



Galileo High Accuracy and Authentication Services for Terrestrial Applications

ITSNT – ENAC – 15/11/2018

Ignacio Fernández Hernández



TABLE OF CONTENTS

- Introduction
- High Accuracy Service
- Authentication Services
- Roadmap
- Conclusions

TABLE OF CONTENTS

- **Introduction**
- High Accuracy Service
- Authentication Services
- Roadmap
- Conclusions

Introduction and Background



2013: Feasibility study for adding other services to Galileo baseline (SoL "reprofiled") and define the Commercial Service.

2017: EU Decision to add the following services:

- **A High Accuracy Service (HAS),** initially at a fee, and in 2018 decided to be offered **for free.**
- **Open Service Navigation Message Authentication (OSNMA):** It consists of ensuring the authenticity of navigation data. Estimated cost of implementation and 10-year operation of NMA < **0.2%** of total Program cost.
- **Commercial Authentication Service (CAS):** access-controlled and provided at a fee. Based on the spreading code encryption of E6C (pilot) plus some ancilliary data in E6B/E1B (incl. OSNMA)

COMMISSION IMPLEMENTING DECISION

setting out the technical and operational specifications allowing the commercial service offered by the system established under the Galileo programme to fulfil the function referred to in Article 2(4)(c) of Regulation (EU) No 1285/2013 of the European Parliament and of the Council

	CS high accuracy	CS authentication	
		Specifications common to the OS and the CS: Authentication of geolocation information	Specifications specific to the CS: Authentication through encrypted codes
General specifications	Provision of high-accuracy data to obtain positioning errors of less than one decimetre in nominal utilisation conditions	Provision of authentication data for OS geolocation information contained in the signals	Authentication of signals through access to encrypted codes contained in the signals
Components of the signals used	E6, component E6-B (data) for the supply of high-accuracy data	E1, component E1-B for the authentication data for OS geolocation information	E6, component E6-B for the access data to the encrypted codes and component E6-C (pilot)
User segment specifications	High-accuracy positioning obtained from the precise positioning algorithms integrated into the receiver and using data transmitted in the signals	Authenticity of the data verified by an asymmetrical cryptography protocol and transmitted in the signals and a public cryptographic key	Authenticity of the signals verified by decrypting the signal encrypted using a private cryptographic key
Geographical coverage	Global	Global	Global

Introduction and Background



2013: Feasibility study for adding other services to Galileo baseline (SoL "reprofiled") and define the Commercial Service.

2017: EU Decision to add the

- **A High Accuracy Service** and in 2018 decided to
- **Open Service Navigation Authentication (OSNMA)** the authenticity of navigation data at a cost of implementation **NMA < 0.2%** of total P
- **Commercial Authentication** access-controlled and on the spreading code encryption of E6C (pilot) plus some ancilliary data in E6B/E1B (incl. OSNMA)



COMMISSION IMPLEMENTING DECISION

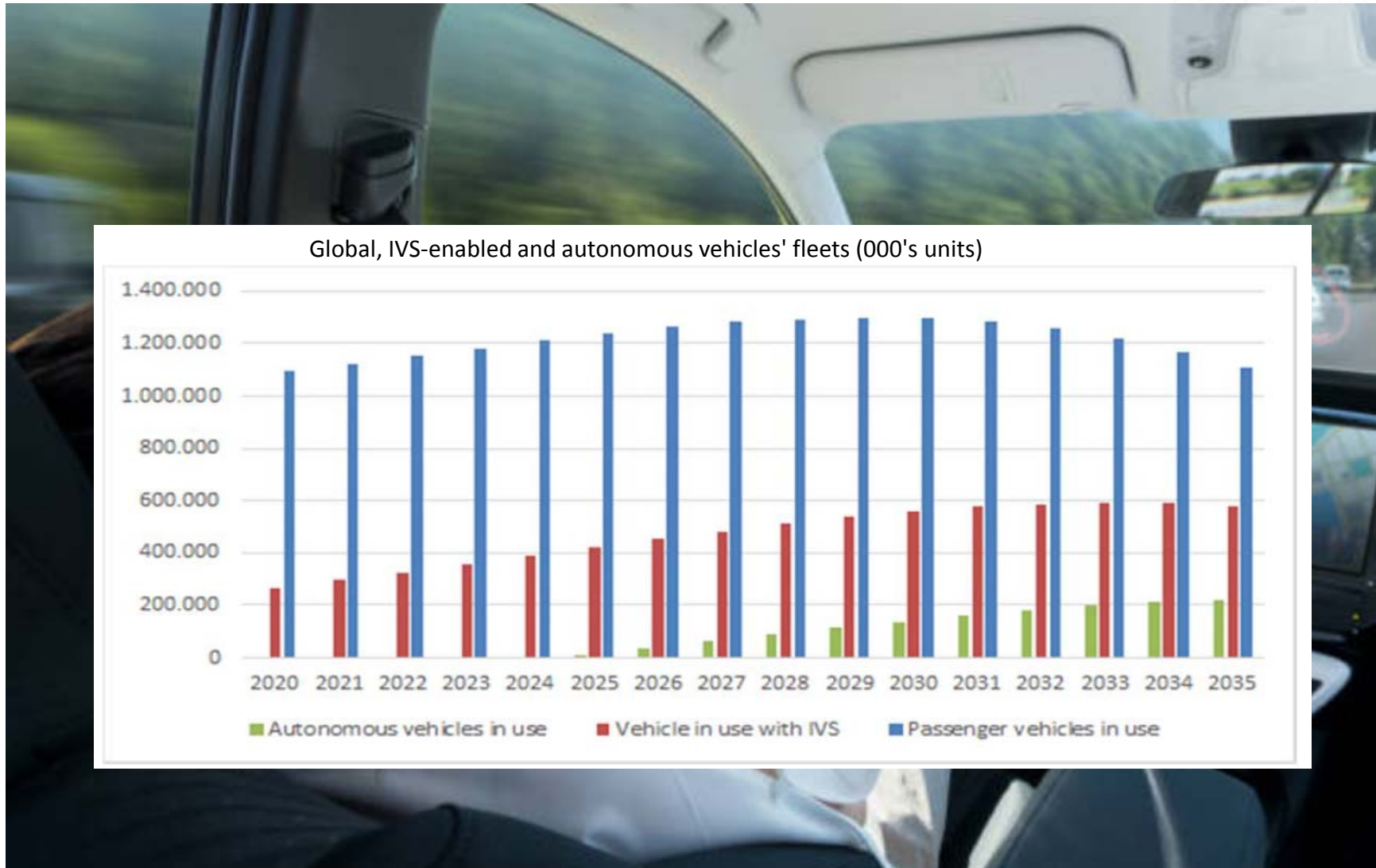
Technical and operational specifications allowing the commercial service to be established under the Galileo programme to fulfil the function defined in article 2(4)(c) of Regulation (EU) No 1285/2013 of the European Parliament and of the Council

		CS authentication	
		Specifications common to the OS and the CS: Authentication of geolocation information	Specifications specific to the CS: Authentication through encrypted codes
OS high accuracy		Provision of authentication data for OS geolocation information contained in the signals	Authentication of signals through access to encrypted codes contained in the signals
OS high accuracy	Provision of high-accuracy data to be used in positioning services with errors of less than one metre in nominal operation conditions	E1, component E1-B for the authentication data for OS geolocation information	E6, component E6-B for the access data to the encrypted codes and component E6-C (pilot)
OS high accuracy	Provision of component E6-B (pilot) for the supply of high-accuracy data	Authenticity of the data verified by an asymmetrical cryptography protocol and transmitted in the signals and a public cryptographic key	Authenticity of the signals verified by decrypting the signal encrypted using a private cryptographic key
User segment specifications	High-accuracy positioning obtained through the precise positioning algorithms integrated into the receiver and using data transmitted in the signals		
Geographical coverage	Global	Global	Global

