

ORGANIZED BY

INTERNATIONAL ASTRONAUTICAL FEDERATION

HOSTED BY

Turkish Space Agency

The 77th International Astronautical Congress (IAC)
Antalya, Türkiye, from 5–9 October 2026

Secure GNSS and Inter-Satellite Link Synchronization for LEO Satellites Supporting Space-Based Aircraft Multilateration

Mahsa **Mohebbi**, Mauro **Leonardi**, Giulio **Sidoretti**

University of Tor vergata, Rome, Italy

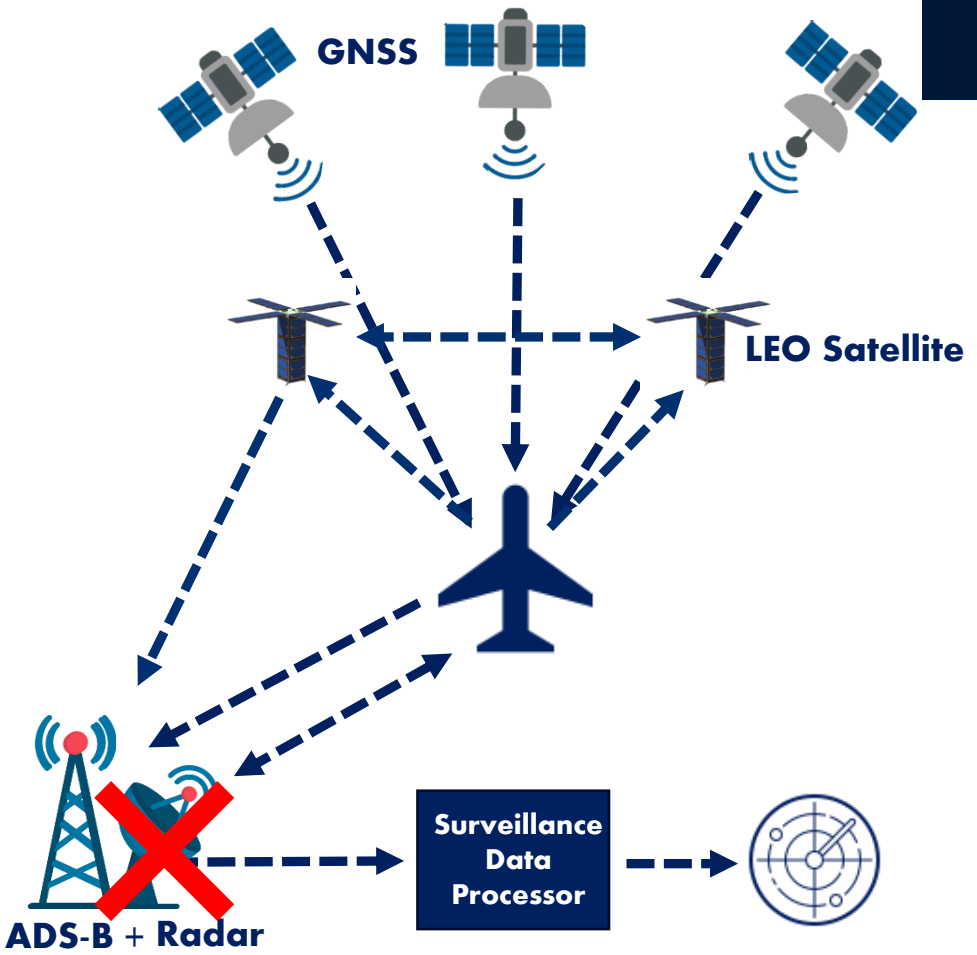
Outline

- Problem and motivation
- SATERA Concept
- LEO Satellite Synchronization strategy
- Performance evaluation framework and attack scenarios
- Results and Performance Analysis
- Conclusion and 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

