International Technical Symposium on Navigation and Timing

ENAC, Toulouse, France

13-16 November 2018

The European Commission's science and knowledge service

Joint Research Centre

European Commission

International Technical Symposium on Navigation and Timing

ENAC, Toulouse, France

14th November 2018

New Concepts and Ideas to Improve the Reliability of PNT Services

Matteo Paonni

European Commission, Joint Research Centre

Directorate for Space, Security and Migration

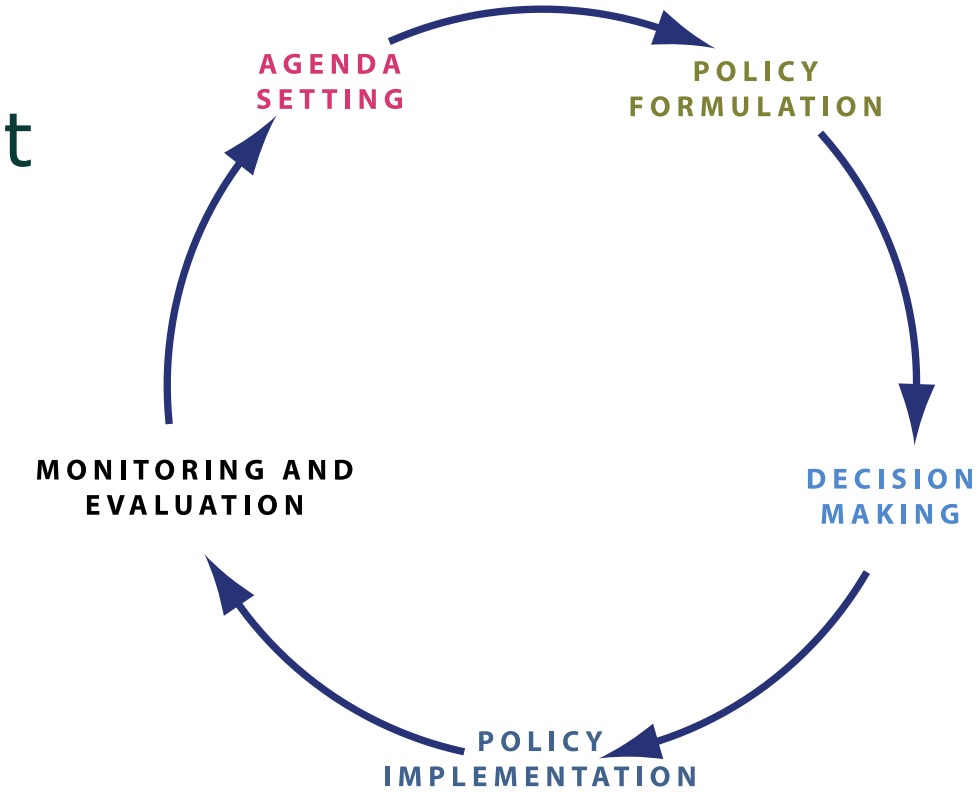
European Commission

Outline

- **Introduction and Context**
- GNSS Performance in the Context of Signal Design
- Galileo I/NAV Optimization
- New Concepts for GNSS Evolution
- A Look at Signal Processing
- Conclusions

JRC Mission

- The Joint Research Centre is the European Commission's **in-house science and knowledge service**
- JRC mission is to support **EU policies** with **independent** evidence throughout the whole **policy cycle**
- **Independent**, policy **neutral**, **transversal** service
- Since 10 years supporting **EGNSS Programme** on a wide range of activities



European Commission

Context

- JRC provides **technical support to EGNSS (EC GROW)** on management of **R&D projects with subject on GNSS** under H2020
  - ✓ Main focus on **mission and service** definition
  - ✓ Some elements from **Future Navigation and Timing Evolved Signals (FUNTIMES) project** part of this presentation

- JRC also performs **anticipatory R&D** on various topics in order to be able to provide high value independent scientific and technical support

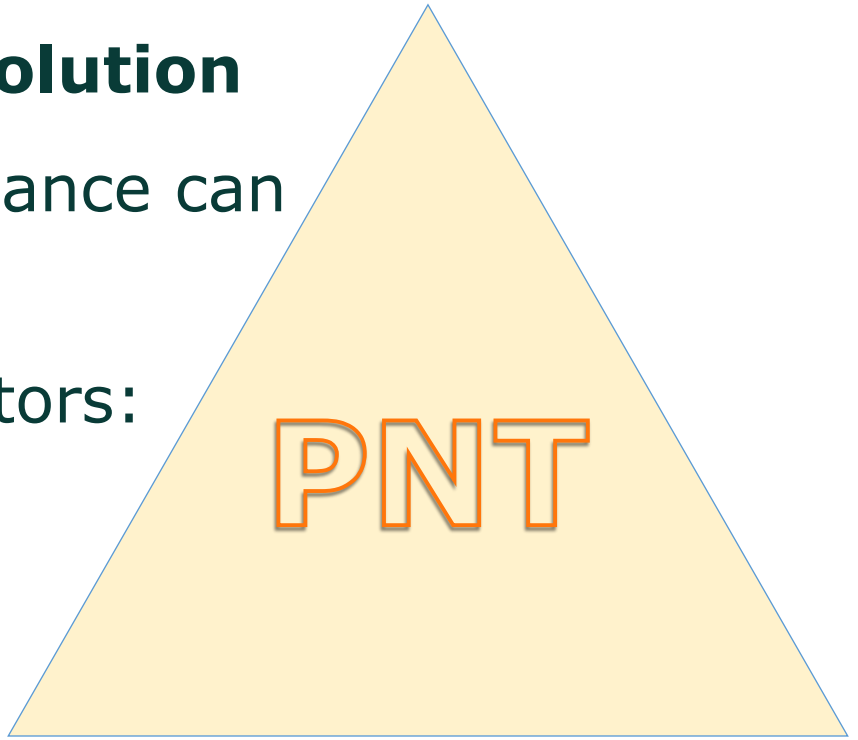
- **Unless explicitly specified, the content is not related to any decision of the European Commission or of the Galileo Programme**

