EU SPACE

Authentication and other new services on Galileo

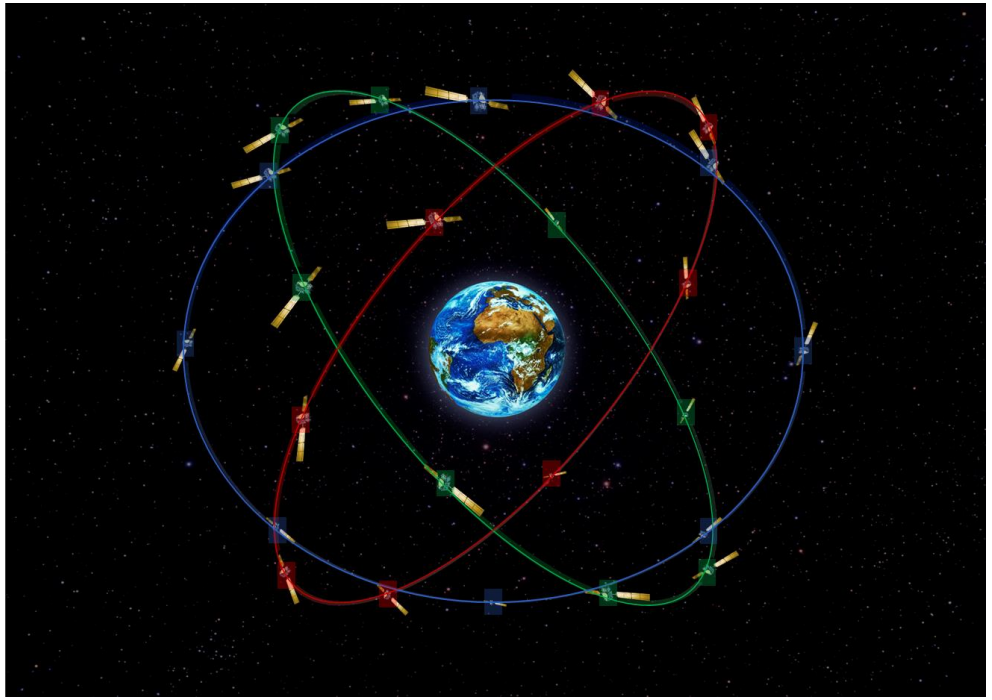
Ignacio Fernández Hernández
European Commission
13 Oct 2022

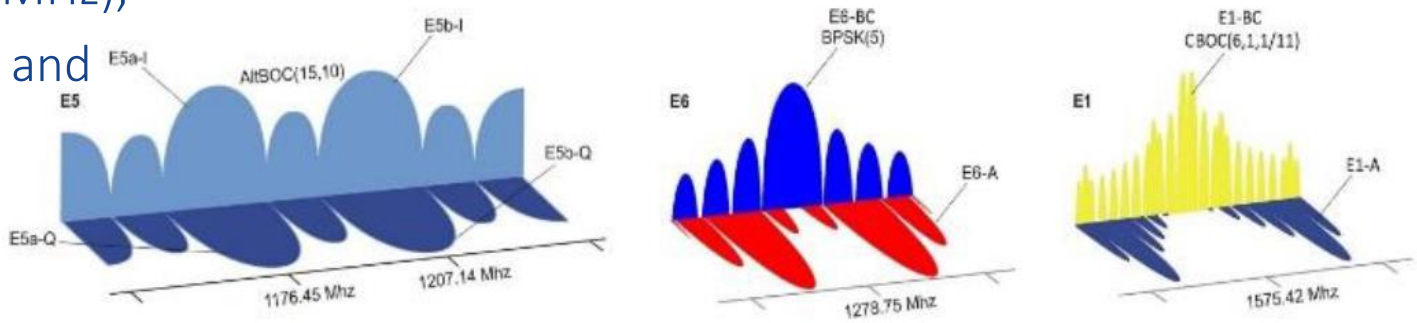
Table of contents

Table of contents

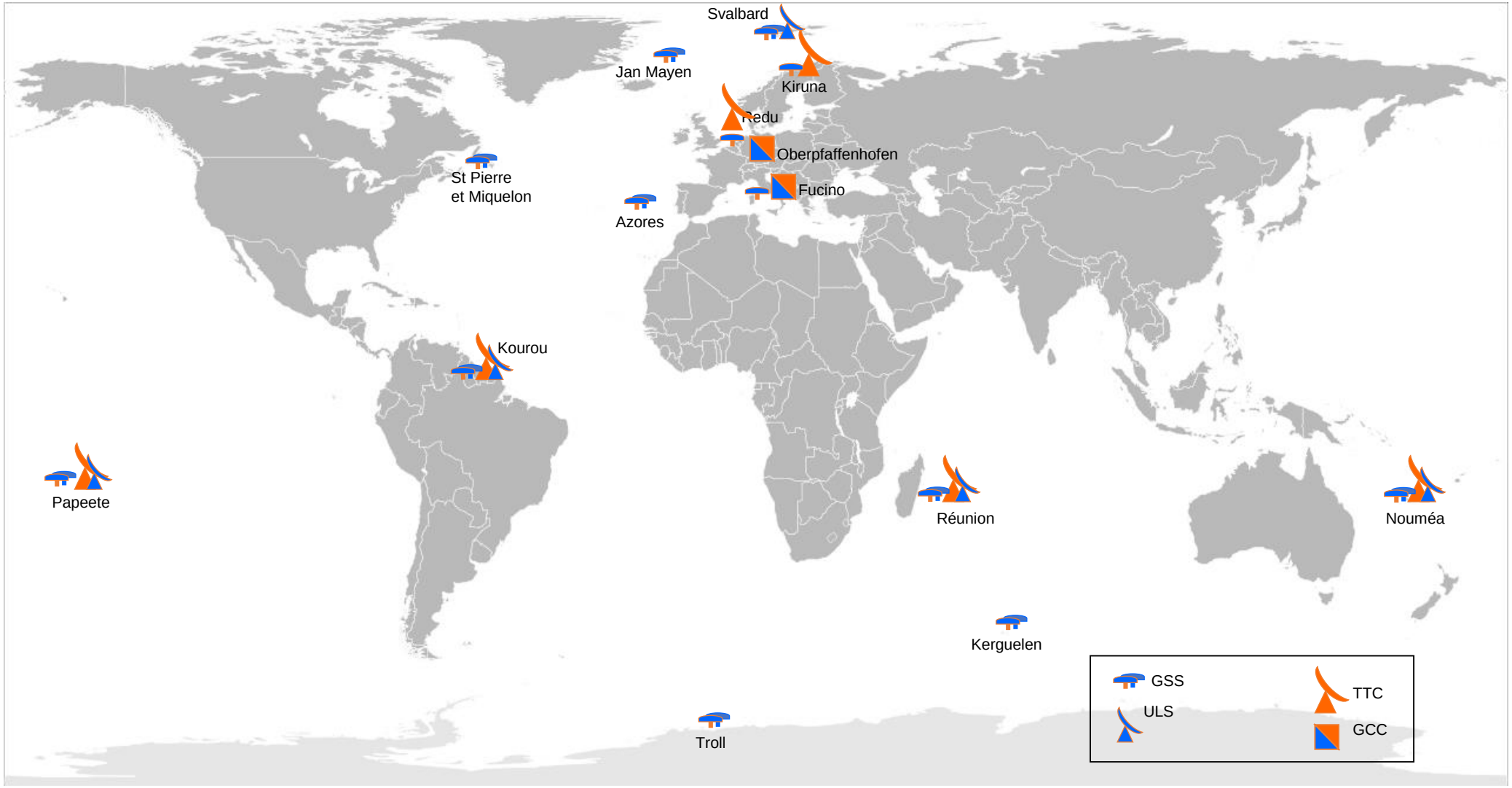
Galileo

- Galileo is the EU satellite navigation system
- Initial service since 2016
- Some data:
  - Space segment: 3 orbital planes, 8 + spare SV per plane. SV altitude: 23,222 km
  - Ground segment: 2 control centers (IT, DE), 14 monitoring stations worldwide, 5 uplink stations, 6 TTC stations
  - 4 carriers: E1 (1575.42 MHz), E5a (1176.45 MHz), E5b(1207.14 MHz), E6 (1278.75 MHz), BOC and BPSK signals



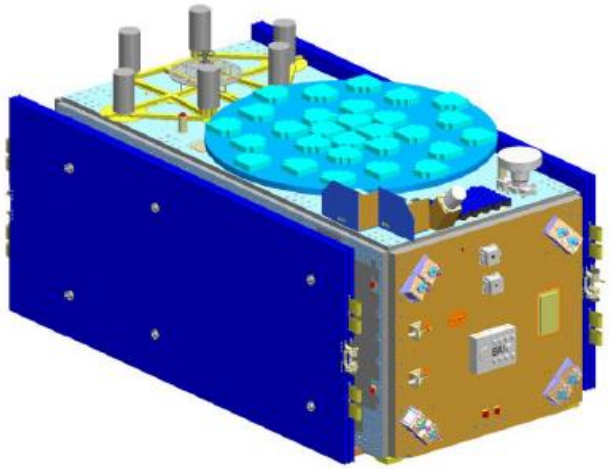


Galileo Ground Segment

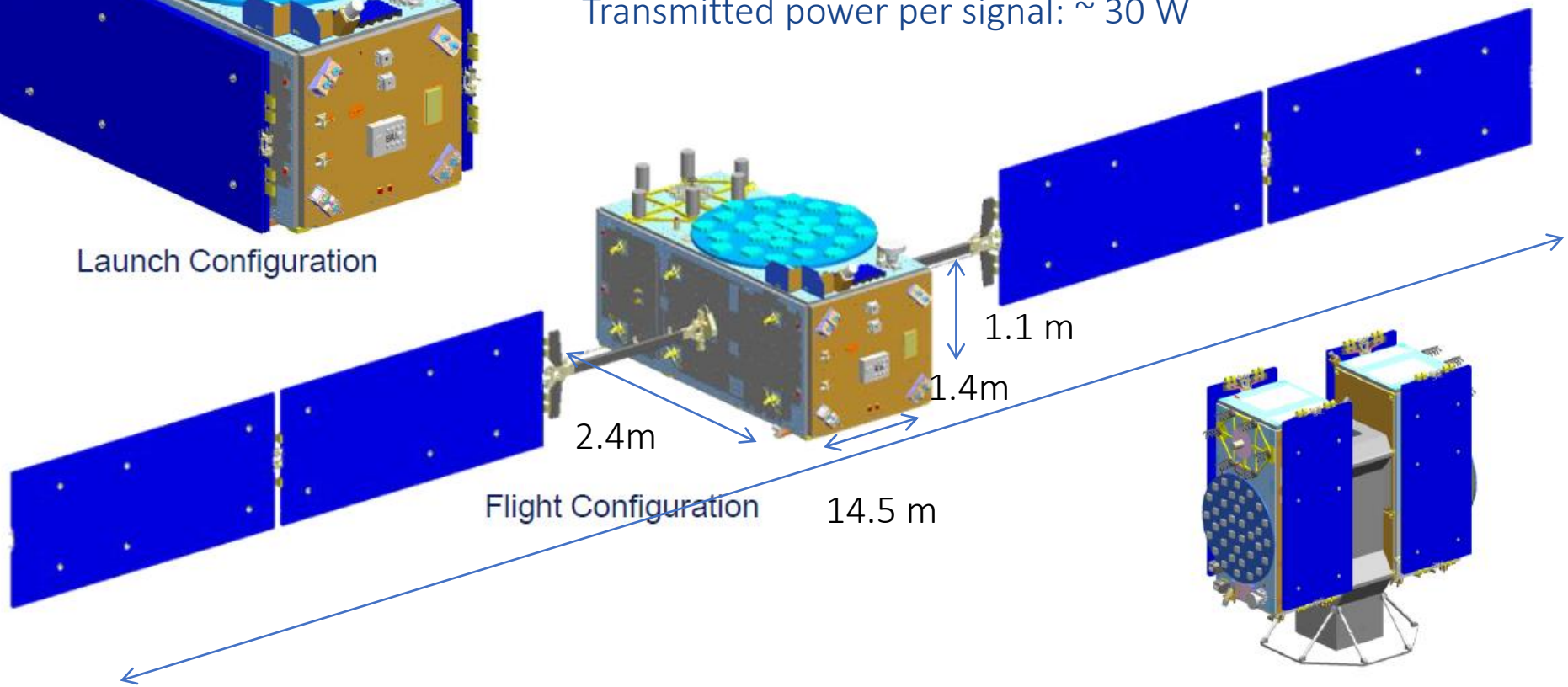


Galileo satellites

Weight: ~ 730 kg
Power consumption: ~ 2000 W
Transmitted power per signal: ~ 30 W



