

ICAO

Hosted by

IFATSEA
International Federation of Air Traffic Safety Electronics Associations

AIR NAVIGATION WORLD

COMMUNICATIONS, NAVIGATION, SURVEILLANCE, AND SPECTRUM

CNSS 2026

12 - 15 October | Kotor, Montenegro

Session 8 - GNSS RFI Today: From Awareness to ACTION

Bulent Atas

Risk Assessment Pilot, Flight Operation/
Turkish Airlines

Flight Deck is the last barrier. What protects that barrier?

Experience · awareness · mitigation · resilience — what improves for the next crew?

Capt. Bülent Ataş

A330 Captain and Technical Pilot · Flight Operations Risk Assessment · Turkish Airlines

GNSS RFI: From Awareness to Action

EXPERIENCE | AWARENESS | MITIGATION | RESILIENCE

1 · EXPERIENCE

Experience teaches the crew. Who else learns?

Four reports expose where planned protection becomes difficult to use.

01 · DUAL GPS LOSS

Diverted to ILS

Plan recovery around an aerodrome the aircraft can still reach.

02 · SPOOFING SUSPECTED

Vectors unavailable in the next FIR

ATC fallback depends on the service actually available en route.

03 · REPEATED TERRAIN ALERTS

Missed approaches, then diversion at night

Applying the guide did not prevent the next approach from being disrupted.

04 · REPORTING FRICTION

Known outage, uncertain value in reporting

Feedback must be useful—and reporting sustainable.

A safe landing proves crew action—not that the underlying risk has reduced.

2 · AWARENESS

Awareness must change the next decision

The next crew, dispatcher and controller need a better decision basis.

CREW REPORTS
Effects + decisions

OEMS
Validate mechanisms

ANSP
Service + capacity limits

DISPATCH
Route · MEL · fuel · alternate

TRAINING
Recognition + recovery

SAFETY + SPECTRUM
Action + feedback

Existing support: EASA/EUROCONTROL reporting guidance · Joint European Action Plan · ICAO RON work

The test is whether it changes the next flight's plan and available support.

A report becomes shared learning only when it changes a decision, procedure or service.

3 · MITIGATION

Mitigation changes the risk we still have to manage

Each measure has conditions, limitations and a recovery requirement.

Vectors — **Available ATC service**

Surveillance, coverage and controller capacity must support the fallback.

Visual — **Adequate visual reference**

Cloud, visibility and darkness determine whether the procedure remains usable.

Inhibition — **Protection changes**

Follow aircraft-specific guidance; know what remains and when to restore it.

Recovery — **PNT**

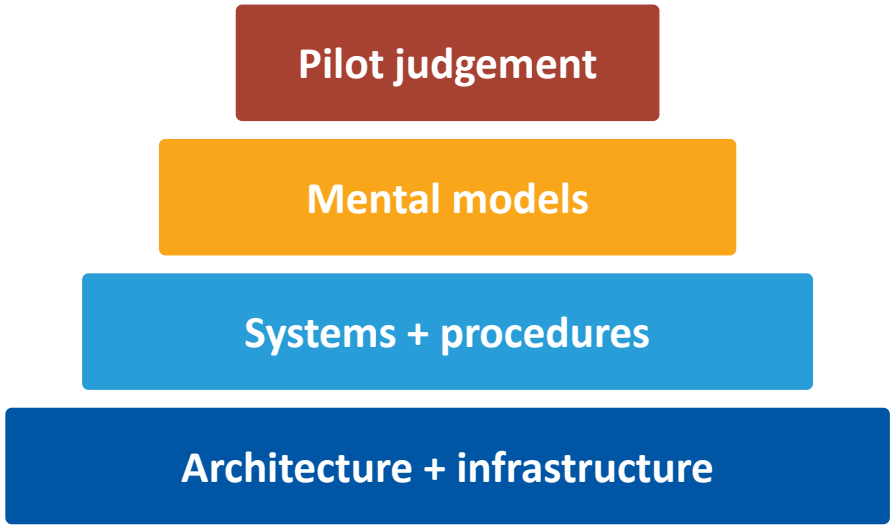
A returned GPS indication alone does not prove every required function is usable.

Repeated alerts erode trust. Familiar workarounds become habit. Training must test when the familiar response is no longer safe.

What capability remains—and what tells the crew to change the plan?

Resilience starts below the flight deck

Every unengineered layer pushes the burden upward—to the crew.



CREW
What remains when nothing below was engineered.

PICTURE
Crew, dispatch and ATC align on what still works.

FALLBACK
Service remains available through a conventional final.

