Next Generation Network-assisted PNT Assurance

E. Roberto MATERA,
THALES SERVICES NUMERIQUES

NTN DAYS 2025
01/10/2025

THALES
Building a future we can all trust

NTN DAYS
Non-Terrestrial Networks
Bridging Space, Air, and Ground
LAAS, Toulouse, France October 1 and 2, 2025

Outline

01 Context

02 Objective and Proposed Solution

03 Methodology

04 Experimental Results

1 – Context

www.thalesgroup.com

Context (1/5)

> GNSS are fundamental for precise positioning, timing, and velocity:

- **transportation** (aviation, maritime, land, unmanned aerial vehicles) and
- **critical infrastructures** (financial services, telecommunications).

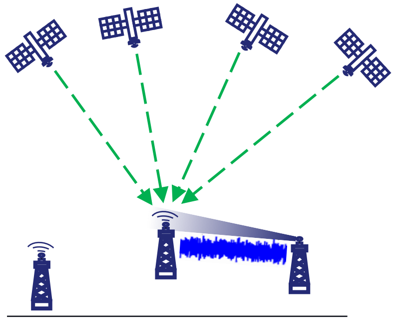
> GNSS vulnerabilities are exposed to malicious attacks:

- inaccurate positioning,
- navigation errors,
- service disruptions,
- **unreliable safety, efficiency, and security**.

> Classic GNSS signals are **weak** and **Open Service**, making them susceptible to interference and manipulation easily accessible to malicious actors.

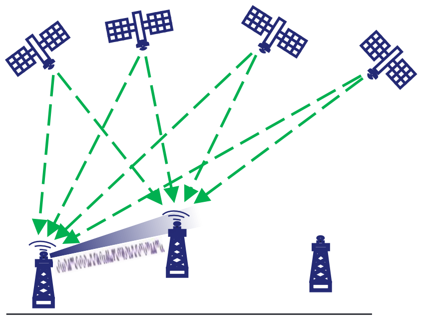
Context (2/5)

> **Jamming** and **Spoofing** attacks exploit inherent GNSS vulnerabilities and are becoming more frequent and affordable to execute



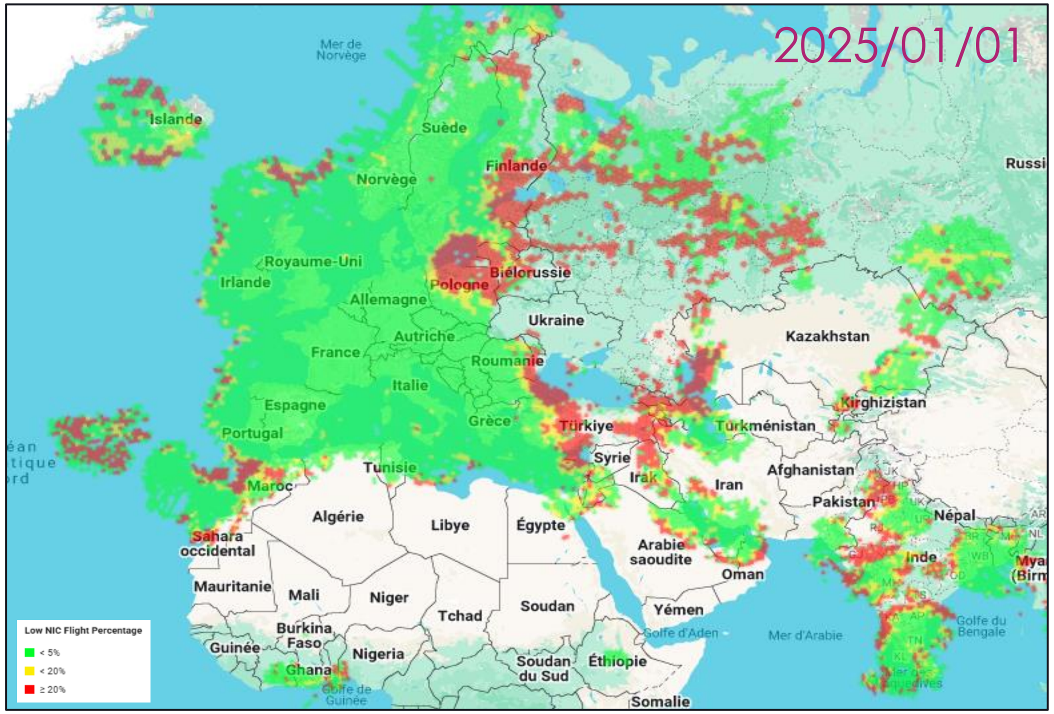
Jamming

Transmitting high-power signals at the desired frequency **to blind target receivers**



Spoofing

Transmitting fake signals that mimic authentic ones at higher power **to cheat target receivers**



[waas-nas.stanford.edu: GNSS Interference Detection using ADS-B]

> **Detecting** and **mitigating** these threats is **essential** to **ensure a robust PNT solution**

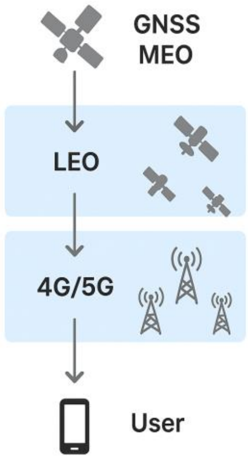
Context (3/5)

> Emergence of NTN (LEO) space signals:

- Widespread deployment of LEO satellite constellations adds many new transmitters and diverse geometries, increasing observability and shortening time to detect anomalies.

> New frequencies & modern modulations:

- Multi-band signals and advanced modulations (wider bandwidths, hybrid waveforms) increase observability and robustness.



Benefits of Diversity

Space	Increased satellite coverage
Frequency	Resilience to interference
Terrestrial	Enhanced reliability

> Cellular & terrestrial networks (4G/5G):

- Cellular networks (4G/5G) bring three useful capabilities: dense reference/time sources, cryptographic authentication of messages (where supported), and a communications channel to distribute network-side integrity/corrections.

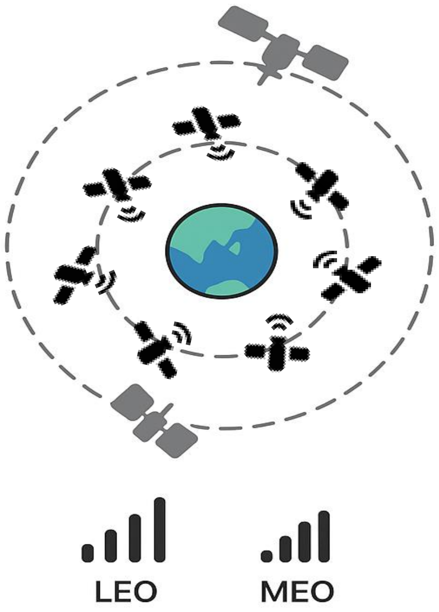
> Why it matters for Assurance:

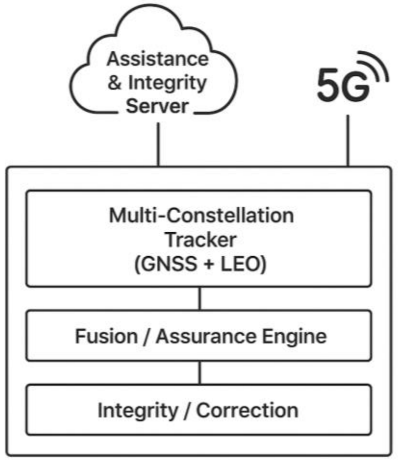
- **Diversity across space, frequency, and technology enables cross-checks, rapid detection of inconsistent measurements, and authenticated corrections.**

Context (4/5)

> LEO satellites:

- Stronger received signals
- Fast orbital motion
- Dense revisit times
- Improved geometry and dilution of precision





> Navigation benefits:

- Improved availability (especially in urban canyons),
- Additional ranging/ Doppler measurements,
- Faster geometry refresh for quicker integrity detection.