Launch Configuration



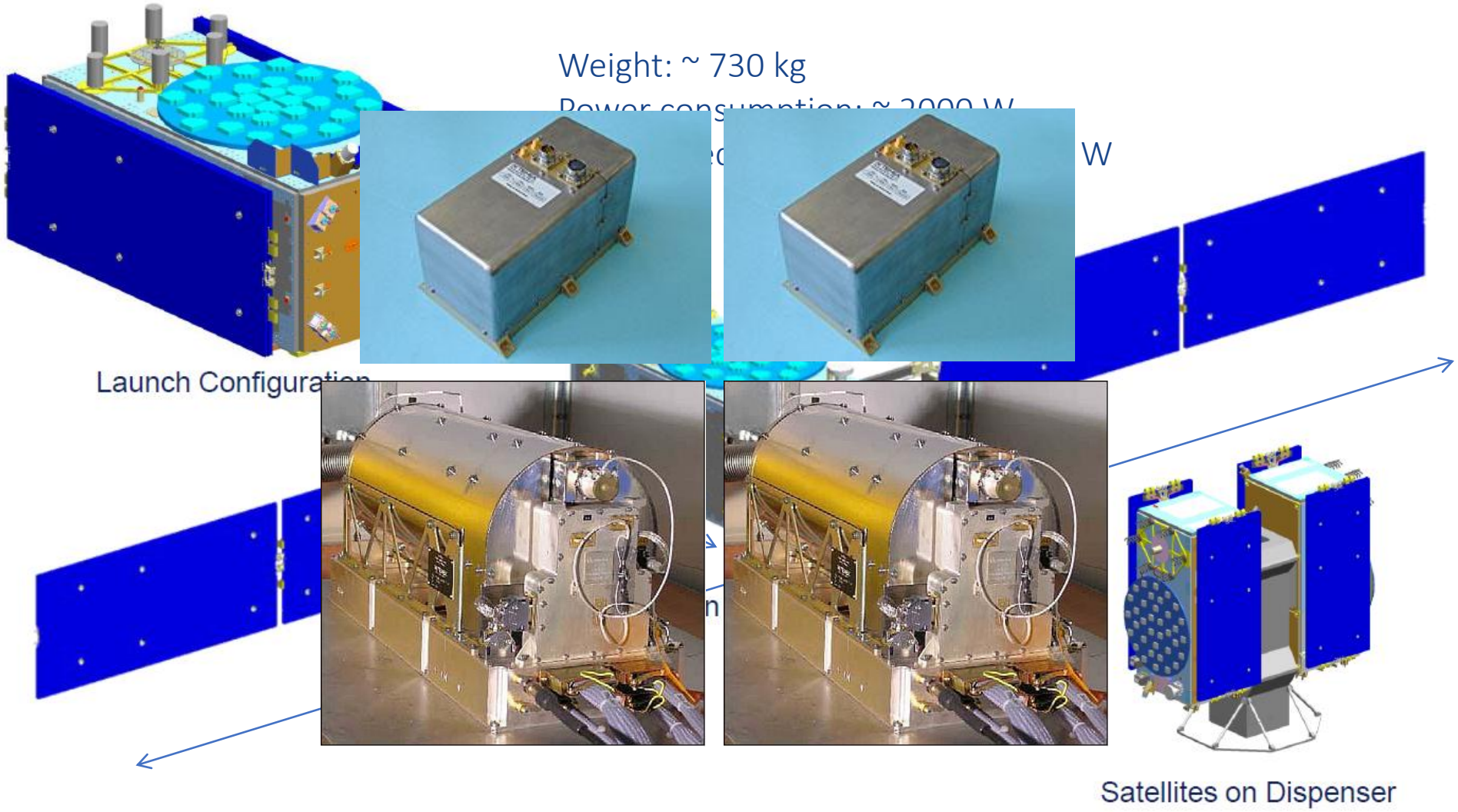
Flight Configuration

Satellites on Dispenser

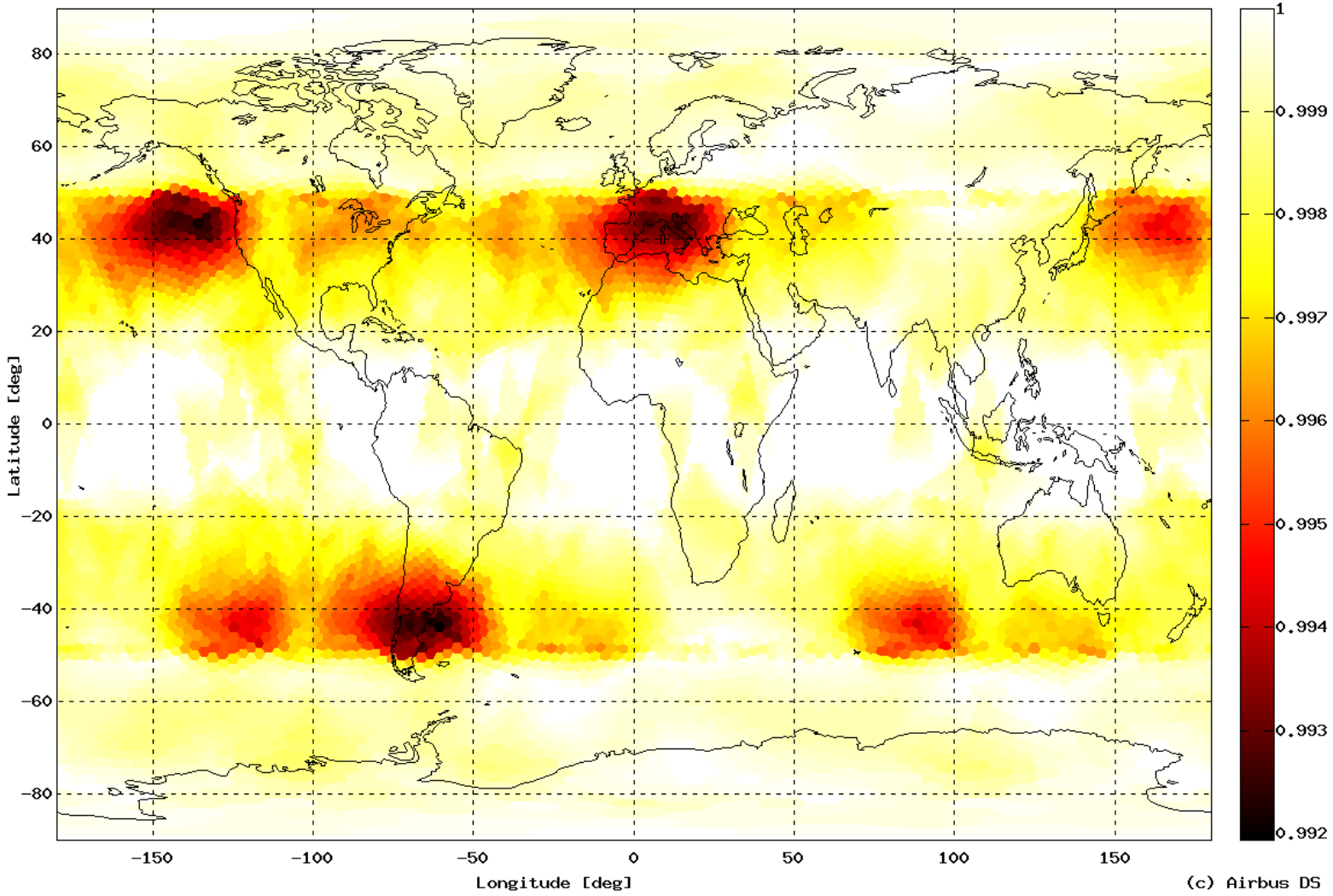
Galileo satellites

Weight: ~ 730 kg

Power consumption: ~ 2000 W



Galileo availability



August 2022. Availability of I/NAV PDOP ≤ 6. Aug'22. Min: 99.19% - Mean: 99.86% - Max: 100%

Galileo

For more information:

https://gsc-europa.eu

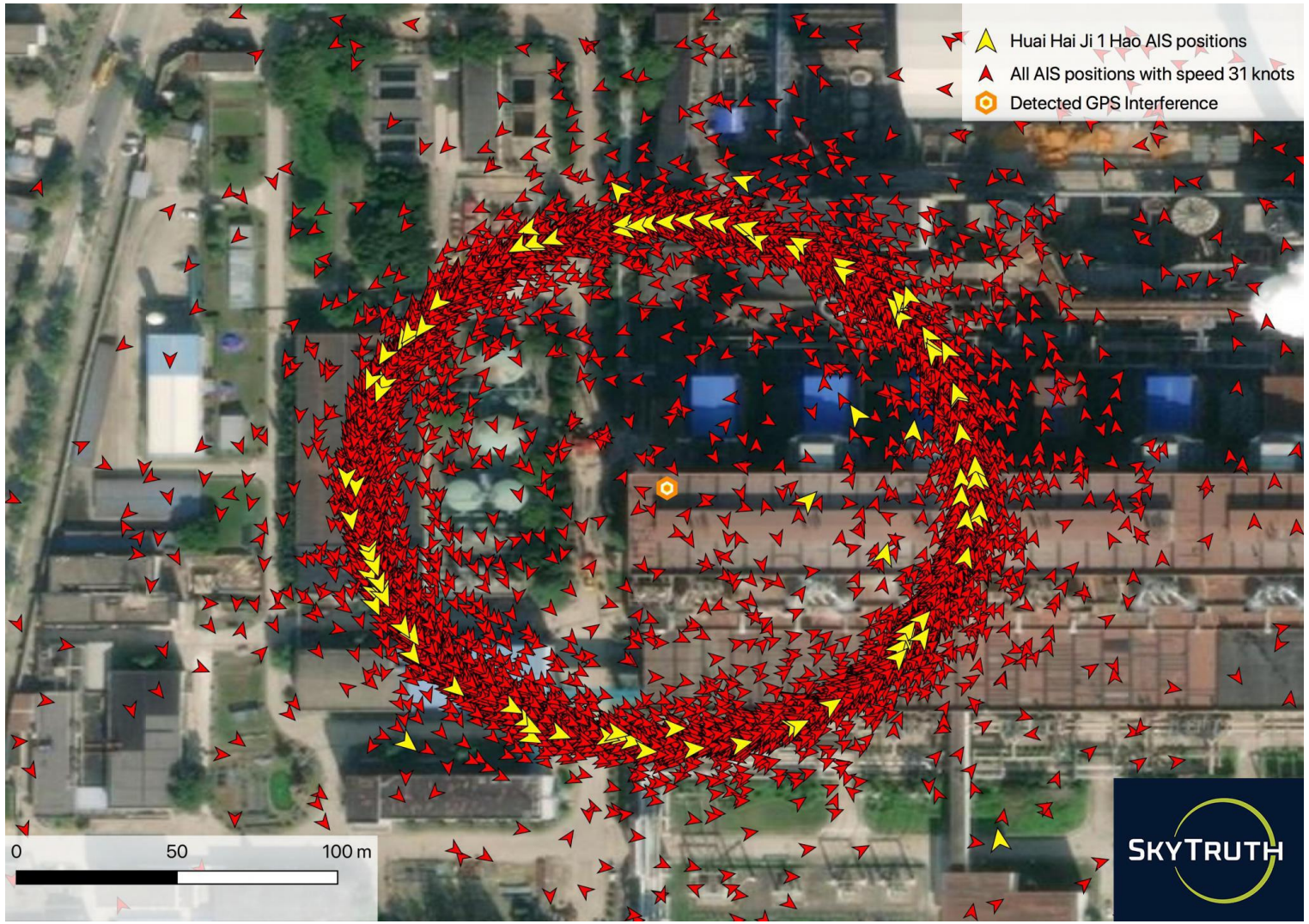
Table of contents

What is Galileo OSNMA

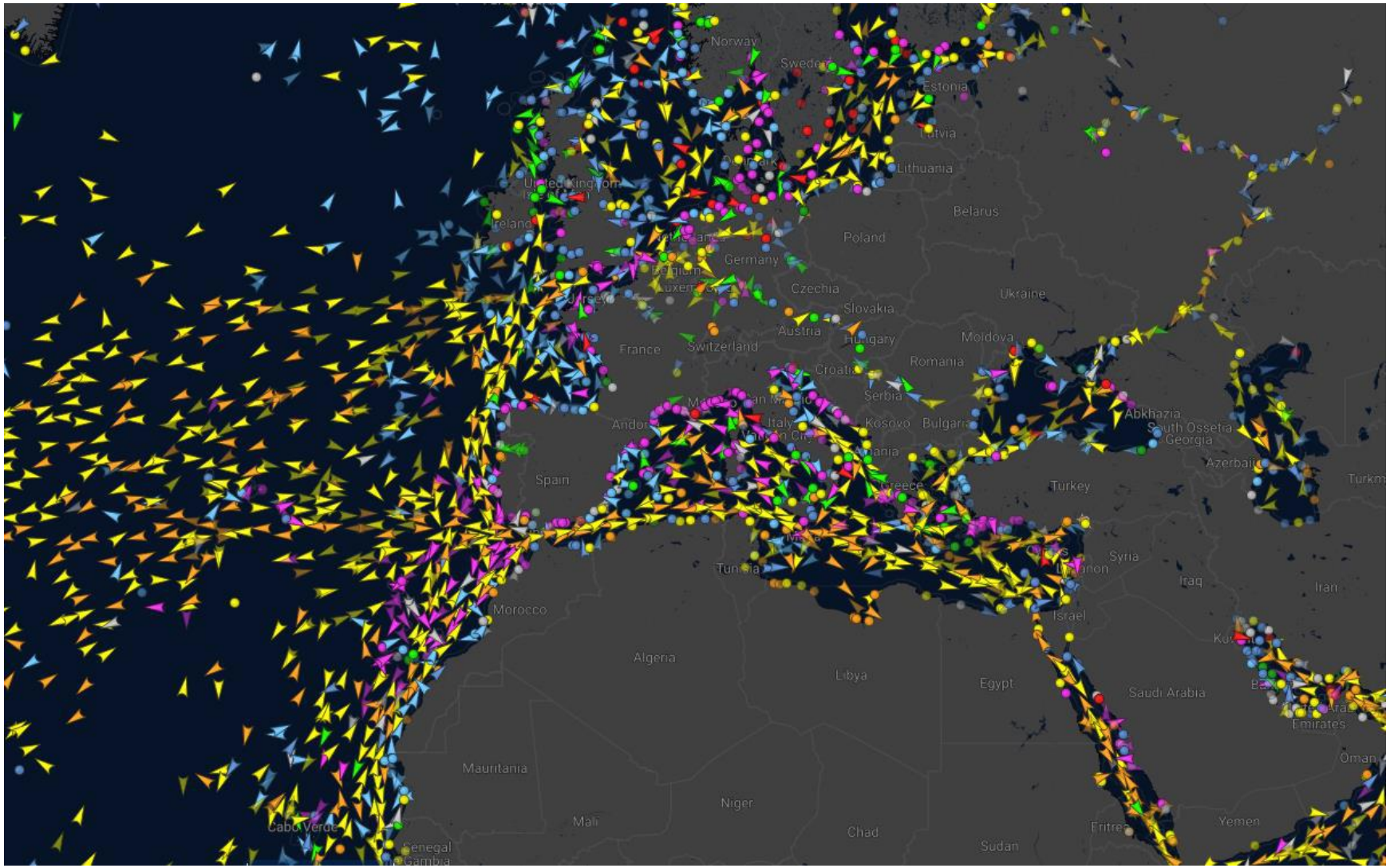
- What is Galileo OSNMA?
  - Stands for Open Service Navigation Message Authentication
  - Mechanism to authenticate the Galileo data used to calculate a position: satellite orbits and clock corrections, satellite status flags, time…
  - Equivalent to a Galileo “digital signature”
  - Transmitted in 40 bits every other second in the Galileo I/NAV message, E1B component, 1575.42 MHz
  - Makes the signal unpredictable

- Why OSNMA?

Why OSNMA

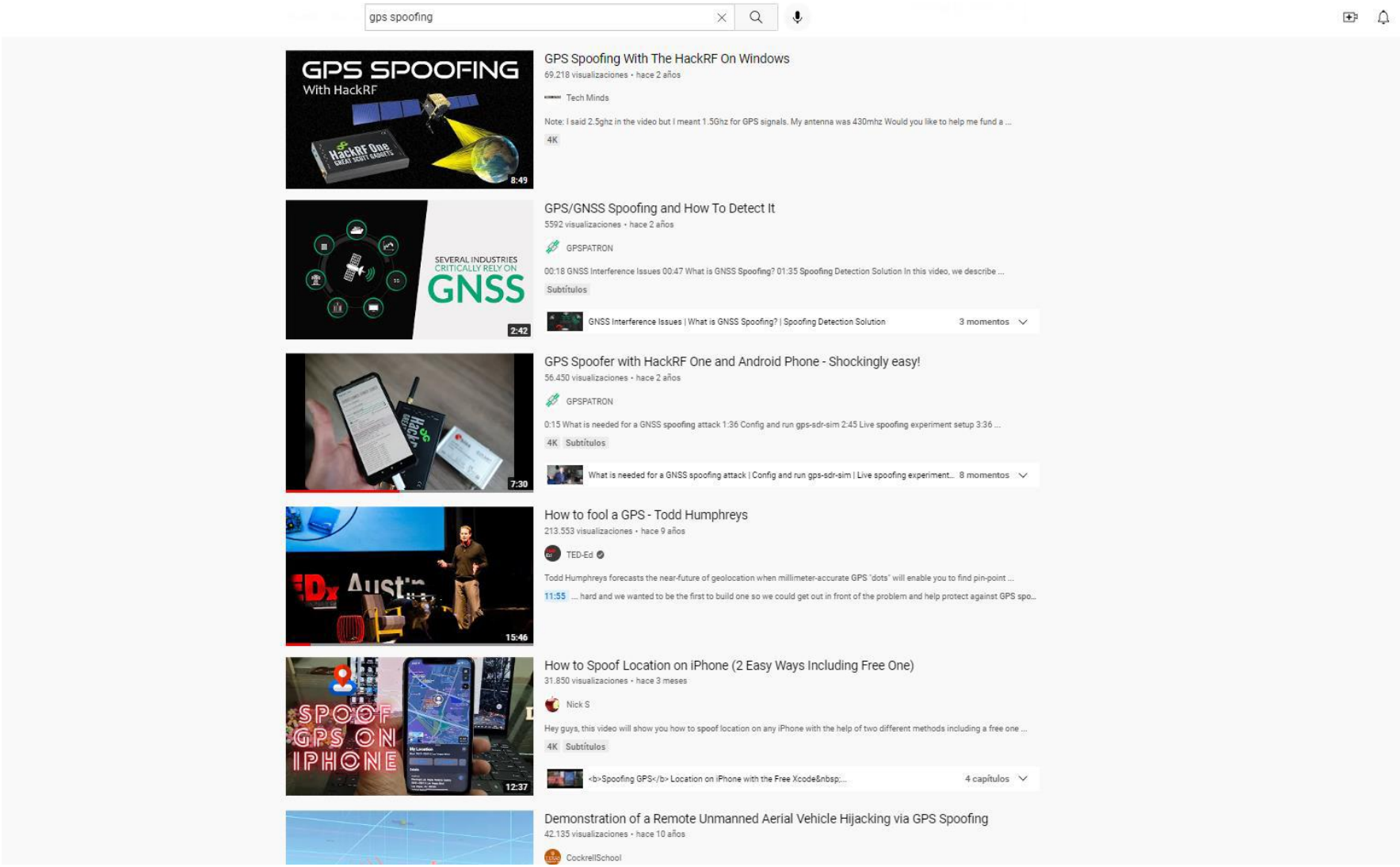

Huai Hai Ji 1 Hao AIS positions
All AIS positions with speed 31 knots
Detected GPS Interference
0
50
100 m
SKYTRUTH