REVERSION
Route · approach · missed approach · alternate.

Mitigation: the crew absorbs the degradation. **Resilience:** the architecture preserves capability.

A safe outcome is not proof of resilient design. What improved for the next crew?

Session 8 - GNSS RFI Today: From Awareness to ACTION

Ken Alexander

Chief Scientist for Satellite Navigation Systems
Federal Aviation Administration

Challenge 1: Pilot Proficiency – Considerations for Spoofing Recognition & Response

- **Training:** Know specific aircraft spoofing effects, mitigation procedures, and limitations
- Maintain (and Practice) PNT situational awareness (SA) as best practical
  - Verify position and position discrepancies relative to independent means (e.g., NAVAIDs, decoupled inertial, terrain features, railroads, roads/highways, power lines, rivers, lakes, other landmarks, etc.)
- Request ATC approval to practice contingency routes/procedures (e.g., RNAV SID/STAR, ILS)
- For training, don't only manually fly the aircraft—manually navigation the aircraft!
- Position & Navigation spoofing: abnormal GNSS Ground Speed (e.g., 30 or Mach 1+)
- EGPWS/TAWS alerts when inappropriate or worse—Missing/No alert of near or actual CFIT
- Degraded Actual Nav Performance (ANP) and be suspicious of "Improved" ANP
- Time Spoofing: be cognizant of abnormal indications or concurrent avionics anomalies CNS, Safety Systems
- Effects can be delayed or last until landing & beyond



Spoofing Training in Simulator

Challenge 2: Evolving Pilot/Controller, Aircraft & Infrastructure “Blind Trust” in the Blue/Magenta GNSS Line to “Trust but Verify” and then “Zero Trust”

FAA AC 20-138D Change 2 Published: 4/7/16 is an Advisory Circular titled "Airworthiness Approval of Positioning and Navigation Systems; Para 5-1.g. *Equipment manufacturers* ***should consider measures to mitigate against the use of erroneous data for GNSS position*** *and navigation solutions.*

Possible measures to consider are: implementing or enabling ***cross-checks of GNSS sensor data against independent position sources*** *and/****or other detection monitors*** *using GNSS signal metrics or data.*

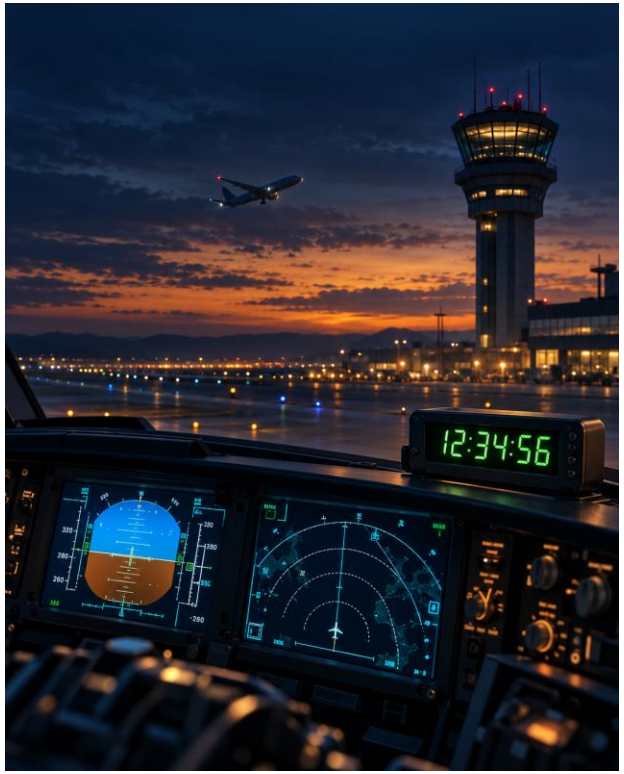
- e.g., Reasonableness checks of GNSS data with source independent of GNSS
- Without independent source, avionics can preform consistency checks of GNSS data
- OEMs should establish Claims Tables for capabilities exceeding minimum specification requirements and maintain as sensitive, proprietary—don’t publish as marketing!
- OEM’s need to work with Standards Bodies to establish and harmonize DME use for both RNAV and RNP initially to RNP-1 , followed by RNP-0.3 where DME & terrain support or DME/Inertial for approach

Challenge 3: It's All about Time—Independent, Resilient Time

- GNSS time spoofing can disrupt both aircraft, ATC, and Operator's systems
- Aircraft, ATC, and Operator Infrastructure systems, applications, and services need:
  - Independent clock (or oscillator) ensembles for installation and use as the primary source of time
  - Checked/synchronized with resilient UTC source
  - Prevent "fake" GNSS time from corrupting aircraft clock

