IEEE 13TH EDITION MetroAeroSpace MADRID 2026

Madrid/ Spain 1-3 July 2026

Robust GNSS-ISL Synchronization in LEO Constellations for Space-Based Aircraft Multilateration: Assessment Using Real Data

Mauro Leonardi, Mahsa Mohebbi, Giulio Sidoretti

University of Tor vergata, Rome, Italy

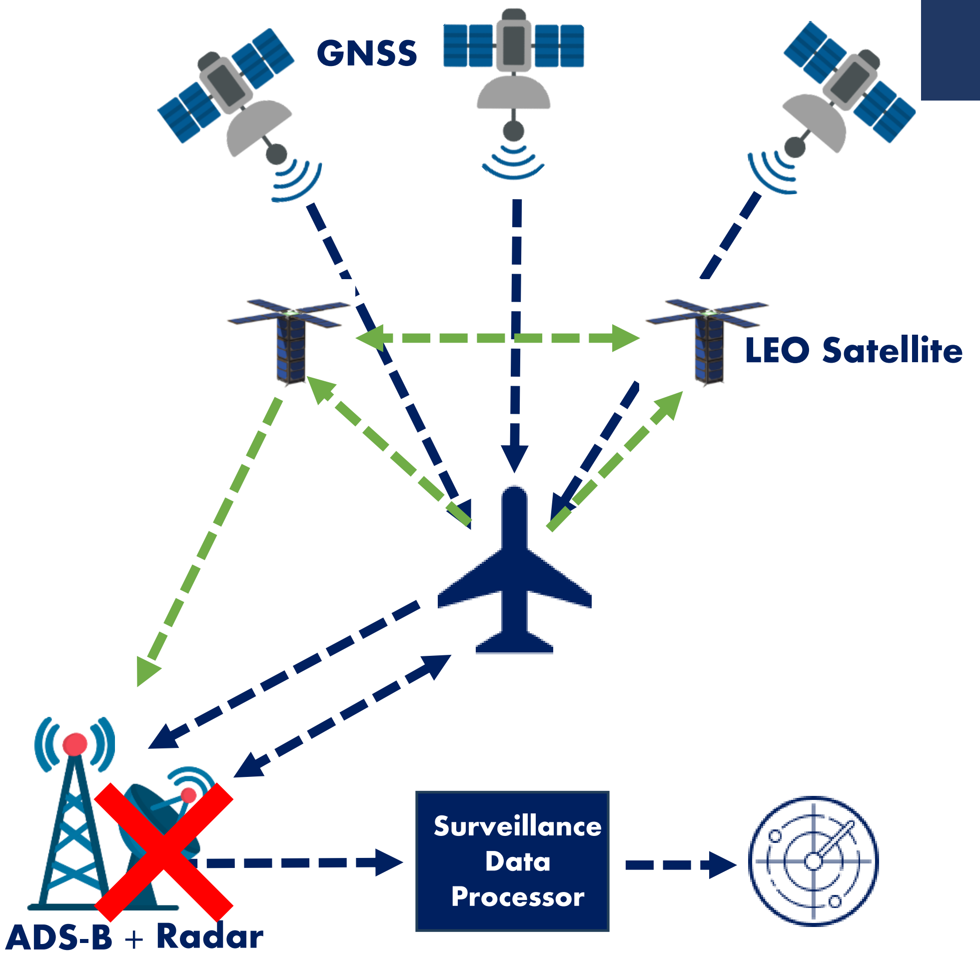
IEEE Advancing Technology for Humanity

Outline

- Problem and motivation
- SATERA Concept
- LEO Satellite Synchronization
  - Architecture overview
  - Performance evaluation framework
  - Attack scenarios
- Conclusion
- Future Work

Problem and motivation

- ❑ Air surveillance **ADS-B**.
  - Aircraft broadcast their GNSS-derived position to the ground.
- ❑ **Radar** validates ADS-B data
- ❑ Radars and ground-based ADS-B receivers are not available in remote areas, such as oceanic regions.
- ❑ Space-based ADS-B solves the coverage problem, but…



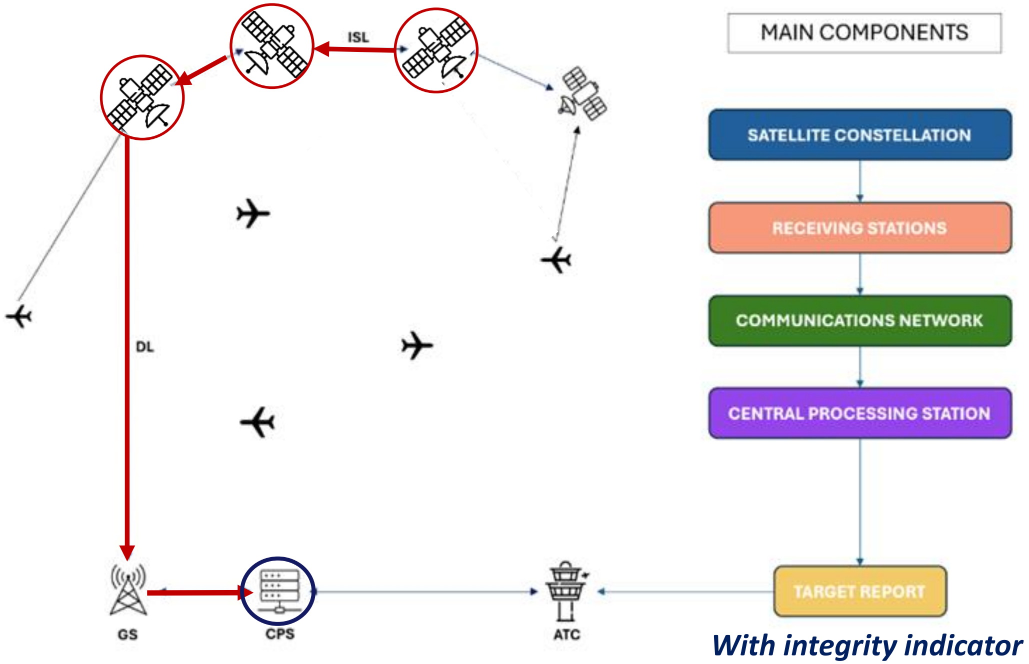
A secondary and independent localization system is required

SATERA

SUPPORTED BY sesar JOINT UNDERTAKING
Co-funded by the European Union
EXPLORATORY RESEARCH

SATERA vision

- LEO Satellites receive ADS-B and measure TOA
- ADS-B data and TOA data are relayed via ISL and DL
- MLAT position estimation performed at the CPS



SATERA system description

Why LEO Satellite synchronization matters?

