
This is the **published version** of the bachelor thesis:

Sardà Martín, Òscar. *SASlib : desenvolupament d'una biblioteca oberta per a l'autenticació de senyal de Galileo (SAS). Correlació de senyal, autenticació de rang i càlcul de PVT*. Treball de Final de Grau (Universitat Autònoma de Barcelona), 2026 (Grau en Enginyeria de Sistemes de Telecomunicació)

This version is available at <https://ddd.uab.cat/record/335928>

under the terms of the  license.



TREBALL DE FI DE GRAU

GRAU EN ENGINYERIA DE SISTEMES DE TELECOMUNICACIÓ

SASlib: desenvolupament d'una biblioteca oberta per a l'autenticació de senyal de Galileo (SAS). Correlació de senyal, autenticació de rang i càlcul de PVT

Òscar Sardà Martín

DIRECTOR: Rafael Terris-Gallego

TUTOR: Rafael Terris-Gallego

DEPARTAMENT SIGNAL PROCESSING FOR COMMUNICATIONS AND NAVIGATION
(SPCOMNAV)

UNIVERSITAT AUTÒNOMA DE BARCELONA

Bellaterra, Juliol 2026

Resum

Els sistemes globals de navegació per satèl·lit (GNSS) són una infraestructura crítica però vulnerable als atacs d'*spoofing*, en què un atacant transmet senyals falsos per induir el receptor a calcular una posició o un temps incorrectes. El programa Galileo hi fa front amb el Servei d'Autenticació de Senyal (SAS), que autentica el senyal a nivell de rang xifrant la component E6-C. Aquest treball desenvolupa i valida la cadena de processament de senyal d'un receptor SAS dins de la biblioteca de codi obert «SASlib» del grup SPCOMNAV. La contribució principal és la implementació de tres blocs: la correlació de les seqüències de codi desxifrades amb la instantània capturada (amb càlcul de la funció d'ambigüitat creuada, integració post-detecció, assistència de fase de codi i mètriques de qualitat), l'autenticador de rang basat en el model d'error E1–E6, i el càlcul de la solució PVT per navegació de temps aproximat. El sistema es valida amb dades reals capturades amb una plataforma SDR bladeRF a les bandes E1 i E6 i amb la campanya de senyal E6-C xifrat de juny de 2025.

Paraules clau: GNSS, Galileo, autenticació de senyal, SAS, spoofing, correlació, PVT autenticada.

Resumen

Los sistemas globales de navegación por satélite (GNSS) son una infraestructura crítica pero vulnerable a los ataques de *spoofing*, en los que un atacante transmite señales falsas para inducir al receptor a calcular una posición o un tiempo incorrectos. El programa Galileo lo afronta con el Servicio de Autenticación de Señal (SAS), que autentica la señal a nivel de rango cifrando la componente E6-C. Este trabajo desarrolla y valida la cadena de procesamiento de señal de un receptor SAS dentro de la biblioteca de código abierto «SASlib» del grupo SPCOMNAV. La contribución principal es la implementación de tres bloques: la correlación de las secuencias de código descifradas con la instantánea capturada (con cálculo de la función de ambigüedad cruzada, integración post-detección, asistencia de fase de código y métricas de calidad), el autenticador de rango basado en el modelo de error E1–E6, y el cálculo de la solución PVT por navegación de tiempo grueso. El sistema se valida con datos reales capturados con una plataforma SDR bladeRF en las bandas E1 y E6 y con la campaña de señal E6-C cifrada de junio de 2025.

Palabras clave: GNSS, Galileo, autenticación de señal, SAS, spoofing, correlación, PVT autenticada.

Abstract

Global Navigation Satellite Systems (GNSS) are a critical infrastructure yet vulnerable to *spoofing* attacks, where an attacker transmits counterfeit signals to mislead the receiver into computing an incorrect position or time. The Galileo programme addresses this threat with the Signal Authentication Service (SAS), which provides range-level authentication by encrypting the E6-C component. This work develops and validates the signal-processing chain of a SAS receiver within the open-source «SASlib» library of the SPCOMNAV research group. The main contribution is the implementation of three blocks: the correlation of the decrypted code sequences against the recorded snapshot (with cross-ambiguity function computation, post-detection integration, code-phase aiding and quality metrics), the range authenticator based on the E1–E6 error model, and the PVT solution via coarse-time navigation. The system is validated with real data captured by a bladeRF SDR platform on the E1 and E6 bands and with the encrypted E6-C signal campaign of June 2025.

Keywords: GNSS, Galileo, signal authentication, SAS, spoofing, correlation, authenticated PVT.

Agraïments

Vull expressar el meu agraïment, en primer lloc, a Rafael Terris-Gallego, director i tutor d'aquest Treball de Fi de Grau, per la seva guia, la seva dedicació i el seu seguiment constant al llarg de tot el projecte.

Agraeixo també al grup de recerca SPCOMNAV de la Universitat Autònoma de Barcelona, dirigit pels professors José A. López-Salcedo i Gonzalo Seco-Granados, l'oportunitat de formar part d'aquesta línia de recerca i els mitjans i el coneixement que han fet possible aquest treball.

Un agraïment especial a Enrique Takiguchi-Medina per la seva ajuda amb la plataforma.

Finalment, a la meva família —el meu pare, la meva mare i el meu germà— per ser-hi sempre i donar-me un suport incondicional.

Índex

Resum	i
Resumen	iii
Abstract	v
Agraïments	vii
Índex de figures	xiii
Índex de taules	xvii
Llista d'acrònims	xix
1 Introducció	1
1.1 Context i motivació	1
1.2 Objectius	2
1.3 Estructura del document	3
2 Estat de l'art i marc teòric	5
2.1 Fonaments dels GNSS	5
2.1.1 Arquitectura i sistemes actuals	5
2.1.2 Principi de posicionament	7
2.1.3 El senyal GNSS: codis i modulacions (BPSK i BOC)	9
2.1.4 Efectes de propagació	13

2.2	El receptor GNSS	14
2.2.1	Front-end de RF i captura SDR	15
2.2.2	Adquisició i funció d'ambigüitat creuada	15
2.2.3	Integració coherent i no coherent	16
2.2.4	Seguiment i receptors snapshot	16
2.2.5	Model de rellotge i referència temporal	17
2.2.6	Detecció de senyal i corbes ROC	18
2.3	Disruptors del senyal i contramesures	19
2.3.1	Pertorbacions no intencionades	19
2.3.2	Pertorbacions intencionades: <i>jamming</i> , <i>meaconing</i> i <i>spoofing</i>	20
2.3.3	Contramesures a nivell de receptor	20
2.3.4	Contramesures a nivell de sistema: autenticació criptogràfica	22
2.3.5	Cap a la segona generació	24
3	Metodologia	27
3.1	Materials i eines	27
3.1.1	Recursos i feina prèvia del departament	27
3.1.2	La biblioteca SASlib	28
3.1.3	Plataforma de captura SDR	29
3.1.4	Dades auxiliars	31
3.1.5	Documents normatius	32
3.1.6	Eines d'intel·ligència artificial generativa	32
3.2	Disseny i procediment	33
3.2.1	Repartiment amb el TFG d'Enginyeria Informàtica	33
3.2.2	El pipeline de SASlib i el flux de processament SAS	33
3.2.3	Metodologia de validació	36
4	Desenvolupament i implementació	37

4.1	Arquitectura dels blocs de processament de senyal	37
4.2	Bloc de processament de correlació	38
4.2.1	Model de senyal i objectiu	38
4.2.2	Càrrega i condicionament de les mostres	39
4.2.3	Generació de les rèpliques de codi	40
4.2.4	Càlcul de la CAF mitjançant la FFT	41
4.2.5	Integració coherent i post-detecció	42
4.2.6	Cerca de Doppler aproximada i fina	43
4.2.7	Reutilització del Doppler entre components	44
4.2.8	Detecció del pic i interpolació sub-mostra	44
4.2.9	Mètriques de qualitat	45
4.2.10	Assistència de fase de codi (SAS)	46
4.2.11	Banda auxiliar E1 i emparellament de període	47
4.2.12	Sortides del bloc	47
4.3	Bloc de processament de rang per satèl·lit	48
4.3.1	Conversió entre mostres i metres	48
4.3.2	Estimació del retard esperat i compensació E1–E6	48
4.3.3	Maneig de la periodicitat i embolcall	49
4.3.4	Llindar d'autenticació	49
4.3.5	Correcció ionosfèrica amb NeQuick-G	51
4.3.6	Calibratge automàtic del biaix del receptor	52
4.3.7	Autenticació de posició	53
4.4	Computador de PVT	54
4.4.1	Plantejament: navegació de temps aproximat	54
4.4.2	Posició del satèl·lit a partir de les efemèrides	55
4.4.3	Conversions de coordenades i models atmosfèrics	56
4.4.4	Etape 1: CT-Doppler	56

4.4.5	Etapa 2: CT-PRange amb resolució d'ambigüitat	57
4.4.6	Casos amb pocs satèl·lits	57
4.4.7	Control de qualitat i validació creuada	58
4.4.8	Sortides i indicadors	58
5	Resultats i discussió	59
5.1	Validació funcional amb senyal E6-C xifrat real	59
5.2	Refinament i autenticació de rang amb captures pròpies	61
5.3	Solució de posició (PVT)	65
5.4	Discussió	66
6	Conclusions i treball futur	69
6.1	Conclusions	69
6.2	Línies de treball pel futur	71
6.3	Publicacions derivades del treball	72
	Bibliografia	75
A	Material addicional	79
A.1	Paràmetres de configuració dels blocs	79
A.2	Exemple de pipeline d'execució	83

Índex de figures

2.1	Els tres segments d'un sistema GNSS i el flux addicional de dades del SAS. Adaptat de [TG24a, Bor23].	7
2.2	Principi de posicionament GNSS i efecte del biaix de rellotge del receptor ($c\delta t_u$), en el cas 2D. Adaptat de [TG24a], Fig. 2.9.	8
2.3	Guany de processament G_c en les tècniques d'espectre eixamplat. Adaptat de [TG24a], Fig. 2.3.	9
2.4	Estructura per capes d'un component de senyal GNSS. Recreada a partir de [TG24a], Fig. 2.5.	10
2.5	Polsos de chip de BPSK, BOC(1,1) i BOC(6,1). Adaptat de [TG24a], Fig. 2.6. . .	11
2.6	Funcions d'autocorrelació dels polsos de Galileo E1 —BOC(1,1), BOC(6,1) i la CBOC(6,1,1/11)— i de l'E6 (BPSK(5)). Adaptat de [TG24a], Fig. 3.6.	11
2.7	Espectre de les bandes GNSS en banda L (GPS, GLONASS, Galileo i BeiDou), amb les bandes E1 i E6 de Galileo.	12
2.8	Efecte del multicamí: (a) geometria de la recepció (senyal directe LOS i rèplica reflectida); (b) distorsió resultant del pic d'autocorrelació. Diagrama conceptual.	14
2.9	Cadena de processament d'un receptor GNSS. Adaptat de [Bor23, TG24a].	14
2.10	Funció d'ambigüitat creuada (CAF) resultant de l'adquisició, en una execució real del bloc <i>SignalCorrelation</i> (vegeu Capítol 5).	16
2.11	Model de rellotge de dos estats (deriva x_d i biaix x_b). Adaptat de [TG24a], Fig. 2.15.	18
2.12	Cadena de claus TESLA, generades amb una funció <i>hash</i> unidireccional F en sentit invers al de revelació. Adaptat de [TG24a].	23

3.1	Front-end web de SASlib: la cadena de processament es representa com un graf de blocs, cadascun amb el seu estat i els seus paràmetres configurables, des del qual es configura i es llança l'execució del pipeline. Captura de [TG26a].	29
3.2	Front-end propi de la plataforma de captura SDR (Signal Capture Control Center), des d'on es configura i es llança l'enregistrament sincronitzat de les dues bandes.	30
3.3	Plataforma de captura SDR ubicada a la UAB: el maletí integra les dues plaques bladeRF de captura sincronitzada E1/E6. Imatge de [TG26a].	31
3.4	Operació del SAS al receptor: les claus TESLA revelades a l'E1-B (a intervals d'una subtrama I/NAV, 30 s) desxifren les RECS descarregades per avançat i en produeixen les ECS (rèpliques locals), que es correlacionen amb la instantània E6-C pregravada de cada interval. El superíndex 'R' indica l'ECS rebuda, afectada per soroll. Adaptat de [TG24b].	34
3.5	Arquitectura de SASlib: els 13 blocs del pipeline amb les seves entrades (fonts de dades) i sortides (artefactes), organitzats segons les quatre etapes del flux de processament. Els blocs de processament de senyal desenvolupats en aquest TFG són <i>SignalCorrelation</i> , <i>SatelliteAuthenticator</i> i <i>PVTComputation</i> . De [TG26a]. . .	35
4.1	Flux de dades dels tres blocs de processament de senyal (verd, dins la zona ombrrejada) i la frontera amb els blocs externs (vermell, discontinu).	38
4.2	Generació de la rèplica local, tot a la mateixa escala (eix de mostres n ; exemple esquemàtic amb $f_s/R_c = 4$ mostres per chip; en realitat $\approx 3,9$ a l'E6 i $\approx 19,55$ a l'E1). (a) El codi PRN és una seqüència de chips, un valor per chip; (b) el sobremostreig $\tilde{c}[n]$ (Eq. (4.2)) repeteix cada chip sobre f_s/R_c mostres consecutives iguals (1 punt per chip a (a) esdevenen f_s/R_c punts a (b)); (c) la subportadora BOC(1,1) $s[n]$ (Eq. (4.3)), només E1, que commuta a la meitat de cada chip; (d) la rèplica $c[n] = \tilde{c}[n]s[n]$ (Eq. (4.4)). Per a l'E6 (BPSK) s'omet (c), i per a l'E6-C xifrat els chips de partida són els de l'ECS.	41
4.3	Caracterització del biaix de maquinari del receptor (HWB): histograma de la diferència de retard de codi entre les dues cadenes BladeRF (mateixa entrada E1-B, PRN 3), amb el seu ajust gaussià —mitjana $\mu = -5,21$ m (el HWB) i desviació $\sigma = 1,05$ m (el <i>jitter</i>)—; a la dreta, la diferència es manté estable al llarg de la captura.	53
4.4	Criteri d'autenticació (esquema): el satèl·lit s'autentica si el residu $\Delta = \tau_{E6} - \hat{\tau}_{E6}$ cau dins la banda $ \Delta \leq \gamma_{\text{auth}}$ (verd); una manipulació per <i>meaconing</i> en desplaça el pic d'E6-C fora. Adaptat de [FH23].	54

4.5	Càlcul PVT snapshot com a refinament progressiu de la incertesa. Partint de cap informació inicial (posició indeterminada, error de temps de fins a hores), la CT-Doppler (a partir del Doppler, inequívoc) redueix la solució a una posició i un temps aproximats ($\sim$ km, $\sim$ s); aquesta llavor permet a la CT-PRange resoldre l'ambigüitat de període N_k amb les fases de codi i arribar a la solució final ($\sim$ m). Adaptat de [FH16, Bor23].	55
5.1	Pic d'autenticació de l'E6-C del PRN 14 amb l'ECS desxifrada, a dalt amb KDI = 0 i a baix amb KDI = 1.	60
5.2	Correlacions de l'E1-B (BOC(1,1)) i l'E6-C (ECS) del PRN 14, amb una vista ampliada dels dos pics.	61
5.3	Perfils de correlació complets de l'E1-B, l'E6-B i l'E6-C per al PRN 14, cadascun amb el pic detectat ($\star$) molt per damunt del soroll.	62
5.4	El mateix que la Figura 5.3, ara per al PRN 18.	63
5.5	Comparació del retard de codi de l'E1-B i l'E6-C, per al PRN 14 (dalt) i el PRN 18 (baix). La franja verda marca la zona autèntica.	64
5.6	Solució PVT semiautenticada calculada sobre la banda auxiliar, situada sobre el terrat del Departament d'Enginyeria Electrònica (UAB). El cercle verd marca el radi d'incertesa de la posició estimada.	66
6.1	Estació de monitoratge del SAS de Galileo (<i>SAS Monitor</i>): estat de la constel·lació —satèl·lits a la vista i rang autènticat (SAS, E6 enfront d'E1)— i <i>sky-plot</i> amb les posicions i trajectòries dels satèl·lits visibles. Els PRN xifrats (14 i 18) hi apareixen ressaltats i el PRN 14 hi consta com a autènticat.	73
6.2	Detall de l'estació de monitoratge: targetes per satèl·lit amb les mètriques per banda (E1-B, E6-B, E6-C), el veredict de l'autenticació de rang (E6-C enfront d'E1-B) i l'historial de les darreres execucions. El PRN 14, que emet l'E6-C xifrat, hi apareix com a autènticat (SAS).	73

Índex de taules

2.1	Segment espacial dels GNSS globals en operació. Estructura adaptada de la Taula 2.1 de [TG24a]; paràmetres de Galileo verificats amb les dades oficials del programa [Eur24a].	6
2.2	Paràmetres principals de les bandes Galileo E1 i E6 emprades en el SAS, segons l'OS SIS ICD [Eur23b].	13
2.3	Comparació dels nous serveis d'autenticació criptogràfica en GNSS. Adaptat de [TG24a].	24
4.1	Paràmetres d'integració per a les bandes E6 i E1 (valors per defecte).	43
4.2	Factor de confiança κ i nivell de confiança associat (distribució normal).	50
4.3	Components de l'interval d'incertesa σ_{auth} (Eq. (4.18)); valors de partida de [FH23] i estimacions experimentals per a aquest receptor (vegeu el text).	50
4.4	Biaix de codi E1–E6 abans i després de la correcció NeQuick-G (efemèrides i coeficients $a_{i0,1,2}$ reals de cada dia). El residual queda molt per sota de $\gamma_{\text{auth}} \approx 13\text{ m}$ amb el model d'error d'aquests conjunts.	52
5.1	Autenticació de rang per PRN amb captures pròpies. El biaix de codi E1-E6 mesurat queda per sota del llindar d'autenticació (13,1 m) en tots dos satèl·lits.	65
A.1	Paràmetres del bloc <i>ConfigInit</i> (arrencada i selecció del cas).	80
A.2	Paràmetres del bloc <i>SignalCorrelation</i> (correlació i detecció del pic).	81
A.3	Paràmetres del bloc <i>SatelliteAuthenticator</i> (test d'autenticació de rang).	82
A.4	Paràmetres del bloc <i>PVTComputation</i> (solució de posició).	83

Llista d'acrònims

A-GNSS Assisted GNSS.

ACAS Assisted Commercial Authentication Service.

ADC Analog-to-Digital Converter.

AES Advanced Encryption Standard.

AGC Automatic Gain Control.

AOA Angle of Arrival.

API Application Programming Interface.

AUC Area Under the Curve.

AVAR Allan Variance.

AWGN Additive White Gaussian Noise.

BGD Broadcast Group Delay.

BOC Binary Offset Carrier.

BPSK Binary Phase-Shift Keying.

C/N₀ Carrier-to-Noise density ratio.

CAF Cross-Ambiguity Function.

CBOC Composite Binary Offset Carrier.

CDMA Code Division Multiple Access.

CHIMERA Chips-Message Robust Authentication.

DLL Delay-Locked Loop.

DSM Digital Signature Message.

DSP Digital Signal Processing.

DSSS Direct-Sequence Spread Spectrum.

ECDSA Elliptic Curve Digital Signature Algorithm.

ECEF Earth-Centered, Earth-Fixed.

ECS Encrypted Code Sequences.

FDE Fault Detection and Exclusion.

FDMA Frequency Division Multiple Access.

FFT Fast Fourier Transform.

G2G Galileo Second Generation.

GNSS Global Navigation Satellite System.

GPS Global Positioning System.

GSC Galileo Service Centre.

GST Galileo System Time.

HAS High Accuracy Service.

HS-GNSS High-Sensitivity GNSS.

HWB Hardware Bias.

ICD Interface Control Document.

IGS International GNSS Service.

INS Inertial Navigation System.

IQ In-phase / Quadrature.

LNA Low-Noise Amplifier.

LOS Line-of-Sight.

LS Least Squares.

-
- MAC** Message Authentication Code.
- MCS** Master Control Station.
- MEO** Medium Earth Orbit.
- MPD** Multi-Peak Detection.
- NCO** Numerically Controlled Oscillator.
- NMA** Navigation Message Authentication.
- NTP** Network Time Protocol.
- OS** Open Service.
- OSNMA** Open Service Navigation Message Authentication.
- PCPS** Parallel Code Phase Search.
- PDI** Post-Detection Integration.
- PLL** Phase-Locked Loop.
- PPP** Precise Point Positioning.
- PPSP** Peak-to-Peak-Side-Peak ratio.
- PRN** Pseudo-Random Noise.
- PRS** Public Regulated Service.
- PVT** Position, Velocity and Time.
- RAIM** Receiver Autonomous Integrity Monitoring.
- RECS** Re-Encrypted Code Sequences.
- RFI** Radio-Frequency Interference.
- RINEX** Receiver Independent Exchange Format.
- ROC** Receiver Operating Characteristic.
- RTK** Real-Time Kinematic.
- SAS** Signal Authentication Service.
- SCA** Spreading Code Authentication.

SCE Spreading Code Encryption.

SCER Security Code Estimation and Replay.

SDR Software-Defined Radio.

SQM Signal Quality Monitoring.

STEC Slant Total Electron Content.

SV Space Vehicle.

TEC Total Electron Content.

TECU Total Electron Content Unit (10^{16} e⁻/m²).

TESLA Timed Efficient Stream Loss-tolerant Authentication.

TOA Time-Of-Arrival.

VSS Vestigial Signal Search.

WGS-84 World Geodetic System 1984.

Capítol 1

Introducció

1.1 Context i motivació

Els sistemes globals de navegació per satèl·lit (Global Navigation Satellite System (GNSS)) proporcionen avui dia posicionament, velocitat i temps (Position, Velocity and Time (PVT)) a milers de milions de dispositius. El que va començar com una capacitat militar (amb el Global Positioning System (GPS)) s'ha transformat en una infraestructura civil crítica de la qual depenen sectors tan diversos com l'aviació, el transport, les xarxes elèctriques, els mercats financers i les xarxes de telecomunicacions, totes elles fortament dependents de la sincronització temporal que ofereix el GNSS [Bor23].

Aquesta dependència creixent contrasta amb una debilitat estructural del senyal GNSS: en arribar a la superfície terrestre després de recórrer més de 20 000 km, la potència rebuda se situa molt per sota del nivell de soroll tèrmic. Aquest fet, sumat a la publicitat de les estructures de codi del servei obert, fa que el senyal sigui especialment vulnerable a dos tipus d'atacs: el *jamming* (interferència que nega el servei) i, sobretot, el *spoofing* —la transmissió de senyals falsificats que imiten els autèntics per induir el receptor a calcular una posició o un temps erronis sense que l'usuari en sigui conscient [Psi16, Hum08]. La proliferació de plataformes de ràdio definida per programari (Software-Defined Radio (SDR)) de baix cost ha reduït dràsticament la barrera tècnica i econòmica d'aquests atacs, fet que ha convertit l'autenticació del senyal GNSS en una línia de recerca prioritària.

Per fer-hi front, el programa europeu Galileo ha estat pioner a incorporar mecanismes criptogràfics d'autenticació directament en el senyal de radiodifusió. Galileo ofereix actualment dues capes d'autenticació complementàries i, fins avui, és l'únic GNSS que les proporciona de manera simultània [FH24]: l'Open Service Navigation Message Authentication (OSNMA), que autentica les dades de navegació, i el Signal Authentication Service (SAS), que afegeix autenticació a nivell

de senyal xifrant la component E6-C i posant a disposició dels usuaris unes seqüències rexifrades (Re-Encrypted Code Sequences (RECS)) que el receptor pot desxifrar i correlacionar amb el senyal rebut [FH23, FH24].

El grup de recerca SPCOMNAV de la Universitat Autònoma de Barcelona ha estat un dels actors principals en la definició i la validació experimental del SAS, des de les primeres propostes de paràmetres de disseny [TG22a, TG22b] fins a la construcció de plataformes SDR de captura sincronitzada E1/E6 [TG23a] i la primera campanya de validació end-to-end amb senyal E6-C xifrat real, duta a terme el juny de 2025 [TG25]. Fruit d'aquest treball, el grup ha desenvolupat SASlib, una biblioteca de codi obert en Python que implementa la cadena completa de processament d'un receptor SAS [TG26a]. Aquest TFG s'emmarca directament en aquest esforç: l'estudiant n'és coautor de l'article que la presenta.

1.2 Objectius

L'objectiu general d'aquest Treball de Fi de Grau és dissenyar, implementar i validar la cadena de processament de senyal d'un receptor del Servei d'Autenticació de Senyal (SAS) de Galileo, capaç de generar mesures de rang autenticades a partir de la correlació de les seqüències desxifrades amb el senyal E6-C rebut, i generar un posicionament semi-autenticat. A més aquest treball es realitza en coordinació amb un TFG complementari de l'àmbit de l'Enginyeria Informàtica (vegeu la Secció 3.2.1), que se n'ocupa de l'arquitectura de programari, la criptografia i la interfície.

Els objectius específics són:

1. **Estudiar l'estat de l'art** dels GNSS (arquitectura, senyal i receptor) i de les tècniques d'autenticació GNSS, tant a nivell de dades (OSNMA) com a nivell de senyal (SAS/ACAS).
2. **Implementar el bloc de correlació** de les bandes E1 i E6, incloent l'adquisició mitjançant la funció d'ambigüitat creuada, la cerca de Doppler aproximada i fina, la integració post-detecció i la detecció robusta del pic de correlació.
3. **Definir i calcular les mètriques de qualitat i d'autenticació** (PPSP, SNR, C/N_0) que permeten decidir si la correlació de la seqüència desxifrada amb el senyal rebut és satisfactòria.
4. **Integrar l'assistència de fase de codi** per acotar la finestra de cerca a la banda E6-C xifrada i reduir el cost i la falsa alarma.
5. **Implementar l'autenticador de rang i el càlcul de PVT** a partir de les mesures autenticades.

6. **Validar** el sistema amb dades reals E1/E6 capturades amb la plataforma SDR bladeRF i amb el conjunt de la campanya E6-C xifrada de juny de 2025 [TG25].

1.3 Estructura del document

La memòria s'organitza en sis capítols que segueixen el fil natural del treball (del marc teòric fins a la validació experimental) més un apèndix de material addicional. Després d'aquesta introducció (Capítol 1), que n'ha fixat el context, els objectius i l'abast, la resta s'estructura de la manera següent.

El Capítol 2 estableix l'estat de l'art i el marc teòric. Comença pels fonaments dels GNSS —arquitectura i sistemes actuals, principi de posicionament, estructura del senyal (modulacions BPSK i BOC) i efectes de propagació—; segueix amb el receptor GNSS, posant l'èmfasi en l'adquisició mitjançant la funció d'ambigüïtat creuada, la integració coherent i no coherent, la detecció basada en corbes ROC i el cas snapshot sobre el qual es fonamenta el SAS; i acaba amb els disruptors del senyal —no intencionats i intencionats (*jamming*, *meaconing* i *spoofing*)— i les contramesures a nivell de receptor i de sistema, entre les quals s'emmarquen l'OSNMA i el SAS/ACAS.

El Capítol 3 descriu la metodologia. D'una banda, els materials i les eines: els antecedents i la feina prèvia del grup SPCOMNAV, la biblioteca SASlib, la plataforma de captura SDR bladeRF, les dades auxiliars (claus TESLA, RECS, BGD, efemèrides) i els documents normatius de referència. De l'altra, el disseny i el procediment: el repartiment de responsabilitats amb el TFG complementari d'Enginyeria Informàtica, el flux de processament del pipeline de SASlib (13 blocs organitzats en quatre etapes) i la metodologia de validació.

El Capítol 4 detalla el desenvolupament i la implementació dels tres blocs de processament de senyal que constitueixen l'aportació pròpia d'aquest TFG: el bloc de correlació (*SignalCorrelation*), amb el càlcul de la CAF per FFT, la cerca de Doppler, la detecció del pic i l'assistència de fase de codi; el bloc de processament de rang per satèl·lit (*SatelliteAuthenticator*), amb la compensació E1–E6, la correcció ionosfèrica NeQuick-G i el llindar d'autenticació; i el computador de PVT (*PVTComputation*), basat en la navegació de temps aproximat.

El Capítol 5 recull els resultats experimentals i la seva discussió: la validació funcional amb el senyal E6-C xifrat real de la campanya de 2025, el refinament i l'autenticació de rang amb les captures pròpies E1/E6, la solució de posició (PVT) i la discussió global dels resultats. Finalment, el Capítol 6 presenta les conclusions i les línies de treball futur.

Tanca la memòria l'Apèndix A, amb material addicional: la referència dels paràmetres de configuració dels blocs i un exemple complet del pipeline d'execució.

Capítol 2

Estat de l'art i marc teòric

Aquest capítol estableix els fonaments necessaris per comprendre la resta del treball i situa la contribució respecte de l'existent. Primer es presenten els fonaments dels GNSS (arquitectura, posicionament, senyal i propagació) (Secció 2.1); tot seguit es descriu el receptor GNSS, amb èmfasi en l'adquisició, la detecció i el cas snapshot sobre el qual es basa el SAS (Secció 2.2); a continuació s'introdueixen els disruptors del senyal (no intencionats i intencionats) i les contra-mesures a nivell de receptor i de sistema, entre les quals s'emmarquen l'OSNMA i el SAS/ACAS (Secció 2.3).

2.1 Fonaments dels GNSS

Un Global Navigation Satellite System (GNSS) és un sistema que proporciona serveis de posicionament, navegació i sincronització de manera global i autònoma [TG24a]. No es redueix a la constel·lació de satèl·lits, sinó que es desplega en tres segments complementaris [Bor23, TG24a]: el segment espacial —la constel·lació de satèl·lits, que radiodifon els senyals de rang amb la informació de temps, òrbita i estat del satèl·lit—; el segment de control —les estacions de terra que en supervisen la salut i n'actualitzen les dades de navegació—; i el segment d'usuari —els receptors, que mesuren el temps de propagació dels senyals i en calculen la Position, Velocity and Time (PVT). Aquesta secció en repassa amb detall l'arquitectura i els sistemes actuals (Secció 2.1.1), el principi de mesura, l'estructura del senyal i els efectes de propagació que el degraden.