> Practical considerations

- Doppler and fast geometry are a double-edged sword: they provide a rich signature to detect spoofing (spoofers must match rapidly changing Doppler/time), but require the receiver to handle higher dynamics.
- **Need for accurate LEO ephemerides and time-clock distribution, higher Doppler rates requiring signal processing adaptation, and heterogeneous signal formats that require flexible receivers.**

Context (5/5)

> Current and Emerging LEO PNT and LEO COM providers

LEO PNT

Company	Country	First Launch	Launched	Frequency Band	Total Planned
Iridium	USA	2017[14]	66	L	66
Xona Space	USA	2022	1 tech demo	L	258
TrustPoint	USA	2023	2 tech demos	C	300
JAXA	Japan	-	0	C	480
ArkEdge Space	Japan	-	0	VHF	50-100
Centispace	China	2018	5 tech demos	L	190
Geely	China	2022	0	L	240
SatNet LEO	China	2024	0	L	506
ESA's FutureNAV LEO-PNT IoD	Europe	-	0	L, S, C, UHF	10 demos (up to 263)

Table . Current and emerging dedicated LEO PNT providers.

LEO COM

Company	Constellation	Country	First Launch	Launched	Frequency	Total Planned
SpaceX	Starlink	USA	2019	7000+	Ku, Ka	42,000
China SatNet	Guowang	China	2024	10	Ku, Ka	12,992
SSST	G60	China	2024	36	Ku	12,000
Hongqing Technology	Honghu-3	China	-	0		10,000
GeeSpace	GEESATCOM	China	2022	30		5,676
Lynk	Lynk	USA	2022	6	L	5,000
Amazon	Kuiper	USA	2023	2	Ku, Ka	3,236
Skykraft	Skykraft	Australia	2023	10	S	2,976
EutelSat OneWeb	OneWeb Gen I	France, UK	2019	634	Ku, Ka	648
Rivada	OuterNET	USA	-	0	Ka	576
CASC	Hongyan-1	China	2018	1	Ka, L	320
SpaceRise	IRIS²	EU	-	0	Ka, S	290
Sateliot	Sateliot	Spain	2023	6	L	250
Telesat	Lightspeed	Canada	-	0	Ku, Ka	198
AST SpaceMobile	Bluebird	USA	2023	5	L, S	168
ArkEdge	ArkEdge	Japan	-	0	VHF	50-100
Iridium	NEXT	USA	2017	80	L	80
Globalstar	Globalstar	USA	1998	48	S	65
Orbcomm	Orbcomm	USA	1995	31	L, S	31

Table . Current and emerging satellite communication providers in LEO as of December 2024.

FrontierSI-State-of-Market-Report-LEO-PNT-2024-Edition-v1.1.pdf

2 – Objective and Proposed Solution

www.thalesgroup.com

Objective (1/2)

> **Objective:** To **provide** an end-to-end **network-assisted Positioning, Navigation, and Timing** (PNT) **Assurance** service counteracting spoofing activities.

> **NAVISP-EL1-040:**

- ESA's Navigation Innovation and Support Program (NAVISP) is a key enabler for innovation and competitiveness and a strategic Tool of ESA to support and develop the overall European POSITIONING, NAVIGATION and TIMING (PNT).
- The main NAVISP objective is to facilitate the generation of Satellite Navigation/PNT innovative propositions with participating States and their industry, in coordination with EU and its institutions. (ESA's NAVISP Programmes)
- Project Led by Telespazio UK, working with Thales Services Numériques, M3 Systems and Chronos Technology

> **Strategy:**

- **Investigating potential system architectures**
- **Developing 'technology enablers'** to provide users with a comprehensive PNT assurance system, including approaches for authentication (of GNSS ranging signal/navigation information, and user time offset), and integrity of SOOP signal acquisition
- Preparing a comprehensive **real-world evaluation for static use cases**, benchmarking the performance of the developed GNSS plus SOOP hybrid positioning techniques using reference network assistance system

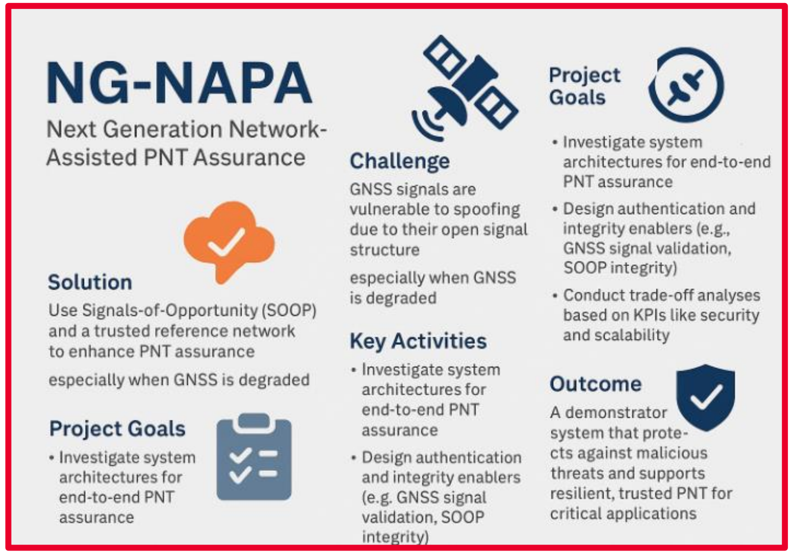
Objective (2/2)

> PNT Assurance

- NG-NAPA aims to provide assured PNT by combining GNSS with Signals of Opportunity (SOOP), such as 5G, LTE, and LEO satellite signals. These alternative signals can complement or even replace GNSS in degraded environments.

> Flexible Deployment

- The **system** is designed to be **adaptable** for both **static and dynamic use** cases, meaning it can support everything from stationary industrial equipment to mobile platforms like vehicles or drones.
- **Malicious Threat Protection**
- NG-NAPA is specifically engineered to detect and mitigate threats to PNT integrity, ensuring users can trust the positioning data even in contested or spoofed environments.
- Industry and National Infrastructure Support
- It supports applications in Industry 4.0, transportation, and national critical infrastructure, where reliable and secure PNT is essential.