Outline

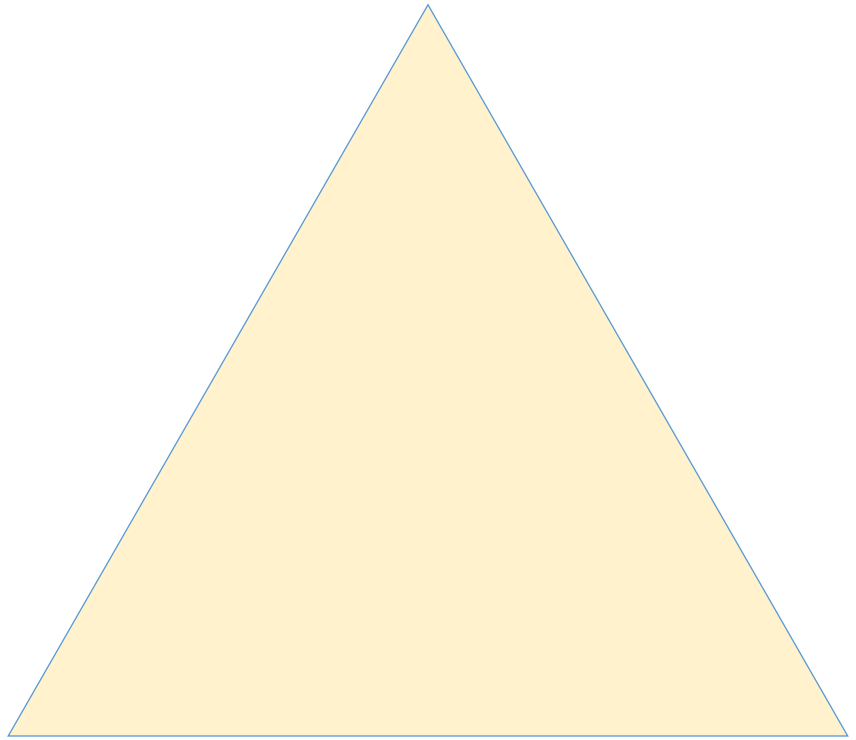
- Introduction and Context
- **GNSS Performance in the Context of Signal Design**
- Galileo I/NAV Optimization
- New Concepts for GNSS Evolution
- A Look at Signal Processing
- Conclusions

PTN solution vs. GNSS performance

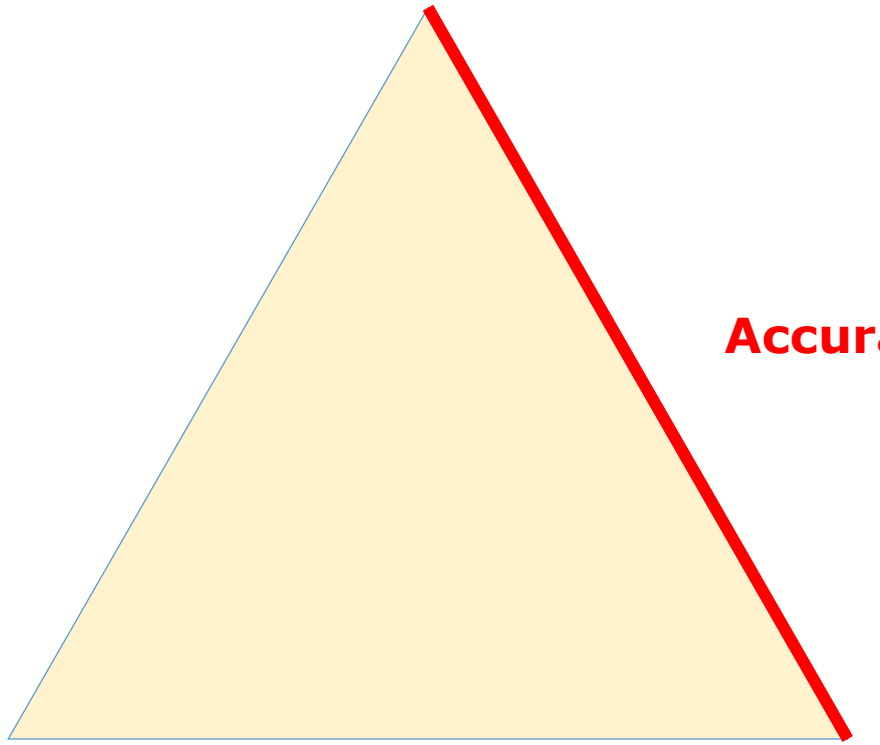
- GNSS provides key **contribution** to user **PNT solution**
- Depending on specific **application** user performance can depend more or less on GNSS
- GNSS performance mainly depends on three factors:
  - ✓**System design** (constellation, signals, …)
  - ✓**Environment** (e.g. propagation channel)
  - ✓**Receiver implementation**
- These three factors strongly relates with each other and impact all **dimensions of GNSS performance**



The Three (+ one) Dimensions of GNSS Performance



The Three (+ one) Dimensions of GNSS Performance



Accuracy

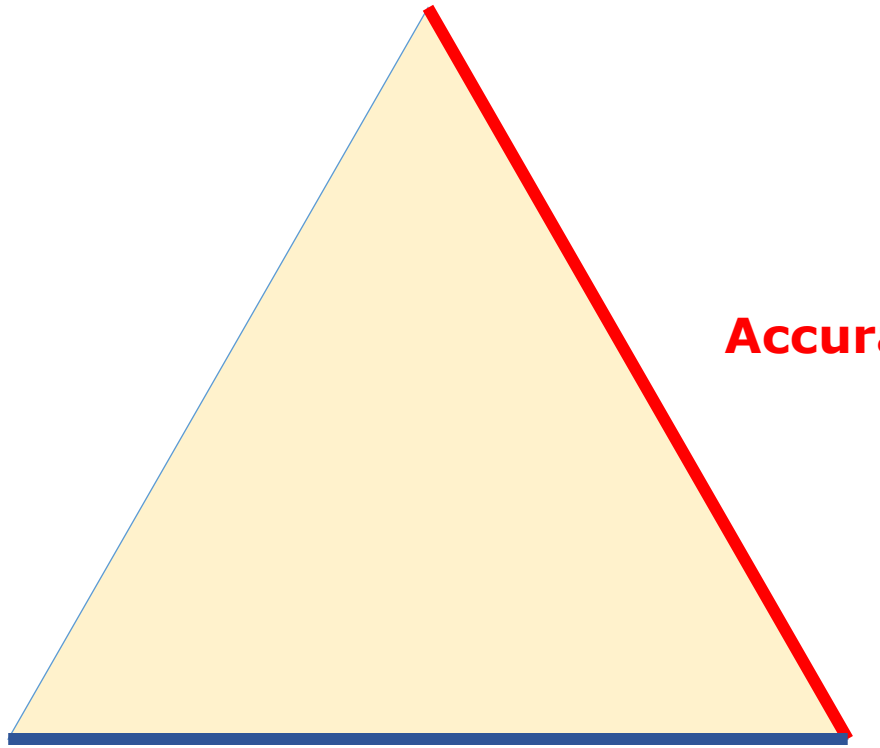
What matters ultimately!

