Funded by the European Union

FUNTIMES I and II – Signals Evolution

Future Navigation and Timing Evolved Signals

2nd Workshop on Horizon 2020 EGNSS Mission And Services

16 February 2022

AIRBUS ENAC LINKS UAB Universitat Autònoma de Barcelona Universität der Bundeswehr München

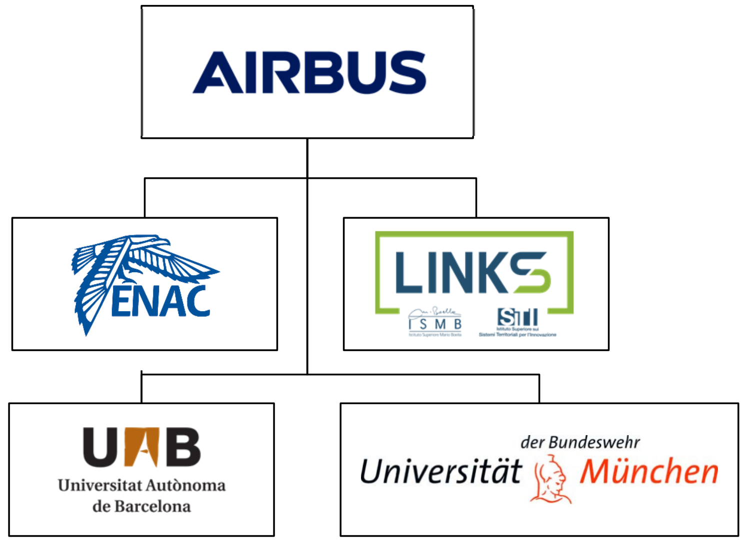
Agenda

- Project overview, objectives, relation to Galileo program
- Starting point:
  - Signal user requirements survey
  - Considered signal design aspects → allocation of tasks / input to G1G & G2G
- Illustration of technical work
- Conclusions

Project Overview (1)

- FUNTIMES I:
  - Consortium:
    - Airbus Defence and Space (Germany, Prime),
    - Ecole Nationale de l'Aviation Civile (France)
    - Istituto Superiore Mario Boella (Italy) (now Fondazione LINKS)
  - Term of contract: 2016 – 2018,   Budget: 600 k€

- FUNTIMES II:
  - Consortium:
    - Airbus Defence and Space (Germany, Prime),
    - Ecole Nationale de l'Aviation Civile (France)
    - Fondazione LINKS (Italy)
    - Universitat Autònoma de Barcelona (Spain)
    - Universität der Bundeswehr München (Germany)
  - Term of contract: 2019 – 2021,   Budget: 600 k€



Project Overview (2)

- Objectives
  - Considering the long process required for introducing new signals and features in a system that is already deployed and in its exploitation phase, there is a clear need for early R&D activities to investigate potential evolutions and new concepts to improve the Galileo signals and services in the short, medium and long term:

    ➔ The FUNTIMES studies aimed at supporting the definition, design and implementation of the future generation of Galileo signals taking into account user feedback, anticipated future user requirements and technology developments

FUNTIMES Project Relation to Galileo Program

- During active working phase, both projects provided inputs to
  - EC Working Group CSI (Compatibility, Signals and Interoperability)
  - EC Working Group EE (EGNSS Evolution)
  - ESA system design

Signal User Requirements Survey

- Starting point in FUNTIMES I
- Two step approach for deriving future needs and resulting evolution of the Galileo signals
  - Analysis of available literature / Lessons learnt from Galileo and GPS
  - Discussion/consultation with representative organizations and or working groups

- Main findings for desired improvements
  - Improved resistance to RFI / Ability to generate robust carrier phase measurements
  - Improved TTFF (in warm or cold start) and acquisition sensitivity
  - Robustness against multipath and NLOS situations
  - Provision of an authentication service (data and pseudo-range)
  - Reliability of the measurements
  - Compatibility/interoperability of open services from multiple GNSS
  - Navigation message: - reliable delivery of key parameters in challenging environments
    - delivery of precise orbit, clock and bias data (e.g. for PPP)
    - provision of an alert/emergency service

UNCLASSIFIED

Considered Signal Design Aspects (1)

- FT I
  - Signal user requirements survey — ENAC
  - Advanced multiplexing techniques — Airbus
  - Improved Signal Acquisition and Authentication — Airbus, ENAC
  - Application of Reed-Solomon codes for improved I/NAV message reception — Airbus
  - Spreading code authentication techniques — ISMB (-> LINKS)
  - Use of CSK and LDPC codes — ENAC
- FT II
  - User segment technology trends — UAB, UFAF
  - Advanced solutions for authentication (cont'd) — LINKS
  - Use of CSK and LDPC codes (cont'd) — ENAC
  - Meta signal processing — UFAF, Airbus
  - Acquisition aiding signal approaches using low bandwidth signal and partial correlation — Airbus, ENAC

Considered Signal Design Aspects (2)

- FT I
  - Signal user requirements survey
  - Advanced multiplexing techniques => under consideration for G2G program
  - Improved Signal Acquisition and Authentication
  - Application of Reed-Solomon codes for improved I/NAV message reception => realized in G1G program
  - Spreading code authentication techniques
  - Use of CSK and LDPC codes
- FT II
  - User segment technology trends => used for G1/2G program
  - Advanced solutions for authentication (cont'd) => promising candidate for G2G program
  - Use of CSK and LDPC codes (cont'd) => under consideration for G2G program
  - Meta signal processing => under consideration for G2G program
  - Acquisition aiding signal approaches using low bandwidth signal and partial correlation => under consideration for G2G program

Advanced Multiplexing Techniques

- Interest on advanced multiplexing methods is triggered by need for new signal components
  → Analysis of modified POCET (Phase-Optimized Constant-Envelope Transmission)

- Principle: determine time series of phases of combined signal for each combination of input signal states by minimizing an optimization function
  → generation of a look-up table (LUT)