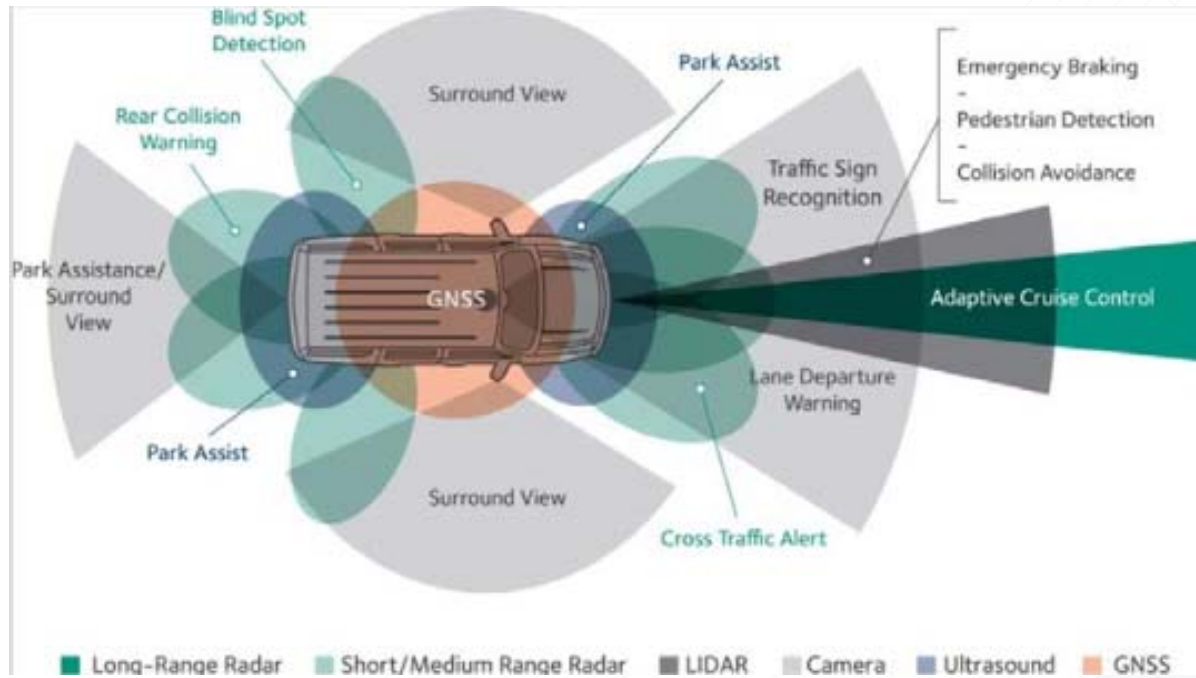
TABLE OF CONTENTS

- Introduction
- **High Accuracy Service**
- Authentication Services
- Roadmap
- Conclusions

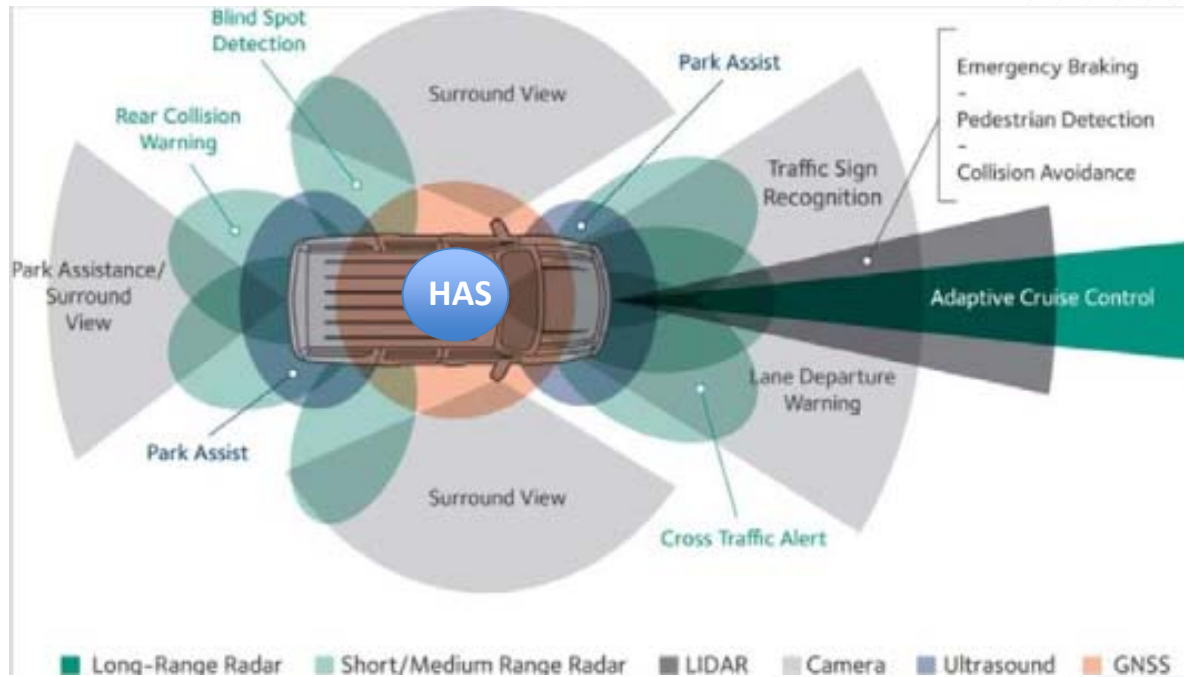




IVS = in-vehicle systems

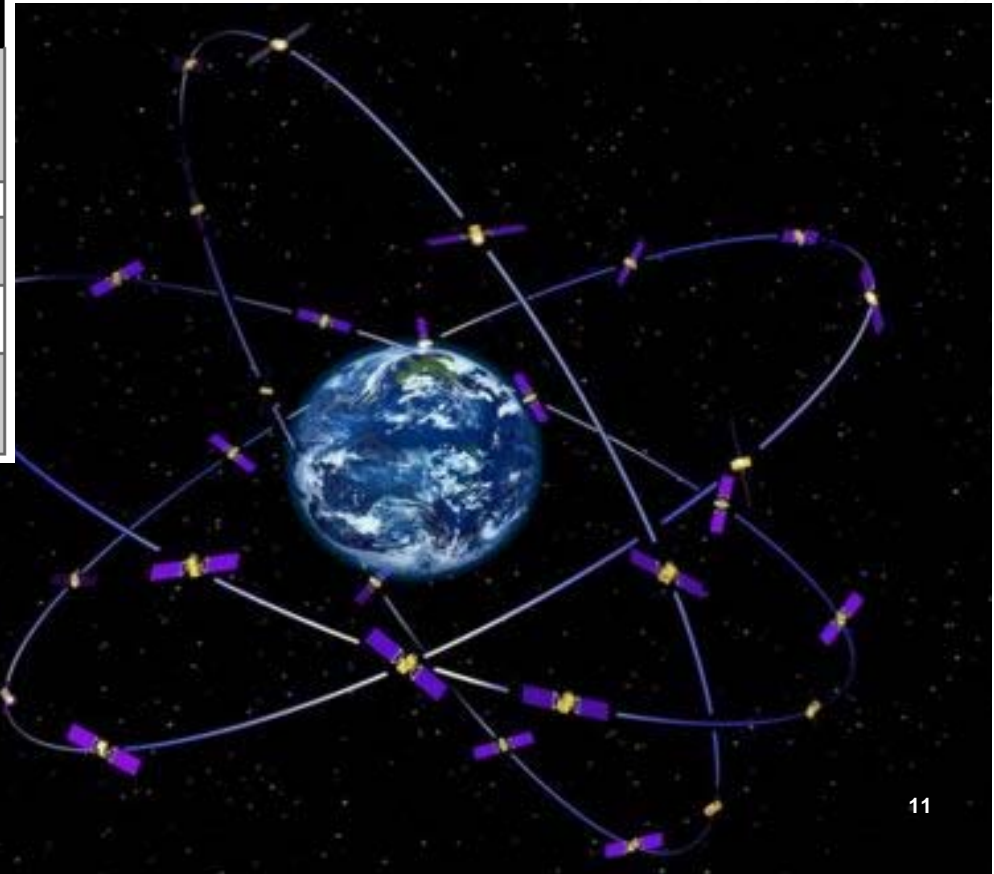


Others: INS, map matching, comm signals.



