Multi-purpose TDM Component for GNSS

Axel Javier Garcia Peña, Olivier Julien, Marco Anghileri, Jean-Jacques Floch, Matteo Paonni

Multi-purpose TDM component for GNSS

Axel Garcia-Pena, Olivier Julien, *Ecole Nationale de l'Aviation Civile (ENAC)*
Marco Anghileri, Jean-Jacques Floch, *Airbus Defence and Space GmbH*
Matteo Paonni, *European Commission-Joint Research Centre (JRC), Directorate for Space, Security and Migration*

BIOGRAPHIES

Axel Garcia Pena *is a researcher/lecturer with the SIGnal processing and NAVigation (SIGNAV) research axis of the TELECOM research group of ENAC (French Civil Aviation University) lab, Toulouse, France. His research interests are GNSS navigation message demodulation, optimization and design, GNSS receiver design and GNSS satellite payload. He received his double engineer degree in 2006 in digital communications from SUPAERO and UPC, and his PhD in 2010 from the Department of Mathematics, Computer Science and Telecommunications of the INPT (Polytechnic National Institute of Toulouse), France.*

Olivier Julien *is the head of the SIGnal processing and NAVigation (SIGNAV) research axis of the TELECOM research group of ENAC (French Civil Aviation University) lab, Toulouse, France. His research interests are GNSS receiver design, GNSS multipath and interference mitigation, and interoperability. He received his engineer degree in 2001 in digital communications from ENAC and his PhD in 2005 from the Department of Geomatics Engineering of the University of Calgary, Canada.*

Marco Anghileri *is an engineering manager at Airbus Defence and Space, where he currently leads various R&D activities on the evolution of the Galileo system and signals. In the past, he was lead systems engineer at IFEN GmbH and research associate at the Institute of Space Technology and Space Applications of the Universität der Bundeswehr in Munich. His main research interests include navigation signal and message design and performance, receiver algorithms as well as navigation systems evolution and modernization. From 2009 to 2013 he supported the European Commission and the European GNSS Agency in different working groups, where he served as technical expert for Germany. He received his M.Sc. in Electrical Engineering from the Politecnico di Milano, Italy in 2006.*

Jean-Jacques Floch *obtained his Engineering diploma in Electronics and telecommunication at the "Institut Supérieur Electronique Numérique", in France in 1998. He has been working in the area of mobile communications for several years. Since 2002 he has been working in the field of navigation satellite as system engineer at the Astrium GmbH. His work mainly focuses on Galileo signal design at system level and evaluation of performances and robustness of Galileo signals.*

Matteo Paonni *is a Scientific Officer within the Directorate for Space, Security and Migration at the Joint Research Centre of the European Commission in Ispra, Italy. Under his position Matteo provides technical and policy support to the EU Satellite Navigation Programmes Directorate and to the European GNSS Agency. Matteo is involved since many years in the Galileo program and his main focus is on GNSS signal design and optimization, RF compatibility and signal processing. From 2007 to 2013 he was a research associate at the Institute of Space Technology and Space Applications at the University of the Federal Armed Forces in Munich.*

ABSTRACT

This article proposes a Time-Division-Multiplexing (TDM) technique applied at PRN code level as a signal design solution able to cope with the provision of several functionalities in one signal component: the allocation of the signal to the different functionalities is made at PRN code level. The functionalities targeted in this article are low-complexity acquisition, fast Time-To-First-Fix Data (TTFFD), Security Code Authentication (SCA) and, additionally, non-coherent signal processing. The interest of using a TDM component signal design lays on the introduction of just one new component to reduce the complexity to be added to the legacy GNSS satellite payload and to the GNSS receiver. Moreover, a TDM signal design solution presents a great flexibility able to adapt the signal design to the different GNSS strategic directives.

The TDM component is constituted of period blocks called short basic blocks and advanced blocks; the introduction of such blocks simplifies the TDM component processing by a GNSS receiver. The TDM component is divided first in a continuous stream of short basic blocks of 20ms, where the short basic blocks are used to provide a signal periodic structure for the acquisition functionality. Then, the short basic blocks are grouped in advanced blocks to provide the signal periodicity for fast TTFFD and SCA.

The low-complexity acquisition functionality is provided by the first PRN codes of a short basic block: PRN codes are selected to have a low duration and are always at the same position inside the block. Code Shift Keying Modulation is used to provide the fast TTFFD and the SCA key delivery.

An example of application on the Galileo E1 civil signals is presented with different target scenarios or type of users: low-complexity user, high performance – no TTFFD, high performance – TTFFD and high dynamics user.

INTRODUCTION

Global Navigation Satellite Systems are in constant evolution as the need for better positioning performance, more accurate, more reliable, etc., arises among the old and the new community of users. This exigence for evolving systems is not new as a quick look into the last decades shows: two new systems have been recently deployed, Galileo and Beidou, and systems evolutions for them as well as for the GPS and Glonass, the two oldest GNSS still in use, are being constantly developed.

Concerning the American system, the conception of the original Global Positioning System, GPS, was proposed in 1973 for the American military as a defensive system [1]. The GPS conception was materialized in 1978 with the launch of the first experimental Block-I GPS, and the GPS satellite constellation was completed in 17th of January of 1994 with the launch of the 24th satellite. The first GPS transmitted only one civil signal, GPS L1 C/A, and one military signal, GPS L1 P(Y). Focusing on the conception/evolution of the transmitted civil signals, in 1998, the U.S. congress decided to deploy two new civilian signals: the first one in the L2 frequency as an evolution/complement to the GPS L1 C/A signal to improve the navigation, positioning and time services [2], and the second one in the L5 frequency to provide for the needs of critical safety-of-life applications such as civil aviation [3]. These signals were called GPS L2C and L5 signals and the overall project was called GPS III. GPS L2C and GPS L5 signals, among other signal improvements, introduced the concept of pilot signal (or dataless) as well as a new navigation message structure with the introduction of channel codes for Forward Error Correction (FEC) purposes. Some years later, due to the continuous growth of positioning service demand in urban environments and in order to cope with some of the shortcomings of the GPS L1 C/A signal, a new GPS civilian signal, GPS L1C, in the same L1 band as GPS L1 C/A was developed and its specifications published in 2006 [4]. As of today, the deployment of the satellites broadcasting the evolved GPS signals is still process. For GPS L2C signal, 19 satellites already broadcast the signal and the Full Operation Capability (FOC) of 24 GPS satellites is expected in 2021 [5]. For GPS L5 signal, 12 satellites already broadcast the signal and the FOC of 24 GPS satellites is expected in 2024 [5]. Finally, for GPS L1C signal, the satellites' first launch should begin this year and the FOC should be reached in the late 2020s [5].

Concerning the Russian system, Glonass, its development began in 1976 just three years after the start of the GPS program [6]. The first satellite was launched in 1982 and the first FOC status was achieved in 1996 while the second and definitive one was reached in December 2011 after a previous decline of the system [6]. Focusing on the broadcast civil signals, with the system rebirth and in addition to the G1 legacy signal, a new civil signal in the G2 band was introduced with the first official satellites launches in 2005. Until 2013, the G1 and G2 civil signals were based on the FDMA technique, but since November 2014, another civil signal is being broadcast in the L3 band based on CDMA [6]. Moreover, the ICDs of two new civil signals in the G1 and G2 bands implementing the CDMA principle were published in 2016 [23]. Finally, further evolutions are expected for Glonass with the introduction of new civil CDMA-based signals transmitted on the L1 and L2 bands [6].

Concerning Galileo, the European Union identified the need to have its own GNSS in the 1990s. This need crystalized in the development of the first Galileo system generation and in the broadcasting of 3 civil signals, Galileo E1 OS, Galileo E5a and Galileo E5b, in the E1, E5a and E5b bands respectively. The conception of these signals was partially inspired in the design of the SBAS signal as well as on GPS L5 signal. The first Signal-in-Space (SiS) ICD was officially published in 2006 [7]. One of the main innovations brought by the Galileo signals was the introduction of the CBOC modulation for the E1 signal [7] (in coordination with GPS L1C signal definition) as well as the introduction of the AltBOC modulation which allowed the use of Galileo E15a and E5b as a unique signal, Galileo E5, for tracking purposes. Nowadays, Galileo, is close to reach the FOC which

should take place along 2020 [8]. At that moment, the Galileo programme will begin the transition towards the Galileo Second Generation (G2G), aiming to provide improved performance and added features.