	Index	1	2		$\mathrm{B} = 2^{\mathrm{N}}$	
Signal	s_1	1	1	$\ldots$	-1	$\mathbf{b}_1 = \{1,1,\ldots,-1,-1\}$
	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
	s_N	1	-1	$\ldots$	-1	$\mathbf{b}_N$
		Phase				
Time	$[0, T_c/M)$	$\theta_{1,1}$	$\theta_{1,2}$	$\ldots$	$\theta_{1,2^N}$	
	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	
	$[(M-1)T_c/M, T_c)$	$\theta_{M,1}$	$\theta_{M,2}$	$\ldots$	$\theta_{M,2^N}$	

$$\boxed{B = M \cdot 2^N}$$

Advanced Multiplexing Techniques

- Several signal combinations considered for proof of feasibility
  - 2 MSK signals having the same or different carrier frequencies (*center freq. 0 or* ($-f_C$, $+f_C$))
  - 3 MSK signals having the same or different carrier frequencies (*center freq. 0 or* ($-f_C$, *0*, $+f_C$))
  - 1 binary signal (e.g. BPSK) and 2 MSK signals with different carrier frequencies (*center freq.* $-f_C$, *0*, $+f_C$)
  - 2 binary signals (*center freq. 0*) and 2 MSK signals with different carrier frequencies ($-f_C$, $+f_C$)

- Conclusion
  - Rules for required look-up table for signal generation could be identified
  - However, resulting efficiency (= usable total power) is only between 70% and 80%
    (except for 2 MSK at center freq. 0: efficiency = ≈90%)

Improved Signal Acquisition and Authentication

- Identified requested properties based on user community inputs
  - A lower Time To First Fix
  - A lower complexity of the acquisition process
  - An authentication service with short Time-To-Authentication

- Approaches
  - Separate signal components for each „need“ based on BOC(m,n) or BPSK(1) with/without carrier offset

  - Multi-purpose time-division-multiplex (TDM) component with CSK modulation

Separate signal components for each Purpose

- Taking into account
  - Ranging performance (acquisition, tracking, multipath)
  - Compatibility with other signals in E1
  - Multiplexing efficiency (with different options considered for the multiplexing technique)
  - Backward compatibility

- A promising signal design option was identified comprising two additional components
  - Low complexity Acquisition and Time-To-First-Fix-Data (E1-D)
  - Security Code Authentication (E1-E)

E1 Signal Component	Correlation Loss [dB]	Power sharing [%]
E1-A	-2.64	54.47
E1-B	-9.61	10.95
E1-C	-9.19	12.05
E1-D	-9.19	12.05
E1-E	-19.58	1.10
All components		**90.62**

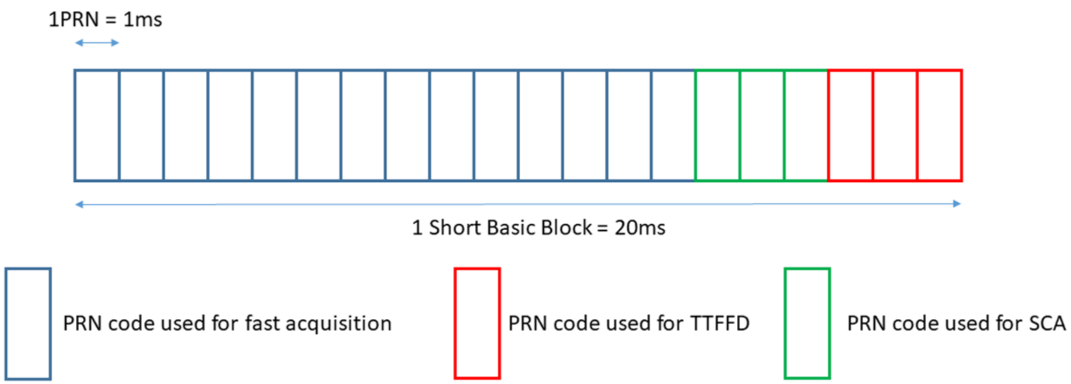
  - All components are multiplexed by a modified interplex scheme

Signal	f_0 [MHz]	Component	Spreading Modulation	
E1	1575.42	A	BOCc(15,2.5)	
		B	BOC(1,1)	
		C	CBOC(6,1,1/11-)	
		D	BOCs(1,1)	BOCs(2,1)
		E	BOC(6,1)	

Multi-Purpose TDM component with CSK modulation

- Motivation
  - Low complexity Acquisition, Security Code Authentication (SCA), Time-To-First-Fix-Data (TFFD), Non-coherent processing of GNSS Signal
  - Compatibility with other signals in E1
  - Multiplexing efficiency (with different options considered for the multiplexing technique)
  - Backward compatibility

- Time Division Multiplexing (TDM) at 1ms PRN code level:
  - each 1ms PRN code is associated to a different functionality
  - continuous flow of short basic blocks of 20ms, several basic blocks generate an advance block of 2 or 3s.
  - (some) PRN codes are CSK modulated to increased the data rate and to allow acquisition



Reed-Solomon Codes for Improvement of I/NAV Message Reception

- Analysis of time-to-first-fix-data (TTFFD) reduction (mainly determined by CED extraction)
  - through the transmission of Reed-Solomon encoded CED words
  - in so far reserved time slots
  - exploiting the erasure correction capability

  - assuming an AWGN channel
  - or a channel model emulating urban propagation

	$TTFFD_{95\%}$ [s]		
	AWGN High C/N_0	2-state Urban v = 50 km/h	2-state Urban v = 5 km/h
I/NAV Baseline	31.6	49.0	54.0
I/NAV LDPC	31.6	40.0	44.0
I/NAV RS-CED	21.7	26.0	28.0

T0 [s]	Page Type	First-Fix-Data
1	2	CED (2/4)
3	4	CED (4/4)
5	6	
7	7 or 9	
9	8 or 10	
11	19	RS-CED
13	20	RS-CED
15	16	RedCED
17	0	Spare
19	0	Spare
21	1	CED (1/4)
23	3	CED (3/4)
25	5	Health Flags
27	16	RedCED
29	0	Spare

User Segment Technology Report

Context, tasks and results

- Comprehensive perspective of current and future (+ 20 years) receiver technologies and techniques