Systems spoofed time can affect include:

- **Communications**: CPDLC and SATCOM
- **Navigation**: position calculations and map displays
- **Surveillance**: aircraft tracking (ADS-B & ADS-C)
- **Safety Systems**: EGPWS/TAWS, weather radar, etc.
- **Avionics**: Internal buses and data exchange
- **ATC**: Automation, Networks, and Safety systems, services & applications



ONE TIME REFERENCE. MANY ATC SERVICES

GNSS Spoofing and ATSEP as a critical technical safety barrier

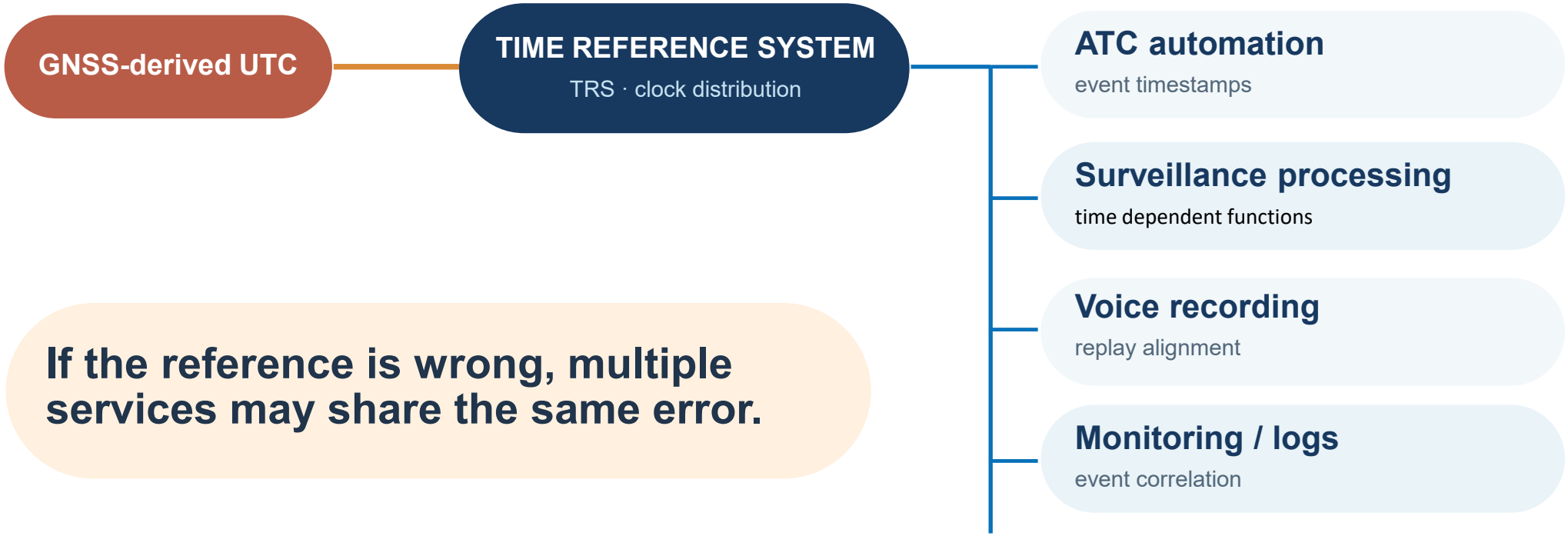
NIKOLA COJIĆ

Aeronautical Systems Specialist Engineer |
Instructor SMATSA
Executive Board Member, IFATSEA

THE HIDDEN DEPENDENCY

One time reference. Many ATC services.

Illustrative CNS/ATM architecture — timing dependencies and integrity requirements vary by implementation



If the reference is wrong, multiple services may share the same error.

A compromised common time reference can affect multiple dependent functions – even when equipment remains operational.

THE DECEPTION

GNSS lost is not GNSS deceived.

A receiver can lose its reference — or continue accepting an incorrect one

JAMMING / REFERENCE LOSS

GNSS becomes unavailable

Loss-of-reference indication

Holdover may be initiated

SPOOFING / FALSE REFERENCE

If spoofing is not detected or rejected

GNSS still appears valid

Receiver may remain LOCKED

Wrong time may propagate

Holdover cannot protect against a false reference that remains accepted.

All green. Is the time trustworthy?

Conceptual monitoring screen — an illustration, not an actual event

TRS / CNS MONITORING

GNSS receiver	LOCKED
Timing distribution	AVAILABLE
Dependent services	ONLINE
Independent integrity evidence	NOT AVAILABLE

ATSEP needs to know:

Is this time reference trustworthy?