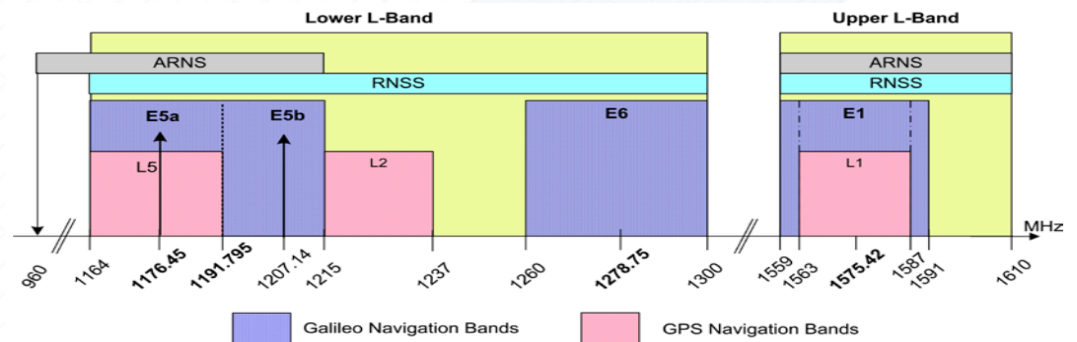
Others: INS, map matching, comm signals.

	Galileo	QZSS	SBAS	Commercial
Coverage	Global	Regional	Regional	Global (except high latitudes)
Satellites orbits	MEO	IGSO	GEO	GEO
Bandwidth per sat.	448 bps	2000 bps	250 bps	from ~2500 bps
Nb sat typically visible (open-sky)	4-6	1-3	1-2	1-2
Band/Frequency	E6, 1278.75 MHz	L6, 1278.75 MHz	E5b, 1207.14 MHz	L-band (~1-2 GHz)

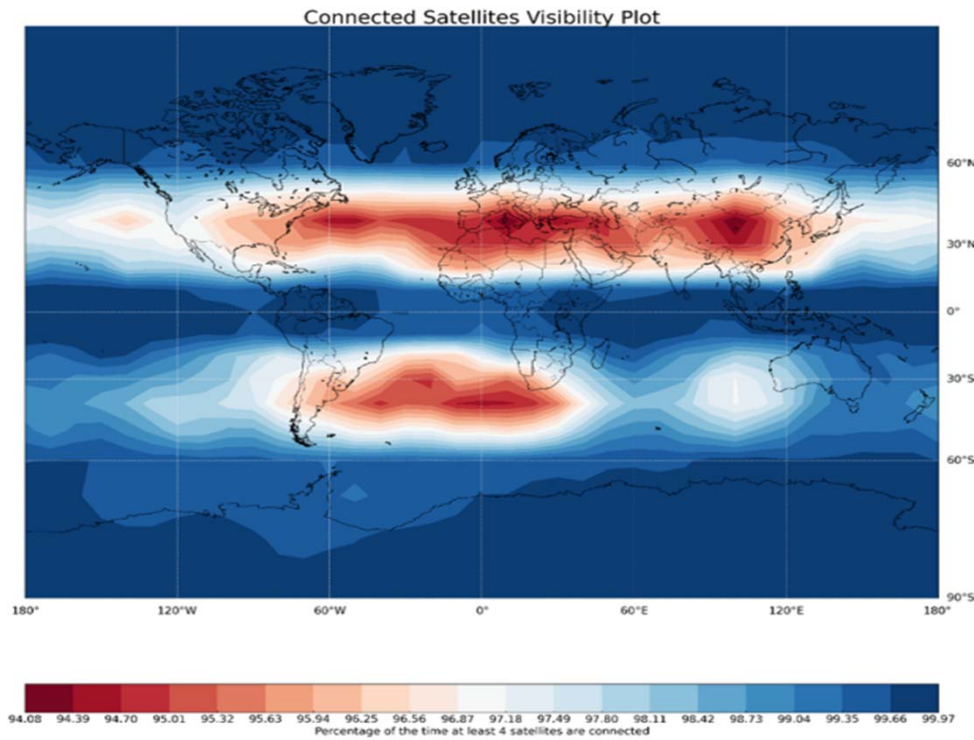


Signal and Data features	
Frequency	1278.75 MHz
Signal	E6B
Min. Power	-158 dBW
Modulation	BPSK(5)
Chip Rate	5.115 Mcps
Code Length	1 ms
Symbol Rate	1000 sps
Data Rate	492 bps
HA Data Rate	448 bps
Data Coding	FEC, as per Galileo OS SIS ICD and interleaving 123 x 8
Spreading Code Encryption	No
Data Format	TBD but based on open standard.
Data (TBC)	Orbit and clock corrections, code and phase biases, SQM, flags, ionospheric information.

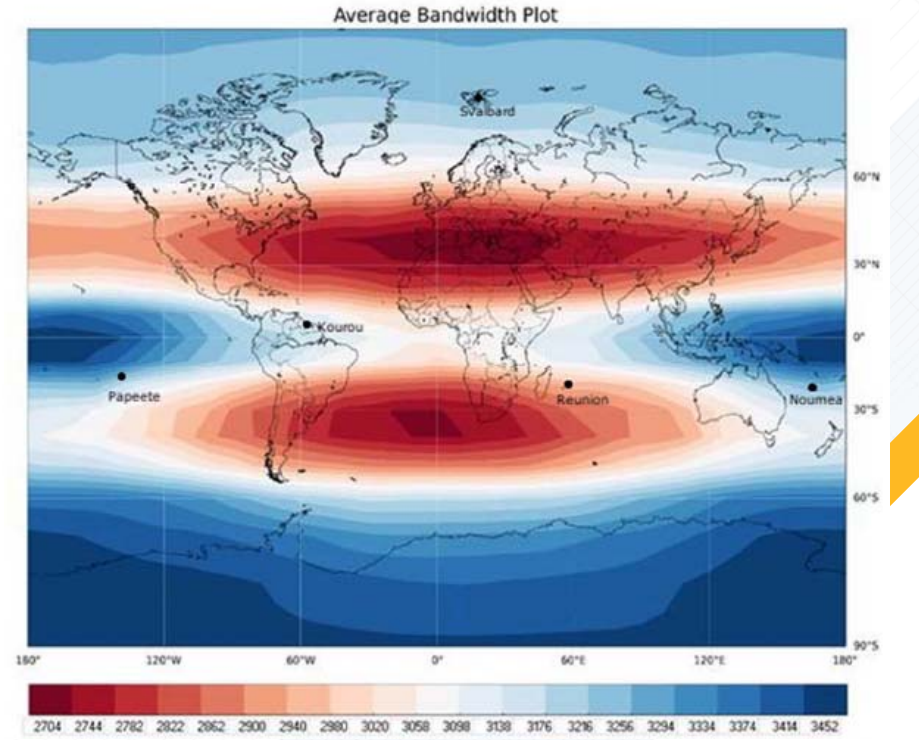
E6 is currently out of the U.S. FCC waiver -> not authorised in the U.S.