- User Technology Report (USTR): GNSS receiver evolution
  (Reference: H2020-FUNX2-TN-ADSO-1000530038, v3, 04.12.2020)
  1. **Core technology evolution**: Basic components (e.g., antenna, RF-FE, CPU, Memory,…)
  2. **Receiver technology evolution**: Architecture, technology and techniques. Four main trends are identified
     a) Cloud-Based solutions
     b) Multi-Antenna solutions
     c) Hybrid solutions
     d) Snapshot solutions
  3. **Market segment mapping**: Overview of expected level of maturity, adoption and benefits of considered solutions on each market segment

User Segment Technology Report

Conclusions

- ▶ Mapping between solutions and market segments (GSA user technology report)

		FUNTIMES-2 USTR			
		Cloud-Based	Multi-Antenna	Hybrid	Snapshot
GSA User Technology Report	MM segment Low-Power High-Accuracy	✓	✗	~	✓
	SCA segment Integrity Robustness	~	✓	✓	✗
	Professional segment High-Accuracy Integrity	✗	✓	✓	✓

Advanced Authentication Solution

Main challenge: Improve the Galileo OS reliability

- **FUNTIMES I** → focused on the **signal aspects**

  Study and design of a *GNSS authentication solution*, by considering the **achievable performance**, the **overall costs** related to the implementation, and the **robustness** against specific spoofing attacks

- **FUNTIMES II** → focused on the **receiver**

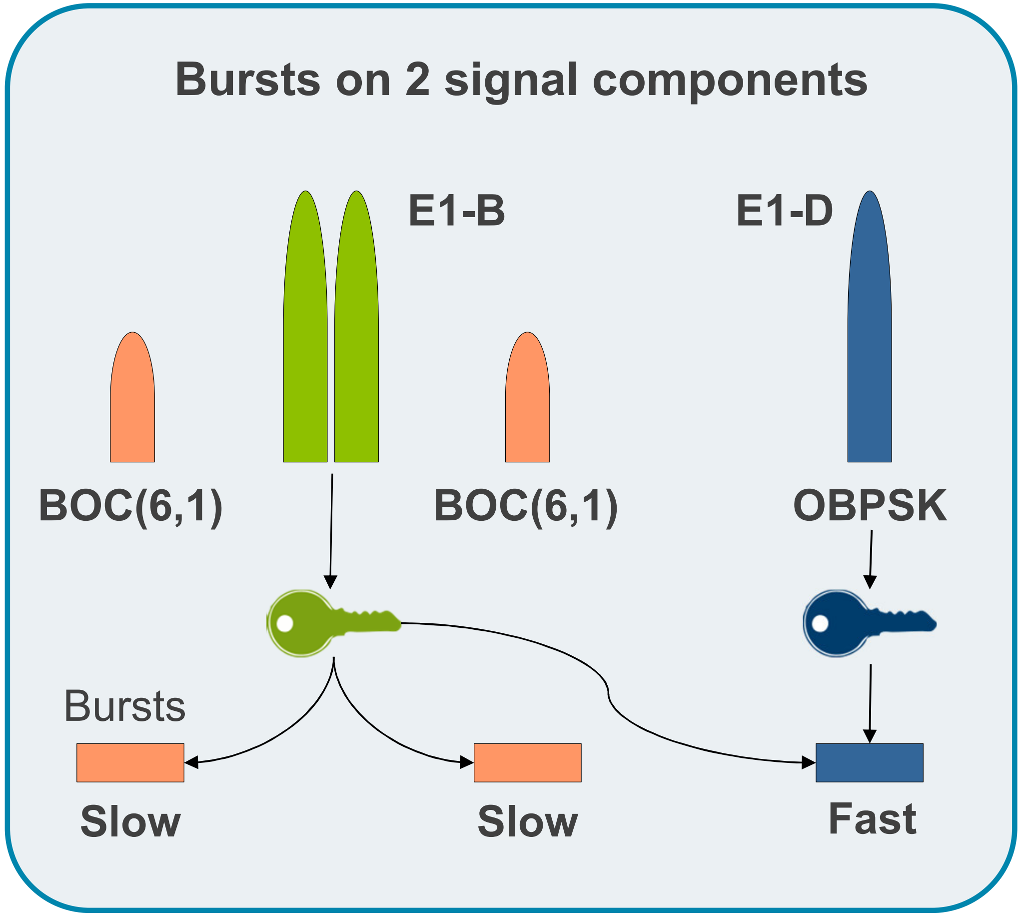
  Study and verification of strategies to be implemented in a receiver, able to **jointly** verify different **authentication solutions**

FUNTIMES I – SNAP concept

- **SNAP** (Spreading code and Navigation data based Authentication Proposal) is a *two-steps* authentication concept for the authentication of **navigation data** and **spreading code chips**
  (starting point for development of currently considered scheme for G2G)

- Designed to be compatible with Galileo E1 OS signal evolutions, exploiting the **OSNMA**

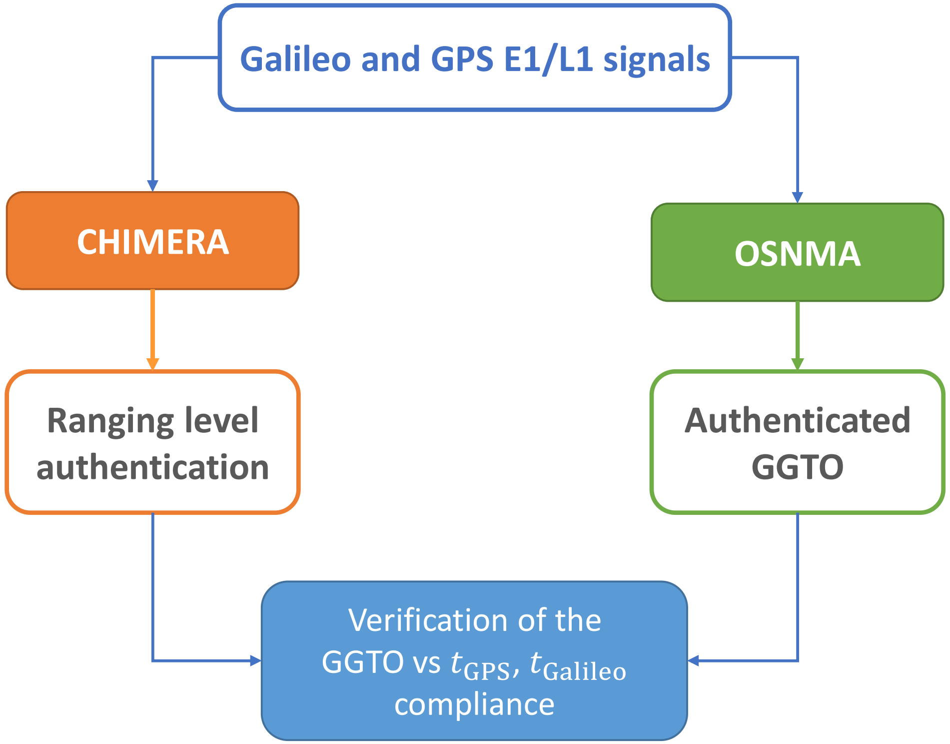
- Performance assessed under different families of spoofing attacks