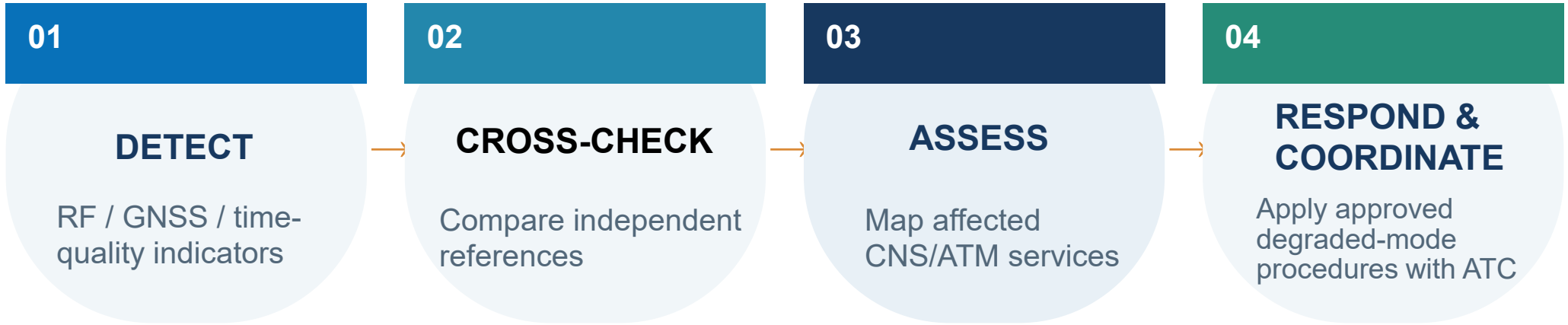
Which CNS/ATM functions depend on it?

What evidence justifies intervention?

LOCKED confirms a synchronisation state – not independently verified UTC accuracy.

ATSEP must turn indications into decisions.

Detection alone does not protect a service



Do not declare the reference trustworthy — or restore normal service — on LOCKED status alone.

Define detection thresholds, time-error limits, escalation and recovery criteria before an event.

Who protects the technical barrier?

ATSEP needs integrity visibility, defined responsibilities and validated response procedures.

Flight crews manage the last operational barrier.

ATSEP safeguards a critical technical barrier.

VISIBILITY

Independent timing-integrity evidence

PREPAREDNESS

ATSEP procedures and exercises

ASSURANCE

Tested detection, holdover and recovery limits

“We cannot expect ATSEP to defend infrastructure against a threat it cannot reliably see.”

Session 8 - GNSS RFI Today: From Awareness to ACTION

Eman Al-marashdah

Senior specialist - ANS Engineering
UAE

The UAE GNSS RFI Experience



From Interference to Resilience: The UAE Response



Operational Impact: When Timing goes wrong

FDPS
LOSS OF CORRELATION

FDPS lost the correlation

Correlation issue was observed.

Investigation results

FDPS time was incorrect and not synchronized to the NTP receivers.

Corrective action

Configured FDPS to synchronize with the NTP receivers.

Result

FDPS time showed correctly.
Observed for a few hours and no further correlation issue reported.

TRACKER
BOTH CHAINS UNAVAILABLE

Both TRACKER chains u/s on MMS

MMS displayed both Tracker chains failed.
Chain A in ready state (orange), Chain B down.

Investigation results

NTP servers showed a significant time offset (≈ 2 minutes ahead).
Due to the time difference, the Tracker rejected the sensors.

Corrective action

Performed chain swapping and restarted the application.
Isolated the timing path and connected NTP1 directly to the anti-jamming unit (bypassing the splitter).
Forced the tracker to take time from NTP1.

Result

Service returned to normal. Radars reconnected and data available to Operations.

Engineering Response: Exploration and Options Assessment

Explore Options → Assess Risks & Feasibility → Define Implementation

Options Explored

We explored several options to enhance the resilience of our timing architecture, with a focus on rapid implementation and long-term sustainability.