Depends on all factors
- ✓ Accurate signals
- ✓ Channel is critical…
- ✓ …as well receiver!

Accuracy has to be delivered!

European Commission

The Three (+ one) Dimensions of GNSS Performance



Accuracy

What matters ultimately!

Depends on all factors
- ✓ Accurate signals
- ✓ Channel is critical…
- ✓ …as well receiver!

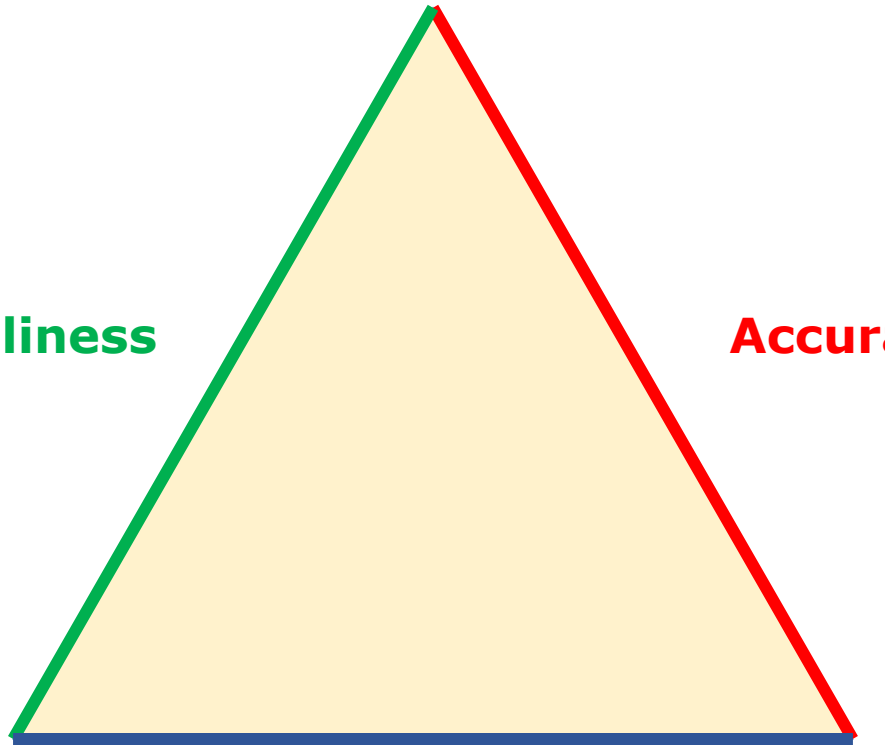
Accuracy has to be delivered!

Sensitivity

Qualifies the conditions at which accuracy is delivered (and kept)

Minimum required C/N_0

The Three (+ one) Dimensions of GNSS Performance



Timeliness

How long does it take?

Time-To-First-Fix

Key for stand-alone

Increasing impact on performance perception

Accuracy

What matters ultimately!

Depends on all factors
- ✓ Accurate signals
- ✓ Channel is critical…
- ✓ …as well receiver!

Accuracy has to be delivered!

Sensitivity

Qualifies the conditions at which accuracy is delivered (and kept)

Minimum required C/N_0

European Commission

The Three (+ one) Dimensions of GNSS Performance

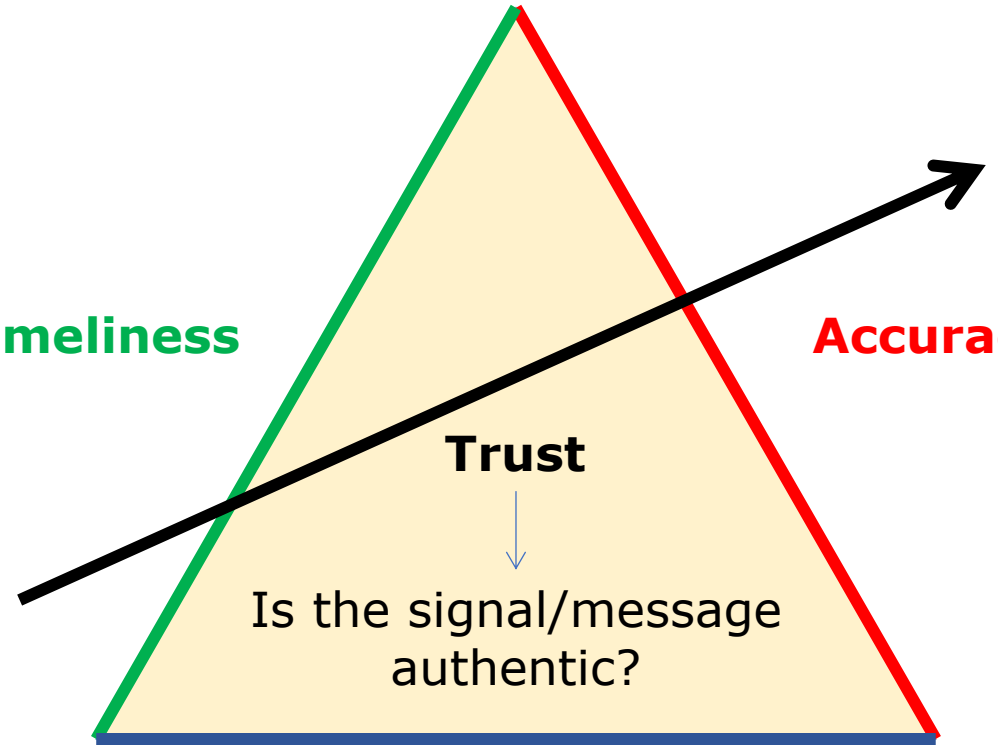
How long does it take?

