NAVISP-EL1-040
Next Generation Network-Assisted PNT Assurance (NG-NAPA)

Final Presentation

Virtual

10 September 2025

Next Generation Network-Assisted PNT Assurance (NG-NAPA)

Final Presentation

1. **Welcome!**

2. Programme of Work
3. Project Context
4. Project Outcomes
   - Concept Consolidation
   - Architecture Definition
   - System Design
   - Demonstrator testbed
   - Performance results
5. Conclusions and Way Ahead
   - Benefit of the proposed architecture
   - Possible Further Work
   - Potential Way Forward

6. **Q & A**

Project Context and Programme of Work

Louise Mercy (Telespazio UK)

Next Generation Network-Assisted PNT Assurance (NG-NAPA)

Led by **Telespazio UK**, working with **Thales Services Numériques**, **M3 Systems** and **Chronos Technology**

Investigating potential system architectures for providing an end-to-end network-assisted Positioning, Navigation, and Timing (PNT) assurance service

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 and dynamic use cases, **benchmarking the performance** of the developed GNSS plus SOOP hybrid positioning techniques using reference network assistance system

Concept Consolidation

* State of the Art review, ConOps and REQs consolidation
* Preliminary Design of concepts
* Trade-off analysis

Detailed Design

* Func/System design
* Security evaluation
* Performance test planning

Implementation

* Implementation and validation of demonstration testbed
* Security review

Demonstration

* Real world performance demo
* Concept results consolidation

Way forward Planning

* Review outcomes and lessons learned
* Gap analysis and next steps proposals

Specification of the **functional and performance REQs for the System Concept, ConOps and use cases** serving as a baseline

Detailed design and justification of the **architecture and functions** of the NG-NAPA concept

Developed, assembled and integrated **SW and HW** for the demo NG-NAPA system

Comprehensive reporting and analysis of a series of **real world performance assessments**

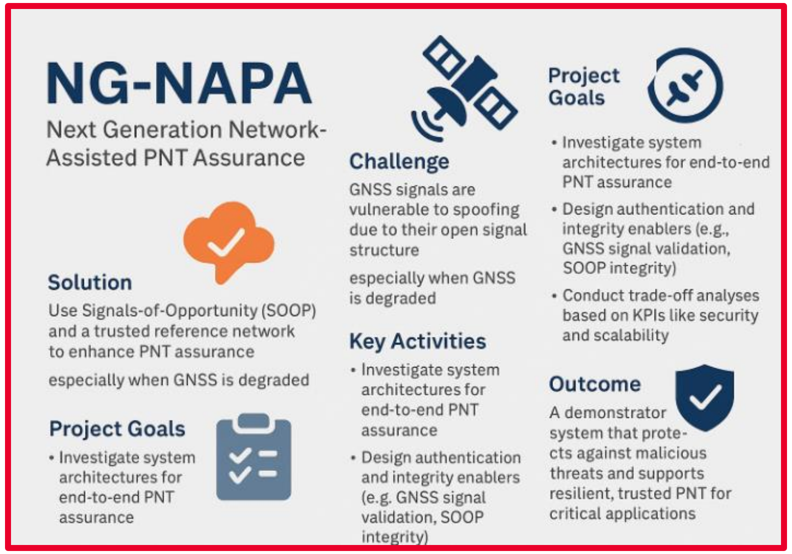
Conclusions on the **achievements of the NG-NAPA** project and recommendations for **future studies**

Project Context

Martin Bransby (Telespazio UK)

Why?

- **GNSS Vulnerability**
  - GNSS signals, such as GPS, are susceptible to spoofing and jamming, which can be done with relatively low-cost equipment. This poses a serious risk to critical infrastructure, transport, and industrial operations that rely on accurate positioning.
  - This threat is now almost omnipresent in some regions of the World such as the Baltic Sea and the Red Sea and eastern Mediterranean, as well as for aviation routes
- **PNT Assurance**
  - NG-NAPA aims to provide assured PNT by combining GNSS with Signals of Opportunity (SOOP) —such as 5G, LTE, and Iridium 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.

Project Outcomes

Tim Whitworth (Telespazio UK)
Didier Lapeyre (Thales Services Numériques)
Aravind Ramesh (M3 Systems)
Tony Flavin (Chronos Technology)

Concept Consolidation

Concepts to be investigated:

1. SOOP Pattern Detection and Datation
2. SOOP Tracking
3. Secure Time Transfer
4. Combining Reference Signals from Multiple Stations
5. SOOP Measurement Authentication
6. Mechanisms to Reduce the OD Error for Satellites
7. GNSS / SOOP Hybridisation Techniques
8. Network Architecture to Reduce Latencies

Concept Consolidation

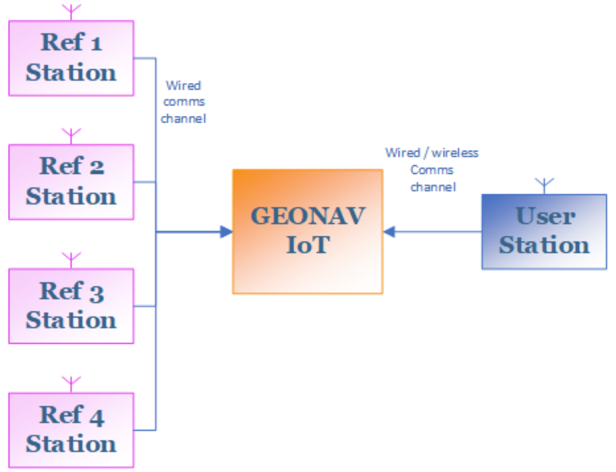
Concepts to be investigated:

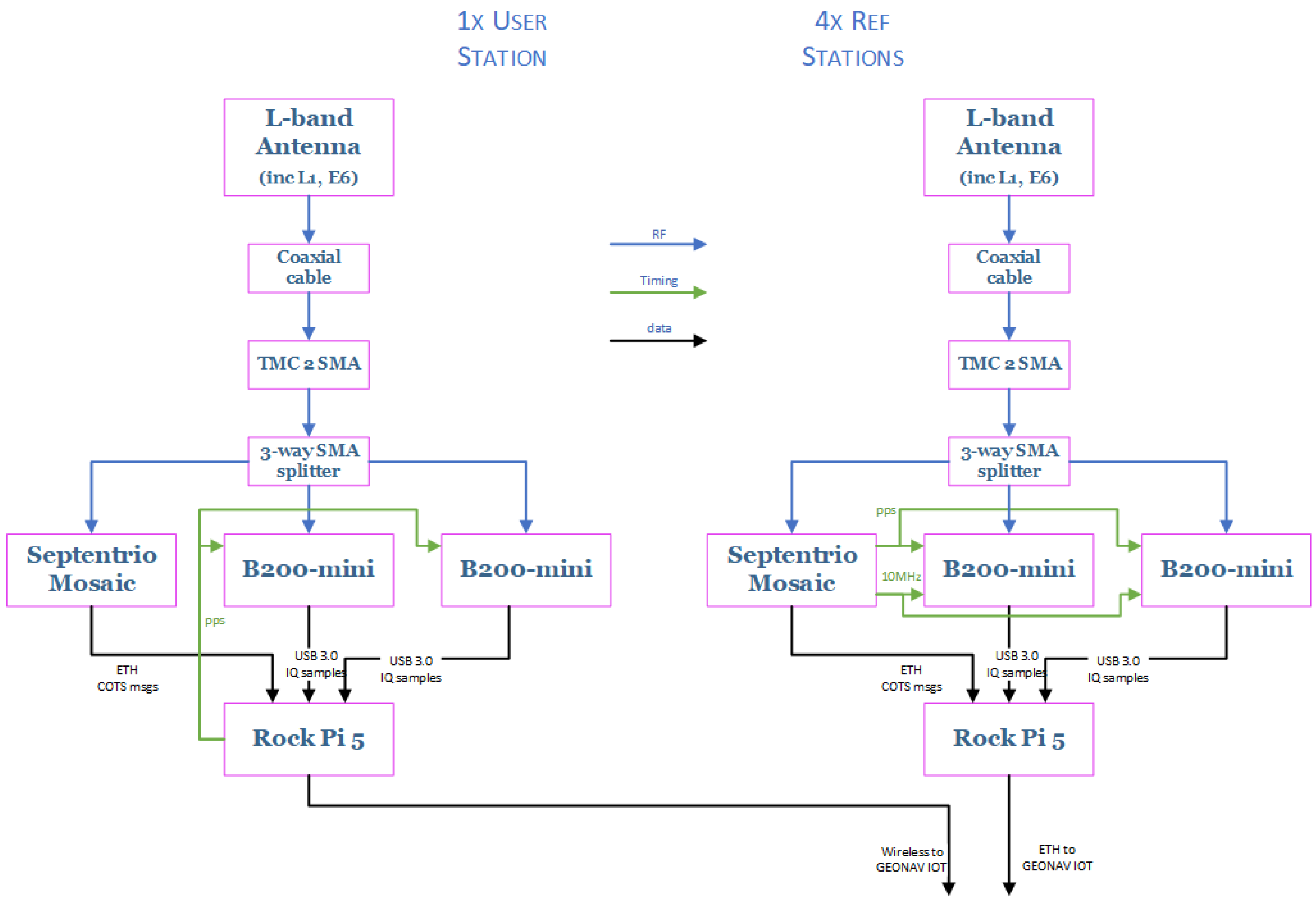
1.	SOOP Pattern Detection and Datation	-	Needed for TDoA solution
2.	SOOP Tracking	-	Difficult to use standard GNSS tracking on snapshot system
3.	Secure Time Transfer	-	A good Use-Case for SOOP
4.	Combining Reference Signals from Multiple Stations	-	Essential for GNSS-encrypted processing, to remove other SVs
5.	SOOP Measurement Authentication	-	Ref Stations may use known components, but User Stations should not
6.	Mechanisms to Reduce the OD Error for Satellites	-	Reference network density analysis, but difficult for demonstrator
7.	GNSS / SOOP Hybridisation Techniques	-	Not such a good Use Case, since PNT-assurance must work SOOP-only
8.	Network Architecture to Reduce Latencies	-	Techniques analysed, but not easy to demonstrate without redesign

Demonstrator System Architecture

Positioning Use Case

- Stations grabbing samples
- Passing snapshots to cloud for SOOP processing
- Positioning and Timing Use Cases