Motella, Beatrice, Margaria, Davide, Paonni, Matteo, "SNAP: An Authentication Concept for the Galileo Open Service," *2018 IEEE/ION Position, Location and Navigation Symposium (PLANS)*, Monterey, CA, April 2018, pp. 967-97.

FUNTIMES II – Joint Chimera/OSNMA scheme

- The **OSNMA** by itself is not able to authenticate the **ranging signal**, but suitable strategies might go in this direction
- The **Joint scheme** exploits specific characteristics of *both authentication techniques*
- High performance, proved by a wide bench of tests, considering different types of spoofing attack and user conditions



B. Motella, M. Nicola and S. Damy, "Enhanced GNSS Authentication Based on the Joint CHIMERA/OSNMA Scheme," in IEEE Access, vol. 9, pp. 121570-121582, 2021, doi: 10.1109/ACCESS.2021.3107871.

PRN code for partial correlations

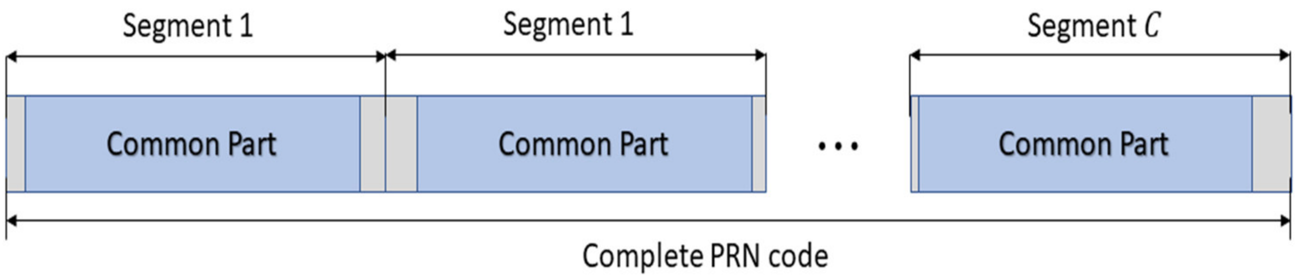
Motivation:

- Low complexity: Low number of operations
- Sensitivity: Minimum C/N_0 required to acquire the signal must be as low as possible.
- Low cross-correlation isolation: To allow acquisition of high-power signals in the presence of low-power signals.
- Flexibility: To allow different acquisition methods to adapt to different situations and/or targeted users.

PRN code for partial correlations

Proposal / Approach:

- Each PRN code is divided in C segments of ~W bits and
- Each PRN segment corresponds to the partial correlation length:
  - Common part to all the segments (in blue) / Variable part unique to the segment (in grey)
- Common part position inside the segment is modified from segment to segment.



Example

PRN code length	Number of segments	Segments lengths	Common part length
1023	8	{127,128,129}	116

Conducted analysis:

- To develop adapted acquisition methods (DBFT inspired)
- To calculate acquisition sensitivity / complexity / cross-correlation isolation

PRN code for partial correlations

Main results:

- PRN codes designed for partial correlations allow (Segments of ~128 chips):
  - To **decrease the complexity** while keeping an **acceptable cross-correlation degradation** value and while having a **decreased sensitivity** if Partial Correlation (PC) acquisition method is implemented.
  - To **keep the same complexity** while having a **small degradation of the cross-correlation** (~1,5-2dB) value and while keeping the **same sensitivity** if traditional acquisition method (over complete PRN code) is implemented.
  - ***Receivers have a high flexibility on the targeted acquisition characteristics***

	Complexity reduction wrt Classic Method	Average Cross-correlation Isolation	Sensitivity decrease wrt Classic Method
1023-chips PRN code	Benchmark	~19,2dB	Benchmark
PC Non-coherent	~4 times	~14,8 dB	~ -4,5dB
PC Coherent	~2 to ~3 times	~17,4 dB	~ -0,8dB
93-chips PRN code	~10 times	~11 dB	~ -4dB
341-chips PRN code	Same	~15,2 dB	~ -2dB

LDPC coding for CSK data modulated GNSS links

- Context: new needs and objectives for GNSS
  - Novel functionalities may necessitate higher data rates: authentication, precise positioning,… (→ reduces time-to-first-fix data (TTFFD))

- Proposal: use of the cyclic code-shift keying (CSK) data modulation
  - Providing transmission of multiple bits per PRN sequence → data rate increase
  - Allowing non-coherent demodulation → no phase est. required
  - Having the potential to increase the robustness of the data link → lower BER/FER

- Goals: design of robust and practical LDPC coding solutions for CSK-modulated GNSS signals including
  - Analysis of the performance and required decoding complexity
  - Comparison regarding the latest technical choices of existing GNSS links

LDPC coding for CSK data modulated GNSS links

- Main tasks accomplished

Funtimes 1

1) Optimization of binary LDPC codes for CSK signals, assumed a pragmatic bit-interleaved coded modulation (BICM) approach with iterative demapping/decoding (ID)

Funtimes 2

2) Performance comparison of several receiver configurations
   a. Considering many channels (AWGN, Rice, urban LMS)
   b. Considering both coherent and non-coherent demodulation scenarios
   c. Comparing with configurations typical of latest GNSS technical choices using BPSK-like signals (e.g. GPS L1C, BeiDou III)