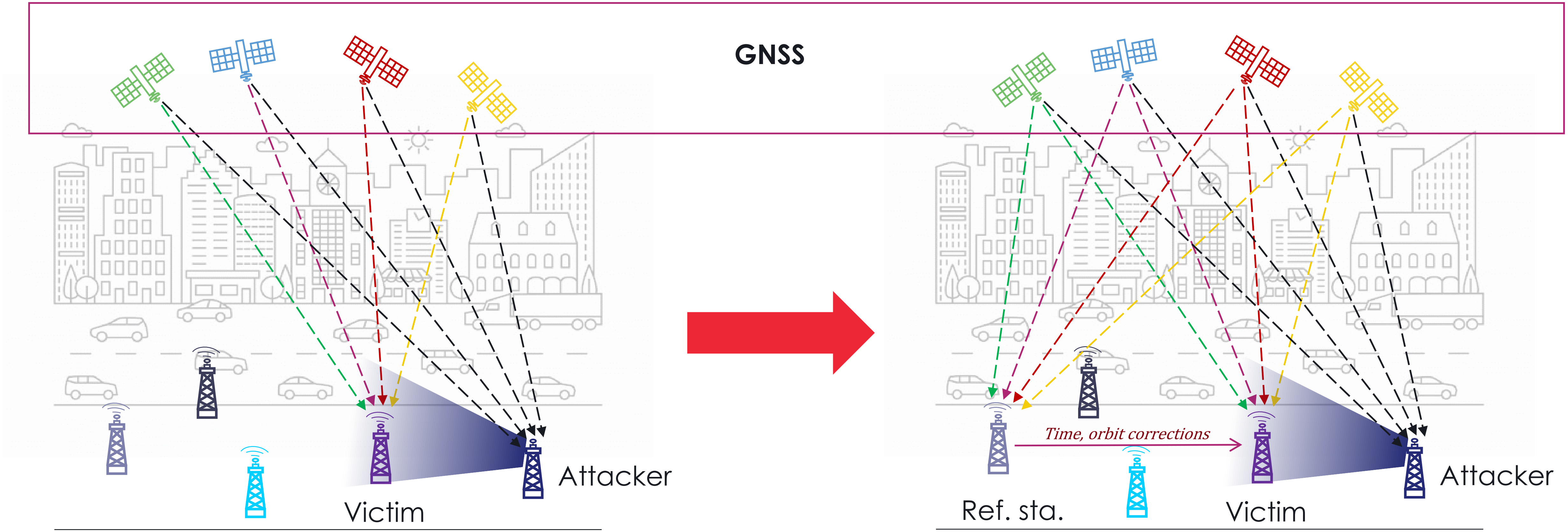


3 – Methodology

www.thalesgroup.com

Proposed Solution (1/7)

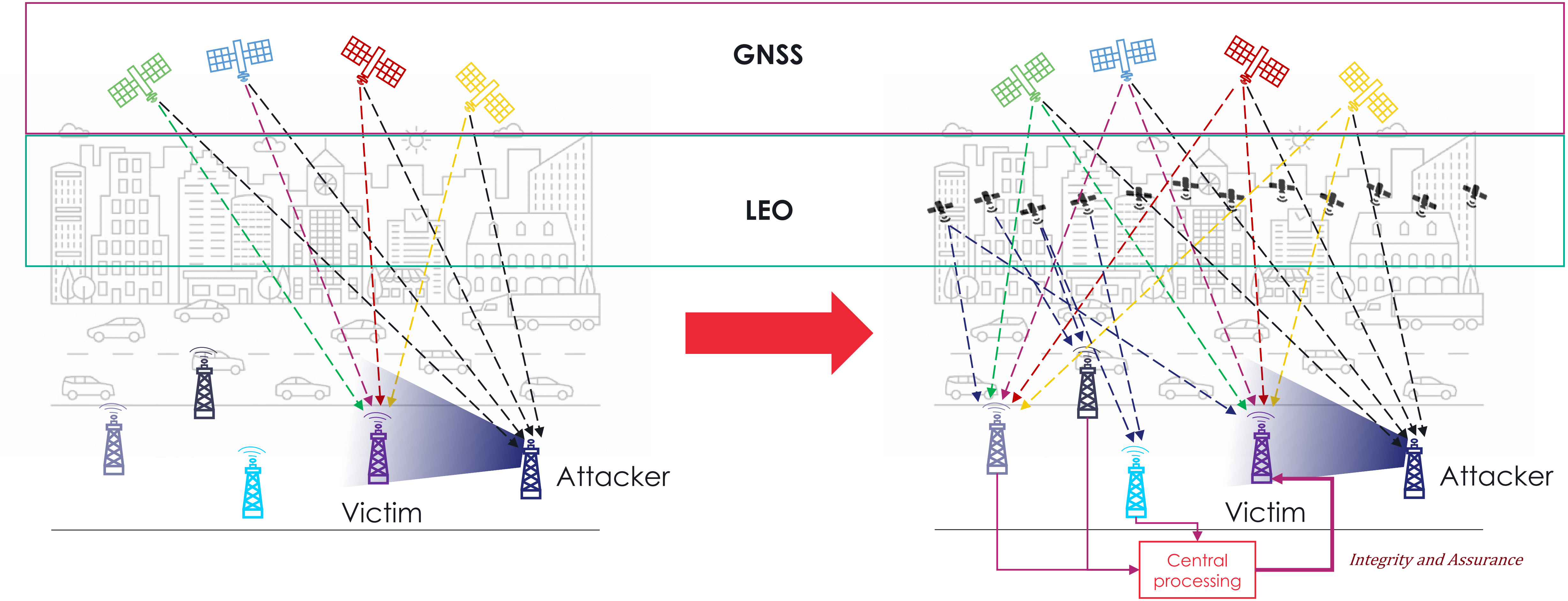
> PNT Assistance :

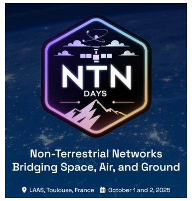


How to be sure about the neutrality of reference station?

Proposed Solution (2/7)

> PNT Assurance :