2.1.1 Arquitectura i sistemes actuals

Avui coexisteixen quatre GNSS globals: el Global Positioning System (GPS) (EUA), Galileo (UE), GLONASS (Rússia) i BeiDou (Xina). Les seves característiques principals es resumeixen a la Taula 2.1. Galileo, operatiu des de 2016, és el sistema civil europeu i destaca per oferir

serveis avançats com l'autenticació, objecte d'aquest treball.

Taula 2.1: Segment espacial dels GNSS globals en operació. Estructura adaptada de la Taula 2.1 de [TG24a]; paràmetres de Galileo verificats amb les dades oficials del programa [Eur24a].

Paràmetre	GPS	Galileo	GLONASS	BeiDou
País / regió	EUA	Europa	Rússia	Xina
Tipus d'òrbita	MEO	MEO	MEO	MEO/IGSO/GEO
Altitud (km)	20180	23222	19100	21530–35790
Plans orbitals	6	3 [†]	3	3
Satèl·lits nominals	24	24	24	30

[†] Galileo desplega 3 plans orbitals (constel·lació Walker 24/3/1: 8 satèl·lits per pla, inclinació 56°), segons els paràmetres orbitals oficials del programa [Eur24a]; la Taula 2.1 de [TG24a] n'indica 6. Els 24 satèl·lits són la constel·lació nominal activa; a més hi ha 6 satèl·lits auxiliars de reserva (fins a 30 en òrbita).

Tot GNSS s'estructura en tres segments [Bor23] (Figura 2.1):

- El **segment espacial**: la constel·lació de satèl·lits (cadascun identificat per un Space Vehicle (SV)) que radiodifonen els senyals de navegació. Per a Galileo, orbiten en Medium Earth Orbit (MEO) a uns 23 222 km d'altitud, amb rellotges atòmics d'alta estabilitat. Es disposen de manera que en tot moment hi hagi un mínim de quatre satèl·lits en línia de visió directa (LOS) des de qualsevol punt de la Terra.
- El **segment de control**: les estacions de terra que monitoren la salut de la constel·lació i actualitzen les dades de navegació (efemèrides, almanac, correccions de rellotge i atmosfèriques). En són components l'estació mestra (Master Control Station (MCS)), les estacions de monitoratge i les de pujada de dades. En el SAS, a més, el segment de terra genera i xifra les RECS.
- El **segment d'usuari**: els receptors, que processen els senyals per calcular la PVT. En varien enormement el cost i les prestacions, des de xips de baix cost en telèfons fins a plataformes de gamma alta per a temps de precisió.

Sobre aquesta infraestructura, Galileo proporciona diversos serveis: el Servei Obert (Open Service (OS)), l'Alta Precisió (High Accuracy Service (HAS), que difon correccions d'òrbita i rellotge a la banda E6-B), el Públic Regulat (Public Regulated Service (PRS), xifrat) i, de manera incremental, els d'autenticació OSNMA i SAS [FH24]. Aquests dos darrers, juntament amb el HAS, són l'evolució de l'antic Servei Comercial [TG24a].

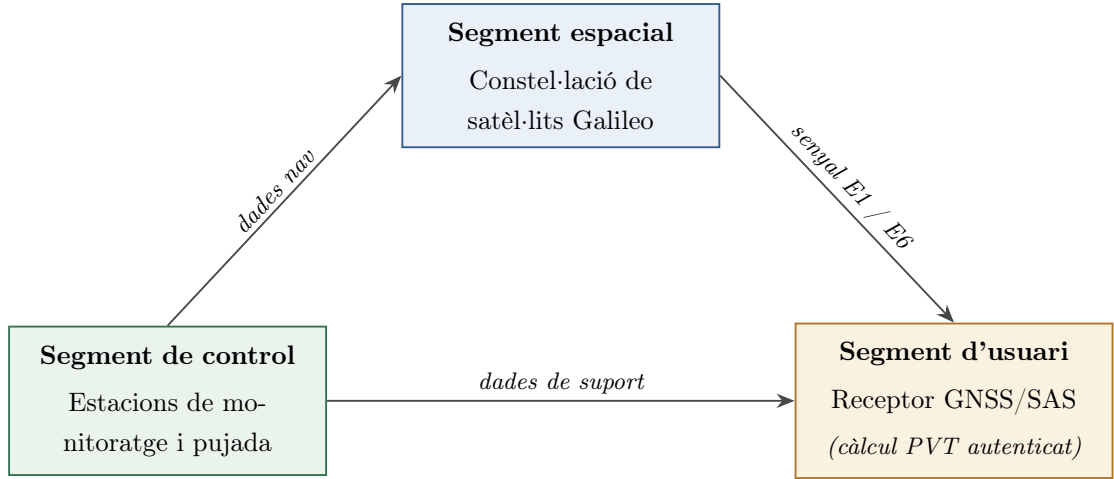


Figura 2.1: Els tres segments d'un sistema GNSS i el flux addicional de dades del SAS. Adaptat de [TG24a, Bor23].

2.1.2 Principi de posicionament

De les múltiples tècniques de localització, els GNSS empren el temps d'arribada (Time-Of-Arrival (TOA)) [Bor23]. Cada satèl·lit transmet una marca de temps $t_s^{(k)}$; el receptor en mesura l'instant de recepció $t_u^{(k)}$ i n'estima el retard de propagació

$$\tau^{(k)} = t_u^{(k)} - t_s^{(k)}. \quad (2.1)$$

A la pràctica, el receptor obté $t_s^{(k)}$ alineant una rèplica local del codi amb el senyal rebut i llegint el seu rellotge intern en aquell instant. La distància (o *rang*) s'obté multiplicant el retard per la velocitat de la llum c : $d^{(k)} = c\tau^{(k)}$. Geomètricament, cada rang defineix una superfície esfèrica centrada al satèl·lit; la intersecció de diverses superfícies dona la posició de l'usuari, en un procés conegut com a *trilateració* (Figura 2.2).

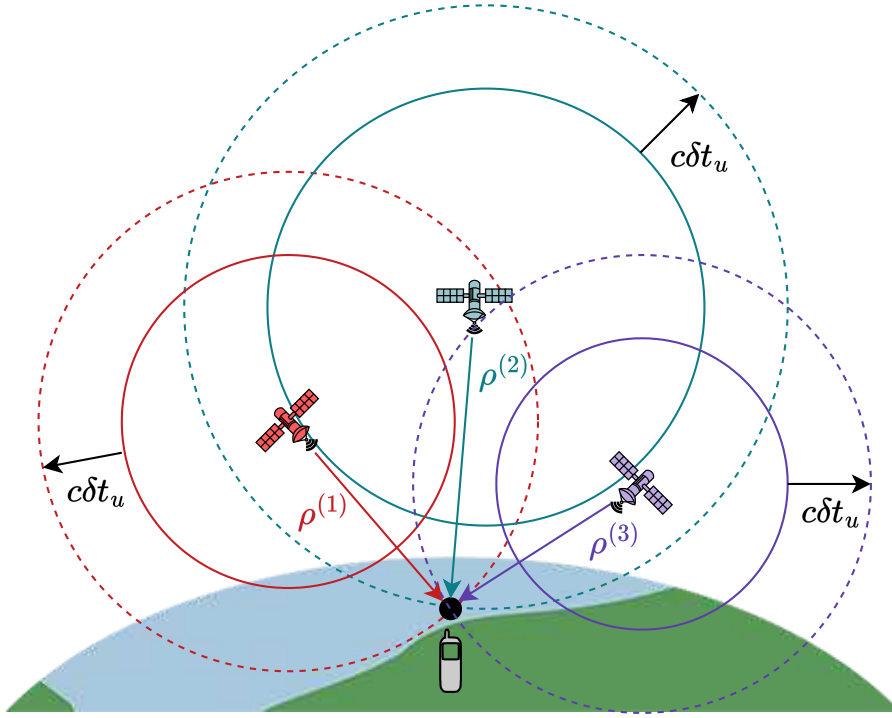


Figura 2.2: Principi de posicionament GNSS i efecte del biaix de rellotge del receptor ($c\delta t_u$), en el cas 2D. Adaptat de [TG24a], Fig. 2.9.

El rellotge del receptor, però, no està sincronitzat amb el temps del sistema: totes les mesures estan desplaçades un terme comú desconegut $c\delta t_u$, on δt_u és el biaix de rellotge de l'usuari. La magnitud mesurada és, doncs, la pseudodistància. Incloent-hi també els retards del satèl·lit i de propagació, per a cada satèl·lit i s'obté el model d'observació estàndard [Bor23, TG24a]:

$$\rho_i = \underbrace{\sqrt{(x_i - x_u)^2 + (y_i - y_u)^2 + (z_i - z_u)^2}}_{d_i} + c\delta t_u + c\delta t^{(i)} + I_i + T_i + \varepsilon_i, \quad (2.2)$$

on (x_i, y_i, z_i) és la posició del satèl·lit, (x_u, y_u, z_u) la incògnita de l'usuari, $\delta t^{(i)}$ el biaix de rellotge del satèl·lit, I_i i T_i els retards ionosfèric i troposfèric, i ε_i el soroll i el multicamí. El sistema té quatre incògnites (les tres coordenades i el biaix de rellotge), de manera que calen com a mínim quatre satèl·lits per a una posició 3D. En resoldre'l, el receptor també queda sincronitzat amb el temps del sistema.

El sistema és no lineal per l'arrel de l'Eq. (2.2). Es resol per dues famílies de mètodes [Bor23, TG24a]: la linealització per sèrie de Taylor de primer ordre al voltant d'una posició aproximada, resolta iterativament per mínims quadrats (Least Squares (LS))—l'enfocament emprat en aquest treball (Capítol 4)—, i els mètodes de forma tancada (algorisme de Bancroft), que eviten la iteració però amplifiquen el soroll. A més de la pseudodistància (mesura de codi), el receptor pot mesurar la fase de portadora, uns dos ordres de magnitud més precisa; les tècniques Real-Time

Kinematic (RTK) i Precise Point Positioning (PPP) hi assolixen precisió centimètrica, davant la mètrica del posicionament per codi [Bor23].

2.1.3 El senyal GNSS: codis i modulacions (BPSK i BOC)

Els senyals GNSS empren espectre eixamplat per seqüència directa (Direct-Sequence Spread Spectrum (DSSS)): el senyal de dades es multiplica per una seqüència binària molt més ràpida (el codi d'eixamplament, els bits del qual s'anomenen chips) de manera que el senyal s'estén sobre una banda molt més ampla i apareix com un senyal de baixa potència, gairebé indistingible del soroll de fons [TG24a]. La relació entre la velocitat de chip R_c i la de símbol R_s és el guany de processament, típicament entre 10 i 60 dB:

$$G_c = \frac{R_c}{R_s}. \quad (2.3)$$

Aquest guany és el que permet recuperar el senyal sota el soroll i el confereix robustesa davant les interferències de banda estreta (Figura 2.3).

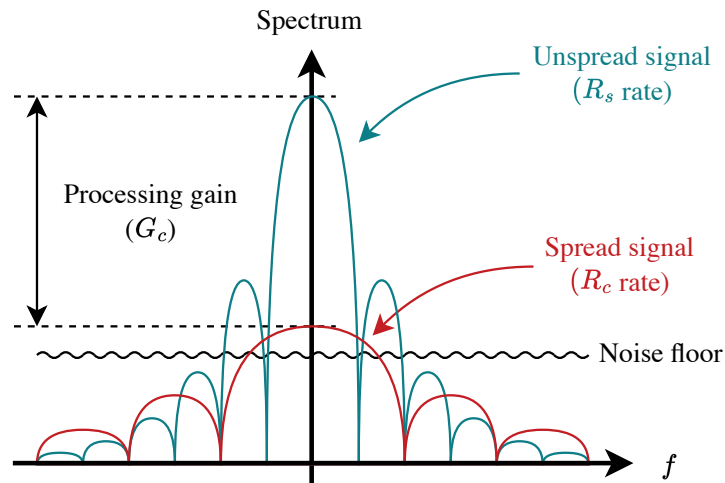


Figura 2.3: Guany de processament G_c en les tècniques d'espectre eixamplat. Adaptat de [TG24a], Fig. 2.3.

Cada satèl·lit modula un codi Pseudo-Random Noise (PRN) característic, amb propietats de correlació semblants al soroll blanc: l'autocorrelació té un pic distingible quan el codi s'alinea amb si mateix i és pràcticament nul·la altrament,

$$R_c[m] = \frac{1}{L} \sum_{n=0}^{L-1} c[n] c[n+m] \approx \begin{cases} 1 & m = 0, \\ \approx 0 & m \neq 0, \end{cases} \quad (2.4)$$

mentre que la correlació creuada entre codis de satèl·lits diferents és gairebé nul·la. Això permet detectar cada satèl·lit individualment i mesurar-ne el retard, i alhora compartir la mateixa banda:

és l'accés múltiple per divisió de codi (Code Division Multiple Access (CDMA)), emprat per GPS, Galileo i BeiDou. GLONASS, en canvi, usa divisió en freqüència (Frequency Division Multiple Access (FDMA)) amb un mateix codi per a tots els satèl·lits [TG24a].

Un senyal GNSS queda definit per quatre elements [TG24a]: la modulació que conforma el pols de chip, el codi de rang (codi primari), els símbols de dades i la freqüència portadora. Aquests elements s'articulen en una estructura per capes (Figura 2.4).

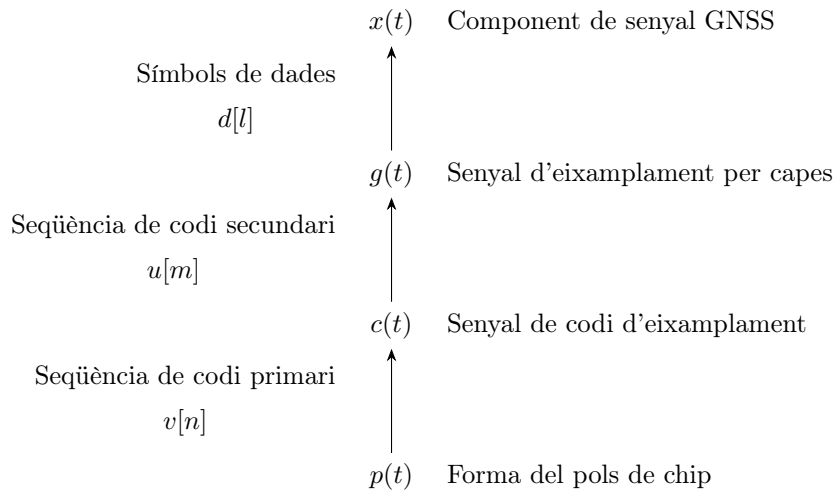


Figura 2.4: Estructura per capes d'un component de senyal GNSS. Recreada a partir de [TG24a], Fig. 2.5.

Modulació del pols de chip. Determina la forma del pic de correlació i, per tant, la resolució temporal i la robustesa davant el multicamí. Se'n distingeixen dues famílies (els polsos es mostren a la Figura 2.5):

- La Binary Phase-Shift Keying (BPSK), en què el codi modula directament la portadora amb un pols rectangular. Dóna una autocorrelació triangular d'un sol pic, d'amplada un chip. El seu pols és $p_{\text{BPSK}}(t) = \Pi(t/T_c)$, amb T_c el període de chip.
- La Binary Offset Carrier (BOC), en què cada chip es multiplica per una subportadora quadrada de freqüència igual o superior a la de chip. El resultat és un espectre dividit en dos lòbuls i una autocorrelació amb un pic central més estret (millor resolució i més immunitat al multicamí) a costa de pics laterals que cal gestionar en l'adquisició. Es denota $\text{BOC}(m,n)$ segons les freqüències de subportadora i de chip (per exemple, $\text{BOC}(1,1)$ o $\text{BOC}(6,1)$).

L'E1 de Galileo no empra una BOC simple, sinó la Composite Binary Offset Carrier (CBOC), denotada $\text{CBOC}(6,1,1/11)$: una BOC multiplexada (MBOC) que combina una $\text{BOC}(1,1)$ de

banda estreta (10/11 de la potència) amb una BOC(6,1) de banda ampla (1/11) [TG24a, Eur23b]. Com que la BOC(1,1) hi domina la potència i la forma de l'autocorrelació (Figura 2.6), en aquest treball l'E1 s'aproxima per BOC(1,1).

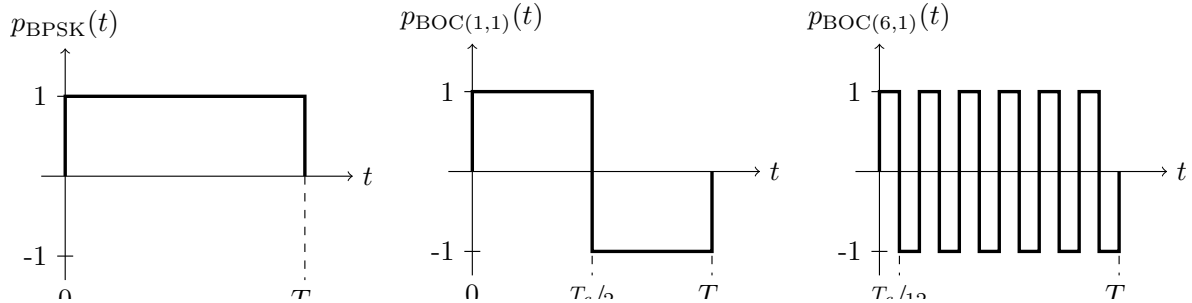


Figura 2.5: Polsos de chip de BPSK, BOC(1,1) i BOC(6,1). Adaptat de [TG24a], Fig. 2.6.

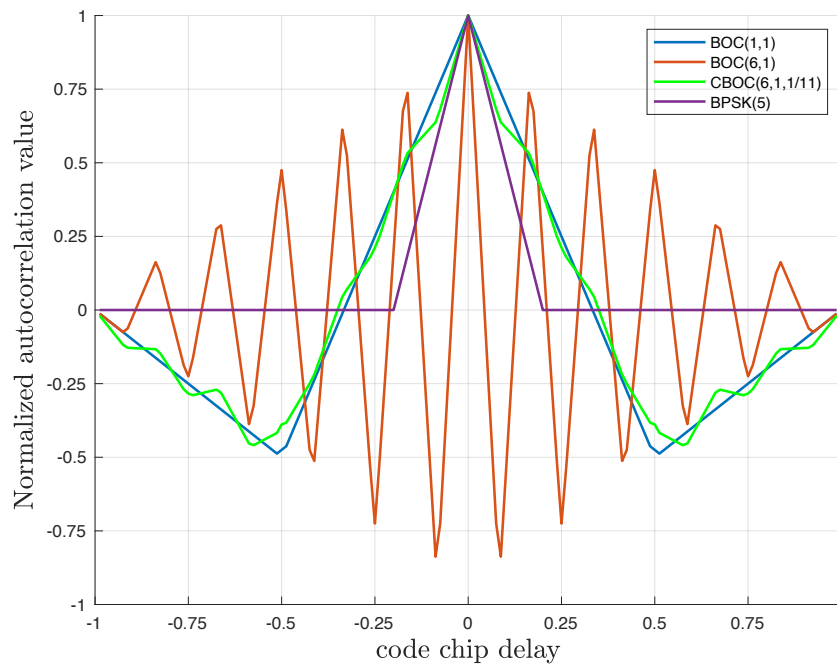


Figura 2.6: Funcions d'autocorrelació dels polsos de Galileo E1 —BOC(1,1), BOC(6,1) i la CBOC(6,1,1/11)— i de l'E6 (BPSK(5)). Adaptat de [TG24a], Fig. 3.6.

Codi de rang i símbols de dades. El codi primari es tria per les seves propietats de correlació; n'hi ha de generats per registres de desplaçament (codis de Gold del C/A del GPS) i de memòria, dissenyats a mida (com l'E6 de Galileo) [TG24a]. Sobre el codi primari es modulen els símbols de dades (el missatge de navegació) i, sovint, un codi secundari conegut a priori que n'allarga el període i en millora la correlació. Segons això es distingeixen dos tipus de canal: els canals de dades, amb símbols desconeguts (missatge de navegació, com l'E1-B), i els canals pilot,

amb símbols coneguts (codi secundari, com l'E6-C), òptims per a integracions llargues.

Freqüència portadora. Els senyals GNSS es transmeten en banda L (de 1,2 a 1,6 GHz), poc afectada per l'atenuació atmosfèrica. Cada senyal ocupa una sub-banda; algunes són compartides entre sistemes per a la interoperabilitat (Figura 2.7).

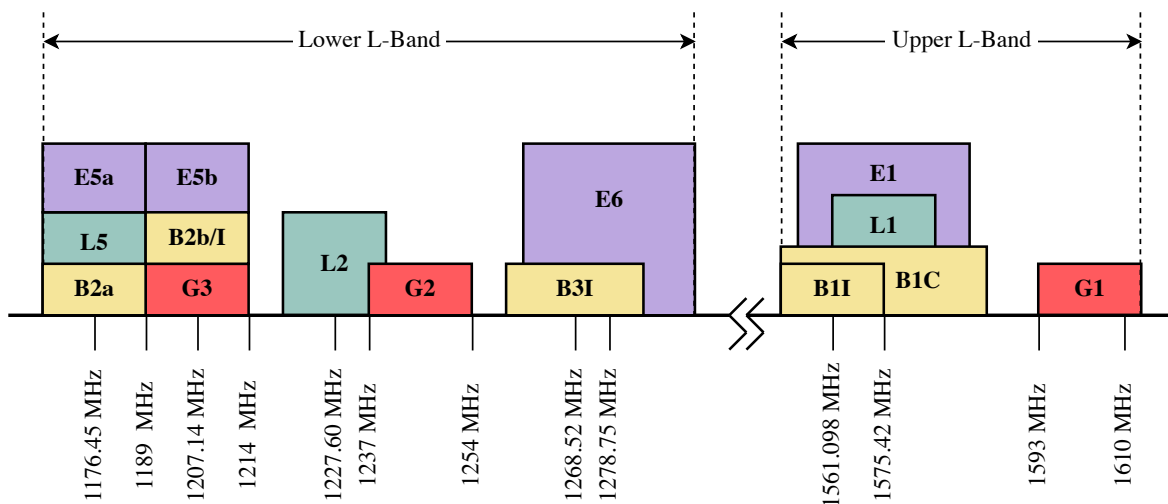


Figura 2.7: Espectre de les bandes GNSS en banda L (GPS, GLONASS, Galileo i BeiDou), amb les bandes E1 i E6 de Galileo.

El SAS opera generalment amb dues bandes ben diferenciades, resumides a la Taula 2.2. La diferència clau és que l'E6 té cinc vegades més resolució de codi que l'E1 ($\approx 58,6\text{m}$ per chip davant $\approx 293\text{m}$), cosa que confereix al SAS la precisió necessària per a l'autenticació de rang i la robustesa davant el multicamí. Cal dir que també es pot operar amb la banda E5, però no s'ha considerat en la part pràctica d'aquest treball.

Taula 2.2: Paràmetres principals de les bandes Galileo E1 i E6 emprades en el SAS, segons l'OS SIS ICD [Eur23b].

Paràmetre	E1	E6
Freqüència portadora	1575,42 MHz	1278,75 MHz
Component d'interès	E1-B (dades, OSNMA)	E6-C (pilot, SAS)
Velocitat de chip	1,023 Mcps	5,115 Mcps
Longitud del codi	4092 chips	5115 chips
Període del codi	4 ms	1 ms
Modulació	CBOC / BOC(1,1)	BPSK(5)
Longitud de chip	≈ 293 m	$\approx 58,6$ m

2.1.4 Efectes de propagació

El rang mesurat es desvia del geomètric per diversos efectes [Bor23, TG24a]:

- **Retard ionosfèric:** la ionosfera és un medi dispersiu; el retard és proporcional al contingut total d'electrons (Total Electron Content (TEC)) i invers al quadrat de la freqüència ($\propto 1/f^2$). Es corregeix amb models (Klobuchar, NeQuick-G) o, millor, amb combinació de doble freqüència. Precisament la seva dependència amb f és l'origen del terme diferencial E1-E6 del model d'error del SAS (Capítol 4). Les scintil·lacions ionosfèriques (fluctuacions ràpides de fase i amplitud) en són un cas sever.
- **Retard troposfèric:** no dispersiu; depèn de pressió, temperatura i humitat. Es modela amb una component seca (hidrostàtica) i una de humida i una funció de mapatge en funció de l'elevació (Saastamoinen, Goad–Goodman).
- **Multicamí:** reflexions del senyal en superfícies properes que arriben amb retard i distorsionen el pic de correlació. És la principal font d'error residual i, per a aquest treball, una font de confusió amb atacs, perquè pot produir distorsions semblants a les d'un spoofing incipient (Figura 2.8).
- **Efectes relativistes i rotació terrestre** (efecte Sagnac): correccions deterministes, de menor magnitud però necessàries per a la precisió.

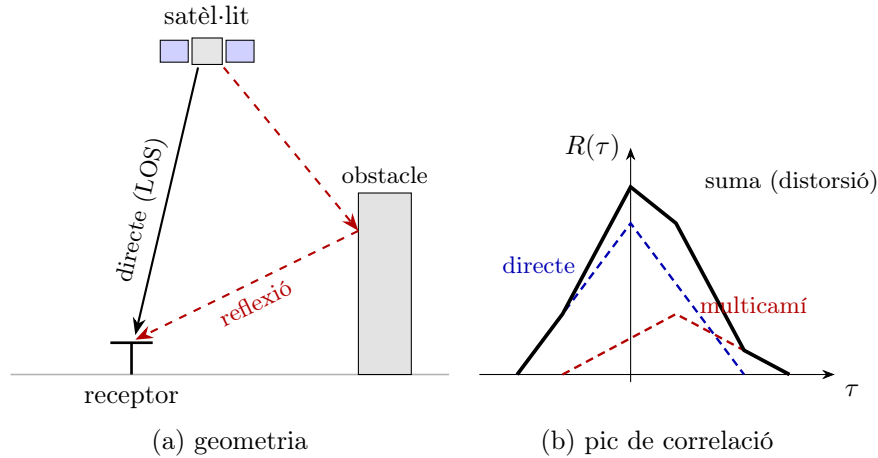


Figura 2.8: Efecte del multicamí: (a) geometria de la recepció (senyal directe LOS i rèplica reflectida); (b) distorsió resultant del pic d'autocorrelació. Diagrama conceptual.

La contribució de tots aquests efectes no corregibles se sintetitza en el terme $\varepsilon^{(k)}$ de la pseudodistància corregida, $\rho^{(k)} = d^{(k)} + c\delta t_u + \varepsilon^{(k)}$. La seva desviació típica és de l'ordre d'1 m amb correccions diferencials i de 5 m a 10 m amb el receptor operant de manera autònoma [TG24a]. Més endavant es veurà que, en un receptor SAS, aquesta desviació és un factor clau per a l'autenticació de rang (Capítol 4).

2.2 El receptor GNSS

Un receptor GNSS converteix el senyal de RF en una solució PVT a través de tres blocs [Bor23, TG24a] (Figura 2.9): el front-end, el mòdul de processament de senyal (adquisició i, opcionalment, seguiment) i el mòdul de navegació. L'adquisició és l'etapa clau per al SAS: com que opera en mode snapshot (sobre una instantània curta), l'autenticació es fonamenta en la detecció d'un pic de correlació, sense seguiment continu.

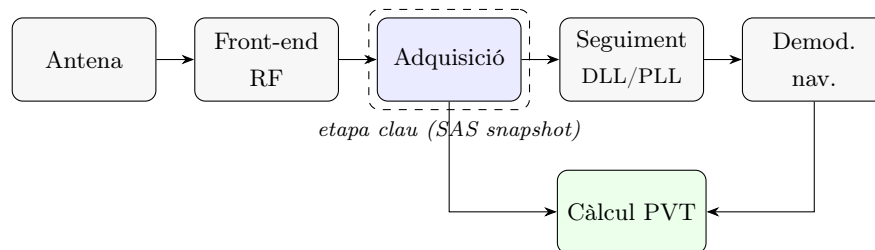


Figura 2.9: Cadena de processament d'un receptor GNSS. Adaptat de [Bor23, TG24a].

2.2.1 Front-end de RF i captura SDR

El front-end converteix el senyal analògic de banda passant captat per l'antena en un senyal digital de banda base, perquè la resta del receptor operi amb tècniques de processament digital (Digital Signal Processing (DSP)). Inclou les tasques clàssiques de condicionament: filtratge passabanda i amplificació de baix soroll (Low-Noise Amplifier (LNA)), conversió a banda base i conversió analògica-digital (Analog-to-Digital Converter (ADC)). El control automàtic de guany (Automatic Gain Control (AGC)) n'ajusta el nivell abans de l'ADC i és, com es veurà, un indicador d'interferència.

En arribar a l'antena, el senyal d'un satèl·lit queda caracteritzat per tres paràmetres [TG24a]: el retard τ (propagació), el desplaçament Doppler f_d (moviment relatiu satèl·lit-usuari) i la fase de portadora θ . Després del condicionament i la digitalització, el senyal en banda base d'un satèl·lit es modela com

$$r[n] = \sqrt{P_r} x[n - n_d] e^{j(2\pi f_d n + \theta)} + w[n], \quad (2.5)$$

on $x[n]$ és la component del senyal (codi $\times$ dades), P_r la potència rebuda, $n_d = \tau/T_s$ i f_d els equivalents discrets del retard i el Doppler, $T_s = 1/f_s$ el període de mostreig, i $w[n]$ un soroll blanc gaussià additiu (Additive White Gaussian Noise (AWGN)) que engloba el soroll de fons, el del receptor i la resta de satèl·lits [TG24a].