National telecommunication service provider clocks



GNSS anti-jamming solutions



Other national clock references (airports / ANSPs)

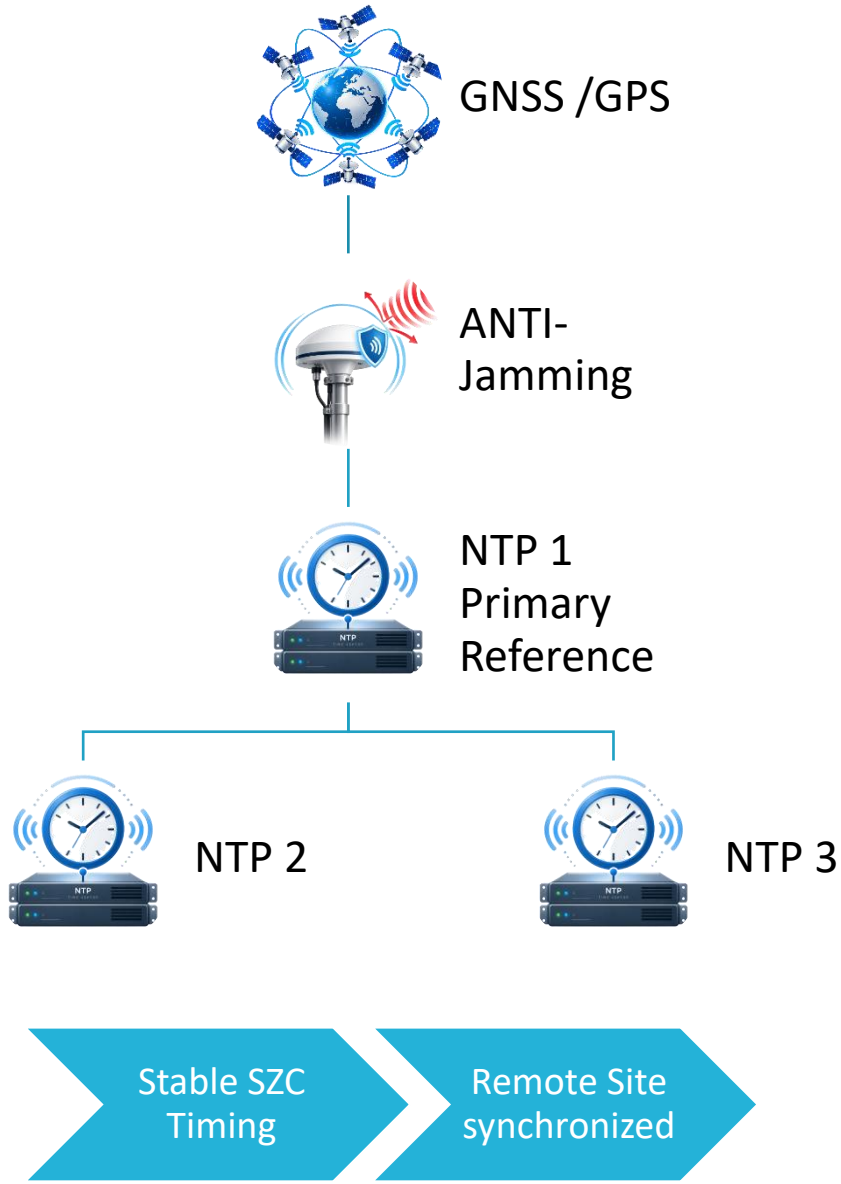


Enhanced internal NTP architecture

Assessment Criteria

- **Risks**
- **Available mitigations**
- **Time constraints**
- **Cost**
- **Supply chain availability**
- **Operational sustainability**
- **Integration / implementation complexity**
- **Resilience and long-term viability**

Engineering Response: Building A Resilient Timing Architecture



Key Takeaways

LESSONS FROM THE UAE EXPERIENCE

SAFE SKIES
THROUGH
RESILIENT
TIMING



01

PROTECT

CRITICAL TIMING SOURCES

Treat timing as critical infrastructure and protect it from interference.

MORE PROTECTION
MORE RELIABLE
OPERATIONS

02

UNDERSTAND

SYSTEM DEPENDENCIES

Know which systems rely on timing and understand the operational impact, constraints and risks.

GREATER AWARENESS
BETTER DECISIONS

03

BUILD IN LAYERS

RESILIENCE, NOT A SINGLE FIX

Combine technical solutions, alternative timing sources and contingency arrangements to enhance resilience.

STRONGER RESILIENCE
FOR THE FUTURE

RESILIENCE IS NOT A SINGLE SOLUTION.

