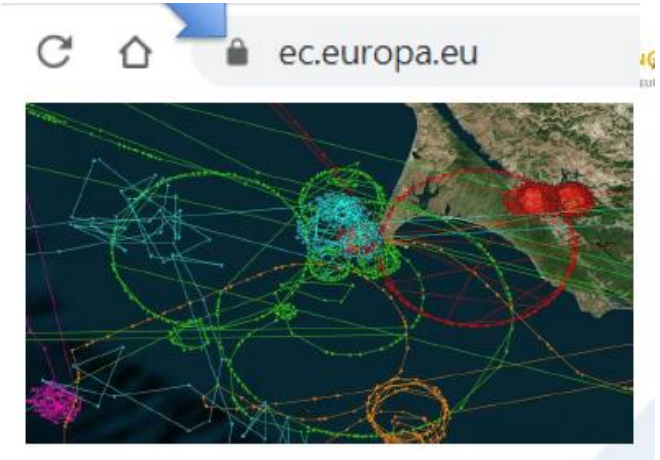
Towards more resilient GNSS

Current use of GNSS

Civil aviation uses exclusively GPS L1 signal + SBAS / GBAS for most demanding Navigation applications → DFMC is still to come

But GNSS signals have low power and hence can be disrupted:

- **Jamming**: intentional interference → loss of availability
- **Spoofing**: fake GNSS signals → potential loss of integrity



GNSS disruptions have been increasing over the last years

More resilient GNSS is a **multi-facet effort**

EU SPACE

Measures to improve GNSS resilience

Panoply of measures to improve GNSS resilience:

1. More resilient GNSS signals <u>and</u> data → Authentication, encryption
2. Use of multi-constellation, multi-frequency GNSS signals
3. Better detection, mitigation and localization of RFI (RF interference) threats
4. Keep and use alternative solutions → MON, Alternative-PNT

Measures to improve GNSS resilience

Panoply of measures to improve GNSS resilience:

1. More resilient GNSS signals and data → Authentication, encryption
2. Use of multi-constellation, multi-frequency GNSS signals
3. Better detection, mitigation and localization of RFI threats
4. Keep and use alternative solutions → MON, Alternative-PNT

GNSS signals and data

Most **digital data** we use everyday is ***protected*** *(e.g. Internet connection to your bank)*

GNSS signals and data are not protected and hence are easy to falsify

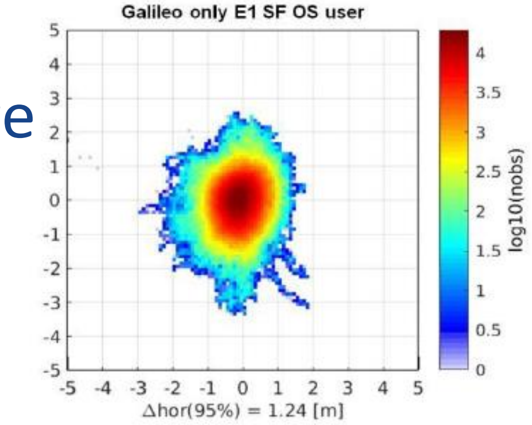
GNSS signals and data **will include authentication and encryption**:

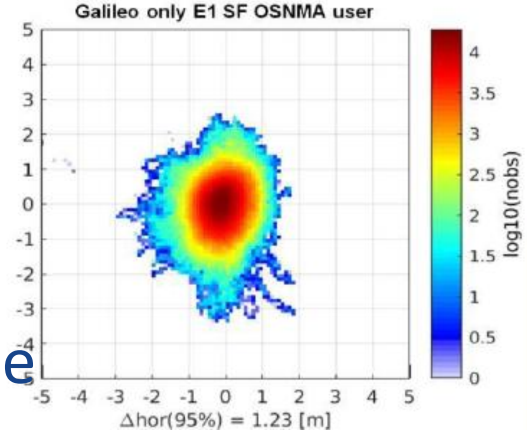
- Galileo OS-NMA, CAS/SAS, GPS III
- DFMC SBAS authentication

Galileo OS NMA

Galileo Open Service – **Navigation Message Authentication**

- It is a **data authentication mechanism** of the Navigation Message (satellite orbits, clocks, time, etc) that allows a GNSS receiver to verify its authenticity and of the entity transmitting it.
- **No degradation of OS PVT accuracy**; Asymmetric cryptography (i.e. public key for user)
- OS NMA signal-in-space already available (“public observation phase”). OSNMA **service declaration in 2023**.
- GPS is considering including authentication feature in GPS-III SVs.
- Galileo OSNMA was presented at ICAO NSP JWGs/9 meeting (June 2022). The goal is to **standardise together with SBAS Authentication.**



