Threat Model Design for new GNSS signals

Jean-Baptiste Pagot, Paul Thevenon, Olivier Julien, Francisco Amarillo-Fernández, Denis Maillard

Threat Model Design for new GNSS signals

J.B. Pagot, P. Thevenon, O. Julien, *ENAC, France*
Francisco Amarillo Fernandez, *ESA, the Netherlands*
Denis Maillard, *CapGemini, France*

BIOGRAPHIES

Jean-Baptiste Pagot is a PhD candidate in the Department of Signal Processing and Satellite-based Navigation at the ENAC (Ecole Nationale de l'Aviation Civile) in Toulouse, France. He received his master degree as an Electronics and Telecommunication engineer in 2013 from the ENAC. He is currently working on GNSS Signal Distortions.

Dr. Paul Thevenon graduated as electronic engineer from Ecole Centrale de Lille in 2004 and obtained in 2007 a research master at ISAE in space telecommunications. In 2010, he obtained a PhD degree in the signal processing laboratory of ENAC in Toulouse, France. From 2010 to 2013, he was employed by CNES, to supervise GNSS research activities. Since the July 2013, he is employed by ENAC as Assistant Professor. His current activities are GNSS signal processing, GNSS integrity monitoring and hybridization of GNSS with other sensors.

Dr. Olivier Julien is the head of the Signal Processing and Navigation (SIGNAV) research group of the TELECOM laboratory of ENAC, in Toulouse, France. 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. His research interests are turned towards the use of satellite-based navigation systems for safe navigation.

Francisco Amarillo-Fernández received his Master's Degree in Telecommunication by the Polytechnic University of Madrid (UPM) Spain in 1997, and his Master's Degree in Surveying Engineering by the UPM in 1992. He has been working for the ESA Navigation Directorate since 2001 and has participated/led in numerous research activities in the GNSS field since 1997.

Denis Maillard received his engineer degree in Electronic and Computer Engineering from Institut National des Sciences Appliquées de Rennes in 2010. Since 2011 he works as a GNSS engineer in the EGNOS team of Capgemini Bayonne. He is currently in charge of the activities linked to GNSS signal processing.

ABSTRACT

This paper proposes threat models (TM) for Galileo E1C, the pilot component of the E1 Open Service signal, (CBOC$(6,1,1/11)$ modulation) and Galileo E5a (BPSK(10) modulation) signals, as they are the Galileo signals that will be used by civil aviation airborne receivers for pseudorange computation. The advent of new GNSS signals requests new definitions for prospective signal distortions. Indeed, new signals and/or new tracking methods change the conception of hazardous signal distortion. The problem was already studied in [1] and [2] but the idea was more about replicating the GPS L1 C/A TM on new signals and on new correlation functions. The justification of using such models with the same Threat Space as GPS L1 C/A was not tackled.

TMs provided in this report are based on the GPS L1 C/A TM established by ICAO (International Civil Aviation Organisation) [3]. The primary aim of such a TM is to look at the entire class of signal anomalies which could lead to important differential pseudo-range error (also called Evil Waveform (EWF)).

INTRODUCTION

In 1993, the first important GNSS signal distortion due to a payload failure was observed on GPS L1 C/A [4]. This raised two important questions among user communities, and more particularly the civil aviation community: Which signal distortions could affect a GPS L1 C/A signal in a hazardous way? How is it possible to protect a user against this threat? More precisely, distortions of interest were called Evil Waveforms (EWF) and were initially defined as signal distortions which could entail a large error on a differential user without being detected. The investigations consisted in considering all signal distortions leading to dangerous correlation function deformations (asymmetry, false peak and dead zones) [3]. The underlying reason for this is that correlation function distortions can be mapped into DLL, and thus pseudorange, biases. A proposition of signal distortion types with such consequences on the correlation function was made in 1999 for GPS L1 C/A [5]. This proposition has been adopted by ICAO with the definition of three Threat Models (TM) [3]:

- TM-A which is associated to a failure in the navigation data unit (NDU), the digital part of a satellite. It consists in considering the positive chips of the GPS L1 C/A PRN signal with a falling edge that leads or lags, by a delay noted Δ, relative to the theoretically correct end-time for that chip.

- TM-B which introduces amplitude modulation and models degradations in the analogue section of a satellite. More specifically, it consists of the output of a second order system when the nominal C/A code baseband signal is the input. Two parameters are defined to characterize this threat model: the damping factor σ and the ringing frequency f_d.
- TM-C which is a combination of the two previous failures.