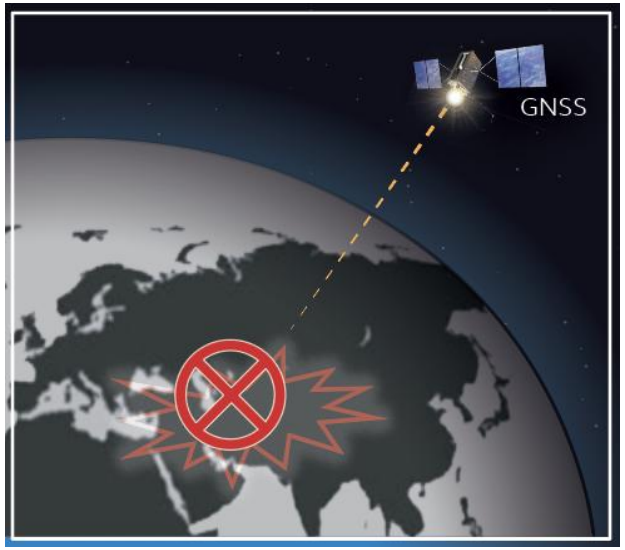
It is built through collaboration, information sharing, and multiple layers of technical solutions working together.

Sai K. Kalyanaraman, Ph.D.

Collins Aerospace

GNSS threats – Reported over last 2+ years

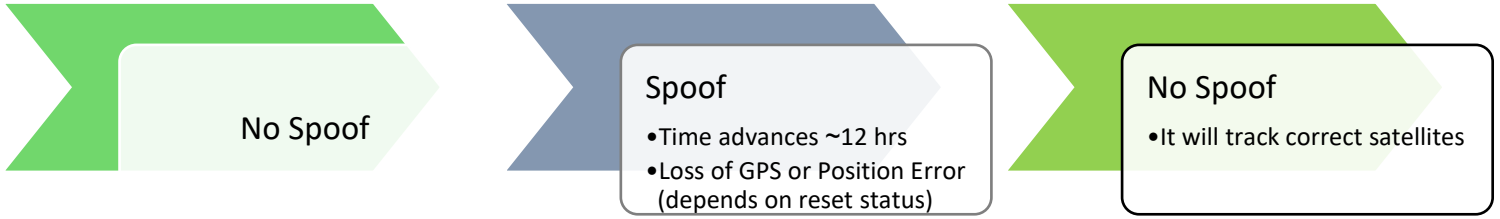
- Multiple Incident reports received from the Field
  - Loss of GNSS for over 2 hours on some flights over the Middle East
  - Time Jumps noticed on Flights over the Syria/Iraqi Airspace
  - Corruption of GPS almanac observed on some flights near the Baghdad airport
  - Repeater based attacks observed on some flights in the Chinese Airspace
  - GPS interference observed in the Dallas Area
  - Spoofer attacks observed in the Baltic Region
- Incidents could result in:
  - No impact
  - Spoofing attacks that result in Time and/or Position Corruption
  - Loss of GPS that recovers autonomously after flying out of RFI region
  - Loss of GPS that recovers after power cycle
  - Loss of GPS that recovers after a factory reset
  - Loss of a variety of functions (timing, comm, surveillance, platform nav) at the aircraft level



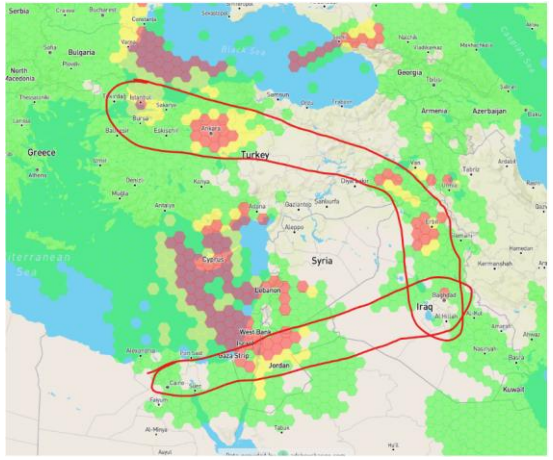
© 2026 Collins Aerospace. | Collins Aerospace Proprietary. | This document does not include any export controlled technical data. U.S. ECCN 7E994

SPOOFING ISSUES REPORTED TO COLLINS

- Events observed on a periodic basis since December 2020
  - GPS time jumps forwards as A/C flies in and out of the spoofer region
  - Loss of GPS occurs for many hours



- Following events observed on GPS radios on XYZ Airways
  - Loss of GPS due to Jamming
  - Position Errors of up to 10 NM
  - Permanent loss of GNSS due to Spoofing
    - Corruption of almanac causes consistency checks to fail within the receiver



© 2026 Collins Aerospace. | Collins Aerospace Proprietary. | This document does not include any export controlled technical data. U.S. ECCN 7E994