✓ Precise synchronization across satellites is critical for localization accuracy

✓ LEO synchronization via GNSS can be a single point of failure

Proposed synchronization approach

✓ Dual synchronization approach

- GNSS-based
- Precise Time Protocol (PTP) over Inter-Satellite Links (ISLs)

✓ Combined via Extended Kalman Filter for accuracy and attack resilience

✓ Three Integrated Integrity Monitoring Checks within the EKF

✓ Simultaneous Detection of GNSS Anomalies, Network Faults, and Measurement Mismatches

Architecture Overview

UTC Reference -> GNSS /CPS -> Satellite clocks

Each satellite:

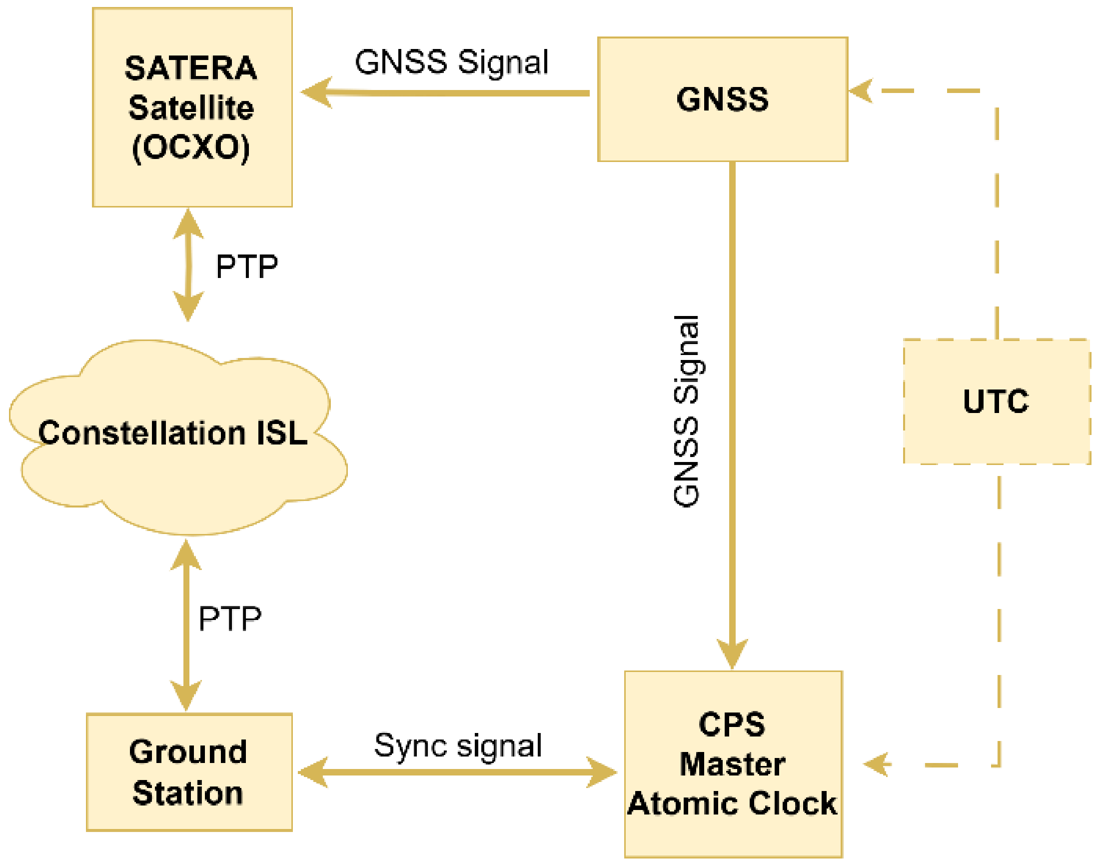
- OCXO onboard clock
- GNSS update: 30 seconds
- PTP update: 60 seconds
- GNSS + PTP synchronized to UTC

Dual synchronization:

- GNSS (primary)
- PTP over ISL (secondary)

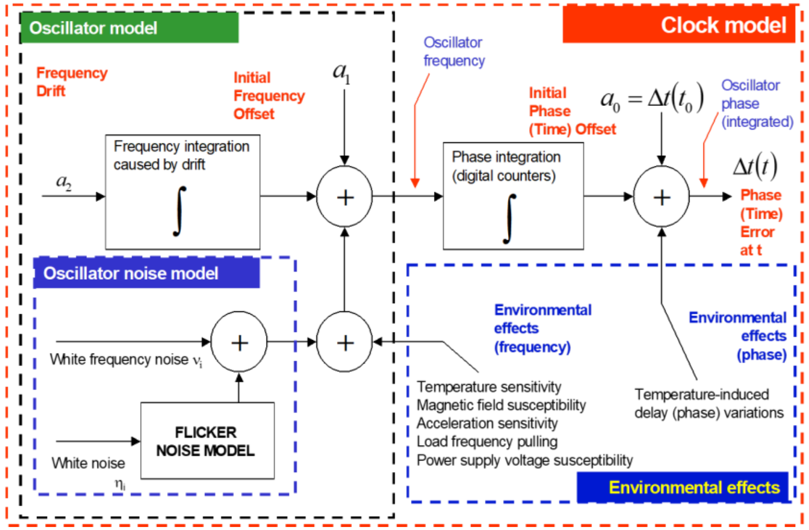
Synchronization Goal:

- Maintain UTC- consistent timing across the constellation
- Enable nanosecond-level MLAT synchronization



SATERA Synchronization process

The clock model



A Stochastic Differential Equation (SDE) model for the clock, combining systematic deviations (time offset, frequency offset, and drift) with key random components (WFM and RWFM) [1] is used.

The model include both deterministic clock dynamics and stochastic noise process

[1] L.Galleani, L.Sacerdore, P.Tavella, and C.Zucca, "A mathematical model for the atomic clock error". Metrologia, vol. 40, no. s257, pp. s257-s264,June 2003.