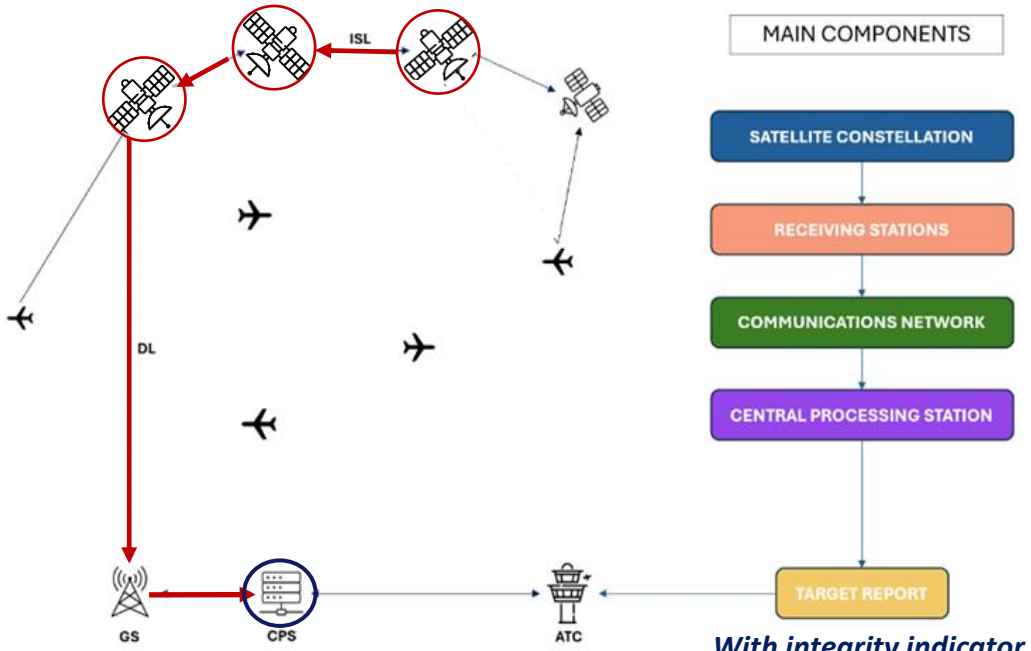
SUPPORTED BY sesar JOINT UNDERTAKING Co-funded by the European Union

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:

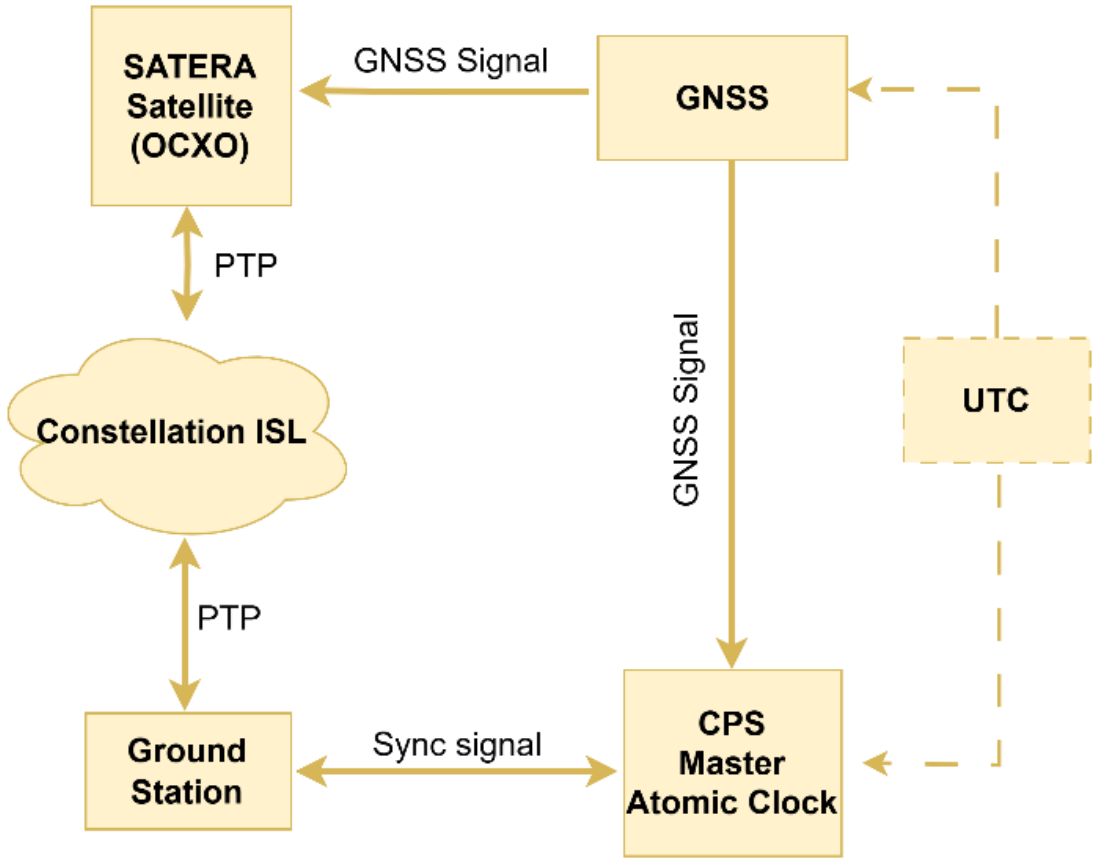
- OCXO onboard clock
- GNSS update: 1 seconds
- PTP update: 10 seconds
- GNSS + PTP synchronized to UTC