System Design

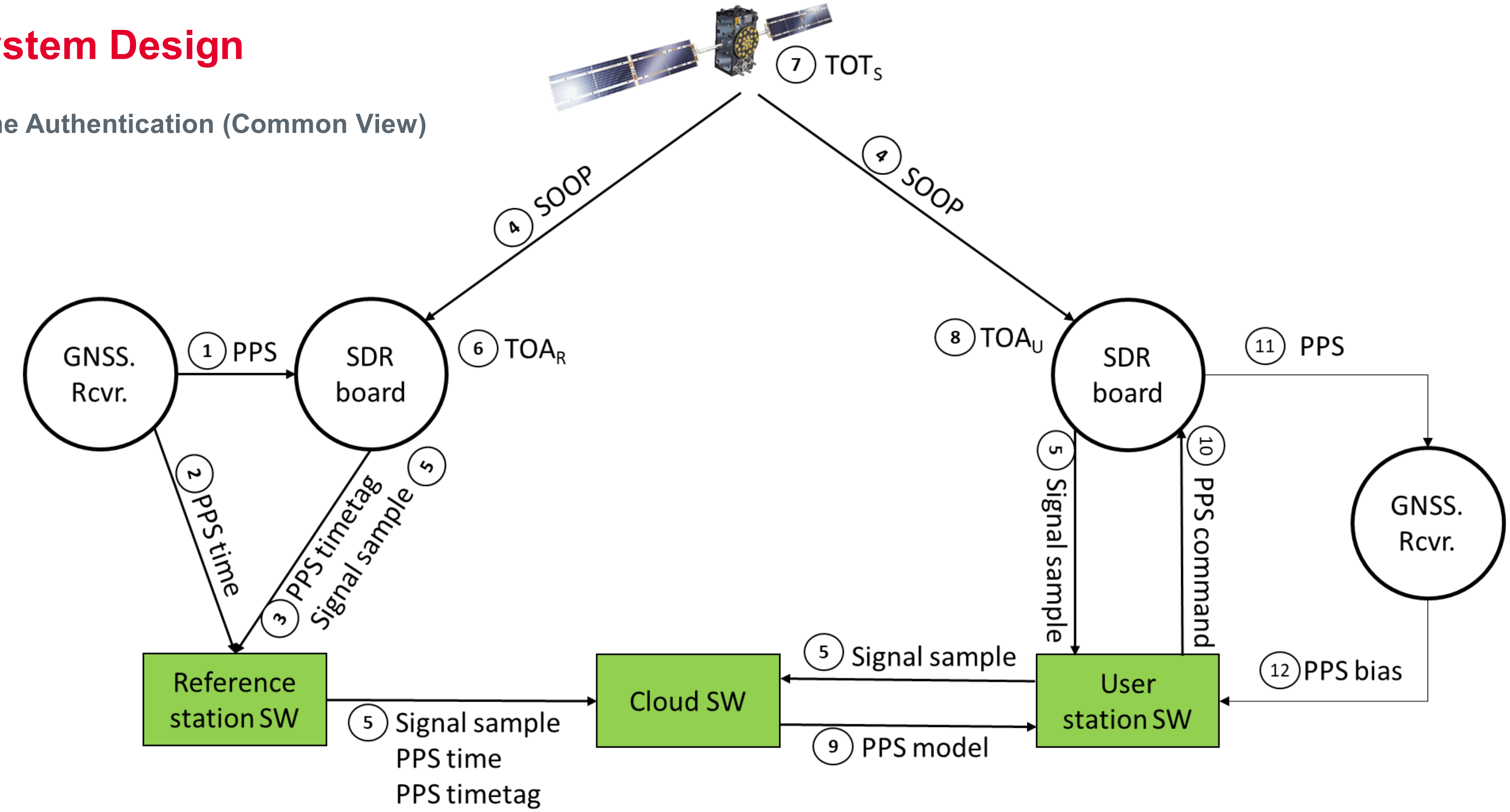
Main Functions and Techniques

- GNSS time authentication function
  - Based on “common view” technique (similar to single difference)
- GNSS position authentication function
  - Based on TDOA technique (similar to double difference)
- SOOP based positioning function
  - Based on TDOA technique (similar to double difference)

- All methods based on the SOOP Time Of Arrival (TOA) measurements

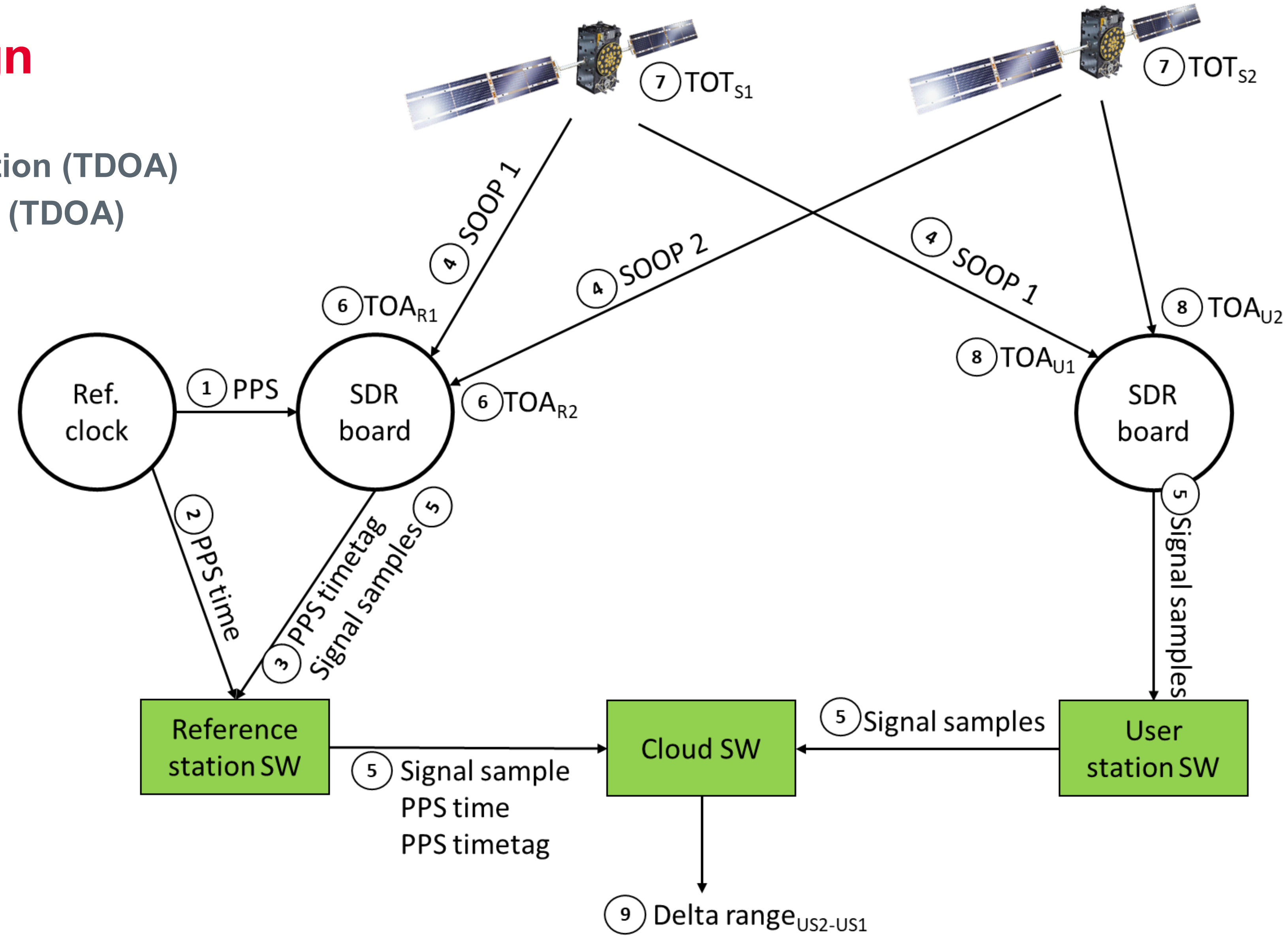
System Design

Time Authentication (Common View)



System Design

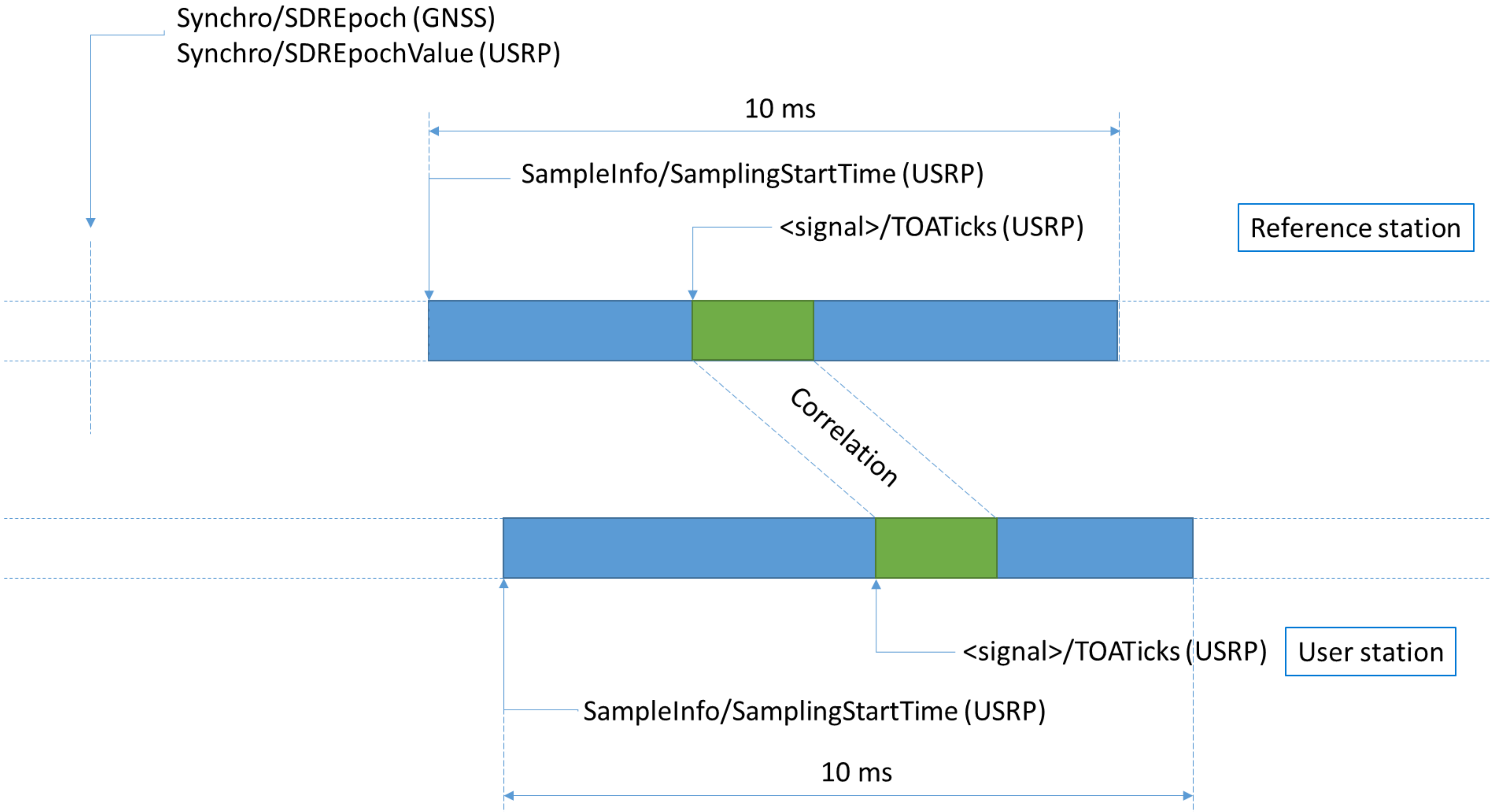
Position Authentication (TDOA)
Position from SOOP (TDOA)



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

System Design

Signal Correlation Technique



System Design

Design Challenges and Limitations (1)

- Identification of the signal source
  - Necessary when working with multiple similar sources like satellites
  - Complex when using unknown signals
  - GNSS encrypted signals :
    - Galileo E6B & E6C are currently not encrypted and have the same signal characteristics resulting in ambiguous PVT estimation.
    - Galileo E6 signals are vulnerable to strong interference from long range air surveillance radar systems.
  - IRIDIUM :
    - Compute expected Doppler shift for all satellites in view and compare to Doppler shift found in signal
    - Good approach as a low number of satellites are visible at the same time
    - Issues found on USRP with high clock drift
  - STARLINK :
    - Doppler shift method does not work as hundreds of satellites are visible at the same time
    - No SIS ICD available so it is not possible to identify the transmitting satellites