The clock state vector contains time deviation and random walk component of frequency deviation:

$$x(t_k) = \begin{bmatrix} x_1(t_k) \\ x_2(t_k) \end{bmatrix}$$

The discrete SDE in matrix notation is:

$$x(t_{k+1}) = Fx(t_k) + B_\tau \mathrm{m} + \mathrm{K_k}$$

Where:

$$x(t_k) = \begin{bmatrix} x_1(t_k) \\ x_2(t_k) \end{bmatrix} \quad F = \begin{bmatrix} 1 & \tau \\ 0 & 1 \end{bmatrix}$$

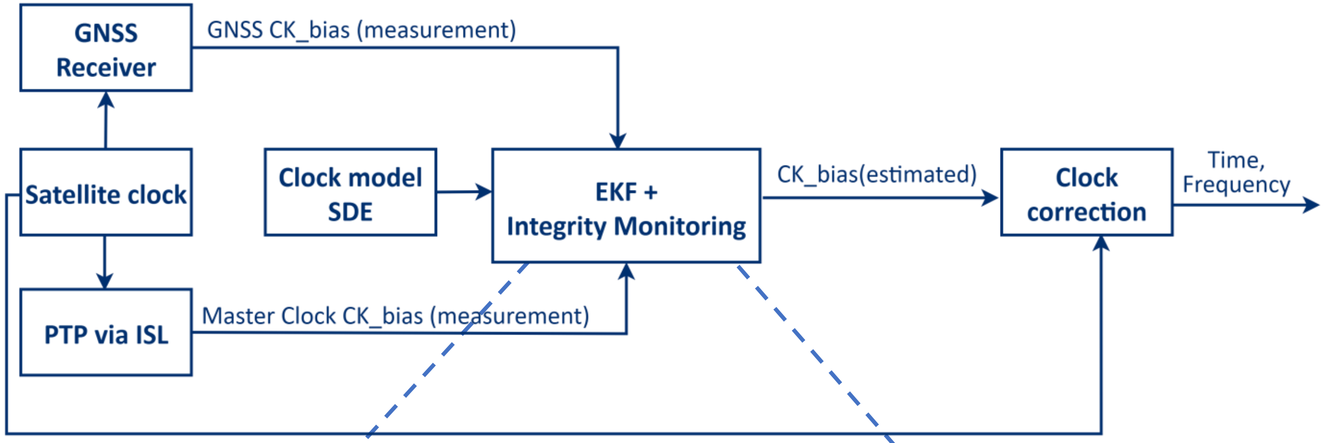
$$B_\tau = \begin{bmatrix} \tau & \frac{\tau}{2} \\ 0 & \tau \end{bmatrix} \quad m_\tau = \begin{bmatrix} \mu_1 \\ \mu_2 \end{bmatrix}$$

$$K_k = [K_{k,1}, K_{k,2}]^\tau \sim \mathcal{N}(0, Q)$$

$$Q = \begin{bmatrix} \sigma_1^2\tau + \sigma_2^2\frac{\tau^3}{3} & \sigma_2^2\frac{\tau^2}{2} \\ \sigma_2^2\frac{\tau^2}{2} & \sigma_2^2\tau \end{bmatrix}$$

Setting σ_1 and σ_2 is possible to choose the type and performance of the on-board clock