3) Computational complexity comparison of all tasks required in the data recovery process
   - Carrier wipe-off, chip-matched filtering, demodulation, demapping, channel decoding

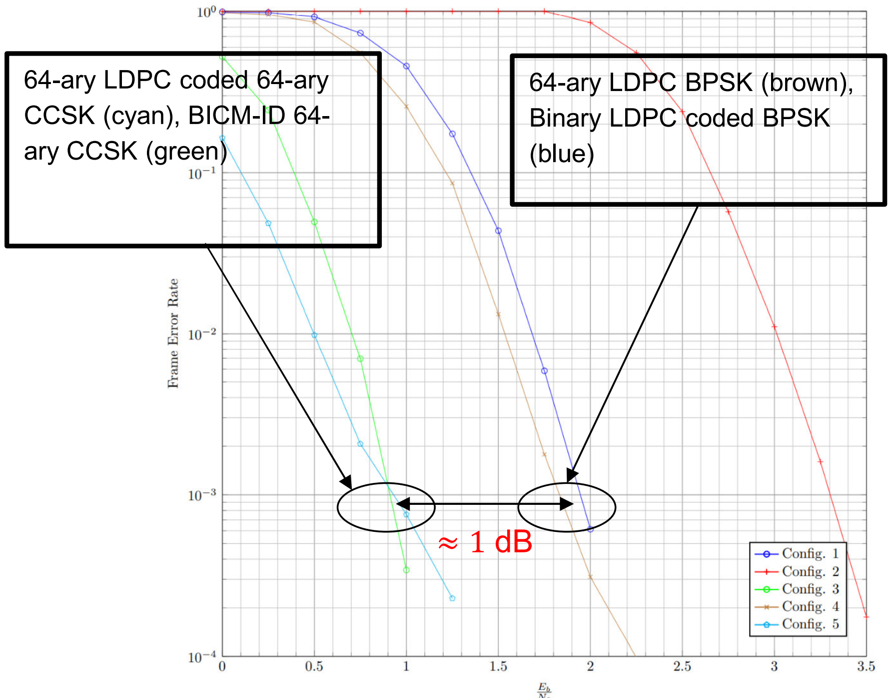
4) Performance and complexity analysis of q-ary LDPC coding for BPSK and CSK signals

5) Proposal of reduced-complexity BICM-ID receivers

LDPC coding for CSK data modulated GNSS links

Main results

- For equal data rates, coded 64-ary CSK have the potential to reduce the data decoding threshold by approximately 1 dB with respect to coded BPSK
- Most of the computational cost increase due CSK demodulation: increase of complexity by an order of magnitude (≈ Factor 6) wrt DSSS/BPSK demodulation
- Computational costs inherent to the decoding of the BICM-ID and q-ary LDPC based solutions are close
- Simple way identified to reduce the number of operations performed during BICM-ID decoding steps (complexity increase reduced to ≈ Factor 2)



Frame Error Rate (FER) in AWGN channel
(1200 bits codeword length)

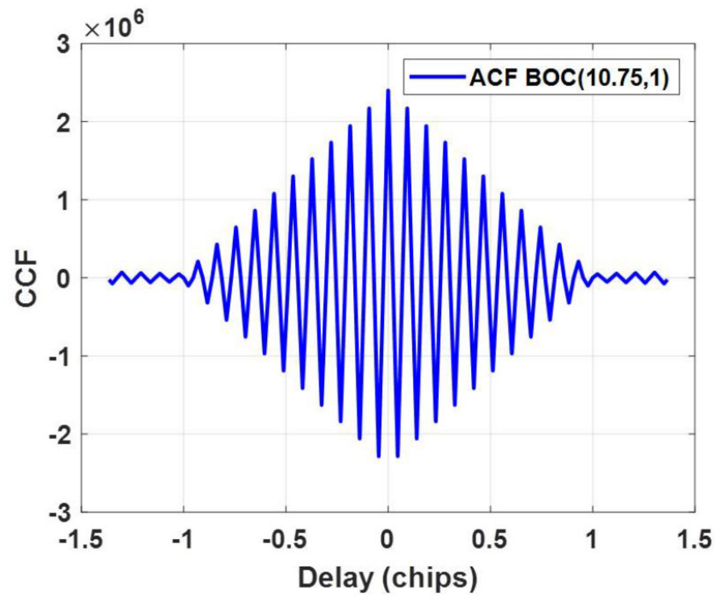
* refer to the technical documents for configurations

Meta-signal Processing

- Meta-signal : idea of tracking two signals on different carrier frequencies as one wideband signal (composed of a spreading code signal plus a sub-carrier signal)

- Purpose: To demonstrate that meta-signal positioning can be realized by resolving sub-carrier ambiguities (≈ a few meters) in the position domain using the LAMBDA ambiguity fixing method to obtain cm level accurate position solutions

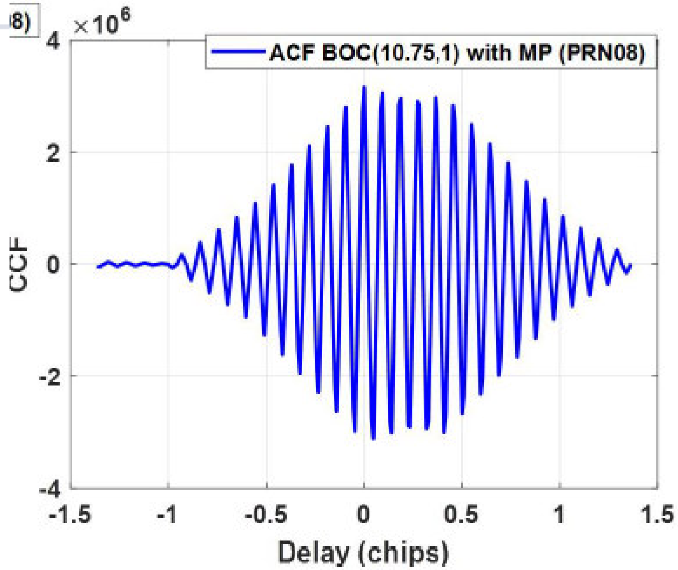
- Positioning done by implementing a Kalman filter based positioning engine that computes Between Satellite Single Difference (BSSD) observations using a single receiver (no reference station) and then applies the LAMBDA method for sub-carrier ambiguity fixing.