System Design

Design Challenges and Limitations (2)

- Computation of the source position at transmission time
  - Based on TLE almanacs + orbit propagator (IRIDIUM, STARLINK)
  - Based on GEONAV A-GNSS information (GPS, GALILEO)
  - Iterative processing from TOA at reference station
  - Allows the computation of the TOT in the same processing loop

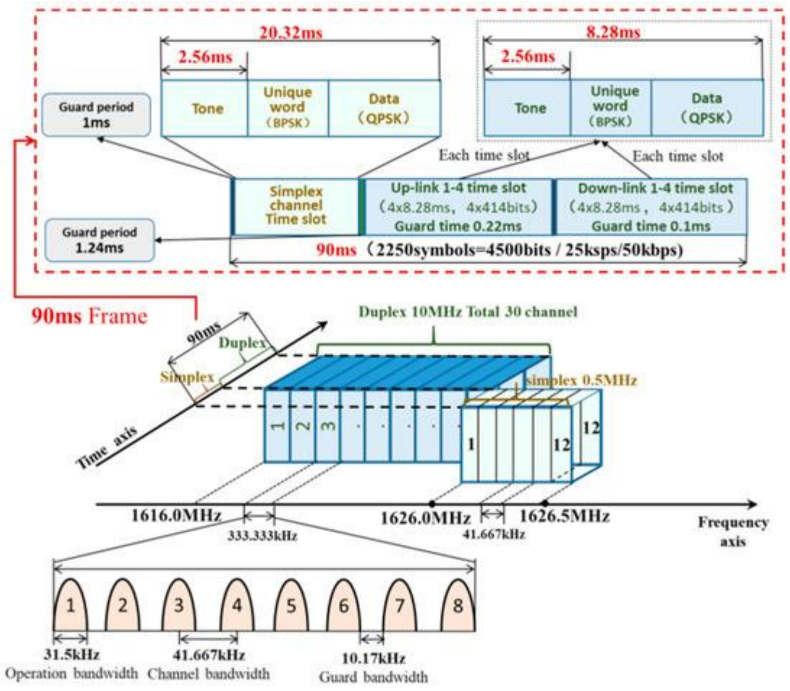
- Synchronisation of the signal acquisition across all reference and user stations
  - Easy at reference station level as USRP is synchronised through the GNSS PPS
  - Needs accurate NTP synchronisation at user station level

- Large amount of data uploaded to the cloud
  - Important processing cycle duration due to low bandwidth on user stations when connected through a wireless network
  - Short signal snapshots => needs accurate synchronisation

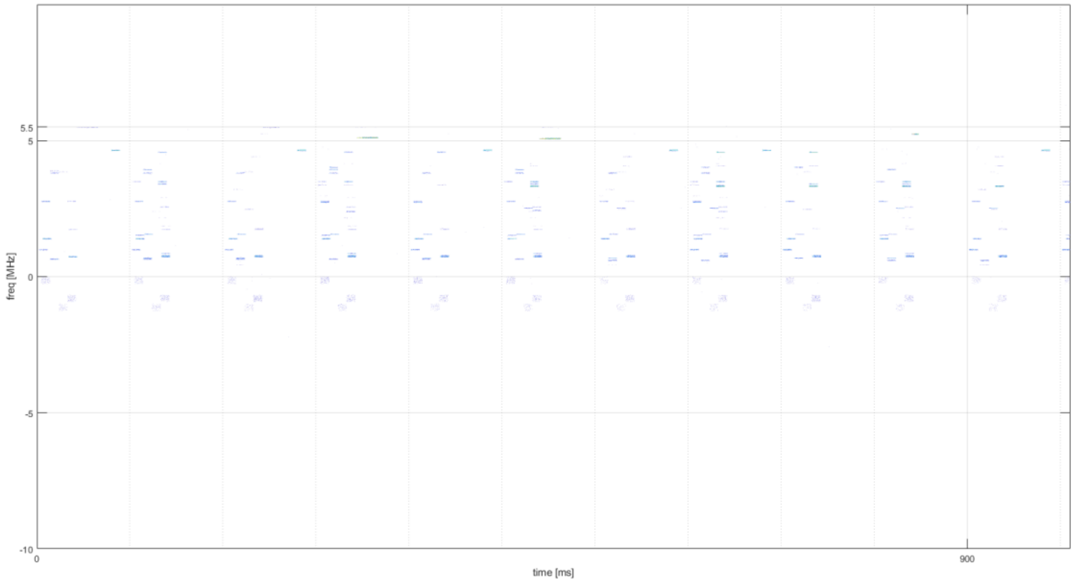
System Design

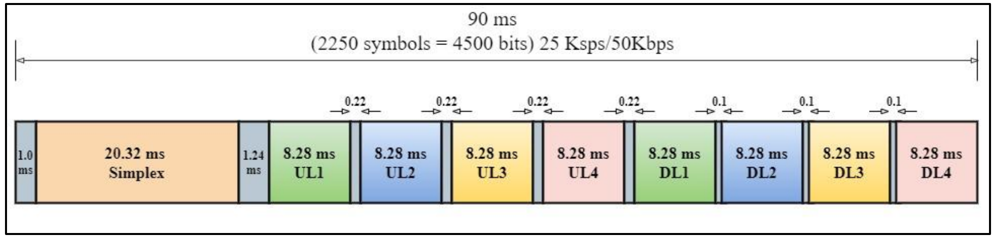
Iridium Processing

- 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

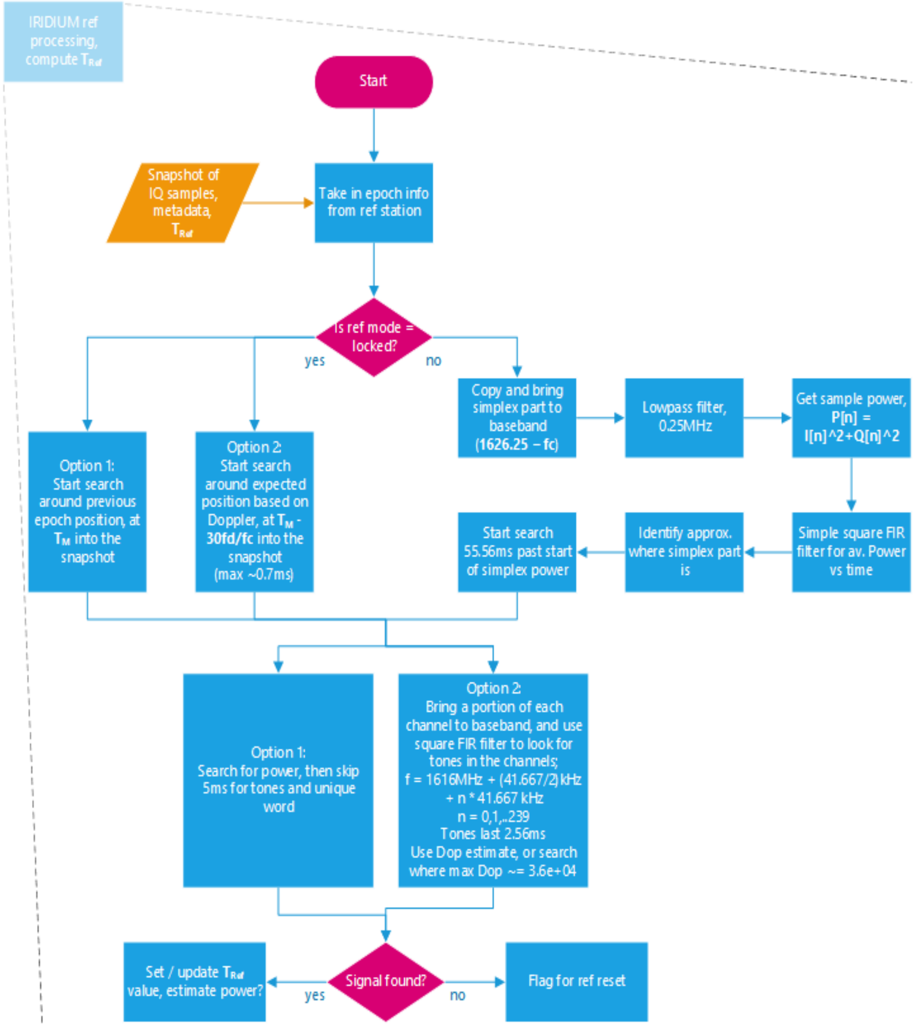




System Design

Iridium Processing

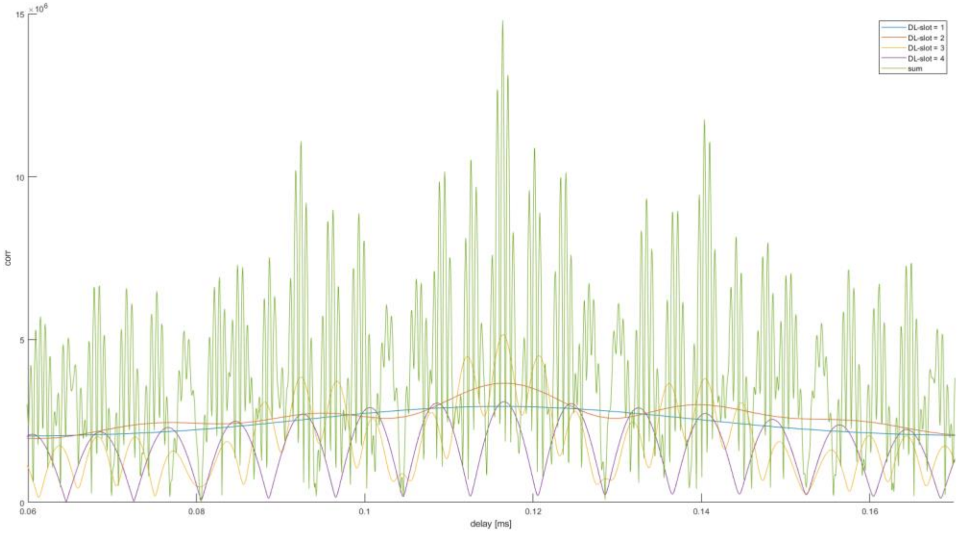
- Initial plan for Reference Station Acquisition:
  - Do an initial sync based on the simplex data slot, as it is in a different band.
  - Look for the frequency bands in use in the DL slots
  - Identify which SV sent them (The number of possible SVs in view is low, and for this static case we know the list of potential Doppler values.)
  - Use the SOOP portion of the signal for correlation against the User capture
- Issues:
  - Would require larger capture sizes than was desirable for the system.
  - Potentially many SVs in view, with comparable CN0 levels, especially because some SVs are sending in more frequency bands.
  - The time (/path) difference between different SVs is enough that removing predictable sequences based on time-only is insufficient.
- Solutions:
  - Take a shorter capture based on where the DL slots will be.
  - Find all the slots in use throughout DL1 – DL4.
  - Assign each to a single SV (at most) based on best Doppler match by looking at the QPSK constellation.
  - For each SV in view, in the freq-domain remove the other bands
  - Then in the time-domain remove the empty slots and the predictable components.