These models are based on modelling possible phenomenon occurring at the satellite level. They do not necessarily represent the reality but are approaching expected signal distortions which could appear on a GPS L1 C/A signal. In fact, these threat models, and their associated parameter ranges, referred to as Threat Space, are powerful and necessary tools to design and test performances of Signal Quality Monitor (SQM), which is in charge, in some augmentation systems, of detecting dangerous distortions. This signal monitoring is necessary to protect users with high requirements in terms of integrity, accuracy, availability, and continuity such as civil aviation users. Nowadays, this monitoring task is performed in SBAS and GBAS systems.

This document describes a general concept to define Threat Models for Galileo signals and the associated Threat Space for Galileo E1C and Galileo E5a. Considering these two signals and an E-L tracking, it appears that correlation function threats are identical to threats defined for GPS L1 C/A: false peak, dead zone and asymmetry. Indeed, tracking techniques are similar and the shape of the correlation function on the tracked area is comparable (triangular shape) for all studied modulations. However, the way to translate it at the signal level is not straightforward due to the different modulation used by Galileo signals and the different payload architecture:
- TM-B can be easily applied to every GNSS signals by representing the effect of the analogue section of a satellite by a second order filter. The method consists in using the current second order filter and aims to find a limit for parameters range (f_d and σ).
- TM-A is more difficult to adapt in a generic way to all GNSS signals with sub-carrier components (CBOC((6,1,1/11) for example). Indeed, the lead/lag specified for the GPS L1 C/A TM-A could affect code chip transition and/or sub-chip transition as well.
- To finish, a TM-C, combination of TM-A and TM-B is envisaged.

This paper proposes a conservative way to established TM (TM-A, TM-B and TM-C) for Galileo E1C and Galileo E5a. These TM propositions are based on two key notions which are:
- The consequences on receivers (user and reference) of distortions included in the Threat Space.
- The model of the distortions. In this document, the ICAO TM defined for GPS L1 C/A is applied on Galileo signals.

GENERAL CONSIDERATIONS TO LIMIT TM PARAMETERS RANGE

Concept

EWF are defined as signal distortions that are caused by a satellite anomaly. As a matter of fact, knowledge about payload components and payload behavior in a faulty case could be sufficient to define EWF. Nevertheless, due to the lack of information about the way payload components could fail and their impact on signal generation, only distortion models (second order ringing phenomenon and lead/lag at positive chips signal falling edges) are defined from payload considerations. Others criteria have to be introduced to establish Threat Model limits.

Criteria used to define the Threat Space, ie the possible values of the TM-B parameters (σ and f_d) and TM-A parameter (Δ), for GPS L1 C/A signal are quickly described in [5]:
For the TM-B:
- It is mentioned that the higher bound for f_d (17 MHz,) has been chosen because higher frequency ringing effects would be filtered out by the satellite RF output filter, which is 20.46 MHz for GPS L1.
- The lower bound for f_d (4 MHz) is justified by the fact that lower frequency ringing will affect the L1 P(Y) code, that is "closely monitored" by military users.
- For σ, lower values ($\sigma < 0.8$ MNepers/s) are not realistic since they would introduce unrealistic instability of the ringing. Larger values ($\sigma > 8.8$ MNepers/s) shall not introduce more error on the user.

For TM-A:
- For Δ, the range of parameters is limited to +/- 0.12 of the chip duration, because larger values are easily detectable by multi-correlator techniques.

Because of the lack of knowledge about payload behavior in a faulty condition, it is assumed in this document that the distortion model is the same for Galileo E1C and Galileo E5a than for GPS L1 C/A. It means that the analogue failure consists on the output of a second order system [3] whereas a lead/lag on falling signal transitions (whether chip or sub-chip) characterizes a digital failure.

However, regarding Threat Space limits, some differences appear compared to the study realized on GPS L1 C/A. Indeed, to establish all parameters' limits (TM-A and TM-B), two quantities are evaluated in order to simplify the definition of the Threat Space:
- *The impact of a distortion on a receiver working with differential corrections*. More precisely, a parameter limitation is established on the analysis of the consequences of a distortion on a differential user's corrected pseudorange measurement. This analysis is based on the use of all possible civil aviation airborne

receiver configurations (essentially different correlator spacings RF front-end filter bandwidths and RF front-end filter types) and the knowledge of the reference station settings to cover the largest number of possible cases and the worst case. If a distortion leads to small differential bias (smaller than a specified maximum differential error: Δ_{err_max}) for all considered user/reference configurations, the corresponding TM parameters can be removed from the Threat Space.