Concerning the Chinese system, BeiDou, although this system was the last one to aim at a global coverage, its idea of conception was proposed in the 1980s with a regional coverage as objective. After the first experimental phase of the project from 1994 to 2003, called BDS-1, BeiDou entered the second phase which lasted to 2012 and was called BDS-2 [9]. Focusing on the civil signals, in the second phase two civil signals at 1561.098 MHz and at 1207.14 MHz, denoted as B1 and B2 signals respectively, were designed and the SiS ICD for the B1 signal was published in 2012 [10]; these signals had Galileo and GPS characteristics. Finally, the third phase, which started after the finalization of the second one and which aims at a global coverage, should be achieved along the year 2020 when the FOC of the system is expected with 35 in orbit satellites [9]. Concerning the civil signals, phase III satellites, also called BeiDou-III or BDS-3, broadcast new civil signals in slightly different bands in addition to the legacy signals: a B1 signal centered at 1575.42 MHz which should have a similar structure to GPS L1C with the introduction of a MBOC modulation and of a navigation message of similar length, a B2 signal centered at 1191.795 MHz which will use an AltBOC-inspired modulation, and a B3I signal centered at 1268.520 MHz. The official ICD for the first two signals was published at the end of 2017 [11][12] and the ICD for the last one in February 2018 [13].

The previous four paragraphs have shown the major efforts done by each one of the existing GNSS and their will to continuously improve the systems and their broadcast signals to provide for new user needs and for new user's communities, and even to follow specific strategic directives. Moreover, this quick look into history has also shown the very significant time interval between the design of new systems features, such as signals, and the time required to deploy new satellites containing such features. Therefore, in order to be able to cope with the future needs of positioning services, GNSS providers must anticipate them, must analyze if their current system is able to meet these needs and, in the event that they are not, must design new system solutions. For example, there have been a proposition to convert the GPS L1 C/A signal into a pure pilot signal [14]. Moreover, some studies have already been conducted about the implementation of an authentication feature in GNSS signals. GPS was the first system to analyze such possibility [14] and more propositions have been made along the years [16][17]. Galileo has also investigated such options with the inclusion of Navigation Message Authentication (NMA) even in the first system generation [18][19].

The aim of this paper consists thus in presenting a global signal solution able to cope with 3, present and future, user community needs identified through a user community survey and from the analysis of the current GNSS signals weak points: a low-complexity acquisition process, the provision of an authentication feature and a low Time-to-First-Fix Data (TTFFD) -the time required to recover the ephemeris for the first time. The signal solution targeted in this paper is the design of a Time Division Multiplexing (TDM) signal component which should be used in combination with the other existing legacy signals' components of the GNSS wanting to implement such solution.

The main motivations to select a TDM signal component as the preferred solution are the problems associated with the continuously increasing number of signals and signals components which are being broadcast by the different systems as the quick look in the different GNSS evolutions history has shown. First, one important trade-off on the design of new GNSS signals is the complexity added to the multiplexing scheme due to the inclusion of new signal components. As it is well known, in order to use the satellite payload's amplifier at its saturation point, an equivalent multiplexed signal with a constant envelope is required. However, with the introduction of new signals / signal components, the multiplexing scheme should become more complex and less efficient. Therefore, the number of new added component should be kept to a minimum if the multiplexing scheme complexity is desired to be minimized. Second, the introduction of new signal components implies an increase of the receiver complexity since new PRN codes will be implemented by the new components, since new correlator or correlations will have to be added to the receiver structure to process the new components and since even new chip modulation generations modules could be required. Therefore, to reduce the number of new signal components to be added should mitigate the receiver's complexity increase.

One important remark which must be made is that although the proposed TDM signal solution is suitable for any GNSS, the final signal conception will depend on the inspected GNSS. In this paper, to provide an example of application, the Galileo E1 civil signals have been selected as the legacy signals to add a TDM signal design targeting different functionalities.

This paper is structured as follows. First, a detailed motivation of the targeted functionalities will be provided in order to justify their selection. Second, the main motivations of using a TDM signal component as the signal design solution to target different functionalities is discussed. Third, the TDM general principle is detailed. Fourth, the TDM signal structure and, more specifically, the structure of the signal parts targeting the different functionalities, is described. Fifth, the figure of merit used to assess the

performance associated to each targeted functionality is presented. Sixth, an example of application of the TDM signal design on the Galileo E1 civil signals is made. Finally, the work is concluded.

Disclaimer: *The content of this paper represents the view of the authors that prepared it and is not related to any decision of the European Commission or of the Galileo Programme.*

DESCRIPTION AND MOTIVATION OF THE TARGETED FUNCTIONALITIES

The main targeted functionalities to be provided, or improved, with respect to the systems legacy signals, are given next:

- Low-complexity Acquisition process: To implement a robust acquisition process requiring the lowest possible number of operations.
- Fast TTFFD (Time-to-First-Fix Data): The TTFFD is the time required to recover the Clock error corrections and Ephemeris Data (CED) for the first time. For all GNSS, this time is always higher than 15-20 seconds which in most new applications is not an exploitable value.
- Security Code Authentication (SCA): SCA is defined as the act of confirming the identity of the received GNSS, belonging to the GNSS satellite provider, by verifying the received signal PRN. In this paper, the SCA description and analysis will mainly focus on the cryptographic key distribution; or in other word, the mechanism to transmit the keys. Moreover, the length of the security code will also be discussed.

Additionally, one last functionality could be targeted:

- Continuous or partial non-coherent signal processing: This functionality is defined as the possibility to allow the receiver to process the received GNSS signal without the need of tracking the signal carrier phase (without using a PLL): only the tracking of the signal carrier frequency is required (only using a FLL). If the receiver never requires tracking the signal carrier phase, the non-coherent signal processing is called *continuous* whereas if the receiver requires to punctually track the signal phase, the non-coherent signal processing is called *partial*.

The main motivations behind the implementation of each one of the previous functionalities are given next:

- Low-complexity Acquisition process: This functionality is already well covered for GPS with GPS L1 C/A signal. Therefore, the main motivations will be customized for Galileo. The first motivation is indeed to compete with GPS L1 C/A for being the dominant acquisition signal since nowadays, GNSS receivers usually acquire first GPS L1 C/A and then pass to process more sophisticated signals which include signals from other constellations. The second reason is the power consumption, mainly for mass-market receivers, cell-phones or the Internet-of-Things (IoT) devices: in order to increase their autonomy, the acquisition and re-acquisition process should be as simple as possible since these types of receivers do not continuously process the signal but just store the last samples and only process them when the user demands a PVT solution calculation. Moreover, if the receiver is limited in complexity and the power consumption is kept constant, the mean acquisition time (MAT) will probably be reduced if the acquisition process complexity is reduced as well since there is a trade-off between the receiver's complexity, the power consumption and the MAT. Finally, the addition of another pilot signal could be used to increase the tracking performance.
- Fast TTFFD: The main reason is to improve the system legacy signals TTFF Data which is currently too high to be exploited by modern positioning services and by some users' community. For example, for Galileo E1B legacy signal component, the TTFFD average value remains around 20s despite the proposed improvements such as the Reed-Solomon solution [21]. Note that this improvement is important for not-connected users but for connected ones as well, since there can always be a situation or a scenario where even the latter types of users cannot access the external links to obtain the predicted ephemeris. Moreover, the use of broadcast ephemeris instead of either predicted ephemeris or ephemeris obtained by external means allows the receiver to use corrections specially tailored for the broadcasted ephemeris (such as for SBAS or for online ARAIM). Finally, Safety-of-Life users require the use of broadcast ephemeris which are generated and authenticated by the GNSS system providers since they cannot use the information generated by external entities.
- Security Code Authentication (SCA): The main reason to provide authentication at the PRN code level is to force the spoofer to use dish antennas: assuming that the implemented SCA is cryptographically secure, if the spoofer does not use (a) dish antenna(s), he will not be able to successfully estimate in advance the security code and thus to successfully attack the receiver. Moreover, assuming that the GNSS already implements a NMA scheme, the introduction of a SCA scheme could further increase the NMA scheme robustness by binding the two schemes in time – time binding: the two authentication schemes must be attacked at the same time in order to be able to spoof the receiver; if not, one schema will help the other one to detect the attack [17][20].

- Continuous or partial non-coherent signal processing: The need for this functionality is focused on high dynamic users needs, probably in urban scenarios, since for these types of users it is quite challenging to obtain good carrier phase measurements allowing them to correctly exploit the GNSS signals.
  First, the inability to track the satellite's received signal carrier phase forbids the receiver to recover the information transmitted in the navigation message (NM). Nowadays, this handicap is currently mitigated by the possibility of getting the navigation message from external sources or from predicting the satellites ephemeris and by the fact that the navigation message information can only be required every two hours (CED time interval update). Nevertheless, due to the introduction of the authentication functionality, as for example it is planned for the NMA scheme of Galileo E1B, the interested users will need to have a continuous access to the keys released by the navigation message. Therefore, taking into account that it is still unclear if an alternative, reliable and authenticated communication channel will be established to broadcast the cryptographic keys, it can be concluded that providing the possibility to obtain the released keys without tracking the signal carrier phase could be significant advantage for a GNSS. Moreover, as stated before, there are benefits from obtaining the CED from the broadcast navigation message instead of from external sources or from predictions.
  Second, the current GNSS signals require to estimate the signal carrier phase in order to achieve the bit or the overlay code synchronization which will allow the receiver to apply the correlation process for a longer integration time (longer than the PRN code duration). Therefore, a signal not requiring the signal carrier phase estimation will enable the exploitation, or the fastest exploitation, of the signals code phase tracking full capacity in difficult signal reception conditions.
  Finally, it must be noted that the design of a signal providing partial or continuous non-coherent signal processing functionality will still allow the traditional coherent processing of the signal.