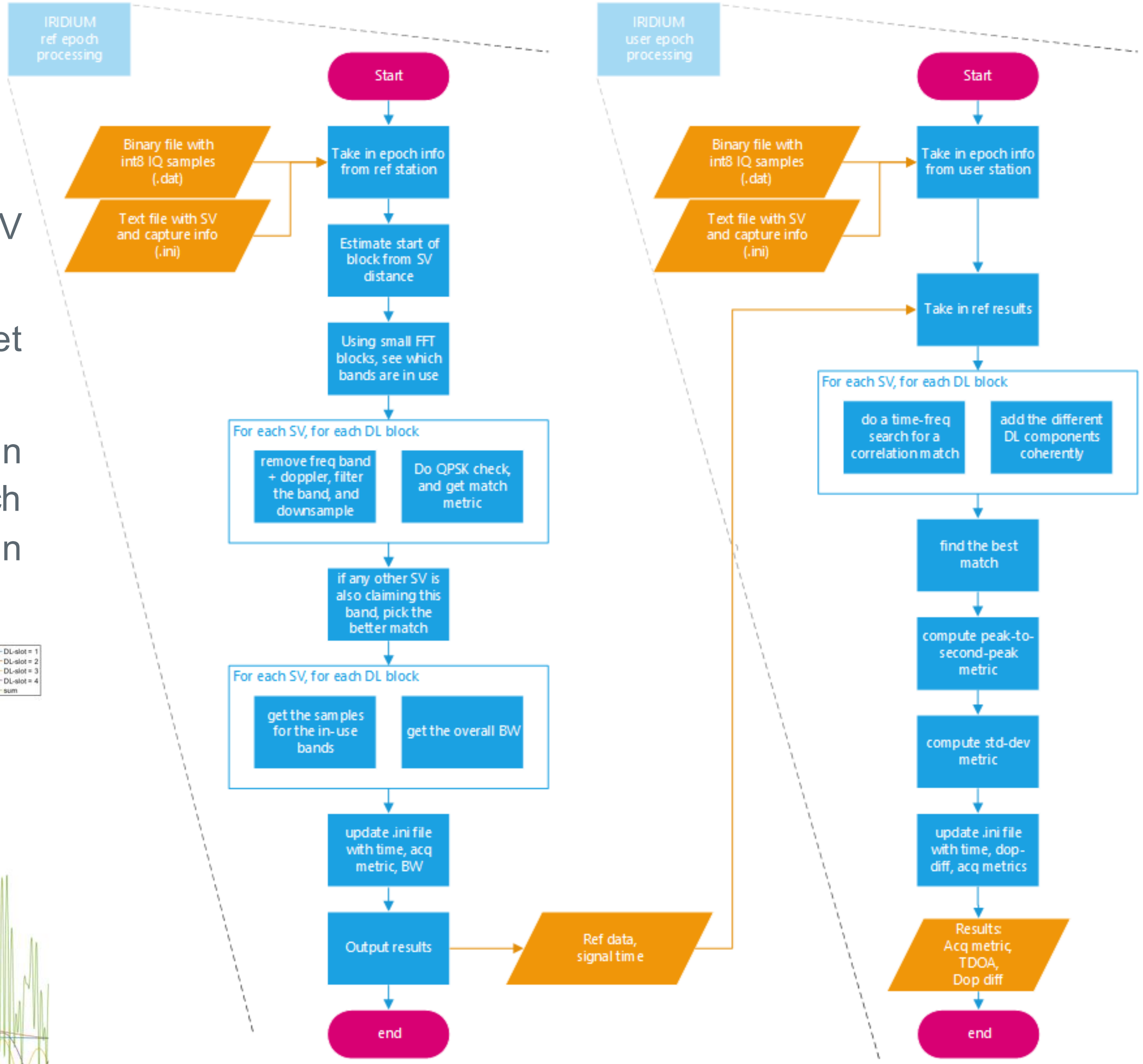


System Design

Iridium Processing

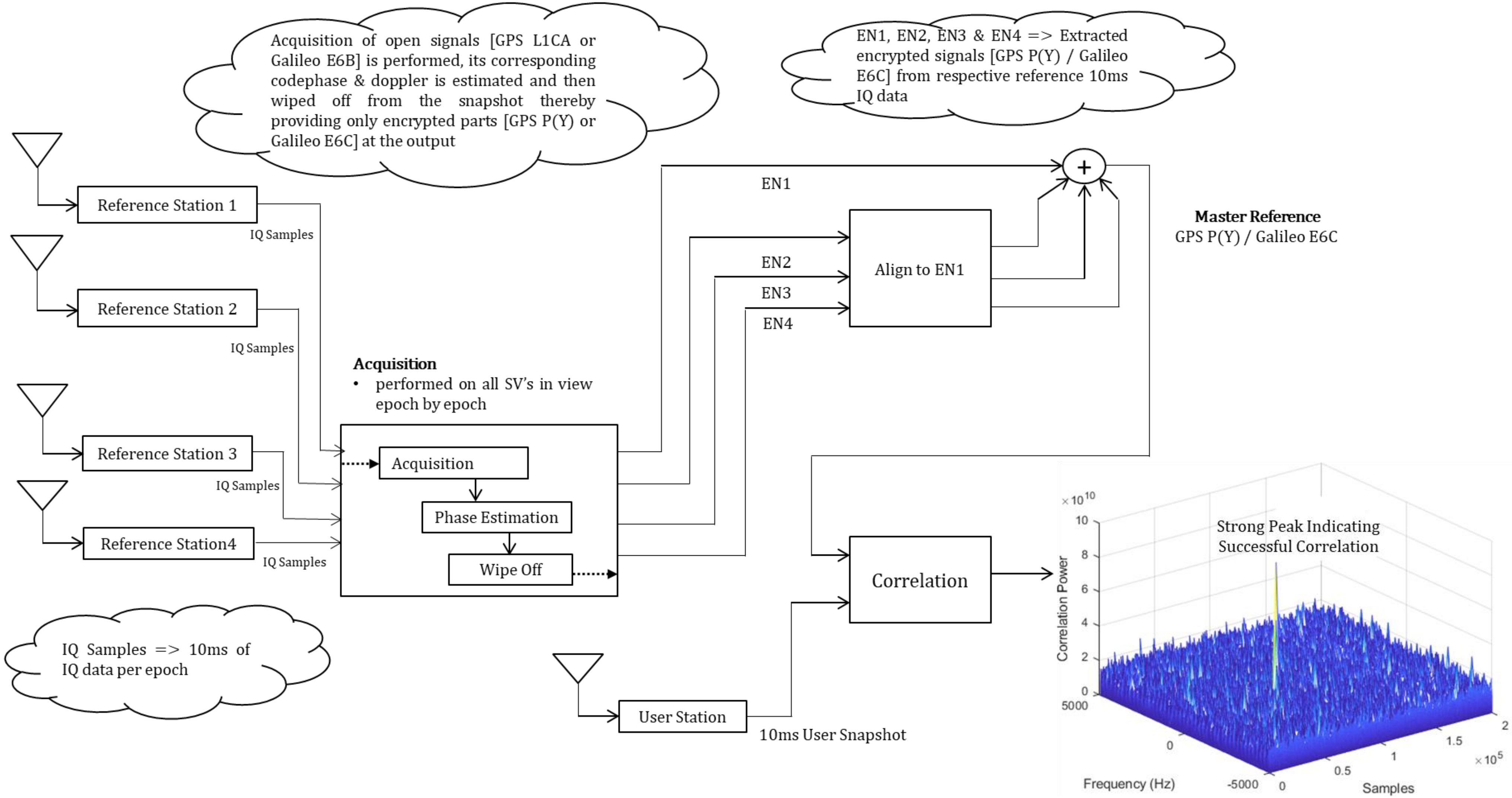
- Final algorithm for Iridium processing.
- Ref outputs a set of data files, containing samples for each SV for each DL slot, along with metadata.
- User does correlation on each, and can add coherently to get the sharpest peak possible.
- Because of sparse frequency usage in some snapshots, can end up with lots of oscillation / periodicity in the ACF, which can add ambiguity in the acquisition, and will worsen performance





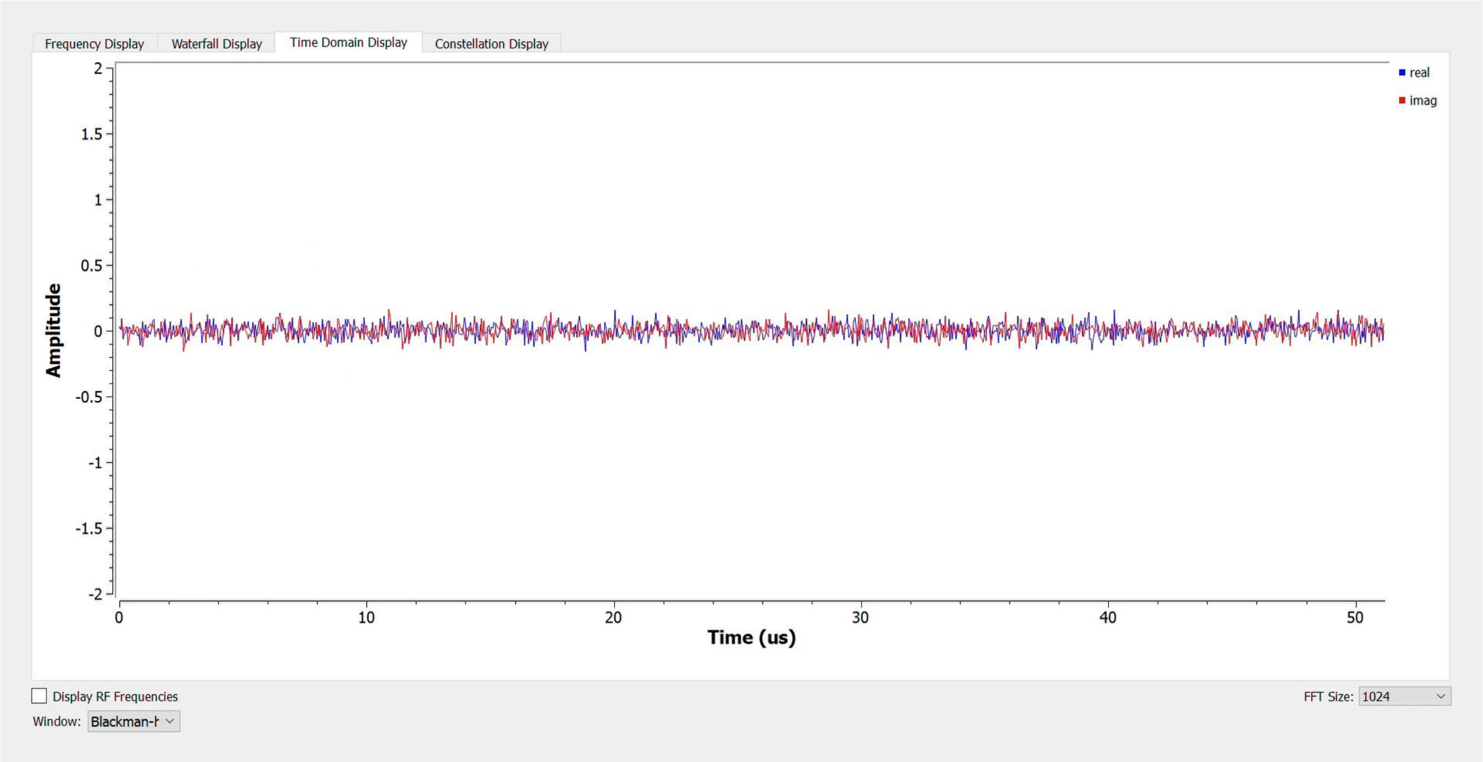
System Design

GNSS Encrypted Processing



System Design

GNSS Encrypted Processing - Interference on E6 Band



- E6 Band: 1260MHz to 1300MHz centered at 1278.75 MHz
- Long-range Air Route Surveillance Radar (ARSR) operates in this range
- They are very high-powered signals
- Can easily overwhelm E6 band
- Video shows the effect of such signals on one of our reference stations initially located in Wavre, Belgium
- Later was moved to Lavernose, France