Building resiliency in the GNSS receive system

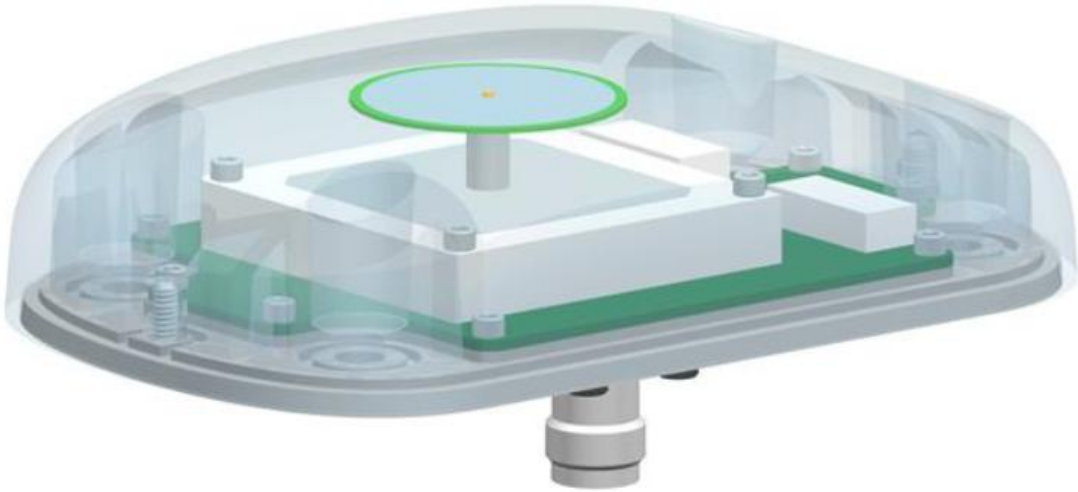
– Anti-Jam and Anti-Spoof

- **Antenna level**
  - CRPA (Controlled Reception Pattern Antenna)
    - Nulling / beamforming
- **GNSS Radio level**
  - RF/IF level
    - AGC detectors /RFI Excision etc.
  - In the baseband signal processing
    - Correlation function based
    - Acquisition phase/tracking phase
    - Carrier to Noise Ratio based detection
- **Platform Aiding mechanisms**
  - Inertial coupling
    - Loose coupling
    - Tight coupling
    - Deep integration

© 2026 Collins Aerospace. | Collins Aerospace Proprietary. | This document does not include any export controlled technical data. U.S. ECCN 7E994

Concentric CRPA

- Combination of a monopole and a patch antenna
- Steers a low elevation null in any azimuthal direction
- Footprint and power compatible with current TSO c190 GNSS aviation antennas providing ***ease of retrofit***
- RTCA DO-301 compliant in non Anti-Jam mode



© 2026 Collins Aerospace. | Collins Aerospace Proprietary. | This document does not include any export controlled technical data. U.S. ECCN 7E994

COLLINS GLU-2100 MULTI-mode receiver

- Collins GLU-2100 Multi-Mode Receiver
  - Level A certified to support SBAS, LPV, GLS CAT 1-2, ILS CAT 1-3, VOR and MB
  - Software defined GNSS Engine that uses Collins patented Universal Channel Technology to support all civil GNSS signals
  - Field Loadable to support DFMC SBAS and ARAIM
  - Field Loadable to support RFI Mitigation techniques to perform jammer detection, spoofer detection and integrity coasting using NAV grade inertial data
    - RASA (Receiver Autonomous Signal Authentication) and,
    - SENTRI (Staggered Examination Of Non-trusted Receiver Information)



© 2026 Collins Aerospace. | Collins Aerospace Proprietary. | This document does not include any export controlled technical data. U.S. ECCN 7E994

RASA / SENTRI

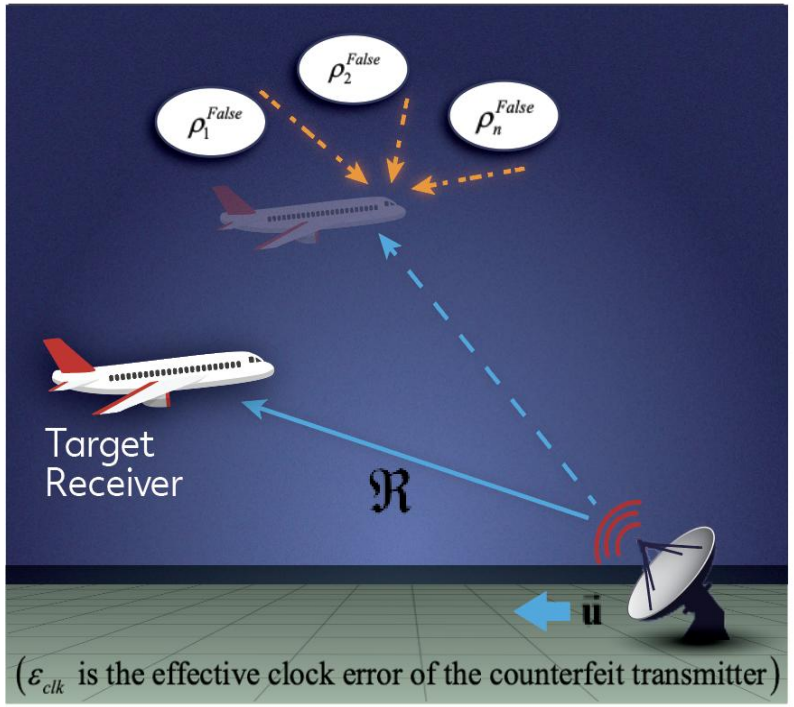
Receiver Autonomous Signal Authentication