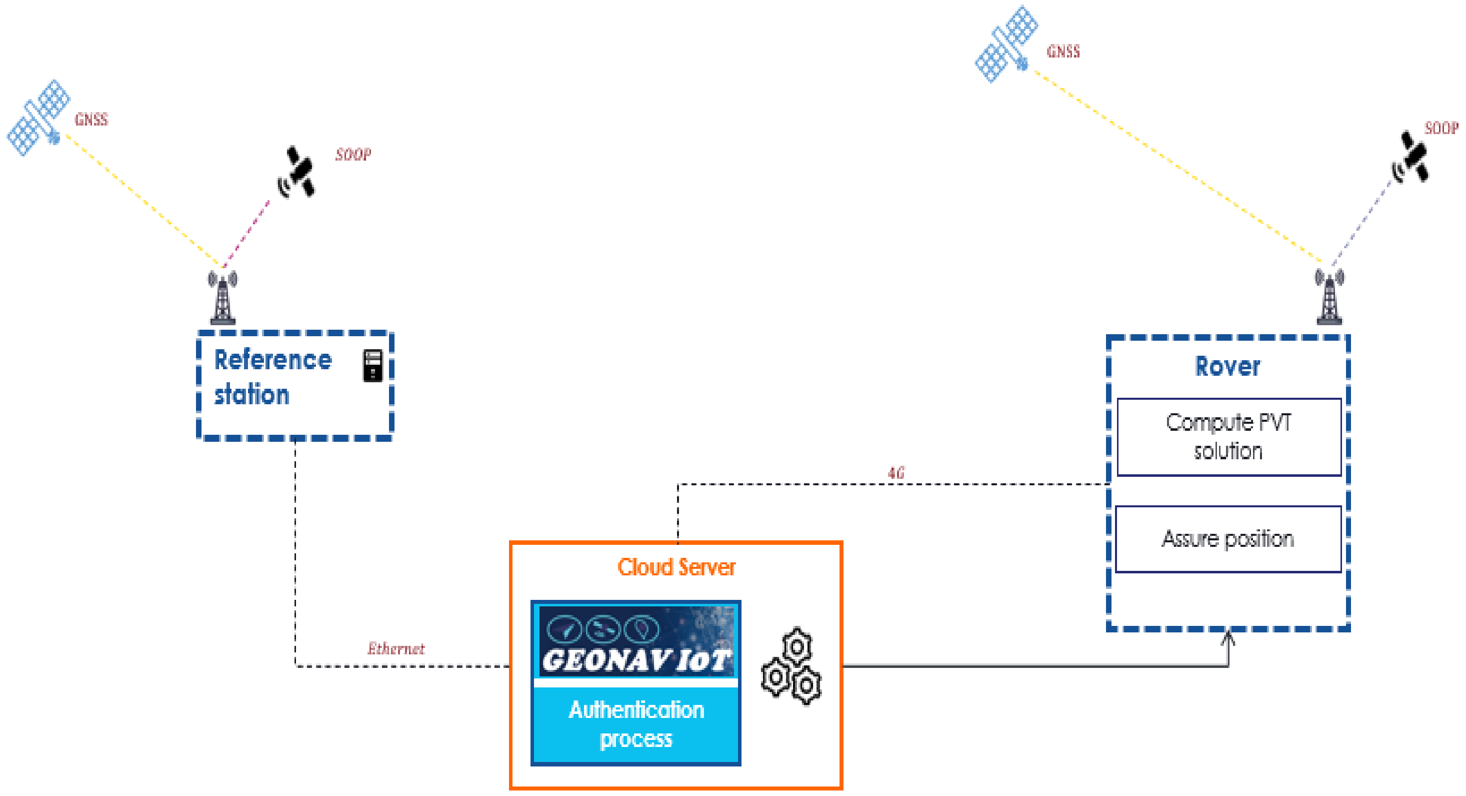




Proposed Solution (3/7)

> PNT Assurance Principles:

- Cloud Process based on GEONAV IoT, allowing real-time Indoor/Outdoor precise tracking at PNT (Position, Navigation, Timing) User level and available worldwide.



GEONAV IoT

Proposed Solution (4/7)

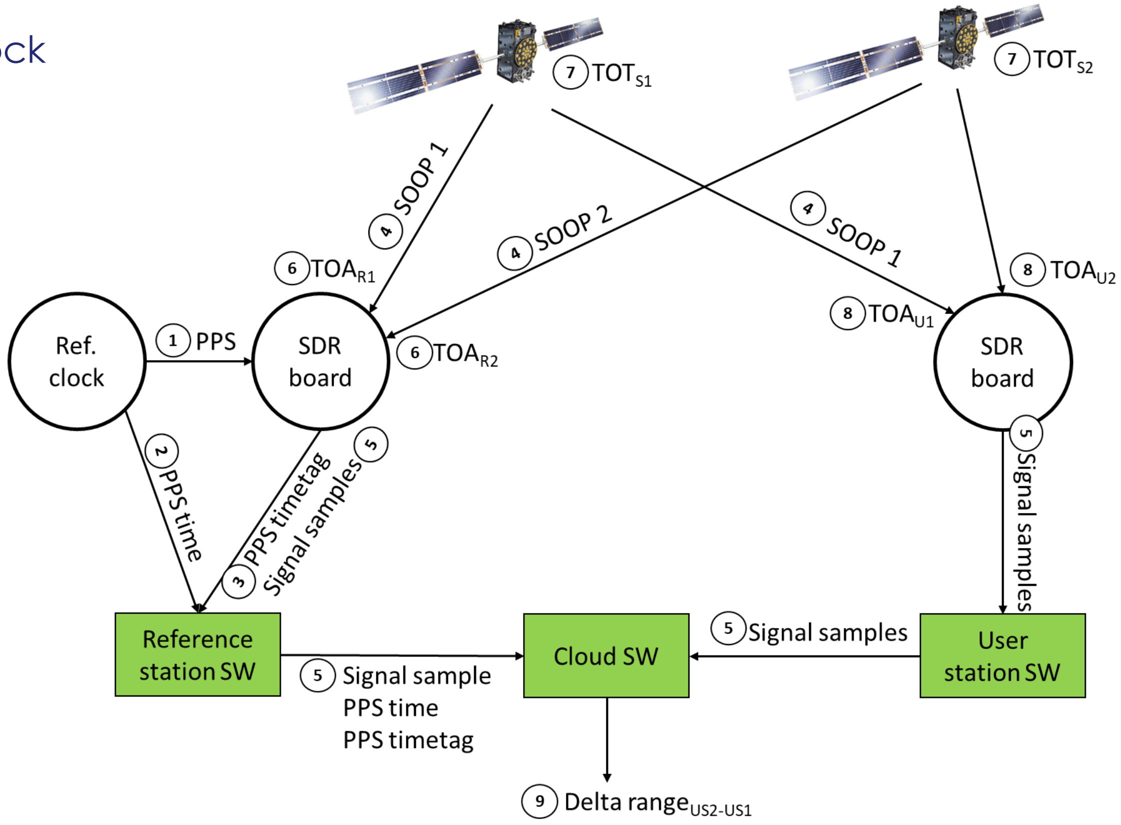
> Investigated Concepts :

1. SOOP Pattern Detection and Datation: Needed for TDOA solution
2. SOOP Tracking: Difficult to use standard GNSS tracking on snapshot system
3. Secure Time Transfer: Best Use-Case with SOOP
4. Combining Reference Signals from Multiple Stations: Essential for GNSS-encrypted processing, to remove other SVs
5. SOOP Measurement Authentication: Ref Stations may use known components, but User Stations should not

Proposed Solution (5/7)

> Position Authentication: Position from SOOP with TDOA Approach

1. SDR is synchronized using the PPS (Pulse Per Second) of reference clock
2. Each PPS corresponds to an exact GNSS reference time
3. SDR's internal clock is aligned with the GNSS PPS
4. SDR records signals of opportunity
5. These signals are uploaded for centralized processing (cloud server)
6. TOA of the signal at the reference station is computed
7. TOT of the signal is deduced
8. TOA of the signal at the rover station is computed
9. Delta range for the SOOP couple sources is calculated



$$\text{Delta range}_{US2\text{-}US1} = \left((TOA_{U2} - TOA_{U1}) - (TOT_{U2} - TOT_{U1})\right) \cdot c$$

Proposed Solution (6/7)

> Position Authentication: Position from SOOP with TDOA Approach

> The Position of a targeted receiver is calculated:

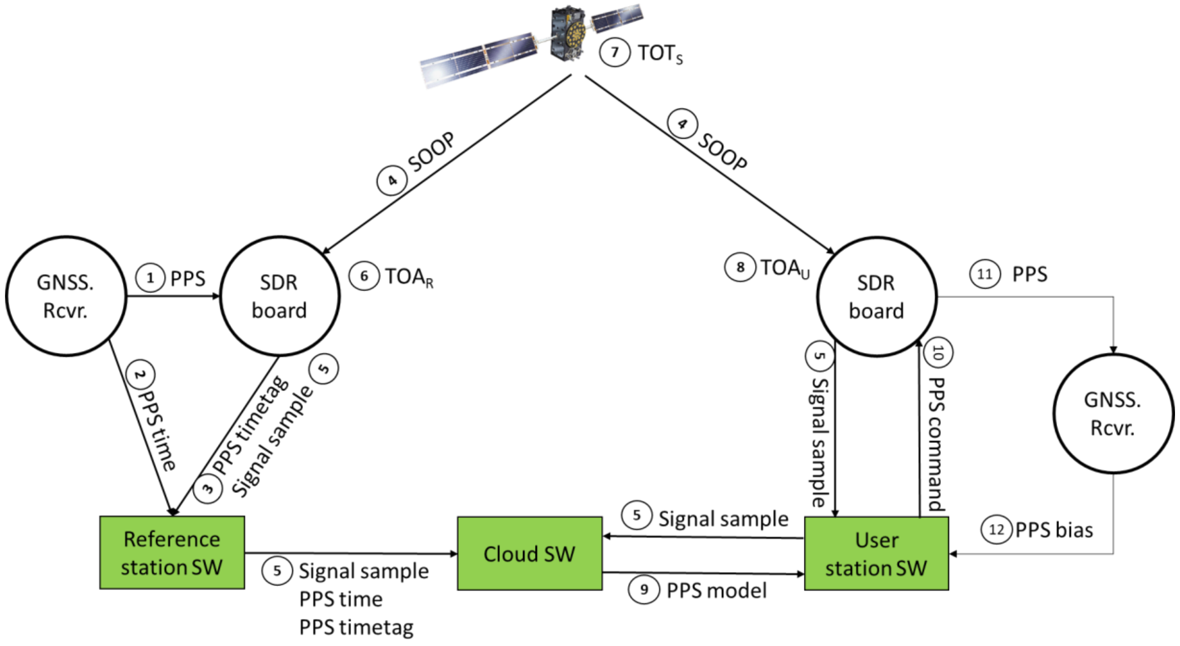
- Requires at least 4 TOA measurements from 4 different sources
- Set the pseudo-range value of the first source to an arbitrary value PR1
- Calculate the pseudo-range of the other sources: PRi = PR1 + (Di – D1)
- Now we can use the PRi as classic pseudorange measurement in a GNSS filter

> The bias between GNSS PVT and SOOP PVT is measured. If the bias is small, then the synchronization is valid and can authenticate the GNSS time.

Proposed Solution (7/7)

> Time Authentication: Common View Time Transfer – TDOA Approach

1. SDR is synchronized using the PPS (Pulse Per Second) of reference clock
2. Each PPS corresponds to an exact GNSS reference time
3. SDR's internal clock is aligned with the GNSS PPS
4. SDR records signals of opportunity
5. These signals are uploaded for centralized processing (cloud server)
6. TOA of the signal at the reference station is computed
7. TOT of the signal is deduced
8. TOA of the signal at the rover station is computed
9. Delta range for the SOOP couple sources is calculated
10. The SDR card is commanded to generate its own PPS (aligned to the GNSS model)
11. This SDR-generated PPS is injected into the GNSS receiver as an external event input
12. The bias between GNSS PPS and SDR PPS is measured.



If the bias is small, then the synchronization is valid and can **authenticate** the GNSS time.