Why OSNMA

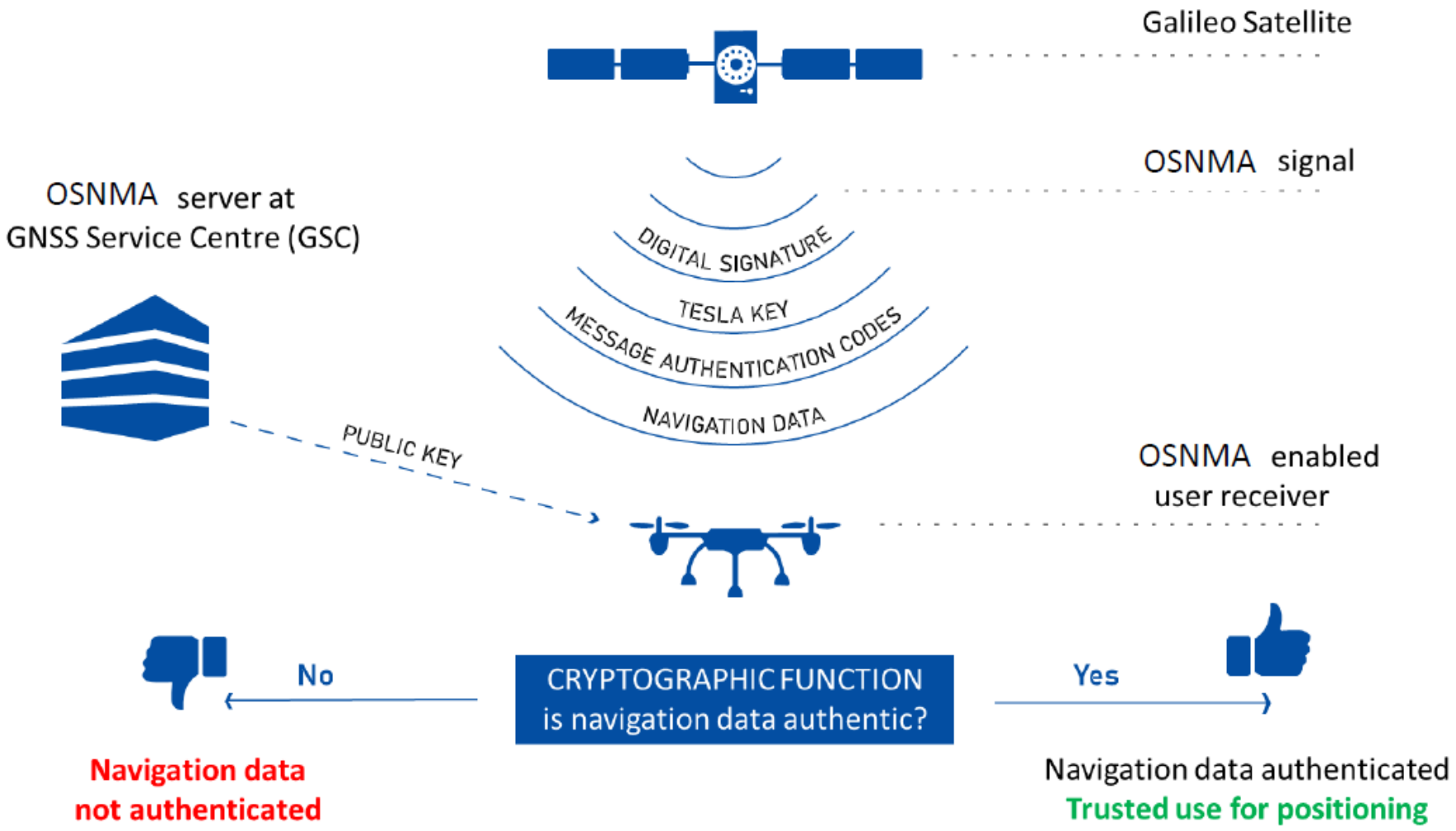


Vesselfinder.com

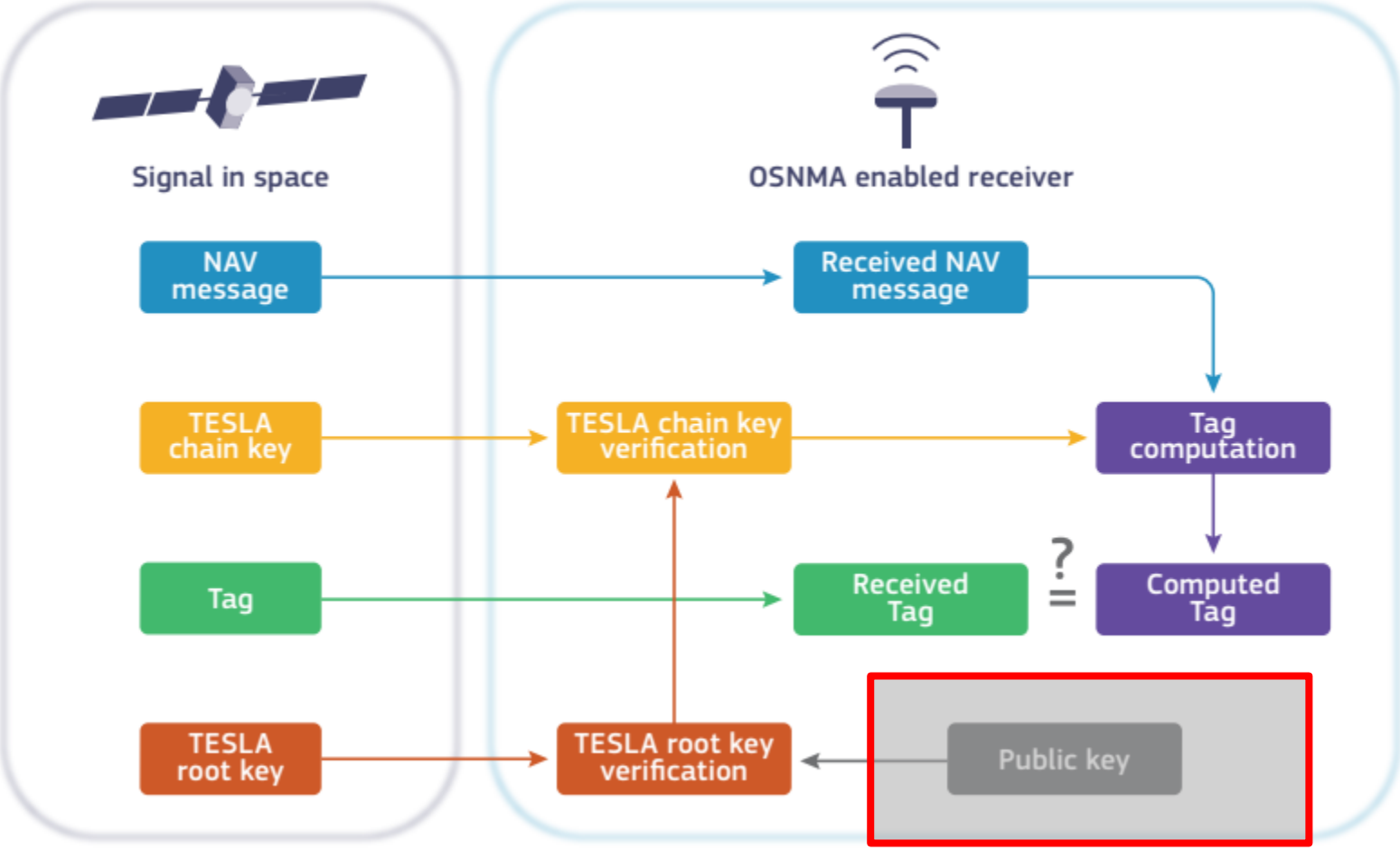
Why OSNMA


gps spoofing
GPS SPOOFING
With HackRF
8:49
GPS Spoofing With The HackRF On Windows
69.218 visualizaciones • hace 2 años
Tech Minds
Note: I said 2.5ghz in the video but I meant 1.5Ghz for GPS signals. My antenna was 430mhz Would you like to help me fund a ...
4K
SEVERAL INDUSTRIES
CRITICALLY RELY ON
GNSS
2:42
GPS/GNSS Spoofing and How To Detect It
5592 visualizaciones • hace 2 años
GPSPATRON
00:18 GNSS Interference Issues 00:47 What is GNSS Spoofing? 01:35 Spoofing Detection Solution In this video, we describe ...
Subtítulos
GNSS Interference Issues | What is GNSS Spoofing? | Spoofing Detection Solution
3 momentos
7:30
GPS Spoofer with HackRF One and Android Phone - Shockingly easy!
56.450 visualizaciones • hace 2 años
GPSPATRON
0:15 What is needed for a GNSS spoofing attack 1:36 Config and run gps-sdr-sim 2:45 Live spoofing experiment setup 3:36 ...
4K Subtítulos
What is needed for a GNSS spoofing attack | Config and run gps-sdr-sim | Live spoofing experiment...
8 momentos
15:46
How to fool a GPS - Todd Humphreys
213.553 visualizaciones • hace 9 años
TED-Ed
Todd Humphreys forecasts the near-future of geolocation when millimeter-accurate GPS "dots" will enable you to find pin-point ...
11:55 ... hard and we wanted to be the first to build one so we could get out in front of the problem and help protect against GPS spo...
SPOOF
GPS ON
IPHONE
12:37
How to Spoof Location on iPhone (2 Easy Ways Including Free One)
31.850 visualizaciones • hace 3 meses
Nick S
Hey guys, this video will show you how to spoof location on any iPhone with the help of two different methods including a free one ...
4K Subtítulos
Spoofing GPS Location on iPhone with the Free Xcode ...
4 capítulos
Demonstration of a Remote Unmanned Aerial Vehicle Hijacking via GPS Spoofing
42.135 visualizaciones • hace 10 años
CockrellSchool