Time-To-First-Fix

Key for stand-alone

Increasing impact on performance perception

Timeliness



Accuracy

What matters ultimately!

Depends on all factors
- ✓ Accurate signals
- ✓ Channel is critical…
- ✓ …as well receiver!

Accuracy has to be delivered!

Sensitivity

Qualifies the conditions at which accuracy is delivered (and kept)

Minimum required C/N_0

European Commission

Signal Design is a Trade-Off Exercise

- Ideal solution that delivers maximum **accuracy** with **authentic** signals at the maximum **sensitivity** and minimum **TTFF** does not exist!
- A further key element to be considered for any design is the corresponding **processing complexity** at receiver level
- Signal design is a **trade-off** exercise targeting a **specific user demand** and considering those **key performance indicators**
- Typically different indicators pull the solution in opposite direction:
  - ✓ **Accuracy** ←→ **Sensitivity**
  - ✓ **TTFF** ←→ **Sensitivity**
  - ✓ **Accuracy** ←→ **TTFF**

  } ←→ **Processing Complexity**

The case of Galileo E1-OS

- In the last years work performed (and still ongoing) on various direction to improve **Galileo E1-OS** performance
  - ✓ **Optimization** of **I/NAV** message following SoL reprofiling
  - ✓ **Evolution** of Galileo signals for **G2G**, including E1-OS
- The main objective is to serve **new user needs** and **emerging applications**
  - ✓ **Low power/low complexity** applications (e.g. IoT, snapshot), progressive introduction of **authentication** functions, higher accuracy and robustness
- One of the **design targets** at performance level is represented by **GPS III Open Service**
  - ✓ GPS III OS means **L1 C/A + L1C**
    - ✓ For L1C we are actually assessing with respect to the expected performance
  - ✓ Current Galileo E1 OS performance are for many aspects between that of C/A and L1C
- Optimization and evolution are all constrained to **backward compatibility**
  - ✓ Legacy signals and users

Outline

- Introduction and Context
- GNSS Performance in the Context of Signal Design
- **Galileo I/NAV Optimization**
- New Concepts for GNSS Evolution
- A Look at Signal Processing
- Conclusions

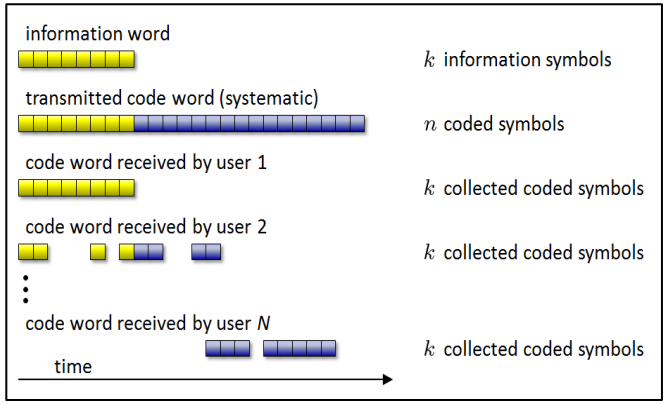
Reduced CED for Fast First Fix

- The idea behind is that mass market users might tolerate an **initial degraded accuracy** to have a **faster position fix**
- Every GNSS user is interested in high accuracy PVT solutions, however:
  - ✓ Many classes of users require very short first fix time (few seconds)
  - ✓ This can be more important than waiting for high accuracy solution
- Confirmed by **3GPP requirement** in support of AGNSS: position fix **within 20 s** with a 2D position error (95%) of 100 m
- Definition of a **compact set of Clock and Ephemeris Data**
  - ✓ To be received in a considerably shorter time than full CED
  - ✓ Full accuracy available as soon as full CED are retrieved
- Complex optimization work resulted in a design **outperforming** the initial target

[REF] M. Anghileri, M. Paonni, E. Gkougkas, B. Eissfeller, *Reduced navigation data for a fast first fix*, NAVITEC 2012

RS Codes for Improving the I/NAV Message

- A technical solution for reducing the Time to First-Fix for non connected users was evaluated:
  - ✓ Use of Reed-Solomon (RS) codes at the Link Layer (outer encoding)
    - MDS "Joker" property
    - Erasure correction capability
    - Error correction capability
    - Systematic implementation to ensure backward compatibility
  - ✓ Example application to the Galileo I/NAV message was assessed
    - Time to CED performance in AWGN and 2-state LMS channel
    - Assessment of RS algorithm complexity



T_0 in sec.	I/NAV on E1-B **RS4**
1	CED 2/4
3	CED 4/4
5	RS CED 1
7	RS CED 2
9	
11	
13	
15	
17	RS CED 3
19	RS CED 4
21	CED 1/4
23	CED 3/4
25	
27	
29	
min. TTFFD	8.000 s
av. TTFFD	13.933 s
95% TTFFD	17.625 s
max. TTFFD	18.000 s

Anticipated Performance (assessment performed within FUNTIMES project):

- Significant improvement of Time-to-CED (50% to 60%) especially in urban environment
- Full backward compatibility with legacy receivers
- Low processing complexity

[REF] Schotsch B., Anghileri M., Ouedraogo M., Burger T., *Joint Time-to-CED Reduction and Improvement of CED Robustness in the Galileo I/NAV Message*, ION GNSS+ 2017

Outline

- Introduction and Context
- GNSS Performance in the Context of Signal Design
- Galileo I/NAV Optimization
- **New Concepts for GNSS Evolution**
- A Look at Signal Processing
- Conclusions

Acquisition Aiding Signal

- After the introduction of solutions at message level, still some performance gaps
  - ✓ Acquisition complexity (and therefore time)
  - ✓ Sensitivity
- Ideal acquisition aiding signal should be characterised by:
  1. low chip rate and short PRN code
     - ✓ **smaller acquisition search space** and therefore **faster acquisition process**
     - ✓ Narrower bandwidth → reduced processing power
  2. To be either a pilot or a very low-rate data channel
     - ✓ the higher the **symbol rate**, the shorter the maximum **coherent integration time**, and therefore the lower the **maximum possible acquisition sensitivity**
  3. Some secondary code to perform almost immediate **hand-over** to other signal components
- **Quasi-pilot** might be interesting option
  - ✓ Pilot signal modulated with a Time-to-Interval which receiver can wipe-off once synchronized