Name	Freq (MHz)	Peak Power (kw)	Ant. Gain (dBi)	Az Beamwidth (deg)	Scan Rate (rpm)	Pulse Width (μs)
ARSR-3	1250-1350	5000	34	1.25	5	2
ARSR-4	1215-1400	60	35	1.4	5	90+60

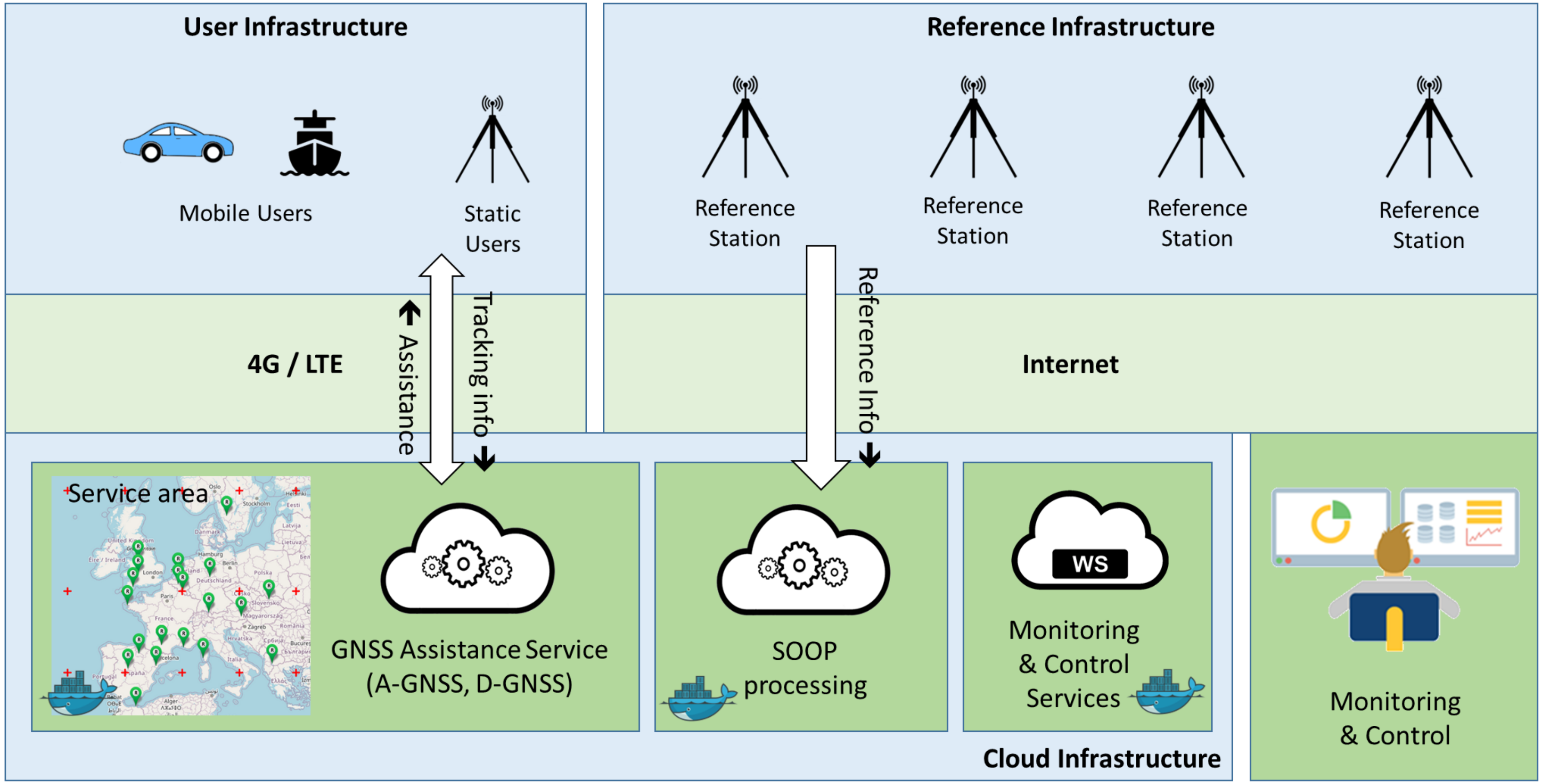
Demonstrator Testbed

Demonstrator Architecture (GEONAV IoT reuse)

User terminal

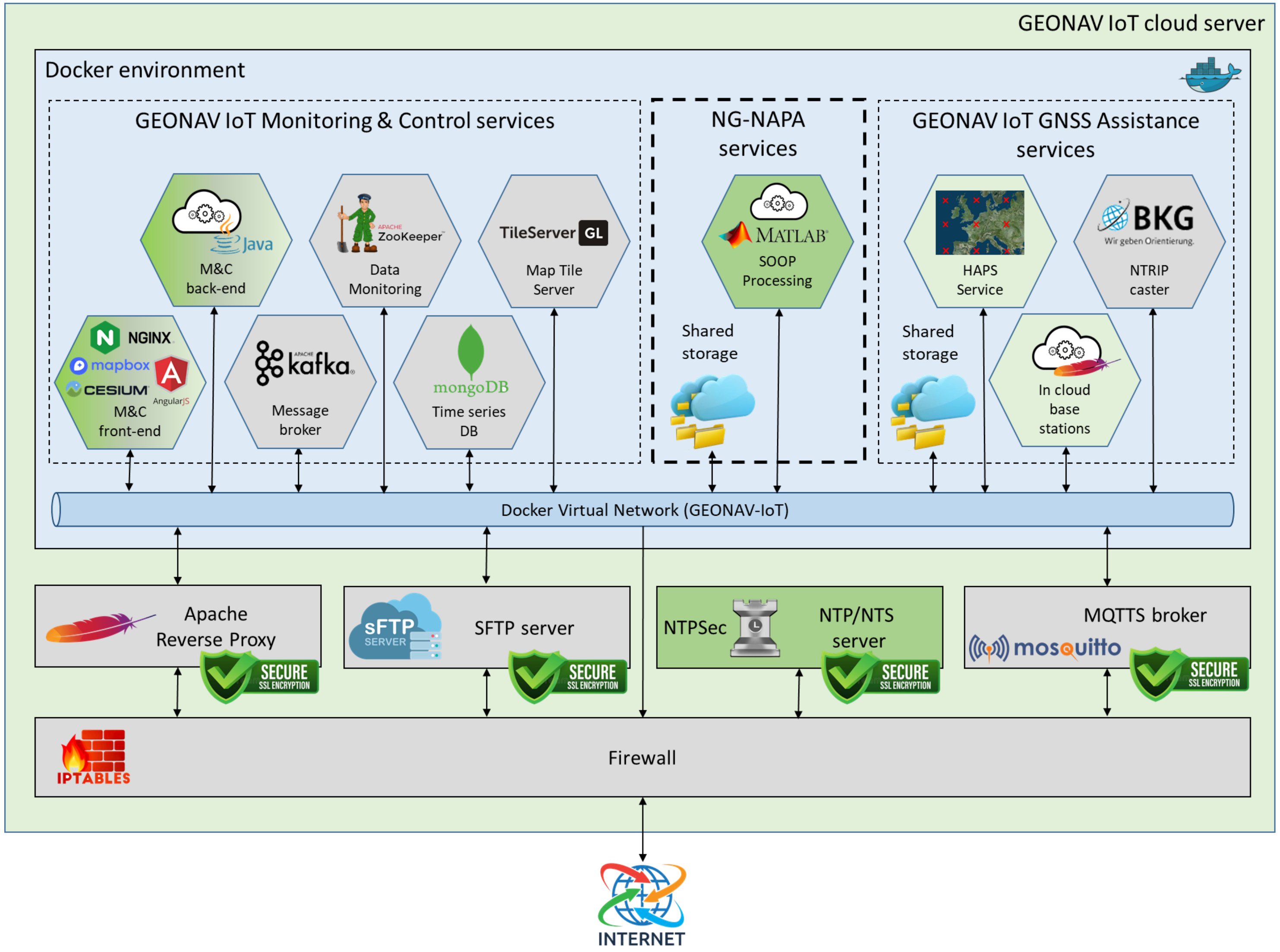
Reference station
User terminal
UWB beacon

Reference station



Demonstrator Testbed

Demonstrator Architecture (Cloud Services)

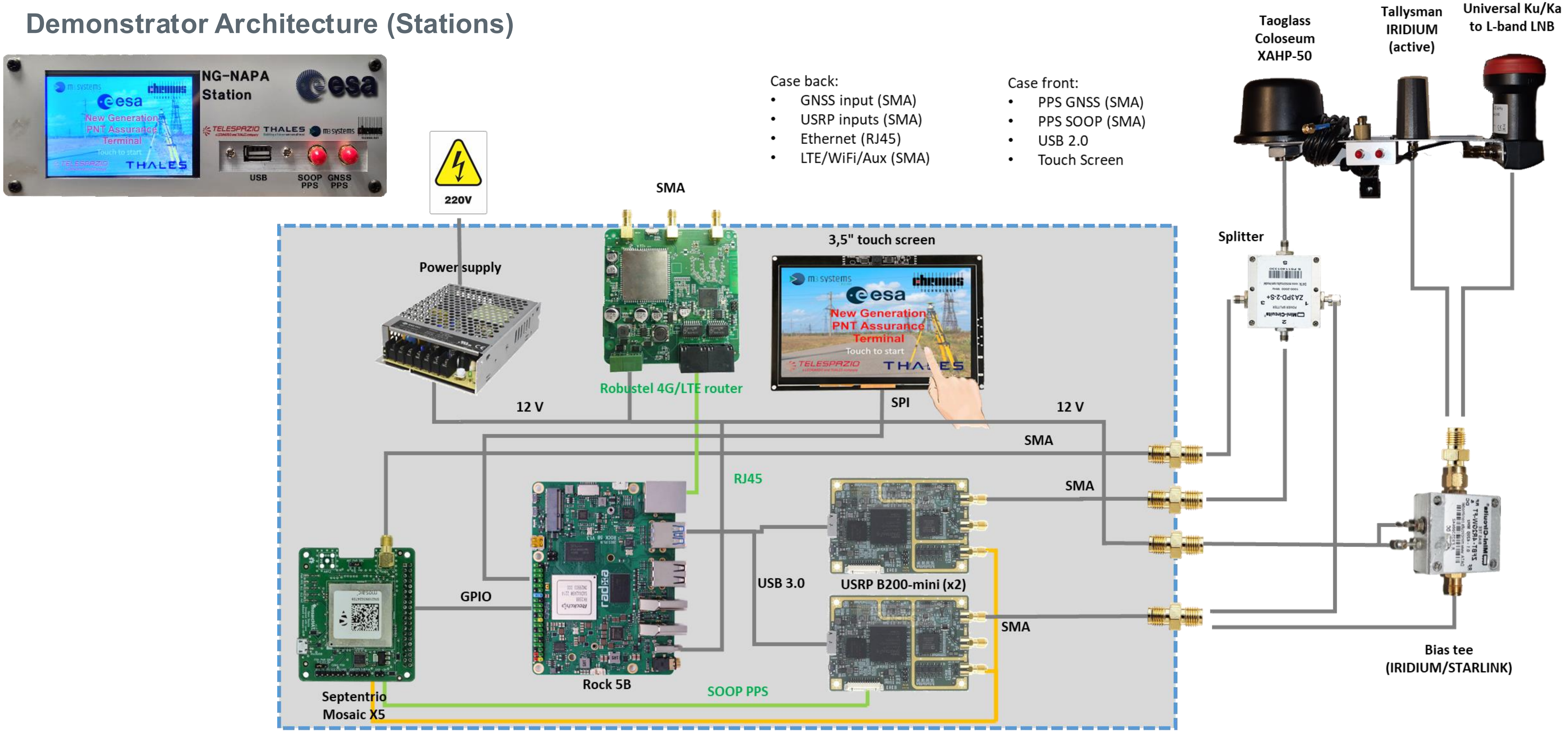


Demonstrator Testbed

Demonstrator Architecture (Stations)