Dual synchronization:

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

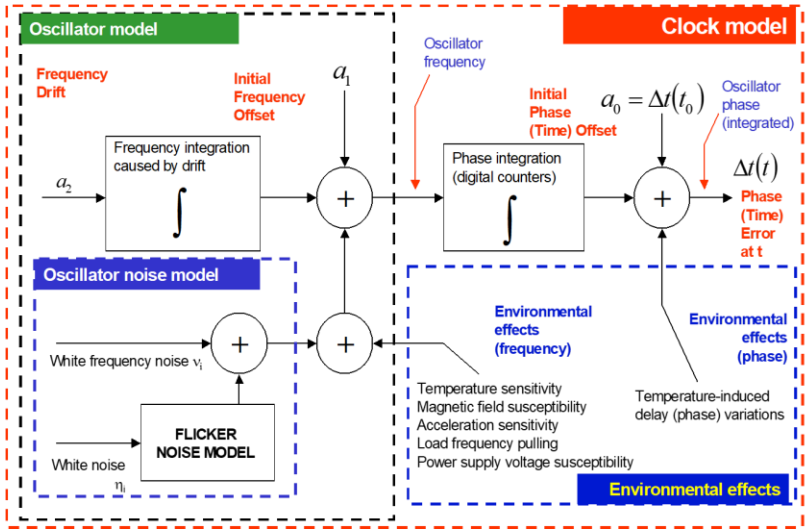
Synchronization Goal:

- 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:

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

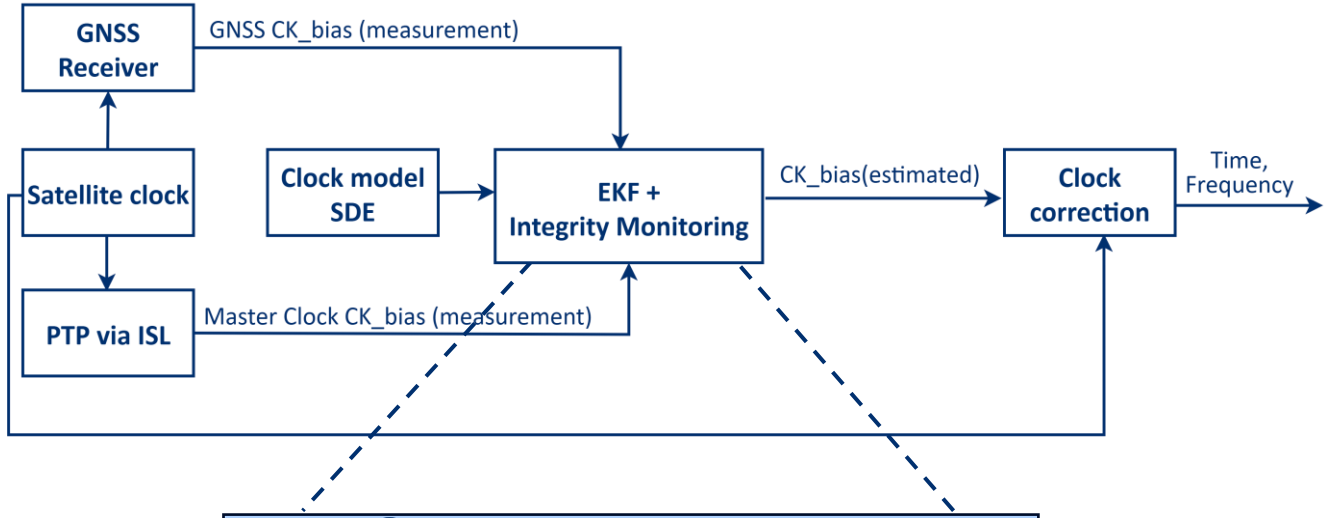
$$B_\tau = \begin{bmatrix} \tau & \frac{\tau}{2} \\ 0 & \tau \end{bmatrix} \qquad m_\tau = \begin{bmatrix} \mu_1 \\ \mu_2 \end{bmatrix}$$