DOWNLINK CAPABILITY (Estimation, Galileo FOC – 2020)



AVG. AVAILABILITY 4 SV [94-99.9%]



AVG. BW: [2704, 3472]

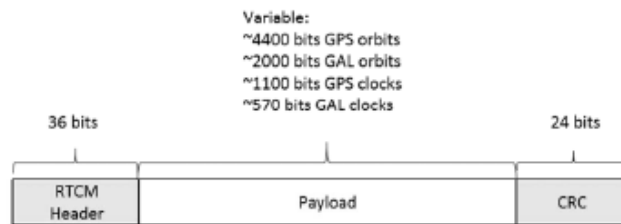
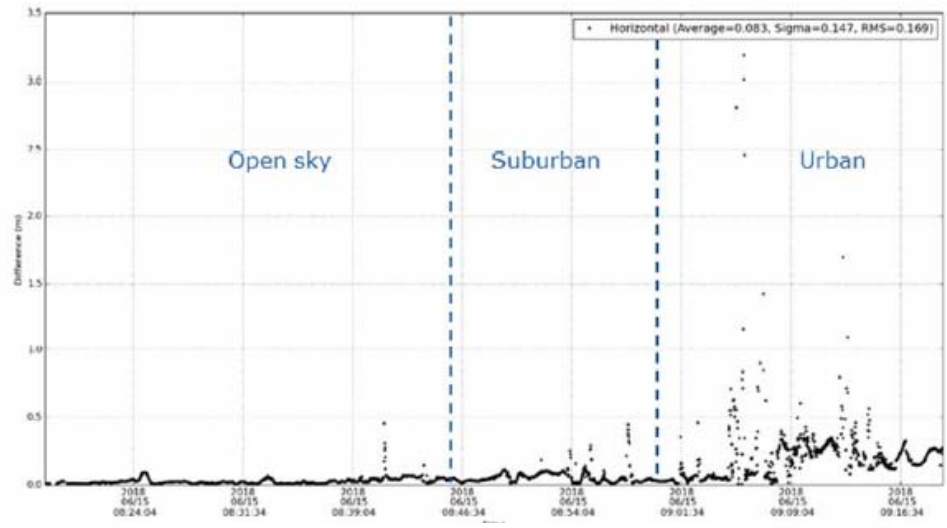
HAS DEFINITION

- High accuracy (PPP) corrections provided in the Galileo E6-B signal component:
 - Satellite orbits
 - Satellite clock corrections
 - Code biases for multi-frequency
 - Signal/correction quality information
 - Phase biases (to be confirmed)
 - Ionosphere in EU (to be confirmed)
- Corrections for Galileo (E1, E5a, E5b, E6, E5 TBC) and GPS (L1, L2, others TBC), and in the future potentially for other GNSS.
- Global coverage when fully operational. Partial coverage before. EU always included.

- HAS data will be transmitted openly, for free, and through an open standard format. **RTCM CSSR used as starting point.** Format currently under definition.
- "user error of less than two decimetres". This depends on user receiver, algorithm and environment.
- Support HAS via terrestrial networks is under consideration.

Sub Type	Sub Type Name	No. of Bit
1	Compact SSR Mask	37 + 60 x Nsys
2	Compat SSR GNSS Orbit Correction	25 + (51 or 49) x Nsat
3	Compact SSR GNSS Clock Correction	25 + 15xNsat
4	Compact SSR GNSS Satellite Code Bias	25 + 11 x Ncode x Nsat
5	Compact SSR GNSS Satellite Phase Bias	25 + 17 x Nphase x Nsat
6	Compact SSR GNSS Satellite Code and Phase Bias	28 + 28 x Nsig x Nsat
7	Compact SSR GNSS URA	25 + 6 x Nsat
8	Compact SSR TEC Correction	25 + 34 x Ngrid

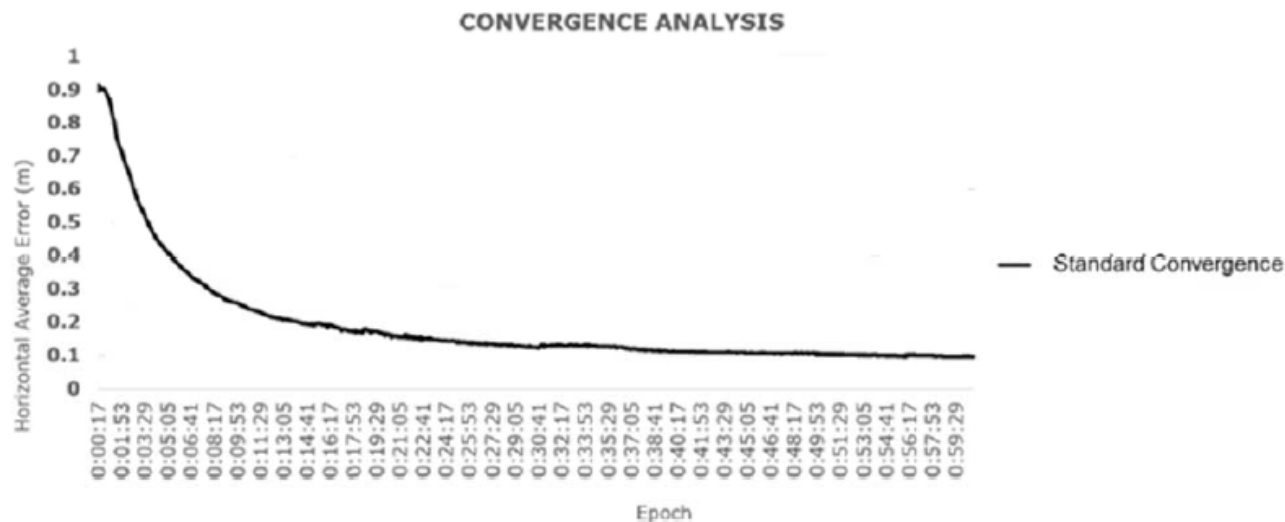
HAS PROSPECTIVE PERFORMANCE



- Same message "transmitted" by all Galileo sats.
- GPS L1/L2 and Galileo E1/E5 corrections
- Possible improvements:
 - More satellites
 - More frequencies
 - SIS format & coding optimization
 - Antenna and receiver: better carrier tracking, less code/carrier noise, better multipath mitigation

HAS PROSPECTIVE PERFORMANCE

- PPP convergence time still *the* problem.
- Assisted users can do RTK-PPP.
- Standalone users can use 3-4 frequencies and/or iono models for quasi-instantaneous (few s) convergence.



HAS PROSPECTIVE PERFORMANCE

- Galileo E6B SIS coding schemes can be key for time to 1st precise fix (several Kbits to receive).
- We compared reception of a 20-page (8320-bit) message in E6B with different coding/packing schemes:
 - size of GPS/Galileo 50-satellite message including orbits, clocks, and code and phase biases for three frequencies.
 - representative of an ionospheric message covering the EU area, including ~200 grid points.