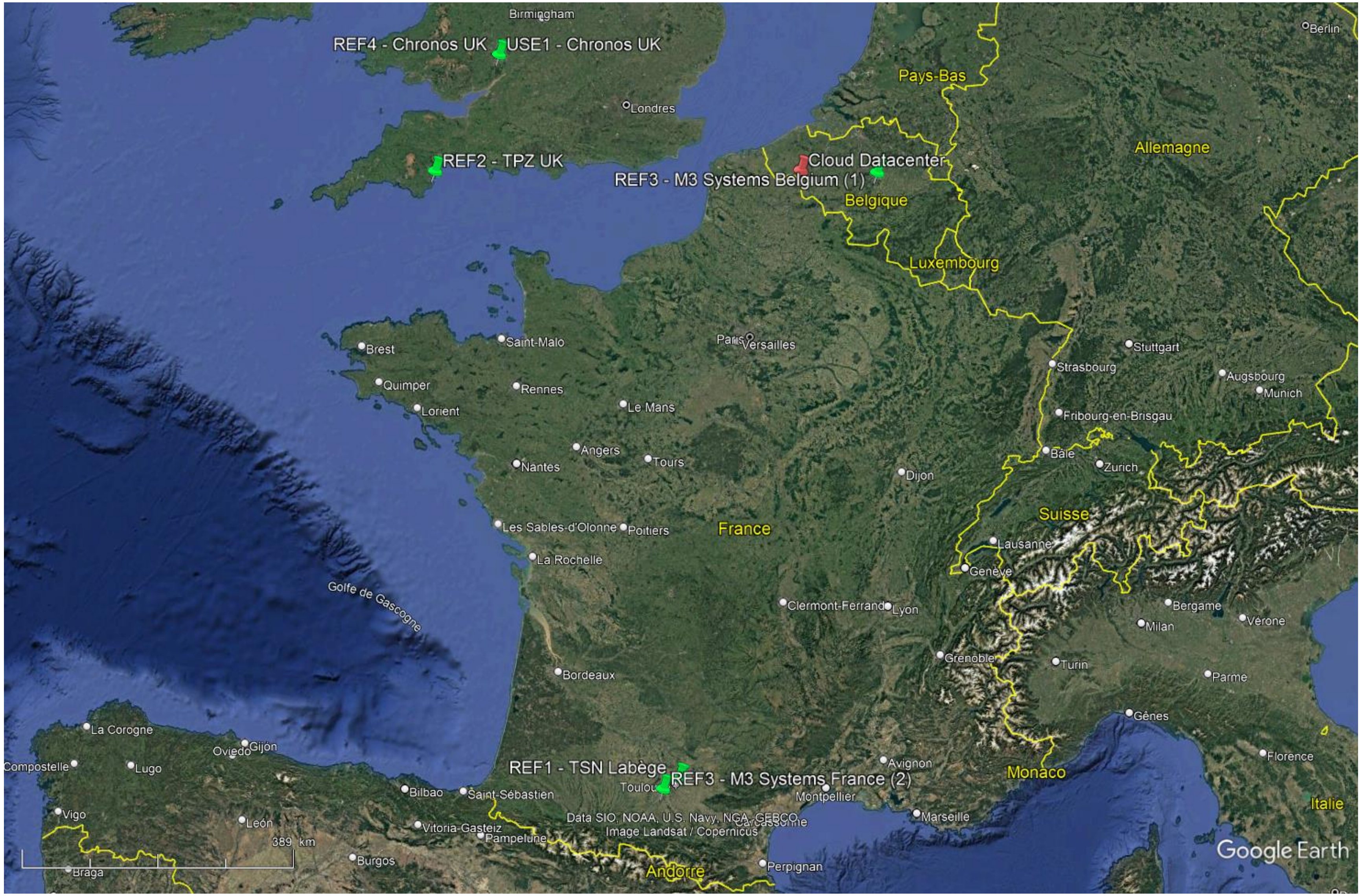
Case back:
- GNSS input (SMA)
- USRP inputs (SMA)
- Ethernet (RJ45)
- LTE/WiFi/Aux (SMA)

Case front:
- PPS GNSS (SMA)
- PPS SOOP (SMA)
- USB 2.0
- Touch Screen



Demonstrator Testbed

Deployment



Demonstrator Testbed

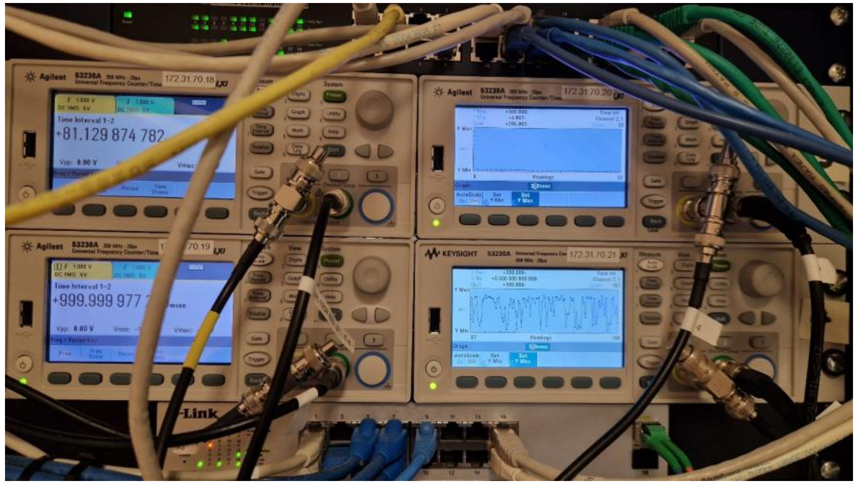
Measurement testbed

Triplicated Caesiums:
3 * MicroSemi 5071A
Long term locked to GNSS

Accuracy better than 10ns
to UTC(usno)

Multiple Timer counters

Only 4 shown here
20ps resolution
Locked to and timed
from Caesium



Demonstrator Testbed

Receiver installs

REF4

Antenna

Clean sky view
minimal local noise
sources

Demonstrator Testbed

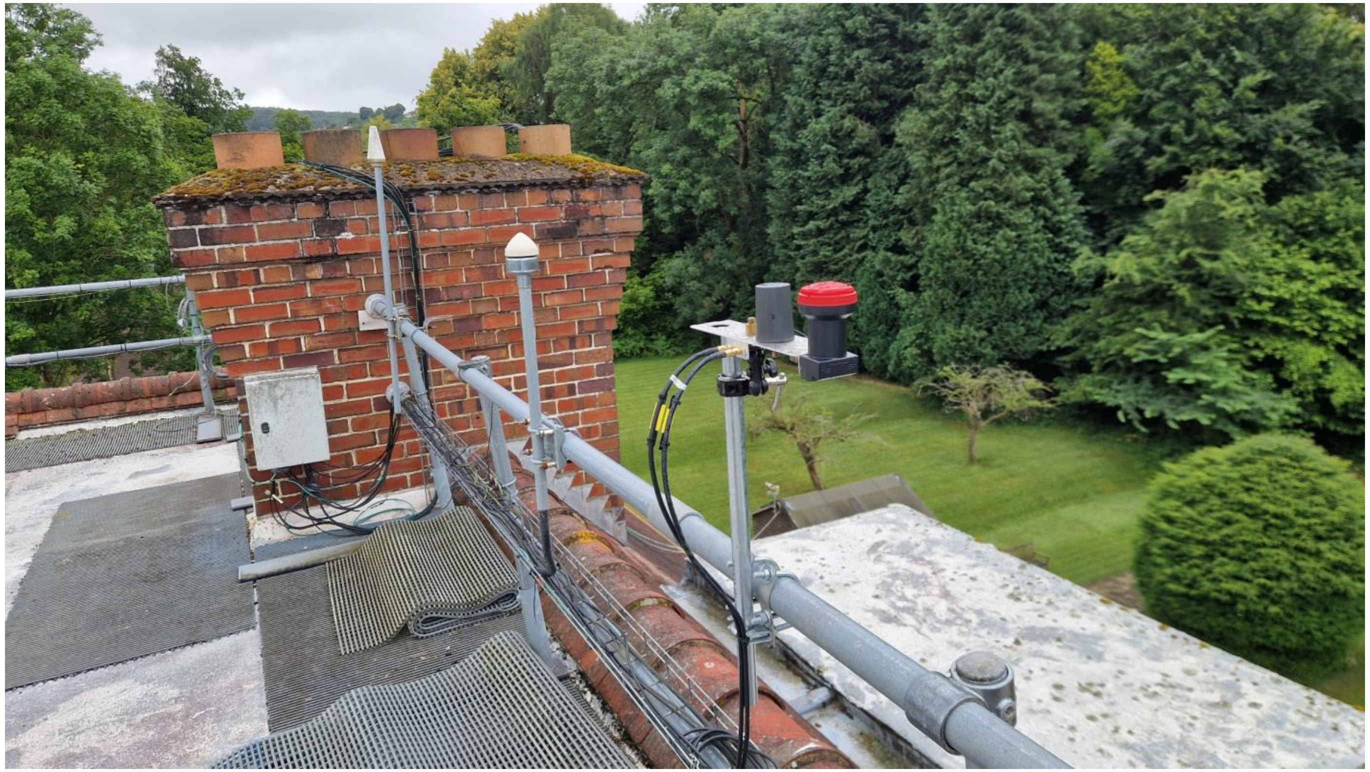
Receiver installs

USE1

Currently “unboxed” to allow external clock feed.