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

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

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

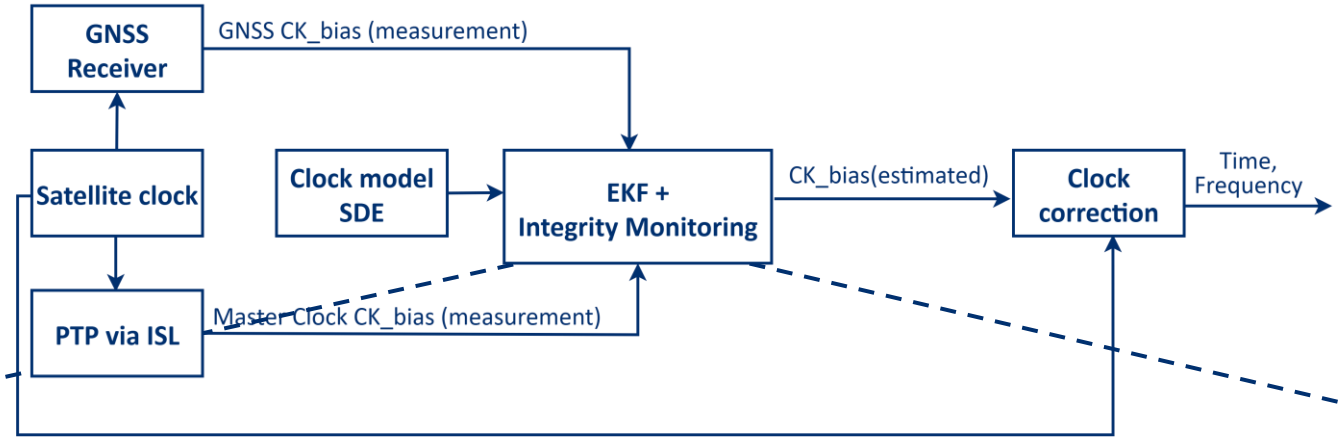
Predict the state of time instant t_{k+1}: $x^p(t_{k+1}) = Fx(t_k)$