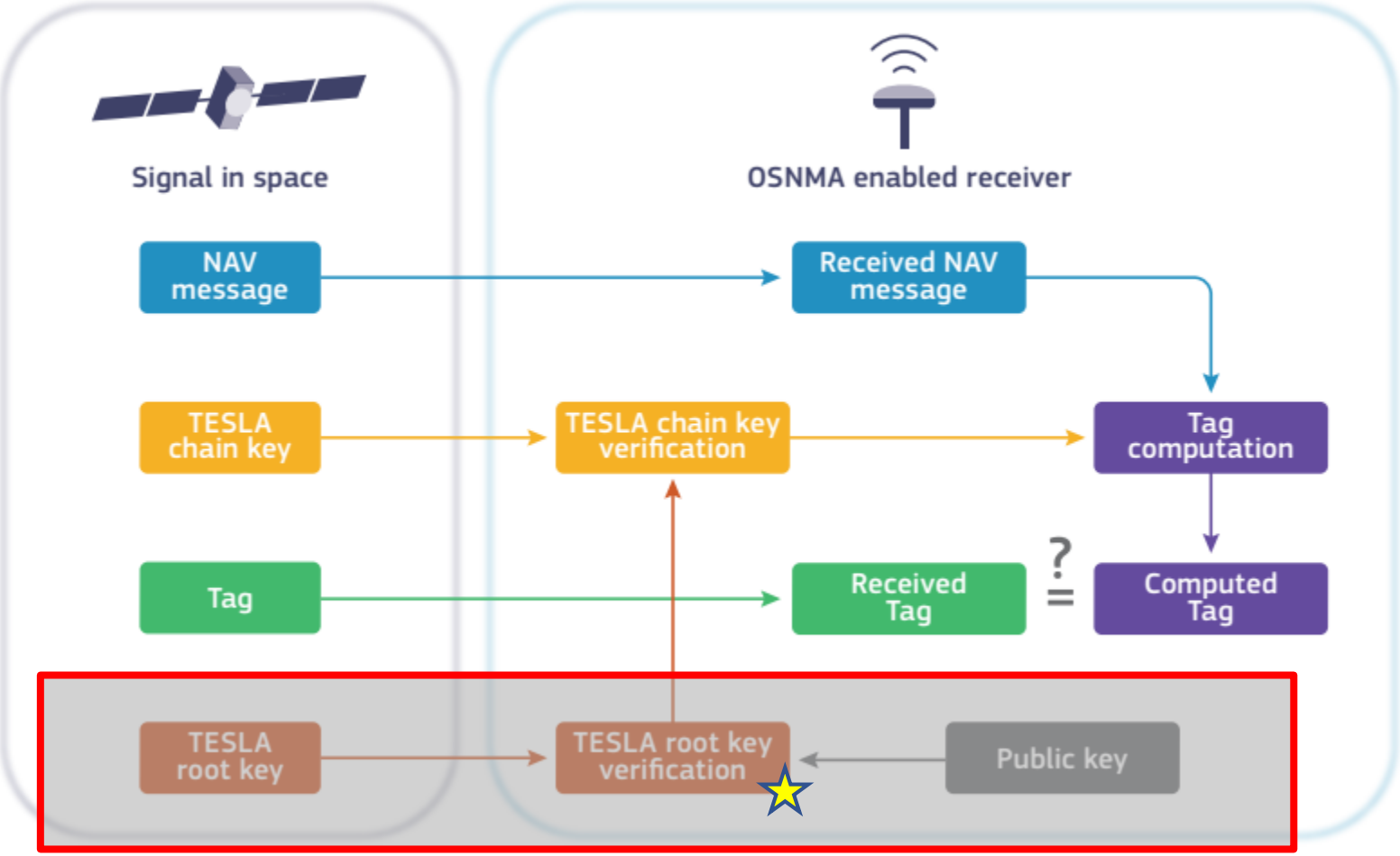
The OSNMA protocol



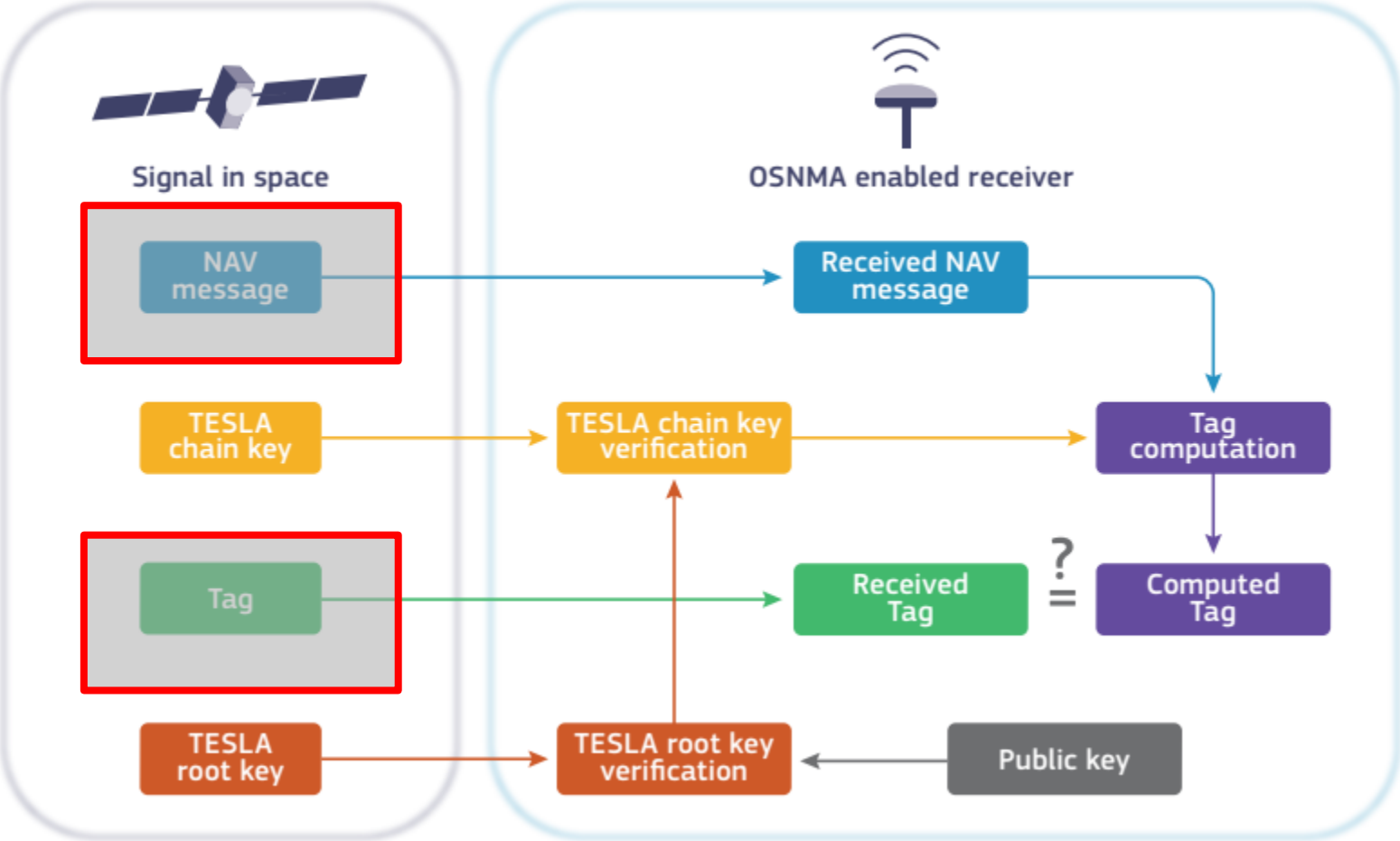
OSNMA Receiver processing logic



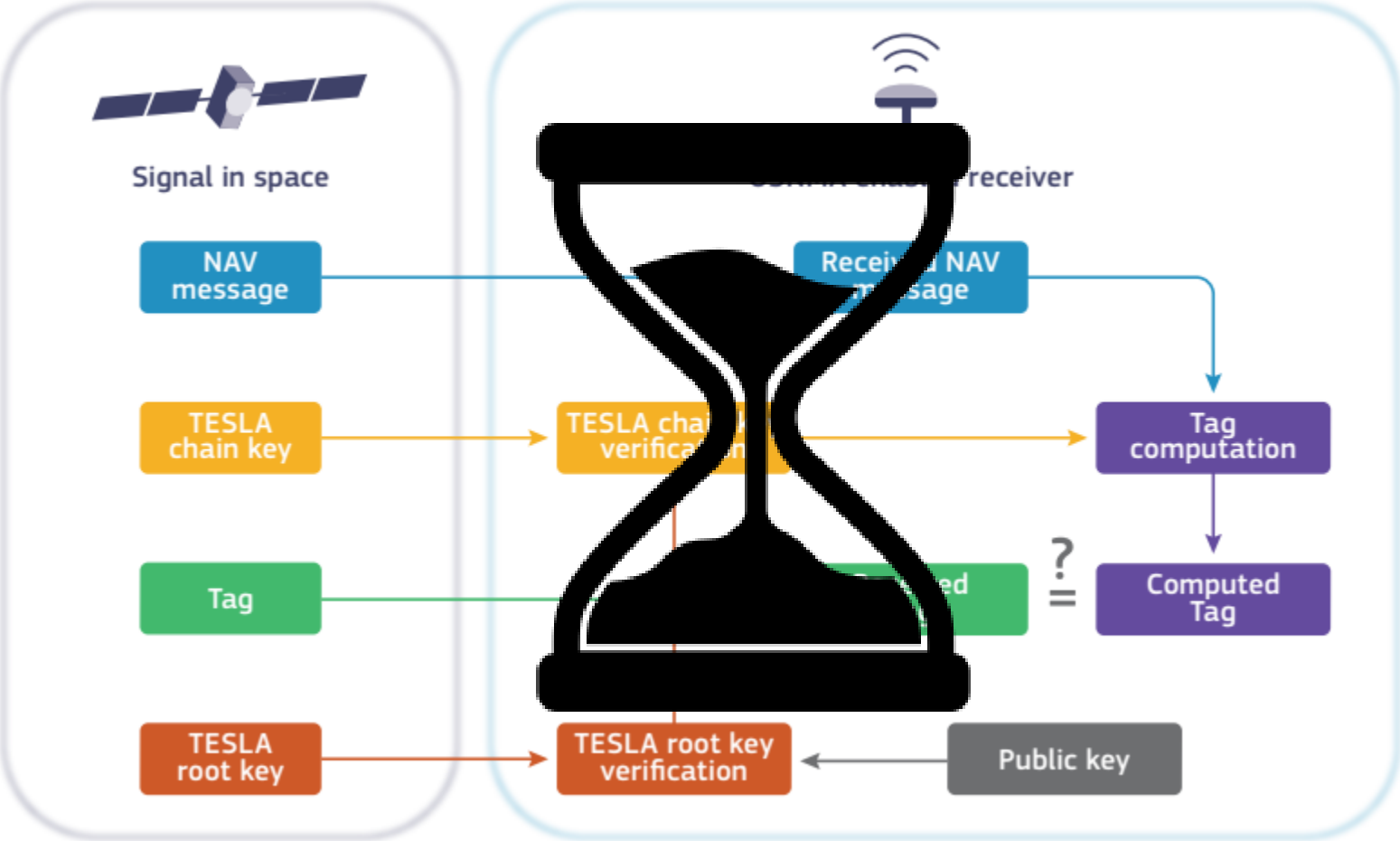
OSNMA Receiver processing logic



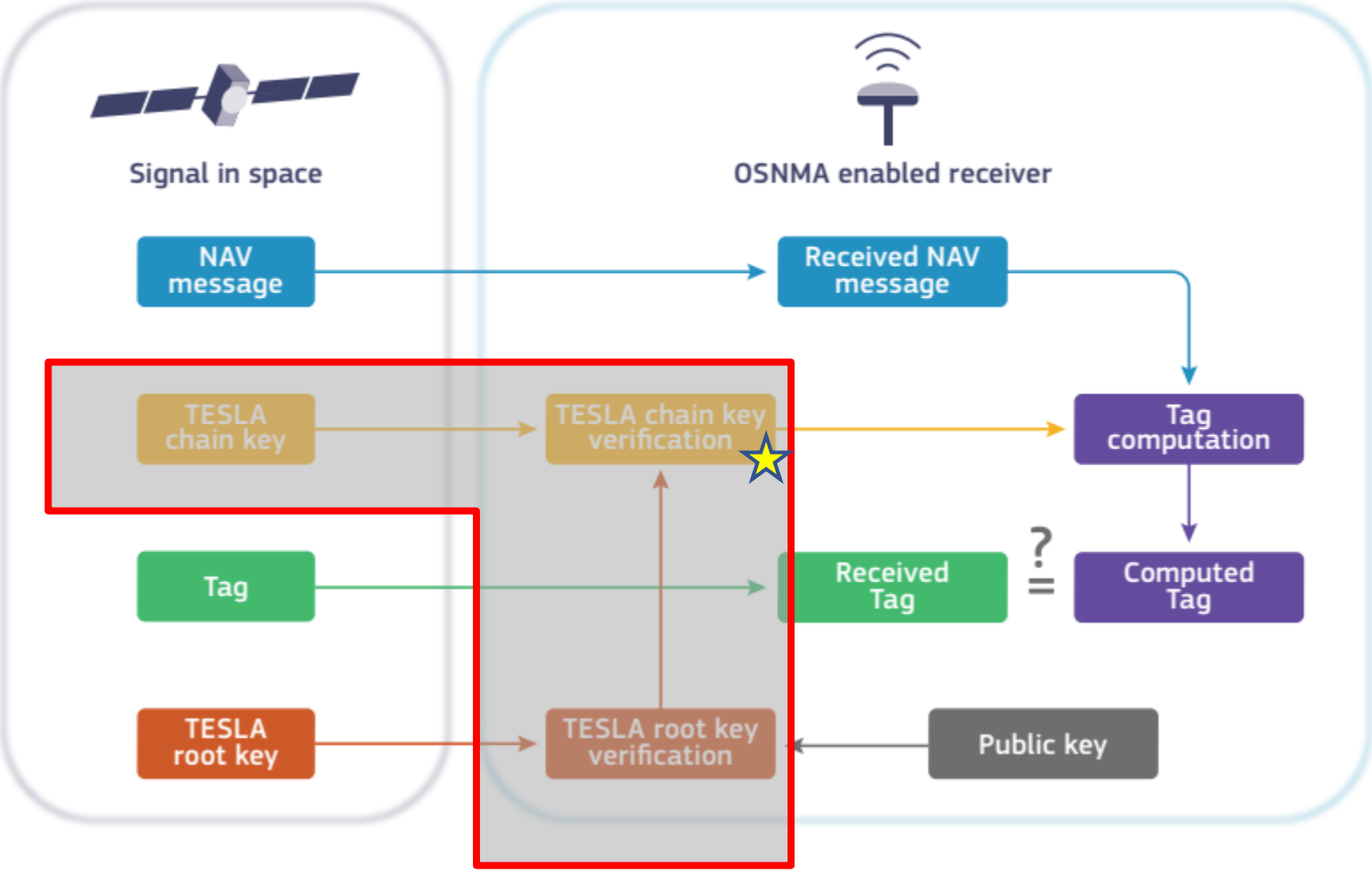
OSNMA Receiver processing logic



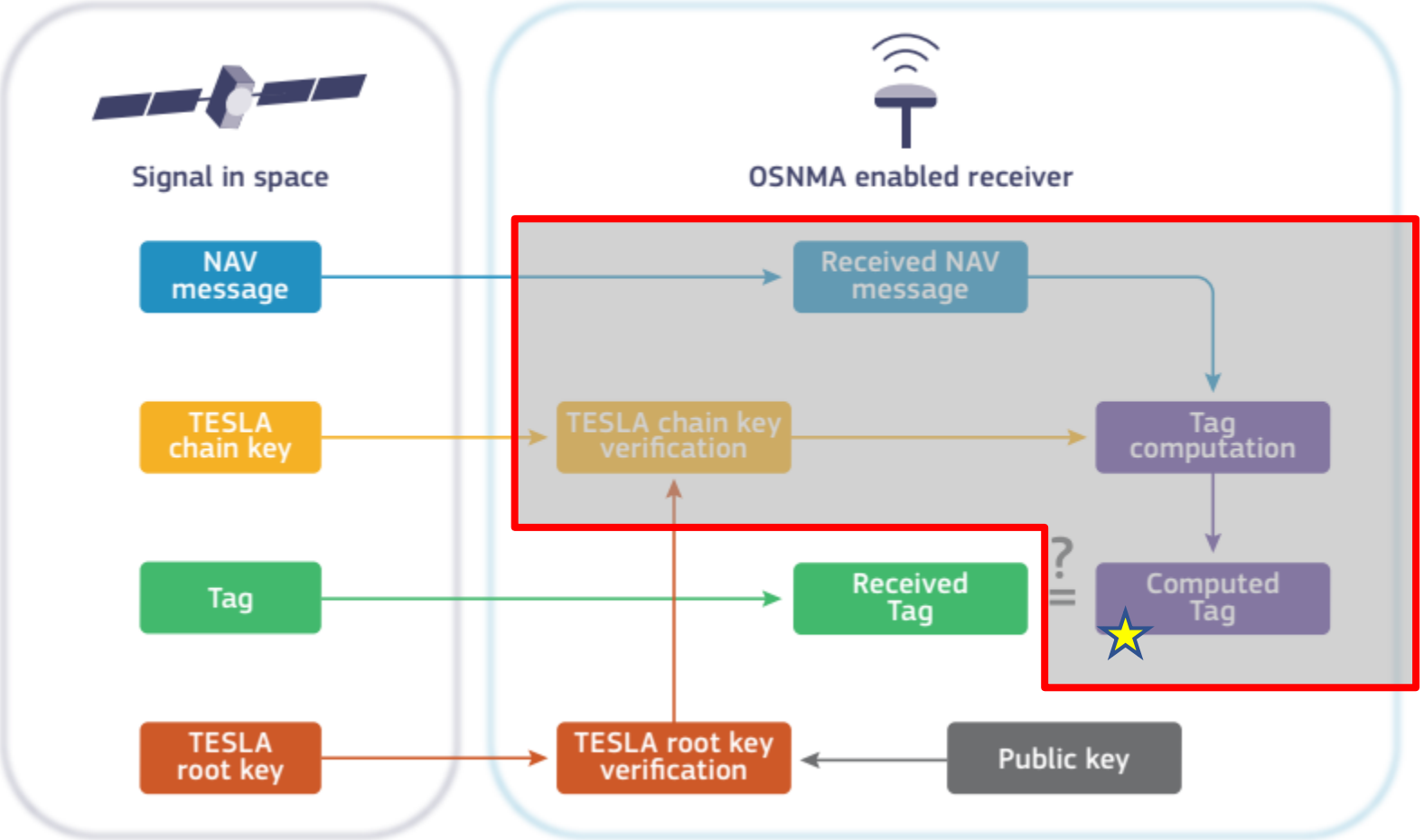
OSNMA Receiver processing logic



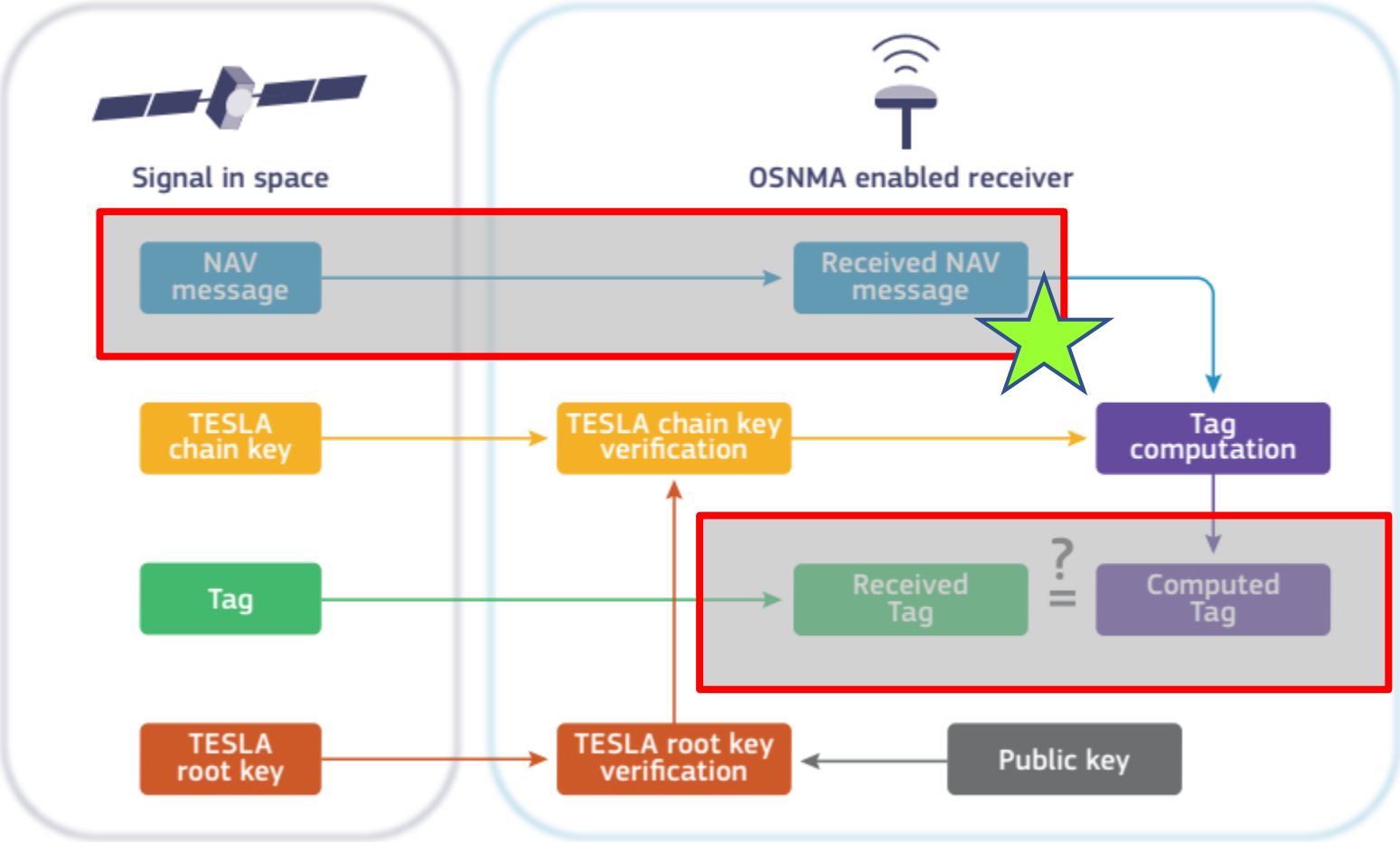
OSNMA Receiver processing logic



OSNMA Receiver processing logic



OSNMA Receiver processing logic

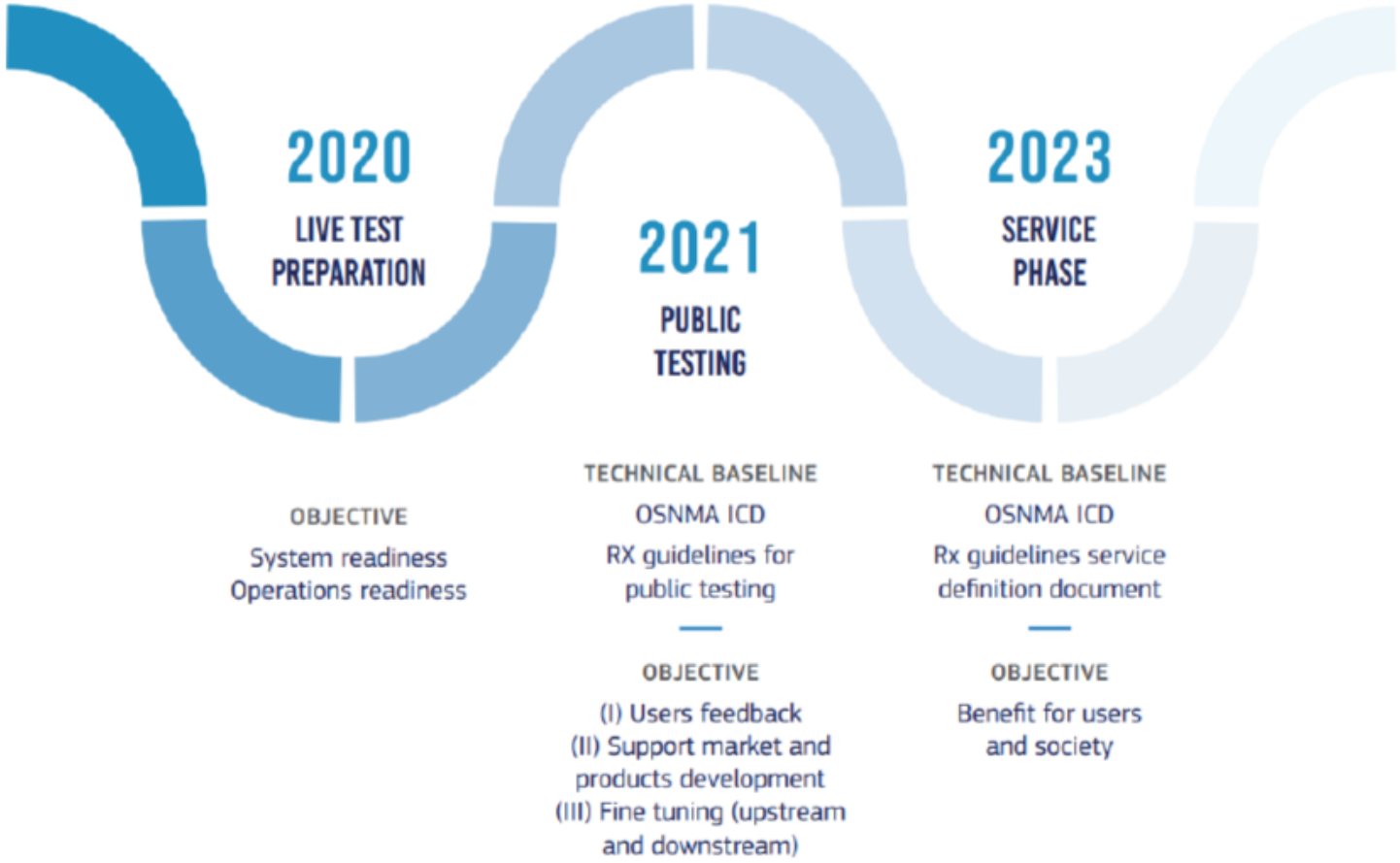


OSNMA current status

- **2014-2020: Studies, design, devpt**
- **2021-2022: Public testing**
- 2023: Service declaration (OSNMA status switch from 'test' to 'operational')

- SIS ICD (test phase), "Info note" and guidelines published*

- SIS reliably transmitted worldwide for almost two years, 1+ year publicly



https://www.gsc-europa.eu/electronic-library/programme-reference-documents#OSNMA

Examples of OSNMA applications

Safety-Critical Applications: OSNMA-secured GNSS positioning to support safety-critical applications, such as in the automotive sector

→ OSNMA included in the EU Digital Tachograph regulation

Telecom: to allow telecom operators to have accurate and consistent time and frequency at distant points of network.

→ Clear interest on GNSS authentication

Insurance telematics: use of GNSS data to increase the fairness of motor insurance for both insurers and subscribers in the frame of usage-based insurance.

→ Liability critical application

More applications can be found in '*Galileo Open Service Navigation Message Authentication (OSNMA) Info Note*', European Union Agency for the Space Programme (EUSPA), 2021.