2.2.2 Adquisició i funció d'ambigüitat creuada

L'adquisició estima, per a cada satèl·lit, una primera estimació aproximada del desplaçament de codi n_d i del doppler f_d ($\pm 6,5$ kHz per a un receptor estàtic). És, doncs, una cerca bidimensional sobre la graella temps $\times$ freqüència (l'espai de cerca) calculant la Cross-Ambiguity Function (CAF):

$$\chi(\tau, f_d) = \frac{1}{N} \sum_{n=0}^{N-1} r[n] c^*[n - \tau] e^{-j2\pi f_d n / f_s}. \quad (2.6)$$

La detecció es declara quan l'envolupant $|\chi(\tau, f_d)|^2$ supera un llindar (Secció 2.2.6). Hi ha tres maneres d'explorar l'espai de cerca [TG24a, Bor23]: la cerca sèrie, que prova cada parell (τ, f_d) individualment ($\mathcal{O}(N^2)$); la cerca paral·lela en fase de codi, que avalua totes les fases de codi alhora per a cada Doppler aprofitant la Fast Fourier Transform (FFT) (la implementada en aquest treball),

$$\chi(\tau, f_d) = \mathcal{F}^{-1}\{ \mathcal{F}\{r[n]\} \cdot \mathcal{F}^*\{c[n] e^{j2\pi f_d n / f_s}\} \}, \quad (2.7)$$

amb un cost $\mathcal{O}(N \log N)$; i la cerca paral·lela en freqüència, dual de l'anterior, que per a cada fase de codi avalua simultàniament totes les freqüències Doppler mitjançant una FFT sobre la dimensió temporal (DoubleFFT). El resultat és una superfície amb un pic net en la posició (τ, f_d) correcta (Figura 2.10).

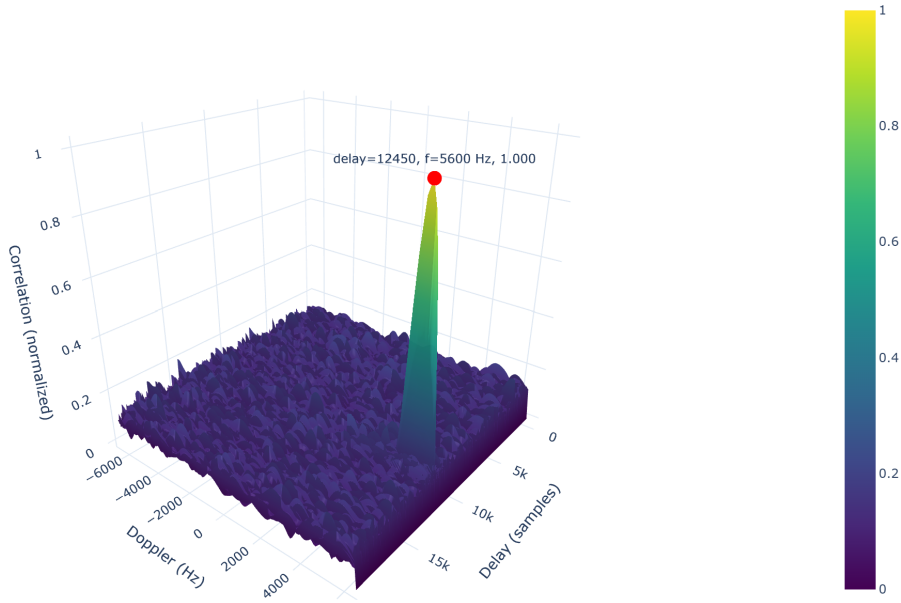


Figura 2.10: Funció d'ambigüitat creuada (CAF) resultant de l'adquisició, en una execució real del bloc *SignalCorrelation* (vegeu Capítol 5).

2.2.3 Integració coherent i no coherent

Per detectar senyals febles cal allargar el temps d'integració, i es pot fer de dues maneres [TG24a]. En la integració coherent se sumen N_c sortides complexes consecutives de la CAF: el guany d'SNR creix linealment amb N_c , però cal mantenir la coherència de fase durant tot l'interval, de manera que queda limitada per les transicions de bit de dades, la deriva de rellotge i el Doppler residual. En la integració no coherent o post-detecció (Post-Detection Integration (PDI)) se sumen els mòduls de N_i blocs: això elimina la restricció de fase a costa de la pèrdua per detecció quadràtica, i el guany creix més lentament (de l'ordre de $\sqrt{N_i}$). La variable de decisió de cada bloc és l'envolupant de la CAF,

$$z = |\chi(\tau, f_d)|^2 = \chi_I^2(\tau, f_d) + \chi_Q^2(\tau, f_d), \quad (2.8)$$

i el temps total d'integració és $T_{\text{int}} = N_c N_i T_{\text{codi}}$. Aquí només se n'introdueix el principi; aquest efecte (un pic de correlació net molt per damunt del soroll) s'explica i s'entén millor amb els resultats sobre senyal real del Capítol 5.

2.2.4 Seguiment i receptors snapshot

Un cop adquirit el senyal, un receptor convencional en refina i manté les estimacions en bucle tancat [TG24a, Bor23]. Empra dos llaços en paral·lel: un Delay-Locked Loop (DLL) per a la fase

de codi i un Phase-Locked Loop (PLL) per a la de portadora. Tots dos consten d'un discriminador, un filtre de llaç i un oscil·lador controlat numèricament (Numerically Controlled Oscillator (NCO)): es compara el senyal amb la rèplica local, el discriminador en genera un senyal d'error, el filtre el suavitza i l'NCO actualitza la rèplica, tancant el llaç. És l'arquitectura adequada quan el receptor opera de manera contínua i necessita demodular el missatge de navegació, i s'enforteix amb tècniques com els filtres de Kalman adaptatius en entorns difícils.

Un receptor snapshot, en canvi, opera en bucle obert sobre una instantània curta del senyal, sense seguiment [FH16]: les estimacions aproximades de l'adquisició (sovint refinades amb una cerca fina de Doppler) es proporcionen directament com a sortida. S'utilitza quan només es disposa d'una captura breu, en receptors d'alta sensibilitat (High-Sensitivity GNSS (HS-GNSS)) i en entorns amb esvaïments, on és més robust per ser menys sensible a les interrupcions; el preu és una precisió menor que la del bucle tancat [TG24a]. Aquesta és l'arquitectura natural del SAS: l'autenticació es fonamenta en una sola instantània. El seu repte és que el receptor no demodula prou missatge per situar-se —li falten el temps absolut i les efemèrides, que ha d'obtenir de fonts auxiliars (OSNMA, GNSS assistit Assisted GNSS (A-GNSS), RINEX)— i que treballar amb codis curts i sense temps absolut introdueix ambigüitats (de període de codi i de mil·lisegon) que es resolen amb la mesura d'una banda de referència, la navegació de temps aproximat i la coherència entre satèl·lits (Capítol 4).

2.2.5 Model de rellotge i referència temporal

El biaix de rellotge del receptor, δt_u , és una de les incògnites de l'Eq. (2.2); a més, les seves inestabilitats introdueixen un soroll que fa derivar la fase de la portadora. Si durant la integració aquesta fase deriva prou —fins a superar un cicle sencer, l'anomenat embolcall de fase (*phase wrapping*)—, les mostres complexes de la CAF deixen de sumar-se en fase i es perd el guany coherent, cosa que limita el temps durant el qual el receptor pot integrar coherentment [TG24a]. La qualitat d'un rellotge s'analitza en termes d'inestabilitat freqüencial: per caracteritzar-la no és útil la desviació típica, ja que divergeix per a alguns tipus de soroll, sinó la variància d'Allan (Allan Variance (AVAR)), o variància de dues mostres, que convergeix a valors finits per als principals tipus de soroll dels oscil·ladors de precisió [All66, TG24a].

Per simular aquest soroll de fase s'usa el model de dos estats (Figura 2.11), amb un estat de biaix x_b i un de deriva x_d [TG24a]:

$$x_d[n+1] = x_d[n] + u_d[n] T_s, \quad (2.9)$$

$$x_b[n+1] = x_b[n] + u_b[n] T_s + x_d[n] T_s, \quad (2.10)$$

on u_b i u_d són dos sorolls gaussians independents i T_s el període de mostreig. La potència de cada soroll depèn del tipus de rellotge i ve fixada per les amplituds espectrals $S_f = h_0/2$ i

$S_g = 2\pi^2 h_{-2}$: els coeficients h_0 (soroll blanc de freqüència) i h_{-2} (camí aleatori de freqüència) caracteritzen, respectivament, l'estabilitat a curt i a llarg termini del rellotge.

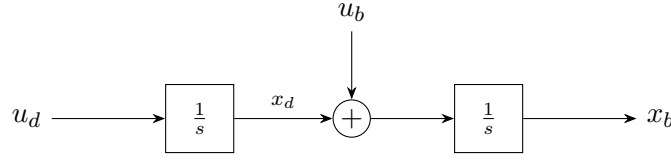


Figura 2.11: Model de rellotge de dos estats (deriva x_d i biaix x_b). Adaptat de [TG24a], Fig. 2.15.

En aquest treball, la referència temporal absoluta s'obté per Network Time Protocol (NTP), que en fixa l'origen amb prou exactitud per acotar la cerca i per satisfer el requisit de sincronització amb el Galileo System Time (GST) que imposa l'OSNMA (entre 30 i 300 s) [Eur24b]. La conversió entre escales de temps ha de tenir en compte el desfasament de segons (*leap seconds*): a les campanyes de 2026, $\text{GST} = \text{UTC} + 18 \text{ s}$. Aquesta referència, juntament amb la navegació de temps aproximat, permet resoldre les ambigüitats sense disposar del temps absolut que donaria un seguiment convencional.

2.2.6 Detecció de senyal i corbes ROC

L'adquisició és, en el fons, un problema de detecció [TG24a]: cal decidir entre la hipòtesi nul·la $\mathcal{H}_0$ (senyal absent o mal alineat) i l'alternativa $\mathcal{H}_1$ (senyal present i alineat), a partir de la variable de decisió $z = |\chi(\tau, f_d)|^2$ de l'Eq. (2.8). Es caracteritza per la probabilitat de falsa alarma P_{fa} i la de detecció P_d :

$$P_{fa}(\gamma) = \Pr\{z > \gamma \mid \mathcal{H}_0\}, \quad P_d(\gamma) = \Pr\{z > \gamma \mid \mathcal{H}_1\}, \quad (2.11)$$

on γ és el llindar de detecció. Amb soroll AWGN, la part real i imaginària de la CAF són gaussianes independents, de manera que sota $\mathcal{H}_0$ la variable z segueix una distribució khi quadrat *central* de 2 graus de llibertat (equivalent a una exponencial), i sota $\mathcal{H}_1$ una khi quadrat *no central* amb paràmetre de no-centralitat λ [TG24a]:

$$z \mid \mathcal{H}_0 \sim \chi_2^2(\sigma_n^2), \quad z \mid \mathcal{H}_1 \sim \chi_{nc,2}^2(\lambda, \sigma_n^2). \quad (2.12)$$

D'aquí surten expressions tancades per a les probabilitats: $P_{fa}(\gamma) = \exp\{-\gamma/2\sigma_n^2\}$ i $P_d(\gamma) = Q_1(\sqrt{\lambda/\sigma_n^2}, \sqrt{\gamma/\sigma_n^2})$, amb Q_1 la funció de Marcum d'ordre 1. Fixada una P_{fa} objectiu, el llindar i la probabilitat de detecció resultants són

$$\gamma = -2\sigma_n^2 \ln P_{fa}, \quad P_d = Q_1\left(\sqrt{\lambda/\sigma_n^2}, \sqrt{-2 \ln P_{fa}}\right). \quad (2.13)$$

En aplicar N_i integracions no coherents, P_d es generalitza amb la funció de Marcum d'ordre N_i , $P_{d,N_i}(\gamma) = Q_{N_i}(\sqrt{N_i \lambda/\sigma_n^2}, \sqrt{\gamma/\sigma_n^2})$ [TG24a]. Finalment, en avaluar tot l'espai de cerca de M

cel·les independents, la probabilitat global de falsa alarma és $P_{FA} = 1 - (1 - P_{fa})^M$, mentre que la de detecció global s'aproxima per la d'una cel·la.

La decisió pot donar quatre resultats (vertader/fals positiu i vertader/fals negatiu) i P_d i P_{fa} no són independents: abaixar el llindar augmenta totes dues. El compromís es visualitza amb la corba Receiver Operating Characteristic (ROC), que representa P_d enfront de P_{fa} en variar γ ; l'àrea sota la corba (Area Under the Curve (AUC)) en resumeix la bondat. Aquest marc és central en aquest treball: les prestacions del SAS s'expressen com P_d per a una P_{fa} fixada [TG22b, FH23], criteri amb què SPCOMNAV ha dimensionat els paràmetres del servei.

2.3 Disruptors del senyal i contramesures

La integritat d'una solució GNSS es pot veure compromesa per disruptors del senyal de naturalesa molt diferent. Convé classificar-los en dos grans grups [TG24a]: les perturbacions no intencionades (Secció 2.3.1), pròpies del sistema, de l'entorn o d'altres serveis de RF, i les intencionades (Secció 2.3.2), causades per un adversari. Davant d'aquestes amenaces, les contramesures actuen a dos nivells complementaris: a nivell de receptor (més aviat *hardware*) (Secció 2.3.3), de manera autònoma i sense criptografia, i a nivell de sistema (Secció 2.3.4), mitjançant l'autenticació criptogràfica que aporten l'OSNMA i el SAS/ACAS —el marc on s'inscriu aquest treball. La Secció 2.3.5 apunta cap a l'autenticació de segona generació.

2.3.1 Pertorbacions no intencionades

No tota degradació del servei és fruit d'un atac [TG24a]. Una part important prové del propi sistema i de l'entorn: el soroll tèrmic del receptor, el multicamí (reflexions que distorsionen el pic de correlació, Secció 2.1.4), els retards atmosfèrics i la pèrdua de visibilitat en entorns urbans o boscosos. Dins d'aquesta categoria, les scintil·lacions ionosfèriques (fluctuacions de fase i amplitud del senyal per irregularitats de densitat electrònica) són una de les fonts d'error principals. Una altra part prové d'altres sistemes: la Radio-Frequency Interference (RFI), que pot ser entre sistemes o dins del mateix sistema, polsant o contínua, de banda ampla o estreta, dins o fora de banda. Un exemple típic és la difusió de televisió digital terrestre (DVB-T), els harmònics de la qual poden coincidir amb les bandes GPS L1 o Galileo E1 [TG24a]. Aquestes perturbacions degraden la disponibilitat i l'exactitud, però no són malicioses; en la majoria de casos es mitiguen amb disseny de front-end, filtratge adaptatiu i models de correcció [Bor23]. La rellevància per a aquest treball és doble: el multicamí, en particular, és la principal font d'error residual i una font de confusió amb atacs, perquè pot produir distorsions del pic semblants a les d'un spoofing.

2.3.2 Pertorbacions intencionades: *jamming*, *meaconing* i *spoofing*

Jamming. Atac de denegació de servei: ús deliberat de soroll o senyals de RF d'alta potència a la banda GNSS per impedir que el receptor distingeixi el senyal autèntic. Degrada severament la relació portadora-soroll o, si satura el front-end, provoca la pèrdua total dels llaços [TG24a]. Fàcil d'executar i de detectar (es perd el servei) via monitorització de potència/AGC. En té variants de banda ampla, de to (CW) i polsant.

Meaconing. Reemissió del senyal genuí amb retard controlat, sense generar-ne cap de nou. Com que els bits són autèntics, supera l'OSNMA; però introdueix un retard anòmal que el SAS, en verificar el temps d'arribada, sí que pot detectar. És una de les motivacions fonamentals del SAS.

Spoofing. L'atacant genera senyals que imiten els autèntics per falsejar la posició o el temps sense que l'usuari ho percebi [Hum08]. Es pot considerar una forma intel·ligent d'interferència i és, comparat amb el jamming, molt més perillós, perquè en lloc de deixar el receptor sense servei li fa creure una solució falsa [TG24a]. Es classifica en tres nivells de sofisticació [Gün14, Psi16]: simplista (no sincronitzat, detectable per salts de posició), intermedi (sincronitzat, arrossega (*drag-off*) els llaços augmentant la potència; durant l'arrossegament coexisteixen els dos senyals, originant un pic vestigial) i sofisticat (multi-antena coordinada). Un cas especial és el Security Code Estimation and Replay (SCER), en què l'atacant estima i reemet els chips en temps real; el SAS hi resisteix perquè el codi E6-C roman xifrat fins després de la captura [FH23].

Tampering. A diferència dels anteriors, suposa l'accés físic de l'atacant al receptor; és especialment crític quan aquest emmagatzema claus criptogràfiques [TG24a]. És un dels motius pels quals el SAS s'ha dissenyat per no requerir claus secretes locals (reaprofita les claus TESLA de l'OSNMA), cosa que evita la necessitat de receptors resistents a la manipulació.

2.3.3 Contramesures a nivell de receptor

Les tècniques no criptogràfiques no modifiquen l'estructura del senyal GNSS: exploten manifestacions físiques ja presents (potència rebuda, temps d'arribada, angle d'arribada, polarització) per decidir si el senyal és autèntic o contrafet [TG24a]. El cost de la contramesura ha de ser proporcional a l'amenaça: algunes s'implementen amb algorismes senzills en programari, mentre que d'altres exigeixen maquinari addicional, reservat a receptors de gamma alta. Per això es classifiquen segons que requereixin o no maquinari extra [Psi16, Gün14].

Basades en programari (sense maquinari adicional).

- **Potència rebuda / amplitud:** la monitorització del nivell rebut o de l'acció de l'AGC detecta canvis anòmals. Un spoofing sol augmentar la potència, cosa que fa baixar el guany de l'AGC per evitar la saturació de l'ADC; aquesta variació delata l'atac [Wes18].
- **Temps d'arribada / pseudodistància:** si es disposa de més satèl·lits que les quatre incògnites de la PVT, la redundància permet comprovar la coherència de les mesures. És la base del Receiver Autonomous Integrity Monitoring (RAIM): el receptor resol la posició sobredeterminada per mínims quadrats i n'examina els residus; si el residu (o l'estadístic de test associat) supera un llindar, conclou que alguna pseudodistància és inconsistent i avisa d'una possible fallada d'integritat. La Fault Detection and Exclusion (FDE) va un pas més enllà i, a més de detectar la fallada, n'identifica i n'exclou la mesura culpable per continuar navegant amb les restants [Gün14]. Com que un *spoofers* difícilment sincronitza totes les pseudodistàncies a la perfecció, aquestes incoherències el poden delatar; ara bé, un atac prou coordinat que les falsegi de manera consistent pot generar una solució amb residus petits i evadir el RAIM/FDE.
- **Signal Quality Monitoring (SQM):** opera en el domini del senyal, a la sortida dels correladors. En absència d'atac el pic de correlació és net; en presència d'un spoofer (o de multicamí) apareix una distorsió o un pic secundari. Se'n distingeixen dos vessants: la Multi-Peak Detection (MPD), que cerca més d'un pic a l'espai de cerca, i el monitoratge de la forma del pic (simetria, amplada, entre d'altres) quan els retards són massa propers per resoldre dos pics [Wes18]. La Vestigial Signal Search (VSS) (cerca del senyal autèntic vestigial que coexisteix amb el contrafet durant l'arrossegament) és la instanciació de MPD desenvolupada al grup [PG24, Win24].

Basades en maquinari (processament espacial i sensors).

- **Angle d'arribada (Angle of Arrival (AOA)):** amb múltiples antenes i mesures diferencials de fase de portadora, els senyals autèntics arriben de direccions diferents, mentre que els d'un spoofer comparteixen un únic origen [Bro16].
- **Polarització:** amb antenes de doble polarització; els senyals autèntics arriben amb polarització circular dretana (RHCP) molt pura, mentre que els contrafets, en seguir un camí comú des de l'spoofers, tendeixen a compartir polarització. Requereix maquinari, però no antenes grans [TG24a].
- **Mesures inercials (Inertial Navigation System (INS)/IMU) i moviment d'antena:** la comparació de la solució GNSS amb dades inercials independents, o la síntesi d'una obertura movent l'antena, revela incoherències pròpies d'un atac [TG24a].

Aquestes tècniques són complementàries a l'autenticació criptogràfica: no requereixen infraestructura del sistema, però tampoc no ofereixen una garantia criptogràfica, i el seu estudi evoluciona constantment [TG24a]. Un principi transversal és la diversitat: com més comprovacions independents afegeix el receptor, més difícil resulta l'atac.

2.3.4 Contramesures a nivell de sistema: autenticació criptogràfica

La protecció més robusta l'aporta el propi sistema, ocultant criptogràficament part de la informació en la generació del senyal de manera que un atacant no la pugui predir ni falsificar [TG24a]. Això es pot fer a dos nivells complementaris [TG24a]:

- **Nivell de dades:** xifrant bits del missatge de navegació. L'atacant pot seguir el senyal, però no demodular el missatge ni, doncs, calcular un PVT autèntic. Aquí s'inscriu la Navigation Message Authentication (NMA), de la qual l'OSNMA n'és la realització de Galileo.
- **Nivell de rang** (o de senyal): xifrant els chips del codi d'eixamplament. Ofereix més protecció, perquè l'atacant no pot ni tan sols seguir el senyal. És el domini de la Spreading Code Authentication (SCA), basada en la Spreading Code Encryption (SCE); els senyals militars (com el codi P(Y) del GPS) ja en fan servir, i el SAS de Galileo n'és la realització civil.

La distinció és essencial per a aquest treball: l'OSNMA garanteix què es transmet, però no quan arriba (per això el *meaconing* el supera); el SAS hi afegeix l'autenticació del temps d'arribada.

Autenticació de dades: OSNMA

L'Open Service Navigation Message Authentication (OSNMA) autentica el missatge de navegació del Servei Obert, declarat operatiu el juliol de 2025 [Eur25]. Aprofita 40 bits reservats del missatge I/NAV a la banda E1-B, mantenint la compatibilitat enrere [Eur23c]. El seu fonament és el protocol Timed Efficient Stream Loss-tolerant Authentication (TESLA), que proporciona autenticació diferida amb una cadena de claus generada recursivament amb una funció *hash* unidireccional F (Figura 2.12):

$$K_i = F(K_{i+1}). \quad (2.14)$$

Les claus es revelen amb retard respecte als codis d'autenticació (Message Authentication Code (MAC)) que protegeixen, de manera que el receptor pot verificar-les a posteriori; això exigeix sincronització amb el GST entre 30 i 300 s [Eur24b]. La cadena s'ancora amb un missatge de signatura digital (Digital Signature Message (DSM)) signat amb Elliptic Curve Digital Signature Algorithm (ECDSA) i validat per un arbre de Merkle. La biblioteca de referència del grup per

a aquest processament és OSNMAlib [GF22, GF25]. Esquemes NMA semblants s'han proposat per a altres GNSS (GPS, BeiDou) i per a SBAS [TG24a]. En aquest treball, la cadena TESLA és precisament la clau a partir de la qual es deriva la clau AES que desxifra les RECS del SAS.

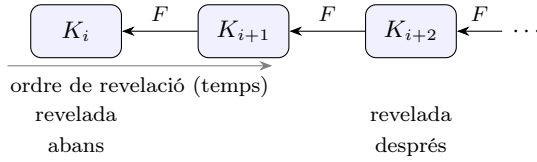


Figura 2.12: Cadena de claus TESLA, generades amb una funció *hash* unidireccional F en sentit invers al de revelació. Adaptat de [TG24a].

Autenticació de rang: SAS / ACAS

El Signal Authentication Service (SAS), originàriament Assisted Commercial Authentication Service (ACAS), afegeix l'autenticació de rang absent en l'OSNMA [FH23, FH24, TG24a]. La component E6-C es transmet amb un codi xifrat; l'atacant no el pot generar, però el receptor tampoc no el pot correlacionar directament. El SAS ho resol amb un esquema semiassistit, el segment de terra rexifra fragments del codi E6-C amb una clau lligada a la TESLA, produint les Re-Encrypted Code Sequences (RECS), que es publiquen al Galileo Service Centre (GSC) abans de la transmissió, per a instants predefinitos i períodes curts (~ 16 ms) [Eur23a]. Quan l'OSNMA revela la clau, el receptor desxifra les RECS, obté les seqüències en clar (Encrypted Code Sequences (ECS)) i les correlaciona amb la instantània E6-C; un pic clar en la posició esperada autentica el rang. Aquest disseny evita que el receptor hagi d'emmagatzemar claus secretes (en reaprofitja les de l'OSNMA), cosa que en redueix el cost i n'elimina la necessitat de resistència a la manipulació [TG24a].

A la metodologia (Secció 3.2.2) es detalla més en profunditat aquest procés, que constitueix el nucli de la contribució d'aquest treball.

Homòlegs en altres GNSS: CHIMERA

L'autenticació criptogràfica no és exclusiva de Galileo. El GPS desenvolupa Chips-Message Robust Authentication (CHIMERA) per al senyal obert L1C, que combina tots dos nivells en un sol servei: la NMA, mitjançant la signatura digital del missatge, i la SCA, inserint marques (*watermarks*) al codi d'exemplament civil substituint-ne petits segments per una seqüència secreta que el receptor podrà reproduir un cop obtingui la clau [TG24a]. CHIMERA opera amb dos canals: un lent (la clau s'obté del missatge de navegació, cadència de minuts) i un ràpid (la clau arriba per un enllaç fora de banda, cadència de segons), i prova alhora modes autònom i assistit [TG24a].

La diferència d'enfocament és clara (Taula 2.3): Galileo ofereix dos serveis diferenciats (OSNMA per a les dades i SAS per al rang), mentre que el GPS busca oferir ambdues autenticacions en un sol servei. Una conseqüència pràctica és que el SAS xifra tota la component pilot E6-C, mentre que CHIMERA només n'altera fragments del L1C, amb una pèrdua de correlació molt menor [TG24a].

Taula 2.3: Comparació dels nous serveis d'autenticació criptogràfica en GNSS. Adaptat de [TG24a].

Servei	Nivell d'autenticació	Banda GNSS	Estat	Mode SCA
OSNMA	Dades	Galileo E1-B	Operatiu	—
SAS	Rang	Galileo E1-B + E6-C	En desenvolupament	Assistit
CHIMERA	Dades i rang	GPS L1C (C+D)	En proves	Assistit + Autònom

2.3.5 Cap a la segona generació

Les solucions actuals (OSNMA i SAS/ACAS) constitueixen una primera generació d'autenticació afegida sobre senyals i serveis ja desplegats. El principi comú a totes elles és dividir el senyal en una component en temps real i una de diferida, i assumir que, en cas d'atac, el senyal autèntic (xifrat) arribarà abans que el contrafet [TG24a].

La Galileo Second Generation (G2G) canviarà aquest plantejament. Es tracta d'una nova generació de satèl·lits (pensada per renovar i ampliar la constel·lació) amb diverses novetats rellevants per a l'autenticació [TG24a]:

- **Càrregues útils digitals i reconfigurables:** els senyals i els serveis es podran reprogramar en òrbita, de manera que les capacitats d'autenticació podran evolucionar sense canviar el maquinari.
- **Enllaços intersatèl·lit,** que reforcen la sincronització i la integritat de la constel·lació.
- **Relotges atòmics millorats,** que n'augmenten l'exactitud temporal i, per tant, la precisió de rang.
- **Seguretat i autenticació natives:** a diferència de l'OSNMA i el SAS (afegits sobre senyals ja existents), la G2G integra la seguretat i l'autenticació des del disseny, amb senyals dedicats.

Aquest pas de l'autenticació afegida a la nativa obre la porta a esquemes més ambiciosos, com l'autenticació de rang en mode autònom (sense assistència contínua d'un servidor), tal com ja exploren CHIMERA i algunes propostes per a Galileo, encara en fase d'anàlisi [TG24a].

Capítol 3

Metodologia

Aquest capítol descriu el disseny de la solució i la justificació de les decisions preses: els materials i les eines emprats (Secció 3.1) i el disseny i el procediment de treball (Secció 3.2).

3.1 Materials i eines

3.1.1 Recursos i feina prèvia del departament

Aquest TFG no parteix de zero: s'inscriu en una línia de recerca consolidada del grup SPCOMNAV de la UAB, que durant els darrers anys ha contribuït de manera sostinguda a la definició, l'anàlisi i la validació experimental del SAS de Galileo (originàriament conegut com a Assisted Commercial Authentication Service (ACAS)) i que n'ha anat acumulant els recursos teòrics, programari i de maquinari sobre els quals es construeix aquest treball. Convé situar amb precisió aquests antecedents, perquè delimiten què és aportació pròpia d'aquest TFG i què es reutilitza.

El model d'autenticació a nivell de senyal. El fonament conceptual del SAS és el semi-assisted signal authentication, una prova de concepte que va demostrar la viabilitat d'autenticar el rang d'un satèl·lit a nivell de senyal [FH23]. Aquesta idea es va formalitzar després com un servei diferenciat de Galileo, amb la seva arquitectura de segment de terra i el seu ICD [FH24]. La tesi doctoral de Terris-Gallego en sistematitza el disseny, l'anàlisi de prestacions i la validació experimental, i n'estableix el model de mesura que relaciona les bandes E1 i E6 i el criteri de decisió d'autenticació [TG24a].

La validació incremental de l'ACAS/SAS a SPCOMNAV. El grup ha validat el servei de manera incremental, refinant a cada pas els paràmetres i les eines. La línia arrenca amb

estudis teòrics i de simulació que en van definir els modes d'operació i en van dimensionar els paràmetres (longitud de la seqüència, latència de revelació de claus, sensibilitat) [TG22b], acompanyats d'unes guies d'implementació per a receptors [TG22a]. A continuació, una avaluació preliminar va demostrar la viabilitat de la tècnica sobre els senyals oberts E1-E6 encara no xifrats, fent servir l'E6 obert com a banda de prova [TG23b]. El pas següent va ser de maquinari: el desenvolupament de la plataforma SDR basada en bladeRF capaç d'enregistrar de manera sincronitzada les bandes E1 i E6, imprescindible per capturar les instantànies que el SAS necessita [TG23a] (Secció 3.1.3). Sobre aquesta base es van proposar tècniques eficients d'assistència E6-B per accelerar la cerca de les seqüències [TG24b]. Tota la línia culmina amb la primera campanya amb senyal E6-C xifrat real (juny de 2025), en què per primera vegada s'autentica rang amb el senyal del SAS realment xifrat a l'espai [TG25]; aquesta campanya constitueix un dels conjunts de validació d'aquest treball (Secció 3.2.3).