The clock bias measurement and EKF



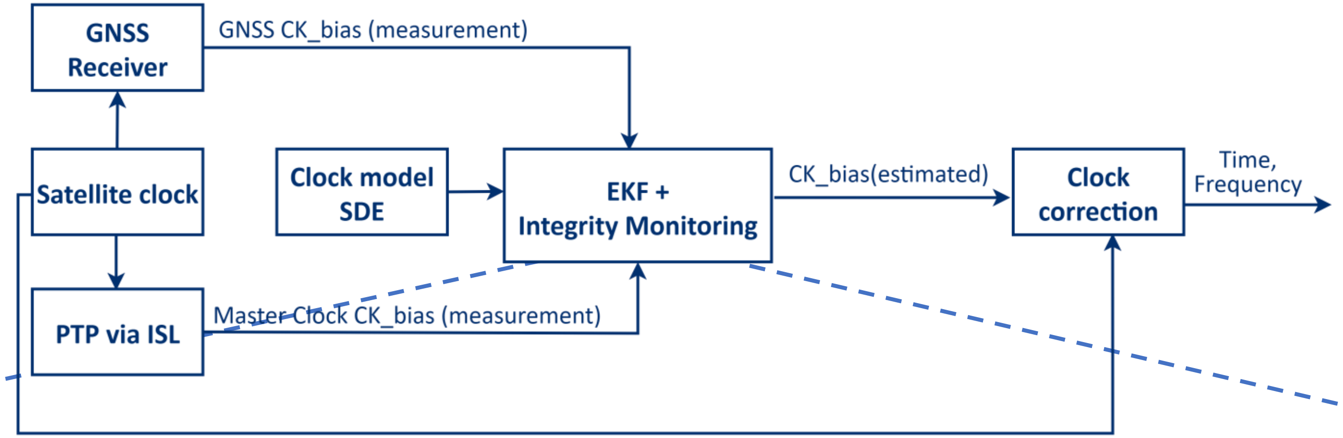
① Prediction

Predict the state of time instant t_{k+1}: $x^p(t_{k+1}) = Fx(t_k)$

Predict the state covariance matrix $P^P(t_{k+1}) = FP(t_k)F^t + Q$

- GNSS CK_bias
- Clock Dynamic model
- PTP CK_bias

The clock bias measurement and EKF



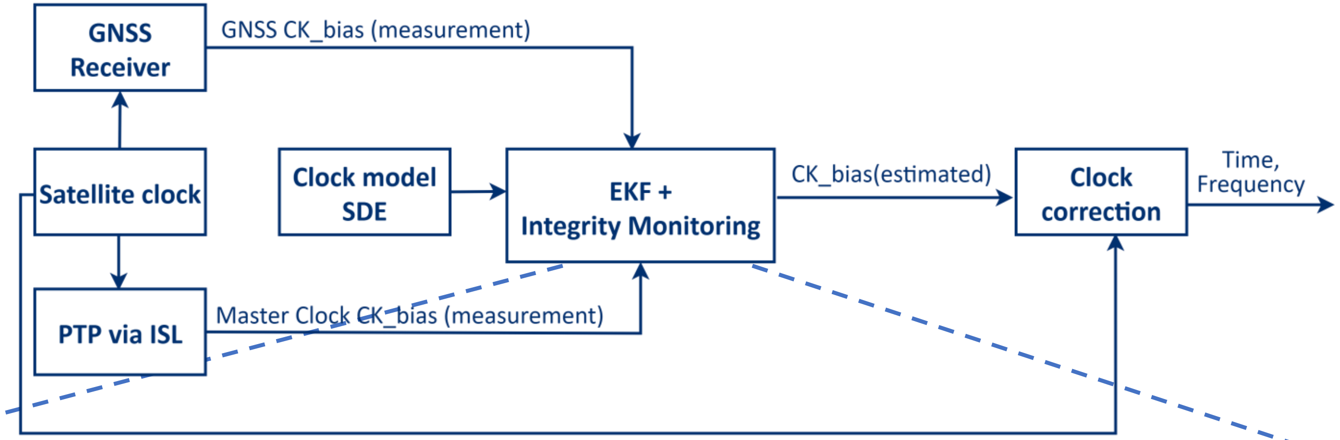
② Innovation Test

- Compute the innovation:
  $I_{k+1} = z(t_{k+1}) - Fx^p(t_{k+1})$
- Compute the innovation covariance matrix:
  $R_{k+1}FP_{K+1}^{P}F^T$
- Forward innovation to integrity monitoring

③ Dual integrity monitoring

- GNSS integrity Test $I_{(k+1)}(1) \geq \sqrt{s_{k+1}(1,1)}$ If violated: → Raise alarm; Reject GNSS Measurement
- PTP integrity check $I_{(k+1)}(2) \geq \sqrt{s_{k+1}(2,2)}$ If violated: → Raise alarm; Reject GNSS Measurement
- Conformance check $z_{GNSS}(k) - z_{PTP}(k) \geq k_c\sqrt{R_K(1,1) + R_K(2,2)}$ If violated: → Measurement mismatch; Possible fault

The clock bias measurement and EKF



④ update

If no alarms are raised, update with both GNSS and PTP

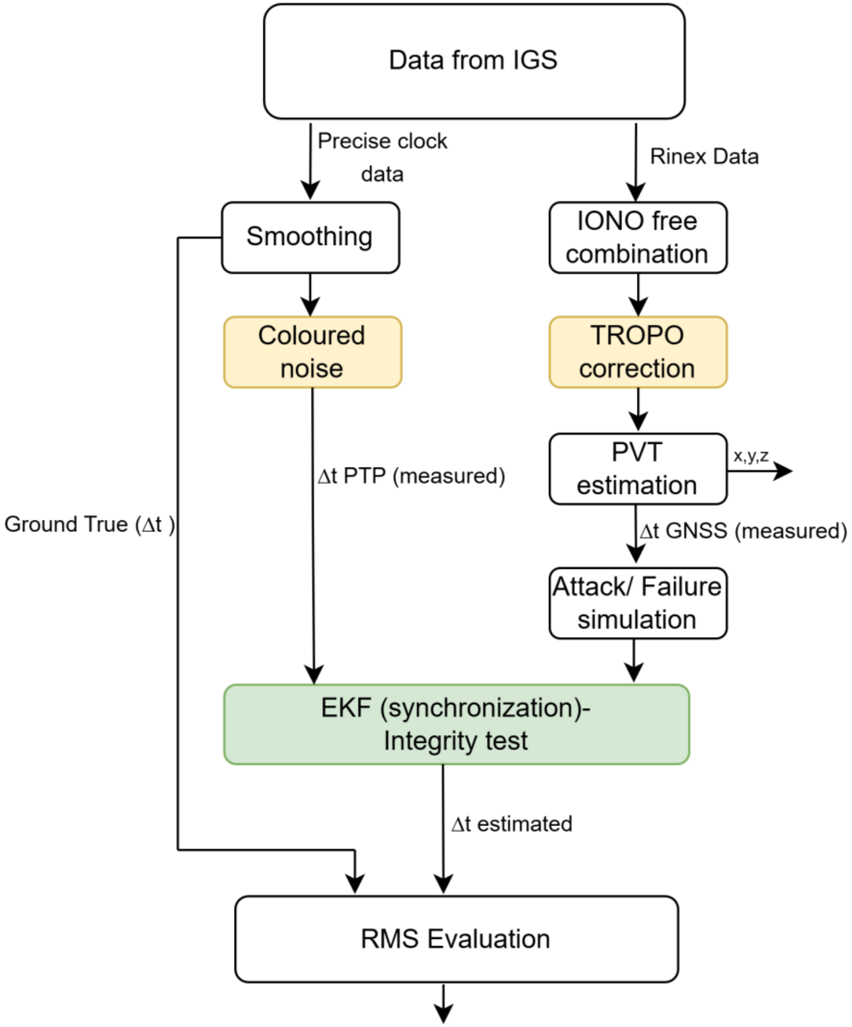
If GNSS Alarm raised, update only with PTP

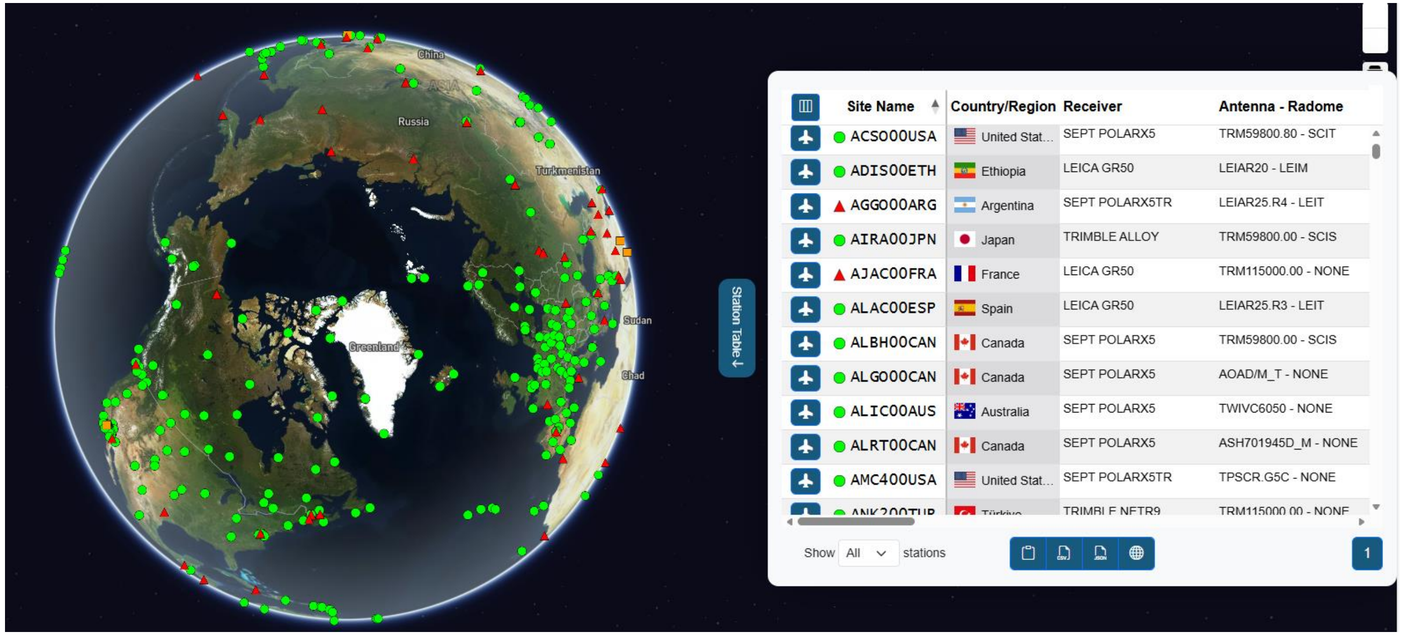
If PTP alarm raised, update only with GNSS