CONSTRAINTS OF THE INCLUSION OF NEW SIGNAL FUNCTIONALITIES

The main constraint imposed in this paper on the inclusion of new signal functionalities is to reduce as much as possible the impact on the GNSS satellite payload and on the receiver complexity.

First, in order to reduce the impact on the GNSS satellite payload, the number of new added signals or signal components must be as low as possible: traditionally GNSS satellites are equipped with one signal generation chain per frequency band which implies that all the signals and/or signal components sharing the same frequency band must use the same amplifier. However, in order to optimally use the amplifier, the input signal must be a constant envelope signal to allow the amplifier to be used at its saturation point. Therefore, previous to their pass through the amplifier, all the signals must be combined together to obtain a constant envelope signal. The techniques generating such a signal are called Constant Envelope Multiplexing (CEM) techniques and their efficiency is calculated by the ratio between addition of the useful signals-to-be-multiplexed power and the resulting signal power. This means that despite the generation of a constant envelope signal which can work at the amplifier's saturation point, part of the amplifier's power is not used on the useful signals due to the application of a CEM technique: the resulting signal has a constant envelope because inter-multiplexing terms are generated to obtain such property and take part of the amplifier's power. Finally, the efficiency of the CEM technique is related to the technique itself and to the number of signals components to be multiplexed; the efficiency decreases along the increase of the number of signal components.

Second, the introduction of a new signal or signal component implies that the GNSS receiver must be adapted to cope with its processing. First of all, the receiver must generate a new PRN code for each satellite of the constellation broadcasting the new signal component. Second, the receiver must increase the numbers of correlators or correlations chains in order to process the new signal components and, at least, this number must be equal to number of satellites which are in view, usually around 8 satellites. Third, when a new signal component is introduced, the new signal may or may not be modulated with a new chip modulation, since the introduction of a new chip modulation could limit the interference with other signals from the same or from other systems (intra- and inter-interference); and this means that a new module generating this chip modulation could be implemented. Therefore, it can be observed that the receiver complexity increases along the increase of the number of new signal components to be introduced.

To summarize, a signal solution technique allowing the implementation of new/improved functionalities requiring as few new signal components as possible should limit the GNSS satellite payload complexity increase and should limit the increase of the receiver complexity.

DESCRIPTION OF THE TDM SOLUTION

In order to design a signal with several functionalities, the Time Division Multiplexing (TDM) technique has been chosen as the preferred solution. The main reason for this choice is that one and only one new signal component is introduced to provide the different targeted functionalities and thus, the constraints presented in the previous section should be mitigated: to reduce as much as possible the impact on the GNSS satellite payload and on the receiver complexity. The fundamentals of the TDM technique proposed in this article will be presented next.

The main idea of the proposed TDM technique is to apply the time division technique at PRN code level: all the chips of a PRN code are associated to the same functionality, but each PRN code can be associated to a different functionality. Note that this implementation is different from the TDM technique applied in GPS L2C [22] and Glonass L1OC [23] where the time division was applied at chip level. The main advantage of PRN code TDM with respect to chip TDM is an a-priori lower complexity demanded to the receiver to process the former type of signal. However, chip TDM seems to present a higher signal design flexibility than PRN code TDM since the percentage of the TDM component assigned to one specific functionality must be a multiple of the TDM fundamental unit' size, chip or PRN code. Therefore, in this paper, the PRN code is selected to be equal to 1ms or 2ms to provide high flexibility to the final signal design.

When designing a new signal component, one method to facilitate its processing at the receiver end consist in constructing a periodic structure. For the PRN code TDM technique, the periodic structure can be based on the repetition of signal blocks where each block contains the same association between PRN codes and one targeted functionality. In this article these blocks are called *short basic blocks* and *advanced blocks*.

A short basic block is associated to the acquisition functionality. This block is defined as a signal block of 20ms and thus spans 20 PRN codes for a selected PRN code of 1ms. A block's length of 20ms has been chosen since this value is the usual maximum time duration used for coherent integration purposes and thus, it is well adapted for acquisition and tracking purposes. Therefore, the TDM signal can be interpreted as continuous flow of short basic blocks. Figure 1 shows an example of a short basic block with the assignment of its PRN codes to the different functionalities: the 20ms short basic block is divided into 20 PRN codes of 1ms each, the first 14 PRN codes are used for fast acquisition purposes, the 15th to 17th PRN codes are used for SCA purposes and the 18th to 20th PRN codes are used for fast TTFF Data purposes

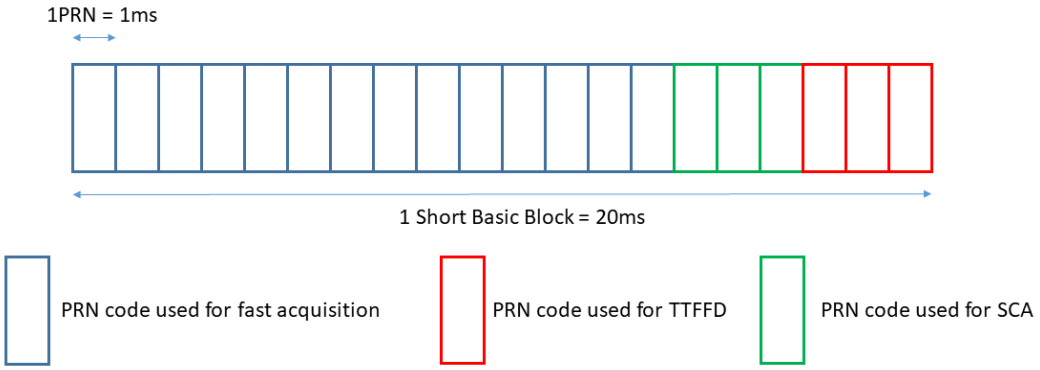

Figure 1: Example of short basic block spanning 20ms with PRN codes of 1ms length

An advanced block is associated to the fast TTFFD and SCA functionalities. An advanced block is constituted of several short basic blocks, where the PRN codes change their functionality assignment from short basic block to short basic block except for the PRN codes assigned to the acquisition functionality; therefore, the complete signal periodic structure is thus guaranteed by the advanced blocks. The duration of an advanced block is set to from 2 seconds up to 6 seconds, depending on the CED and SCA keys repetition rate. This means that the CED and SCA cryptographic keys codewords positions inside the signal are determined by the advanced blocks. Note that the introduction of advanced blocks allows to overcome the lack of flexibility of short basic blocks. Figure 2 presents a graphical example of a signal defined by using advanced blocks: in this example the last 3 PRN codes of each short basic block vary their assigned functionality: 1st and 3rd short basic blocks have the last 3 PRN codes targeting SCA functionality whereas the 2nd and last short basic block have the last 3 PRN codes targeting fast TTFF Data functionality.

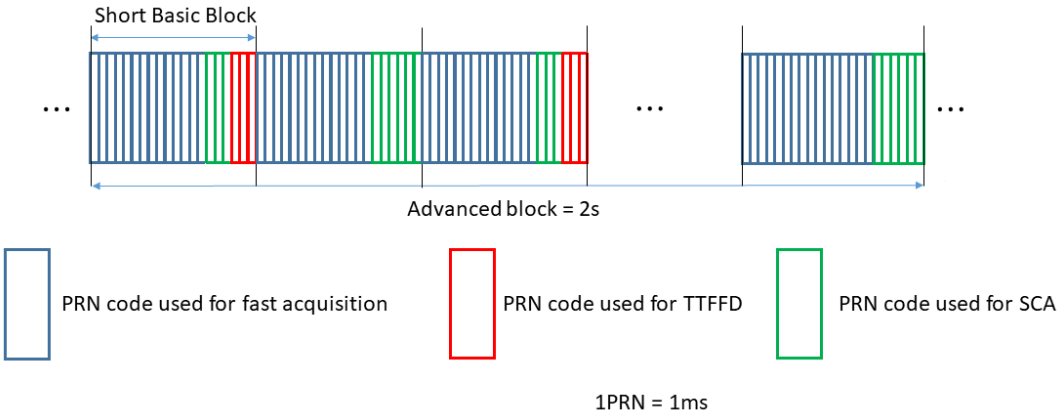

Figure 2: Example of a 2second advanced block providing several functionalities

Finally, it is important to remark that the introduction of short basic blocks is mainly necessary for the acquisition functionality. In fact, the PRN codes associated to the acquisition functionality have the PRN code assigned in every short basic block. Therefore, if the acquisition functionality is not targeted, the signal could be directly designed from advanced blocks. Moreover, in this event, longer PRN codes could also be chosen, such as 4ms duration PRN codes.