Some EU projects exploiting OSNMA

PATROL: Development, supply and testing of an **OSNMA user terminal** for **smart tachographs.**

Galileo-based timing platform (TRL7), using OSNMA and EGNOS corrections.

Design, integration and V&V of a shipborne receiver **dual-frequency multi-constellation Galileo OS enabled including OSNMA** and IEC GNSS approval.

Assessment of the benefits introduced by **Galileo authenticated signals** (OSNMA) in the specific context of **synchronisation of 5G telecommunication** networks.

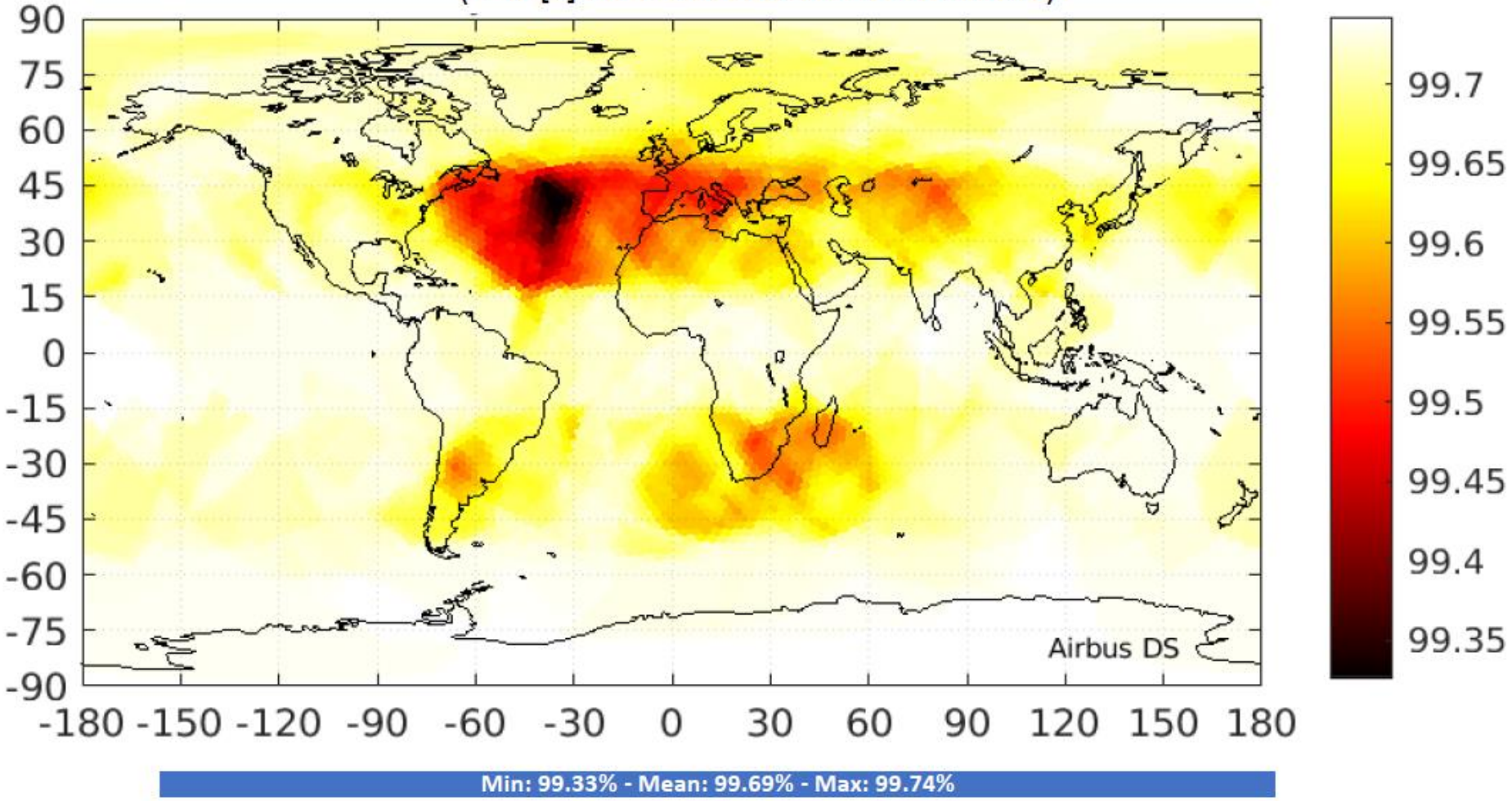
Python 3.8 passing | Python 3.9 passing | Python 3.10 passing

OSNMAlib

Open-source OSNMA library: https://github.com/Algafix/OSNMA

OSNMA availability

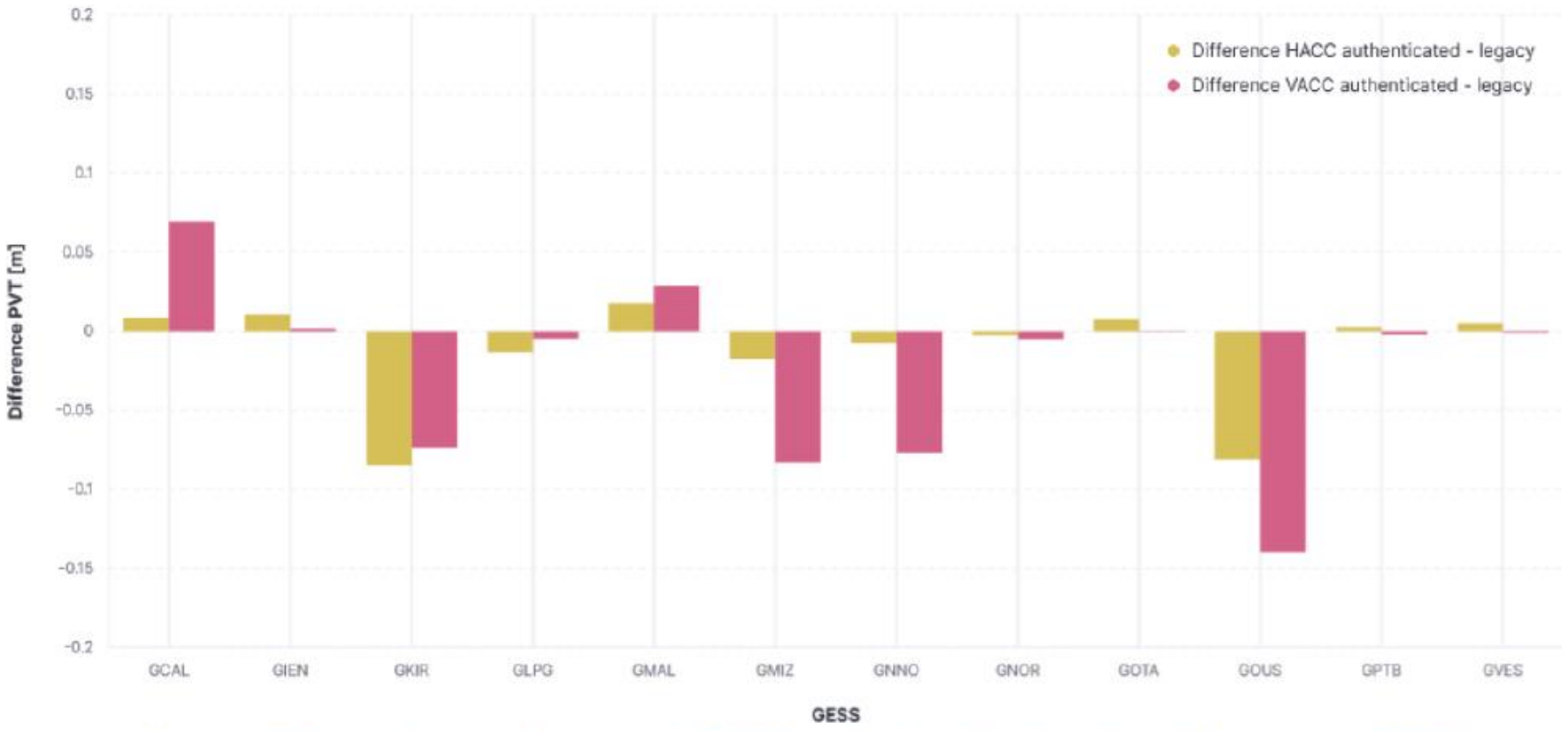
Availability of Tags for Galileo I/NAV orbit & clock data (ADKD0), for target security level and for at least 4 SV in view (120 [s] 80-bit accumulation window)



August 2022

Source: ADS/EUSPA

OSNMA accuracy



Average difference between legacy and OSNMA vertical and horizontal position accuracy (95%) measured at each TGVFx GESS from 1st May until 30th June 2022

Next Steps

- Continue public testing
- Publication of Service ICD (Q4'22/Q1'23). Mostly compatible with current (test) ICD
- Publication of operational cryptographic data to be installed in receivers for the operational phase
- Operational service declaration: 2023 (date TBC EUSPA)
- To be complemented by signal authentication (ACAS) and HAS data authentication in Galileo 1st Generation, then ranging authentication in all frequencies in Galileo 2nd Generation