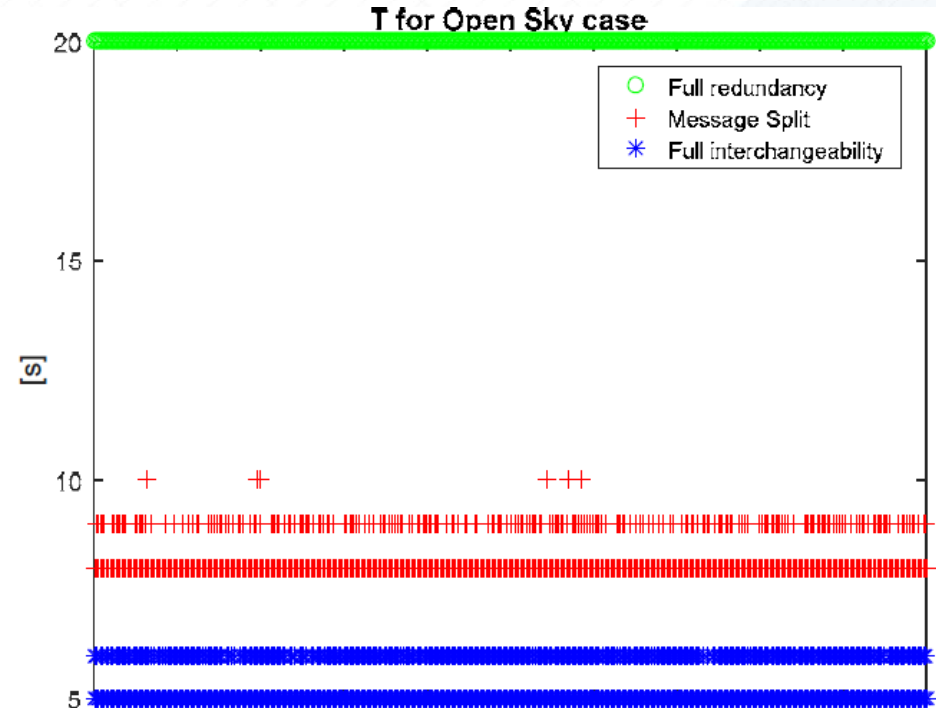
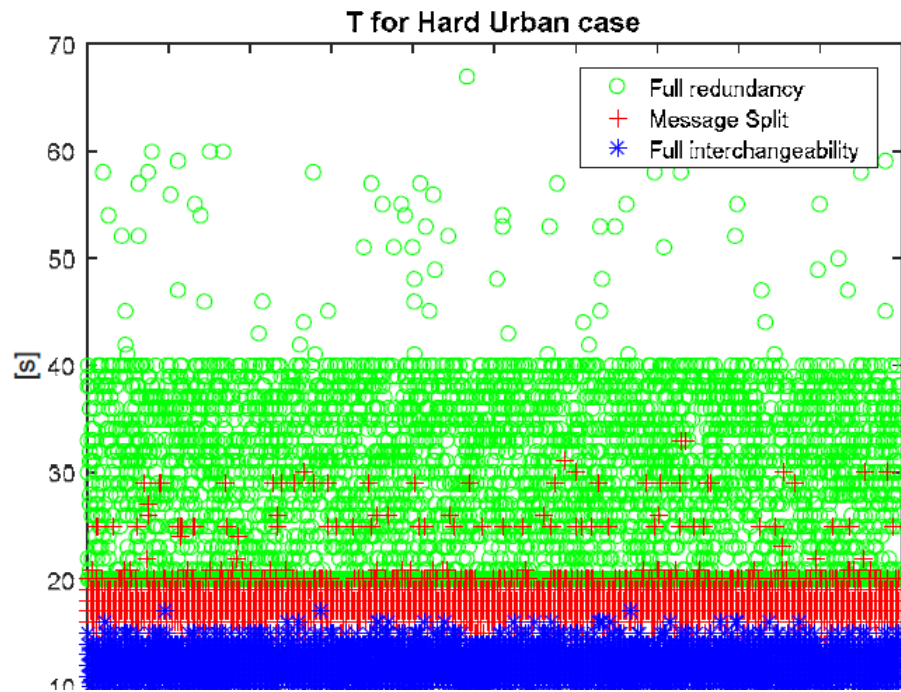


TABLE OF CONTENTS

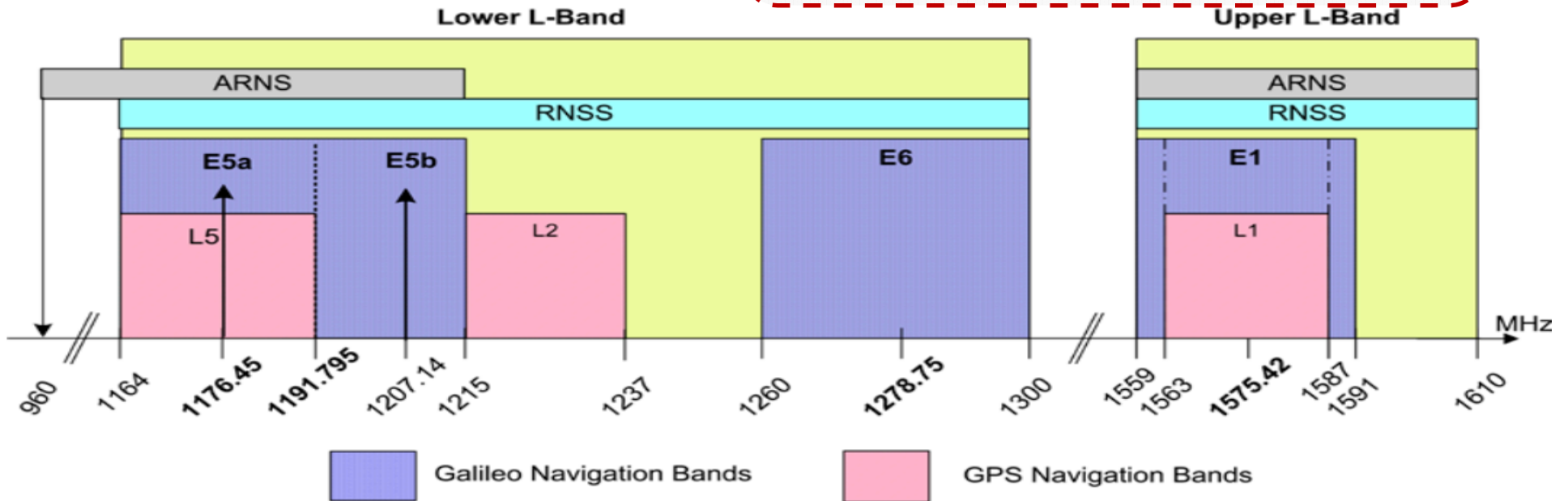
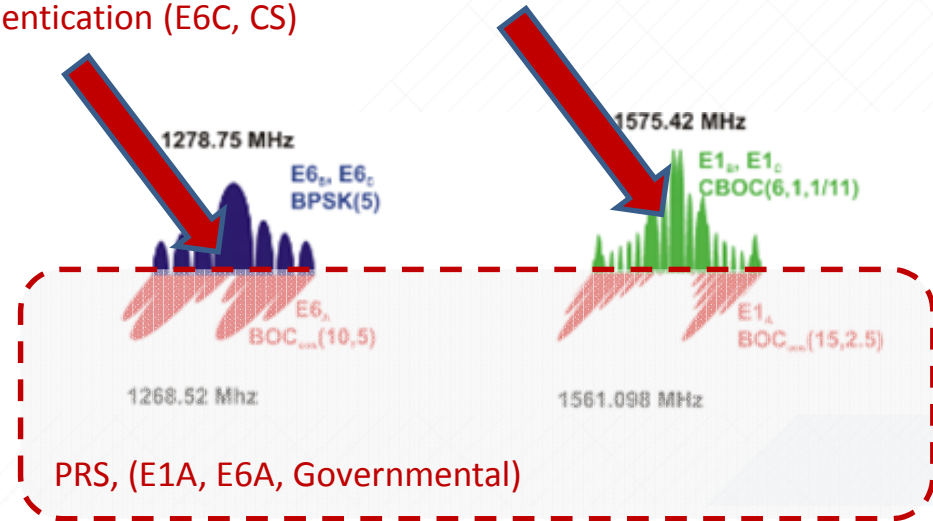
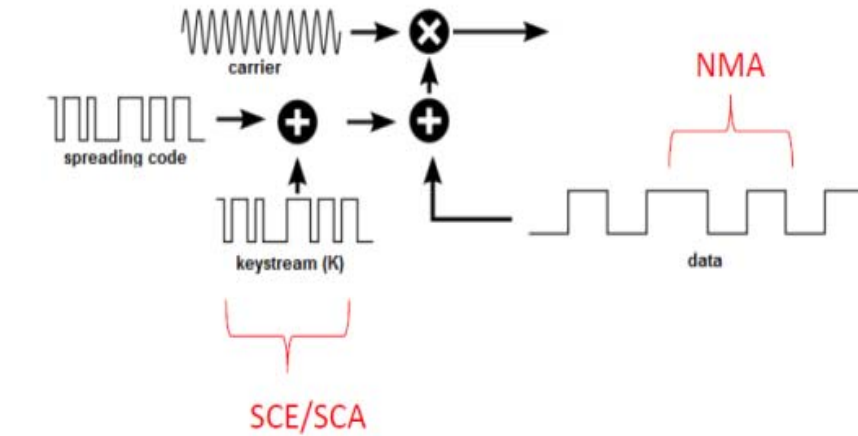
- Introduction
- High Accuracy Service
- **Authentication Services**
- Roadmap
- Conclusions

