tool to monitor aircraft false GNSS (spoofing) position “jumps”

Number indicates count of “Improbable” aircraft position changes detected in public ASD-B data

Live GPS Spoofing Tracker (skai-data-services.com) developed by SkAI Data Services and Zurich University of Applied Sciences – Centre for Aviation
Eurocontrol Summary to ICAO Forum

- Multi-DME Navigation can make a significant contribution for resilient navigation—Not same as DME/DME (single pair) broadly known today
  - INS and DME can, and should, support ADS-B
  - DME is not the solution for all environments or all aircraft
  - Needs harmonized “integration upgrades” with FMS, DFMC GNSS and INS
  - “DME Forever” will not work for spectrum reasons, need evolution path

- Avionics integration needs to become more resilient & take better advantage of available complementary sensors to reduce CNS interdependencies
  - Need to overcome “magic is in the box” mentality
  - Similar efforts required at CNS ground system level
  - Need improved cooperation and common performance language

- ANSP need to improve service provision for GNSS contingency
Ensuring resilience of ICAO CNS/ATM systems and services

Resiliency to interference needs to be improved by maximizing integration of all suitable ground infrastructure, space infrastructure and airborne components in a complementary and cooperative manner to be as robust as possible to cases of satellite-based service disruptions or environments where false or deceptive signals are present.

Recognizing both aircraft on-board & ground infrastructure . . . need to be adapted to include . . . interference detection, mitigation and reporting.

Acknowledging loss of crew's situational awareness from malicious origin is classified as a cyber-security threat & cannot be tolerated in civil aviation.

. . . and that intentionally sending misleading signals to replace the accurate signal is a far more serious threat to flight safety than loss of GNSS signal.
**ICAO Headquarters Recommendations (Slide 1 of 5)**

*All Stakeholders* Be aware of potential safety & capacity impacts of GNSS interference, jamming, and spoofing

*Civil Aviation Authorities (CAAs)* Ensure Air Navigation Service Providers (ANSPs) deploy & maintain adequate Distance Measuring Equipment (DME) Infrastructure & DME Performance Based Navigation procedures

**CAAs** Enable aircraft operators use of Multi DME & Multi-DME/Inertial Reference System (IRS) complementary solutions

- To maintain PBN operations during GNSS local or regional events

**CAAs** Ensure ANSPs implement & maintain Minimum Operational Networks (MON), or greater, of Navigation Aids & Radar infrastructures

- Including VHF Omni-directional Range (VOR)
- Instrument Landing System (ILS) Cat I/II/III &
- DME

... to ensure resilience for navigation when core constellations or their augmentations are unusable
ICAO Headquarters Recommendations (Slide 2 of 5)

**ANSPs** Develop GNSS RFI event contingency procedures (Tech & Ops) to minimize any Ops impacts & ensure continuous safe air traffic Operations

– Note: Contingency procedures may require provision of reliable surveillance coverage resilient to GNSS interference

**ANSPs** Implement/maintain GNSS independent time source(s) for CNS/ATM infrastructure

**CAAs/ANSPs** Facilitate or deploy real-time monitoring & detection for GNSS RFI situational awareness -- recognizing aircraft operator responsible to determine ability to navigate

**ANSPs** Issue timely GNSS RFI Notice to Airmen (NOTAMs) in coordination with neighboring regions on sharing Navigation infrastructures when GNSS RFI might result in air traffic diversions
ICA0 Headquarters Recommendations (Slide 3 of 5)

**CAAs/ANSPs** Improve civil-military coordination in GNSS testing & conflict zone risks to ensure uninterrupted & reliable use for diverse applications

**National Military Authorities** Coordinate GNSS RFI with National Spectrum Regulators, CAAs and ANSPs (to extent possible)
• To enable mitigation of any safety impacts to civil aviation

**CAAs** Foster RFI collaboration with National Spectrum Regulators

**National Spectrum Regulators** Locate and determine GNSS RFI source & attempt to resolve (as appropriate)
• May require coordination with authorities at national/regional levels

**National Spectrum Regulators** Report frequent, unresolved GNSS RFI to ITU Radiocommunication Bureau, describing impacts experienced or as reported by registered aircraft
ICAO Headquarters Recommendations (Slide 4 of 5)

**Aircraft Operators** Develop crew GNSS RFI procedures to notify ATC

**Aircraft Operators** Notify aircraft & avionic manufacturers (OEMs) & acft’s State of design CAA by safety channels when encountering safety effects

**Aircraft Operators** Develop procedures & training based upon information from aircraft & avionics OEM and aircraft’s State of design CAA

**Aircraft Operators** Place add’l emphasis on flight crews closely monitoring aircraft equipment performance for any discrepancies/ anomalies
  - Promptly inform ATC of any apparent GNSS degradation and be prepared to operate without GNSS navigation systems

**Original Equipment Manufacturers (OEMs)** Improve equipment (capabilities) & provide add’l aircraft equipment guidance/information on GNSS RFI effects & mitigations (incl. interference, jamming & spoofing)
ICAO Headquarters Recommendations (Slide 5 of 5)

**OEMs** Ensure aircraft equipment quickly recovers and resumes GNSS navigation once no longer impacted by GNSS RFI event(s)

**ICAO Navigation Systems Panel (NSP)** Develop recommendations on sharing information on GNSS RFI (NOTAM or other measures)

**All stakeholders** Collaborate on simple & automated GNSS RFI reporting

**All stakeholders** Continue to evolve solutions and leverage ICAO NSP as common focal point

**ICAO** Continue raising awareness and supporting States, as required
New Threats Dictate new Strategies for Operational and Technical Mitigations

Contact Info:
Christina Clausnitzer
Christina.Clausnitzer@faa.gov
+1.303.342.1965

and
Ken Alexander
Ken.Alexander@faa.gov
+1.202.236.9794

Questions
BACKUPS
2014 FAA Guidance for Industry to address GNSS Misleading Position and Navigation Threats

- May 2014, FAA modified AC 20-138D *Airworthiness Approval of Positioning and Navigation Systems* and avionics standards to enable spoofing mitigations
  - Prescriptive Guidance mitigates spoofing as well as re-radiators

2014 FAA Aviation Circular (AC20-138D) as well as GPS, GBAS, & SBAS FAA Technical Order Standards and RTCA/EUROCAE MOPS state:

- *Improperly used or installed GNSS re-radiators can present misleading information to GNSS equipment*

- *Equipment manufacturers should consider measures to mitigate against use of erroneous data for GNSS position and navigation*

- *Possible measures to consider include implementing or enabling cross-checks of GNSS sensor data against independent position sources and/or use of other detection monitors using GNSS signal metrics or data*
EASA actions in response GNSS RFI


→ ‘Over-reliance on satellite navigation’ is a safety issue (SI-0034) under assessment (CAT CAG) => completion by 2024 with proposed mitigations

→ CARI (CAW) for TCH & OEM to evaluate effects of GNSS jamming or spoofing on CS25/CS29 products at system and aircraft level

→ EASA/IATA Workshop on PNT Resilience hosted at EASA premises on 25 January 2024