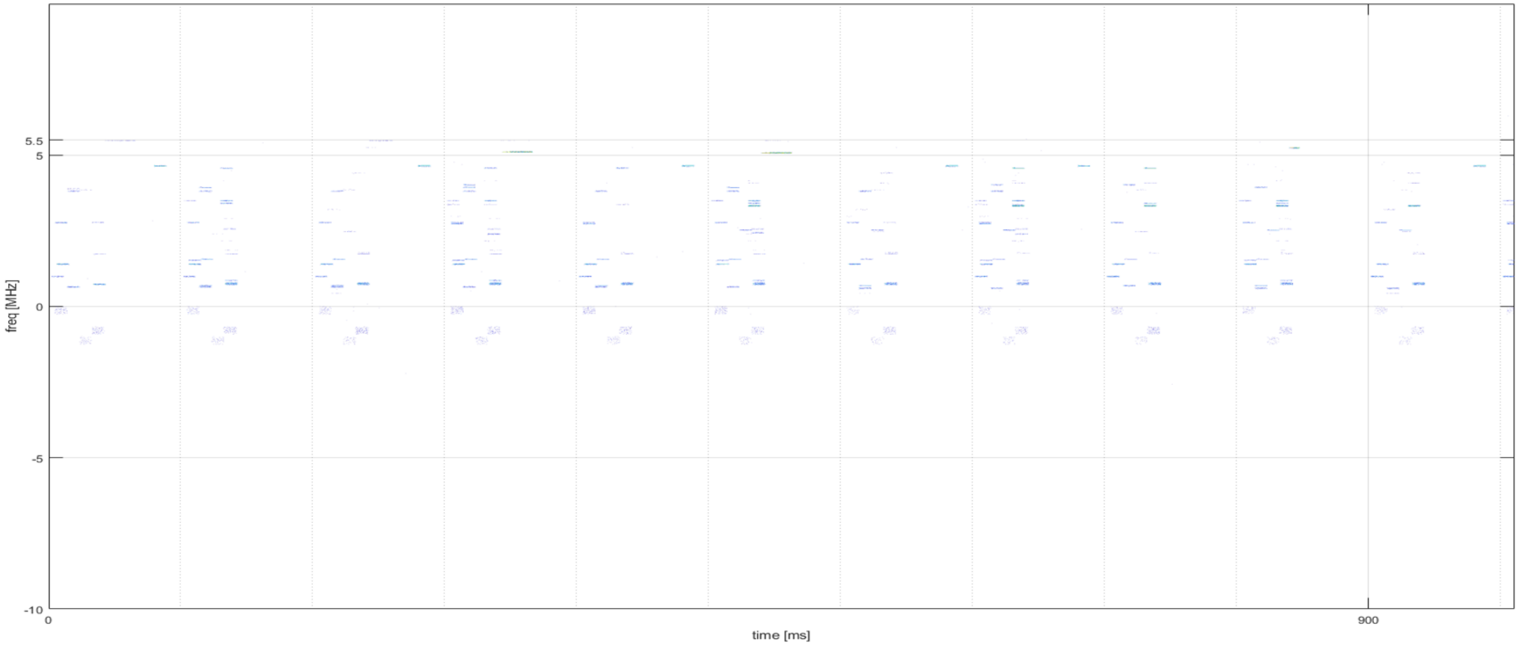
4 – Experimental Results

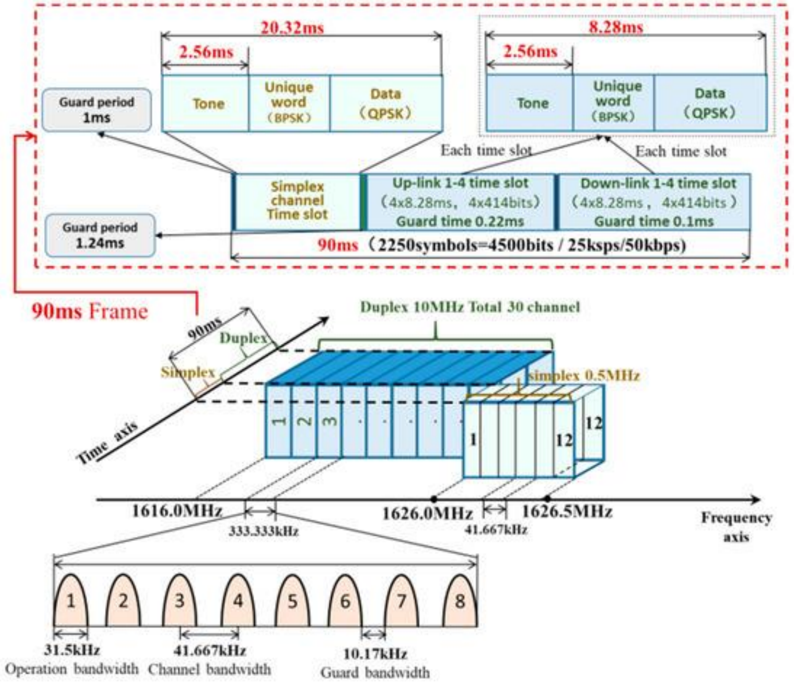
www.thalesgroup.com

Experimental Results (1/6)

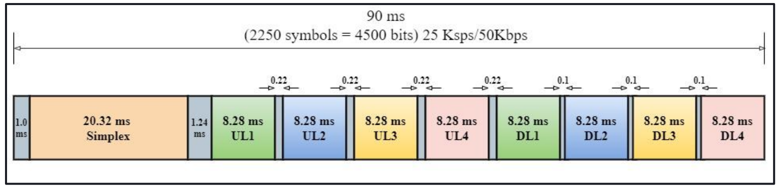
> Iridium Processing

- Signal is in a 10.5 MHz band
- FDMA structure, with ~31.5 kHz per frequency access
- TDMA structure built on 90 ms frame
  - We look for downlink slots D1 – D4, as they are likely to be seen by both User Station and Reference Station
  - Each 8.28 ms timeslot has a mixture of predictable signal (tone, unique word) and unpredictable (data) signal





Positioning Using IRIDIUM Satellite Signals of Opportunity in Weak Signal Environment - Zizhong Tan et al.

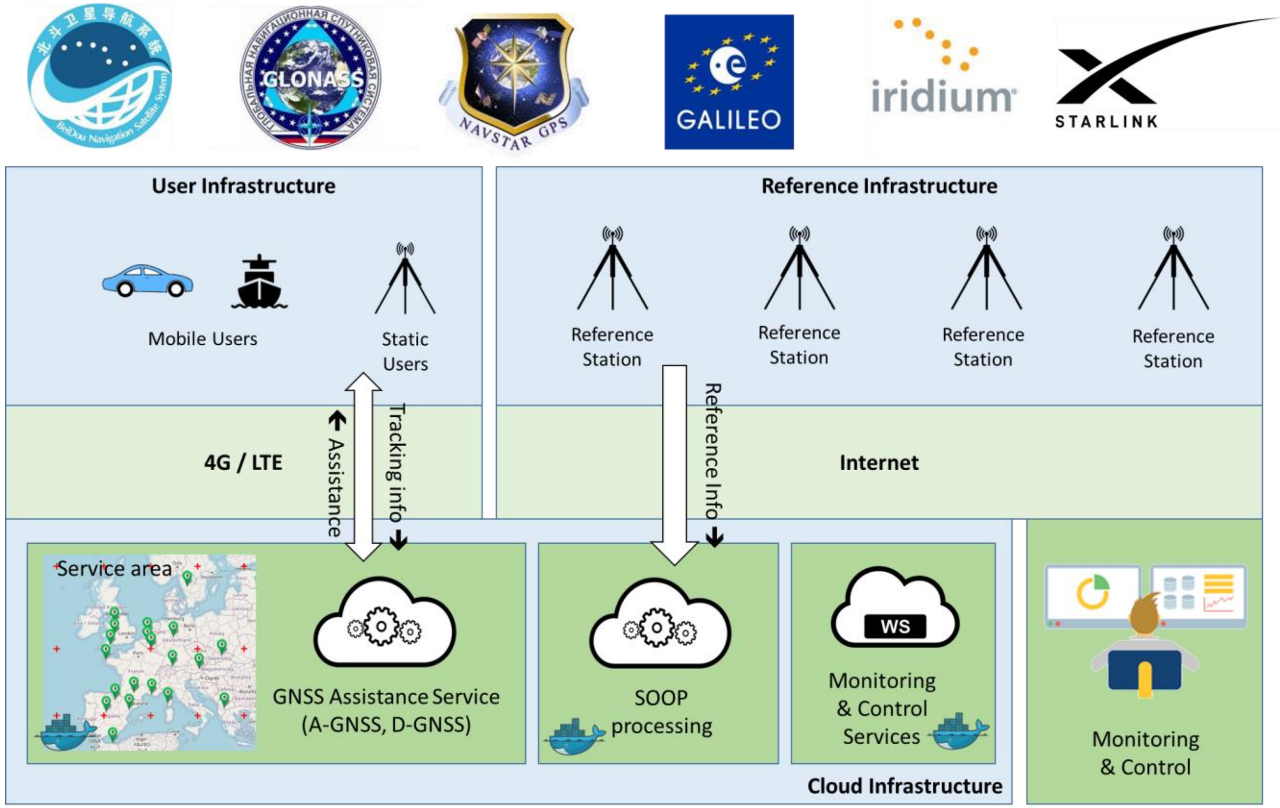


Experimental Results (2/6)

> Demonstrator Testbed: Architecture (GEONAV IoT)