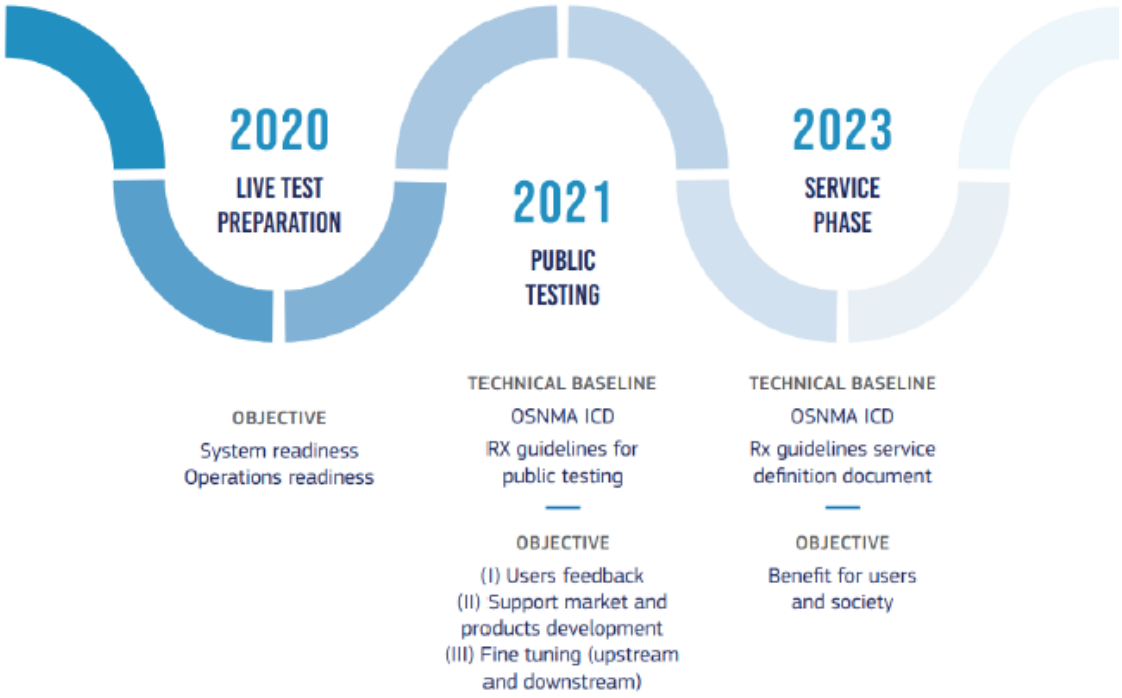
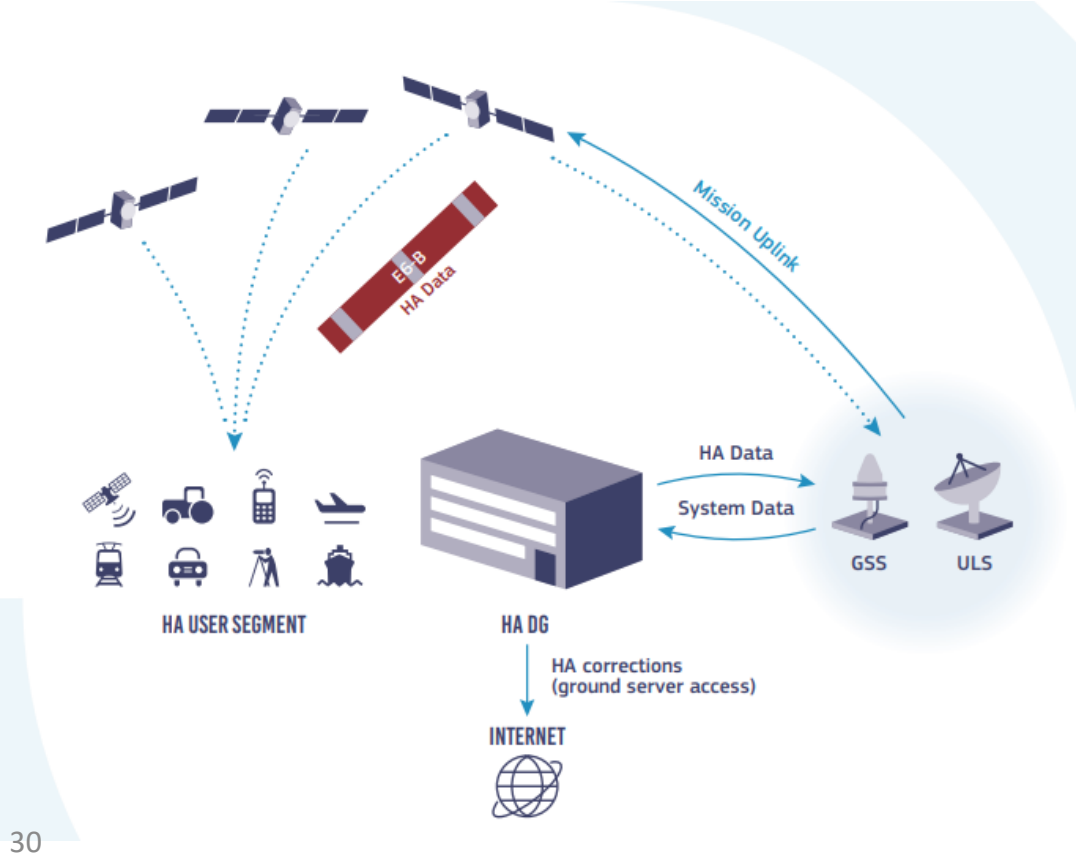


Table of contents

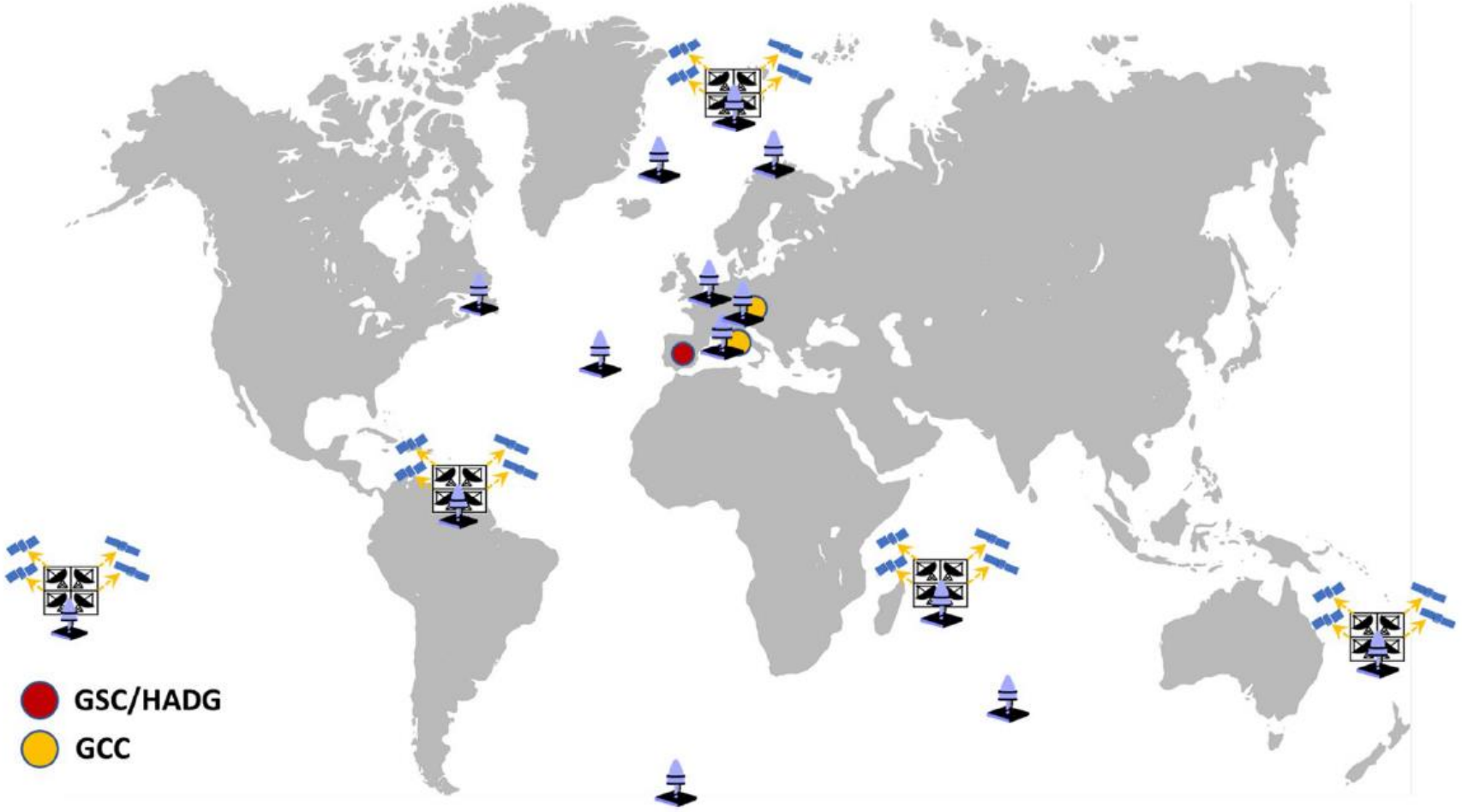
Overview of Galileo HAS

- Galileo HAS provides precise corrections, allowing PPP positioning worldwide and for free
- Corrections provided for orbits, clocks, code biases and phase biases: Galileo I/NAV, E1, E5a,E5b, E6B/C; GPS CNAV, L1C/A, L2C, L2P
- SIS dissemination through E6B (1278.75 MHz) and ground dissemination channel through a real-time connection in RTCM-like format



European Union Agency for the Space Program (EUSPA), "Information Note on Galileo High Accuracy Service," 2020. [Online]. Available: https://www.gsc-europa.eu/sites/default/files/sites/all/files/Galileo_HAS_Info_Note.pdf.

HAS infrastructure



Galileo HAS Phase 1 architecture. The 14 GSS (Galileo Sensor Stations) are depicted with a single antenna, and the five ULS (Up-Link stations) are depicted with four antennas

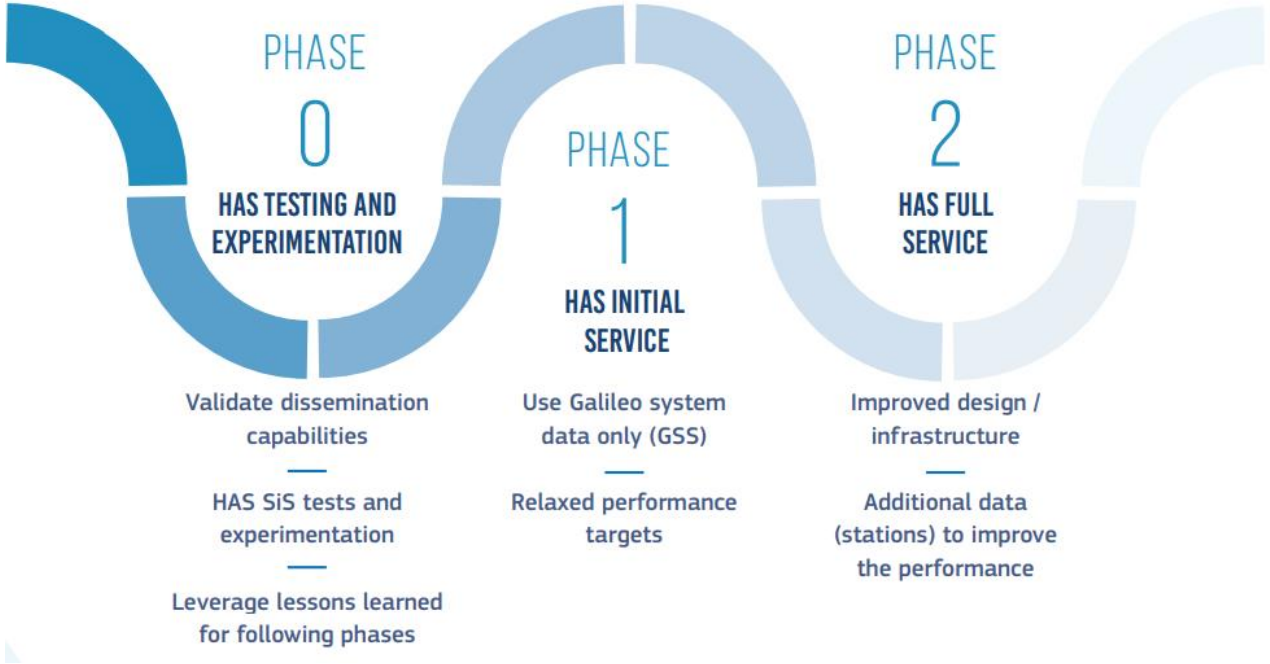
Fernandez-Hernandez, I., et al., "Galileo high accuracy service: initial definition and performance". GPS Solutions, 26(3), 1-18, 2022

HAS current status

- Three phases:
  - Phase 0 (testing)
  - Phase 1 (initial service)
  - Phase 2 (full service)

- Current status: Finishing Phase 0
  - HAS SIS ICD available since May 22*
  - SIS readily available worldwide (HAS Status flag = 'test' mode)

- Initial Service declaration by end2022/early2023



NEW
GALILEO
HAS SIS ICD
PUBLISHED

*https://www.gsc-europa.eu/sites/default/files/sites/all/files/Galileo_HAS_SIS_ICD_v1.0.pdf

Galileo HAS phases and performance targets

	Phase 0 SIS Testing	Phase 1 Initial Service	Phase 2 Full Service
Coverage	EU+	EU+	Global
Clock biases	Y	Y	Y
Phase biases	N	Y	Y
Galileo corrected signals	E1, E5a, E5b, E6	E1, E5a, E5b, E6	E1, E5a, E5b, E5, E6
GPS corrected signals	L1, L2P	L1, L2P, L2C	L1, L2C, L5
Horizontal accuracy requirement 95%	N/A	<20 cm TBC	<20 cm
Vertical accuracy requirement 95%	N/A	<40 cm TBC	<40 cm
Availability	N/A	99% TBC	99%
Convergence time requirement Global, no ionosphere (SL1)	N/A	<300 s TBC	<300 s
EU, Ionosphere corrections (SL2)	N/A	N/A	<100 s
Ground channel	N	Y	Y
Authentication	N	N	Y
Start	2020	2022-23	2024+