DESCRIPTION OF THE TDM SIGNAL STRUCTURE

In this section, the general structure of a TDM signal component is presented. The TDM signal structure is defined by the signals' parts providing the identified targeted functionalities: fast acquisition, fast TTFF Data and SCA scheme. Moreover, the TDM component must be designed in order to allow the non-coherent processing of the TDM component and the signal legacy components ensemble: this means that each signal part structure must be specifically adapted to the targeted functionality and must allow its non-coherent processing. Therefore, the first step towards the conception of the targeted TDM signal component consist in listing all the signal processes which require the estimation of the signal carrier phase:

- Overlay code synchronization / Bit synchronization
- Codeword synchronization
- Navigation message demodulation
- SCA keys demodulation
- SCA verification

From the previous list, it can be seen that a TDM signal component allowing a continuous signal processing must allow a non-coherent demodulation of the transmitted data and a non-coherent synchronization of the transmitted codeword or, in this article, of the advanced blocks (since they determine the codewords position). The solution chosen in this work to allow a non-coherent demodulation is the implementation of a CSK modulation [24][25] and the solution to allow a non-coherent codeword synchronization is the introduction of a non-coherent, CSK modulated, overlay sequence.

Therefore, taking into account the previous statements, the final list of general signal structures defining the targeted TDM signal component is:

- Low complexity Acquisition
- Fast TTFFD
- Non-coherent overlay sequence
- SCA: key delivery and GNSS Time
- SCA: encrypted spreading code

In the following subsections, the signal structure definition of each item of the list is given as well as a brief comment about their signal processing method.

Signal structure definition – Low complexity Acquisition
The signal part used to provide the fast acquisition functionality is defined by the short basic block, the number of PRN codes of the short basic block providing this functionality and the PRN code structure.

As discussed in the previous section, the short basic block structure has a length of 20ms and the number of PRN codes inside the basic block depends on the PRN code duration, 1 or 2ms, see Figure 1. Note that the PRN code duration, chip rate and chip modulation will determine the acquisition process complexity. Therefore, leaving up the chip rate and the chip modulation choice to each GNSS for interference constraints requirements, a small PRN code duration has been chosen in this work to minimize the acquisition process complexity. Nevertheless, note that the recommended value for the chip rate is 1 Mchip/s or lower and the recommended chip modulation is BPSK or BOC(1,1).

Coming back to the short basic block structure, its first X ms are always used for fast acquisition purposes and the remaining $(20 - X)$ ms are used for other objectives. From now on, a short basic block using the first X ms for fast acquisition purposes will be called *Acq X*. The PRN codes used for fast acquisition purposes always have the same polarity, or in other words, an overlay code is not implemented on them whereas the PRN codes not used for acquisition purposes are always CSK modulated, as commented on the following sub-sections. This means that although the CSK modulated PRN codes cannot be used for acquisition purposes, they are a priori transparent during the acquisition phase. Therefore, direct long coherent integrations of 20ms can be implemented since due to the lack of an overlay code and due to the presence of CSK modulated codes, there cannot be destructive combinations of PRN codes. Obviously, long coherent integrations should improve the acquisition robustness against the noise, which means that, in addition to allow the possibility of conducting a low complexity acquisition process, the TDM component will also allow for a more robust acquisition process. The short basic block characteristics are summarized in Table 1. Figure 2 provides a graphical example of a succession of short basic block codes of 20ms with primary PRN codes of 1ms and with the first 14ms being used for acquisition purposes; using the proposed notation, this type of structure is denoted as *Acq 14*.

Short basic block length	20ms
Number of ms used for acquisition purposes	X – Notation: Acq X
Position of the ms inside the short basic block	Beginning
PRN code characteristics	1-2ms
PRN codes polarity	Always the same – No overlay code

Table 1: Short basic block characteristics for providing low complexity acquisition

Different methods can be applied to acquire the TDM signal component. Three are briefly commented in this article, the classic method, the minimum method and the maximum method. The minimum and maximum methods are designed to be applied specifically on the TDM component since they take into account its specific structure, whereas the classic method can be applied to the TDM component plus the legacy components. The minimum method has as objective a low complexity acquisition and thus conducts coherent correlations of 1ms and non-coherent accumulations of 1ms; moreover, note that smart accumulations can be made where the correlations over the CSK modulated PRN codes can be excluded. The maximum method has as objective to provide a robust acquisition performance, low detection probability threshold, and thus conducts coherent integrations of 20ms and non-coherent accumulations of 20ms; again, note that smart blanks can be input to the correlation to avoid the CSK modulated PRN codes. Finally, in this paper, the classic method denotes the *Y*ms+*Y*ms method [26], with coherent effective accumulations of *Y*ms and non-coherent accumulation of *Y*ms as well; this method targets the combination of the TDM component and the legacy components for acquisition purposes. For example, for Galileo E1 civil signal, the *Yms* value is set to 4ms which is the PRN code duration. Finally, it is important to note that whereas the minimum method is the recommended method for the low complexity acquisition, the classic and maximum methods compete in terms of acquisition performance, acquisition probability for a given C/N_0 value, to be the predominant high sensitivity acquisition method (see appendix Table 9).

Signal structure definition – Fast TTFFD
The signal part in charge of providing the fast TTFFD is described in this section. The elements defining the signal part in charge of providing the fast TTFFD are the codeword content, data modulation, codeword structure and the codeword repetition rate.

The codeword content is only the CED information. First, this information must be received to obtain a first fix. Second, if a fast TTFF Data objective is imposed, a fast repetition of the codewords allowing the accumulation of received codewords is necessary. And to allow such accumulation, the received codewords must contain only information which is repeated.

The modulation of the transmitted data is imposed by the fast TTFF data objective as well as for the non-coherent processing (demodulation) objective. First, in order to have fast TTFFD, short codewords in time are needed, which implies a high useful data rate. And, in its turn, a high useful data rate implies short BPSK symbols or a higher order data modulation. Second, in order to allow a successful non-coherent data demodulation process, the implemented modulation cannot depend on the estimation of the signal carrier phase. A solution fulfilling both needs is the use of a CSK modulation which provides useful high data rates as well as the option of implementing a non-coherent demodulation.

The codeword structure is defined by the channel code applied to the CED information. The selected channel code depends on the information word size and on the data modulation. Therefore, in this article, a LDPC(1000, 500) ARB50 channel code has been implemented [27]. This channel code is specially designed to be implemented in a CSK modulation and presents a good compromise between users using iterative decoding (BICM-ID) and users using classic decoding (BICM) [27]. Note that LDPC channel codes presenting better results than the selected code for BICM-ID decoding have also been developed [27]; nevertheless, it is uncertain if all users will choose to implement a high-complexity iterative decoding instead of a less-complex classic decoding, such as mass-market or IoT devices. Therefore, a channel code providing a good compromise for both type of decoding algorithms has been selected.

Finally, the repetition rate of the CED codeword is set to 1, 2 or 3 seconds since the TTFFD decreases along the CED codeword repetition.

Table 2 presents a summary of the signal structure characteristics, where the CED size is the one used for Galileo E1B signal. Table 3 presents the different number of CSK symbols necessary to transport the 1000 bits codeword as a function of the CSK modulation order.

Initial CED size	496 bits
Considered size	500 bits
Selected Channel code	LDPC(1000,500) ARB50
Data Modulation	Code Cyclick Shift Keying (CSK) Modulation

Table 2: Characteristics of Clock error correction and Ephemeris Data (CED) codeword

Bits per CSK symbol	**10**	**9**	**8**	**7**	**6**	**5**
Number of symbols per CW	100	112	125	143	167	200

Table 3: CED codeword number of symbols as a function of the selected CSK modulation order

The association between the symbols and the short basic block structure is made following a set of specific rules:

- Every symbol is represented by 1 or more than 1 PRN code of the short basic block structure.
- All the symbols are represented by the same number of PRN codes (they have the same duration).
- The position of the PRN codes associated to a symbol of the CED word can vary from short basic block to short basic block.
- The position of the PRN codes associated to a symbol of the CED word is the same from advanced to advanced block

The methods proposed to recover the CED information are the BICM and BICM-ID demodulation/decoding algorithms [24] while the accumulation of words is taken into account at the loglikelihood ratio level. Moreover, the demodulation algorithms can be applied in a coherent [24] or in a non-coherent manner [28].

Signal structure definition – Non-coherent synchronization overlay sequence

The fundamental or principle of a synchronization technique consists in sending a known data sequence inside the stream of bits (data component) or in a completely different component (pilot component). For every designed GNSS signal, the overlay code chips or the data bits are phase modulated, BPSK modulation, and thus, a coherent synchronization method is required. A non-coherent synchronization block sequence/method pair consists in essentially the same: to transmit a known sequence where the

secondary code chips are modulated by a modulation which allows a non-coherent demodulation/detection; for example, a CSK modulation.

A general implementation of an overlay synchronization sequence allowing a non-coherent synchronization is the following one:

- A specific synchronization sequence is modulated with a CSK modulation.
- The synchronization sequence has a period equal to the block to be synchronized; in this case an advanced block.
- The number of symbols required to encode the synchronization sequence goes from 1 symbol to the number of PRN codes inside the block.