- *The impact of a distortion on a reference receiver.* More precisely, if a signal distortion leads to reference tracking bias higher than a specified limit, the distortion is not included in the Threat Space because detected by the ground segment (regarding a P_{fa} and a P_{md} probabilities). Today, no such requirement on the tracking error detection at the reference level is defined. However, such strong hypothesis is useful to limit the Threat Space. It is presumed that the reference station is able to detect an absolute tracking bias higher than 20 meters with another process than the Signal Quality Monitor. Nowadays no algorithm exists to perform this task but it is assumed in this document that in the future such detectors will be provided. The value of 20 meters is chosen to be reachable and conservative.

Selected Reference and User Configurations

A user-oriented approach is used to determine the Threat Space. This approach results in the fact that the TM is dependent on the user and reference station configurations, and notably on the following parameters:

- The tracking technique (including the local replica)
- The correlator spacing
- The RF front-end (technology, bandwidth, maximum group delay variation).

Values and information about these parameters are given Table 1. These parameters represent expected civil aviation configurations.
Note that different types of filters are used, to account for the wide variety of filters encountered across multiple receiver manufacturers. All these filters satisfies ICAO requirements:

- *Filter1*: 6-order Butterworth.
- *Filter2*: resonator filter type with a group delay equal to zero.
- *Filter3*: resonator filter type with a concave group delay and a 150 nsec differential group delay.
- *Filter4*: 6-order Butterworth for the phase and the smallest order Butterworth filter leading to a differential group delay higher than 150 nsec for the phase.

Δ_{err_max} Value

This parameter is of primary importance because it represents the limit of the acceptable differential error in presence of EWF. Signal distortions which entail smaller differential errors than this limit are not included in the TM. The smaller Δ_{err_max} is, the wider the Threat Space is.

Δ_{err_max} is defined in a noise-free configuration. This follows the actual TM and Signal Quality Monitoring (SQM) concepts. Indeed, the SQM currently in use for GPS L1 C/A was designed using noise-free simulations. The noise is then taken into account in the SQM detector threshold determination. The concept is to ensure that distortions included in ICAO TM are either detected or create a differential error smaller than a limit. This limit was fixed to 3.5m for current GPS L1 C/A airborne receiver.

Using the presented configurations (Table 1) the Threat Space (TS) is defined by fixing Δ_{err_max} regarding civil aviation required performances and the TS is defined from this Δ_{err_max} value. This TS includes all signal distortions leading to differential errors higher than Δ_{err_max} for all considered reference/user configurations. With this TS, the range for σ parameter range is far beyond the one used nowadays for GPS L1 C/A as it will be shown.

To be conservative, in this document, Δ_{err_max} is fixed to 1m. This value grants conservativism compared to the former GPS L1 C/A study, which considers a value of 3.5m. It means that the TM includes all signal deformations (TM-B like) leading to differential error higher than 1m. This choice was made for three reasons:

- Future aircraft operations could require an improved positioning accuracy and integrity, with limits below the current value of 3.5m.

	Galileo E1C signal (CBOC(6.1)) and GPS L1 C/A		**Galileo E5a signal (BPSK(10))**	
	reference	user	Reference	user
Tracking technique	E-L (BOC(1.1) local replica)	E-L (BOC(1.1) local replica)	E-L (BPSK(10) local replica)	E-L (BPSK(10) local replica)
Correlator spacing	0.1 chip	0.08 and 0.12 chip	1 chip	0.8 and 1.2 chip
Pre-correlation bandwidth (double sided)	24 MHz	12, 14, 16, 18, 20, 22, 24 MHz	24 MHz	12, 14, 16, 18, 20, 22, 24 MHz
Equivalent reception filter	4 filters are tested (6-th order Butterworth, 0-group delay resonator, 150 nsec differential group delay resonator, 150 nsec differential group delay 6-th order Butterworth)			

Table 1. *Tested user and reference configurations*

- The dual-frequency case requires considering smaller errors on each signal component. Indeed, holding that the total maximum tolerable error is currently 3.5m and considering that the pseudo range bias is the same for both E1C and the E5a components, we have the following relations due to dual-frequency iono-free pseudo-range combinations:

$$3.5 = 2.26\rho_{bias\_E1} + 1.26\rho_{bias\_E5}$$
$$\rightarrow 3.5 = 2.26\rho_{bias} + 1.26\rho_{bias}$$
$$\rightarrow \rho_{bias} \approx 1m$$

  Consequently, an important margin should be adopted to deal with the dual-frequency configuration.
- A natural margin is necessary because the worst case cannot be reached due to the fact that considered user configurations are limited in this document to the ones described in Table 1, while in reality, they could be infinite. This margin would then be considered as a margin for the error modelling.