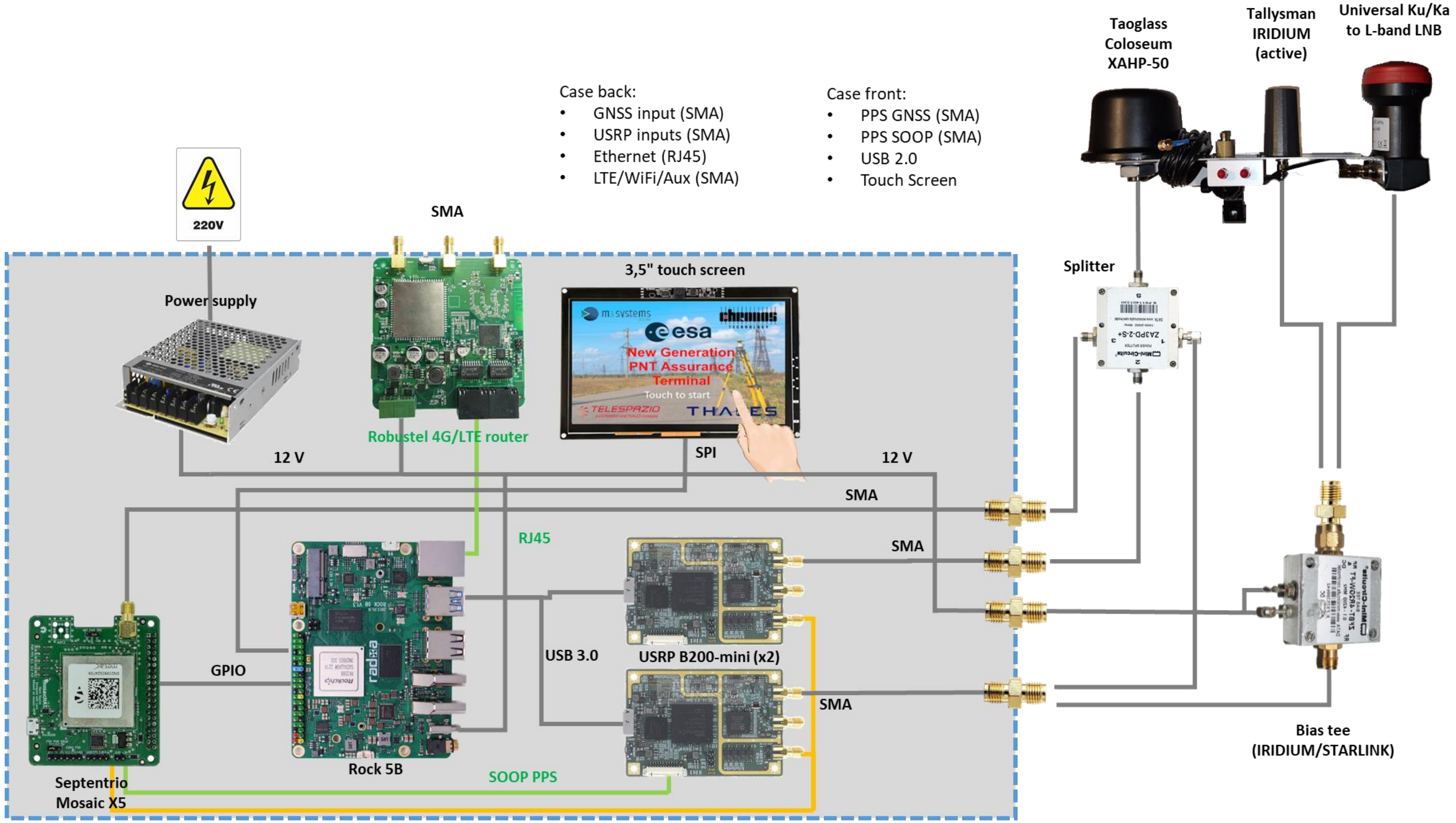
User terminal

Reference station



Experimental Results (3/6)

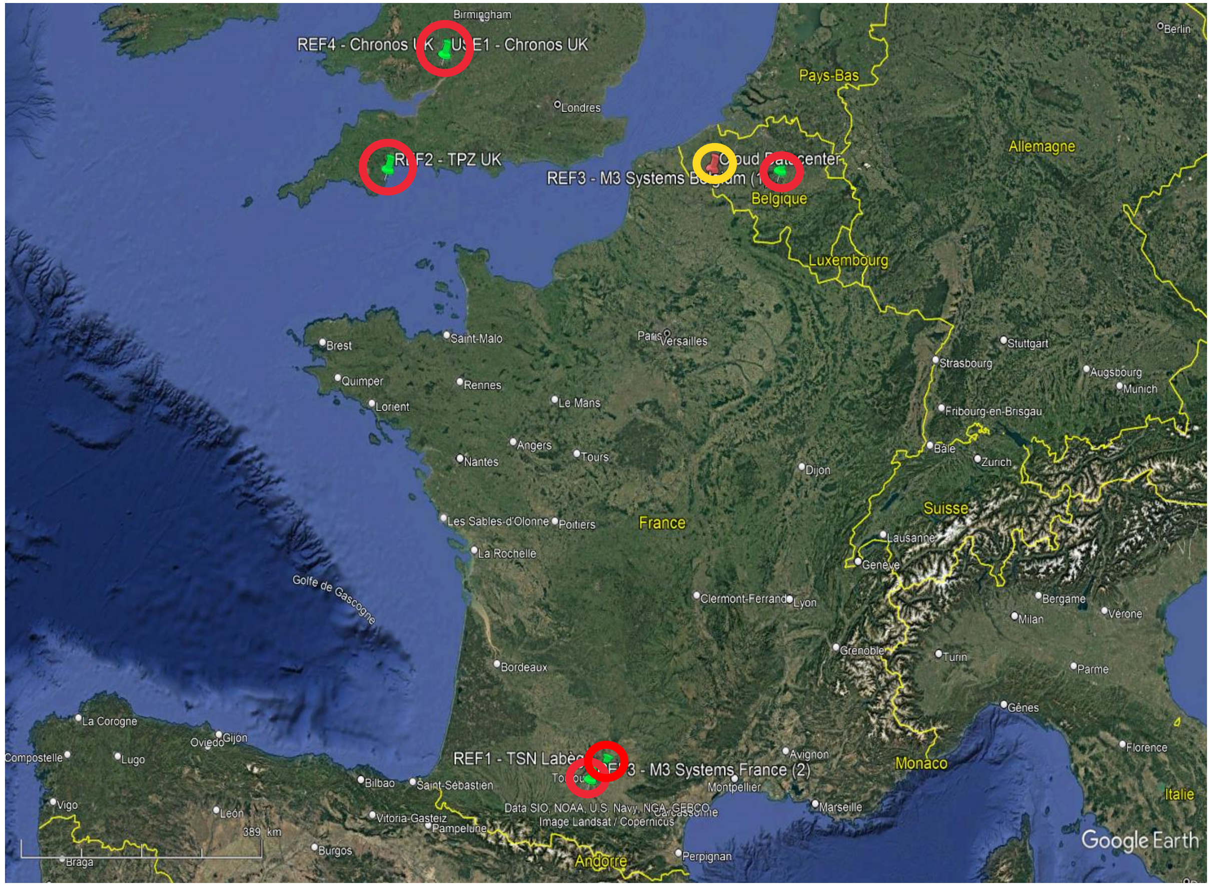
> Demonstrator Testbed: Station Architecture



Experimental Results (4/6)