Finally, it is important to note that in order to avoid the interference between the CED codeword CSK data symbols and the CSK non-coherent overlay sequence, a smart global CSK mapping must be made. The optimal solution will consist in having two disjoint CSK mappings knowing that both CSK modulation use the same fundamental PRN code: CSK symbols used for the CED codeword cannot be used for the non-coherent overlay synchronization sequence.

The method proposed to identify the non-coherent overlay synchronization sequence inside the continuous stream of PRN codes consist first, in interpreting the different shifts of the non-coherent sequence inside an advanced block as different symbols of an orthogonal M-ary modulation, and second, in applying a MAP symbol estimator of an orthogonal M-ary modulation [29]. This method assumes that short basic blocks have already been synchronized and that the non-coherent synchronization sequence pattern inside an advanced, position and symbols values, is known.

Signal structure definition – SCA Cryptographic Key Delivery and GNSS Time

This signal part is designed to transmit the SCA cryptographic keys as well as the GNSS time. The codeword transmitting this information has a repetition rate set to 2s in order to provide even to the most exigent applications with a very fast Time-Between-Authentications (TBA). The size of the cryptographic key has been set to around 381 bits since around 384 bits are necessary for a protection to potential quantum computer attacks [30]. The GNSS time is represent by 19 bits for a total information message size of 400 bits. The channel code selected to protect the codeword is the LDPC(800,400) ARB50 channel code [27] which is specially designed to be implemented in a CSK modulation and presents a good compromise between BICM-ID and BICM decoding algorithms. A summary of the signal structure characteristics is given in Table 4.

Information Word size	***Channel code***
400 bits	LDPC(800,400) ARB50

Table 4: Characteristics of the SCA cryptographic keys codeword

A CSK modulation is implemented in order to allow for a fast data transmission, for a low percentage of occupation of the TDM component and for the possibility to implement a non-coherent demodulation process. Moreover, in order to maximize the probability of recovery of the transmitted key (and GNSS time), the codeword containing this information can be sent more than once. The idea behind the multiple codeword retransmissions is to increase the time diversity of the information and thus to mitigate the bad signal receptions conditions introduced by the propagation channel. For this signal design and in order to still keep the (TBA) equal to 2s, only the following cases will be considered: the codeword is transmitted either only once or twice. Moreover, note that the codewords containing the key must always be broadcast after the security code transmission.

Important remark: In order to maximize the probability of recovering the cryptographic keys for all the satellites, a TESLA key chain must be implemented [31]. The principle of a TESLA key chain is that from key n, a secure one-way operation is applied to obtain key $(n+1)$ (key n cannot be obtained from key $(n+1)$, this operation is assumed to be not computationally feasible), and thus, a one-way time key chain can be created: having a key $(n+m)$ as trusted key at epoch t, the receiver is able to verify the authenticity of the received key n' at epoch $t+k$, if the result of applying k times the secure one-way operation to key n' results in key $(n+m)$. Therefore, using the TESLA key principle, the probability of recovering the cryptographic keys for all the satellites can be improved if at epoch t, the cryptographic key of satellite i is $(n(t)+i)$ but the satellite transmits the TESLA key $n(t)$ instead; then, if the same principle is applied to the other satellites, the recovery of TESLA key $n(t)$ at epoch t by means of any satellite link would allow the generation of the cryptographic keys at epoch t of all the satellites: to recover key $(n(t)+i)$ the one-way secure function must be applied i times to received key $n(t)$.

The method proposed to recover the cryptographic key transmitted by the TDM component should exploit the shared TESLA key chain of the broadcasting satellites. Therefore, instead of demodulating/decoding each message independently, a receiver should demodulate/decode them jointly. The proposed method consists thus on the following steps:

1) To calculate the joint coherent or non-coherent log-likelihood ratio of the key codeword from the symbols received from all the constellation satellites in view.
2) To apply the BICM or BICM-ID decoding algorithms.
3) To re-apply steps 1 and 2 if the codeword is transmitted for a second time.

Signal structure definition – SCA: Encrypted Spreading Code

This article does not focus on the complete SCA scheme and thus, no specific explanation will be provided about its structure. Nevertheless, the reader is referred to [20] to find a SCA scheme which suits the TBA value of 2 seconds adopted in this work. The only SCA scheme characteristics which are targeted, and thus commented, are the signal structure implemented to deliver the cryptographic keys and the number of milliseconds inside an advanced block which should be provided to the security code. The key delivery structure was explained previously and thus this section will comment only on the security code time characteristics.

A security code generated by a new cryptographic key must be transmitted at least once during the duration of an advanced block; therefore, in this case a new security code must generated every 2 seconds. Moreover, the security code must share the TDM component with the signal parts targeting other functionalities. This means that the security code will not probably be transmitted continuously but in bursts where the bursts length has a major impact on the security code non-coherent verification process: whereas for a coherent verification the entire security code can be coherently accumulated, for a non-coherent verification non-coherent accumulations of PRN code bursts must be conducted. Note that instead of burst, the term time-symbol or symbol could be used.

Another important characteristic of the security code is its total length. The total length can be calculated by multiplying the burst length by the number of bursts and has two impacts on the verification process. First, the security code length is proportional to the security code energy where a high energy means a higher probability of having a successfully verification when the true security code was received. Second, a longer length may imply that the verification process is most robust to signal outages since there is a higher probability that part of the security code can still be received in good reception signal conditions.

Finally, the last important characteristic of the security code is the power at which the code is transmitted. In this analysis, only the inclusion of the security code in the TDM component will be presented, which means a high-power component in this case. A high-power component implies a higher possibility of a successful key recovery but is also weaker to spoofing attacks; the size of the spoofer dish antenna required to successfully guess the security code is smaller. Therefore, the best solution should probably be the additional inclusion of a low power component only containing a very long security code [20]. Nevertheless, internal analyses have shown that such a component is not well suited for a non-coherent verification process.

The method proposed to apply the SCA verification process is to conduct a Neyman-Pearson test to the correlation output between the received security code and the local generated security code. The correlation process differs between the coherent and non-coherent verification processes and thus the a priori calculated threshold to obtain a given probability of false alarm is different as well.

FUNCTIONALITIES PERFORMANCE DESCRIPTION

In this section, the performance analyzed for the different targeted functionalities and signal parts are presented. The performance is calculated for the methods presented for each one of the signal parts and they are the basis of the example of application presented in the next section. However, no numerical values are presented in this section since they are outside the scope of this article, only performance values are given for the final signal candidates of the example of application (see appendix).

Acquisition performance analysis

Two different acquisition performance figures of merit are calculated for the acquisition signal part. The first one is the number of operations required to conduct the different acquisition methods, minimum, maximum and classic. This figure of merit will allow to provide a relative complexity performance between the analyzed methods and the application of the classic method to GNSS legacy components only.

The second figure of merit is the acquisition sensitivity to obtain a probability of detection equal to 95% or 99% with a probability of false alarm equal to the inverse of the total number of cells/combinations to inspect. This figure of merit should provide the method providing the best acquisition sensitivity (lower threshold). However, it must be remained that the TDM component has as target to complement existing legacy signals. Therefore, on possible signal design solution would be to provide part of the new additional amount of power to the legacy signals instead of providing all the new amount of power to the TDM component. Therefore, the classic acquisition sensitivity figure of merit is not well adapted since it does not take into account that the minimum and the maximum methods can only be applied on the TDM component while the classic method can be jointly applied to the TDM component and the legacy signals. To overcome this problem, this analysis has used as figure of merit an acquisition sensitivity normalized to the GNSS legacy components power. This performance was calculated assuming an AWGN channel.

Time-To First-Fix Data performance analysis
The figure of merit used to quantify the performance of the fast TTFF data functionality are the statistics of the TTFF data:

- Average: mean time to recover the CED information for the first time.
- 95% value: 95% of the time, the TTFFD will be lower than this value.
- Maximum value: the maximum TTFFD value that a user could expect.

The TTFFD statistics are presented for a user in an urban environment, modelled by a 2-states mobile channel, where the user moves at 2 different speeds, a pedestrian user at a 5 km/h and a car user at a 50 km/h.

Non-coherent overlay sequence synchronization performance analysis
The figure of merit used to quantify the synchronization process performance of the non-coherent overlay sequence is the probability of wrongly identifying the position of the sequence inside an advanced block, which can also be called probability of miss detection. The inspected propagation channel is an AWGN channel.

Authentication performance analysis – Keys Demodulation
The figure of merit used to determine the performance of the SCA key delivery is the probability of wrongly demodulating the key codeword, or, in other words, the key codeword error rate (or word error rate, WER). The inspected users and the propagation channels mathematical models are the same as for the TTFFD analysis: pedestrian and car user and a 2-states mobile channel.

However, it is important to remark that the conducted analysis represent the reception of *ONE AND ONLY ONE* satellite link; which means that the shared TESLA key chain property has not yet been exploited.

Authentication performance analysis – SCA Verification
The figure of merit used to determine the performance of the encrypted code verification process is the probability of miss-authentication: the probability of failing to verify the authenticity of the security code when the true security code was received. The inspected users and the propagation channels mathematical models are the same as for the TTFFD analysis: pedestrian and car user and a 2-states mobile channel.