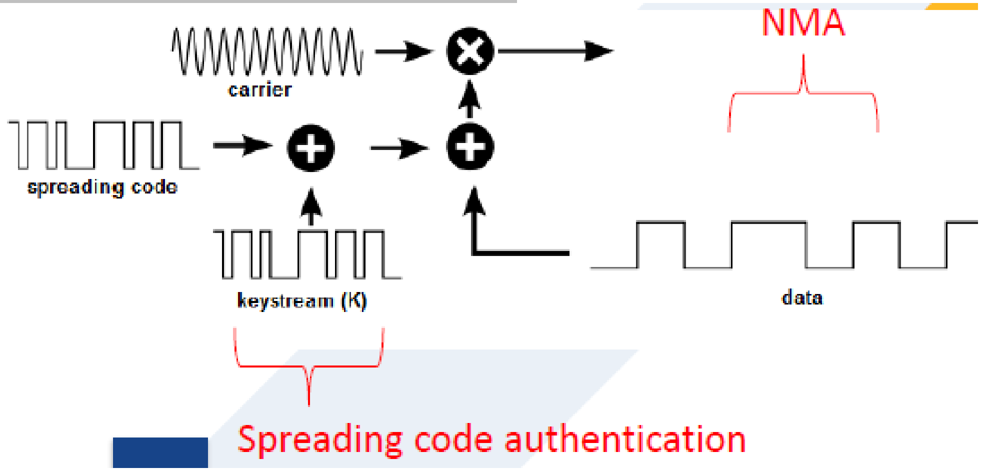


Galileo CAS / SAS

Galileo CAS/SAS stands for **Commercial/Signal Authentication Service**

- It is a **spreading code authentication** mechanism to authenticate the range measurement.
- It will be based on existing signals (E6C) and services (OS NMA).