Eines de programari heretades. A nivell de dades, l'autenticació del missatge de navegació (OSNMA) es resol amb OSNMAlib, biblioteca oberta de referència del grup [GF22, GF25], de la qual SASlib reaprofitja la sortida (Secció 3.1.4). Pel que fa a la detecció no criptogràfica d'spoofing, el grup disposa d'un TFG previ que va implementar i caracteritzar tècniques de receptor snapshot (Vestigial Signal Search (VSS) i Signal Quality Monitoring (SQM)) [PG24], i la literatura recent proposa la combinació de la VSS amb l'ACAS com a especialment robusta enfront del spoofing [Win24] tot i que no estan implementades, ho seran pròximament en la llibreria; aquestes tècniques són el punt de partida de l'estudi de detecció complementari d'aquest TFG.

Síntesi. Tots aquests recursos —el model de mesura, els paràmetres operatius, la plataforma de captura, les biblioteques d'autenticació de dades i les tècniques de detecció— conflueixen en la biblioteca oberta SASlib [TG26a], de la qual l'estudiant és coautor, i que materialitza en programari de codi obert la cadena completa del receptor SAS. Les seccions següents en descriuen la biblioteca (Secció 3.1.2), la plataforma de captura (Secció 3.1.3), les dades auxiliars (Secció 3.1.4) i els documents normatius de referència (Secció 3.1.5); la metodologia de validació i els conjunts de dades emprats es detallen a la Secció 3.2.3.

3.1.2 La biblioteca SASlib

El desenvolupament d'aquest TFG es realitza dins de SASlib [TG26a], una biblioteca de codi obert en Python (licència EUPL-1.2) que implementa la cadena completa de processament d'un receptor SAS, des de la captura del senyal fins a la solució PVT autenticada. La biblioteca s'organitza en una arquitectura de tres capes [TG26a]: una capa de presentació (interfície web, Figura 3.1), una capa de lògica (orquestració del pipeline, amb un motor d'execució i la gestió

d'estat) i una capa de processament formada pels blocs funcionals. Aquesta separació permet desenvolupar, provar i validar cada bloc de manera independent, i és el que ha fet possible repartir-ne el desenvolupament entre dos TFG (Secció 3.2.1).

El nucli de la biblioteca és un pipeline de 13 blocs encadenats amb una interfície comuna (Figura 3.5). Cada bloc s'acompanya d'un esquema de configuració en JSON que declara de manera explícita quines dades consumeix i produeix, els paràmetres configurables i les condicions d'execució; el motor és, doncs, dirigit pels esquemes: construeix les entrades de cada bloc a partir d'un context d'execució compartit i n'encadena les sortides, sense que els blocs es coneguin entre si. Aquest disseny desacobla els blocs i en facilita tant la substitució com la prova unitària. Els blocs poden declarar-se per executar-se en paral·lel (per exemple, la descàrrega i el desxifrat de les dades auxiliars mentre s'enregistra la instantània) o de manera condicional (la cadena criptogràfica només s'activa quan el satèl·lit objectiu emet senyal xifrat). Per veure més detall del pipeline es pot consultar la Secció 3.2 o el mateix paper associat [TG26a].

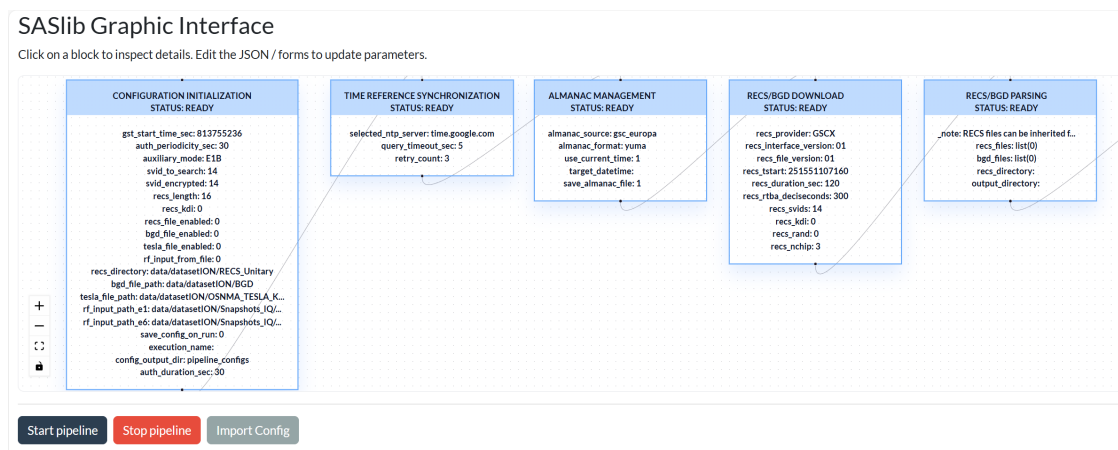


Figura 3.1: Front-end web de SASlib: la cadena de processament es representa com un graf de blocs, cadascun amb el seu estat i els seus paràmetres configurables, des del qual es configura i es llança l'execució del pipeline. Captura de [TG26a].

3.1.3 Plataforma de captura SDR

Les dades de senyal s'obtenen amb una plataforma Software-Defined Radio (SDR) multiban- da basada en dues plaques bladeRF, ubicada físicament a la UAB i integrada en un maletí portàtil (Figura 3.3) [TG23a]. De moment, dues plaques enregistren de manera sincronitzada les dues bandes que el SAS necessita —E1 (1575,42 MHz, o la banda auxiliar escollida) i E6 (1278,75 MHz)—, alimentades des d'una mateixa antena a través d'un divisor i disciplinades per un rellotge de referència comú, de manera que les dues captures comparteixen base de temps. La sincronització E1/E6 amb precisió de sub-mil·lisegon és un requisit essencial del SAS, ja que el rang autènticat es mesura comparant el retard de codi de les dues bandes.

Cada instantània s'etiqueta temporalment amb l'hora obtinguda en disciplinar el maletí contra un servidor ntp de la pròpia UAB, fet que proporciona una referència de temps coherent i traçable per a totes les captures i que el receptor empra com a punt de partida per a la finestra de cerca. Les mostres s'emmagatzemen en format sc16 (enters de 12 bits, components IQ) amb una freqüència de mostreig de 20 Msps tot i que és personalitzable com es pot veure a la figura 3.2.

L'enregistrament es controla des del front-end propi de la plataforma, el Signal Capture Control Center (Figura 3.2), des del qual es configuren els paràmetres de cada placa bladeRF (freqüència, freqüència de mostreig, ample de banda i guany) i la durada de la captura, i es llança l'enregistrament sincronitzat de totes dues bandes; opcionalment, hi des a també les claus TESLA d'OSNMA associades a la instantània. A més, la plataforma s'integra amb SASlib: el bloc *SnapshotRecording* en pot comandar la captura a través d'una API dedicada, de manera que les instantànies E1/E6 s'obtenen sota demanda i s'alimenten directament a la cadena de processament.

The screenshot displays the SnapSyncGNSS Signal Capture Control Center interface. At the top, there's a navigation bar with tabs for Light, GNSS, Setup, Admin, and Logout. Below this is the 'Recording Workspace' section, which includes a sub-header 'Record' and a description: 'Configure capture jobs, monitor pending operations, and inspect completed records.' The main area shows 'Devices found: 2' and lists two devices: BLADE_1 and BLADE_3. Each device has a set of configuration parameters: frequency (Hz), sample_rate (sps), bandwidth (Hz), gain (dB), gain_mode (Default), bias_tee (checked), and agc_enabled (unchecked). To the right of the device configurations is a 'Record Details' panel with a 'Record time length (seconds)' dropdown set to 1, checkboxes for 'Record now' and 'Save OSNMA TESLA Keys' (both checked), a 'Selected Devices' list showing BLADE_1 and BLADE_3, a checkbox for 'VSS' (unchecked), and a note about the approximate size: 'Aprox size: 76.29 MB (1 device/s)'. A large red 'Start' button is positioned to the right of the Record Details panel.

Figura 3.2: Front-end propi de la plataforma de captura SDR (Signal Capture Control Center), des d'on es configura i es llança l'enregistrament sincronitzat de les dues bandes.

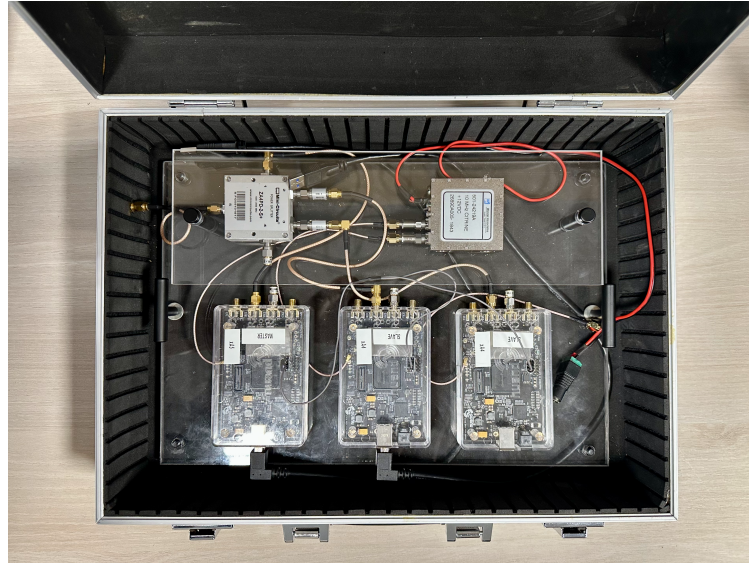


Figura 3.3: Plataforma de captura SDR ubicada a la UAB: el maletí integra les dues plaques bladeRF de captura sincronitzada E1/E6. Imatge de [TG26a].

3.1.4 Dades auxiliars

A més del senyal capturat, el receptor SAS necessita un conjunt de dades auxiliars descarregades de fonts oficials i d'una clau que prové de l'OSNMA:

- Les claus TESLA revelades a l'E1-B, que el receptor obté a través d'OSNMAlib [GF25]. OSNMAlib és la biblioteca oberta de referència per a l'OSNMA: implementa tota la cadena del protocol —cadena de claus TESLA, els codis d'autenticació MAC, el missatge de signatura digital amb ECDSA i l'arbre de Merkle que valida la clau pública— i en publica, un cop verificades, les claus revelades. Aquesta clau és precisament la que permet desxifrar les seqüències del SAS; SASlib n'aprofita la sortida sense haver de reimplementar l'OSNMA.
- Les seqüències rexifrades (RECS) i el retard de grup (BGD) del Galileo Service Centre (GSC), necessàries per reconstruir la rèplica desxifrada (ECS) i per corregir el biaix entre bandes.
- Les efemèrides de difusió en format RINEX (de l'ESA GSSC) i l'almanac de Galileo, per calcular la posició dels satèl·lits, la seva visibilitat i les elevacions.

Cal remarcar una limitació operativa important: les RECS encara no estan disponibles públicament. Per això aquest treball les obté d'un servidor privat que les serveix en temps real, i actualment només estan xifrats (i, per tant, autenticables a nivell de senyal) els satèl·lits PRN 14 i PRN 18 de Galileo. Aquesta restricció condiciona l'abast de la validació: és possible autenticar

el rang d'aquests satèl·lits, però l'autenticació a nivell de posició (que requeriria prou satèl·lits xifrats simultàniament) queda pendent de la disponibilitat de més senyal xifrat a l'espai.

3.1.5 Documents normatius

El disseny dels blocs s'ajusta als documents oficials que en defineixen les interfícies i els criteris, de manera que el receptor sigui interoperable amb el sistema real. Per a la part d'autenticació de dades (OSNMA), són de referència l'OSNMA SIS ICD [Eur23c], que en fixa el format del senyal a l'espai, i les OSNMA Receiver Guidelines [Eur24b], que en recomanen la implementació al receptor. Per a la part d'autenticació de senyal (SAS), el document de referència és l'ACAS Specification Proposal [Eur23a], complementat amb els articles del grup que en formalitzen el servei i el model de mesura [FH23, FH24, TG24a], tot i que s'està treballant en nous ICDs oficials. Finalment, l'estructura del senyal de les bandes E1 i E6 segueix l'OS SIS ICD de Galileo [Eur23b]. Aquests documents es fan servir com a especificació; el detall criptogràfic i de formats queda fora de l'abast d'aquest TFG i correspon al treball complementari d'Enginyeria Informàtica.

3.1.6 Eines d'intel·ligència artificial generativa

En el desenvolupament d'aquest TFG s'han emprat eines d'intel·ligència artificial generativa com a suport, i és just reflexionar sobre quin paper hi han tingut i quins en són els límits. GitHub Copilot s'ha utilitzat per a l'autocompletat de codi en tasques repetitives (estructures de configuració, generació de gràfiques i codi auxiliar de proves), i models conversacionals com Claude (Anthropic) i ChatGPT (OpenAI) s'han fet servir per a consultes tècniques puntuals, per a la depuració d'errors concrets i per a l'estructuració, la redacció i la correcció lingüística d'aquesta memòria.

Ara bé, el nucli del treball —el disseny de la cadena de processament de senyal, l'elecció dels algorismes de correlació i d'autenticació, la interpretació física dels resultats i la validació amb dades reals— és obra de l'estudiant. L'aportació de la IA ha estat la d'accelerar tasques rutinàries i oferir un primer esborrany sobre el qual treballar, mai la de prendre les decisions d'enginyeria ni de substituir la comprensió del problema. De fet, bona part de la dificultat d'aquest treball —la depuració d'una cadena llarga i fortament acoblada, on un error en qualsevol baula impedeix que el pic es formi— ha exigít un raonament i un coneixement del domini que aquestes eines no proporcionen.

La lliçó més rellevant d'aquest ús ha estat la necessitat de verificació crítica. Els models generatius produeixen amb facilitat respostes plausibles però incorrectes (referències inexistents, fórmules mal aplicades o explicacions versemblants però errònies), de manera que tot el que han suggerit s'ha contrastat sistemàticament amb les fonts primàries —la tesi doctoral de referència

[TG24a], els documents ICD oficials i el codi de SASlib— i, sobretot, amb el comportament real del sistema sobre les dades capturades. En un context com aquest, on la correcció depèn de la física del senyal i de la coherència amb la mesura, la IA és una eina útil però subordinada: el criteri, la responsabilitat i la verificació del resultat final són, necessàriament, de l'estudiant.

3.2 Disseny i procediment

3.2.1 Repartiment amb el TFG d'Enginyeria Informàtica

La realització d'un receptor SAS funcional és multidisciplinària i abasta des del processament de senyal de RF fins a la gestió de dades, la criptografia i la interfície. Per això el desenvolupament de SASlib s'ha estructurat en dos TFG complementaris:

- Un TFG d'Enginyeria Informàtica, centrat en l'arquitectura de programari (motor d'execució del pipeline, context d'execució, gestió d'estats), la gestió de dades auxiliars (descàrrega i parsing de RECS/BGD/claus), el processament criptogràfic (cadena TESLA i desxifratge AES de les RECS) i la interfície gràfica a més d'una altra interfície gràfica de monitoratge 24 hores per saber quins satèl·lits estan actius i l'estat actual d'encriptatge dels mateixos satèl·lits a temps real.
- Aquest TFG, de l'àmbit de les Telecomunicacions, centrat en el processament de senyal: adquisició i correlació, autenticació de rang i càlcul de PVT, i estudi de tècniques de detecció d'spoofing.

La frontera és neta i es materialitza en l'intercanvi de dades a través del context d'execució: el bloc de desxifratge (Informàtica) lliura la seqüència desxifrada ECS i el pressupost d'incertesa, que el bloc de correlació (Telecomunicacions) consumeix; recíprocament, la correlació publica les mesures de rang i les mètriques que consumeixen l'autenticador i el càlcul de PVT.

3.2.2 El pipeline de SASlib i el flux de processament SAS

Descrita ja l'arquitectura de la biblioteca (Secció 3.1.2), aquesta secció en recorre el flux de processament bloc a bloc. Abans, però, convé entendre el principi d'operació del SAS que el pipeline materialitza, perquè és el que dona sentit a tota la cadena.

Principi d'operació del SAS al receptor. El SAS es basa en el xifratge del senyal pilot E6-C i en les claus TESLA que l'OSNMA revela a la banda E1-B [FH24]. Al segment de terra, fragments del codi d'eixamplament del senyal E6-C xifrat (les seqüències xifrades, o ECS) es

tornen a xifrar amb una clau encara no revelada i donen lloc a les seqüències rexifrades (RECS), que es publiquen abans de l'emissió del senyal en un repositori accessible, juntament amb el seu instant d'emissió [TG24b]. La Figura 3.4 il·lustra l'operació resultant al receptor. Aquest descarrega les RECS per avançat, per poder operar de manera autònoma durant un període. Quan el senyal E6-C s'emet, el receptor n'enregistra una instantània (snapshot) al voltant de l'instant en què s'esperen les RECS, determinat a partir de les capçaleres dels fitxers. Les claus TESLA es revelen a l'E1-B a intervals regulars (una subtrama I/NAV, 30 s); a mesura que es revela cada clau K'_j , el receptor desxifra la RECS_j corresponent i n'obté l'ECS_j, que actua de rèplica local. Aquesta rèplica es correlaciona amb la instantània E6-C pregravada del mateix interval; si s'hi detecta el pic de correlació, es mirarà la diferència d'aquest pic amb els pics del senyal auxiliar i, si el rang entre aquests dos pics compleix un barem preestablert, es pot afirmar que el senyal és autèntic, per això es diu autenticació de rang. A més, com que la clau prové de l'OSNMA a posteriori, el receptor no ha d'emmagatzemar cap clau secreta, fet que evita el maquinari resistent a manipulacions i en redueix el cost [TG24a].

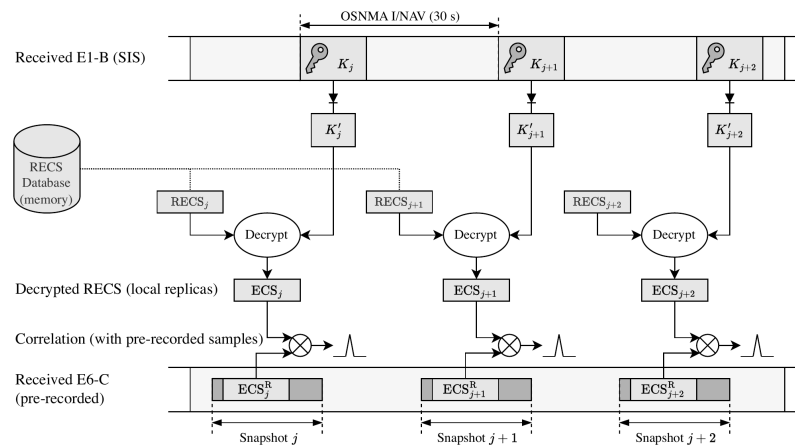


Figura 3.4: Operació del SAS al receptor: les claus TESLA revelades a l'E1-B (a intervals d'una subtrama I/NAV, 30 s) desxifren les RECS descarregades per avançat i en produeixen les ECS (rèpliques locals), que es correlacionen amb la instantània E6-C pregravada de cada interval. El superíndex 'R' indica l'ECS rebuda, afectada per soroll. Adaptat de [TG24b].

Els 13 blocs en quatre etapes. La cadena s'organitza en quatre etapes funcionals (Figura 3.5): arrencada, captura, generació de l'ECS i processament de senyal i autenticació. El diagrama mostra, per a cada bloc, les seves entrades (les fonts de dades) i les seves sortides (els artefactes que produeix) [TG26a].

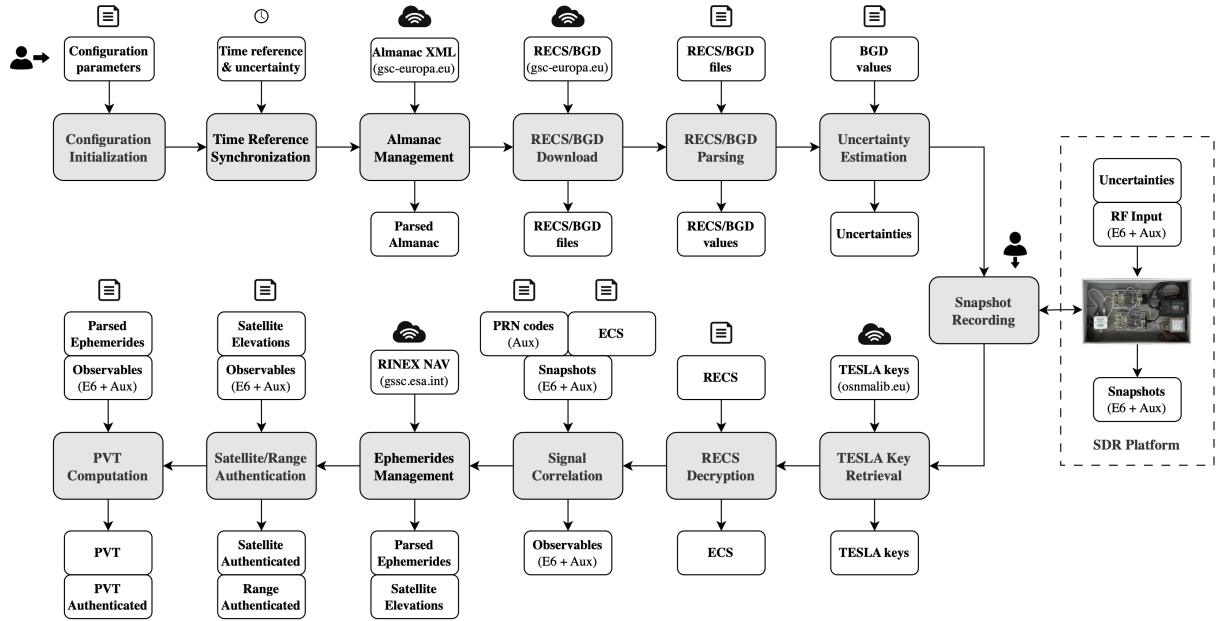


Figura 3.5: Arquitectura de SASlib: els 13 blocs del pipeline amb les seves entrades (fonts de dades) i sortides (artefactes), organitzats segons les quatre etapes del flux de processament. Els blocs de processament de senyal desenvolupats en aquest TFG són *SignalCorrelation*, *SatelliteAuthenticator* i *PVTComputation*. De [TG26a].

(1) Mòduls d'arrencada. Preparen el receptor abans de l'emissió del senyal, amb connexió a Internet:

- *ConfigInit* — inicialitza la configuració i els ajustos d'usuari (instant i durada de l'autenticació, periodicitat de les RECS, banda auxiliar...).
- *TimeReferenceSynchronizer* — obté la referència temporal inicial i la seva incertesa via NTP.
- *AlmanacManagement* — descarrega l'almanac de Galileo (XML del GSC); és una dada d'assistència opcional que estima la visibilitat i el Doppler/retard esperats per reduir l'espai de cerca.
- *BGDandRECSdownloader* i *BGDandRECSparser* — descarreguen (d'un servidor configurable, en un TAR) i parsegen els fitxers RECS, BGD i SLOG, d'on recuperen els bits de les RECS, els valors de BGD i l'estat del servei.

(2) Mòduls de captura. Enregistren la instantània E6-C a prop de l'instant d'autenticació:

- *UncertaintyModule* — suma les contribucions d'incertesa (deriva del rellotge, retard de propagació de fins a 20 ms, paràmetres del SAS) que fixen la longitud de la instantània.

- *SnapshotRecording* — comanda la captura E6-C (i, opcionalment, de la banda auxiliar) a la plataforma SDR via l'API dedicada (Secció 3.1.3), o carrega instantànies pregravades.

(3) Mòduls de generació de l'ECS. Produeixen les rèpliques locals un cop revelades les claus:

- *TESLAkeyManagement* — recupera de l'OSNMA les claus TESLA quan es revelen a l'E1-B.
- *RECSDecryption* — desxifra les RECS amb aquelles claus (AES en mode CBC, segons l'ICD del SAS) i n'obté les ECS [FH24].

(4) Mòduls de processament de senyal i autenticació. Etapa on conflueixen els dos TFG; els tres blocs ressaltats són els d'aquest TFG i es detallen al Capítol 4:

- *SignalCorrelation* — correlaciona les mostres E6-C amb les ECS i n'extreu les observables (retard de codi, Doppler, C/N_0); la banda auxiliar permet estrènyer la finestra de cerca [TG24b].
- *EphemeridesManagement* — descarrega les efemèrides (RINEX NAV, ESA GSSC) i en calcula les elevacions dels satèl·lits.
- *SatelliteAuthenticator* — decideix si el rang és autèntic comparant el pic de correlació amb el soroll o amb el pic secundari (PPSP), i contrasta el retard de codi de l'E6-C amb el de la banda auxiliar.
- *PVTComputation* — calcula la solució PVT; amb quatre o més rangs autenticats de satèl·lits diferents la solució s'autenticaria a nivell de posició (encara no possible, Secció 3.1.4).

3.2.3 Metodologia de validació

La validació es recolza en dos conjunts de dades complementaris. D'una banda, el conjunt de dades de la campanya ION GNSS+ 2025 (la primera amb senyal E6-C xifrat real, amb el satèl·lit PRN 14 xifrat) [TG25], emprat en els primers passos del desenvolupament i com a referència per verificar el funcionament correcte de la cadena de processament. De l'altra, les captures pròpies E1/E6 obtingudes amb la plataforma bladeRF (Secció 3.1.3) durant la campanya actual, que permeten validar el receptor end-to-end amb senyal en viu dels satèl·lits xifrats.

Sobre aquests conjunts, cada bloc es valida de manera incremental: primer, amb proves unitàries que en verifiquen el funcionament aïllat; després, amb proves d'integració end-to-end de tot el pipeline. Les mètriques de qualitat de la correlació (PPSP, C/N_0) actuen com a portes de qualitat que filtren les mesures abans de l'autenticació i del càlcul de PVT, i el veredict de l'autenticació es contrasta amb el resultat esperat (senyal autèntic enfront de senyal manipulat).

Capítol 4

Desenvolupament i implementació

Aquest capítol constitueix el nucli del treball i en concentra la càrrega tècnica. Descriu en detall la implementació dels tres blocs de processament de senyal desenvolupats: el bloc de processament de correlació (Secció 4.2), el bloc de processament de rang per satèl·lit (Secció 4.3) i el computador de PVT (Secció 4.4). Per a cada bloc es presenta el model matemàtic, l'algorisme implementat, les decisions de disseny i la seva justificació, ancorades en el codi real de SASlib [TG26a].

4.1 Arquitectura dels blocs de processament de senyal

Els tres blocs reproduïxen, en mode snapshot, la cadena de processament d'un receptor GNSS (Secció 2.2): el bloc de processament de correlació fa l'adquisició sobre la instantània capturada —sense etapa de seguiment, com correspon a un receptor snapshot, que opera en bucle obert i processa el senyal per blocs amb la FFT [Bor23]—; el bloc de processament de rang per satèl·lit hi afegeix el test d'autenticació de rang propi del SAS, que contrasta el retard de codi de l'E6-C amb el de la banda auxiliar; i el computador de PVT resol la navegació. L'arquitectura segueix l'esquema de receptor snapshot descrit al capítol 9 de [Bor23] (escrit pels mateixos autors que van definir el SAS), en què el processament es divideix en el bloc de senyal (adquisició) i el de càlcul de posició.

La Secció 3.2.2 ja ha presentat els tretze blocs del pipeline de SASlib i la funció de cadascun; per no repetir-ne el context, aquí només hi situem els tres blocs de processament de senyal. La Figura 4.1 en recorda els contractes de dades i la frontera amb els blocs externs (*RECSDecryption*, *UncertaintyModule* i *EphemeridesManagement*) que en delimiten l'entrada i la sortida.

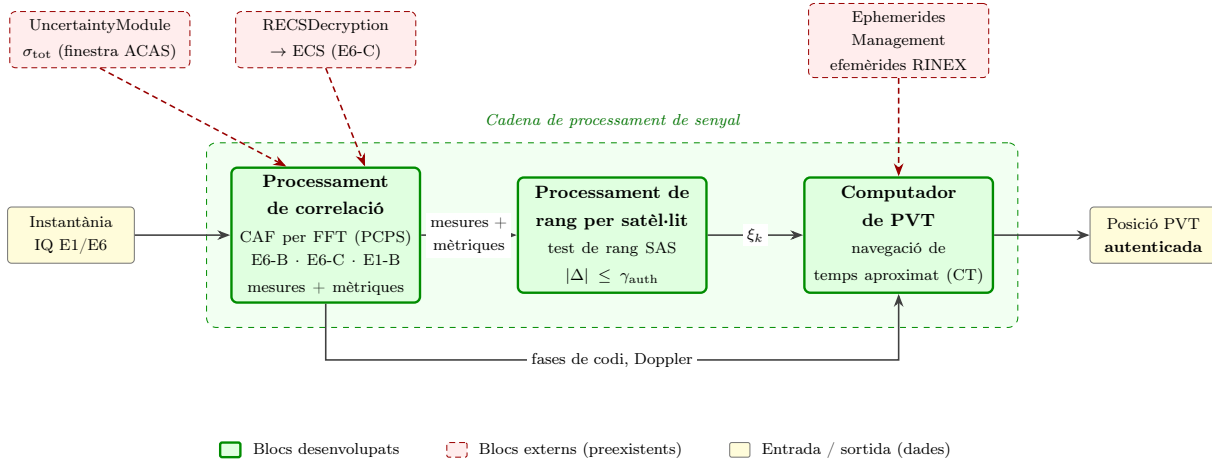


Figura 4.1: Flux de dades dels tres blocs de processament de senyal (verd, dins la zona ombrejada) i la frontera amb els blocs externs (vermell, discontinu).

4.2 Bloc de processament de correlació

És el bloc més complex i el que requereix més processament. La seva funció és correlacionar les seqüències de codi amb la instantània capturada i produir, per a cada satèl·lit, les mesures de fase de codi i Doppler i les mètriques de qualitat que en quantifiquen la fiabilitat.

4.2.1 Model de senyal i objectiu

El senyal en banda base, després del *front-end*, es modela per a un satèl·lit com:

$$r[n] = A d[n] c[n - \tau_0] e^{j(2\pi f_{d,0} n / f_s + \phi_0)} + w[n], \quad (4.1)$$

amb A l'amplitud, $d[n]$ les dades de navegació (absents a la component pilot E6-C, de dades nul·les), $c[n]$ el codi d'eixamplament, τ_0 el desplaçament de codi, $f_{d,0}$ el Doppler, ϕ_0 la fase de portadora i $w[n]$ soroll blanc gaussià complex de variància σ_w^2 . L'objectiu és estimar, per a cada satèl·lit, els dos paràmetres del model de l'Eq. (4.1) que interessen per al rang: el desplaçament de codi τ_0 —l'instant d'arribada del codi, del qual es deriva el rang (la distància) al satèl·lit— i el Doppler $f_{d,0}$ —el desplaçament de freqüència de la portadora causat per la velocitat relativa satèl·lit-receptor. Cap dels dos no es coneix d'entrada, de manera que s'han de cercar.