EXAMPLE OF APPLICATION – GALILEO E1 CIVIL SIGNALS

In this section, an example of application of the TDM signal design solution is presented. The targeted GNSS and signals are the Galileo system and the Galileo E1 civil signals.

The main objective of this example is first to illustrate the potential of the TDM signal design solution to cope with different functionalities with just one signal component and second, to show the flexibility of the solution to adapt the final signal design to different high-level strategic directives: which types of users or which functionalities are privileged with respect to the others.

In this section, first the type of different scenarios which could be strategically targeted by the GNSS provider are presented. Second, high-level TDM signal design options are presented. The high-level options represent possible high-level conception decisions which could be applied to the TDM signal design such as the allocation of the extra power between the TDM component and legacy components, and which functionalities are directly discarded from the design. From each high-level design option, a couple of low-level signal designs were derived presenting the best signal performance; nevertheless, the derivation is not

presented in this article. Third, the methodology used to identify the best low-level signal design option to each scenario is presented. Finally, the identified low-level signal designs are briefly presented.

Description of Types of users/Scenarios

Four types of users or scenarios where identified as potential targets: low complexity scenario, high performance – no TTFFD scenario, high performance – TTFFD scenario and high dynamic user scenario. A better description of each scenario is given next.

1) Low complexity: This scenario accords more importance to a signal design which will allow a receiver complexity as low as possible. Therefore, it can target IoT devices or cheap mass-market receivers.
2) High Performance – No TTFFD: This scenario represents the case of users targeting the best possible performance without giving too much importance to the required receiver complexity. This scenario could represent car users or high sensitivity receivers. However, in this scenario, the CED information is not assumed to be obtained through the new component: the CED is recovered either using Galileo E1B or and external source.
3) High Performance – TTFFD: This scenario is essentially the same as before but in this case the users are interested in receiving the Galileo satellites ephemeris from the TDM signal component. Such users could be RPAS (Remote Pilot Air System), etc.
4) High Dynamic users: The scenario represents users with high dynamics which could require to use the non-coherent processing mode of the Galileo E1 civil signals in order to ensure a high continuity or availability of the service. Such users could be cellphone users.

Initial Signal Options

The design of a TDM signal component will depend on the targeted functionalities and on the power allocated to the TDM component. First, not all the identified functionalities must be provided by the TDM component, in fact, their relevance and their inclusion on the final design will depend on the GNSS strategic directive. Second, the power allocated to the TDM component could be provided to the legacy signal components: there is a trade-off between the allocation of the new amount of power between the new TDM component and the legacy signal components. Therefore, several high-level options can be identified depending on these two high level choices.

Concerning the functionalities, the TDM component always provides SCA but the provision of acquisition or TTFFD will depend on the signal option. Concerning the signal power, TDM component has always allocated the same power as Galileo E1B or E1C. Moreover, some signal options have 3dB of extra power which can be allocated to either the TDM component, to the legacy signal components or to both. Table 5 presents the summary of high-level signal design options.

Option	***SCA scheme complexity***	***TDM provides***		***C/N0 (dB-Hz)***		***Total power***
		Acquisition	***TTFFD***	***Legacy E1 (E1B+E1C)***	***TDM***	
1.1	Low	No	No	40	37	C
1.2	Low	Yes	No	40	40	$C + 3dB$
1.3	Low	No	No	41.764	37	$C + 3dB$
2.1	High	Yes	No	40	37	C
2.2	High	Yes	No	40	40	$C + 3dB$
3.1	High	No	Yes	40	37	C
3.2	High	No	Yes	40	40	$C + 3dB$
4.1	High	Yes	Yes	40	37	C
4.2	High	Yes	Yes	40	40	$C + 3dB$
4.3	High	No	Yes	41.764	37	$C + 3dB$
4.4	High	No	Yes	40-41.764	37-40	$C + 3dB$

Table 5: Summary of the characteristics of the high-level design options chosen for adding SCA, low complexity acquisition and fast TTFFD to Galileo E1 civil signals

- Table remark 1: the SCA scheme chosen as example for options 1.1, 1.2 and 1.3 in this work is defined in [20]. The particularity of this scheme is that allows for two types of authentication procedures, one less secure but with a low-complexity level, and another more secure but with a high-complexity level. Therefore, this scheme is adapted for the low complexity scenario. The SCA scheme chosen for the remaining options is a typical SCA security code with a high level of complexity.

- Table remark 2: An effective C/N_0 value of 40 dB-Hz is assumed for the Galileo E1B or E1C legacy signals [21]. An effective C/N_0 represents the C/N_0 when considering an open sky propagation channel. For the simulations results, an instantaneous fading was introduced to take into account the signal propagation through a mobile channel.

Then, from each one of these high-level signal design options, one or two low-level design options were generated: PRN length (1 or 2ms), number of PRN codes of a short basic block used for acquisition purposes, CSK modulation order and number of PRN codes constituting a symbol for TTFFD signal part, time signal characteristics, etc.

Finally, the best signal design option for each one of the identified scenarios in the previous section was selected by using a trade-off method presented in the next subsection.

Methodology

The method used to select the low-level signal design option best suiting each one of the identified scenarios consists in conducting a trade-off analysis by using a variation of the Analytical Hierarchy Process (AHP) / pairwise comparison method.

1) Select the high-level system operational requirement to be analyzed: To design a TDM component which provides SCA, low-complexity acquisition and fast TTFFD functionalities.
2) Select the Evaluation criteria: To allocate points to signal performance levels. The list of evaluation criteria is: Normalized acquisition Sensitivity, Acquisition complexity, TTFFD (Coherent Demodulation – 5 and 50 km/h, Non-coherent Demodulation – 5 and 50 km/h), SCA verification (Coherent Demodulation – 5 and 50 km/h, Non-coherent Demodulation – 5 and 50 km/h) SCA verification process complexity, SCA Key Delivery (Coherent Demodulation – 5 and 50 km/h, Non-coherent Demodulation – 5 and 50 km/h) and total allocated signal power. Several levels are defined per each performance and points from 0 to 5 are allocated.
3) Select the Weighting on Evaluation Criteria: To allocate more weight to a given criterion depending on the targeted scenario. For the low complexity scenario, the criteria which are prioritized are the acquisition and SCA verification process complexity. For the High Performance – No TTFFD scenario, the normalized acquisition sensitivity and the SCA coherent processes are given more weight. For the High Performance – TTFFD scenario, the same criteria as before are privileged plus the coherent TTFFD performance. Finally, for high dynamic users, more weight is given to all the non-coherent processes.
4) Select Candidate Solutions: The selected signal candidates are the low-level signal solutions derived in the previous sub-section
5) Rate Each Candidate Against Evaluation Criteria
6) Determine the Preferred Solution: For each scenario a different solution was identified.

Results and Observations

After applying the proposed method, the following results were obtained. For low complexity scenario, solution 1.2 was selected. For High Performance – No TTFFD scenario, solution 2.2 was selected. For High Performance – TTFFD scenario, solution 4.3 was selected. For High Dynamics user scenario, solution 4.4. was selected. In appendix, the signal characteristics as well as the signal performance for High Performance – No TTFFD scenario solution 2.2 and High Dynamics user scenario solution 4.4 are presented. From the results presented in the appendix several conclusions can be extracted.

Concerning the High Performance – TTFFD scenario, the signal design was optimized to have 60% of the component reserved to provide acquisition functionality and around 36% to SCA. Several observations can be made. First, it can be seen that even with only 60% of the signal space, the acquisition performance obtained using only the TDM component with the maximum method is the same as the performance of the classic acquisition method (which uses the 3 components); and when the receiver does not generate a CBOC local replica, the maximum method always outperforms the classic method. Moreover, the TDM component allows a low-complexity acquisition process. Therefore, it could be seen that the proposed acquisition structure inside the TDM structure was well optimized. Second, even with only 32% of the time, the SCA key distribution can be guaranteed with a good

probability when the iterative decoding method is implemented; besides, the results are presented for one and only one satellite link and thus, they should be greatly improved when taking into account all the satellite links (joint processing). Therefore, in general, it could be concluded that the use of a TDM component satisfactorily addressed the targeted scenario.

Concerning, the High Dynamics scenario, the signal was optimized to have 40% of the component reserved for the TTFFD functionality, around 54% to SCA and 0% to acquisition. Several observations can be made. First, the main reason to not provide any signal space to acquisition was that a low-complexity process was not a driving factor and too much signal space had to be provided to the acquisition to obtain performance at the same level or better than providing just energy to the legacy signals (taking into account that signal space must be reserved for the other two functionalities). Second, only proving 40% of the signal space to TTFFD functionally is enough to provide very good average values of less than 2 seconds for 50 km/h users and about 5-6s for 5 km/h users. Therefore, it can be concluded that the proposed TDM signal component structure perfectly provides this functionality. Third, looking at the SCA key delivery performance, good performance values were obtained for the iterative decoding when one and only one satellite link was used and thus, they should be greatly improved when taking into account all the satellite links (joint processing). Therefore, as well as stated for the previous commented scenario, it could be concluded that the use of a TDM component satisfactorily addressed the targeted scenario.