Due to its frequency band (E6C), **not planned for use in aviation.**



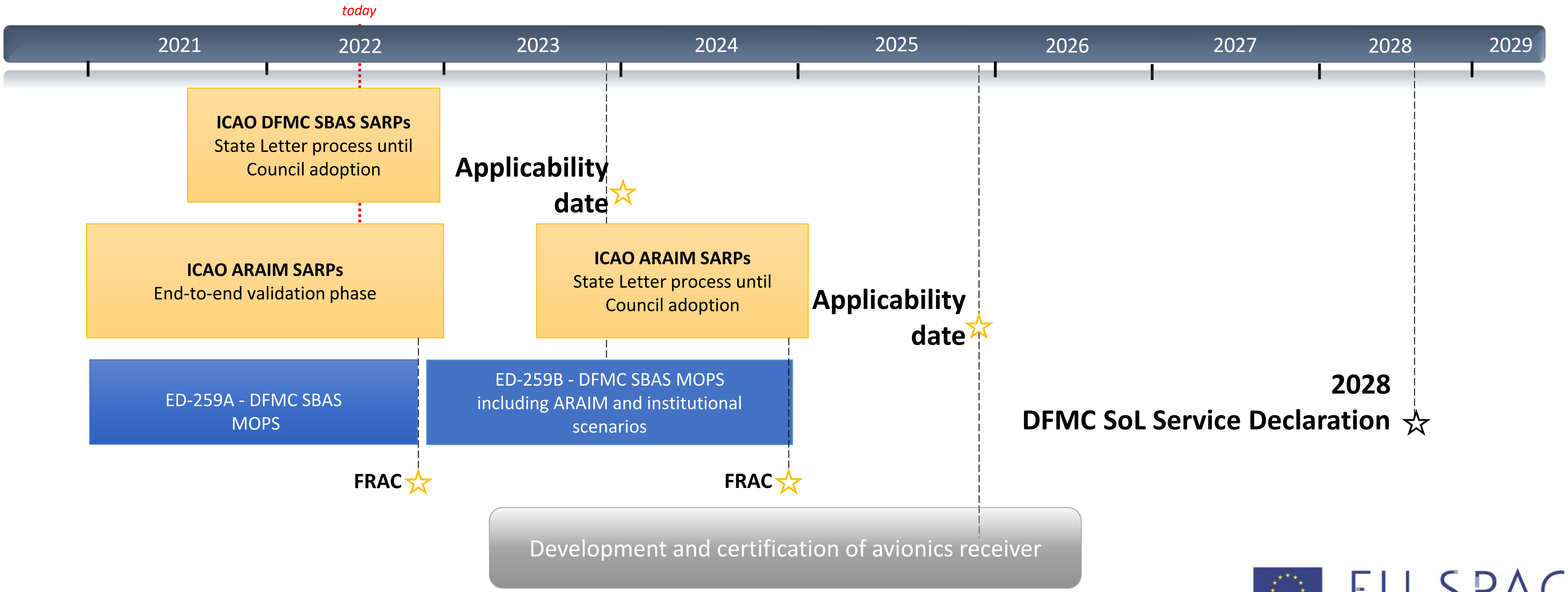
Measures to improve GNSS resilience

Panoply of measures to improve GNSS resilience:

1. More resilient GNSS signals <u>and</u> data → Authentication, encryption
2. Use of Multi-constellation, multi-frequency GNSS signals
3. Better detection, mitigation and localization of RFI threats
4. Keep and use alternative solutions → MON, Alternative-PNT

Multi-constellation, multi-frequency (DFMC)

Timeline – DFMC SBAS Standardisation activities



today

2021
2022
2023
2024
2025
2026
2027
2028
2029

ICAO DFMC SBAS SARPs
State Letter process until
Council adoption

Applicability date ☆

ICAO ARAIM SARPs
End-to-end validation phase

ICAO ARAIM SARPs
State Letter process until
Council adoption

Applicability date ☆

ED-259A - DFMC SBAS MOPS

ED-259B - DFMC SBAS MOPS including ARAIM and institutional scenarios

FRAC ☆

FRAC ☆

2028
DFMC SoL Service Declaration ☆

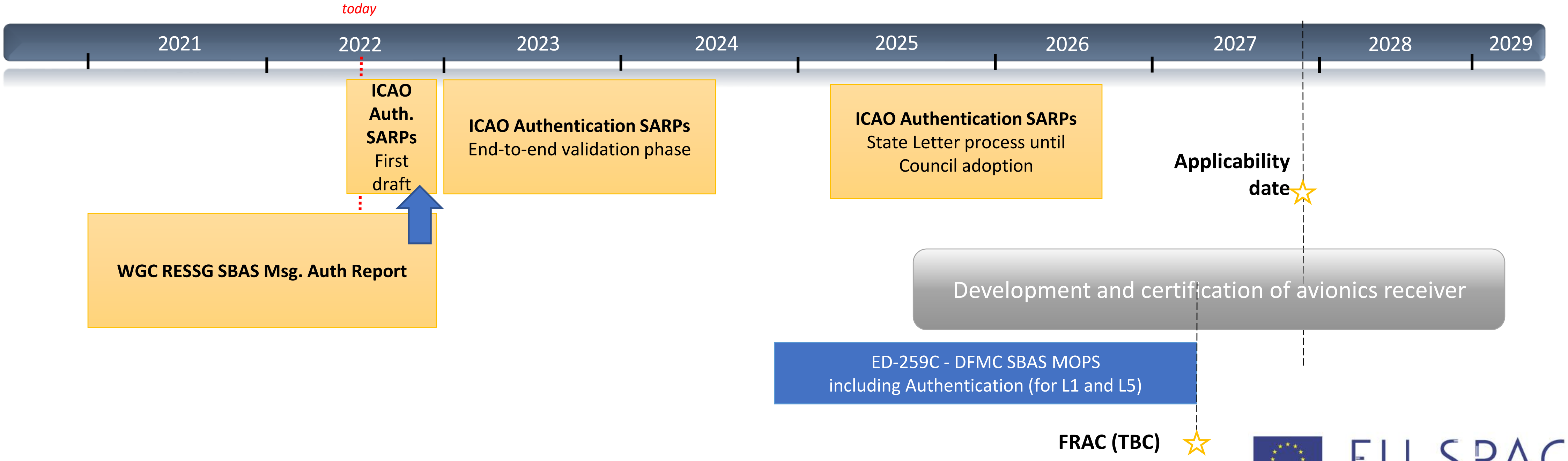
Development and certification of avionics receiver

EU SPACE

DFMC SBAS including Authentication

Work ongoing on SARPs development and validation, CONOPS finalization, risk analysis, and key management.