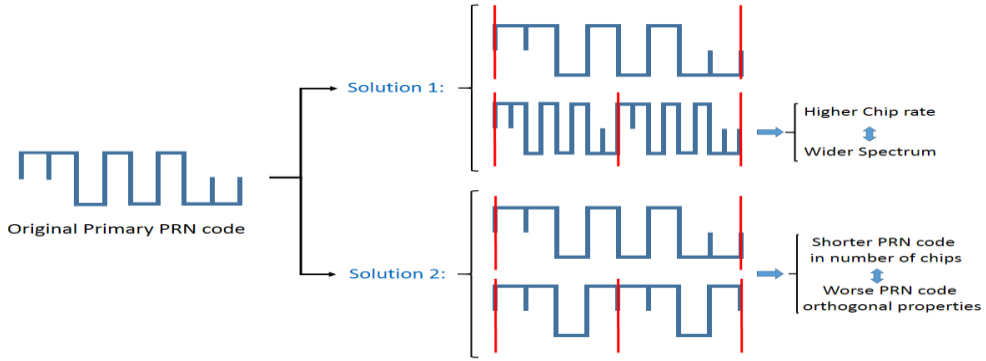
[REF] M. Paonni, M. Bavaro, M. Anghileri, B. Eissfeller, *Design of a GNSS Acquisition-Aiding Signal*, Inside GNSS, Jan/Feb 2014
M. Paonni, M. Anghileri, D. Fontanella, B. Eissfeller, *Quasi-Pilot Signals: Improving Sensitivity and TTFF without Compromises*, ION/GNSS 2011

Code Shift Keying (CSK) for GNSS Signals - Background

- Several problems are addressed with the implementation of a **CSK modulation** on the GNSS signal **data component**:

1) Amount of data which can be currently broadcasted by a GNSS signal is **limited**. This limitation is imposed by the DS-SS structure of a GNSS signal:

- ✓ increasing the chip rate which directly implies an increase of the signal bandwidth
- ✓ decreasing the PRN code length (number of chips) which implies a degradation of the PRN code properties



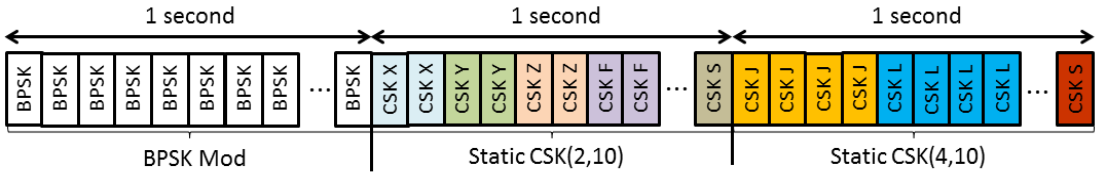
2) Data component of current GNSS signals is **designed as a communication signal** without taking into account the GNSS specificities: data has different degrees of relevance and variable data rates could be of high interest.

3) In urban environments, the **data demodulation** becomes **difficult** to due to the **harsh reception conditions** affecting the **signal carrier tracking** up to a PLL loss-of-lock.

[REF] Chauvat R., Garcia-Pena A., Anghileri M., Floch J.J., Paonni M., *Ultra-Sparse Binary LDPC Codes with CSK Signals for Increased Data Rate in GNSS Signals*, Navitec 2018

Code Shift Keying (CSK) for GNSS Signals - Expected Benefits

1) **Bit rate increase of a DS-SS signal without**:
   - ✓ increasing the PRN code number of chips, and without increasing the signal chip rate (bandwidth constraint)
   - ✓ Increased rate can be used to increase the number of services or to improve available services.
2) **Flexibility of the signal bit rate**: allows to dynamically change the number of symbols of the modulation
   - ✓ More robustness to fundamental data and less robustness to less relevant
   - ✓ Optional data since the bit rate is directly related to the demodulation sensitivity



3) **Possibility of implementing a non-coherent demodulation** process: non-coherent demodulation does not require the estimation of the incoming signal carrier phase
   - ✓ Increase the amount of data recovered in an urban environment and/or high dynamic users

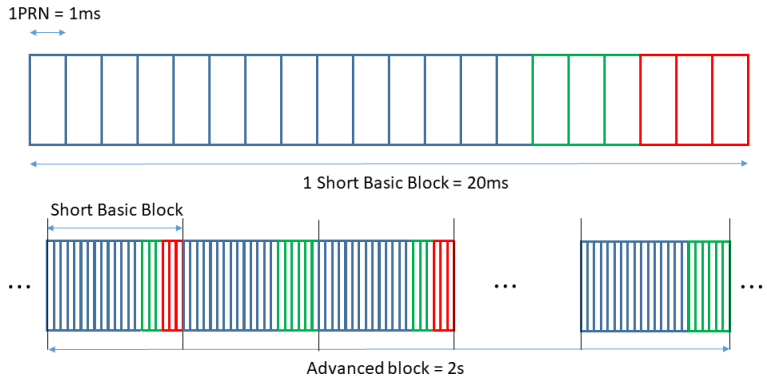
Possible issues and drawbacks

- Impossibility to use a CSK modulated signal for ranging: the receiver does not know which cyclic shift of the fundamental PRN code is expected at each correlation epoch.
- Complexity of the receiver is significantly increased → FT/IFT demodulator

European Commission

Multi-Purpose TDM Signal Component

- **1st Objective:** to design a signal component targeting **several functionalities**, e.g.:
  1) Fast/Low complexity Acquisition
  2) Fast TTFFD
  3) Authentication