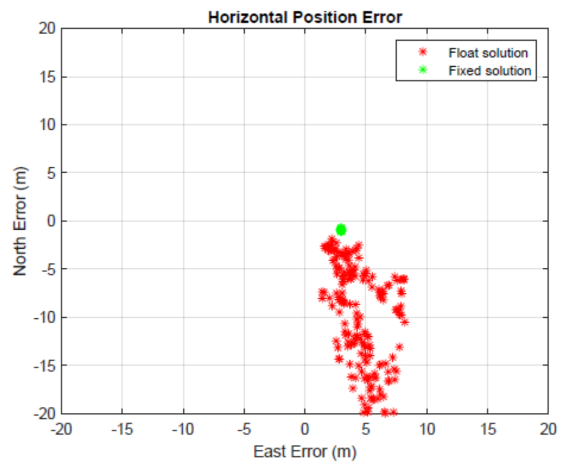


Meta-signal Processing

- Example test case: strong static multipath (optimized filter)
- KPIs : time to successful subcarrier fixing and position accuracy after subcarrier fixing

- Main Conclusions
  - LAMBDA ambiguity fixing can successfully resolve sub-carrier ambiguities given that a suitable filter is employed.
  - Filter convergence is highly dependent on the quality of code observations → higher code multipath results in higher convergence time.
  - Sub-carrier ambiguity resolution in position domain can realize dm level accurate position solutions without RTK.
  - Furthers tests needed to consolidate findings for dynamic user case.





Acquisition aiding signal approaches using a "low bandwidth signal”

- Idea: Use of a low rate MSK signal (250 sps) overlaid to E1B/C
  - to decrease frequency uncertainty such that E1B/C acquisition is reduced to code phase delay estim.
  - to provide a time marker for resolving time uncertainty of one week

- Performed tasks
  - Signal design: power (limited due to ITU regulations in E1/L1 -> $C/N_0 \approx 33$ *dBHz*), access scheme (FDMA), modulation (MSK), FEC (conv. Code: $r=1/3, K=7$), data frame structure
  - Preliminary receiver algorithm design and performance evaluation

- Main conclusions
  - Complexity is significantly reduced compared to classical E1B/C and combined E1D & E1B/C acquisition, although channelizer needed to separate signals from different satellites
  - Frequency estimation delivers required results
  - However, detection/false alarm probability and FER after decoding suffer from very low nominal power caused by ITU restriction in E1 band for narrowband signals

Conclusion (1)

- FUNTIMES I and II have explored and analysed a large variety of navigation signal design aspects driven by
  - Feedback of the user community
  - Scientific literature
  - Lessons learned from Galileo and GPS
  - Expected technology trends

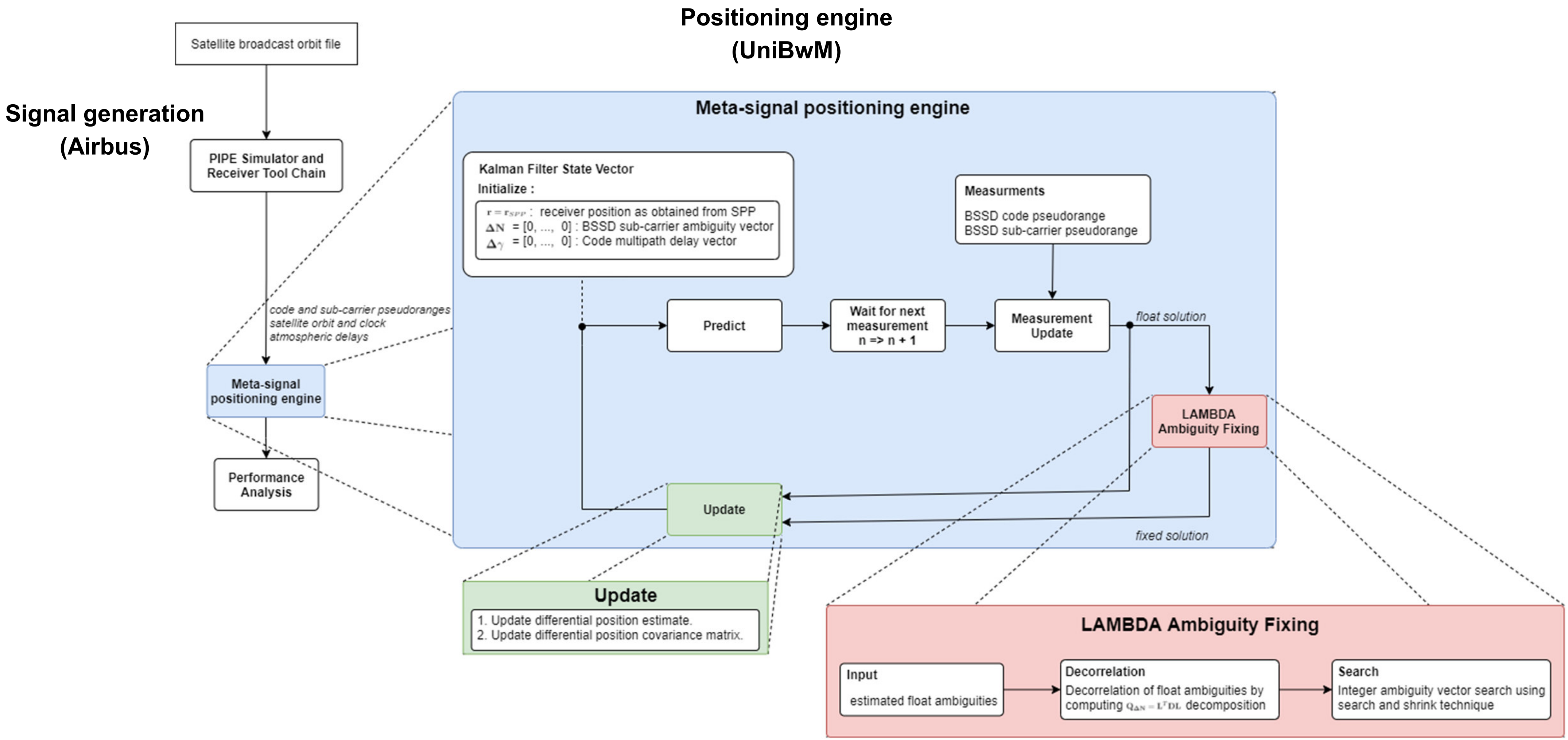
- Some features are already foreseen for the implementation in G1/2G
  - Application of Reed-Solomon codes for improved I/NAV message reception
  - User segment technology trends
- while others are seriously taken into account in the G2G design
  - Advanced solutions for authentication
  - Use of CSK and LDPC codes, Meta signal processing
  - Advanced multiplexing techniques, Acquisition aiding signal approaches using partial correlation