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



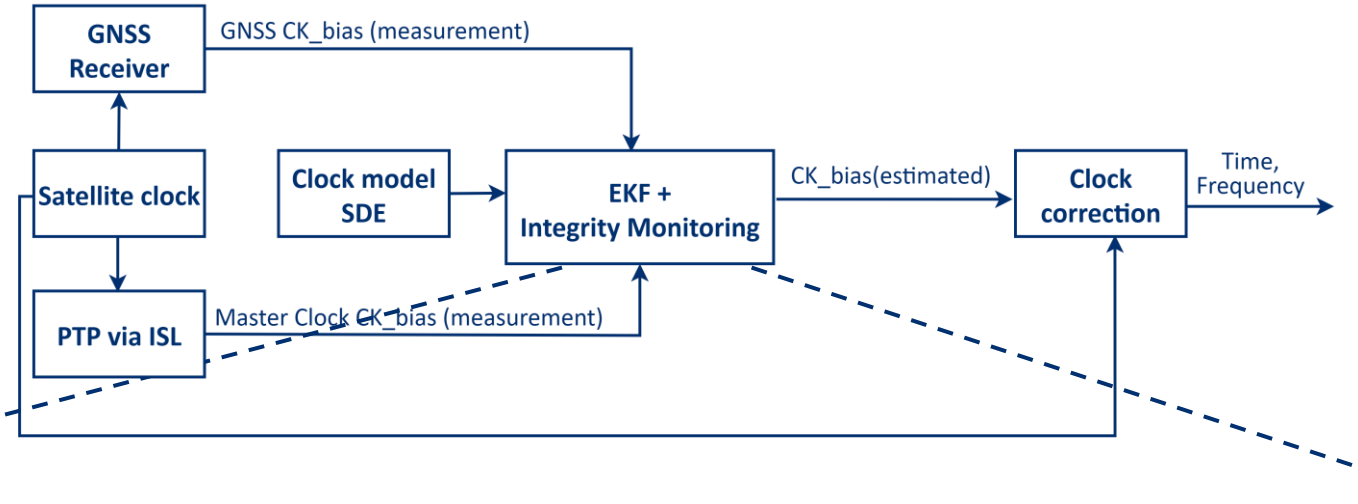
② Innovation Test

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

③ 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:
$$G_{k+1} = P^P_{k+1} C^T_{k+1} (S_{k+1})^{-1}$$
- 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

A robust Monte Carlo framework for evaluating LEO satellite clock synchronization resilience against cyber-attacks and signal anomalies under realistic colored noise conditions.

Parameter	Value	Operational Context
Monte Carlo Runs	100 Runs	Ensures statistical robustness across stochastic trials
GNSS Error (σ_{GNSS})	15 ns (Colored Noise)	Correlation factor $\rho_{GNSS} \in \{0.9, 0.99, 0.999\}$
PTP Network Error (σ_{NET})	500 ns (Colored Noise)	Inter-Satellite Link network noise with $\rho_{NET} = 0.9$
Update Frequencies	GNSS: 1 s | PTP: 10 s	GNSS renewal rate = 1 sec, Network renewal = 10 sec
Onboard Clock (OCXO)	WFM: 10-12 s | RWFM: 10-12 Hz	Quartz OCXO modeling WFM (σ_1) and RWFM (σ_2)
Detection Thresholds	$k_G = k_N = k_c = 2.5$	Calibrated to maintain False Alarm Probability (P_{fa}) < 5%

Simulated attacks

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

Performance assessment

- RMS clock error
- Attack window 50000-60000s
- Triple integrity monitoring check

Attack Scenario: GNSS Jamming (STD step 1000ns)

Attack starts (t=50000s) → **Attack detected (Innovation test)** → **Corrupted GNSS rejected**

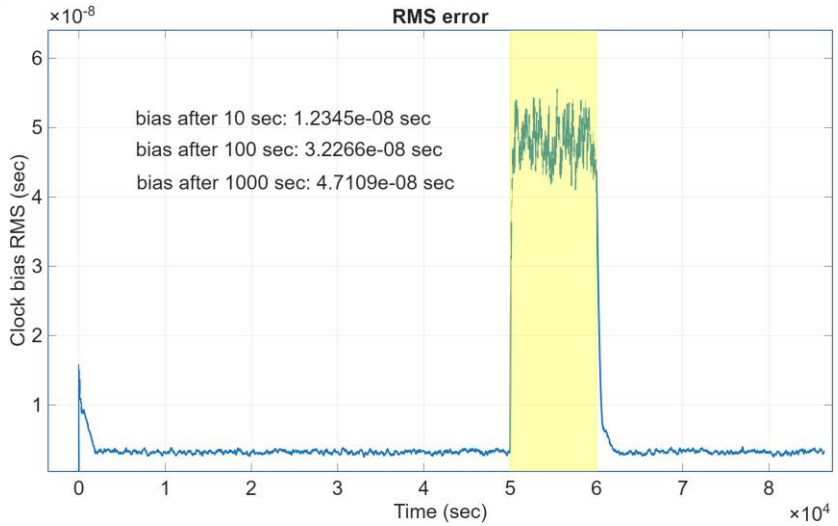
Without Integrity Monitoring (DET = 0)

- ✗ Degraded/noisy GNSS measurements directly corrupt state estimation.
- ✗ Clock bias RMS error escalates to 47.11 ns after 1000 s (peaking ~55 ns).
- ✗ Clock drift RMS error degrades by an order of magnitude.