La idea és intuïtiva: el receptor genera una rèplica local del codi i la prova a alinear amb la instantània rebuda. Per a cada parell de prova (τ, f_d) desfà primer el Doppler f_d del senyal i, tot seguit, correlaciona la rèplica desplaçada τ amb el senyal rebut; la correlació mesura quant s'assemblen tots dos. Quan la rèplica queda ben alineada en temps i en freqüència, l'energia del senyal se suma de manera coherent i la correlació es dispara; si està desalineada, només en queda

soroll. Aquesta correlació coherent, avaluada sobre tota la graella de proves (τ, f_d) , és la Cross-Ambiguity Function (CAF), $\chi(\tau, f_d)$: una superfície que quantifica la qualitat de l'alineament. Estimar $(\tau_0, f_{d,0})$ es redueix, doncs, a trobar-ne el màxim.

Correlacionar el senyal amb la rèplica del codi conegut no és una tria arbitrària: és exactament el filtre adaptat (*matched filter*) al codi, l'operació que maximitza la relació senyal-soroll a la sortida quan es vol detectar una forma d'ona coneguda immersa en soroll [Bor23]. Per això, sota soroll blanc gaussià, maximitzar la CAF no només és raonable sinó òptim: és alhora l'estimador de màxima versemblança de $(\tau_0, f_{d,0})$ (els valors que fan més probable la mostra de senyal observada) i el detector òptim en el sentit de la relació senyal-soroll. Aquest resultat dona fonament teòric a tota la cadena d'adquisició.

Com que es treballa en mode snapshot, tot el procés s'aplica en bucle obert sobre un únic tram de senyal enregistrat: les estimacions s'extreuen directament de la instantània, en un sol processament per blocs, sense l'etapa de seguiment (*tracking*) que en un receptor convencional aniria refinant i seguint el senyal de manera contínua un cop adquirit [Bor23, FH16]. La particularitat del SAS és el codi de l'E6-C: en lloc del codi públic, s'empra la seqüència desxifrada (ECS), de manera que detectar-ne el pic és el que confereix l'autenticació de rang.

Per a cada PRN visible, el bloc executa fins a tres correlacions amb papers diferenciats:

- **E6-B** (codi públic): proporciona una estimació robusta del Doppler de la banda E6, que es reutilitza per a l'E6-C.
- **E6-C** (amb ECS si el PRN és xifrat, o codi públic altrament): és la correlació d'autenticació pròpiament dita.
- **E1-B** (banda auxiliar, en mode multibanda): proporciona la referència temporal per al test d'autenticació i mesures de rang per al PVT.

4.2.2 Càrrega i condicionament de les mostres

Les mostres es llegeixen del fitxer IQ en format **sc16** (enters de 16 bits amb 12 bits útils, components *I* i *Q* entrellaçades) i es converteixen a un vector complex de doble precisió. La lectura admet una finestra de processament definida pels paràmetres *start_sample* i *num_samples*, de manera que es pot processar només el tram de senyal d'interès al voltant de l'instant previst de la RECS, cosa que redueix la memòria i el cost. La freqüència de mostreig per defecte és $f_s = 20$ MHz; quan es processa la banda E1 en mode multibanda, es carrega un segon fitxer amb la mateixa finestra temporal per garantir la correspondència entre bandes.

4.2.3 Generació de les rèpliques de codi

Per a cada banda i component es genera la rèplica local del codi a la freqüència de mostreig:

- **E6-B/E6-C públics:** codis primaris de 5115 chips a 5,115 Mcps, sobremostrejats a f_s per repetició de chip.
- **E6-C xifrat (ECS):** la seqüència desxifrada arriba del bloc *RECSDecryption* com una cadena hexadecimal de chips, que es converteix a una rèplica bipolar (± 1). A diferència del codi públic, l'ECS és aperiòdic (abasta diversos períodes de codi) i només cobreix l'interval de la RECS.
- **E1-B:** codi de 4092 chips a 1,023 Mcps modulats amb la subportadora BOC(1,1).

Formalment, la rèplica es genera a partir de la seqüència de chips del codi, $c_k \in \{+1, -1\}$ amb $k = 0, \dots, L-1$, en dos passos. Primer, el sobremostreig a f_s per manteniment d'ordre zero assigna a cada mostra el chip que li correspon,

$$\tilde{c}[n] = c_{\lfloor n R_c / f_s \rfloor}, \quad n = 0, 1, \dots, N-1, \quad (4.2)$$

on R_c és la taxa de chip i N el nombre de mostres; cada chip es repeteix, doncs, al llarg de f_s/R_c mostres ($\approx 3,9$ a l'E6 i $\approx 19,55$ a l'E1). Segon, només per a l'E1-B, es multiplica per la subportadora BOC(1,1) (b), una ona quadrada que avança al doble de la taxa de chip,

$$s[n] = 2(\lfloor 2 R_c n / f_s \rfloor \bmod 2) - 1 \in \{+1, -1\}, \quad (4.3)$$

que commuta de signe a la meitat de cada chip. La rèplica local $c[n]$ que entra al correlador és, per tant (Figura 4.2),

$$c[n] = \tilde{c}[n] s[n] \quad (\text{E1-B}), \quad c[n] = \tilde{c}[n] \quad (\text{E6, BPSK}). \quad (4.4)$$

Per a l'E6-C xifrat, els chips c_k no són els del codi públic sinó els de la seqüència desxifrada (ECS), aperiòdica. Aquest $c[n]$ és el mateix codi que apareix al model de senyal (Eq. (4.1)) i que el correlador compara amb la instantània $r[n]$ als apartats següents.

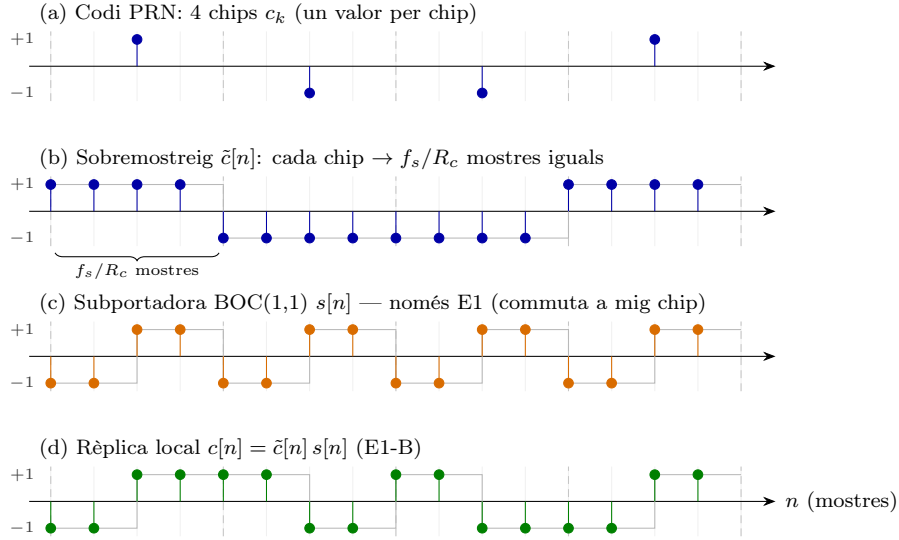


Figura 4.2: Generació de la rèplica local, tot a la mateixa escala (eix de mostres n ; exemple esquemàtic amb $f_s/R_c = 4$ mostres per chip; en realitat $\approx 3,9$ a l'E6 i $\approx 19,55$ a l'E1). (a) El codi PRN és una seqüència de chips, un valor per chip; (b) el sobremostreig $\tilde{c}[n]$ (Eq. (4.2)) repeteix cada chip sobre f_s/R_c mostres consecutives iguals (1 punt per chip a (a) esdevenen f_s/R_c punts a (b)); (c) la subportadora BOC(1,1) $s[n]$ (Eq. (4.3)), només E1, que commuta a la meitat de cada chip; (d) la rèplica $c[n] = \tilde{c}[n] s[n]$ (Eq. (4.4)). Per a l'E6 (BPSK) s'omet (c), i per a l'E6-C xifrat els chips de partida són els de l'ECS.

4.2.4 Càlcul de la CAF mitjançant la FFT

La CAF es calcula en el domini de la freqüència, mètode conegut com a cerca paral·lela en fase de codi (Parallel Code Phase Search, PCPS). En lloc d'avaluar la correlació desplaçament a desplaçament, s'avaluen totes les fases de codi alhora amb una única transformada, seguint la implementació de FFT única descrita al capítol 9 de [Bor23]. Per a cada hipòtesi de Doppler f_d de la graella, primer es desmodula la portadora (*wipe-off*) multiplicant el senyal per la portadora complexa conjugada,

$$r_{f_d}[n] = r[n] e^{-j2\pi f_d n / f_s}, \quad (4.5)$$

i tot seguit es correlaciona amb la rèplica $c[n]$ aprofitant que una correlació en el temps és un producte conjugat en freqüència:

$$\chi(\tau, f_d) = \mathcal{F}^{-1}\{\mathcal{F}\{r_{f_d}[n]\} \cdot \mathcal{F}^*\{c[n]\}\}. \quad (4.6)$$

Així el cost passa de $\mathcal{O}(N^2)$ a $\mathcal{O}(N \log N)$ per bin de Doppler, on N és el nombre de mostres processades. La rèplica es transforma una sola vegada i es reutilitza per a tots els bins de Doppler, cosa que abarateix encara més la cerca.

Cal, però, una precaució important. La correlació via FFT/IFFT implementa una correlació circular, no lineal [Bor23]: el resultat és periòdic amb el període de la FFT, de manera que

rèpliques desplaçades en el temps es poden solapar (*time-aliasing*). Per evitar-ho, s'aplica el mètode *overlap-save*, que exigeix una longitud de transformada d'almenys el doble del període de codi ($T_{\text{FFT}} \geq 2T_{\text{codi}}$) [Bor23]. A la pràctica, totes dues seqüències s'omplen amb zeros (*zero-padding*) fins a la potència de dos immediatament superior a $N_{\text{senyal}} + N_{\text{rèplica}} - 1$, i de la sortida només se'n conserva la regió de correlació lineal vàlida (les primeres $N_{\text{senyal}} - N_{\text{rèplica}}$ mostres). El mateix reblit permet, a més, correlar senyal i rèplica de longituds diferents: és el cas de l'ECS de l'E6-C, una seqüència aperiòdica molt més llarga que un període de codi públic, que s'eixampla amb zeros fins a N_{FFT} igual que la resta. Finalment, convé no confondre els dos eixos de la cerca. Aquesta transformada opera en el temps: la IFFT de l'Eq. (4.6) retorna la correlació al llarg de la fase de codi (el retard τ), amb una resolució d'una mostra per bin ($c/f_s \approx 15$ m a $f_s = 20$ MHz). La resolució en Doppler, en canvi, no la fixa aquesta FFT sinó el temps d'integració coherent, amb $\Delta f_d \approx 1/T_{\text{coh}}$ (Secció 4.2.5) [Bor23].

4.2.5 Integració coherent i post-detecció

Per detectar senyals febles cal acumular energia durant intervals d'observació llargs: és el principi d'alta sensibilitat (HS-GNSS) dels receptors snapshot [Bor23]. L'acumulació es fa en dos nivells encadenats.

Integració coherent. Primer se sumen N_c CAF de períodes de codi consecutius conservant la fase, és a dir, sumant-les com a nombres complexos (Eq. (4.6)):

$$\bar{\chi}_k(\tau, f_d) = \sum_{m=1}^{N_c} \chi_{k,m}(\tau, f_d). \quad (4.7)$$

Com que el senyal s'hi suma en fase i el soroll no, el guany de processament és proporcional a N_c —el màxim possible. Ara bé, mantenir la fase alineada al llarg dels N_c períodes només és viable mentre res no la desalineï: les transicions de bit de les dades de navegació, la deriva de Doppler i la inestabilitat del rellotge limiten fins on es pot allargar la part coherent [Bor23].

Integració post-detecció (PDI). Tot seguit s'acumula el mòdul de N_i blocs coherents successius, cosa que n'elimina la dependència de la fase:

$$P_{\text{PDI}}(\tau) = \sum_{k=1}^{N_i} |\bar{\chi}_k(\tau)|^p, \quad (4.8)$$

on p és l'exponent de la integració (paràmetre `exp_n_coh`, típicament $p = 2$: suma de potències, mètode NPDI). En prescindir de la fase, la PDI és immune a les limitacions anteriors i permet estendre el temps d'integració tant com calgui; el preu és la pèrdua per quadratura: en elevar al quadrat, els termes soroll×soroll s'acumulen i el guany creix més lentament ($\propto \sqrt{N_i}$) que en

el cas coherent ($\propto N_c$). El temps total d'integració és $T_{\text{int}} = N_c N_i T_{\text{codi}}$ [Bor23]; l'estratègia òptima és, doncs, allargar la part coherent (N_c) fins al límit que imposen les transicions i la deriva, i cobrir la resta amb PDI (N_i).

La component pilot E6-C, sense dades de navegació, no pateix transicions de símbol i admet blocs coherents més llargs que un canal de dades —per al qual la pràctica habitual de mitigar les transicions desconegudes és el mètode “half-bit” [Bor23]. Amb els valors per defecte ($N_c = 1$, Taula 4.1) cada bloc és un sol període de codi i el guany prové sobretot de la PDI; l'excepció és l'ECS de l'E6-C, que es tracta com un únic bloc coherent llarg, com es detalla tot seguit.

La correlació d'autenticació explota aquesta propietat al màxim. L'ECS desxifrada (aperiòdica, ~ 16 ms) es correlaciona com un únic bloc totalment coherent —un sol χ_k que abasta tota la seqüència, sense integració post-detecció. La PDI només té sentit per al codi públic periòdic, en què sumar el mòdul de blocs successius captura energia de períodes repetits; aplicar-la a una seqüència aperiòdica sumaria un bloc de senyal i $N_i - 1$ blocs de soroll, i n'esborraria el pic. La integració completament coherent maximitza el guany de processament i la nitidesa del pic d'autenticació, però en fa la detecció molt sensible al Doppler: un bloc de 16 ms té una amplada de bin de només $\Delta f \approx 1/T_{\text{int}} \approx 62$ Hz, cosa que condiciona la cerca de Doppler de l'E6-C (Secció 4.2.7).

La implementació parametriza per separat les dues bandes: per a la banda E6 s'empra per defecte $N_i^{E6} = 20$ ($T_{\text{int}}^{E6} = 20$ ms, ja que $T_{\text{codi}}^{E6} = 1$ ms), i per a la banda auxiliar E1 $N_i^{aux} = N_i^{E6}/4$, de manera que el temps d'integració de totes dues bandes sigui comparable (perquè $T_{\text{codi}}^{E1} = 4 T_{\text{codi}}^{E6}$). La Taula 4.1 resumeix aquests valors.

Taula 4.1: Paràmetres d'integració per a les bandes E6 i E1 (valors per defecte).

Banda	T_{codi}	N_c	N_i
E6 (E6-B / E6-C)	1 ms	1	20
E1 (E1-B aux.)	4 ms	1	5

4.2.6 Cerca de Doppler aproximada i fina

La cerca de Doppler es fa en dues etapes per equilibrar resolució i cost. Una cerca aproximada escombra una graella uniforme (per defecte $[-6500, +6500]$ Hz amb pas de 100 Hz, 131 bins) i el màxim de la CAF integrada en dona una estimació inicial; tot seguit, una cerca fina la refina al voltant d'aquell màxim, sobre ± 100 Hz amb pas de 1 Hz.

Opcionalment s'aplica la correcció de Doppler de codi: el Doppler de la portadora no només desplaça la freqüència, sinó que comprimeix o dilata lleugerament el codi (el període rebut és

$T_{\text{codi}}/(1 + f_d/f_{\text{port}})$). Es compensa de dues maneres: reescalant la freqüència de chip de la rèplica per $(1 + f_d/f_{\text{port}})$, i ajustant l'inici de la finestra de cada bloc de post-detecció amb el període escalat pel Doppler. Sense aquest segon ajust (el condicionament de mostreig per blocs, “block-wise sampling correction”, [Bor23], cap. 9), encadenar els blocs amb el pas nominal els desplaça progressivament de l'època de codi i eixampla el pic; aplicar-lo elimina el residu sistemàtic E6-B↔E6-C que apareixia amb temps d'integració llargs.

4.2.7 Reutilització del Doppler entre components

En teoria, l'E6-B i l'E6-C comparteixen la portadora de la banda E6 i, per tant, tenen el mateix Doppler. Per això el Doppler estimat sobre l'E6-B (el codi públic, fàcil d'adquirir) sembla la cerca de l'E6-C, que només l'ha de refinar en una finestra estreta en lloc d'escombrar tota la graella: és una forma d'adquisició assistida, anàloga a la del senyal GPS L5 ajudat per L1 [Bor23] (cap. 8), que redueix l'espai de cerca i la falsa alarma.

El que és idèntic, però, és el Doppler real, no l'estimació de l'E6-B. Aquesta prové d'una integració no coherent de blocs d'1 ms i oscil·la desenes de hertz, mentre que l'ECS es correlaciona com un únic bloc coherent de ~ 16 ms (Secció 4.2.5), molt més sensible al Doppler (amplada de bin ≈ 62 Hz). Copiar l'estimació directament en faria baixar el pic (la pèrdua creix amb l'error de Doppler i només l'anul·la del tot si s'acosta a l'amplada de bin); per minimitzar-la, l'E6-C fa la seva pròpia cerca fina (pas de pocs hertz) al voltant d'aquella llavor i es queda amb el bin que en maximitza el pic.

Entre bandes diferents (E1↔E6), en canvi, el Doppler ja no és el mateix: s'escala per la relació de portadores, $f_{d,E6} = f_{d,E1} (f_6/f_1)$ —la mateixa relació que s'empra a la validació creuada del Doppler E1/E6 del bloc PVT (Secció 4.4.7).

4.2.8 Detecció del pic i interpolació sub-mostra

Fixat el millor Doppler, s'extreu el perfil de potència unidimensional $P(\tau)$ al llarg de la fase de codi. La detecció del pic distingeix dos casos:

- Per a la component pública de l'E6 (E6-B i E6-C públic) s'aplica una detecció de primer pic (amb lllindar relatiu de 0,7 respecte al màxim global): si existeix un pic anterior al màxim que en superi el 70 %, es pren aquell. La motivació és privilegiar la component de línia de vista (LOS) davant les rèpliques de multicamí, que arriben sempre més tard i amb menys potència. És una forma de detecció de multicamí de baixa complexitat, en la línia de la que descriu [Bor23] (cap. 9) per a receptors snapshot.
- Per a l'E1-B es pren el màxim global del perfil, que dona la posició de codi més precisa

quan el lòbul central de la BOC(1,1) domina (cosa garantida per l'alta C/N_0 de l'E1-B); la detecció de primer pic es manté com a diagnòstic de multicamí i d'ambigüitat BOC (Secció 4.2.11), però no substitueix la mesura.

- Per a l'E6-C xifrat (ECS) s'utilitza directament el màxim global, perquè la finestra de cerca està acotada per l'assistència ACAS (Secció 4.2.10) i el que interessa és el pic d'autenticació.

Com que a $f_s = 20$ MHz només hi ha $\approx 3,9$ mostres per chip a E6, la resolució nativa de la graella és insuficient. La interpolació sub-mostra del pic de correlació és, de fet, una etapa pròpia i necessària dels receptors snapshot, que processen blocs de mida entera amb la FFT i no disposen d'un llaç de seguiment que refini la fase de codi [Bor23] (cap. 9). La posició del pic es refina amb interpolació parabòlica de tres punts: donats els valors P_{-1}, P_0, P_{+1} al voltant del màxim discret τ_0 , el vèrtex de la paràbola que els ajusta és:

$$\delta = \frac{1}{2} \frac{P_{-1} - P_{+1}}{P_{-1} - 2P_0 + P_{+1}}, \quad \hat{\tau} = \tau_0 + \delta, \quad (4.9)$$

amb $\delta \in [-0,5, 0,5]$ el desplaçament fraccionari (mode `quadratic-polynomial-3-points`). Aquesta interpolació és essencial: com es veurà a la Secció 4.3, el llindar d'autenticació és de l'ordre d'una fracció de mostra, de manera que sense interpolació no seria possible discriminar correctament.

4.2.9 Mètriques de qualitat

Per a cada correlació es calculen tres mètriques que permeten decidir si la detecció és fiable i que actuen com a portes de qualitat per als blocs posteriors.

PPSP. El Peak-to-Peak-Side-Peak ratio (PPSP) és la relació, en dB, entre la potència del pic principal i la del pic secundari més gran situat fora d'una zona d'exclusió de $\pm \text{ppsp_exclusion_chips}$ (50 chips per defecte) al voltant del principal:

$$\text{PPSP} = 10 \log_{10} \frac{P_{\text{pic}}}{\max_{|\tau - \hat{\tau}| > W_{\text{excl}}} P(\tau)}. \quad (4.10)$$

És la mètrica de detecció clau: un PPSP elevat indica un pic net i inequívoc. Per a l'ECS aperiòdic la cerca del segon pic es fa sobre tota la finestra; per als codis periòdics, dins d'un període.

SNR. Relació entre la potència del pic i una estimació robusta del soroll, presa com la mediana del perfil de potència (insensible a la presència del propi pic): $\text{SNR} = 10 \log_{10} (P_{\text{pic}} / \text{med}\{P(\tau)\})$.

C/N_0 . La densitat de potència portadora a soroll (en dB-Hz) és la mètrica que es relaciona directament amb la probabilitat de detecció (Secció 2.2), però en una finestra curta no es pot mesurar de la manera habitual: les estimacions de SNR a la sortida del correlador necessiten mitjanes llargues per separar el senyal del soroll. S'empra, per això, l'estimador no coherent post-correlació de López-Risueño i Seco-Granados [LR05, SG12], que combina dues mesures de la mateixa instantània:

- la potència del senyal d'entrada $\hat{P} = \overline{|r[n]|^2}$, que en un senyal feble és gairebé només el nivell de soroll ($\hat{P} \approx N_0 B_n$, amb $B_n = f_s$ l'amplada de banda);
- la potència del pic de la correlació $R_{NC} = |\chi_{pic}|^2 N_{sc}^2/N_i$, que ja porta tot el guany del filtre adaptat (acumula $N_c N_{sc}$ mostres de manera coherent i N_i blocs de manera no coherent).

La idea és que la correlació concentra el senyal al pic amb un guany que creix amb el nombre de mostres integrades, mentre que el soroll, incoherent, no s'hi acumula igual: per això el pic (R_{NC}) i el nivell d'entrada ($\hat{P}$) depenen de la potència de portadora C i de la densitat de soroll N_0 amb pesos diferents. Les dues mesures formen, doncs, un sistema de dues equacions amb dues incògnites (C i N_0) que s'aïlla per donar directament la relació

$$\frac{\hat{C}}{N_0} = \frac{R_{NC} B_n - N_c N_{sc} \hat{P} f_s}{(N_c N_{sc})^2 \hat{P} - R_{NC}}, \quad (4.11)$$

amb N_{sc} les mostres per període de codi i N_c, N_i les integracions coherent i no coherent. En ser una densitat (per hertz), la C/N_0 no depèn del temps d'integració i permet comparar directament bandes i configuracions amb períodes de codi diferents.

4.2.10 Assistència de fase de codi (SAS)

La cerca cega del pic E6-C sobre tota la finestra és costosa i augmenta la falsa alarma. La implementació acota la finestra de cerca quan disposa de la informació temporal necessària, materialitzant el mode nominal SAS (Secció 2.3.4). A partir de l'instant GST de la instantània, de l'instant d'inici de la RECS i de l'interval d'incertesa total (provinent del bloc *UncertaintyModule*), es prediu la posició del pic dins de la instantània carregada:

$$\Delta t = t_{RECS} - t_{snapshot}, \quad n_{pred} = \Delta t \cdot f_s - n_{start}, \quad N_{cerca} = 2 \sigma_{tot} \cdot f_s, \quad (4.12)$$

on σ_{tot} és la incertesa total en temps i n_{start} el desplaçament de la finestra de mostres carregada. La cerca es restringeix a una finestra de $N_{cerca} = 2 \sigma_{tot} f_s$ mostres ancorada a la predicció n_{pred} . La lògica de decisió es resumeix a l'Algorisme 4.1: si la predicció cau fora de la instantània carregada, el sistema recorre automàticament a la cerca completa, garantint robustesa davant errors de configuració temporal.

```

1  si (mode == ECS) i (snapshot_gst, recs_gst, sigma_tot disponibles):
2      delta_t = recs_gst - snapshot_gst
3      abs_sample = round(delta_t * fs)
4      predicted = abs_sample - start_sample
5      si 0 <= predicted < N_mostres:
6          cp_est = predicted # inici de la finestra de cerca
7          ns_acq = round(2 * sigma_tot * fs) # amplada de la finestra
8      altrament:
9          cp_est = 0; ns_acq = 0 # -> cerca completa
10 altrament:
11     cp_est = 0; ns_acq = 0 # -> cerca completa

```

Listing 4.1: Assistència de fase de codi (ACAS) per a l'E6-C.

4.2.11 Banda auxiliar E1 i emparellament de període

En mode multibanda, el bloc correlaciona també l'E1-B amb la seva modulació BOC(1,1). L'autocorrelació BOC presenta pics laterals a banda i banda del principal (Secció 2.1) —el conegut repte d'ambigüitat [Bor23] (cap. 10)—, que pot fer que el receptor s'enganxi a un lòbul lateral. El risc s'atenueja perquè, en bona relació senyal-soroll, el lòbul central és el màxim absolut (prendre el màxim global ja l'encerta) i perquè la validació creuada del Doppler E1↔E6 del bloc PVT (Secció 4.4.7) descarta les correlacions falses; la detecció de primer pic (Secció 4.2.8) es manté com a diagnòstic.

A més, l'E1-B i l'E6-C es mesuren en instants diferents de la mateixa instantània: l'E1-B prop de l'inici i l'ECS de l'E6-C centenars de mil·lisegons més tard (on apunta l'assistència ACAS, Secció 4.2.10). Entremig, la fase de codi deriva per la velocitat radial del satèl·lit, de manera que no es poden comparar directament. Per això es propaga la fase de l'E1-B fins a l'època de l'E6-C (propagació per velocitat de rang, [FH23]):

$$\hat{\tau}_{E1}(t_{E6}) = \hat{\tau}_{E1}(t_{E1}) - \frac{f_{d,E1}}{f_1} (t_{E6} - t_{E1}) f_s, \quad (4.13)$$

on $f_{d,E1}$ és el Doppler de portadora de l'E1-B, f_1 la seva freqüència i $(t_{E6} - t_{E1}) f_s$ la separació en mostres entre els dos pics; la propagació també fixa quin període de l'E1-B correspon al pic de l'E6-C. Sense aquesta correcció el residu de rang quedaria dominat per la deriva (centenars de metres per a separacions de centenars de mil·lisegons); amb ella, es redueix al biaix de maquinari E1/E6 del receptor, que compensa el calibratge (Secció 4.3.6).

4.2.12 Sortides del bloc

El bloc produeix, per a cada PRN i component, un registre amb el desplaçament de codi (en mostres, interpolat), el Doppler, la potència del pic i les tres mètriques (PPSP, SNR, C/N₀), a

més dels perfils de potència complets per a la visualització. Aquests resultats es publiquen al context d'execució i els consumeixen el bloc de processament de rang per satèl·lit i el computador de PVT.

4.3 Bloc de processament de rang per satèl·lit

Aquest bloc implementa el test d'autenticació del SAS seguint el model de mesura de [FH23] (Eqs. (20)–(24)). La idea és comparar el retard de codi mesurat a l'E6-C amb el retard esperat derivat de l'E1-B: si coincideixen dins d'un marge estadístic, el rang és autèntic.

4.3.1 Conversió entre mostres i metres

Les mesures de la correlació són en mostres, però el model d'error s'expressa en metres. La conversió depèn de la banda, ja que la resolució de chip és diferent. Una mostra correspon a

$$\ell_{\text{mostra}} = \frac{c}{f_s}, \quad (4.14)$$

que a $f_s = 20$ MHz val ≈ 15 m. La longitud d'un chip és $\ell_c^{E1} = c/R_c^{E1} \approx 293,05$ m i $\ell_c^{E6} = c/R_c^{E6} \approx 58,61$ m, cosa que il·lustra de nou per què l'E6 dona una autenticació de rang molt més precisa.

4.3.2 Estimació del retard esperat i compensació E1–E6

El retard esperat de l'E6-C s'estima a partir de l'E1-B (Eq. 20 de [FH23]):

$$\hat{\tau}_{E6} = \tau_{E1} + \delta_{E1,E6}, \quad (4.15)$$

Aquesta comparació directa entre bandes és legítima perquè la major part dels termes que componen el retard són comuns a l'E1 i a l'E6 i es cancel·len en la diferència $\tau_{E6} - \tau_{E1}$: un cop totes dues mesures es refereixen al mateix instant (per la propagació per velocitat de rang de la Secció 4.2.11), el rang geomètric, el rellotge del satèl·lit i la correcció relativista són idèntics en les dues bandes, i la troposfera, en ser no dispersiva, també hi afecta per igual. Només sobreviuen els biaixos que depenen de la banda, que $\delta_{E1,E6}$ (Eq. 14) aplega:

- el **retard de grup de difusió** (BGD), biaix de maquinari del satèl·lit entre les cadenes E1 i E6.
- el **diferencial ionosfèric** $\delta I_{E1,E6}$, conseqüència de la dependència $\propto 1/f^2$ del retard ionosfèric, que val $I_{E1} (f_1^2/f_6^2 - 1)$ i que en aquest treball s'estima amb el model NeQuick-G (Secció 4.3.5);

- el **biaix de maquinari del receptor** (HWB), per les diferents cadenes RF d'E1 i E6.