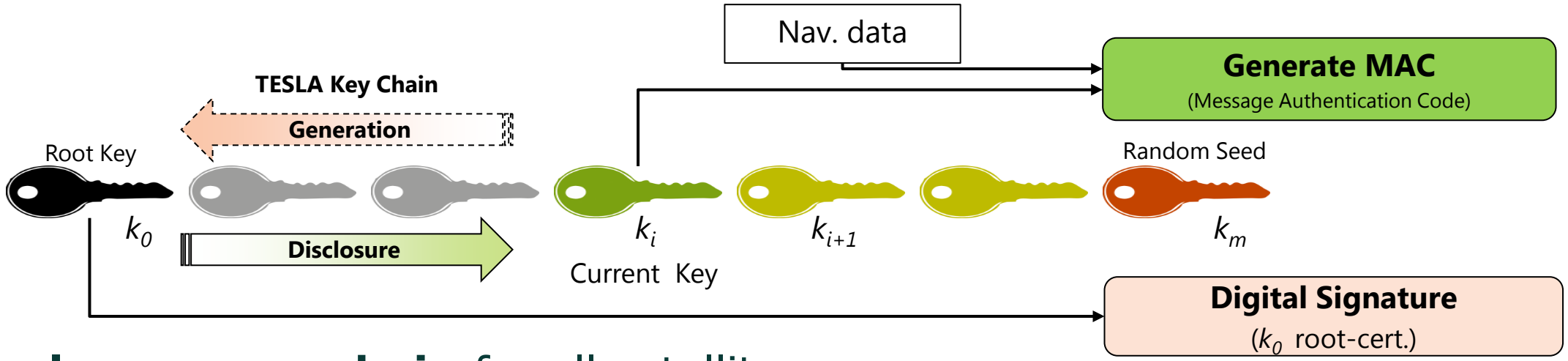


- **2nd Objective:** to design a signal component allowing continuous or partial non-coherent processing
- Time Division Multiplexing chosen as the main signal structure for various reasons:
  - ✓Reduced complexity implementation at satellite payload
  - ✓higher efficiency of multiplexing
- TDM considered at **PRN code level**: each PRN code associated to a different functionality
- This option present a **high flexibility** if PRN codes are short

[REF] Garcia-Pena A., Julien O., Anghileri M., Floch J.J., Paonni M., *Multi-purpose TDM Component for Galileo E1 OS*, ION GNSS+ 2018

Proposed NMA solution for Galileo E1 OS

- Based on **TESLA** (Timed Efficient Stream Loss-tolerant Authentication) scheme
- Chain of keys generated through a one-way function (e.g., SHA-256)
  - ✓ *Message Authentication Code* (MAC) to authenticate the Nav. Message
  - ✓ Current key (used to compute MAC) released with a delay (e.g., 10 s later)

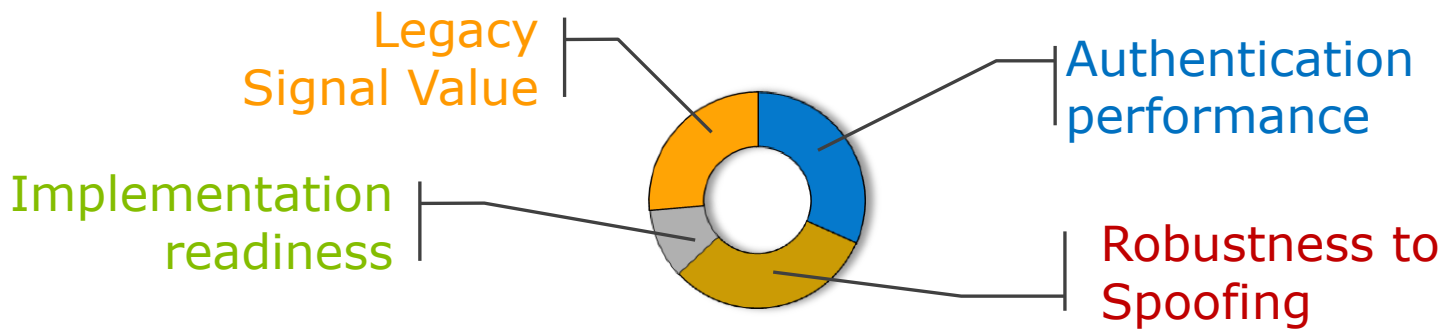


- ✓ **Single one-way chain** for all satellites
- ✓ **Root key** (k_0) signed with a **public-private signature** scheme

[REF] I. Fernández-Hernández, et al., "A navigation message authentication proposal for the Galileo open service," *Navigation, Journal of The Institute of Navigation*, vol. 63, no. 1, pp. 85-102, Spring 2016.

Ranging Authentication in a SNAP (1/4)

- SNAP is an Authentication concept designed for the Galileo Open Service
- Design performed within the FUNTIMES project following specific trade-off criteria



- **Authentication Performance**
  used to assess the authentication technique, mainly in terms of Time Between Authentications (TBA) and Time To Alarm (TTA)
- **Spoofing Robustness**
  measures the level of resilience to specific spoofing attacks (e.g., those involving spoofers with a single high-gain directional antenna)
- **Implementation Readiness**
  assesses the level of complexity required both at the system and receiver levels and the backward compatibility
- **Legacy Signal Associated Value**
  assesses the level of reuse and valorization of the current signal and messages

[REF] B. Motella, D. Margaria, M. Paonni, *SNAP: an Authentication Concept for the Galileo Open Service*, IEEE/ION PLANS 2018

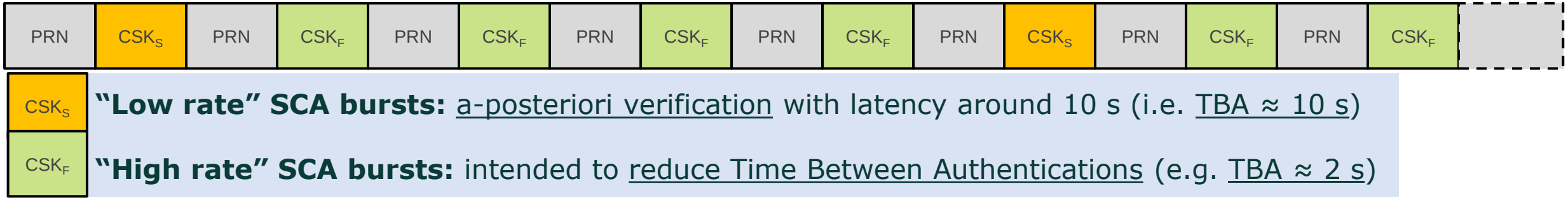
Ranging Authentication in a SNAP (2/4)