Antenna

Clean sky view
minimal local noise sources



Demonstrator Testbed

Receiver installs

REF 2

Devon, UK

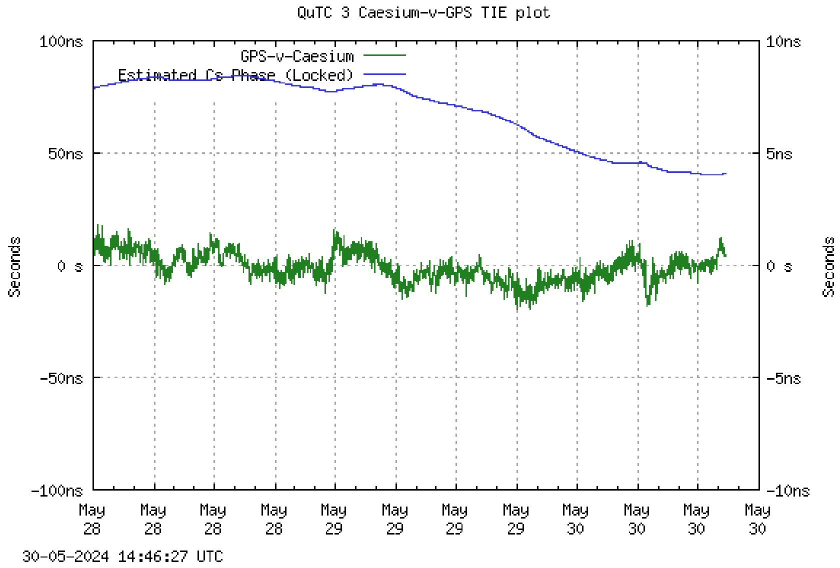
Antenna

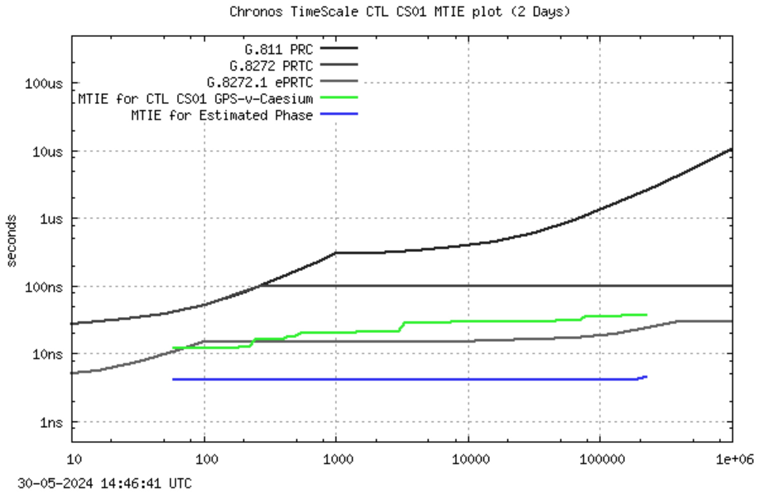
Clean sky view
minimal local noise
sources

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.

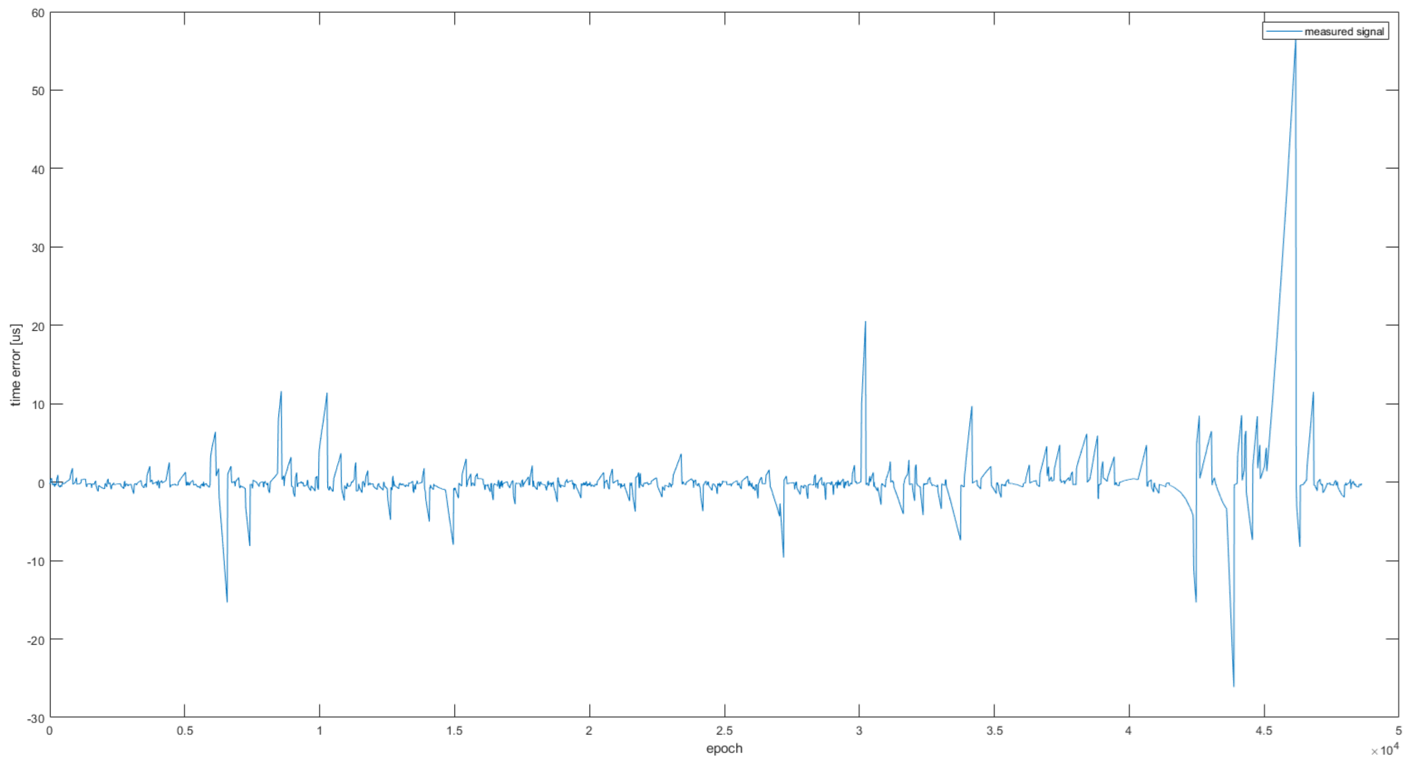




Performance Results

Timing

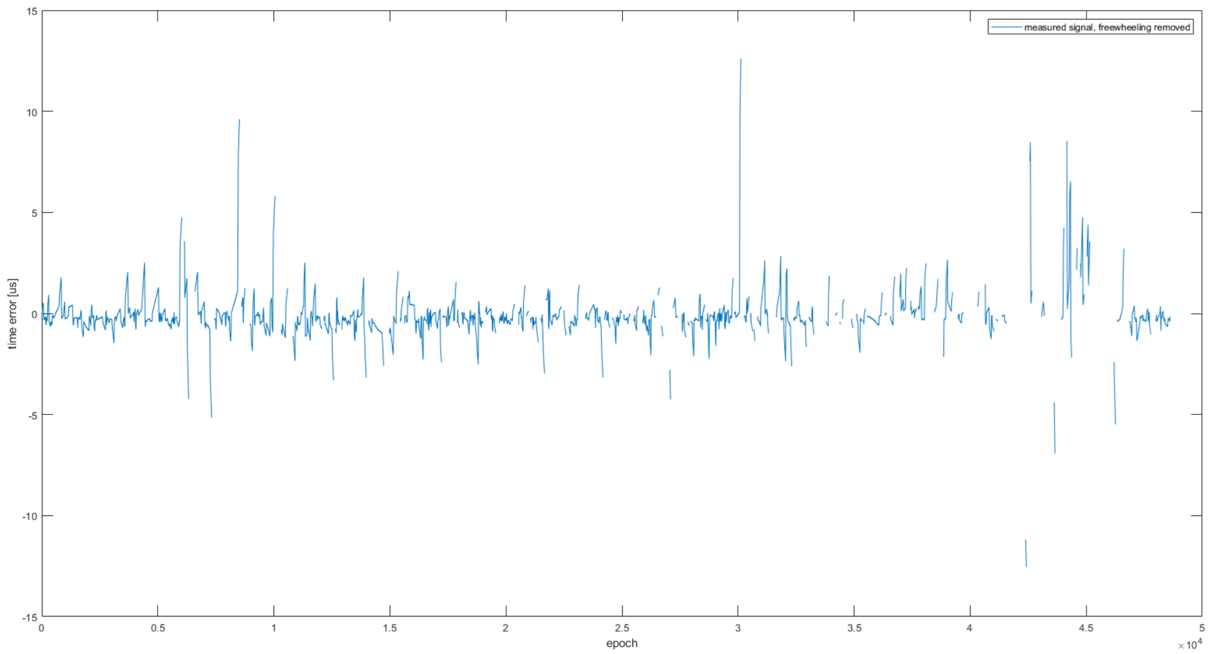
- During a 12-hr run, found that availability of good (high-BW) Iridium was inconsistent
- When signals are unavailable for many epochs, the clock model will be freewheeling and can drift a long way off
- Although the resulting performance may spend a lot of time with low error, there are many spikes

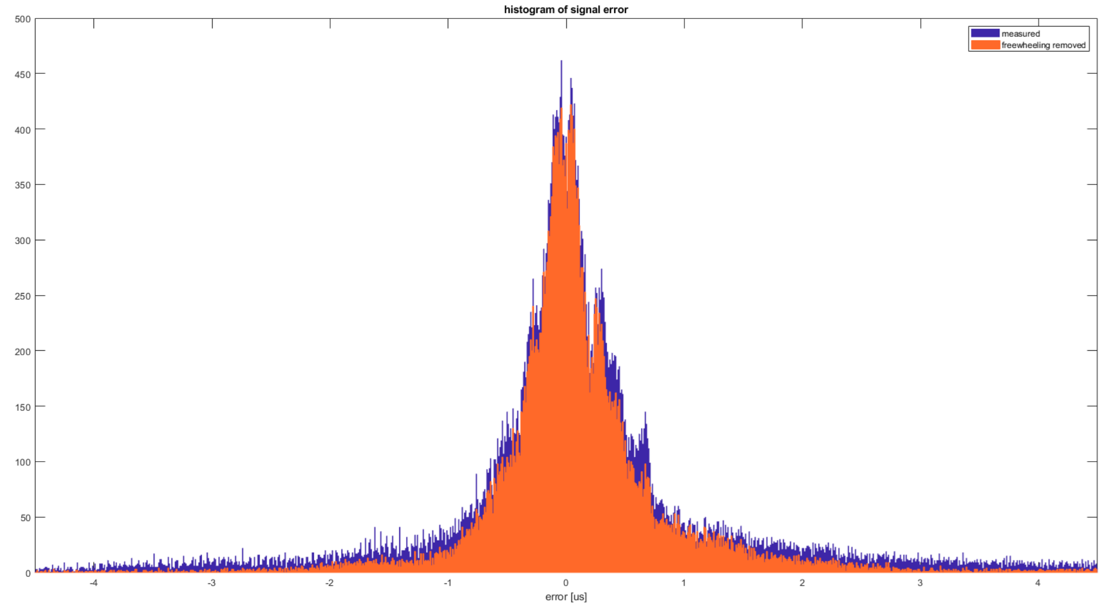


Performance Results

Timing

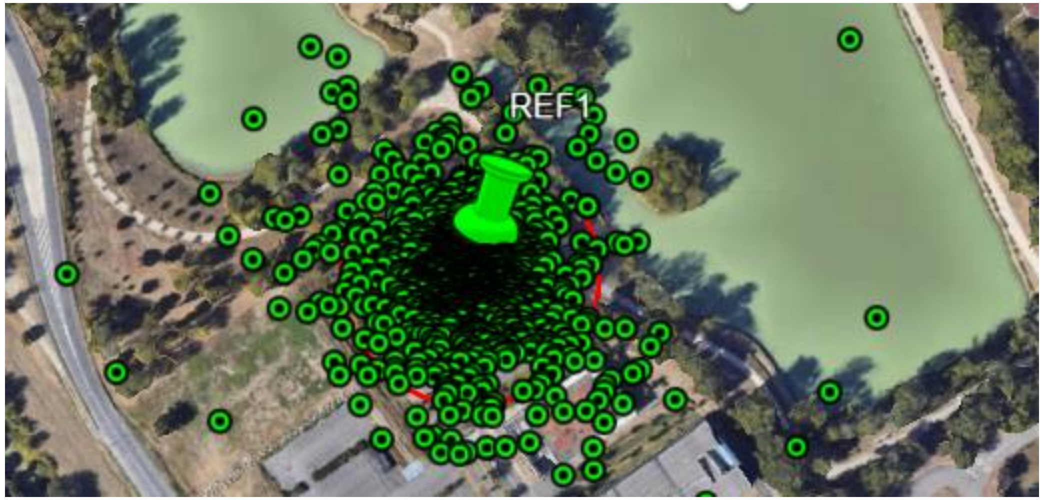
- Removing the epochs where the clock was freewheeling, the plot is better, but still does have spikes
- Could be due to the system using a medium-to-low BW signal to get its estimate for that epoch
- Could also be due to selecting the wrong peak in the ACF
- Without freewheeling the system is achieving:
  - < 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.