Conclusion (2): Desired Improvements – Considered Signal Aspects

- Main findings for desired improvements
  - Improved resistance to RFI / Ability to generate robust carrier phase measurements
  - Improved TTFF (in warm or cold start) and acquisition sensitivity
  - Robustness against multipath and NLOS situations
  - Provision of an authentication service (data and pseudo-range)
  - Reliability of the measurements
  - Compatibility/interoperability of open services from multiple GNSS
  - Navigation message: - reliable delivery of key parameters in challenging environments
    - delivery of precise orbit, clock and bias data (e.g. for PPP)
    - provision of an alert/emergency service

End of the Presentation

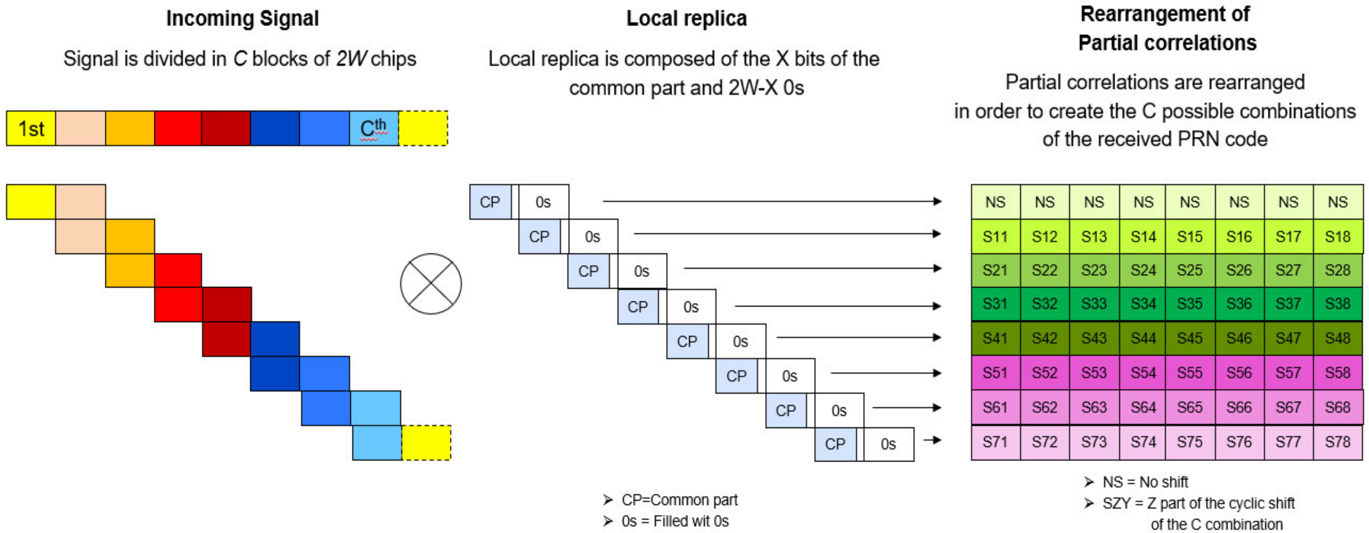
Meta-signal processing

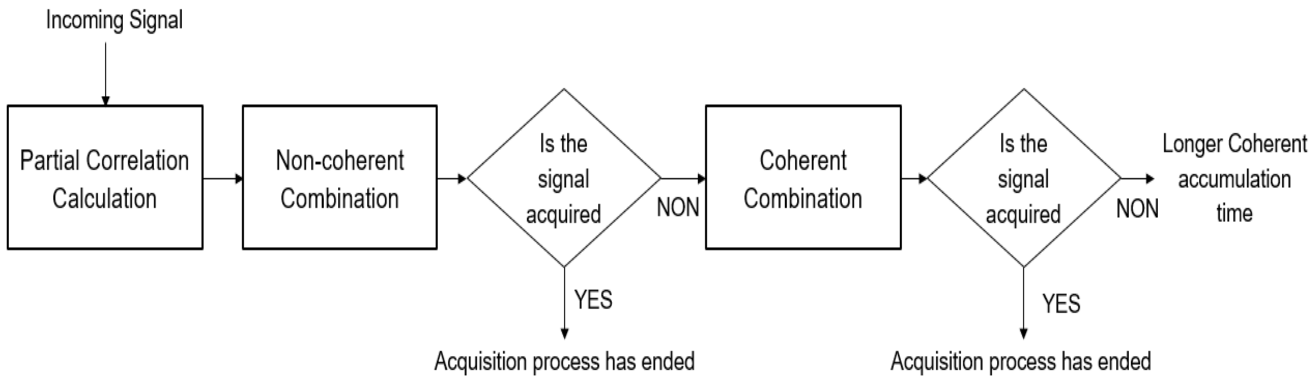


PRN code for partial correlations

Conducted analysis:

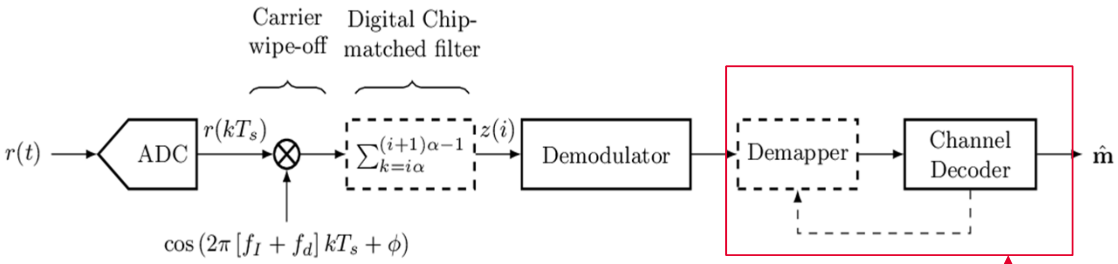
- To develop adapted acquisition methods (DBFT inspired)