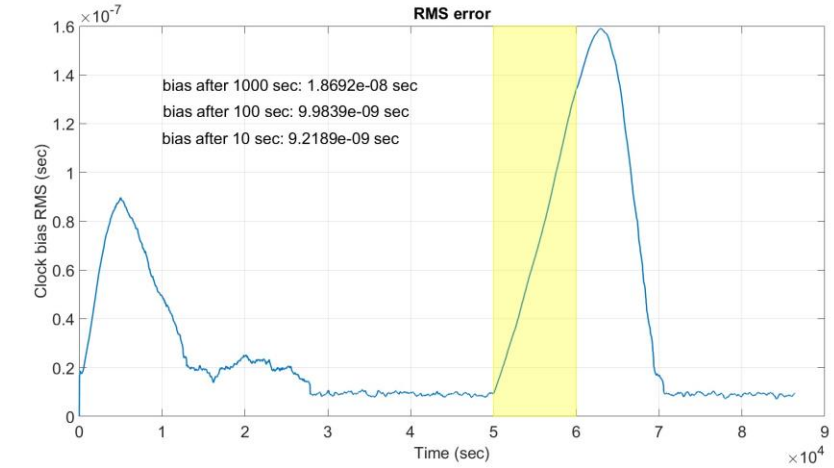
With Integrity Monitoring (DET = 1)

- ✓ Innovation check detects statistical anomaly instantly ( ).
- ✓ Corrupted GNSS rejected; clock steered reliably via ISL PTP link.
- ✓ Clock bias error remains bounded and sub-nanosecond level stability preserved.

Integrity check OFF



Integrity check ON



Results and attack mitigation

Comparison of maximum clock bias RMS error (ns) between unprotected (DET=0) and protected (DET=1) modes under realistic colored noise conditions ( ). $\sigma_{GNSS} = 0.9$

Attack	*Without Integrity*				*With Integrity*			
	Clock bias RMS error(ns)							
	Nominal	Under attack			Nominal	Under attack		
		100 s	1000 s	Max		100 s	1000 s	Max
DOS	~4	3.31	6.7	~35	~4	4	6.4	~37
Jamming STD Step 1000	~4	32.26	47.1	~55	~4	~4	7.5	~80
Jamming STD Step 5000	~4	149	240	~300	~4	~4	8.1	~80
Jamming STD Step 17000	~4	495.22	933.87	~1000	~4	~4	7.2	~98
Spoofing Bias step 1000	~4	297.7	1207.2	~1300	~4	~4	7.2	~230
Spoofing Bias step 5000	~4	1490.5	6036.4	~6000	~4	~4	8.03	~60
Spoofing Bias step 17000	~4	5068.6	20523	~21000	~4	~4	6.4	~55
Spoofing Bias ramp 10^-7	~4	1534.6	87550	~1000000	~4	~4	6.9	~53
Spoofing Bias ramp 10^-9	~4	15.59	874.87	~10000	~4	~4	8.2	~72

Results and attack mitigation

Comparison of maximum clock bias RMS error (ns) between unprotected (DET=0) and protected (DET=1) modes under realistic colored noise conditions ( ). $\sigma_{GNSS} = 0.99$

Attack	*Without Integrity*				*With Integrity*			
	Clock bias RMS error(ns)							
	Nominal	Under attack			Nominal	Under attack		
		100 s	1000 s	Max		100 s	1000 s	Max
DOS	~10	9.25	19.16	~60	~10	9.5	19	~60
Jamming STD Step 1000	~10	10	9	~10	~10	9.9	18.6	~130
Jamming STD Step 5000	~10	140.04	230.49	~300	~10	10.5	19.4	~137
Jamming STD Step 17000	~10	475.85	896.44	~900	~10	11.2	20.6	~155
Spoofing Bias step 1000	~10	298	1205.8	~1200	~10	9.9	19.8	~230
Spoofing Bias step 5000	~10	1489.8	6035.4	~6000	~10	9.1	18.2	~125
Spoofing Bias step 17000	~10	5068.5	20523	~21000	~10	9.7	18.6	~118
Spoofing Bias ramp 10^-7	~10	1535.6	87551	~1000000	~10	10.4	19.6	~130
Spoofing Bias ramp 10^-9	~10	18.07	876.29	~10000	~10	10.5	20.2	~130