Introduction and Background

Galileo Frequency Plan

NMA: OS
Navigation
Message
Authentication
(E1B, OS)

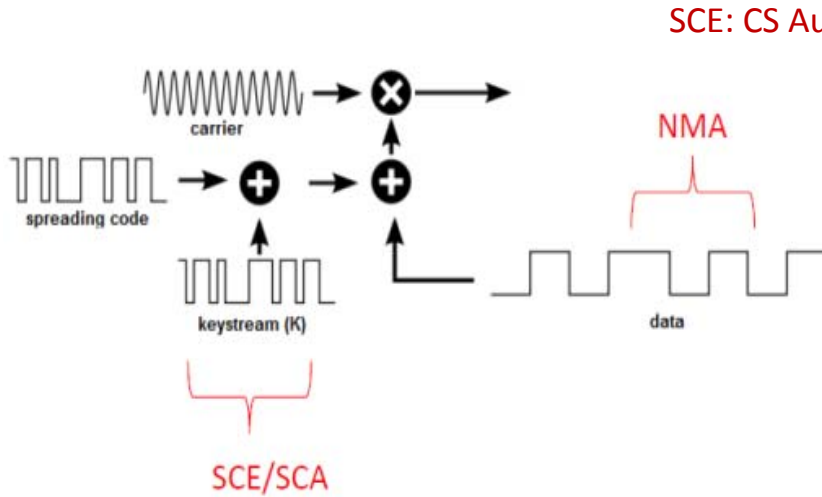
SCE: CS Authentication (E6C, CS)



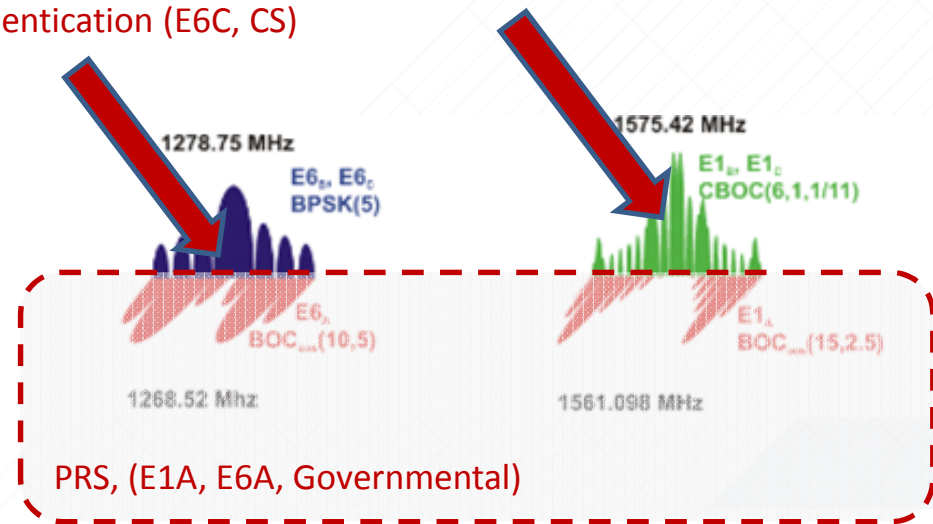
Introduction and Background

Galileo Frequency Plan

NMA: OS
Navigation
Message
Authentication
(E1B, OS)

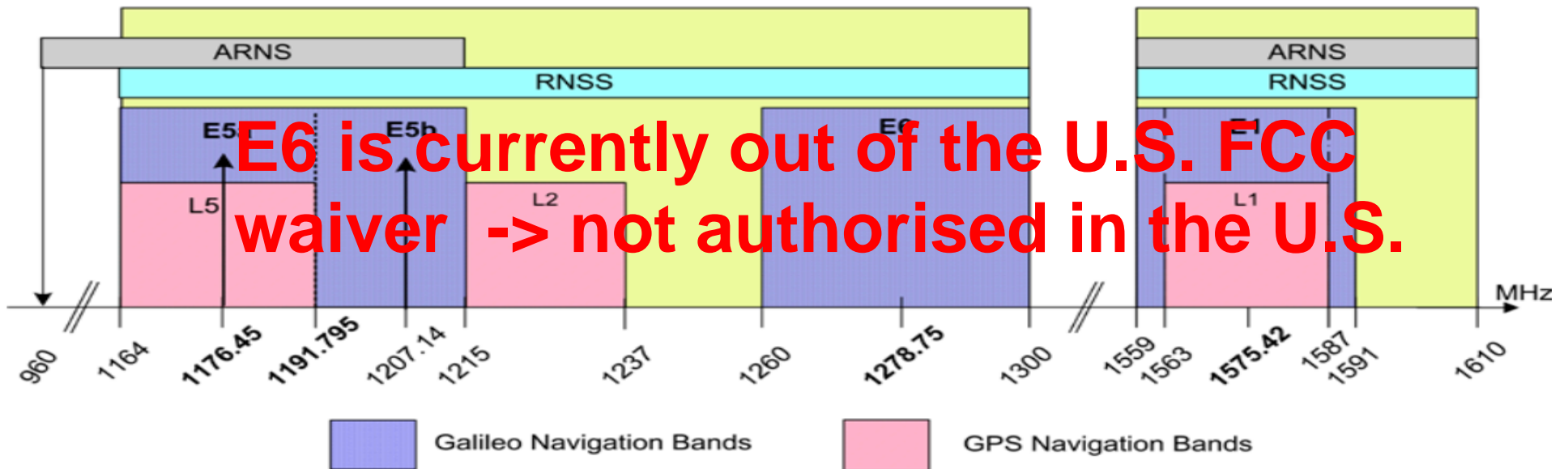


SCE: CS Authentication (E6C, CS)