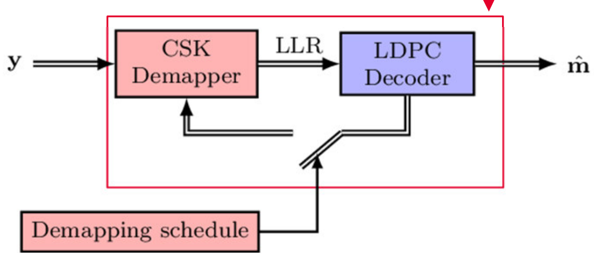


LDPC coding for CSK data modulated GNSS links

- Receiver Block Diagram



Generic data decoder structure



BICM-ID receiver with constrained demapping schedule

LDPC coding for CSK data modulated GNSS links

- Main results

Configuration	Code	Modulation	Demapping	Decoding
1	Binary LDPC (GPS L1C subframe 2)	BPSK	(log-)MAP	OMS
2	Binary LDPC (Compromise)	64-ary CSK	Non-iterative Max Log MAP	OMS
3	Binary LDPC (Compromise)	64-ary CSK	Iterative (log-)MAP	OMS
4	64-ary LDPC (BeiDou III B1C subframe 2)	BPSK		EMS
5	64-ary LDPC (BeiDou III B1C subframe 2)	64-ary CSK		EMS
6	Binary LDPC (Compromise)	64-ary CSK	Iterative (log-)MAP with incomplete demapping schedule ($E = 3$, $I_{dem}^{max} = 10$)	OMS

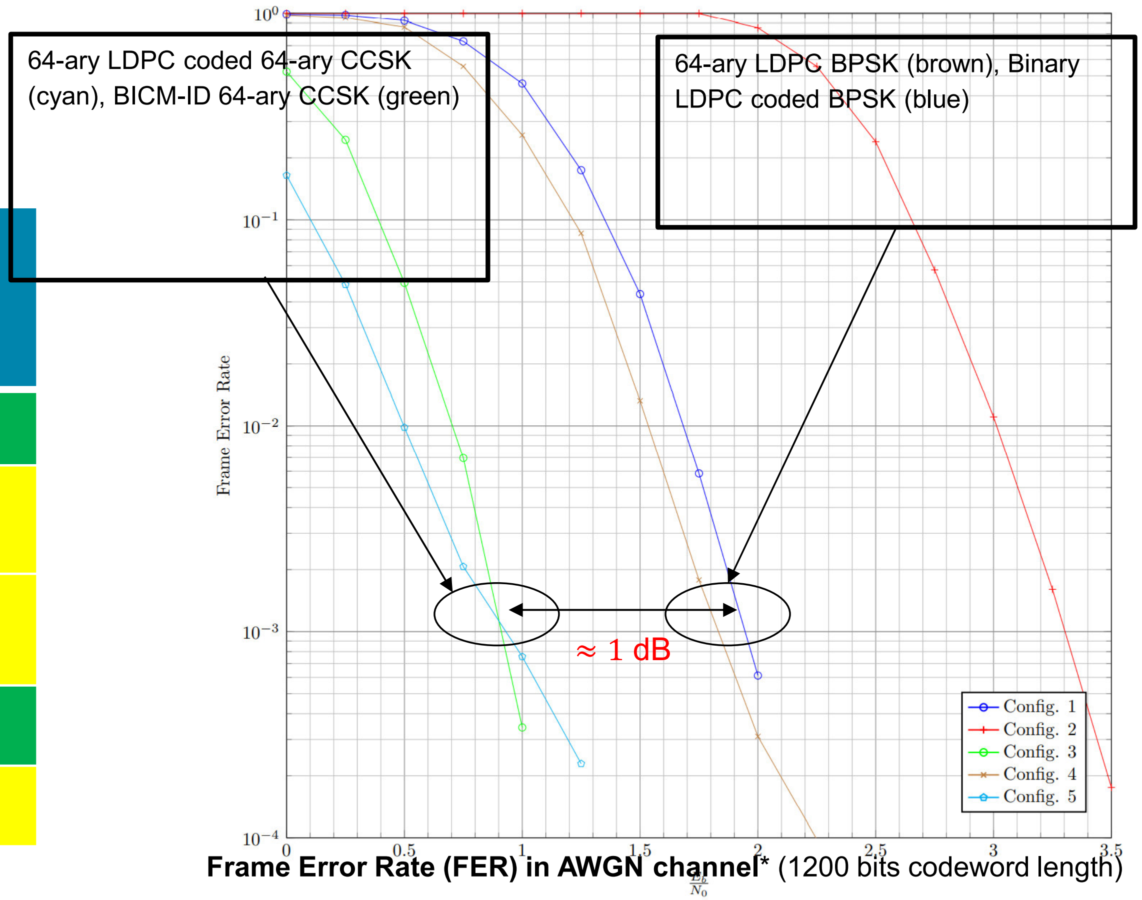
Table 36 Evaluated configurations for "moderate" code length ($\tilde{N} = 1200$)

UNCLASSIFIED

LDPC coding for CSK data modulated GNSS links

- Main results

Conf.	Modulation and Code	Increase factor of the overall number of operations for data recovery* w.r.t. config 1
1	BPSK and binary LDPC	$\times 1$
2	BICM with 64-ary CSK and binary LDPC	$\sim \times 2 / \times 6$
3	BICM-ID with 64-ary CSK and binary LDPC	$\sim \times 2 / \times 6$
4	BPSK and 64-ary LDPC	$\sim \times 1$
5	64-ary CSK and 64-ary LDPC	$\sim \times 2 / \times 6$



Frame Error Rate (FER) in AWGN channel* (1200 bits codeword length)

AIRBUS ENAC LINKS UAB Universitat Autònoma de Barcelona Universität der Bundeswehr München