HAS message

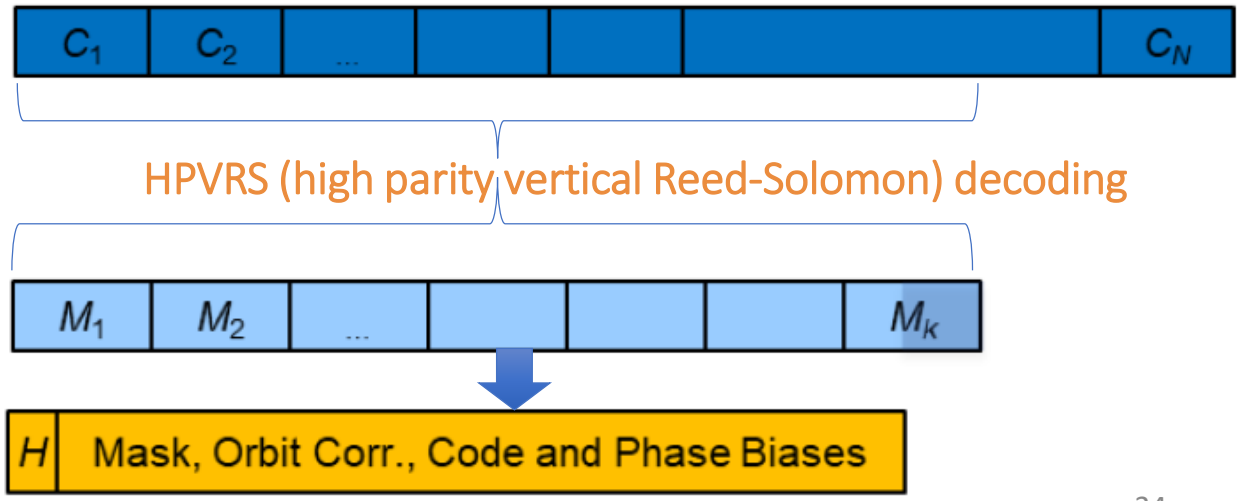
Sync	Symbols
16	984

Total (symbols)
1000

C/NAV Page			
Reserved	HAS Page	CRC	Tail
14	448	24	6

Total (bits)
492

HAS Page	
HAS Page Header	HAS Encoded Page
24	424

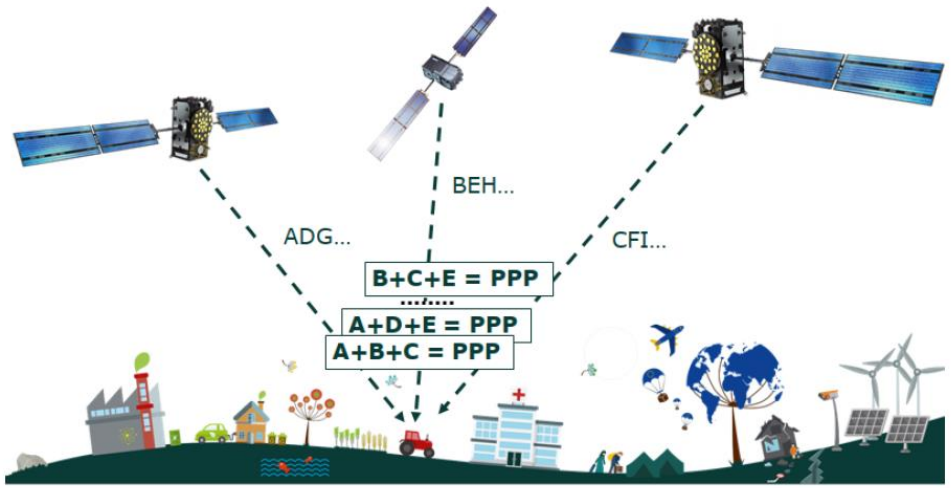


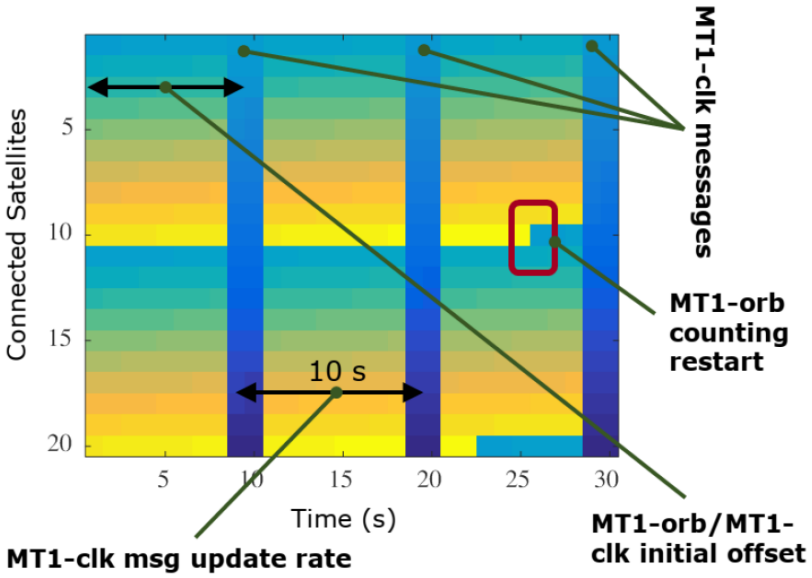
- Current sequence every 10s:
  - 7 “slow” message pages: mask, orbit, CB, PB
  - 2 “fast” message pages: clock
  - 1 dummy message
- Message size independent. Typically 17 pages (“slow”) + 2 pages (“fast”).
- Total: around 8000 bits

Galileo HAS fields (Phase 1)

Correction	Range	Scale factor	Unit	Size (bits)
Orbit: delta radial	± 10.2375	0.0025	m	13
Orbit: delta in-track	± 16.376	0.0080	m	12
Orbit: delta cross-track	± 16.376	0.0080	m	12
Delta clock	– 10.2375 to + 10.2350	0.0025	m	13
Code bias	± 20.46	0.02	m	11
Phase bias	± 10.23	0.01	cycles	11

HAS message reception performance



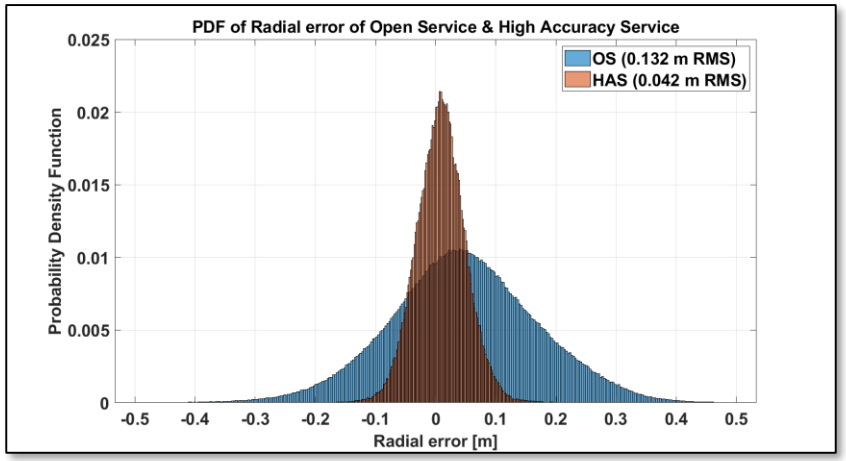


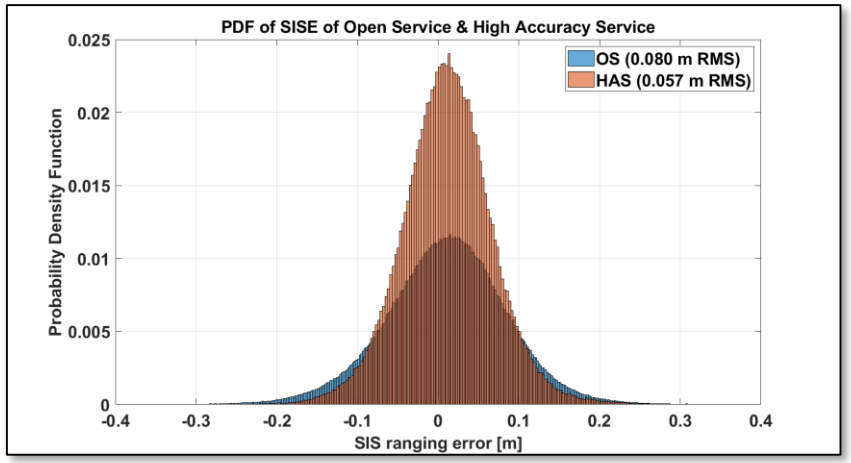
	Mean [s]	Mode [s]	Median [s]	95% Quantile [s]	Max [s]	Min [s]
FEB 27A	8.46	7	8	13	33	6
FEB 27B	8.71	7	7	17	65	4
FEB 28A	11.16	7	8	32	152	4
FEB 28B	7.61	6	6	14	36	5

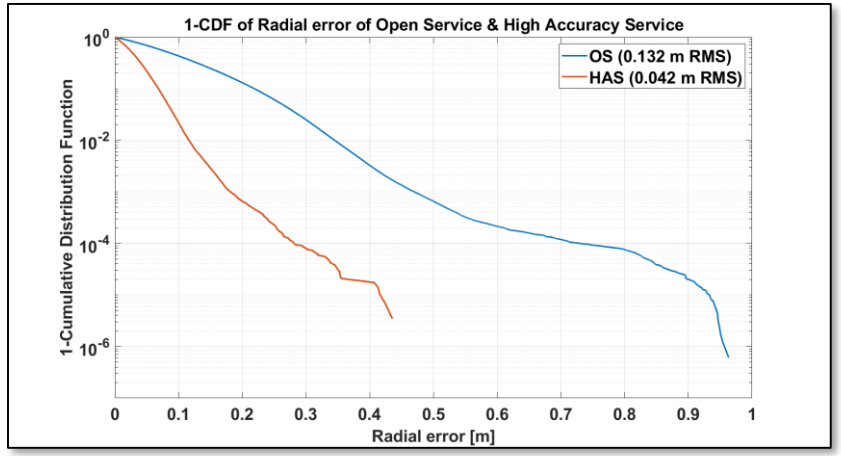
Borio et al., https://insidegnss.com/galileos-high-accuracy-service-field-experimentation-of-data-dissemination-schemes/

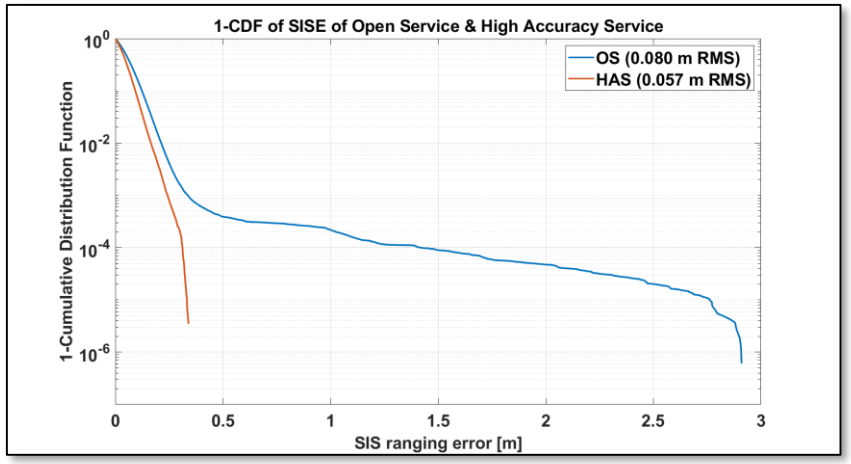
HAS orbit & clock correction accuracy

- HAS orbit and clock with live signals between May 2021 and June 2022
- Septentrio PolaRx5S rx with Trimble Zephyr 2 antenna @JRC EC (Italy)
- HAS broadcast test signals and performance might not be representative of final service ones





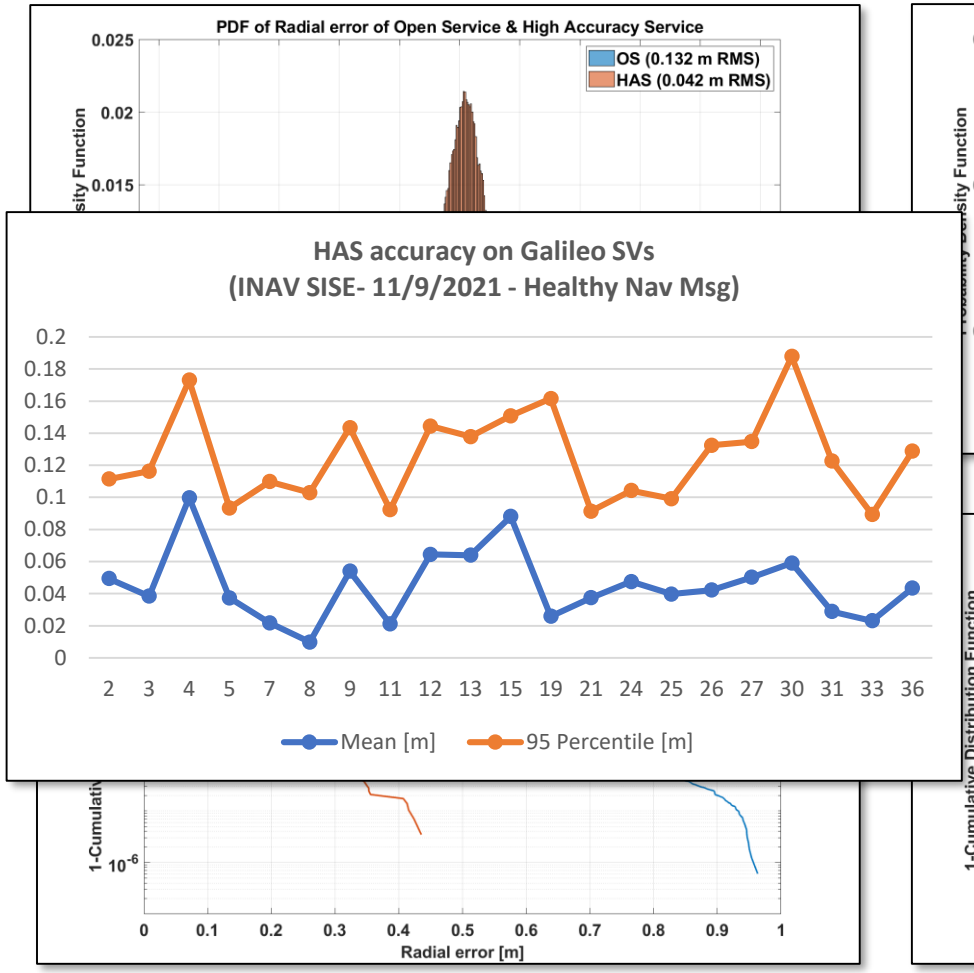


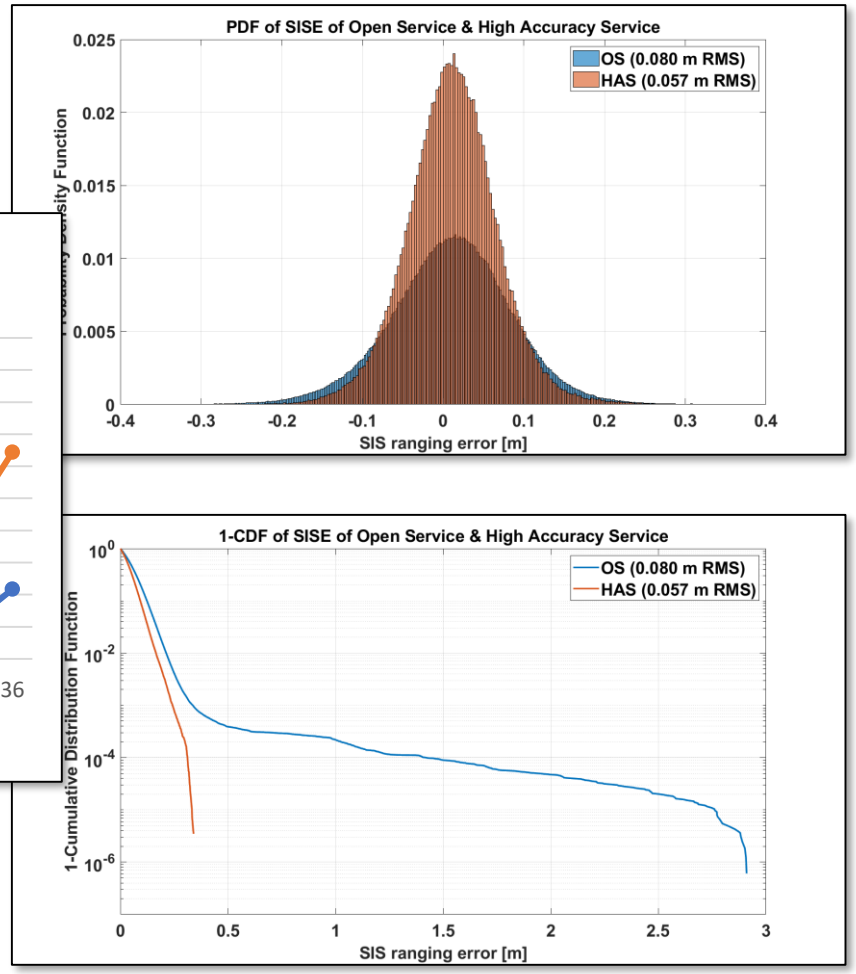


I. Martini, M. Susi, I. Fernandez-Hernandez, "PPP and Galileo High Accuracy Service with Satellite Selection Strategies for Kinematic Applications", IONGNSS+2022

HAS orbit & clock correction accuracy

- HAS orbit and clock with live signals between May 2021 and June 2022
- Septentrio PolaRx5S rx with Trimble Zephyr 2 antenna @JRC EC (Italy)
- HAS broadcast test signals and performance might not be representative of final service ones





I. Martini, M. Susi, I. Fernandez-Hernandez, "PPP and Galileo High Accuracy Service with Satellite Selection Strategies for Kinematic Applications", IONGNSS+2022

HAS PPP user performance

- User PPP accuracy from HAS signal tested worldwide
- Conditions: static, open sky (GMV's monitoring network)
- Performance measured in stationary mode <u>after convergence</u>
- RMS and 95th percentile of errors from 6 days: 31/8-6/9
- PPP configuration used:
  - Multiconstellation GAL+GPS
  - Double frequency E1-E5a and L1C/A-L2CL (Iono-free + ionospheric estimation)
  - PPP float