Lower L-Band

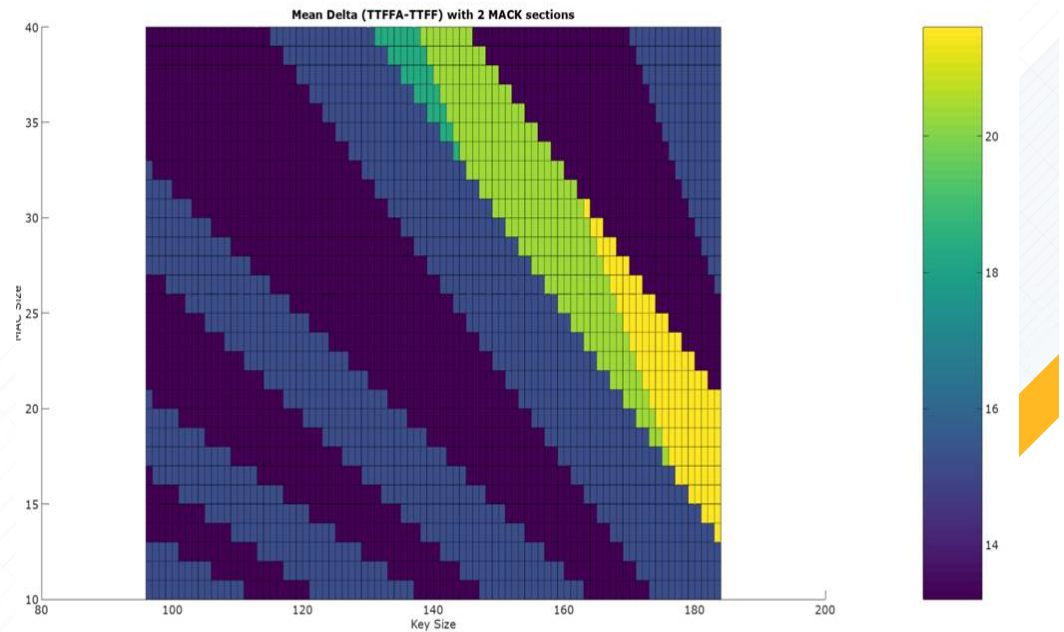
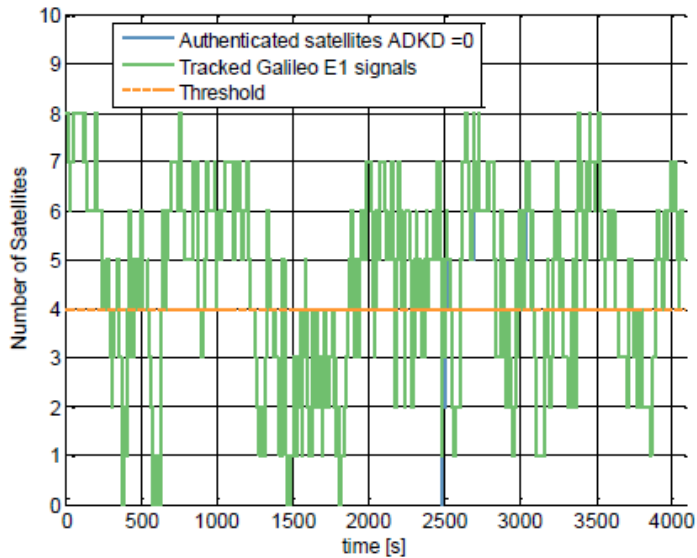
Upper L-Band



Navigation Message Authentication

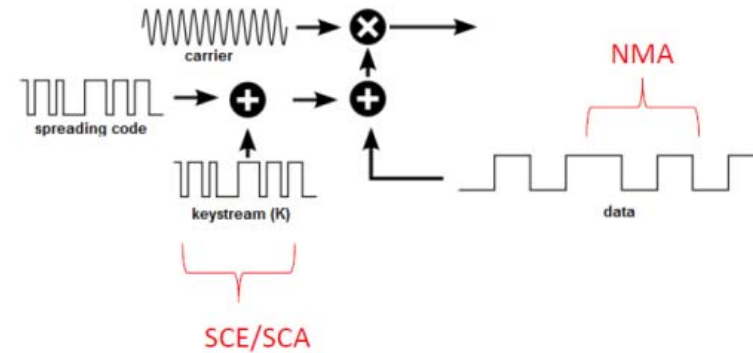
GNSS NMA Performance

- NMA does not degrade availability or accuracy. Degradation of TTFAF vs. TTFF of some seconds.