Els errors que també difereixen entre bandes però són aleatoris (el multicamí i el soroll tèrmic, independents en E1 i E6) no esbiaixen $\hat{\tau}_{E6}$: no entren en $\delta_{E1,E6}$ sinó que n'eixamplen la incertesa, i es recullen en la variància σ_{auth}^2 que fixa el llindar de decisió (Eq. 24 de [FH23]).

4.3.3 Maneig de la periodicitat i embolcall

L'E1-B és periòdic: el seu codi es repeteix cada 4 ms (4092 chips), de manera que la correlació en localitza el pic dins d'un període però no indica en quin període de la finestra cau —és l'ambigüitat de fase de codi pròpia dels receptors snapshot [FH16]. L'ECS de l'E6-C, en canvi, és aperiòdic i dóna una posició inequívoca dins de la finestra. Per comparar-les, totes dues mesures es redueixen a la fase dins d'un període de codi E1-B (la posició dins del cicle de 4 ms, $\phi = \tau \bmod N_{\text{per}}^{E1}$), on $N_{\text{per}}^{E1} = f_s T_{\text{codi}}^{E1} = f_s \cdot 4092 / R_c^{E1}$ és el període en mostres (80 000 a 20 MHz).

Aquesta fase és una magnitud circular, com un angle: els valors 0 i N_{per}^{E1} representen el mateix punt del cicle. Per això la diferència Δ entre la fase mesurada i l'esperada no es pot prendre restant els valors sense més, sinó pel camí més curt al voltant del període. Quan Δ supera mig període, es corregeix per embolcall sumant o restant un període sencer:

$$\Delta \leftarrow \begin{cases} \Delta - N_{\text{per}}^{E1} & \text{si } \Delta > N_{\text{per}}^{E1}/2, \\ \Delta + N_{\text{per}}^{E1} & \text{si } \Delta < -N_{\text{per}}^{E1}/2, \\ \Delta & \text{altrament.} \end{cases} \quad (4.16)$$

Sense aquesta correcció, un parell genuí que caigués a banda i banda de la frontera del període (una fase a prop de 0 i l'altra a prop de N_{per}^{E1}) mostraria una diferència artificialment gran, de gairebé un període sencer, i es rebutjaria com a no autèntic tot i estar a poques mostres de distància real. L'embolcall garanteix que Δ reflecteixi sempre la separació física entre els dos pics.

4.3.4 Llindar d'autenticació

La diferència entre el retard mesurat i l'esperat es compara amb un llindar:

$$\Delta = \tau_{E6} - \hat{\tau}_{E6}, \quad \xi = \begin{cases} 1 \text{ (autèntic)} & |\Delta| \leq \gamma_{\text{auth}} \\ 0 \text{ (no autèntic)} & |\Delta| > \gamma_{\text{auth}}. \end{cases} \quad (4.17)$$

El llindar és $\gamma_{\text{auth}} = \kappa \sigma_{\text{auth}}$, amb κ el factor de confiança (Taula 4.2) i σ_{auth} la desviació estàndard total de l'error de mesura, calculada com l'arrel de la suma de variàncies de set fonts d'error independents (Eq. 24):

$$\sigma_{\text{auth}}^2 = \sigma_{\text{HWB}_{rx}}^2 + \sigma_{\text{BGD}}^2 + \left(\sigma_{I,E1} \left(\frac{f_1^2}{f_6^2} - 1 \right) \right)^2 + \sigma_{\text{MP},E1}^2 + \sigma_{\text{MP},E6}^2 + \sigma_{n,E1}^2 + \sigma_{n,E6}^2, \quad (4.18)$$

on el factor $(f_1^2/f_6^2 - 1) = 0,518$ surt directament de les portadores $f_1 = 1575,42$ MHz i $f_6 = 1278,75$ MHz (Eq. 18 de [FH23]). Com que la ionosfera retarda més les freqüències baixes, l'E6 (de freqüència inferior) pateix un retard addicional respecte a l'E1, i el diferencial $\delta I_{E1,E6} = I_{E1} (f_1^2/f_6^2 - 1)$ entra en el barem proposat a través d'aquest factor. La Taula 4.3 recull els valors per defecte (receptor sense correccions) i els corregits (amb fitxer BGD i model NeQuick-G), que donen $\sigma_{\text{auth}} \approx 9,2$ m i $\approx 5,5$ m respectivament. El test es realitza internament en mostres ($\gamma_{\text{auth}}^{[\text{mostres}]} = \gamma_{\text{auth}} f_s/c$), de manera que els l·lindars equivalen a fraccions de mostra —cosa que justifica la interpolació de l'Eq. (4.9).

Taula 4.2: Factor de confiança κ i nivell de confiança associat (distribució normal).

κ	1	2	3	4
Confiança (%)	68,27	95,45	99,73	99,99

Taula 4.3: Components de l'interval d'incertesa σ_{auth} (Eq. (4.18)); valors de partida de [FH23] i estimacions experimentals per a aquest receptor (vegeu el text).

Component	Sense corregir [m]	Corregit [m]
$\sigma_{\text{HWB}_{rx}}$ (biaix de maquinari rx)	0,0	0,0
σ_{BGD} (retard de grup)	1,5	0,0
$\sigma_{I,E1}$ (ionosfera E1) $\times 0,518$	15,0	3,5
$\sigma_{\text{MP},E1}$ (multicamí E1)	3,0	3,0
$\sigma_{\text{MP},E6}$ (multicamí E6)	0,6	0,6
$\sigma_{n,E1}$ (soroll E1, snapshot)	3,0	3,0
$\sigma_{n,E6}$ (soroll E6, snapshot)	2,5	2,5
σ_{auth} (RSS total)	$\approx 9,2$	$\approx 5,5$
γ_{auth} ($\kappa = 3$)	$\approx 27,6$	$\approx 16,5$

Cal remarcar que alguns d'aquests valors —en particular el soroll de mesura en mode snapshot ($\sigma_{n,E1}$ i $\sigma_{n,E6}$) i les magnituds pre-correcció del retard de grup i de la ionosfera— són experimentals: s'han escollit després de les proves sobre els conjunts de dades reals analitzats i no són constants universals, sinó que depenen de la C/N_0 , l'elevació, la dinàmica i l'entorn de cada captura —una limitació que el mateix [FH23] reconeix en qualificar de preliminars les seves estimacions. Els valors de la taula són, doncs, ordres de magnitud representatius per a aquest receptor i aquestes campanyes, i el l·lindar operatiu es recalcula amb les condicions de cada captura

(per això la Taula 4.4 en cita $\gamma_{\text{auth}} \approx 13$ m). Una caracterització estadística rigorosa d'aquestes components, sobre un conjunt més ampli de captures i condicions, queda com a treball futur (Capítol 6).

4.3.5 Correcció ionosfèrica amb NeQuick-G

Dels tres biaixos de l'Eq. (4.15), el diferencial ionosfèric és el dominant i el més variable: depèn de l'hora del dia, de l'estació de l'any i de l'elevació del satèl·lit. De fet, el valor $\sigma_{I,E1} = 3,5$ m de la columna corregit de la Taula 4.3 és el residual que resta després d'aplicar una correcció ionosfèrica; sense correcció el terme puja a ~ 15 m i, pel factor 0,518, gairebé duplica γ_{auth} . Per això s'ha incorporat el càlcul explícit d'aquest retard.

S'empra el model NeQuick-G, el model ionosfèric oficial de Galileo per a usuaris d'una sola freqüència [Eur16], basat en NeQuick 2 [Nav08]. El model es controla amb els tres coeficients de difusió (a_{i0}, a_{i1}, a_{i2}) que Galileo radiodifon al missatge de navegació i que apareixen a la capçalera GAL de les efemèrides RINEX. A partir d'aquests coeficients, de la posició del receptor i del satèl·lit i de l'època, NeQuick-G retorna el contingut total d'electrons obliquè (STEC, en TECU). El retard de codi a l'E1 i el diferencial E1–E6 s'obtenen amb

$$I_{E1} = \frac{40,3}{f_1^2} \text{STEC} \approx 0,162 \text{STEC [TECU]}, \quad \delta I_{E1,E6} = I_{E1} \left(\frac{f_1^2}{f_6^2} - 1 \right). \quad (4.19)$$

Pel que fa a la implementació, s'han pres tres decisions de disseny:

- Model i biblioteca. S'integra la implementació de referència del JRC [FM24] en lloc de reimplementar el model, atesa la seva complexitat (mapes CCIR estacionals, MODIP). Els coeficients $a_{i0,1,2}$ es prenen de la capçalera de les pròpies efemèrides del dia; la posició del receptor s'extreu del nom del fitxer de snapshot (tot i que es pot computar en el següent bloc) i la del satèl·lit de les efemèrides.
- Correcció per satèl·lit. Com que el STEC obliquè depèn de l'elevació i l'azimut de cada satèl·lit, $\delta I_{E1,E6}$ es calcula per a cada PRN dins del bucle d'autenticació, i no com un únic escalar comú.
- Disponibilitat d'efemèrides. Els productes horaris d'efemèrides sovint ometen els satèl·lits d'òrbita excèntrica (E14, E18) i, en fitxers fusionats, eliminen la capçalera GAL. Quan falta un PRN sol·licitat o els coeficients, el bloc d'efemèrides recorre automàticament al producte diari combinat de l'IGS[Int25], que inclou tots els satèl·lits Galileo i els coeficients ionosfèrics.

La Taula 4.4 mostra l'efecte de la correcció sobre els dos conjunts de dades reals analitzats, amb efemèrides i coeficients descarregats per a cada dia. El contrast és coherent amb la física.

NeQuick-G calcula el STEC de cada satèl·lit integrant el contingut d'electrons al llarg del raig real receptor-satèl·lit; per això depèn tant de l'estat de la ionosfera (l'hora del dia: la ionització solar és més alta de dia que de nit) com de la geometria, mitjançant l'angle d'incidència. Com més baixa és l'elevació, més obliquament travessa el raig la ionosfera i més llarg és el camí dins seu, de manera que el STEC creix per damunt del contingut vertical pel factor d'obliquïtat, que val 1 al zenit i augmenta com més baixa és l'elevació. En els dos conjunts analitzats domina aquest efecte geomètric: PRN 18, mesurat a només 16,3° d'elevació, dona un STEC de 55,2 TECU, gairebé el doble del de PRN 14, mesurat a 40,0° (30,6 TECU); la captura de migdia de PRN 18, davant de la nocturna de PRN 14, hi contribueix en el mateix sentit. Després de la correcció, el biaix residual baixa a l'ordre del metre i correspon ja al maquinari (HWB, BGD) i al soroll de mesura. Tots dos residuals queden molt per sota de γ_{auth} , de manera que els satèl·lits autèntiquen sense recórrer al calibratge empíric de la Secció 4.3.6 —el mode coherent amb el model de [FH23].

Taula 4.4: Biaix de codi E1–E6 abans i després de la correcció NeQuick-G (efemèrides i coeficients $a_{i0,1,2}$ reals de cada dia). El residual queda molt per sota de $\gamma_{\text{auth}} \approx 13$ m amb el model d'error d'aquests conjunts.

Conjunt (època)	Elev.	STEC	$\delta I_{E1,E6}$	Biaix cru	Residual
	[°]	[TECU]	[m]	[m]	[m]
PRN 14 (200626, nit)	40,0	30,6	2,57	3,09	0,51
PRN 18 (230626, migdia)	16,3	55,2	4,64	9,45	4,80

4.3.6 Calibratge automàtic del biaix del receptor

El terme HWB_{rx} (biaix entre les cadenes RF d'E1 i E6 del propi receptor) és un offset sistemàtic comú a tots els satèl·lits. Un experiment dedicat (correlacionant el mateix senyal E1-B a les dues cadenes BladeRF) en confirma el caràcter: el biaix és un desplaçament estable ($\mu \approx -5,2$ m), amb poc *jitter* ($\sigma = 1,05$ m) i sense deriva apreciable al llarg de la captura (Figura 4.3). El bloc l'estima de manera automàtica a partir de les pròpies mesures —per exemple, com la mediana de les diferències Δ del conjunt de satèl·lits amb detecció fiable— i el resta abans d'aplicar el test. Aquest calibratge redueix els falsos negatius deguts a una calibració imperfecta del maquinari, sense necessitat d'una calibració externa prèvia. Tanmateix, és un ajust empíric que requereix diversos satèl·lits i pot emascarar un atac; per això, un cop la component ionosfèrica es compensa de manera determinista amb NeQuick-G (Secció 4.3.5), el calibratge automàtic esdevé opcional i els conjunts analitzats autèntiquen amb $\delta_{E1,E6}$ purament determinista.

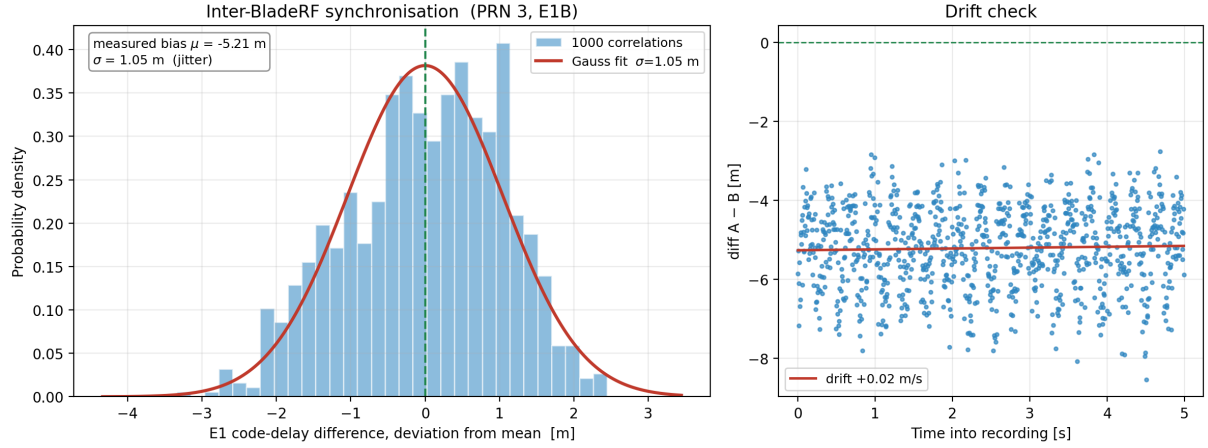


Figura 4.3: Caracterització del biaix de maquinari del receptor (HWB): histograma de la diferència de retard de codi entre les dues cadenes BladeRF (mateixa entrada E1-B, PRN 3), amb el seu ajust gaussià —mitjana $\mu = -5,21$ m (el HWB) i desviació $\sigma = 1,05$ m (el *jitter*)—; a la dreta, la diferència es manté estable al llarg de la captura.

4.3.7 Autenticació de posició

L'autenticació de cada satèl·lit (Eq. (4.17)) encara s'ha de traslladar a la posició. Com que la solució PVT es construeix amb les mesures de tots els satèl·lits alhora, n'hi ha prou que una de manipulada hi entri perquè en desplaci el resultat; per això la posició només es considera autenticada quan tots els satèl·lits que hi contribueixen superen el seu test individual:

$$\Xi = \prod_{k=1}^K \xi_k = 1 \iff \text{posició autenticada.} \quad (4.20)$$

És, doncs, una conjunció lògica (el producte de les decisions binàries ξ_k): un sol satèl·lit que caigui fora de la seva banda ($\xi_k = 0$) fa $\Xi = 0$ i invalida tot el conjunt. Aquesta passa és la que converteix l'autenticació de senyal, satèl·lit a satèl·lit, en autenticació de la posició, que és l'objectiu final del servei [FH23]. La Figura 4.4 en resumeix el criteri de manera esquemàtica. El bloc, a més, genera les gràfiques de qualitat de publicació (la comparació dels pics E1-B i E6-C i el diagrama de Δ per PRN) i persisteix el veredictes i totes les magnituds en format JSON.

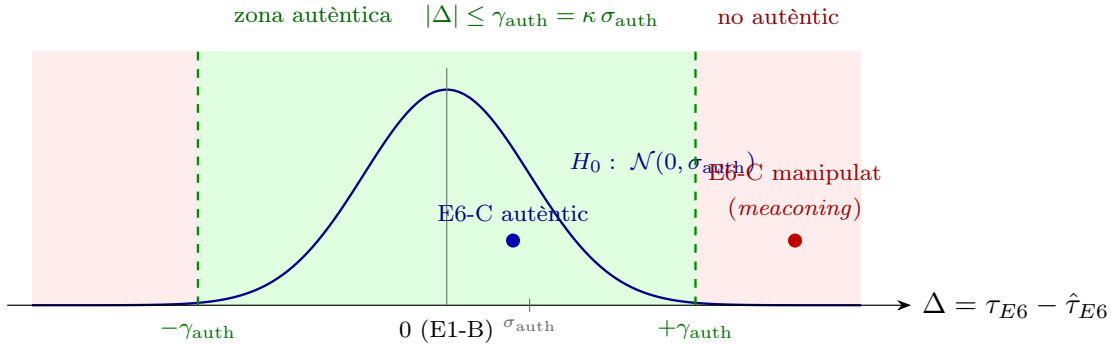


Figura 4.4: Criteri d'autenticació (esquema): el satèl·lit s'autentica si el residu $\Delta = \tau_{E6} - \hat{\tau}_{E6}$ cau dins la banda $|\Delta| \leq \gamma_{\text{auth}}$ (verd); una manipulació per *meaconing* en desplaça el pic d'E6-C fora. Adaptat de [FH23].

4.4 Computador de PVT

Aquest bloc calcula la solució de posició, velocitat i temps a partir de les mesures (autenticades) de la correlació. Implementa l'algorisme de posicionament snapshot sense informació inicial de Fernández i Borre [FH16, FH15], adaptat a Galileo (port de la referència MATLAB “snaprx”).

4.4.1 Plantejament: navegació de temps aproximat

D'una instantània de pocs mil·lisegons, el receptor només pot extreure una fase de codi fracciònia —coneguda mòdul el període (4 ms a E1-B, una ambigüïtat de $c \cdot 4 \text{ ms} \approx 1200 \text{ km}$)— i, en operar en bucle obert sense desxifrar el missatge de navegació, tampoc no en coneix el temps absolut amb precisió. Calen, doncs, dues coses: resoldre l'ambigüïtat de període (l'enter de codis sencers N_k que completa la pseudodistància) i tractar el temps aproximat com una incògnita addicional, ja que un error de temps desplaça les posicions dels satèl·lits. Aquesta segona idea és la navegació de temps aproximat (“coarse-time navigation”), que afegeix una cinquena incògnita Δt a les equacions de navegació [Bor23].

La particularitat de l'algorisme de Fernández i Borre [FH16, FH15] és que no necessita cap estimació inicial de posició ni de temps (pot arrencar amb errors de temps de més d'una hora). Es resol en dues etapes iteratives de mínims quadrats (LS) de cinc estats cadascuna (Figura 4.5). Primer, la CT-Doppler fixa una posició i un temps aproximats a partir del Doppler, que és inequívoc —no pateix l'ambigüïtat de codi. Aquesta llavor permet després a la CT-PRange resoldre l'ambigüïtat N_k i refinar la solució amb les fases de codi.

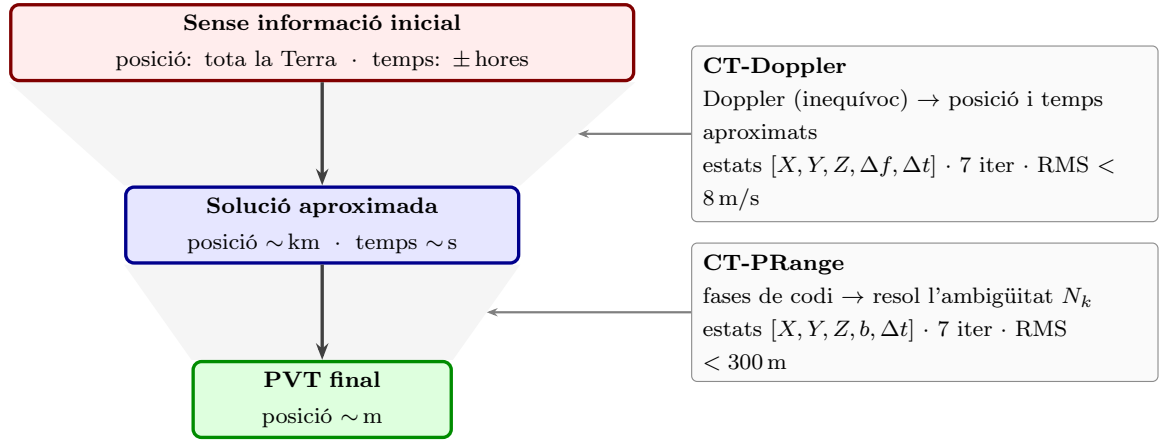


Figura 4.5: Càlcul PVT snapshot com a refinament progressiu de la incertesa. Partint de cap informació inicial (posició indeterminada, error de temps de fins a hores), la CT-Doppler (a partir del Doppler, inequívoc) redueix la solució a una posició i un temps aproximats ($\sim\text{km}$, $\sim\text{s}$); aquesta llavor permet a la CT-PRange resoldre l'ambigüitat de període N_k amb les fases de codi i arribar a la solució final ($\sim\text{m}$). Adaptat de [FH16, Bor23].

4.4.2 Posició del satèl·lit a partir de les efemèrides

Per a cada satèl·lit cal la seva posició ECEF a l'instant de transmissió. Les efemèrides de difusió (RINEX) no la donen directament, sinó un conjunt de paràmetres orbitals quasi-keplerians (semeix major, excentricitat, inclinació...) més uns termes de correcció harmònica que en modelen les pertorbacions, vàlids només unes hores al voltant d'una època de referència t_{oe} . A partir d'aquests paràmetres, el bloc reconstrueix la posició amb l'algorisme estàndard d'efemèrides de difusió, especificat a l'ICD de Galileo [Eur23b] (idèntic al de GPS) i implementat com a port de la rutina de Borre [Bor23].

El nucli de l'algorisme és resoldre l'equació de Kepler per a l'anomalia excèntrica E ,

$$E = M + e \sin E, \quad (4.21)$$

on M és l'anomalia mitjana, que avança linealment amb el temps des de t_{oe} ; es resol per iteració. Amb E s'obté la posició al pla orbital, s'hi sumen les correccions harmòniques de segon ordre (els coeficients $c_{uc}, c_{us}, c_{rc}, c_{rs}, c_{ic}, c_{is}$ de les efemèrides) a l'argument de latitud, el radi i la inclinació, i es projecta a coordenades ECEF. Finalment s'apliquen la correcció de rellotge del satèl·lit (polinomi $a_{f0} + a_{f1} dt + a_{f2} dt^2$), la relativista $\Delta t_r = F e \sqrt{a} \sin E$ i el BGD, i una rotació $R(\Omega_e \tau)$ que compensa el gir de la Terra durant el temps de propagació τ del senyal. El model treballa sobre l'el·lipsoide WGS-84-84.

4.4.3 Conversions de coordenades i models atmosfèrics

El bloc implementa les conversions clàssiques (ports de les rutines de Kai Borre [Bor23]): `cart2geo/togeod` (ECEF→geodèsic per iteració de Bowring), `geod2cart` (geodèsic→ECEF) i `topocent` (vector ECEF→azimut, elevació i distància, via rotació ENU). Les correccions atmosfèriques són la troposfèrica (model de Goad–Goodman en funció de l'elevació) i la ionosfèrica (model de Klobuchar, si es disposa dels coeficients α, β), que es recalculen a cada iteració amb l'elevació actualitzada de cada satèl·lit.

4.4.4 Etapa 1: CT-Doppler

La primera etapa estima una posició i un temps aproximats a partir només del Doppler. A diferència de la fase de codi, el Doppler no és ambigu: cada satèl·lit, segons la seva geometria i velocitat relativa, en té un de diferent, i això permet trobar la solució sense cap informació inicial.

El Doppler de portadora de cada satèl·lit es converteix en velocitat de rang (el ritme amb què canvia la distància satèl·lit-receptor), $\dot{\rho} = f_d c / f_{\text{port}}$. A partir de les velocitats de rang de tots els satèl·lits visibles s'estimen cinc estats $\mathbf{x} = [X, Y, Z, \Delta f, \Delta t]^\top$: la posició del receptor, l'“offset” de freqüència del seu rellotge Δf (que afecta per igual tots els Doppler) i una correcció del temps aproximat Δt .

El punt subtil (i l'aportació de Fernández i Borre [FH16]) és com hi entra Δt : un error de temps desplaça els satèl·lits al llarg de la seva òrbita, i això canvia la velocitat de rang en proporció a l'acceleració relativa satèl·lit-receptor, $\dot{\rho}(t) \approx \dot{\rho}(t_0) + \ddot{\rho} \Delta t$. Linealitzant al voltant d'una estimació, l'equació d'observació de cada satèl·lit k té, doncs, tres contribucions (posició, rellotge i temps aproximat):

$$\delta \dot{\rho}_k = \mathbf{e}'_k \cdot \delta \mathbf{r} + \delta f + \ddot{\rho}_k \delta t, \quad (4.22)$$

on $\mathbf{e}'_k$ (la derivada del vector de línia de vista) dóna la sensibilitat a la posició, δf és comú a tots els satèl·lits i $\ddot{\rho}_k$ és la sensibilitat al temps aproximat. Apilant aquestes equacions per a tots els satèl·lits s'obté el sistema, que es resol per mínims quadrats iteratiu (7 iteracions):

$$\Delta \mathbf{x} = (\mathbf{H}^\top \mathbf{H})^{-1} \mathbf{H}^\top \Delta \dot{\boldsymbol{\rho}}, \quad (4.23)$$

amb $\mathbf{H}$ formada per les files de l'Eq. (4.22). Les velocitats i acceleracions dels satèl·lits es calculen numèricament avaluant-ne la posició en instants separats 1 s. Es conserva la solució de menor residu de totes les iteracions i es declara convergència quan l'RMS baixa de 8 m/s.

Quan no es disposa de cap posició inicial (arrencada en fred), l'etapa es resol amb una cerca en graella sobre la superfície terrestre (pas de 30° en latitud i longitud): s'executa la CT-Doppler

des de cada punt de partida i es conserva la millor solució. Com que hi ha cinc incògnites, calen com a mínim cinc satèl·lits.

4.4.5 Etapa 2: CT-PRange amb resolució d'ambigüitat

La segona etapa refina la solució amb les fases de codi, molt més precises que el Doppler. Els cinc estats són $\mathbf{x} = [X, Y, Z, b, \Delta t]^\top$: la posició, el biaix de rellotge del receptor b (en metres) i, igual que abans, la correcció del temps aproximat Δt . El paral·lisme amb la CT-Doppler és il·lustratiu: allà el temps aproximat entrava per l'acceleració del satèl·lit; aquí ho fa per la seva velocitat —un error de temps el desplaça per l'òrbita i en canvia la pseudodistància en $\dot{\rho}_k \Delta t$. L'equació d'observació de cada satèl·lit és, doncs,

$$\delta \rho_k = -\mathbf{e}_k \cdot \delta \mathbf{r} + \delta b + \dot{\rho}_k \delta t, \quad (4.24)$$

amb $\mathbf{e}_k$ el vector de línia de vista (sensibilitat a la posició) i $\dot{\rho}_k$ la velocitat de rang —el terme que distingeix la navegació de temps aproximat de la PVT clàssica [Bor23].

El pas crític és formar les pseudodistàncies completes. La fase de codi ϕ_k només es coneix mòdul el període (4 ms), de manera que la pseudodistància real és $\rho_k = \phi_k + N_k T_{\text{codi}} c$ i cal determinar l'enter de períodes sencers N_k de cada satèl·lit —l'ambigüitat. La posició aproximada de la CT-Doppler ja ho fa possible: l'algorisme pren com a referència el satèl·lit de més elevació (el menys afectat per multicamí i atmosfera), n'estima l'ambigüitat N_0 i resol les dels altres per consistència geomètrica,

$$N_k = \text{round} \left(\frac{N_0 T_{\text{codi}} + \phi_0 - \phi_k + (\hat{\rho}_k - \hat{\rho}_0)}{T_{\text{codi}}} \right), \quad (4.25)$$

on $\hat{\rho}$ són les pseudodistàncies predites per la posició actual. A cada iteració s'apliquen, a més, les correccions troposfèrica, ionosfèrica, de rellotge del satèl·lit, relativista i BGD (Seccions 4.4.2 i 4.4.3), i el sistema es resol per mínims quadrats iteratiu (7 iteracions); es declara convergència quan l'RMS dels residus baixa de 300 m.

4.4.6 Casos amb pocs satèl·lits

Quan es disposa de menys de 5 satèl·lits, la implementació admet dues estratègies per reduir el nombre d'incògnites: fixar el temps aproximat (`fix_time`), que redueix el problema a 4 estats $[X, Y, Z, b]$; i afegir una restricció d'altitud ("altitude constraint"), una equació addicional que fixa l'altura sobre l'el·lipsoide, cosa que permet calcular una solució amb només 3 satèl·lits (3 mesures + 1 restricció = 4 equacions). Si es disposa de pseudodistàncies completes no ambigües, s'inclou també un solucionador clàssic de mínims quadrats de 4 estats.

4.4.7 Control de qualitat i validació creuada

Abans i durant el càlcul, el bloc aplica diversos controls per garantir la robustesa:

- Salut del satèl·lit: es descarten els satèl·lits marcats com a no saludables a les efemèrides.
- Portes de qualitat: es rebutgen les mesures amb $\text{PPSP} < 3 \text{ dB}$ o $\text{C/N}_0 < 38 \text{ dB-Hz}$ (valors per defecte).
- Validació creuada de Doppler E1/E6: es comprova que el Doppler de l'E1-B sigui consistent amb el de l'E6-B escalat per la relació de portadores, $f_d^{E1} \approx f_d^{E6} (f_1/f_6)$; una discrepància superior a 500 Hz delata una enganxada de correlació falsa i la mesura es descarta.

4.4.8 Sortides i indicadors

El bloc retorna la posició en coordenades geodèsiques (latitud, longitud, altitud sobre l'el·lipsoide WGS-84), el biaix de rellotge, el temps total estimat i els indicadors de dilució de la precisió ($\text{GDOP} = \sqrt{\text{tr}\{(\mathbf{H}^\top \mathbf{H})^{-1}\}}$, PDOP). Quan es configura una posició de referència, es calcula l'error de posició. La solució i totes les magnituds intermèdies (residus, ambigüitats, elevacions, azimuts) es persisteixen en format JSON.