Finally, from the application of this example, it can be observed that the TDM technique applied at a PRN code level allows for a great signal design flexibility to accommodate different functionalities in just one component and allows to privilege some of these functionalities to follow high level system strategic directives.

CONCLUSIONS

In this article, Time-Division-Multiplexing (TDM) technique applied at code level has been presented and proposed as a potential signal design solution to target different functionalities. The TDM technique has been presented as a complement to the existing legacy signals of a GNSS rather than a standalone solution; therefore, TDM technique should also be used for overcoming legacy signal weak points.

The main reason behind the proposal of the TDM technique is to be able to provision new functionalities and to overcome legacy signal weak points with just the introduction of one and only one signal component. The effects of just introducing one new signal component are first the mitigation of the GNSS satellite payload complexity: to limit the constant envelope multiplexing (CEM) technique complexity and thus reducing its loss of its efficiency with respect to the legacy signal component multiplexing only. Second, the limitation of the number of new components to broadcast should limit the receiver complexity increase.

Moreover, in this article, the structures of the TDM signal parts responsible to provide the different functionalities have been defined. The targeted functionalities were low-complexity acquisition, fast Time-To-First-Fix Data (TTFFD) and Security Code Authentication (SCA). Additionally, non-coherent processing of the signal was targeted as well.

Finally, an example of application on the Galileo E1 civil signals was made. This example showed the TDM technique potential and flexibility to accommodate different signals design that prioritize some functionalities with respect to others.

ACKNOWLEDGMENTS

This article presents some findings of the Future Navigation and Timing Evolved Signals (FUNTIMES) project funded by the European Commission under the Horizon 2020 Framework Program (Funding Reference No. 435/PP/GRO/RCH/15/8384).

REFERENCES

1. Parkinson B.W., Stansell T., Beard R., Gromov K., “A history of satellite navigation”, *Navigation ISSN 0028-1522*, 1995
2. Gore A., “Enhancement to the Global Positioning System that will benefit civilian users worldwide”, March 30, 1998
3. Gore A., “New Global Positioning System Modernization Initiative”, January 25, 1999
4. ARINC Engineering Services, “Navstar GPS space Segment/User segment L1C interfaces, Draft IS-GPS-800”, Aug 04, 2006
5. Web page: https://www.gps.gov/systems/gps/modernization/civilsignals/
6. Langley R.B., “Innovation: GLONASS — past, present and future”, *GPS World*, November 1, 2017, http://gpsworld.com/innovation-glonass-past-present-and-future/

7. European Space Agency, “Galileo OS SIS ICD Draft 1”, February 2008
8. European Commission, “Regulation (EU) No 1285/2013 of the European Parliament and of the Council of 11 December 2013 on the implementation and exploitation of European satellite navigation systems and repealing Council Regulation (EC) No 876/2002 and Regulation (EC) No 683/2008 of the European Parliament and of the Council”, December 11, 2013
9. The State Council Information Office of the People’s Republic of China, “China’s BeiDou Navigation Satellite System”, June 2016.
10. China Satellite Navigation Office, “BeiDou Navigation Satellite System Signal In Space Interface Control Document – Open Service Signal (Version 1.0)”, December 27, 2012
11. China Satellite Navigation Office, “BeiDou Navigation Satellite System Signal In Space Interface Control Document – Open Service Signal B1C (Version 1.0)”, December 2017
12. China Satellite Navigation Office, “BeiDou Navigation Satellite System Signal In Space Interface Control Document – Open Service Signal B2A (Version 1.0)”, December 2017
13. China Satellite Navigation Office, “BeiDou Navigation Satellite System Signal In Space Interface Control Document – Open Service Signal B3I (Version 1.0)”, February 2018
14. Stansell, Thomas A., Betz, John W., van Diggelen, Frank, Kogure, Satoshi, "Proposed Evolution of the C/A Signal," *Proceedings of the 28th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2015)*, Tampa, Florida, September 2015, pp. 1807-1825.
15. Scott, L., "Anti-Spoofing & Authenticated Signal Architectures for Civil Navigation Systems," *Proceedings of the 16th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS/GNSS 2003)*, Portland, OR, September 2003, pp. 1543-1552.Oregon Convention Center
16. Wesson, K., Rothlisberger, M., Humphreys, T., "Practical Cryptographic Civil GPS Signal Authentication", *NAVIGATION, Journal of The Institute of Navigation*, Vol. 59, No. 3, Fall 2012, pp. 177-193.
17. Anderson, Jon M., Carroll, Katherine L., DeVilbiss, Nathan P., Gillis, James T., Hinks, Joanna C., O’Hanlon, Brady W., Rushanan, Joseph J., Scott, Logan, Yazdi, Renee A., "Chips-Message Robust Authentication (Chimera) for GPS Civilian Signals," *Proceedings of the 30th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2017)*, Portland, Oregon, September 2017, pp. 2388-2416.
18. European Commission, “Galileo Navigation Message Authentication Specification for Signal-In-Space Testing – v1.0”, 2016
19. Fernández-Hernández I. and G. Seco-Granados, "Galileo NMA signal unpredictability and anti-replay protection," *2016 International Conference on Localization and GNSS (ICL-GNSS)*, Barcelona, 2016, pp. 1-5.
20. Motella, Beatrice, Margaria, Davide, Paonni, Matteo, "SNAP: An Authentication Concept for the Galileo Open Service," *Proceedings of IEEE/ION PLANS 2018*, Monterey, CA, April 2018, pp. 967-977.
21. Schotsch, Birgit E., Anghileri, Marco, Ouedraogo, Mahamoudou, Burger, Thomas, "Joint Time-to-CED Reduction and Improvement of CED Robustness in the Galileo I/NAV Message," *Proceedings of the 30th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2017)*, Portland, Oregon, September 2017, pp. 1544-1558.
22. ARINC Engineering Services, “Navstar GPS space Segment/ Navigation User Interfaces, Draft IS-GPS-200H”, September 24, 2013
23. Russian Space System, “Interface Control Document - Code Division Multiple Access Open Service Navigation Signal in L1 frequency band - Edition 1.0”, 2016
24. Garcia-Pena, A., Salos, D., Julien, O., Ries, L., Grelier, T., "Analysis of the use of CSK for Future GNSS Signals," *Proceedings of the 26th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2013)*, Nashville, TN, September 2013, pp. 1461-1479.
25. Garcia-Peña A., Aubault-Roudier M., Ries L., Boucheret M.-L., Poulliat C., Julien O. and Hein G., “Code Shift Keying - Prospects for Improving GNSS Signal Design,” *Inside GNSS,Nov./Dec. 2015*, pp. 52-62
26. C. Yang, C. Hegarty and M. Tran, “Acquisition of the GPS L5 Signal Using Coherent Combining of I5 and Q5”, *Proceedings of the 17th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2004)*, Long Beach, CA (USA), September 2004, pp. 2184 – 2195.
27. Chauvat R., Garcia-Pena A., Anghileri M., Floch J-J., Paonni M., “Ultra Sparse Binary LDPC Codes with CSK Signals for Increased Data Rates in Future GNSS”, *2018 9th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, ESA/ESTEC, The Netherlands, December 2018
28. Garcia-Pena A., Paimblanc P., Julien O., Ries L., Grelier T.“Analysis of different CSK configurations in an urban environment when using non-coherent demodulation”, *Navitec – Conference article*, ESA/ESTEC, The Netherlands, December 2014
29. Proakis J.G. and Salehi M., “Digital Communications – 5th Edition”, *McGrawhill International Edition*, 2008

30. Neish, Andrew, Walter, Todd, Enge, Per, "Quantum Resistant Authentication Algorithms for Satellite-Based Augmentation Systems," *Proceedings of the 2018 International Technical Meeting of The Institute of Navigation*, Reston, Virginia, January 2018, pp. 365-379.
31. Perrig A., Canetti R., Tygar J.D. and Song D., "Efficient authentication and signing of multicast streams over lossy channels," *Proceeding 2000 IEEE Symposium on Security and Privacy. S&P 2000*, Berkeley, CA, USA, 2000, pp. 56-73.

APPENDIX A

In this appendix the signal design characteristics and the signal performance of the signals design solutions chosen for the High Performance – No TTFFD scenario, Table 6 to Table 12, and High Dynamics user scenario, Table 13 to Table 20, are presented.

Table 6 and Table 13 present the assumptions made on the received C/N_0. Table 7 and Table 14 present the general signal characteristics whereas Table 8 and Table 15 present the signal time structure. Table 9 and Table 16 present the acquisition sensitivity normalized to the Galileo E1 civil legacy signals power results, or in other words, they present the maximum acceptable decrease of the received signal power (expressed in dBs), with respect to Galileo E1 civil signals, which still allows to obtain the same probability of detection as the Galileo E1 civil legacy signals when taking into account the new signals power distribution (to the TDM component and to the legacy signals). The results are presented for the classic method, combining E1B+E1C+TDM, and the maximum method, only using TDM component, and for the case where the receiver implements a BOC(1,1) chip modulated legacy signals local replica or for the case where it implements a CBOC chip modulation. For example, Table 9 shows that the proposed signal solution will improve the legacy signal acquisition threshold by a margin between 0.6 to 2.2 dBs; moreover, it can be observed that the choice between the classic and maximum method will depend on the implemented local replica chip modulation and on the total non-coherent accumulated time (or dwell time).