If conformance check alarm is raised, no update

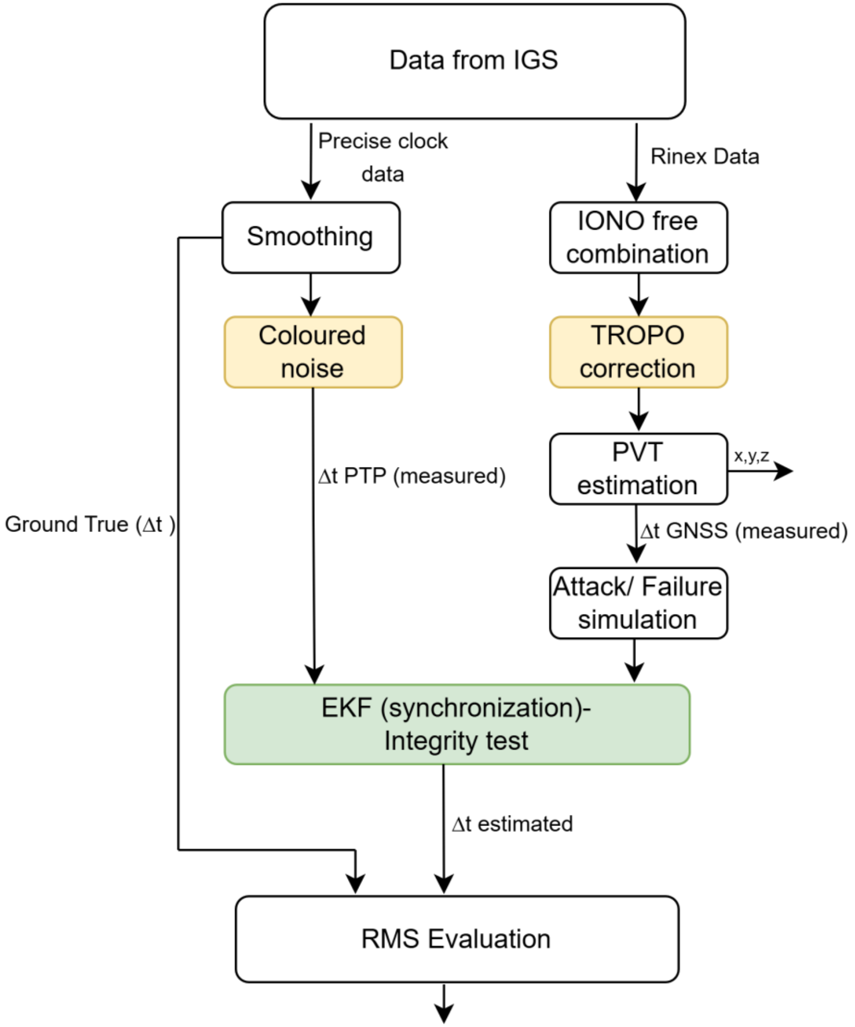
- Compute Kalman gain:
  $$G_{k+1} = P^P_{k+1} C_{k+1} (R_{k+1} + F P^P_{K+1} F^T)$$
- Update the clock state vector
  $$x(t_{k+1}) = x^P(t_{k+1}) + G_{k+1} I_{k+1_k}$$
- Update the state covariance matrix
  $$P(t_{k+1}) = (1 - G_{k+1} F) P^P_{k+1}$$

Performance Evaluation Framework





Performance Evaluation Framework



Parameter	Value
GNSS error: σ_{GNSS}	30ns
NET error: σ_{NET}	500ns
NET ρ	0.9
GNSS renewal time	30sec
NET renewal time	60sec
Clock:σ_1(WFM)	2×10^{-13}
Clock:σ_2(RWFM)	10^{-12}
Detection Threshold K_G	2.5
Detection Threshold K_N	2.5
Detection Threshold K_C	2.5

Simulated attacks

- Denial-of-service
- GNSS jamming
- Bias step spoofing
- Bias ramp spoofing

Performance assessment

- RMS clock error
- Attack window 50000-60000s
- Recovery window
- With / without integrity check

Spoofing Attack Scenario: Effect of Integrity Monitoring

Example (NOT100ITA)

Attack starts → Attack detected → Corrupted GNSS rejected

Spoofing (Bias step 1000 ns) ⇒

Without integrity monitoring:

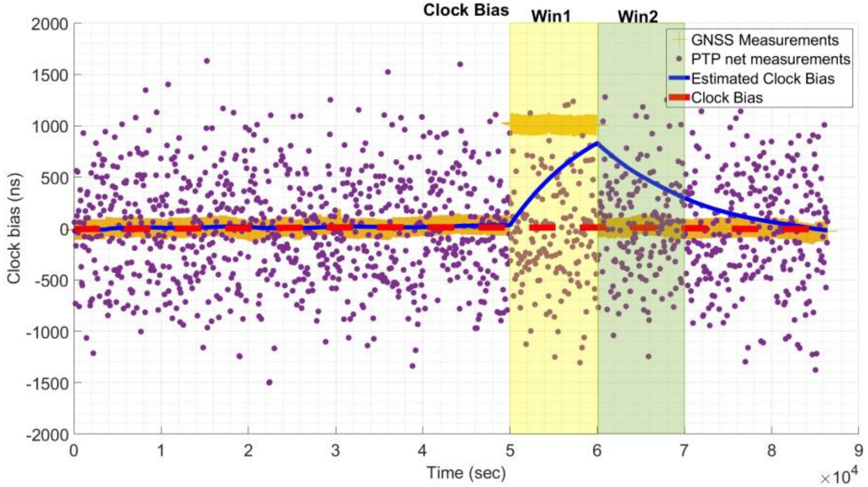
- Spoofed measurements corrupt clock estimation
- Synchronization accuracy degrades

With integrity monitoring:

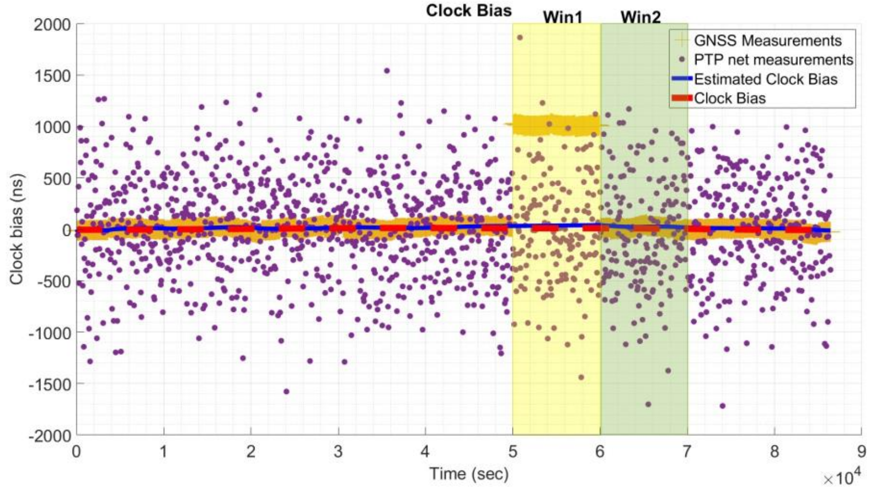
- Reliable measurements are retained
- Synchronization performance is preserved

Integrity monitoring prevents the spoofed measurements from contaminating the clock estimate

Without Integrity Checks



With Integrity Checks



Spoofing Attack Scenario: Effect of Integrity Monitoring

Example (MAT100ITA)

Spoofing (Bias ramp 10^{-9})

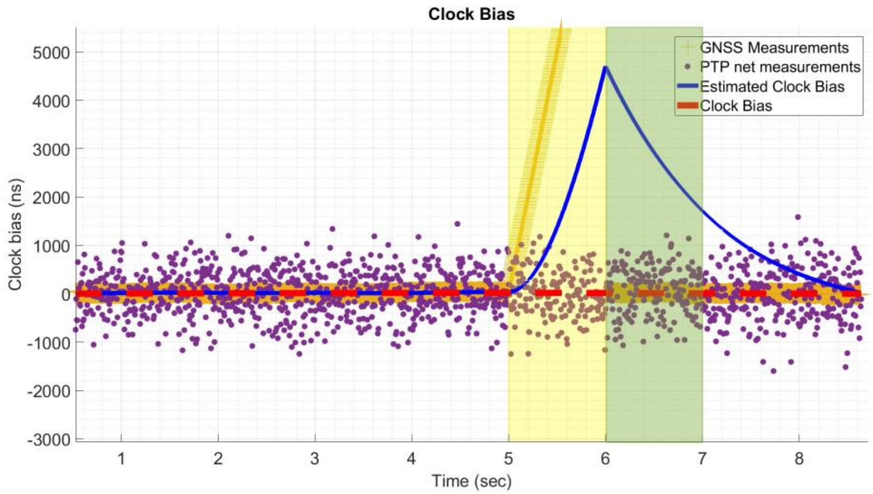
Without integrity monitoring:

- GNSS spoofing corrupts clock bias estimation
- Large synchronization error

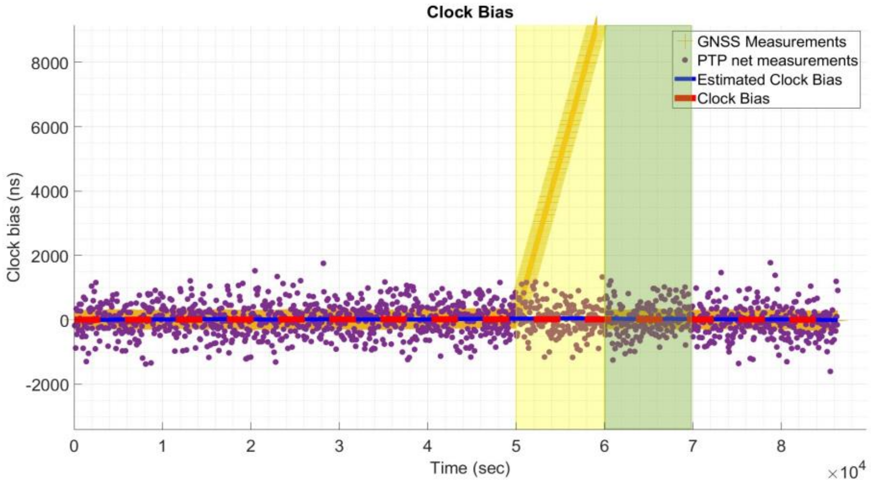
With integrity monitoring:

- Attack detected and isolated
- Clock estimation remains stable

Without Integrity Checks



With Integrity Checks



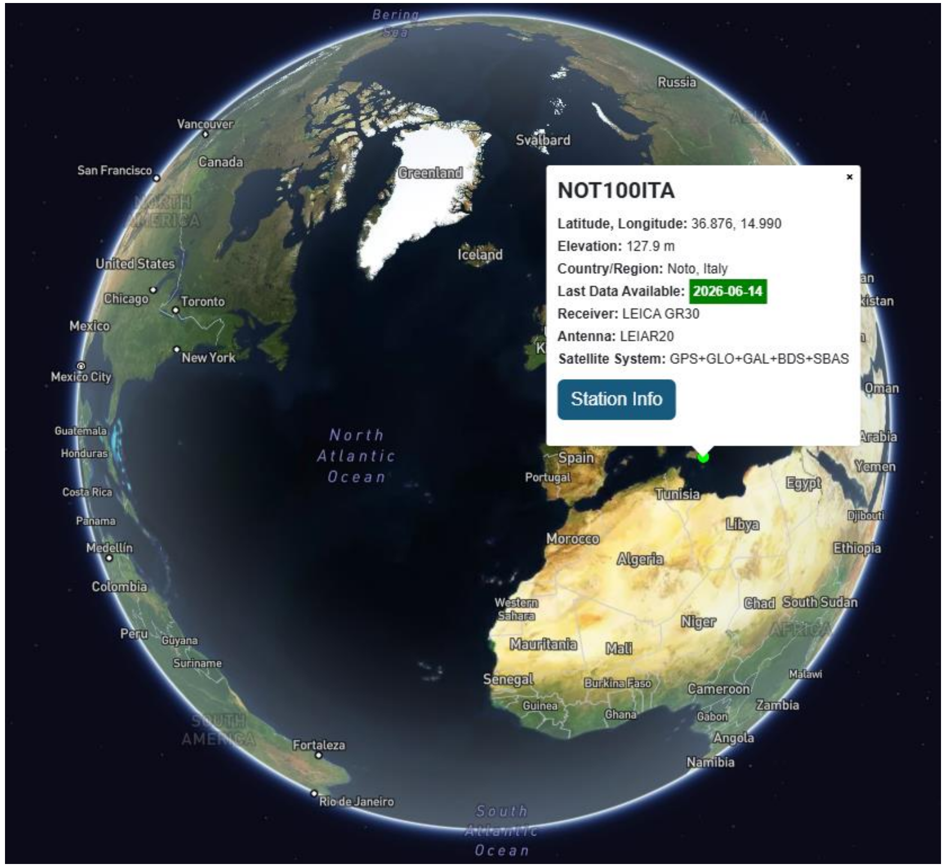
Integrity monitoring prevents the spoofed measurements from contaminating the clock estimate

Synchronization Performance Under Cyberattacks

NOTO100ITA Station

Attack	***Without Integrity***		***With Integrity***	
	Clock bias RMS error (ns)			
	Win1	win2	Win1	Win2
DOS	26.39	18.62	26.39	18.72
Jamming STD Step 1000	23.99	40	26.77	19.54
Jamming STD Step 5000	210.13	45.63	26.51	19.19
Jamming STD Step 17000	670	189.86	26.31	18.80
Spoofing Bias step 100	64.86	62.36	59.27	84.48
Spoofing Bias step 500	274.23	276.13	26.59	18.87
Spoofing Bias step 1000	536.53	543.57	26.35	18.67
Spoofing Bias step 5000	2636.8	2683.8	26.42	18.76
Spoofing Bias ramp 10^-7	219990	311560	26.38	18.76
Spoofing Bias ramp 10^-8	22007	31164	26.45	18.76
Spoofing Bias ramp 10^-9	2208.5	3004.8	26.77	18.89

Nominal:
Win1= 15.27, Win2= 10.10



Integrity monitoring reduces synchronization error by more than one order of magnitude during attacks.

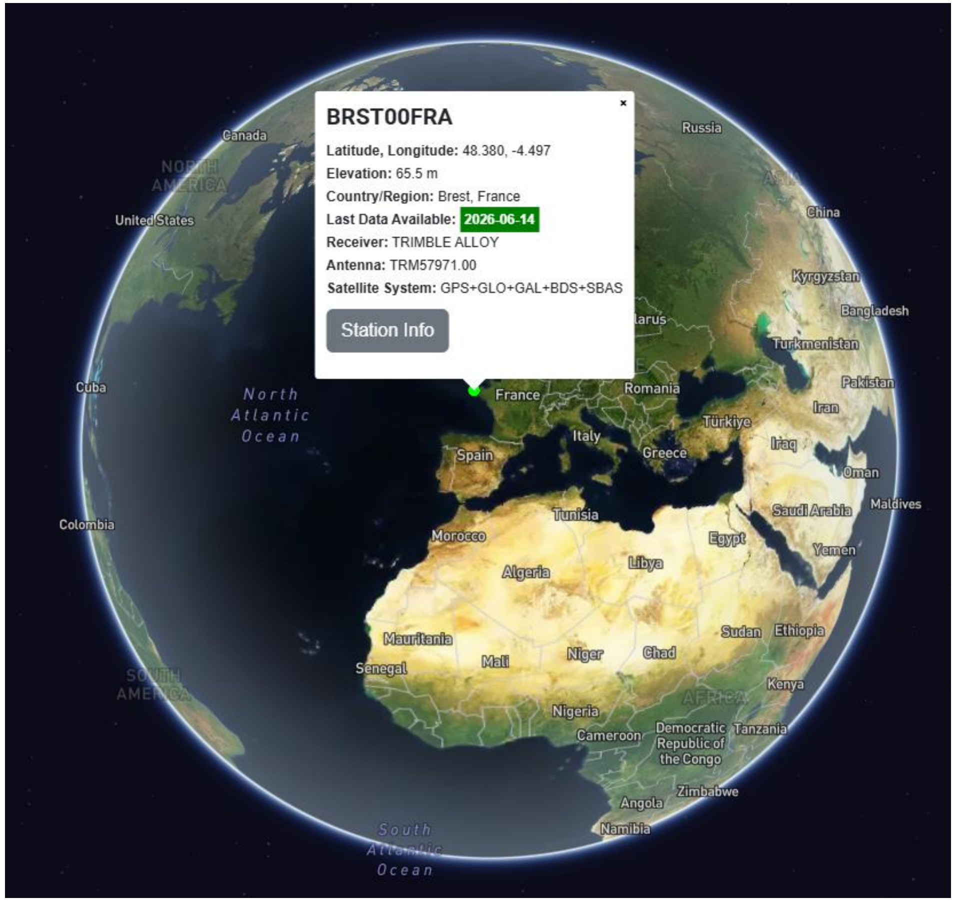
Synchronization Performance Under Cyberattacks

BRST00FRA Station

Attack	Without Integrity		With Integrity	
	Clock bias RMS error(ns)			
	Win1	win2	Win1	Win2
DOS	20.53	13.54	20.33	13.22
Jamming STD Step 1000	43.07	23.08	20.79	13.87
Jamming STD Step 5000	127.34	150.01	20.67	13.90
Jamming STD Step 17000	519.21	67.19	20.73	13.74
Spoofing Bias step 100	65.36	61.90	32.55	41.80
Spoofing Bias step 500	274.74	275.69	20.51	13.39
Spoofing Bias step 1000	537.24	543.35	20.56	13.45
Spoofing Bias step 5000	2637.3	2683.4	20.64	13.51
Spoofing Bias ramp 10^-7	219990	311560	20.34	13.27
Spoofing Bias ramp 10^-8	22007	31163	20.35	13.28
Spoofing Bias ramp 10^-9	2208.9	3123.7	20.95	13.65

Integrity monitoring reduces synchronization error by more than one order of magnitude during attacks.