Performance Results

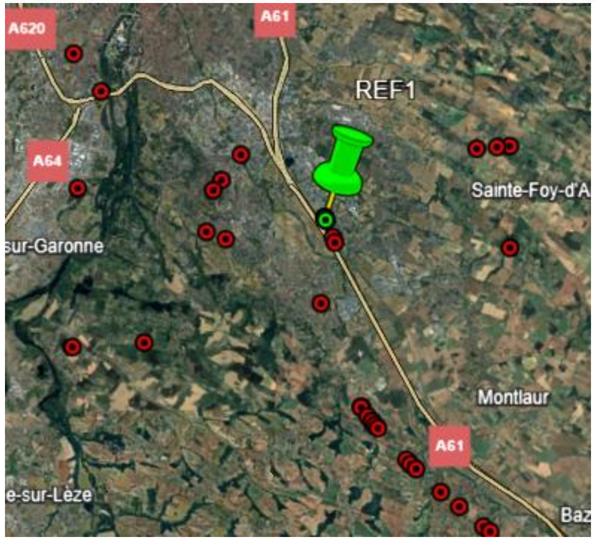
GPS L1



GPS L1CA -> Known

Setup: 2 Reference stations (Lavernose, France + London, UK) + 1 User (Labege, France)

- HPE/VPE CEP50 : 21.77m/36.38m
- Start Time: 2025-09-06 T 00:00
- End Time: 2025-09-08 T 00:00
- Number of computed positions: 1446
- Number of valid positions: 1118
- Outliers: ~22.68%



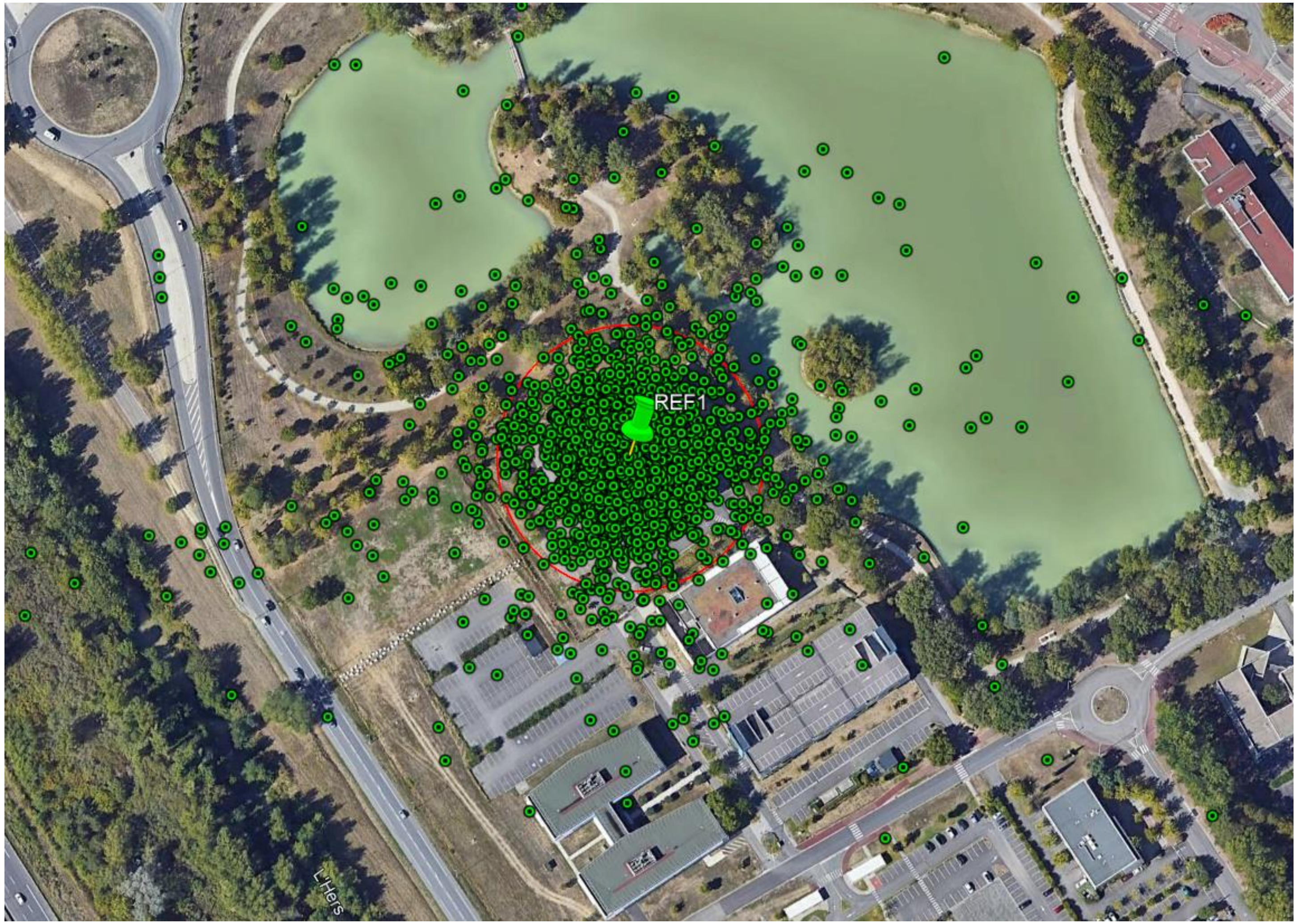
GPS P(Y) -> Encrypted/Unknown

Setup: 2 Reference stations (Lavernose, France + London, UK) + 1 User (Labege, France)

- HPE/VPE CEP50 : 14.59m/4.16m
- Start Time: 2025-09-08 T 10:00
- End Time: 2025-09-09 T 13:29
- Number of computed positions : 137
- Number of valid positions : 5
- Outliers: ~96.35%

Performance Results

Galileo E6BC



Galileo E6C -> Assumed to be encrypted/unknown

Setup: 2 Reference stations (Lavernose, France + London, UK) + 1 User (Labege, France)

- HPE/VPE CEP50 : 11.33m/17.87m
- Number of computed positions : 7068
- Number of valid positions : 6342
- Outliers: ~10.27%

Conclusions and Way Ahead

Tim Whitworth (Telespazio UK)
Martin Bransby (Telespazio UK)

Conclusions

- **Security**:
  - Designed a system where the User only uses SOOP signals in its processing
  - Resilient to spoofing of predictable signals
  - Timing solution resilient to jamming of GNSS
- **Demonstrator**:
  - Developed and deployed a User and four Reference Stations
  - Epoch based snapshots with cloud processing, to limit data transfer and to ease development complexity
  - System design is scalable – the Reference network can support many Users
- **Performance**:
  - Timing using Iridium is fairly good, but inconsistent. Can provide the assurance of a standalone solution if GNSS is jammed, or validation that GNSS is not being spoofed. There are several methods identified that could improve the performance.
  - Positioning using GNSS encrypted signals is done. This will not hold up to jamming but will prevent spoofing attacks. Integrating with IMU could improve performance, but it is unlikely to be suitable for the automotive Use Case identified.

Way Ahead and Recommendations

Possible Further Work

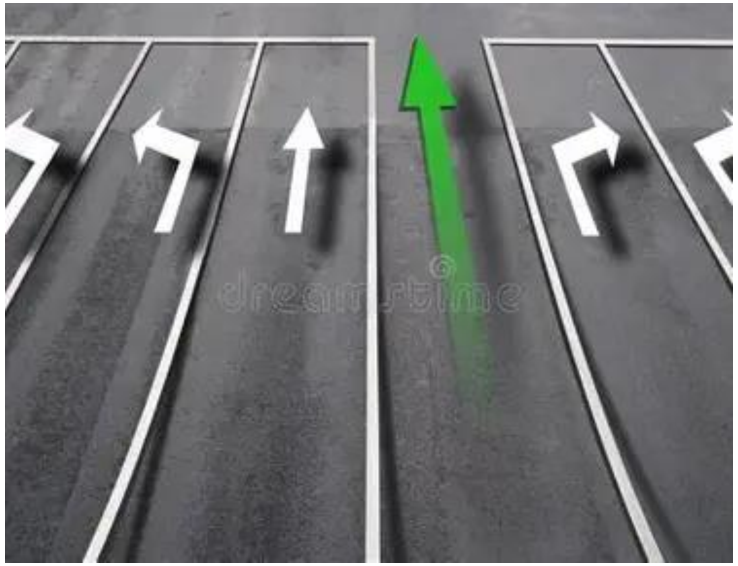
Item/problem	Way forward
HW Constraints including cost/quality	Migrate to improved HW with large ecosystem and well-maintained OS
HW failures in transport	Hardening components for transportation & ILS
Proprietary HW/SW	Migrate the infrastructure to IPR free hardware and software
Authentication delay – demo based on cloud SP with wireless connections causing delay	Migrate a part of the authentication processing at user terminal level
Coding Language – MATLAB used to reduce the development and validation effort, but long run time	Migrate the signal processing functions to a more efficient language supported by open-source signal processing libraries
User clock stability – Poor quality, based internal USRP clock. Clock model suffers for SOOP PPS generation	Use a more stable clock like a CSAC
LEO SOOP – Inconsistent usage of the Iridium platform makes it difficult to get high-BW snapshots for good timing performance	Take more snapshots at both the RS and UT. It would process on the RS to determine the snapshot with the *best* signal inside, and send *only* this to the UT, reducing the data transfer from RS to the cloud
SNR	RS could use antenna arrays to improve SNR and remove inter-satellite-interference issues
Other improvements in SP	• GNSS encrypted - estimate the chips rather than adding samples. This could be the P(Y) code chips, or the underlying W code chips. • Iridium - attempt symbol detection. This should improve SNR (as it won't be a noisy copy), and it would decrease the data needed to be sent to the cloud/UT

Way Ahead and Recommendations

Potential Way Forward

A way forward has been identified, as follows:

- Implementation of the further work is required for a more robust/reliable system of this PoC
- Integration with other techniques on the user side
- Potential integration into other assurance products utilising SOOP
- Market Analysis and definition of value proposition
- Definition and design of a service wrapper based on MA.



Q&A

NG-NAPA Project Team

CONTACTS

Martin Bransby
Head of Navigation (TPZ-UK)
Martin.Bransby@telespazio.com

Louise Mercy
Navigation Project Manager (TPZ-UK)
Louise.Mercy@telespazio.com

Tim Whitworth
Technical Lead (TPZ-UK)
Tim.Whitworth@telespazio.com

Jean-Christophe Casteran
Engineering Delivery Manager (TSN)
jean-christophe.casteran@thalesgroup.com

Aravind Ramesh
Radionavigation and Signal processing Engineer (M3S)
aravind.ramesh@m3systems.eu

Tony Flavin
Manager of Strategic Research (CTL)
tony.flavin@chronos.uk

THANK **YOU**
FOR YOUR ATTENTION

telespazio.co.uk