Capítol 5

Resultats i discussió

La validació es fa en dues etapes. Primer, una validació funcional end-to-end amb el senyal E6-C xifrat real de la campanya de juny de 2025 [TG25], que valida el bloc més crític de la cadena (la correlació i la detecció) i constitueix els primers resultats de SASlib, recollits també a [TG26a]. Després, un refinament amb captures pròpies E1/E6 que tanca el pressupost d'error determinista i executa el test d'autenticació de rang (Secció 5.2).

5.1 Validació funcional amb senyal E6-C xifrat real

Es processen amb SASlib les dades de la campanya en què el satèl·lit excèntric E14 (PRN 14) va emetre l'E6-C xifrat [TG25, FH24], exercitant tot el flux del receptor: parsing de la RECS, recuperació de la clau TESLA, desxifratge (AES-CBC), generació de la rèplica ECS i correlació amb la instantània E6-C ($f_s = 20$ MHz). En aquesta etapa l'objectiu era sobretot trobar el pic de l'ECS, ja que detectar-lo implica que tota la cadena funciona correctament. Es tracta, doncs, d'una validació funcional de la cadena de processament i no d'una caracterització estadística completa de prestacions [TG26a]. A més, era un test ja preparat (post-processat d'una instantània enregistrada amb els paràmetres coneguts d'antuvi), de manera que no hi intervenien altres factors que sí que apareixerien en una execució a temps real, com la incertesa de rellotge i d'època més gran, l'espera a la divulgació en viu de la clau TESLA entre d'altres.

La Figura 5.1 mostra el resultat central: el perfil de correlació de l'E6-C amb l'ECS desxifrada, per a les dues configuracions de KDI. En tots dos casos apareix un pic únic i net molt per damunt del soroll; com que només es forma si la seqüència desxifrada coincideix amb el senyal rebut, la seva detecció és l'autenticació de rang. A més, la separació entre els pics (938 146 i 1 258 145, és a dir 319 999 mostres ≈ 16 ms) coincideix amb el desplaçament de KDI de l'ICD [FH24], cosa que verifica tota la cadena cripto-temporal. Les mètriques de la banda E6 (PPSP = 13,6 dB a l'E6-B

d'ajut; $PPSP = 7,54 \text{ dB}$, $SNR = 10,8 \text{ dB}$ a l'E6-C amb ECS) confirmen un marge de detecció ampli, i la cerca es va acotar amb l'assistència ACAS (Secció 4.2.10).

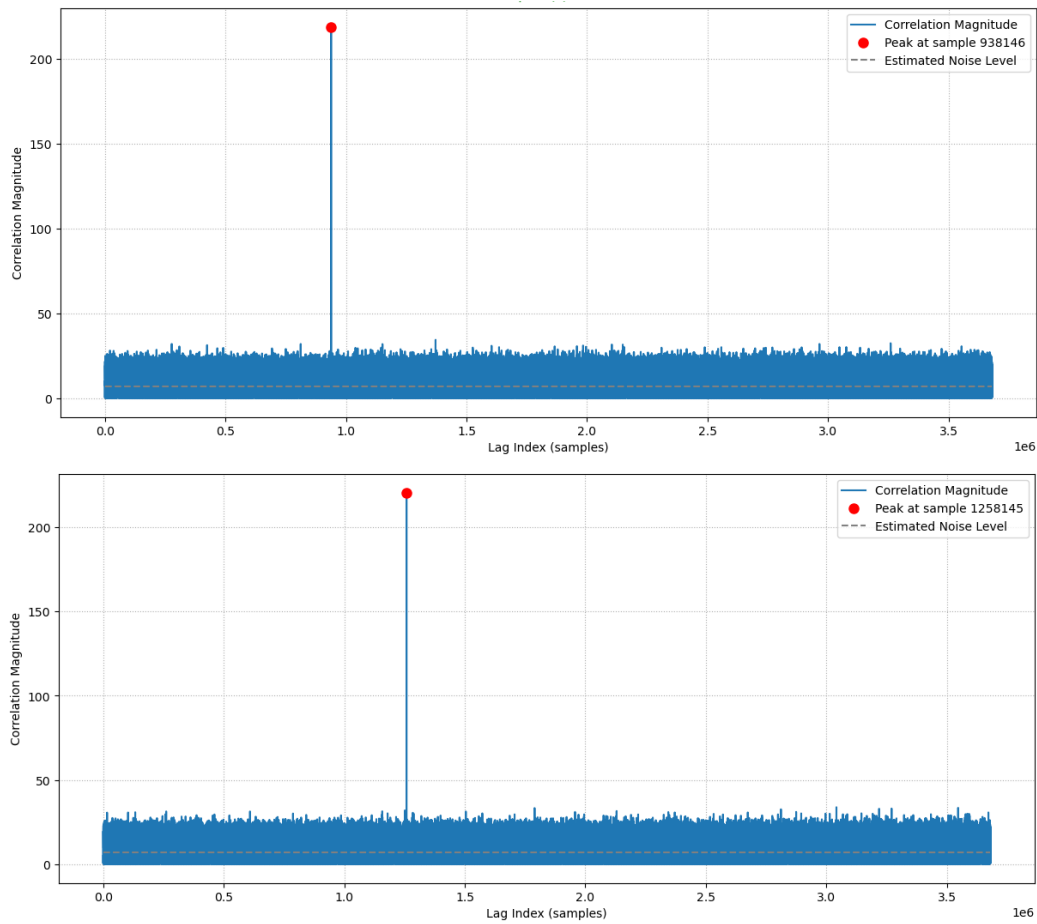


Figura 5.1: Pic d'autenticació de l'E6-C del PRN 14 amb l'ECS desxifrada, a dalt amb $KDI = 0$ i a baix amb $KDI = 1$.

Finalment, el mecanisme del SAS exigeix que el retard de codi de l'E6-C sigui consistent amb el de l'E1-B (Secció 4.3). La Figura 5.2 compara els pics d'E1-B (BOC(1,1)) i E6-C: la diferència de fase és de 0,697 mostres ($\approx 10,45 \text{ m}$), el residu Δ que alimenta el test d'autenticació, ja dins de la zona autèntica fins i tot amb el pressupost sense corregir ($\gamma_{\text{auth}} \approx 27,6 \text{ m}$, Taula 4.3).

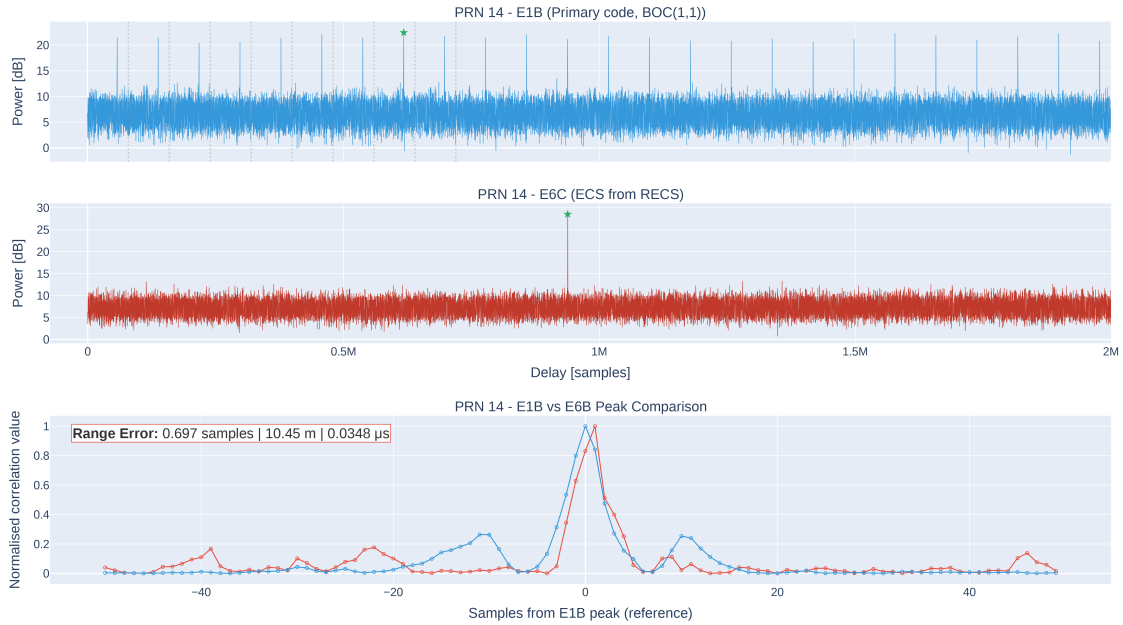


Figura 5.2: Correlacions de l'E1-B (BOC(1,1)) i l'E6-C (ECS) del PRN 14, amb una vista ampliada dels dos pics.

Aquests resultats validen tota la cadena de processament sobre senyal xifrat real (el bloc més complex i decisiu reproduceix les plataformes de referència [TG25]) i cobreixen els objectius 2, 3 i 4 del Capítol 1. Encara no inclouen, però, els matisos deterministes del test de rang (BGD, propagació *range-rate* i calibratge, Seccions 4.3.2–4.3.6) ni l'autenticació a nivell de posició (només E14 i E18 xifren l'E6-C), que es completen a continuació.

5.2 Refinament i autenticació de rang amb captures pròpies

Durant el 2026, els dos satèl·lits excèntrics de proves de la constel·lació Galileo, l'E14 (PRN 14) i l'E18 (PRN 18), van xifrar el senyal E6-C i emeten el SAS a temps real; les RECS necessàries per desxifrar-lo, però, de moment només són d'accés privat.

Sobre captures pròpies E1/E6 d'aquests dos satèl·lits —l'E14 (PRN 14, captura nocturna del 20/06/2026) i l'E18 (PRN 18, captura de migdia del 23/06/2026)— s'executa la cadena sencera de SASlib amb tots els matisos del Capítol 4: compensació de la taxa de rang, assistència ACAS i test de rang sense calibratge empíric. Com que l'E14 i l'E18 són satèl·lits d'òrbita excèntrica i sovint manquen dels productes d'efemèrides horaris, el bloc d'efemèrides recorre automàticament al producte diari combinat de l'IGS per obtenir la posició del satèl·lit.¹

¹Per al PRN 14 es fa servir la captura de les 22:34:00 UTC (parell 223400), amb una mesura d'E1-B neta; una altra captura del mateix lot (223335) presenta un E1-B més sorollós i no s'hi inclou.

Correlació i detecció. Les Figures 5.3 i 5.4 mostren els perfils de correlació complets de l'E1-B, l'E6-B i l'E6-C (amb l'ECS desxifrada) per al PRN 14 i el PRN 18 sobre tota la finestra de cerca, cadascun amb un pic únic i net per damunt del soroll (marcat amb ★). La detecció del pic de l'E6-C (que només es forma si la seqüència desxifrada coincideix amb el senyal rebut) és, en si mateixa, l'autenticació de rang. Les mètriques de detecció són àmplies (E6-C: PPSP = 18,6 dB, SNR = 31,0 dB per al PRN 14; PPSP = 14,1 dB, SNR = 26,8 dB per al PRN 18), amb la cerca acotada per l'assistència ACAS (Secció 4.2.10).

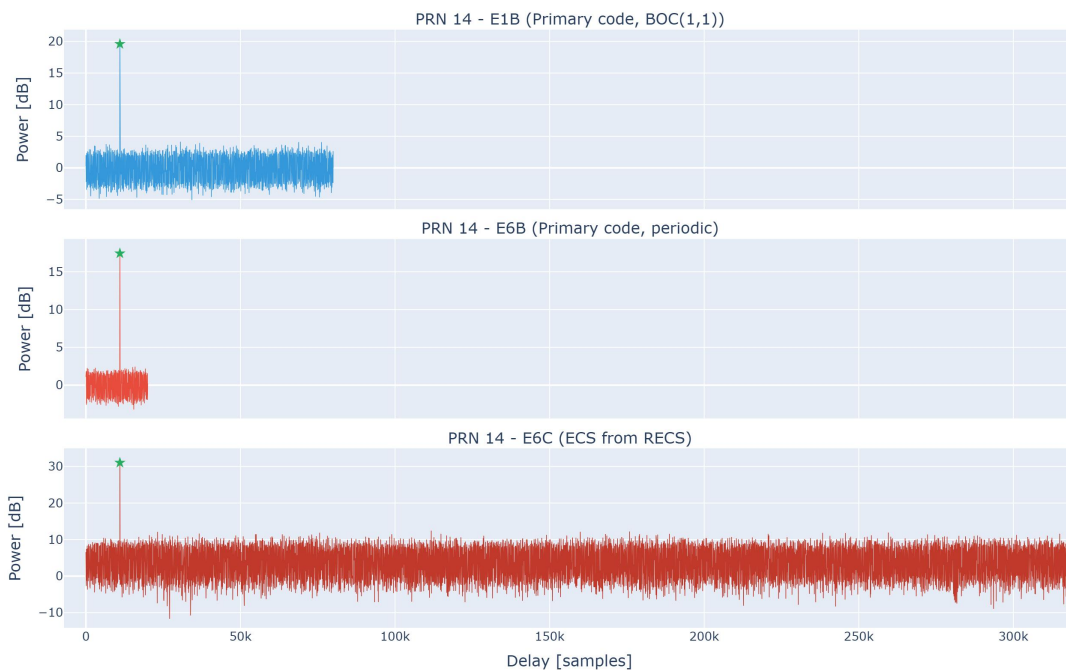


Figura 5.3: Perfils de correlació complets de l'E1-B, l'E6-B i l'E6-C per al PRN 14, cadascun amb el pic detectat (★) molt per damunt del soroll.

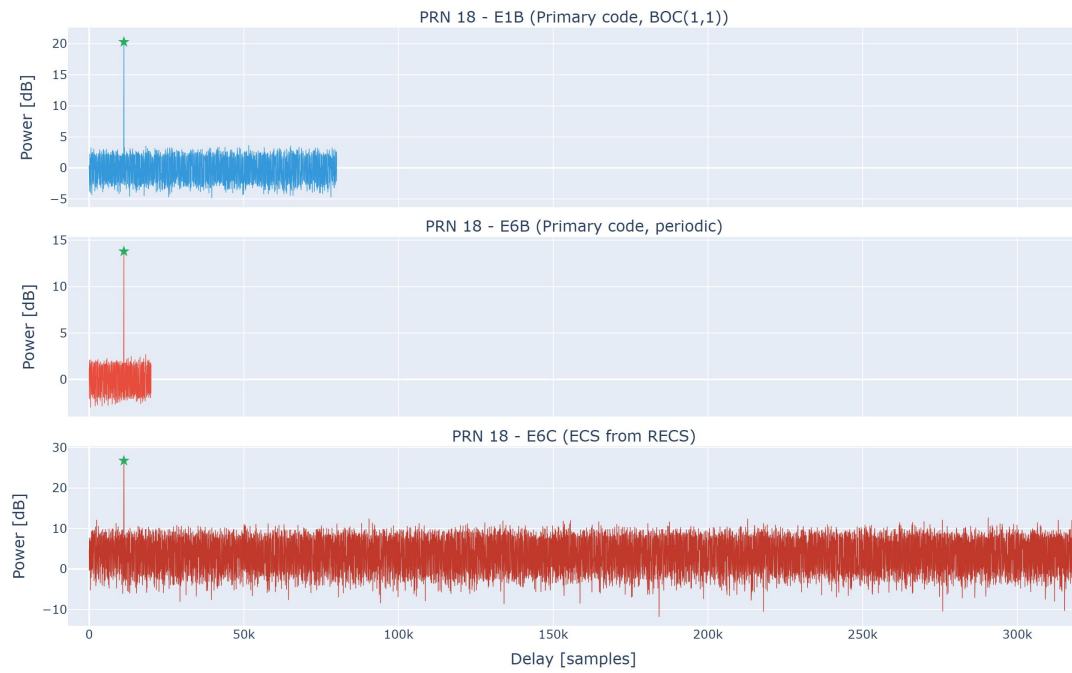


Figura 5.4: El mateix que la Figura 5.3, ara per al PRN 18.

Autenticació de rang. La Figura 5.5 compara el pic de l'E6-C (ECS desxifrada, presa com a referència) amb el de l'E1-B públic. El biaix de codi entre les dues bandes queda per sota del llindar d'autenticació en tots dos satèl·lits, tal com recull la Taula 5.1.

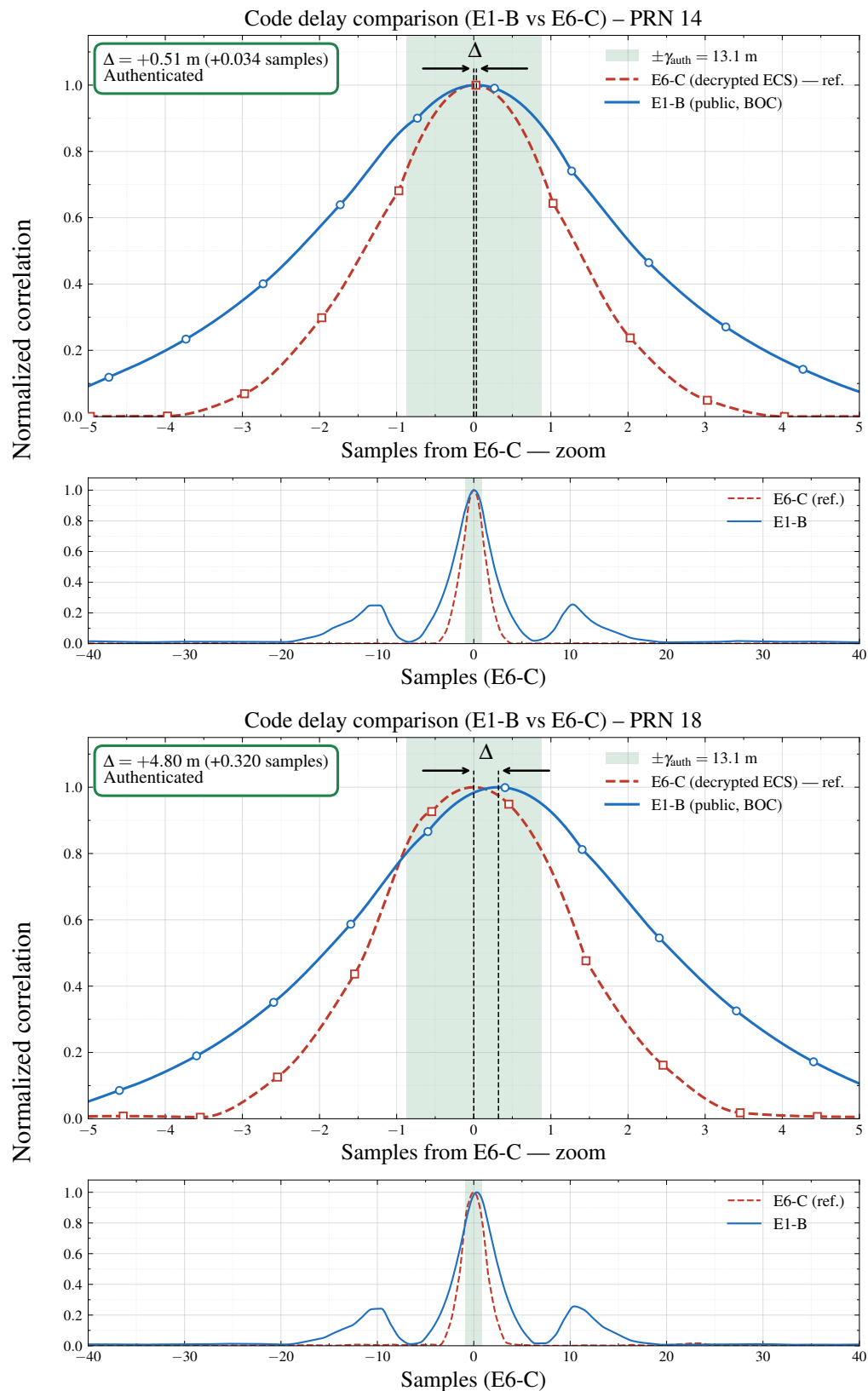


Figura 5.5: Comparació del retard de codi de l'E1-B i l'E6-C, per al PRN 14 (dalt) i el PRN 18 (baix). La franja verda marca la zona autèntica.

Taula 5.1: Autenticació de rang per PRN amb captures pròpies. El biaix de codi E1-E6 mesurat queda per sota del llindar d'autenticació (13,1 m) en tots dos satèl·lits.

PRN	Captura (cond.)	PPSP _{E6C} [dB]	Biaix [m]	Auth.
14	20/06, nit	18,6	+3,09	✓
18	23/06, migdia	14,1	+9,45	✓

En tots dos satèl·lits el biaix mesurat queda per sota del llindar d'autenticació, de manera que autèntiquen sense recórrer al calibratge empíric del biaix (Secció 4.3.6), el mode determinista coherent amb [FH23]. El biaix més gran del PRN 18 és consistent amb la seva baixa elevació (més soroll de mesura) i amb els biaixos de maquinari residuals (BGD, HWB) no compensats explícitament.

5.3 Solució de posició (PVT)

Com que de moment només dos satèl·lits xifren l'E6-C, l'autenticació a nivell de posició (Secció 4.3.7) encara no es pot tancar i queda preparada per a quan n'hi hagi quatre o més; mentrestant, la solució PVT es calcula sobre les mesures de la banda auxiliar i la posició resultant és, per tant, una solució semiautenticada. La Figura 5.6 en mostra un exemple, situat sobre el mapa de la zona del receptor.



Figura 5.6: Solució PVT semiautenticada calculada sobre la banda auxiliar, situada sobre el terrat del Departament d'Enginyeria Electrònica (UAB). El cercle verd marca el radi d'incertesa de la posició estimada.

Per poder donar un barem fiable de la solució cal que es compleixin certes condicions: una geometria de satèl·lits prou bona i una potència de senyal suficient en cadascun dels satèl·lits. Si no s'assoleixen, el barem de l'error creix. A més, cal tenir present que es treballa en posicionament snapshot, sense seguiment continu del senyal: cada solució s'obté d'una única instantània, sense la suavització que aporta el *tracking*. En aquestes condicions s'han arribat a observar errors residuals 3D de l'ordre de 25 a 35 metres.

5.4 Discussió

L'estratègia de validació en dues etapes separa dues preguntes diferents. La primera etapa, sobre el senyal E6-C xifrat real de la campanya de 2025, demostra que el nucli criptogràfic i de correlació del receptor funciona end-to-end: la detecció del pic de l'ECS desxifrada ja és, en si mateixa, una autenticació de rang, perquè aquest pic només es forma si la rèplica generada a partir de la RECS coincideix amb el senyal rebut. La segona etapa, amb captures pròpies E1/E6 dels satèl·lits E14 i E18, trasllada aquesta capacitat a un escenari complet i hi afegeix els matisos deterministes que fan rigorós el test de rang.

El resultat més rellevant és que el biaix de codi mesurat entre l'E1-B i l'E6-C queda per sota del llindar d'autenticació en tots dos satèl·lits sense recórrer al calibratge empíric. Això vol dir

que la cadena decideix l'autenticitat a partir d'un pressupost d'error físicament justificat i no d'un ajust ad hoc. El biaix lleugerament més gran del PRN 18 és coherent amb la seva baixa elevació (més soroll de mesura) i amb els biaixos de maquinari residuals no compensats: el marge respecte al llindar es manté, però es redueix en les condicions menys favorables.

A nivell de posició, la solució és encara semiautenticada i s'obté en mode snapshot, sense seguiment continu del senyal. Aquesta condició explica els errors residuals 3D observats, de l'ordre de 25 a 35 metres en els casos menys favorables: sense la suavització que aporta el *tracking*, la qualitat de cada solució depèn directament de la geometria instantània dels satèl·lits i de la potència rebuda, i el barem de l'error creix de manera apreciable quan aquestes condicions no es compleixen.

Aquests resultats s'han d'emmarcar en les seves limitacions. Que només l'E14 i l'E18 xifrin l'E6-C impedeix encara tancar l'autenticació a nivell de posició (que necessita quatre o més mesures autenticades) i redueix la mida de la mostra, de manera que constitueixen una validació funcional de la cadena i no una caracterització estadística completa en termes de probabilitat de detecció i de falsa alarma (Secció 2.2). El calibratge automàtic del biaix (Secció 4.3.6), tot i no caldre en aquests casos, és intrínsecament empíric i podria emascarar un atac que introduís un biaix lent; aquesta tensió entre comoditat operativa i seguretat és la que motiva la integració de tècniques anti-spoofing, recollida com a treball futur al Capítol 6.

Capítol 6

Conclusions i treball futur

6.1 Conclusions

L'objectiu general d'aquest Treball de Fi de Grau —generar mesures de rang autenticades i un posicionament semiautenticat a partir del senyal SAS de Galileo, dins de la biblioteca de codi obert SASlib i en coordinació amb el TFG complementari d'Enginyeria Informàtica— s'ha assolit: la cadena detecta el pic de la seqüència desxifrada sobre el senyal E6-C rebut, i aquesta detecció és, en si mateixa, l'autenticació de rang.

Convé remarcar el lloc que ocupa aquesta autenticació dins del panorama de la seguretat GNSS. L'OSNMA autentica les dades de navegació, però no impedeix que un atacant retransmeti o retardi el senyal mateix (atacs de *replay* i de *meaconing*) per falsejar el rang i, amb ell, la posició i el temps. El SAS actua precisament en aquesta capa: en lligar l'autenticitat a la correlació amb una seqüència xifrada que l'atacant no pot predir, autentica el senyal i no només el seu contingut. La cadena desenvolupada en aquest treball materialitza aquesta capa de defensa complementària, que tanca un forat que l'autenticació a nivell de dades no pot cobrir per si sola.

Dur aquesta capa de defensa a la pràctica, però, ha estat tan exigent com dissenyar cada bloc per separat. La detecció del pic de l'E6-C és el final d'una seqüència llarga i fortament acoblada —recuperació de la clau TESLA, desxifratge de la RECS, generació de l'ECS, predicció de la posició del satèl·lit i de la finestra de cerca, i correlació—, de manera que un error en qualsevol baula impedeix que el pic es formi, sovint sense cap símptoma que n'assenyali la causa. Aquesta dependència en cadena ha obligat a validar cada bloc de manera aïllada i a recolzar-se en mètriques i senyals de diagnòstic intermedis abans no ha estat possible tancar el processament complet.

Bona part de les dificultats pràctiques han vingut de la sincronització de la plataforma i de les convencions de temps. La captura simultània de l'E1 i l'E6 amb la plataforma SDR exigeix

un alineament temporal acurat entre les dues bandes, i cada fitxer de dades arrossega la seva pròpia referència temporal —la marca de temps del nom, el rellotge intern o l'elecció entre GST i UTC amb el salt de segons intercalars—, una font d'errors recurrent que ha calgut identificar i homogeneïtzar amb cura. El fet de treballar amb instantànies, sense un seguiment continu que doni continuïtat entre èpoques, agreuja aquesta sensibilitat: cada solució s'ha de resoldre de manera autònoma a partir d'una sola captura, sense l'ajut de la història temporal. A més, el posicionament per instantànies no és l'enfocament més habitual (la majoria de receptors es basen en el seguiment continu del senyal), de manera que es disposa de menys referències i d'eines de comparació i que validar cada part del processament resulta més laboriós.

En aquest context, l'estructura modular del receptor (blocs independents connectats per un pipeline configurable) ha estat decisiva, perquè ha permès aïllar i corregir cada problema sense afectar la resta de la cadena i reutilitzar els blocs entre escenaris. Aquesta separació clara de responsabilitats, juntament amb una bona estructura de disseny, és, més enllà dels resultats numèrics, una de les principals lliçons d'enginyeria del treball.

Cal tenir present, també, que el receptor no és autònom: depèn de diverses fonts externes —les efemèrides precises de l'IGS, l'assistència de fase de codi ACAS i, sobretot, les RECS que permeten desxifrar l'E6-C—, de manera que la seva fiabilitat queda lligada a la disponibilitat, la confiança i la vigència d'aquestes entrades. Això vol dir que un desplegament real no és un sistema que es posa en marxa i s'oblida, sinó que demana manteniment continuat: actualitzar i validar els productes d'efemèrides, seguir els canvis de format i de distribució de les RECS (avui encara d'accés privat) i adaptar-se a l'evolució de les convencions i dels serveis dels quals depèn la cadena.

Més enllà de cada bloc, el treball deixa una eina oberta i reproduïble que integra tota la cadena en una sola biblioteca, i que confirma la viabilitat pràctica d'autenticar el rang d'un senyal Galileo a partir de la correlació de la seqüència desxifrada amb una instantània capturada. El fet que la decisió d'autenticitat es basi en un pressupost d'error físic, i no en un ajust arbitrari, en fa una base sòlida per a treballs posteriors de seguretat del posicionament. La seva arquitectura modular i el seu caràcter obert la deixen, a més, oberta a nombroses millores i ampliacions (nous blocs, models o bandes de senyal) i en faciliten la integració amb altres biblioteques de processament GNSS.

La implementació forma part de la biblioteca de codi obert SASlib (llicència EUPL-1.2), disponible públicament a <https://github.com/SPCOMNAV/GalileoSASlib> [TG26a]; els tres blocs de processament de senyal desenvolupats en aquest TFG són *SignalCorrelation*, *SatelliteAuthenticator* i *PVTComputation*, integrats en la cadena completa.

6.2 Línies de treball pel futur

La línia més immediata és la implementació completa i la validació quantitativa de les tècniques anti-spoofing VSS i SQM integrades a SASlib, amb una avaluació enfront d'atacs sintètics superposats que aprofiti la sinergia entre la VSS i el SAS. En paral·lel, cal caracteritzar les prestacions del detector de manera estadística, amb corbes ROC i probabilitat de detecció en funció de la relació senyal-soroll i del temps d'integració, sobre un ventall ampli d'escenaris reals que la mostra actual, limitada a dos satèl·lits, encara no permet. A la validació amb atacs sintètics caldria afegir-hi proves amb spoofing real i, en particular, mesurar l'abast i la robustesa del receptor en una campanya com el Jammertest, on es reproduïen interferències i suplantacions en condicions controlades però realistes. Aquest ventall hauria d'incloure, també, entorns degradats i dinàmics: totes les captures d'aquest treball són estàtiques i en cel obert (terrat), de manera que provar el receptor en entorn urbà i amb multicamí, i amb un receptor en moviment, tancaria el cas d'ús real, sobretot tenint en compte que el multicamí ja és el terme dominant del pressupost d'error.