LOWER LIMIT FOR PARAMETERS σ AND f_d

In this section, the lower Threat Space bounds are defined: firstly the ringing frequency f_d and then the damping factor σ. Only the impact of a distortion on a reference receiver is necessary to fix these two limits.

Ringing frequency f_d

It is noticeable that distortions due to low f_d have a strong impact on all receivers including the reference. Figure 1 presents the influence of such signal distortion as a function of the damping factor for Galileo E5a and Galileo E1C signals.

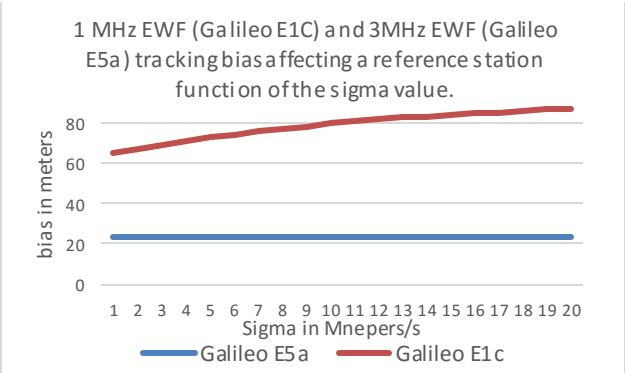

Figure 1. *1MHz (Galileo E1C) and 3MHz (Galileo E5a) EWF consequences on a standalone receiver without applying filtering*

These plots indicate that the impact of a 1 MHz for Galileo E1C signal (respectively 3MHz for Galileo E5a) distortion on the reference is higher than 20 meters whatever the value of σ is. It is also possible to show that the impact is stronger when the frequency is lower. By consequences all frequencies smaller than 1 MHz for Galileo E1C (respectively 3MHz for Galileo E5a) should be detected at the reference station level by the complementary monitor on the absolute bias. Therefore, it seems legitimate to remove these low frequencies from the TM.

Damping factor σ

Without any consideration, the lowest value of σ is taken equal to zero. Negative values lead to divergent signals and are not physically conceivable.

UPPER BOUNDS FOR PARAMETERS σ AND f_d

The highest f_d and damping factor σ values are estimated in this part. Firstly, the impact of a distortion on a user working with differential corrections is assessed. This consideration permits to limit f_d. Secondly the impact of a distortion on a reference receiver is evaluated in order to limit σ.

Maximum differential tracking error entailed by second order distortions

The following plots represent the worst differential tracking error for 4 different reference configurations (4 different filters) and 42 user configurations ($4\,(filter) \times 2(correlator\ spacing) \times 7(bandwidth)$). The withheld TS is the parameter range leading to differential error higher than $\Delta_{err\_max} = 1m$ (dark colour area on right plots). Results are presented for Galileo E1C in Figure 2 and Galileo E5a signals in Figure 3.

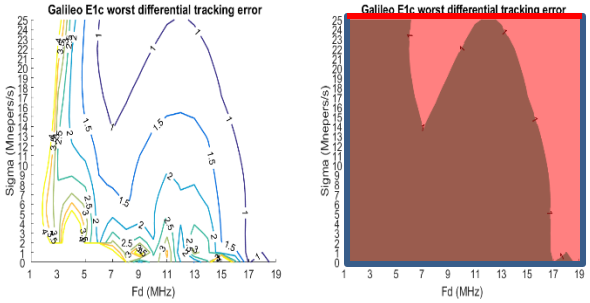

Figure 2. *Worst differential tracking error for different signal distortion parameters. On the right, only the 1m limit is shown. Blue limits give the remaining conservative TM. Red limit underline that the TM cannot be bound for high sigma values. Galileo E1C*

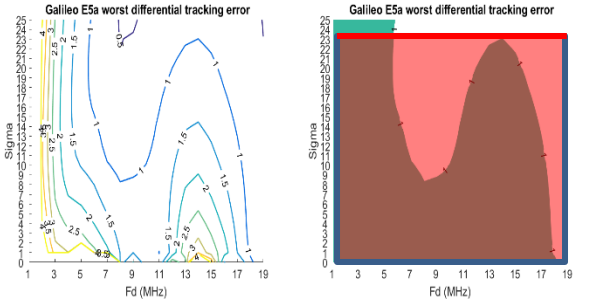

Figure 3. *Worst differential tracking error for different signal distortion parameters. On the right, only the 1m limit is shown. Blue limits give the remaining conservative TM. Red limit underline that the TM cannot be bound for high sigma values. Galileo E5a*