Nominal:
Win1= 15.83, Win2= 8.97

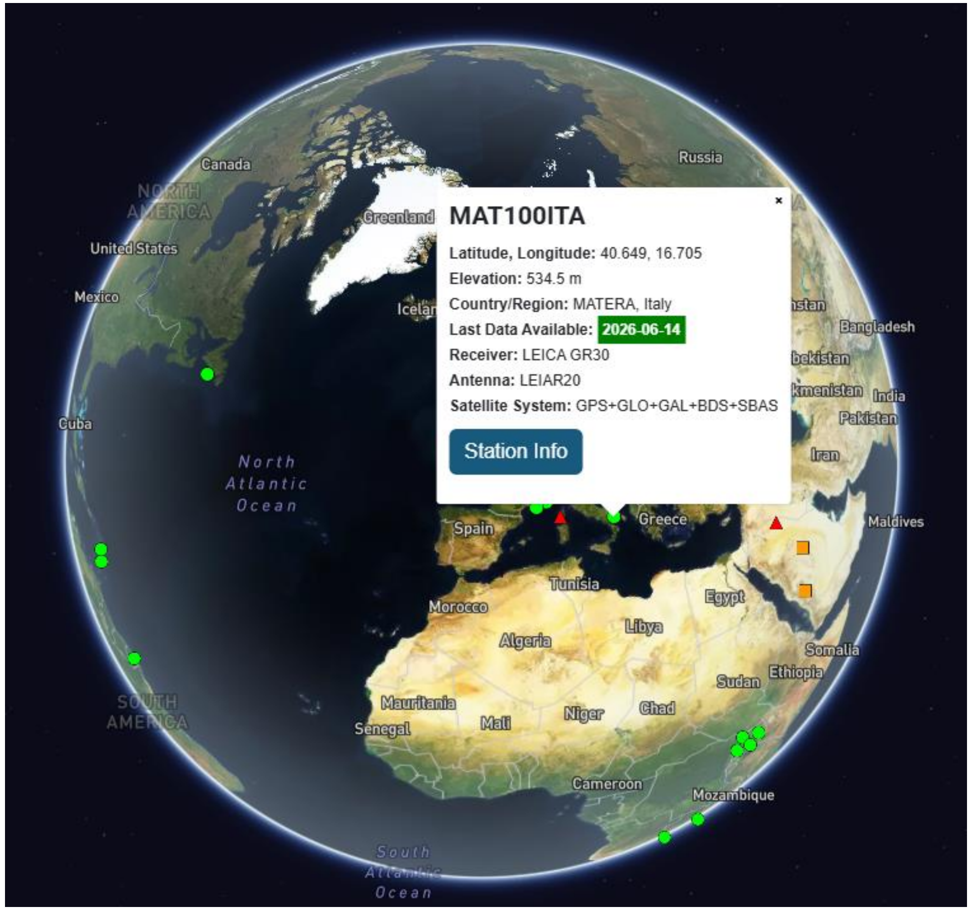


Synchronization Performance Under Cyberattacks

MAT100ITA Station

Attack	Without Integrity		With Integrity	
	Clock bias RMS error (ns)			
	Win1	win2	Win1	Win2
DOS	25.36	19.62	25.13	19.34
Jamming STD Step 1000	42.31	20.03	25.96	20.44
Jamming STD Step 5000	146.50	61.19	25.19	19.87
Jamming STD Step 17000	505.47	518.44	25.18	19.41
Spoofing Bias step 100	66.41	65.13	49.34	58.20
Spoofing Bias step 500	275.83	279.03	25.07	19.36
Spoofing Bias step 1000	583.25	546.53	25.04	19.27
Spoofing Bias step 5000	2638.5	2686.8	25.24	19.33
Spoofing Bias ramp 10^-7	219990	311560	25.19	19.35
Spoofing Bias ramp 10^-8	22008	31166	25.10	19.24
Spoofing Bias ramp 10^-9	2210.3	3127	25.79	19.73

Nominal:
Win1= 16.12, Win2= 12.30



Integrity monitoring reduces synchronization error by more than one order of magnitude during attacks.

Conclusion

Key contribution:

- ✓ 🛰️ Dual GNSS/PTP synchronization
- ✓ 🛡️ Three integrity monitoring checks
- ✓ ⚠️ Resilience against DoS, jamming and spoofing
- ✓ 📊 Validation using real IGS clock data

Key findings:

- ✓ Consistent performance across all datasets
- ✓ Nominal accuracy $\approx 15ns$
- ✓ **For all major attack scenarios below 30ns accuracy**
- ✓ Suitable for MLAT applications

GNSS-ISL synchronization with integrity monitoring provides resilient nanosecond-level timing for space-based aircraft multilateration

Future work

🛰️ **Satellite-Level Validation**

- Evaluate the framework using real LEO constellation dynamics
- Evaluate OD& Timing algorithms
- Evaluate other integrity checks such as T-RAIM

🌐 **Network Effects**

- Investigating large ISL topologies and communication delays

🎯 **Advanced Threat Models**

- Coordinated spoofing attacks
- Simultaneous GNSS/PTP attacks
- Adaptive attackers

🚀 **Integration within SATERA**

- End-to-end evaluation of synchronization impact on aircraft localization accuracy

Thank you for your attention

This research was conducted within the SATERA project. SATERA has received funding from the SESAR 3 Joint Undertaking (JU) under grant agreement No 101164313. The JU receives support from the European Union's Horizon Europe research and innovation programme and the SESAR 3 JU members other than the Union. The content of this paper reflects solely the views of its authors. The European Commission is not liable for any use that may be made of the information contained therein