Table 10 and Table 17 present the probability of miss detection of the non-coherent overlay sequence; this result is issued from a preliminary analysis since the probability has been calculated in AWGN channel conditions and has assumed a received C/N_0 of 27dB-Hz to account for major attenuations, 12 to 13 dB, of the received signal. Table 11 and Table 18 present the WER of the SCA cryptographic key codeword. These results have been obtained when using *ONE AND ONLY ONE* satellite link meaning that the property of a shared TESLA key chain has not yet been exploited. In fact, from the presented results, it can be observed that the implementation of a TESLA key chain is mandatory. Table 12 and Table 19 present the probability of miss-authentication, failing to successfully very the security code when the right cryptographic key is used. These tables show good results for a 50 km/h user and degraded results for a 5km/h user; however, these values should be refined by removing from the calculation the situations where the signal will not be used by the receiver due to its bad reception conditions: if the signa will not be used, it does not matter whether the SCA verification is successful or not. Additionally, note that the ideal results for a SCA scheme is that after exploiting the TESLA key chain property, Table 11 and Table 18 results must be very similar to Table 12 and Table 19 results.

Finally, Table 20 presents the TTFFD performance metrics. From this table, it can be seen that good results are expected for a 50 km/h user for coherent and non-coherent signal processing methods but that the TTFFD values for a 5km/h user are still a bit high, an average about 5s. However, as well as said for the SCA verification results, the TTFFD calculation include some situations where, even if the CED could be recovered, the signal will still not be exploited due to the degraded received signal conditions or even because the signal could not be tracked. Therefore, these situations must be excluded from the TTFFD performance calculation.

APPENDIX B – HIGH PERFORMANCE – NO TTFFD SIGNAL STRUCTURE AND PERFORMANCE:

	E1B	*E1C*	*TDM*
Assumption on the Received C/N_0 (dB-Hz)	37	37	40

Table 6: Assumption on the received signals C/N_0 values for High Performance – No TTFFD signal option

	Acquisition	*TTFFD*	*Overlay Seq.*	*SCA – Key*	*SCA – Code*
Structure	*Acq 12*	---	10 symb	LDPC(800,400) ARB50, CW repetition (x2)	10 symb/bursts
Data Modulation	---	---	CSK	CSK-5b	---
Symbol duration	12ms	---	8ms	4ms	8ms
Advanced block duration	---	---	2s	2s	2s
Time occupation	60%	0	4%	32%	4%

Table 7: High level TDM signal structure for High Performance – No TTFFD signal option

	1s/2s			**2s/2s**	
Num. Short basic blocks	5	10	35	5	45
Acquisition	12ms	12ms	12ms	12ms	12ms
Overlay Sequence	1 symb	0	0	1 symb	0
SCA – Code	0	8ms	0	0	0
CED	0		0	0	0
SCA – Key	0		2 symb	0	2 symb

Table 8: Detailed TDM signal structure for High Performance – No TTFFD signal option

Total accumulated time	*Detection probability*	*Chip Modulation*	*Acquisition Method*	
			Classic (E1B+E1C+TDM)	**Maximum (TDM alone)**
200ms	**0.95**	**BOC(1,1)**	-1.33	-1.45
		CBOC	-1.27	-0.63
	0.99	**BOC(1,1)**	-1.35	-1.45
		CBOC	-1.38	-0.63
400ms	**0.95**	**BOC(1,1)**	-1.29	-1.85
		CBOC	-1.28	-1.02
	0.99	**BOC(1,1)**	-1.30	-1.86
		CBOC	-1.22	-0.96
1s	**0.95**	**BOC(1,1)**	-1.23	-2.26
		CBOC	-1.28	-1.41
	0.99	**BOC(1,1)**	-1.25	-2.24
		CBOC	-1.33	-1.42

Table 9: Primary PRN code acquisition performance for High Performance – No TTFFD signal option

Non-Coherent overlay sequence – Probability of wrong synchronization at 27 dB/Hz	1.4e-04

Table 10: Non-coherent overlay sequence synchronization performance for High Performance – No TTFFD signal option

Dem. Method		**Coherent**				**Non-Coherent**			
User Speed		**50 km/h**		**5 km/h**		**50 km/h**		**5 km/h**	
Decoding Method		**Classic**	**Iterative**	**Classic**	**Iterative**	**Classic**	**Iterative**	**Classic**	**Iterative**
Num. of Acc. CW	**1**	26.9	19.2	33.1	25.4	34.3	28.8	39.3	32.3
	2	11	6.5	17.7	13.8	18.5	15.8	24.4	20.2

Table 11: SCA – Key delivery performance (WER) for High Performance – No TTFFD signal option – One and only one satellite link

Type of Processing	**Coherent**		**Non-Coherent**	
Type of User	**50 km/h**	**5 km/h**	**50 km/h**	**5 km/h**
Probably of verification failure	0.08%	0.77%	1.5%	1.9%

Table 12: SCA – Code verification performance (complete) for High Performance – No TTFFD signal option

APPENDIX C – HIGH DYNAMIC USER SIGNAL STRUCTURE AND PERFORMANCE:

	E1B	*E1C*	*TDM*
Assumption on the Received C/N_0 (dB-Hz)	37.821	37.812	39

Table 13: Assumption on the received signal C/N_0 values for High Dynamics users signal option

	Acquisition	*TTFFD*	*Overlay Seq.*	*SCA – Key*	*SCA – Code*
Structure	---	LDPC(1000,500) ARB50	16 symb	LDPC(800,400) ARB50 CW repetition (x2)	19 symb/bursts
Data Modulation	---	CSK-10b	CSK	CSK-7b	---
Symbol duration	---	4ms	8ms	4ms	8ms
Advanced block duration	---	1s	2s	2s	2s
Time occupation	0%	40%	6.4%	46%	7.6%

Table 14: High level TDM signal structure for High Dynamics users signal option

	1s/2s				**2s/2s**		
Num. Short basic blocks	8	17	1	24	8	17	25
Acquisition	0	0	0	0	0	0	0
Overlay Sequence	1 symb	0	0	0	1 symb	0	0
SCA - Code	0	8ms	16ms	0	0	0	0
CED	3 symb	3 symb	1 symb	1 symb	3 symb	3 symb	1 symb
SCA - Key	0	0	0	4 symb	0	2 symb	4 symb

Table 15: Detailed TDM signal structure for High Dynamics users signal option

Total accumulated time	*Detection probability*	*Chip Modulation*	*Acquisition Method*	
			Classic (E1B+E1C)	**Maximum**
200ms	**0.95**	**BOC(1,1)**	-0.82	---
		CBOC	-0.82	---
	0.99	**BOC(1,1)**	-0.82	---
		CBOC	-0.82	---
400ms	**0.95**	**BOC(1,1)**	-0.82	---
		CBOC	-0.82	---
	0.99	**BOC(1,1)**	-0.82	---
		CBOC	-0.82	---
1s	**0.95**	**BOC(1,1)**	-0.82	---
		CBOC	-0.82	---
	0.99	**BOC(1,1)**	-0.82	---
		CBOC	-0.82	---

Table 16: Primary PRN code acquisition performance for High Dynamics users signal option

Non-Coherent overlay sequence – Probability of wrong synchronization at 27 dB/Hz	2.4e-07

Table 17: Non-coherent overlay sequence synchronization performance for High Dynamics users signal option

Dem. Method		Coherent				Non-Coherent			
User Speed		50 km/h		5 km/h		50 km/h		5 km/h	
Decoding Method		Classic	Iterative	Classic	Iterative	Classic	Iterative	Classic	Iterative
Num. of Acc. CW	1	24.3	17.4	30.6	23.8	31.8	26.1	35.2	28
	2	9.9	5.8	16.9	13.1	18	14.1	20.9	17.9

Table 18: SCA – Key delivery performance (WER) for High Dynamics users signal option – One and only one satellite link

Type of Processing	Coherent		Non-Coherent	
Type of User	50 km/h	5 km/h	50 km/h	5 km/h
Probably of verification failure	0.06%	0.75%	1.9%	2.4%

Table 19: SCA – Code verification performance (complete) for High Dynamics users signal option

Dem. Method		Coherent				Non-Coherent			
User Speed		50 km/h		5 km/h		50 km/h		5 km/h	
Decoding Method		Classic	Iterative	Classic	Iterative	Classic	Iterative	Classic	Iterative
Statistics	Mean	1.73	1.56	5.35	4.53	1.97	1.76	5.89	5.13
	95%	5	4	29	25	6	5	31	28
	Max	15	14	81	81	23	20	82	81

Table 20: SCA – TTFF Data performance for High Dynamics users signal option