- Authentication schemes can be implemented on different **Signal Component**:
  - ✓By modifying an **existing signal component** (e.g., E1-B, E1-C, E5a, E5b)
    - Possible performance degradations for non-participant users ($\Delta C/N_0$)
  - ✓Introducing a **new component**
    - More flexibility in the design of the authentication scheme, thus reducing some constraints related to the backward compatibility
- The choices for the **Relative Power Level** of the authentication component are:
  - ✓**Same power** as other open components
  - ✓**Lower power** level
  - ✓**Variable power** (i.e. amplitude modulation)
    - Low power level options tend to increase the robustness against some spoofing attacks
    - However the power level can affect the achievable authentication performance for participant receivers (e.g., TBA, TTA, reduced effective C/N_0)
- Any solution has to identify a trade-off among these (and other) aspects

[REF] B. Motella, D. Margaria, M. Paonni, *SNAP: an Authentication Concept for the Galileo Open Service*, IEEE/ION PLANS 2018

Ranging Authentication in a SNAP (3/4)

- **High-level idea**
  - ✓ Possible re-use of E1-B OS NMA data → Additional protection to OS NMA ("time binding" concept)
  - ✓ Initially inspired from SSSC, Supersonic Codes, and Signature-Amortization concepts



- "Fast" bursts for **all satellite signals** generated from **same code chips**, by using a **future NMA key** (k_j+1):

$$\text{crypto key}_m \;\propto\; \text{Hash}\{\, k_j+1 \;\mid\; \text{GST}_m\}$$

- **Different CSK shifts** applied to each burst, depending on **Sat. ID, previous key** (k_j), and **next NMA bits**:

$$\text{shift}_m \;\propto\; \text{Hash}\{\, \text{Sat. ID} \;\mid\; k_j \;\mid\; \text{next 'Reserved 1' field}\,\}$$

[REF] B. Motella, D. Margaria, M. Paonni, *SNAP: an Authentication Concept for the Galileo Open Service*, IEEE/ION PLANS 2018

Ranging Authentication in a SNAP (4/4)

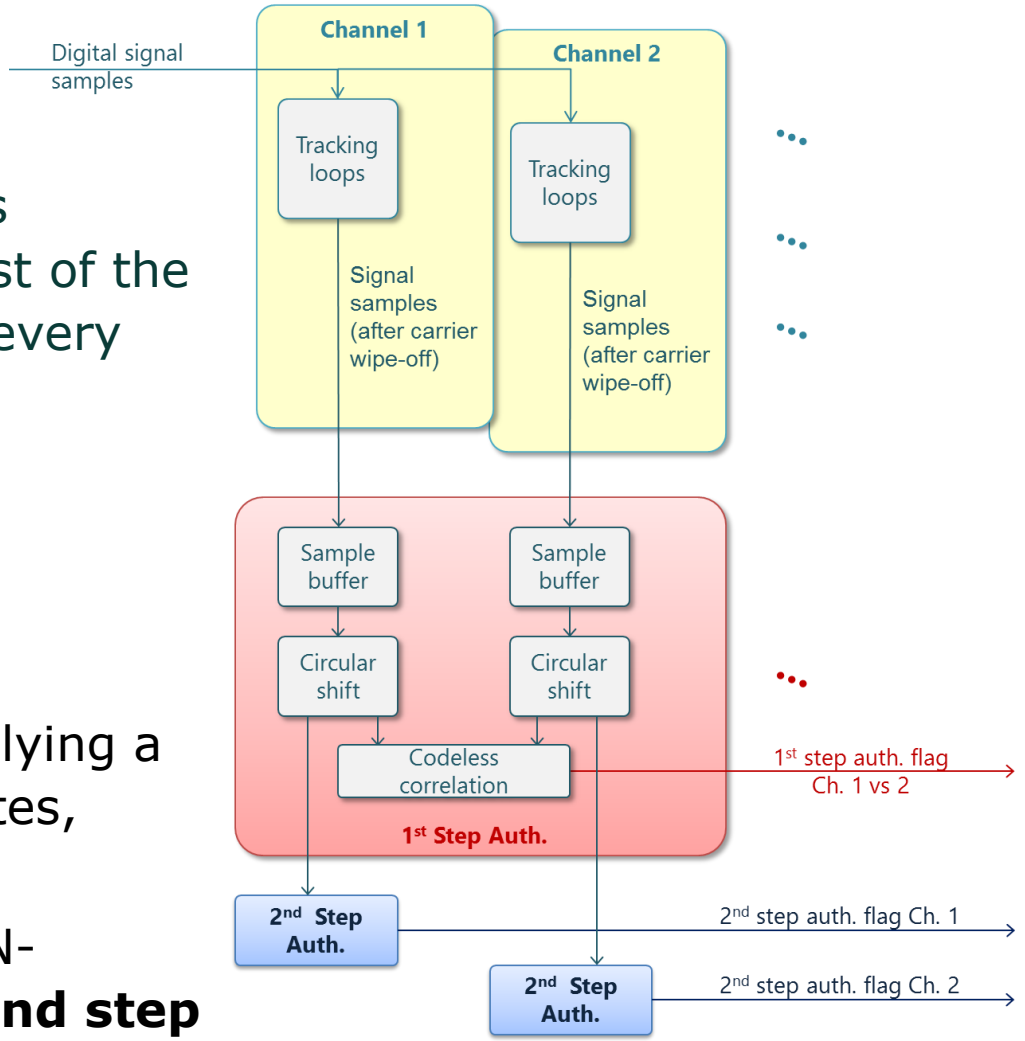
✓ crypto key$_m$ ∝ Hash { k_j+1 | GST$_m$}

✓ shift$_m$ ∝ Hash { Sat. ID | k_j | next 'Reserved 1' field }

Being the crypto key independent from the Sat. ID, the bursts received from different satellites at a given time instant consist of the same code chips sequence, just shifted in a different way for every satellite.