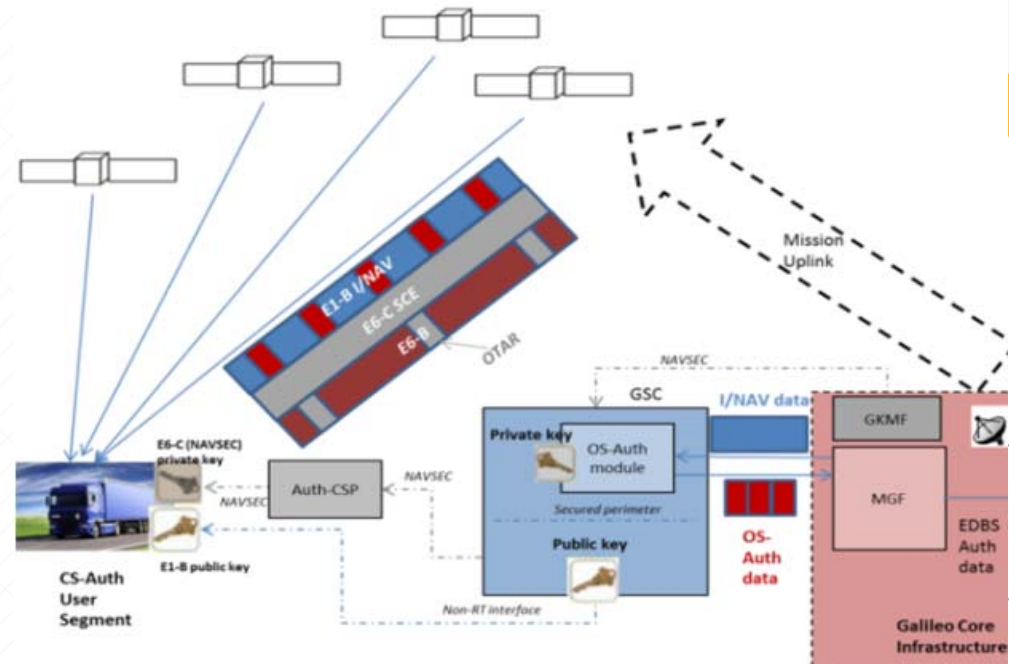


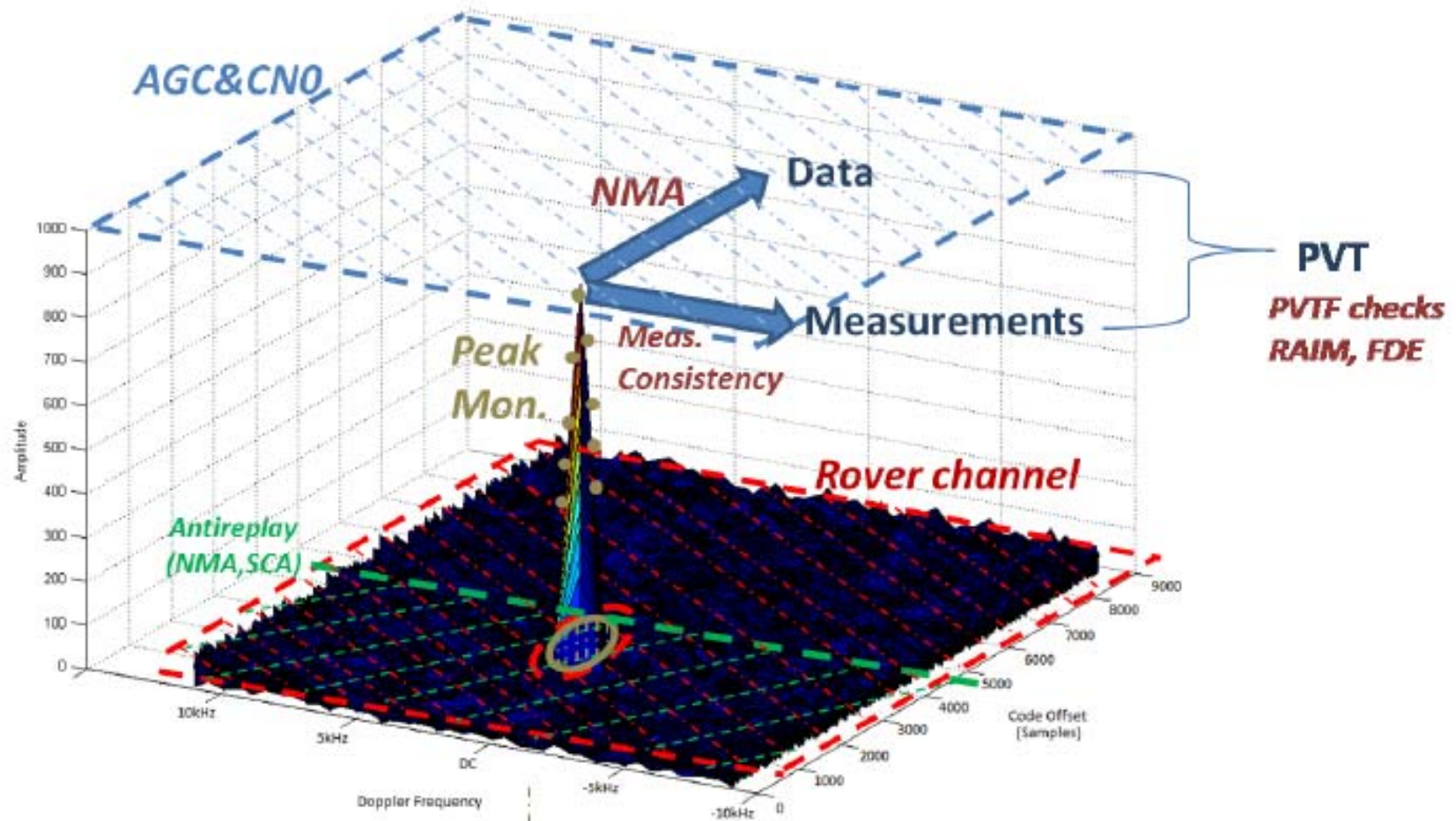
Commercial Authentication Service

- Based on the full encryption of the Galileo E6C component + OSNMA (E1B) + E6B data.



- Provides the highest physically possible level of GNSS signal protection.





Signal and data authentication is understood in combination with receiver measures.

TABLE OF CONTENTS

- Introduction
- High Accuracy Service
- Authentication Services
- **Roadmap**
- Conclusions

GALILEO AUTHENTICATION ROADMAP

- OSNMA draft specification (v1.0) available since 2016.
- OSNMA specification consolidated (v1.1; minor modifications and some additions wrt. v1.0) and currently under implementation in Galileo infrastructure.
- OSNMA Test SIS foreseen in 2019.
- OSNMA Service in 2020.
- CAS SIS tests foreseen in 2020. Service in 2021-22.
- Signal authentication also in Galileo 2nd Generation (2030) OS.

HIGH ACCURACY ROADMAP – UNDER CONSOLIDATION

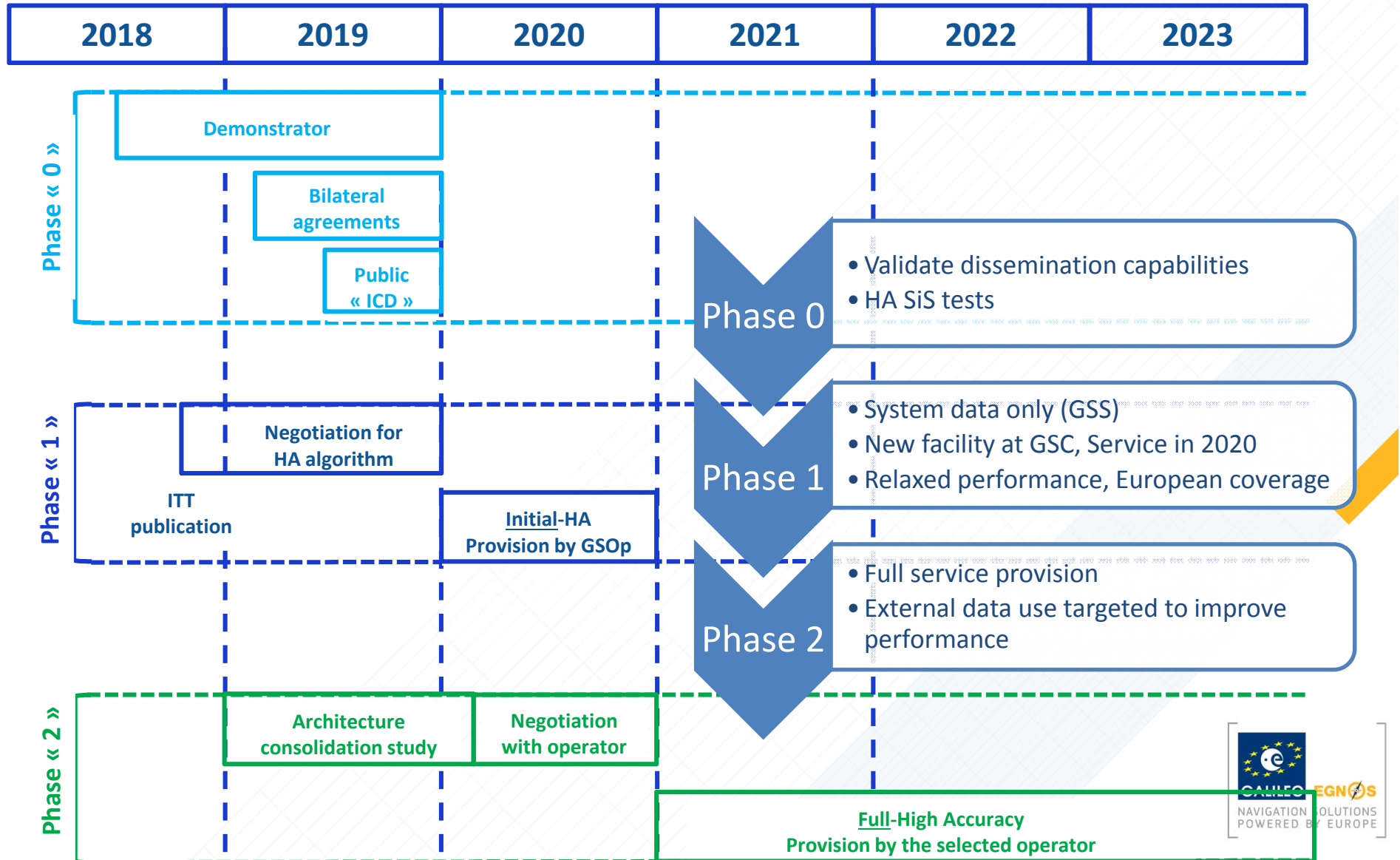


TABLE OF CONTENTS

- Introduction
- High Accuracy Service
- Authentication Services
- Roadmap
- **Conclusions**

CONCLUSIONS

- The Galileo Programme will include a free and open High Accuracy Service (HAS) based on the transmission of PPP corrections globally through the E6-B Galileo signal component.
 - Based on open standards (RTCM CSSR as starting point)
 - 2018 : Initial testing phase. 2020 : Operational phase
 - Target accuracy: <20 cm.
- Galileo civil authentication services (OSNMA, CAS) in baseline since 2017. Added due to the growing spoofing threat.
 - OSNMA specification consolidated and currently under implementation.
 - OSNMA Test SIS foreseen in 2019. Service in 2020.
 - CAS Test SIS foreseen in 2020. Service in 2021-22.



Acknowledgements: S. Cancela, T. Senni, D. Calle, G. Vecchione

THANK YOU

ESA/CNES/ARIANESPACE-Service Optique CSG, S. Martin



Ignacio Fernández Hernández

INTERGEO 16/10/2018, Frankfurt, DE