Implementation optional for SBAS Service Provider, L1 and L5.



ICAO Auth. SARPs First draft

ICAO Authentication SARPs End-to-end validation phase

ICAO Authentication SARPs State Letter process until Council adoption

Applicability date

WGC RESSG SBAS Msg. Auth Report

Development and certification of avionics receiver

ED-259C - DFMC SBAS MOPS including Authentication (for L1 and L5)

FRAC (TBC)

EU SPACE

Measures to improve GNSS resilience

Panoply of measures to improve GNSS resilience:

1. More resilient GNSS signals and data → Authentication, encryption
2. Use of multi-constellation, multi-frequency GNSS signals
3. Better detection, mitigation and localization of RFI threats
4. Keep and use alternative solutions → MON, Alternative-PNT

Assessment to improve GNSS resilience

DG DEFIS project **AIRING** (end Q1 2023) objectives: identify and assess RFI threats on GNSS signals and the resulting risks:

- Several **techniques** are being reviewed to detect, mitigate and localize RFI threats (**on-board**, **on ground**, **in space**) → lab testing and live demos.
- Propose reqs for GNSS standards, monitoring means and reporting.
- Develop a **CONOPS** with mitigation actions and contingency plans for operational stakeholders (ATCOs, ANSPs, Pilots, Network Manager, etc.).
- Selected (most promising) techniques will **reduce impact on operations**.

Assessment to improve GNSS resilience

Conclusions of AIRING in developing the CONOPS so far:

- Coordination procedures should be defined/established between stakeholders (mainly with involved ANSPs).
- ATC should handle these operational events even if they are unlikely.
- The **GNSS RFI detection time is key** (especially for GNSS misleading info).
- Surveillance and Communications should **not use only GNSS for timestamping**.
- Operations based on GNSS (PBN IR) → MON as contingency measure

Measures to improve GNSS resilience

Panoply of measures to improve GNSS resilience:

1. More resilient GNSS signals and data → Authentication, encryption
2. Use of multi-constellation, multi-frequency GNSS signals
3. Better detection, mitigation and localization of RFI threats
4. Keep and use alternative solutions → MON, Alternative-PNT

MON / Alternative PNT

Alternative PNT for aviation already exists and needs to be maintained for contingency operations (MON)

In addition, DG DEFIS is assessing PNT services independent from GNSS:

- Seven technologies (also non-EU) demonstrated for DEFIS (Demo Day took place on 18 May) → not suited / standardised for aviation.
- **European Radio Navigation Plan v2** will include recommendations for resilient PNT services (general recommendations, not focused to dedicated markets)

EU SPACE

BACK-UP SLIDES

Assessment to improve GNSS resilience

Both impact and contingency plans depend on GNSS status.

(Example) Major impact for GNSS misleading (spoofing):

NAVIGATION	COMMs	SURVEILLANCE	CONTINGENCY OPs	IMPACT
RNAV 10, 5, 1 operations → Still possible based on other sensors RNP 1 operations, RNP APCH procedures, GLS procedures → Not usable	• VHF/UHF/HF without impact • CPDLC → Depends on the duration of the interference	• ADS-B and MLAT unusable • Primary and Secondary Radars still usable → Depends on the area of the interference	• Aircraft GNSS only → Vectored by ATC / Use conventional procedures /Alternative aerodrome • Increase aircraft separation (no nominal procedures) • Use only PSR and SSR for surveillance • Use only VHF/UHF/HF for communication	• ATC workload increase → Manage aircraft only RNP APCH capable / Radar vectoring • Onboard monitoring increase • Aircraft only RNP APCH capable should land visually • AD capacity reduction • Potential safety impact

WGC-RESSG (EU-US Resilience Subgroup)

- **EU-US Cooperation Agreement** includes WGC, for the development of system/service evolutions.
- WGC includes the Resilience Subgroup (RESSG), with focus on:
  - **GNSS RFI detection/mitigation technical solutions and standards**
  - Alternative PNT
  - Aviation prioritized, but other communities also treated.
- Forum to discuss latest developments on resilience in EU-US: R&D, programs/projects, operations, policy, etc.
- Some WGC-RESSG concrete outcomes:
  - Jamming/Spoofing framework proposal for aviation (J1-4/S1-7)
  - Report on interference monitoring capabilities
  - SBAS Message Authentication report (under finalisation).

EU SPACE

ignacio.alcantarilla-medina@ec.europa.eu