A mitjà termini, el processament es pot estendre a la banda E5 i a altres components del senyal, i la correcció ionosfèrica NeQuick-G, ja integrada al bloc d'autenticació, es pot portar també al càlcul de PVT i refinar a baixa elevació, on el residu de rang és més gran. En aquesta mateixa direcció, ponderar les mesures segons l'elevació i la relació senyal-soroll hauria de millorar tant la robustesa de l'autenticació com la qualitat de la solució de posició, especialment en les condicions de geometria i potència menys favorables identificades en els resultats. Convindria, també, revisar els paràmetres del bloc d'autenticació de rang per afinar encara més el biaix residual entre l'E1 i l'E6 i, amb ell, estrènyer el llindar de decisió. En la mateixa línia, caracteritzar i compensar de manera explícita els biaixos de maquinari —el retard de grup del satèl·lit (BGD) i el biaix entre les cadenes RF d'E1 i E6 del receptor (HWB), que un experiment dedicat ja permet mesurar— reduiria el residu de rang que avui queda sense corregir, més notable a baixa elevació.

Finalment, en el pla de la implementació, optimitzar en C++ els blocs més costosos (o les seves parts crítiques) acostaria el receptor al funcionament en temps real, més enllà del processament per instantànies. A més llarg termini, la biblioteca s'hauria d'adequar als nous models d'autenticació de senyal que es van definint per a Galileo i ampliar les seves integracions amb altres biblioteques de processament GNSS, de manera que la cadena SAS es pugui combinar amb fluxos de treball ja existents.

6.3 Publicacions derivades del treball

El treball desenvolupat en aquest TFG s'emmarca en l'activitat investigadora del grup SPCOM-NAV i ha donat lloc (o està donant lloc) a diverses publicacions de les quals l'estudiant és coautor:

- **SASlib: An Open Python Library for Galileo Signal Authentication Service**, presentat a l'ESA NAVITEC 2026 [TG26a]. Presenta la biblioteca SASlib (la cadena completa del receptor SAS sobre la qual s'ha construït aquest treball) i n'anuncia la disponibilitat pública.
- **A Galileo SAS Monitoring Station**, en preparació per a l'IEEE NAVICON 2026 (Munic) [TG26b]. Descriu una estació de monitoratge en viu del SAS de Galileo (Figures 6.1 i 6.2): executa la cadena de SASlib de manera contínua sobre tots els PRN visibles i en mostra l'estat de correlació i d'autenticació a temps real.
- **Validating Galileo SAS Range Authentication and Positioning with Live Signal-in-Space**, en preparació per a l'ION GNSS+ 2026 (Orlando) [SM26]. Valida el SAS de Galileo end-to-end (autenticació de rang i posicionament) amb senyal real en viu, a partir del mateix conjunt de dades emprat en aquest treball.

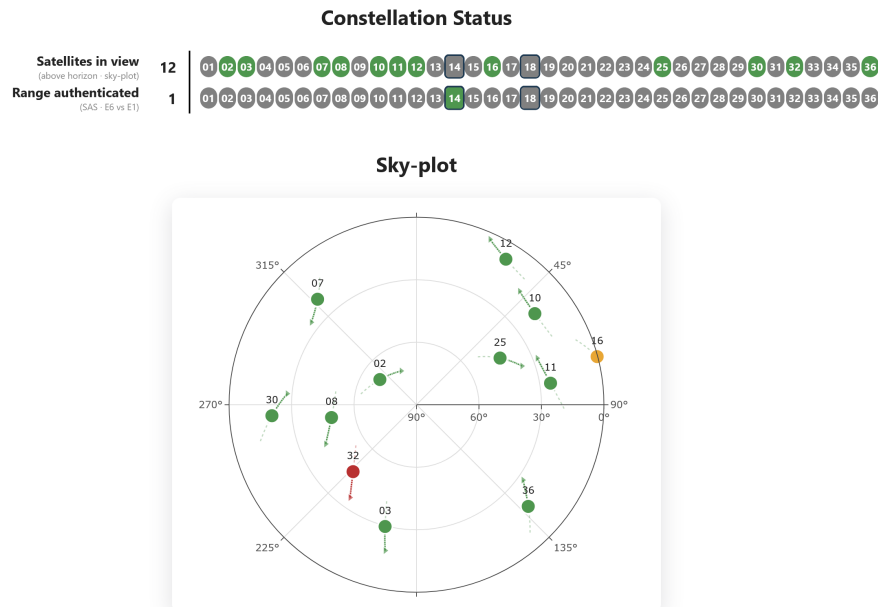


Figura 6.1: Estació de monitoratge del SAS de Galileo (*SAS Monitor*): estat de la constel·lació — satèl·lits a la vista i rang autenticat (SAS, E6 enfront d'E1)— i *sky-plot* amb les posicions i trajectòries dels satèl·lits visibles. Els PRN xifrats (14 i 18) hi apareixen ressaltats i el PRN 14 hi consta com a autenticat.

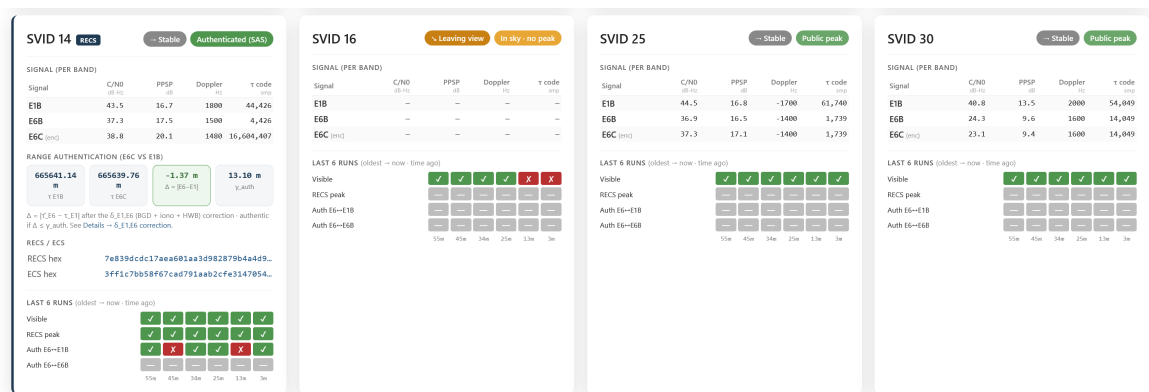


Figura 6.2: Detall de l'estació de monitoratge: targetes per satèl·lit amb les mètriques per banda (E1-B, E6-B, E6-C), el veredictat d'autenticació de rang (E6-C enfront d'E1-B) i l'historial de les darreres execucions. El PRN 14, que emet l'E6-C xifrat, hi apareix com a autenticat (SAS).

Bibliografía

- [All66] D. W. Allan, “Statistics of atomic frequency standards”, *Proceedings of the IEEE*, Vol. 54, nº 2, pags. 221–230, 1966.
- [Bor23] K. Borre, I. Fernández-Hernández, J. A. López-Salcedo, M. Z. H. Bhuiyan, *GNSS Software Receivers*, Cambridge University Press, 2023.
- [Bro16] A. Broumandan, A. Jafarnia-Jahromi, S. Daneshmand, G. Lachapelle, “Overview of spatial processing approaches for GNSS structural interference detection and mitigation”, *Proceedings of the IEEE*, Vol. 104, nº 6, pags. 1246–1257, 2016.
- [Eur16] European Commission, “European GNSS (Galileo) open service: Ionospheric correction algorithm for Galileo single frequency users (NeQuick-G)”, Tech. Rep. Issue 1.2, European Commission, 2016, <https://www.gsc-europa.eu>.
- [Eur23a] European Commission DG DEFIS.C2, “Galileo assisted commercial authentication service (ACAS) specification proposal”, Tech. Rep. Version 1.2, European Commission, 2023.
- [Eur23b] European Union, “Galileo open service signal-in-space interface control document (OS SIS ICD)”, Tech. Rep. Issue 2.1, European Union, 2023.
- [Eur23c] European Union / EUSPA, “Galileo OSNMA signal-in-space interface control document (SIS ICD)”, Tech. Rep. Issue 1.1, European Union Agency for the Space Programme, 2023.
- [Eur24a] European GNSS Service Centre / EUSPA, “Galileo programme: Constellation and orbital parameters”, 2024, walker 24/3/1, 3 orbital planes, 23222 km MEO. <https://www.gsc-europa.eu/galileo/programme>.
- [Eur24b] European Union / EUSPA, “Galileo OSNMA receiver guidelines”, Tech. Rep. Issue 1.3, European Union Agency for the Space Programme, 2024, <https://www.gsc-europa.eu>.
- [Eur25] European GNSS Service Centre, “Galileo OSNMA service”, 2025, <https://www.gsc-europa.eu/galileo/services>.
- [FH15] I. Fernández-Hernández, *Snapshot and Authentication Techniques for Satellite Navigation*, PhD Thesis, Aalborg University, Denmark, 2015.
- [FH16] I. Fernández-Hernández, K. Borre, “Snapshot positioning without initial information”, *GPS Solutions*, Vol. 20, nº 4, pags. 605–616, 2016.

- [FH23] I. Fernandez-Hernandez, *et al.*, “Semiassisted signal authentication for Galileo: Proof of concept and results”, *IEEE Trans. Aerospace and Electronic Systems*, Vol. 59, n^o 4, pags. 4393–4404, 2023.
- [FH24] I. Fernandez-Hernandez, *et al.*, “Galileo signal authentication service (SAS)”, *Proc. ION GNSS+ 2024*, pags. 3292–3307, Baltimore, MD, USA, 2024.
- [FM24] M. G. Fernández-Marín, European Commission JRC, “NeQuickJRC: Python implementation of the NeQuick-G ionospheric model”, 2024, <https://github.com/mgfernand/NeQuickJRC>.
- [GF22] A. Galan-Figueras, I. Fernandez-Hernandez, L. Cucchi, G. Seco-Granados, “OSNMAlib: An open Python library for Galileo OSNMA”, *Proc. ESA NAVITEC 2022*, pags. 1–12, Noordwijk, The Netherlands, 2022.
- [GF25] A. Galan-Figueras, C. Iñiguez, I. Fernandez-Hernandez, S. Pollin, G. Seco-Granados, “Improving OSNMAlib: New formats, features, and monitoring capabilities”, *IEEE J. Indoor and Seamless Positioning and Navigation*, Vol. 3, pags. 117–127, 2025.
- [Gün14] C. Günther, “A survey of spoofing and counter-measures”, *NAVIGATION: Journal of the Institute of Navigation*, Vol. 61, n^o 3, pags. 159–177, 2014.
- [Hum08] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O’Hanlon, P. M. Kintner, “Assessing the spoofing threat: Development of a portable GPS civilian spoofer”, *Proc. ION GNSS 2008*, pags. 2314–2325, Savannah, GA, USA, 2008.
- [Int25] International GNSS Service (IGS), “Multi-GNSS broadcast ephemeris product (BRDC00IGS, daily merged navigation RINEX)”, 2025, distribuït per BKG, <https://igs.bkg.bund.de>.
- [LR05] G. López-Risueño, G. Seco-Granados, A. García, “Evaluation of GPS indoor positioning using real measurements and one-shot software receiver”, *Proc. European Navigation Conf. (ENC-GNSS)*, pags. 1–9, 2005.
- [Nav08] B. Nava, P. Coïsson, S. M. Radicella, “A new version of the NeQuick ionosphere electron density model”, *Journal of Atmospheric and Solar-Terrestrial Physics*, Vol. 70, n^o 15, pags. 1856–1862, 2008.
- [PG24] Andrés Pisco Granda, *Vestigial Signal Search (VSS) and Signal Quality Monitoring (SQM) techniques for GNSS spoofing detection*, Treball de fi de grau, Universitat Autònoma de Barcelona, 2024.
- [Psi16] M. L. Psiaki, T. E. Humphreys, “GNSS spoofing and detection”, *Proceedings of the IEEE*, Vol. 104, n^o 6, pags. 1258–1270, 2016.
- [SG12] G. Seco-Granados, J. A. López-Salcedo, D. Jiménez-Baños, G. López-Risueño, “Challenges in indoor global navigation satellite systems”, *IEEE Signal Processing Magazine*, Vol. 29, n^o 2, pags. 108–131, 2012.
- [SM26] Òscar Sardà-Martín, Rafael Terris-Gallego, *et al.*, “Validating Galileo SAS range authentication and positioning with live signal-in-space”, *Proc. ION GNSS+ 2026*, Orlando, FL, USA, 2026, en preparació.

- [TG22a] Rafael Terris-Gallego, I. Fernandez-Hernandez, J. A. López-Salcedo, G. Seco-Granados, “Guidelines for Galileo ACAS implementation”, *Proc. ICL-GNSS 2022*, Tampere, Finland, 2022.
- [TG22b] Rafael Terris-Gallego, J. A. López-Salcedo, G. Seco-Granados, I. Fernandez-Hernandez, “Operating modes and performance evaluation of Galileo ACAS”, *Proc. ION GNSS+ 2022*, Denver, CO, USA, 2022.
- [TG23a] Rafael Terris-Gallego, J. A. López-Salcedo, G. Seco-Granados, I. Fernandez-Hernandez, “E1-E6 SDR platform based on bladeRF for testing Galileo ACAS”, *Proc. ENC 2023*, Noordwijk, The Netherlands, 2023.
- [TG23b] Rafael Terris-Gallego, J. A. López-Salcedo, G. Seco-Granados, I. Fernandez-Hernandez, “Preliminary evaluation of Galileo ACAS using existing E1-E6 open signals”, *Proc. ION GNSS+ 2023*, pags. 1388–1402, Denver, CO, USA, 2023.
- [TG24a] Rafael Terris-Gallego, *Analysis and Implementation of Anti-Spoofing Detection Methods based on Galileo Signal Authentication Service*, PhD Thesis, Universitat Autònoma de Barcelona, 2024.
- [TG24b] Rafael Terris-Gallego, I. Fernandez-Hernandez, J. A. López-Salcedo, G. Seco-Granados, “Efficient detection of Galileo SAS sequences using E6-B aiding”, *Proc. ENC 2024*, Noordwijk, The Netherlands, 2024.
- [TG25] Rafael Terris-Gallego, J. A. López-Salcedo, G. Seco-Granados, “Testing Galileo SAS with encrypted signal-in-space”, *Proc. ION GNSS+ 2025*, Baltimore, MD, USA, 2025.
- [TG26a] Rafael Terris-Gallego, Òscar Sardà-Martín, E. Takiguchi-Medina, A. Galan-Figueras, J. A. López-Salcedo, G. Seco-Granados, I. Fernandez-Hernandez, “SASlib: An open Python library for Galileo signal authentication service”, *Proc. ESA NAVITEC 2026*, Noordwijk, The Netherlands, 2026, preprint / en revisió.
- [TG26b] Rafael Terris-Gallego, Òscar Sardà-Martín, *et al.*, “A Galileo SAS monitoring station”, *Proc. IEEE NAVICON 2026*, Munich, Germany, 2026, en preparació.
- [Wes18] K. D. Wesson, J. N. Gross, T. E. Humphreys, B. L. Evans, “GNSS signal authentication via power and distortion monitoring”, *IEEE Trans. Aerospace and Electronic Systems*, Vol. 54, n^o 2, pags. 739–754, 2018.
- [Win24] J. Winkel, *et al.*, “Combining Galileo’s assisted commercial authentication service (ACAS) with vestigial signal search for good protection”, *Proc. ION GNSS+ 2024*, 2024.

Apèndix A

Material addicional

Aquest apèndix recull material complementari de suport a la memòria: la referència completa dels paràmetres de configuració dels blocs desenvolupats o configurats en aquest TFG (Secció A.1) i un exemple del *pipeline* d'execució amb què s'han obtingut els resultats (Secció A.2).

A.1 Paràmetres de configuració dels blocs

Tot el comportament del receptor es controla amb fitxers de configuració en JSON, sense modificar el codi: cada bloc declara els seus paràmetres en un esquema i el motor d'execució en construeix les entrades a partir d'un fitxer global del *pipeline*. Les Taules A.1 a A.4 recullen els paràmetres dels quatre blocs implicats en aquest treball —*ConfigInit* (arrencada i selecció del cas) i els tres blocs de processament de senyal *SignalCorrelation*, *SatelliteAuthenticator* i *PVTComputation*— amb una breu descripció de la seva funció.

Taula A.1: Paràmetres del bloc *ConfigInit* (arrencada i selecció del cas).

Paràmetre	Descripció
<code>gst_start_time_sec</code>	Instant d'inici de l'autenticació, en temps Galileo (GST), en segons.
<code>auth_duration_sec</code>	Durada de la finestra d'autenticació (s).
<code>auth_periodicity_sec</code>	Interval de revelació de claus TESLA i de publicació de les RECS (30 s).
<code>scheduled_time_doy</code>	Instant programat de la captura (dia de l'any i hora UTC).
<code>svid_to_search</code>	PRN del satèl·lit que es vol processar.
<code>svid_encrypted</code>	PRN del satèl·lit que emet l'E6-C xifrat.
<code>auxiliary_mode</code>	Banda auxiliar de referència per al test de rang (p. ex. E1B).
<code>recs_length</code>	Longitud de la seqüència RECS/ECS (ms).
<code>recs_kdi</code>	Índex de derivació de clau (KDI) de la RECS.
<code>calibration_active</code>	Activa el calibratge empíric del biaix del receptor.
<code>rf_input_from_file</code>	Carrega les instantànies des de fitxer (<code>rf_input_path_e1/e6</code>) en lloc de comandar la captura SDR.
<code>recs_file_enabled</code>	Usa les RECS locals de <code>recs_directory</code> en lloc de descarregar-les.
<code>tesla_file_enabled</code>	Usa les claus TESLA locals de <code>tesla_file_path</code> .
<code>bgd_file_enabled</code>	Usa el fitxer BGD local de <code>bgd_file_path</code> .
<code>execution_name</code>	Nom de l'execució (carpeta de resultats).

Taula A.2: Paràmetres del bloc *SignalCorrelation* (correlació i detecció del pic).

Paràmetre	Descripció
<code>sample_rate_hz</code>	Freqüència de mostreig de les instantànies (20 MHz).
<code>start_sample</code>	Primera mostra del retall de la instantània que es processa.
<code>num_samples</code>	Nombre de mostres del retall; dimensiona la finestra i el temps d'integració.
<code>nc_coherent_e6 / ni_periods_e6</code>	Períodes coherents N_c i blocs no coherents N_i de l'E6.
<code>nc_coherent_aux / ni_periods_aux</code>	N_c i N_i de la banda auxiliar (E1).
<code>doppler_min_hz / doppler_max_hz</code>	Marges de la cerca de Doppler aproximada.
<code>doppler_step_hz</code>	Pas de la graella de Doppler de baixa resolució.
<code>fine_doppler_search</code>	Activa la cerca fina de Doppler al voltant del màxim.
<code>fine_doppler_range_hz</code>	Marge de la cerca fina de Doppler.
<code>correct_code_doppler</code>	Compensa el Doppler de codi (<i>smear</i>) durant la integració no coherent.
<code>correct_range_rate</code>	Corregeix la deriva de rang (<i>range-rate</i>) entre èpoques de mesura.
<code>pdi_method / exp_n_coh</code>	Mètode d'integració post-detecció (NPDI) i el seu exponent.
<code>interpolation_mode</code>	Mètode d'interpolació sub-mostra del pic (paràbola de 3 punts).
<code>ppsp_exclusion_chips</code>	Zona d'exclusió, al voltant del pic, per cercar el segon màxim del PPSP (<i>chips</i>).
<code>save_all_cafs</code>	Desa totes les CAF (diagnòstic).

Taula A.3: Paràmetres del bloc *SatelliteAuthenticator* (test d'autenticació de rang).

Paràmetre	Descripció
<code>auth_reference_signal</code>	Banda de referència per al test (AUTO/E1B/E6B).
<code>kappa</code>	Factor de confiança κ del llindar ($\gamma = \kappa \sigma$).
<code>sigma_auth_m</code>	Sigma d'autenticació imposada manualment (buit = calculada del pressupost).
<code>auto_calibrate_offset</code>	Activa l'autocalibratge del biaix del receptor.
<code>receiver_offset_samples</code>	Offset del receptor imposat manualment (mostres).
<code>iono_correction</code>	Mètode de correcció ionosfèrica (nequick).
<code>iono_gal_coeffs</code>	Coefficients ionosfèrics de Galileo (a_{i0}, a_{i1}, a_{i2}) per a NeQuick-G.
<code>iono_e1_delay_m</code>	Retard ionosfèric E1 imposat manualment (m).
<code>bgd_e1_e6_m</code>	Retard de grup de difusió E1–E6 (m).
<code>receiver_altitude_m</code>	Altitud del receptor (m), per a la geometria ionosfèrica.
<code>min_snr_db / min_ppsp_db</code>	Portes de qualitat (SNR, PPSP) per acceptar la mesura.
<code>sigma_hwbrx_m /</code> <code>sigma_bgd_m</code>	Components d'error: biaix de maquinari del receptor (HWB) i BGD.
<code>sigma_iono_e1_m</code>	Component d'error: residu ionosfèric a E1.
<code>sigma_mp_e1_m /</code> <code>sigma_mp_e6_m</code>	Components d'error: multicamí a E1 i E6.
<code>sigma_noise_e1_m /</code> <code>sigma_noise_e6_m</code>	Components d'error: soroll tèrmic a E1 i E6.
<code>generate_plots /</code> <code>save_results</code>	Genera gràfiques i desa els resultats.

Taula A.4: Paràmetres del bloc *PVTComputation* (solució de posició).

Paràmetre	Descripció
pvt_algorithm	Algorisme de resolució (<code>least_squares</code>).
min_satellites	Nombre mínim de satèl·lits per resoldre la PVT (4).
use_authenticated_only	Usa només les mesures autenticades.
min_elevation_deg	Màscara d'elevació mínima.
weight_by_cn0 / weight_by_elevation	Ponderació de les mesures per C/N ₀ o per elevació.
min_ppsp_db / min_cn0_dbhz	Portes de qualitat (PPSP, C/N ₀) per admetre mesures al PVT.
reference_latitude / longitude / altitude	Posició de referència coneguda, per a la validació creuada.

A.2 Exemple de pipeline d'execució

Les figures de resultats del Capítol 5 s'han generat amb captures reals E1/E6 dels satèl·lits xifrats. Aquest conjunt de dades es publicarà properament però, de moment, encara no és d'accés públic —igual que les RECS necessàries per desxifrar l'E6-C (Secció 3.1.4). A tall d'exemple reproduïble, el Llistat A.1 reproduïx la configuració completa del *pipeline* (tots els blocs) amb què es va autenticar el PRN 18 (captura del 23/06/2026, `dataset230626`); se n'han ofuscat les credencials i s'han abreujat les rutes als fitxers.

```
1 {
2   "metadata": {
3     "execution_id": "dataset230626_sat18_fast",
4     "version": "1.0"
5   },
6   "module_configs": {
7     "ConfigInit": {
8       "gst_start_time_sec": 846937156.0,
9       "auth_periodicity_sec": 30,
10      "auth_duration_sec": 5.0,
11      "scheduled_time_doy": "174 12:19:19",
12      "auxiliary_mode": "E1B",
13      "svid_to_search": "18",
14      "svid_encrypted": "18",
15      "recs_length": 16,
16      "recs_kdi": 0,
17      "calibration_active": false,
18      "bgd_file_enabled": false,
19      "tesla_file_enabled": true,
```



```

20     "recs_file_enabled": true,
21     "rf_input_from_file": true,
22     "recs_directory": "data/dataset230626/RECS/parsed_rcs",
23     "tesla_file_path": "data/dataset230626/tesla_keys/converted.json",
24     "rf_input_path_e1": "data/dataset230626/snapshots/0756_20260623_121858Z_
        ..._E1_s_5s_opensky.bin",
25     "rf_input_path_e6": "data/dataset230626/snapshots/0755_20260623_121858Z_
        ..._E6_s_5s_opensky.bin",
26     "execution_name": "dataset230626_sat18"
27 },
28 "TimeReferenceSynchronizer": {
29     "selected_ntp_server": "time.google.com",
30     "query_timeout_sec": 5.0,
31     "retry_count": 3
32 },
33 "AlmanacManagement": {
34     "almanac_source": "gsc_europa",
35     "almanac_format": "xml",
36     "use_current_time": false,
37     "target_datetime": "2026-06-23T12:19:19Z",
38     "save_almanac_file": true
39 },
40 "UncertaintyModule": {
41     "enabled": true,
42     "satellite_clock_uncertainty_ms": 0.05,
43     "receiver_clock_uncertainty_ms": 0.1,
44     "propagation_uncertainty_ms": 40.0
45 },
46 "SnapshotRecording": {
47     "manual_mode": true,
48     "manual_snapshot_path": "data/dataset230626/snapshots/0755
        _20260623_121858Z_..._E6_s_5s_opensky.bin",
49     "api_base_url": "https://<sdr-platform>",
50     "api_username": "<user>",
51     "api_password": "*****",
52     "frequency_e6": 1278750000,
53     "frequency_e1": 1575420000,
54     "sample_rate": 20000000,
55     "bandwidth": 10000000,
56     "gain": 60,
57     "duration_seconds": 5,
58     "record_now": false,
59     "set_id": "a1",
60     "info_tag": "dataset230626"
61 },
62 "BGDandRECSdownloader": {
63     "recs_provider": "GSCX",

```

```

64     "recs_interface_version": "01",
65     "recs_file_version": "01",
66     "recs_tstart": "174 12:19:00",
67     "recs_duration_sec": 60,
68     "recs_rtba_deciseconds": 10,
69     "recs_svids": "18",
70     "recs_kdi": 0,
71     "recs_rand": 0,
72     "recs_nchip": 4,
73     "ssh_enabled": false,
74     "ssh_host": "<host>",
75     "ssh_port": 22,
76     "ssh_username": "<user>",
77     "online_server_url": "https://<host>:<port>"
78 },
79 "BGDandRECSparser": {
80     "recs_files": [
81         "data/dataset230626/RECS/01_261741218000_000060_00010_18_0_0_4_01.bin",
82         "data/dataset230626/RECS/01_261741219000_000060_00010_18_0_0_4_01.bin"
83     ],
84     "bgd_files": [],
85     "recs_directory": "data/dataset230626/RECS",
86     "output_directory": "data/dataset230626/RECS/parsed_rcs_pipeline"
87 },
88 "TESLAkeyManagement": {
89     "manual_mode": true,
90     "osnma_url": "https://osnmalib.eu/septentrio/subframe_json",
91     "filter_enabled": false,
92     "export_format": "json"
93 },
94 "RECSDecryption": {
95     "prefer_manual_key": false,
96     "prn_encrypted_list": "18",
97     "recs_kdi": 0,
98     "target_epoch_override": 846937159,
99     "tesla_json_path": "data/dataset230626/tesla_keys/converted.json",
100    "recs_directory": "data/dataset230626/RECS/parsed_rcs",
101    "window_before_sec": 60.0,
102    "window_after_sec": 60.0,
103    "use_next_key_if_needed": true,
104    "include_padding": false,
105    "save_ecs": true,
106    "output_basename": "ecs_dataset230626_sat18"
107 },
108 "SignalCorrelation": {
109     "sample_rate_hz": 20000000.0,

```

```

110     "start_sample": 60790000,
111     "num_samples": 1800000,
112     "nc_coherent_e6": 1, "ni_periods_e6": 40,
113     "nc_coherent_aux": 1, "ni_periods_aux": 20,
114     "doppler_min_hz": 4500.0, "doppler_max_hz": 5900.0,
115     "doppler_step_hz": 50.0,
116     "fine_doppler_search": true, "fine_doppler_range_hz": 50.0,
117     "correct_code_doppler": true, "correct_range_rate": true,
118     "pdi_method": "NPDI", "exp_n_coh": 2.0,
119     "save_all_cafs": false,
120     "interpolation_mode": "quadratic-polynomial-3-points",
121     "ppsp_exclusion_chips": 50
122 },
123 "EphemeridesManagement": {
124     "ephemerides_source": "esa_gssc",
125     "ephemerides_type": "broadcast",
126     "precise_product_type": "rapid",
127     "use_current_time": false,
128     "target_datetime": "2026-06-23T12:19:19Z",
129     "prn_filter": "18",
130     "save_ephemerides_file": true
131 },
132 "SatelliteAuthenticator": {
133     "kappa": 3,
134     "sigma_auth_m": "",
135     "auth_reference_signal": "AUTO",
136     "auto_calibrate_offset": false,
137     "receiver_offset_samples": 0,
138     "bgd_e1_e6_m": 0,
139     "iono_e1_delay_m": 0,
140     "iono_correction": "nequick",
141     "receiver_altitude_m": 146.0,
142     "iono_gal_coeffs": "120.50,0.56641,0.022064",
143     "min_snr_db": 10, "min_ppsp_db": 5,
144     "sigma_hwbrx_m": 0, "sigma_bgd_m": 0,
145     "sigma_iono_e1_m": 3.5,
146     "sigma_mp_e1_m": 3, "sigma_mp_e6_m": 0.6,
147     "sigma_noise_e1_m": 0.4, "sigma_noise_e6_m": 2.5,
148     "generate_plots": true, "save_results": true,
149     "output_directory": "results/authentication"
150 },
151 "PVTComputation": {
152     "pvt_algorithm": "least_squares",
153     "min_satellites": 4,
154     "use_authenticated_only": false,
155     "min_elevation_deg": 5.0,
156     "weight_by_cn0": false, "weight_by_elevation": false,

```

```
157         "min_ppsp_db": 3.0, "min_cn0_dbhz": 38.0,  
158         "reference_latitude": 41.5007,  
159         "reference_longitude": 2.1136,  
160         "reference_altitude": 146.0  
161     }  
162 }  
163 }
```

Listing A.1: Configuració completa del *pipeline* per al PRN 18 del dataset230626.

Amb aquesta configuració el receptor mesura el retard de codi de l'E6-C (amb l'ECS desxifrada), de l'E6-B i de l'E1-B sobre la mateixa finestra, i el bloc d'autenticació contrasta el biaix $E1-B \leftrightarrow E6-C$ amb el llindar; per al PRN 18 el veredicté és autèntic (vegeu el Capítol 5).