> Demonstrator Testbed: Deployment

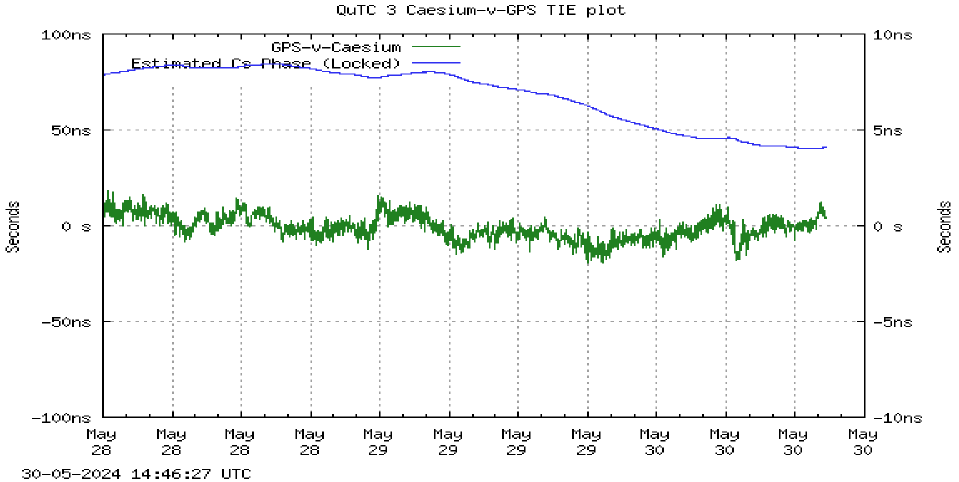
- Four stations:
  - Thales SN
  - TPZ UK
  - Chronos UK
  - M3S France
  - M3S Belgium
- One cloud datacenter

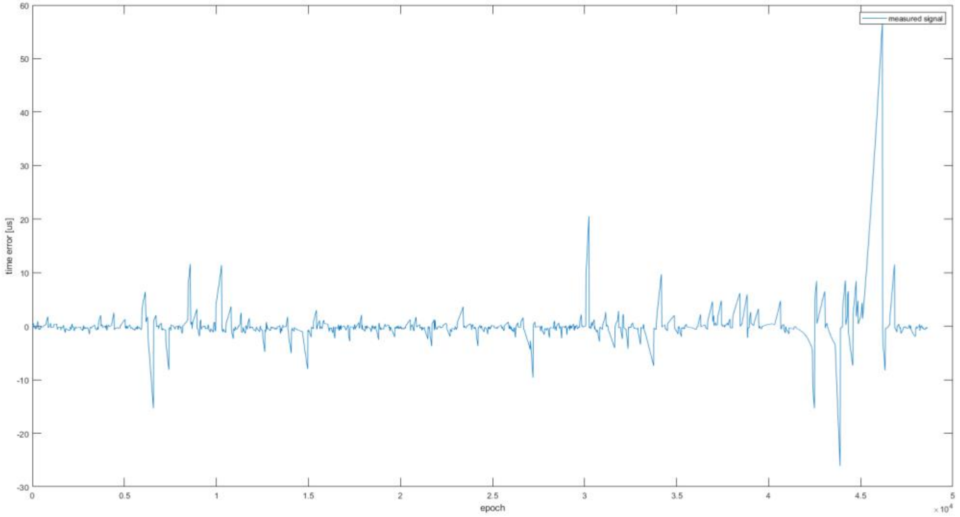


Experimental Results (5/6)

> Performance Results: Timing

- The measurement system is designed to monitor long term clock performance as shown in the example
- Unfortunately, time has not allowed us to resolve all of the signal reception issues and short correlation periods to determine likely performance.
- During a 12-hr run, found that availability of good (high-BW) Iridium was inconsistent
- When signals are unavailable for many epochs, the clock model will be freewheeling and can drift a long way off
- Although the resulting performance may spend a lot of time with low error, there are many spikes

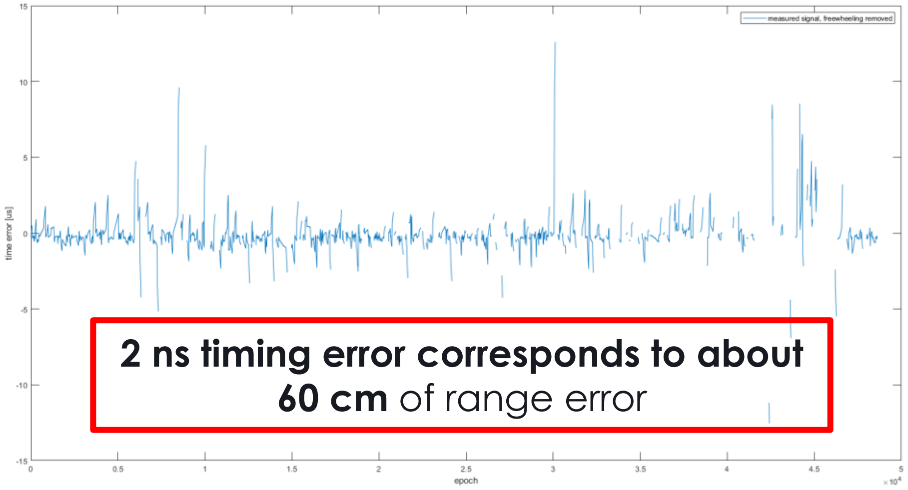


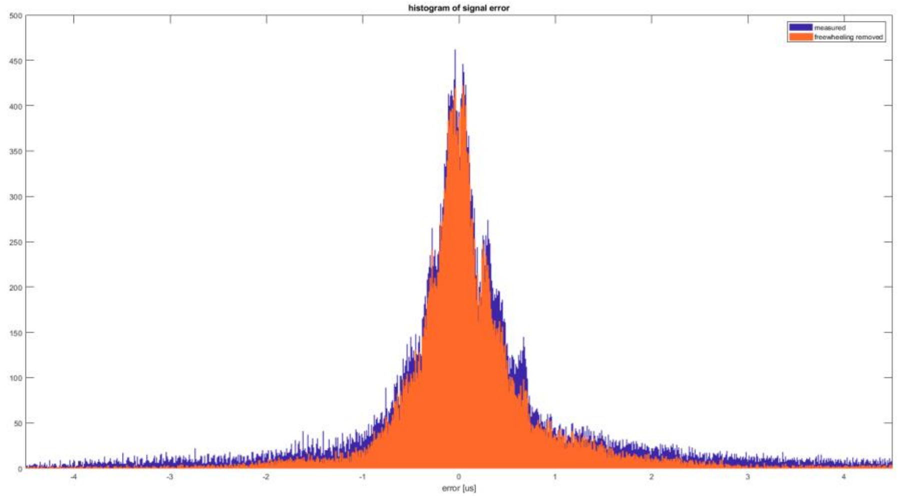


Experimental Results (6/6)

> Performance Results: Timing

- Removing the epochs where the clock was freewheeling, the plot is better, but still does have spikes
- Could be due to the system using a medium-to-low BW signal to get its estimate for that epoch
- Could also be due to selecting the wrong peak in the ACF
- Without freewheeling the system is achieving:
  - < 0.3μs about 50% of the time
  - < 1.35μs 90% of the time
  - < 2μs 95% of the time
- A better internal oscillator would allow the system to be more accurate, by ignoring all but the best epochs, but a new clock model would be needed as well.





THALES
Building a future we can all trust

Thanks

Any questions?

Roberto MATERA

GNSS Expert Engineer

eustachio-roberto.matera@thalesgroup.com

Olivier LAGRANGE

Program Manager

+33 (0)7 64 70 77 84

olivier.lagrange@thalesgroup.com