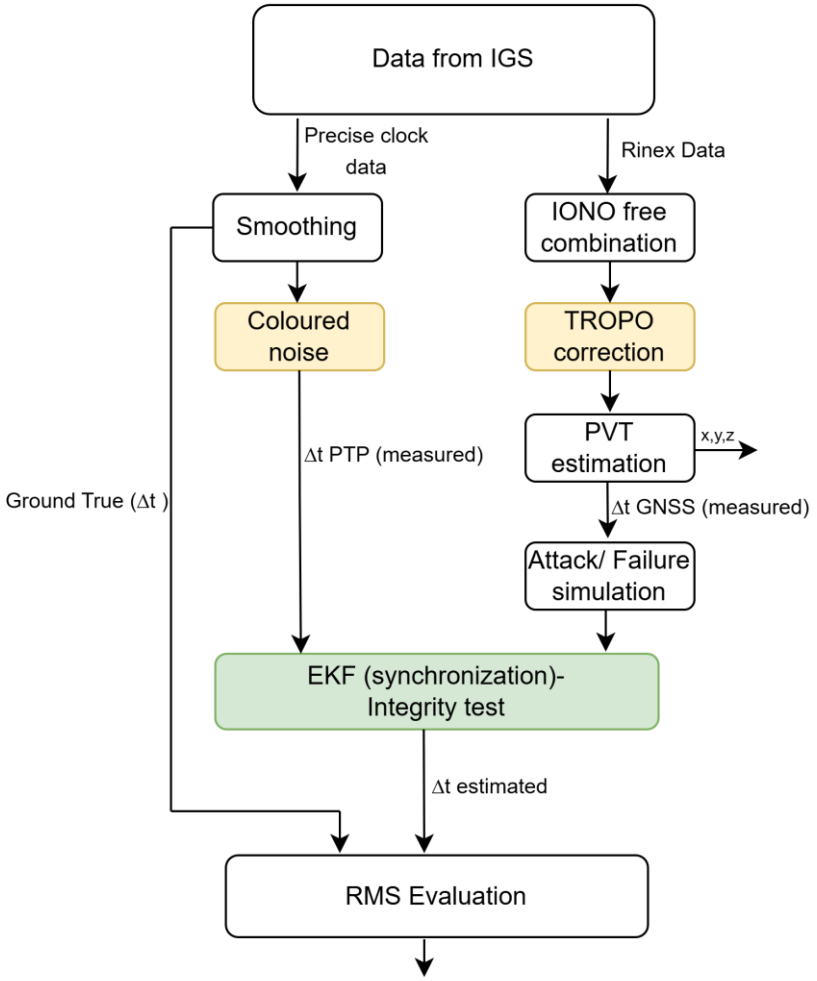
Results and attack mitigation

Comparison of maximum clock bias RMS error (ns) between unprotected (DET=0) and protected (DET=1) modes under realistic colored noise conditions ( ). $\sigma_{GNSS} = 0.999$

Attack	*Without Integrity*				*With Integrity*			
	Clock bias RMS error(ns)							
	Nominal	Under attack			Nominal	Under attack		
		100 s	1000 s	Max		100 s	1000 s	Max
DOS	~15	16.59	26.45	~70	~20	~20	28.8	~77
Jamming STD Step 1000	~15	33.90	51.33	~60	~20	28.7	37.2	~170
Jamming STD Step 5000	~15	160.15	259.82	~310	~20	~20	23.8	~165
Jamming STD Step 17000	~15	518.99	814.32	~1000	~20	33.3	38.7	~190
Spoofing Bias step 1000	~15	300.68	1208.4	~1200	~20	33.5	37.9	~245
Spoofing Bias step 5000	~15	1490.9	6036.1	~6000	~20	20.6	29.3	~160
Spoofing Bias step 17000	~15	5068.2	20524	~21000	~20	~20	28.7	~190
Spoofing Bias ramp 10^-7	~15	1535.4	87550	~1000000	~20	~20	27.5	~135
Spoofing Bias ramp 10^-9	~15	20.47	875.39	~10000	~20	25.9	31	~170

Experimental Validation: Using IGS Station Data

(as established in [MetroAeroSpace, 2026])





Experimental Validation: Using IGS Station Data

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

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

Nominal:
Win1= 16.12, Win2= 12.30



Conclusion

Key contribution:

- ✓ 🛰️ Dual GNSS/PTP synchronization
- ✓ 🛡️ Three integrity monitoring checks
- ✓ ⚠️ Resilience against DoS, jamming and spoofing

Nanosecond-Level Accuracy: Achieves sub-microsecond timing precision (< 30 ns steady-state) under all nominal and adversarial scenarios.

Future work

- ✓ 🛰️ Constellation dynamics
- ✓ 🛡️ Advanced threat detection
- ✓ ⚠️ End to End SB-MLAT Integration

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