A. Chamorro, et al. "Early Demonstration of Galileo HAS user Performances", IONGNSS+ 2022

HAS PPP user performance

Europe & Africa	Errors RMS (cm)		
	North	East	Height
SPTR	4.5	6.6	13.8
ROBU	5.7	6.6	14.0
SWOJ	6.5	6.1	14.6
NAWI	4.0	5.3	14.4

Europe & Africa	Errors p95 (cm)	
	Horizontal	Vertical
SPTR	19.5	26.5
ROBU	17.3	26.8
SWOJ	13.5	28.3
NAWI	18.1	25.3

America	Errors RMS (cm)		
	North	East	Height
USNA	6.0	8.3	17.5
CABU	6.1	9.0	21.9
CHSA	8.8	13.7	24.0
FRTA	9.1	9.7	24.2

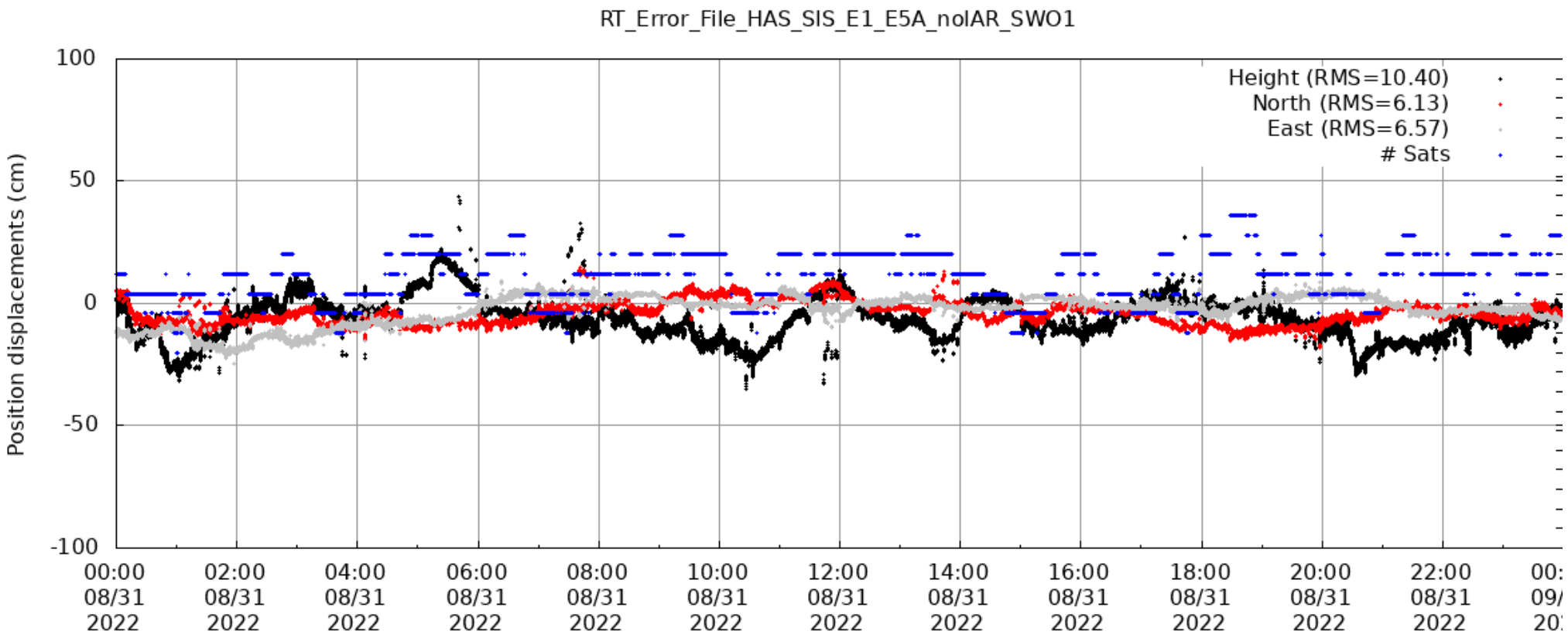
America	Errors p95 (cm)	
	Horizontal	Vertical
USNA	19.8	32.9
CABU	21.4	38.1
CHSA	26.5	36.1
FRTA	27.0	40.7

Asia	Errors RMS (cm)		
	North	East	Height
INKO	5.8	8.7	21.8
TATA	8.6	15.9	27.0

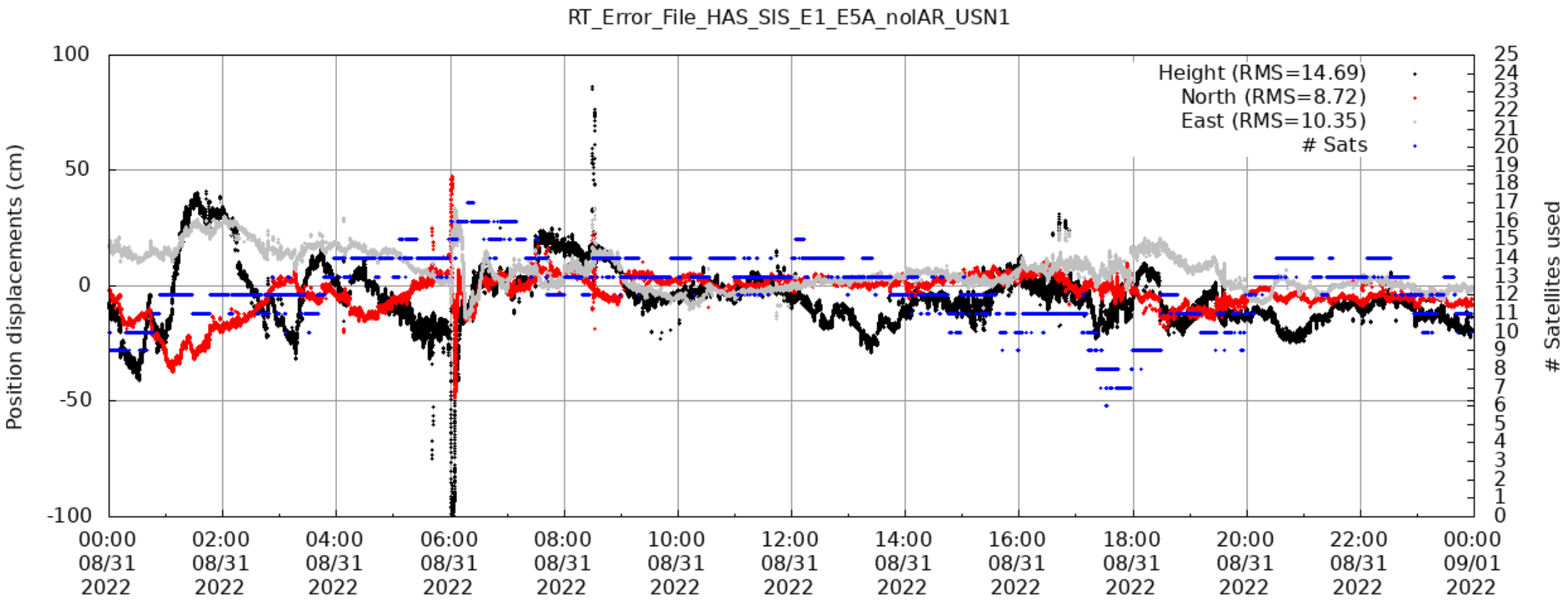
Asia	Errors p95 (cm)	
	Horizontal	Vertical
INKO	19.1	35.7
TATA	33.1	52.2

A. Chamorro, et al. "Early Demonstration of Galileo HAS user Performances", IONGNSS+ 2022

HAS user PPP, Sweden

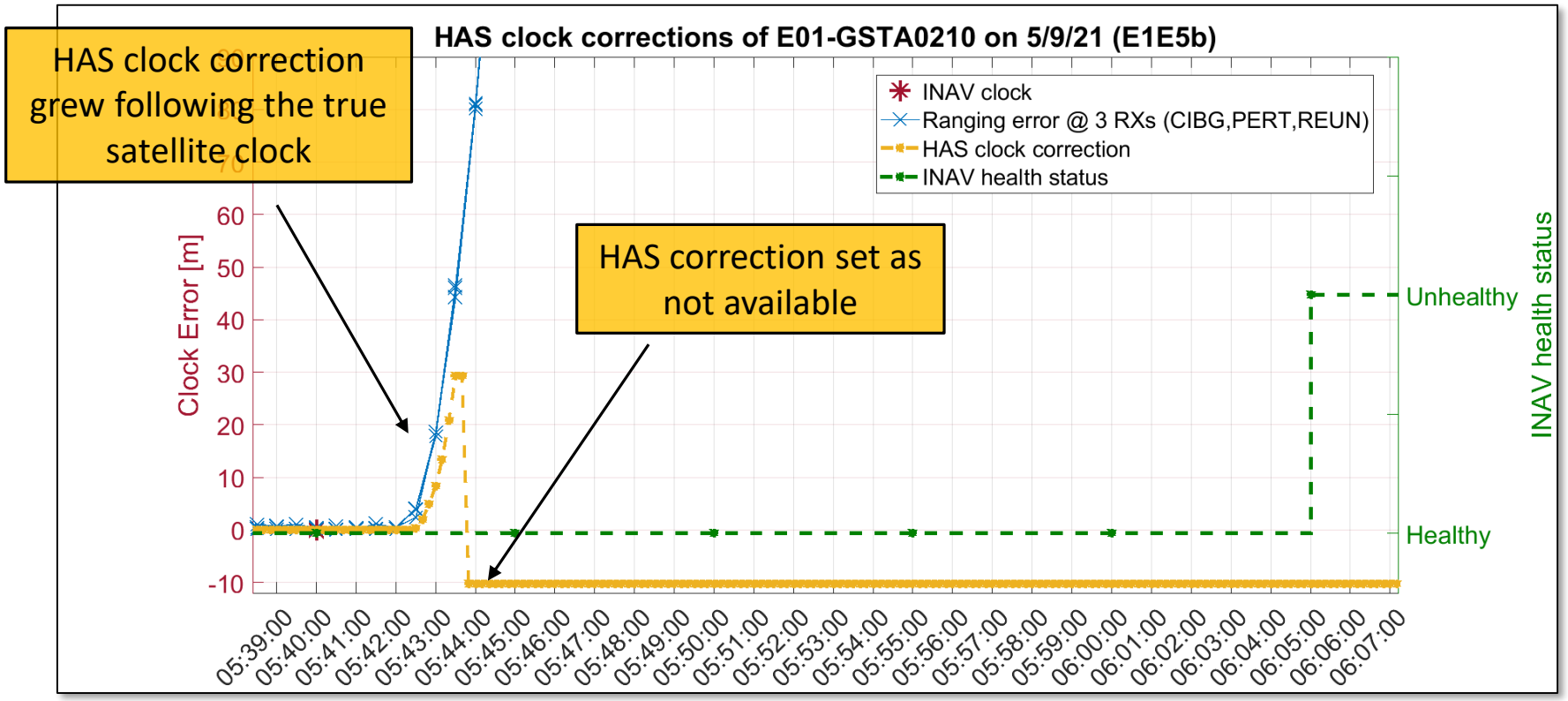


HAS user PPP, US



HAS and fault detection (not integrity!)

- If the HAS correction value grows and shows a degradation of the orbit and/or clock error, the user excludes the satellite to avoid impact on the position performance
- In addition, the HAS message informs the user that the satellite shall not be used

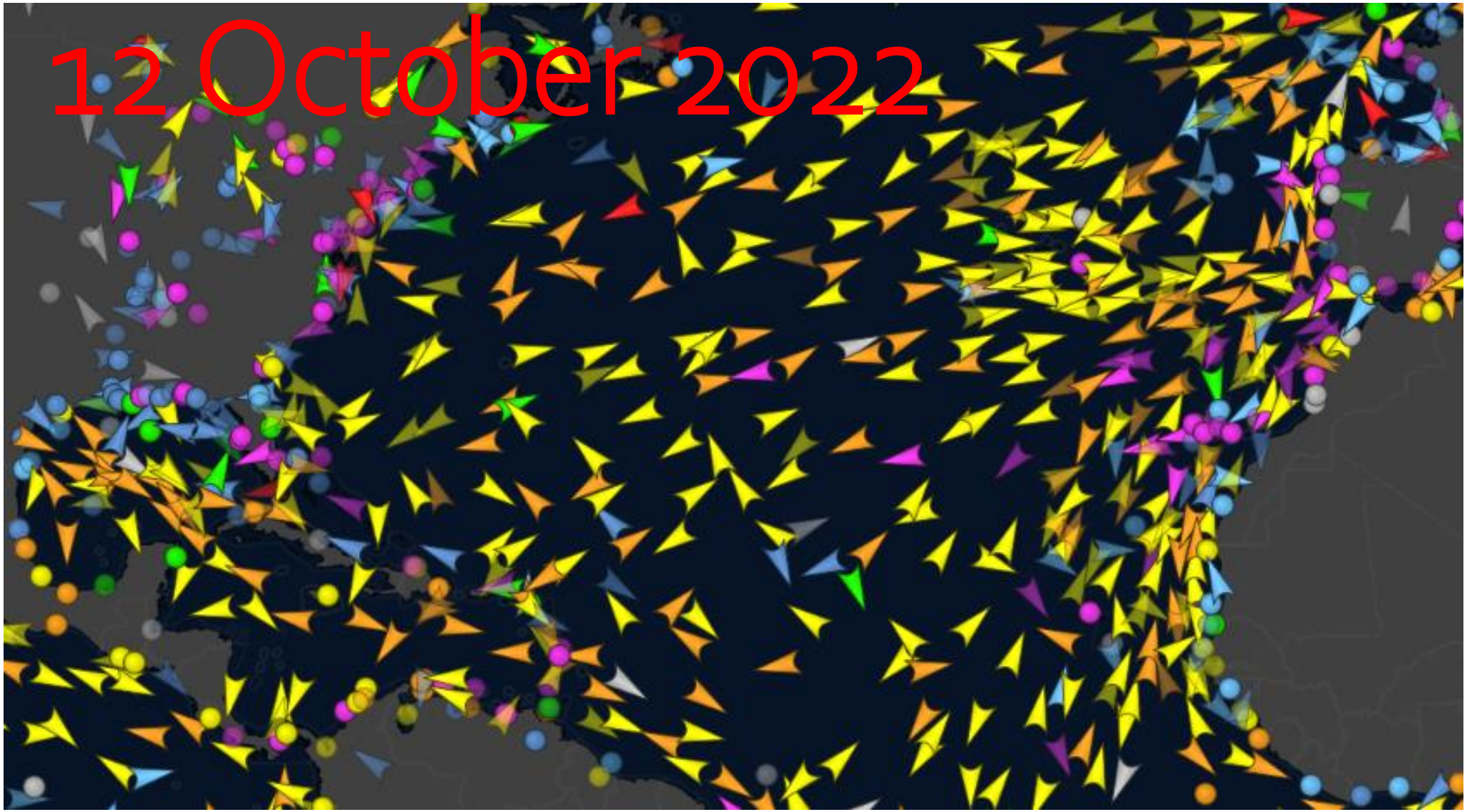


I. Martini et al. "Satellite Anomaly Detection with PPP Corrections: A Case Study with Galileo's High Accuracy Service" ION ITM January 2022

Summary

- Galileo, the European GNSS, is providing global coverage with very good performance for the last years
- In addition, OSNMA and HAS already transmitted freely and worldwide, and to be officially declared next year
- OSNMA offers data authentication and signal unpredictability for Galileo. It is a pioneering, long awaited feature to protect against spoofing
- HAS is a PPP corrections service for GPS/Galileo. Aiming at 20/40cm 95% accuracy
- Next step: spreading code authentication in E6

12 October 1492


12 October 2022

EU SPACE

Thank you for your attention

Authentication and other new services on Galileo

Ignacio Fernández Hernández
European Commission

Acknowledgements: Galileo OSNMA/HAS teams (EC, EUSPA, ESA, PAULA, HADG, GSC…)