The receiver would be able to:

1. first cross-authenticate couples of satellite signals by applying a codeless CSK correlation between bursts from two satellites, properly shifted and aligned → **first step**
2. a-posteriori verify both 'slow' and 'fast' bursts with a NON-codeless correlation, as soon as k_j+1 is disclosed → **second step**



[REF] B. Motella, D. Margaria, M. Paonni, *SNAP: an Authentication Concept for the Galileo Open Service*, IEEE/ION PLANS 2018

Outline

- Introduction and Context
- GNSS Performance in the Context of Signal Design
- Galileo I/NAV Optimization
- New Concepts for GNSS Evolution
- **A Look at Signal Processing**
- Conclusions

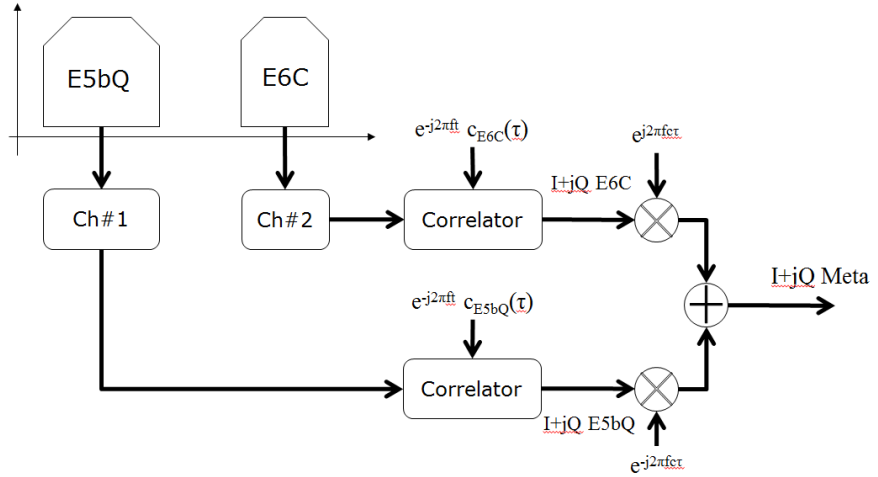
Meta-signal processing for better accuracy (1/3)

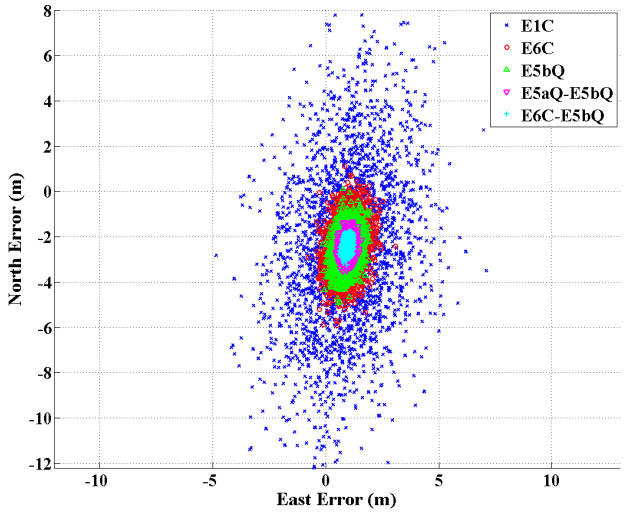
- GNSS broadcast **different signals** on a range of **different centre frequencies**
- Many precision GNSS receivers **process multiple signals** from each available satellite
- Signals are often **combined** within the receiver at **measurement** or at discriminator level
- However, addition of a second signal significantly improves the single-point ranging accuracy **over that of the better of the two signals**
- Idea of **Meta-signal** is to process different signals broadcast on different carrier frequencies **as a single signal:**
  - ✓Any pair of synchronized signals could be chosen
  - ✓Some are more appropriate than other
  - ✓The properties of the resulting correlation function depend on both the frequency separation and relative chipping rates

[REF] J.-L. Issler, M. Paonni, B. Eissfeller, *Toward Centimetric Positioning Thanks to L- and S-Band GNSS and to Meta-GNSS Signals*, Proceedings of NAVITEC 2010

Meta-signal processing for better accuracy (2/3)

- Initial demonstration with real signals in static conditions **Galileo E5b-E6BC** meta-signal
  - ✓Vector receiver architecture
  - ✓Tracking and PVT (using the four IOV satellites)
- Post-correlation combining of upper and lower sidebands
  - ✓Acquisition and then convergence of each individual component
  - ✓Composite signal obtained by rotating and adding correlator values of composite parts
  - ✓Vector-assistance constrained by fixed PVT
  - ✓Performance assessment in terms of correlation function and position error





	3D Position Error (3s) [m]
E1-C	20.690
E6-C	6.004
E5b-Q	4.128
E5ab-Q	2.250
MetaSignal E5b-Q/E6-C	1.850

[REF] M. Paonni, J.T. Curran, M. Bavaro, J. Fortuny-Guasch, *GNSS Meta Signals: Coherently Composite Processing of Multiple GNSS Signals*, ION GNSS+ 2014

Meta-signal processing for better accuracy (3/3)

- Inter-channel **biases** due to front-end and possibly different ionospheric **delay**
  - ✓More work to be done for effective **inter-channel calibration**
- Approach needs to be demonstrated in **dynamic conditions** (e.g. presence of multipath)
  - ✓Unbiased tracking due to complex correlation function might be an issue
  - ✓To build upon recent advancements in the context of **high-order BOC** processing
- This kind of approached to become more relevant with
  - ✓**More signals** available at various **carrier frequencies**
  - ✓Advancement in receiver capabilities
- Interesting use case:
  - ✓**Beidou B1I-B1C** signals transmitted from Beidou-3 satellites

Outline

- Introduction and Context
- GNSS Performance in the Context of Signal Design
- Galileo I/NAV Optimization
- New Concepts for GNSS Evolution
- A Look at Signal Processing
- **Conclusions**

Wrap-up

- Review of innovative ideas introduced in the last few years, especially in the context of Galileo E1-OS optimization and evolution
- Relevant work performed under the H2020 FUNTIMES project
- Some solutions available within the next few years
- Many opportunities for innovation
- User segment to close the gaps that will always be there and to go beyond signal design expectation (as usual!)

Thanks

Any questions?

matteo.paonni@ec.europa.eu

European Commission