Counterfeit Transmissions

$$\begin{bmatrix} \rho_1^{False} \\ \rho_2^{False} \\ \vdots \\ \rho_n^{False} \end{bmatrix} + \begin{bmatrix} \varepsilon_{clk} \\ \varepsilon_{clk} \\ \vdots \\ \varepsilon_{clk} \end{bmatrix}$$

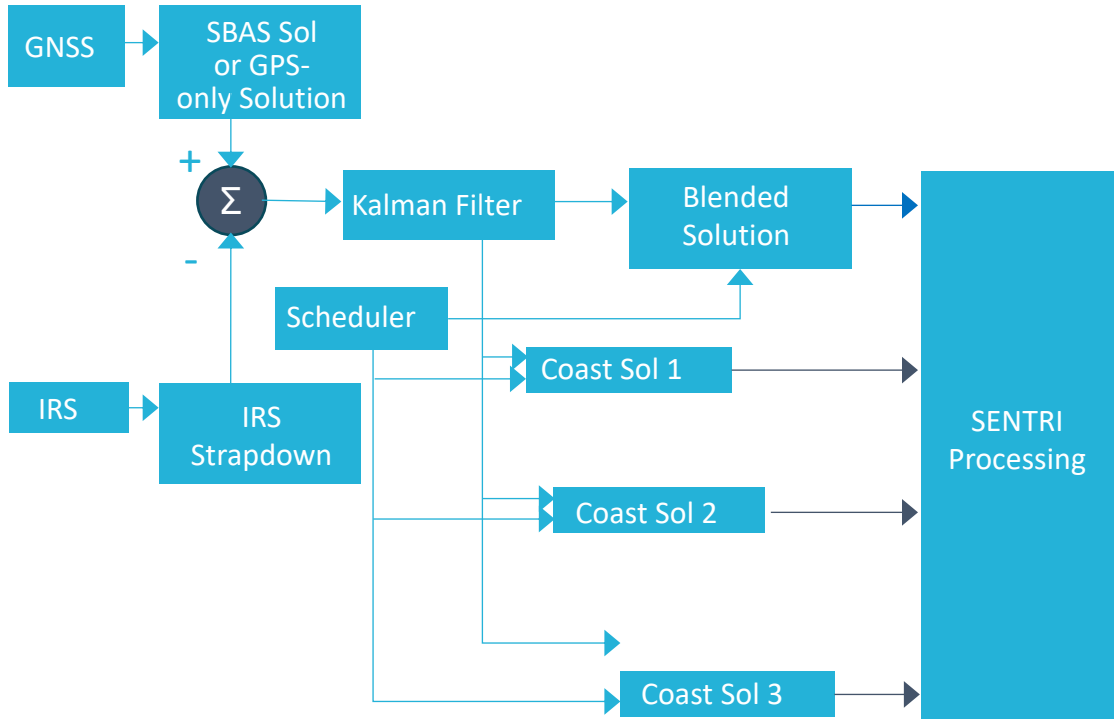
Received Transmissions

$$\begin{bmatrix} \rho_1^{False} + \varepsilon_{clk} + \Re \\ \rho_2^{False} + \varepsilon_{clk} + \Re \\ \vdots \\ \rho_n^{False} + \varepsilon_{clk} + \Re \end{bmatrix}$$



Spoofer detected by using the Spoofer's effect on the receiver's clock estimate

Staggered Examination Of Non-trusted Receiver Information



Spoofer detected by using divergence of Staggered coasted solutions from the Spoofer affected GNSS solutions

RASA and SENTRI work together to detect the spoofer using independent means

© 2026 Collins Aerospace. | Collins Aerospace Proprietary. | This document does not include any export controlled technical data. U.S. ECCN 7E994

AJ



Join SLIDO