To have a simple TM definition, it is decided to adopt a rectangular Threat Space. Blue lines represent the TM limits for f_d and low σ that can be fixed from differential tracking error considerations or that have been fixed in the previous section. However, it is noticeable that a problem appears for high σ distortions when f_d is low. The limit cannot be fixed for high σ values and is represented by the red line.
Nevertheless it is decided to define a first area which is called area 1 based on the red rectangle visible on Figure 2 and Figure 3. By consequence, area 1 limits are defined for Galileo signals by:

Galileo E1C

$$f_d = 1 \; to \; 19 \; MHz$$
$$\sigma = \; 0 \; to \; 26 \; Mnepers/s$$

Galileo E5a

$$f_d = 3 \; to \; 19 \; MHz$$
$$\sigma = \; 0 \; to \; 24 \; Mnepers/s$$

This area 1 does not take into account high σ distortions. Another complementary area, called area 2 has to be defined to include all second order threatening distortions. This area is defined in the next part.

$\frac{\sigma}{(f_d)^2}$ function of f_d representation

Another representation to observe the impact of high σ on the tracking error is to plot the tracking error for signal distortions in a $(\frac{\sigma}{(f_d)^2}; f_d)$ system as shown in Figure 4.
Figure 4 and Figure 5 illustrate the concept of this new representation. Figure 5 gives the differential tracking error applying filter 3 for the user and filter 1 for the reference.

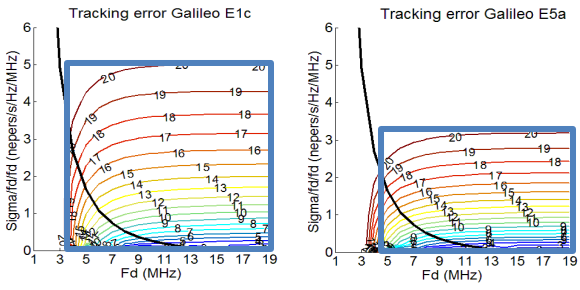

Figure 4. *Tracking error affecting the reference in meter generated by a* 2^{nd} *order filtering function of* $\frac{\sigma}{(f_d)^2}$ *and* f_d. *Blue rectangles represent area2 limits, black lines area1 upper limits.*

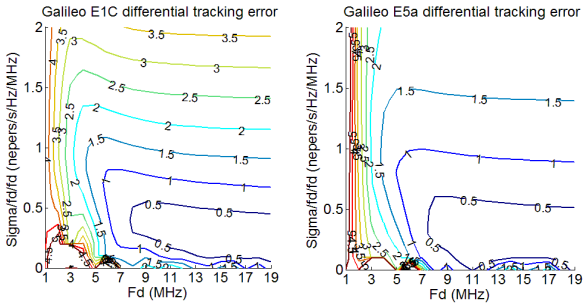

Figure 5. *Differential tracking error in meter generated by a second order filtering function of* $\frac{\sigma}{(f_d)^2}$ *and* f_d.

It is noteworthy that differential errors can also be large (ie larger than the considered $\Delta_{err\_max} = 1m$ limit) for high σ values. Galileo E1C results are presented on the left and Galileo E5a results on the right.

This new $(\frac{\sigma}{(f_d)^2}; f_d)$ representation has a lot of interest because it illustrates that the tracking error is (almost) constant for a given $\frac{\sigma}{(f_d)^2}$ and high frequencies. One of the consequence is that a constant $\frac{\sigma}{(f_d)^2}$ upper limit can estimate an upper σ limit for distortions of interest based on reference capability to detect large bias.

Consequently it is decided to establish the area 2 upper limit ($\frac{\sigma}{(f_d)^2}$ representation) based on the reference station capability to detect large absolute bias. As introduced previously, it is assumed in this document that the reference minimum detectable bias is equal to 20 meters.

The area 2 lower limit is based on the complementarity with area 1. To be conservative, for Galileo E1C the lower limit is given by:

$$\left(\frac{\sigma}{(f_d)^2}\right)_{min} = \frac{26}{19^2} \approx 0.07 \; nepers/s/Hz/MHz$$

And for Galileo E5a by:

$$\left(\frac{\sigma}{(f_d)^2}\right)_{min} = \frac{24}{19^2} \approx 0.06 \; nepers/s/Hz/MHz$$

One important point is that distortions with $\frac{\sigma}{(f_d)^2}$ value higher than $\left(\frac{\sigma}{(f_d)^2}\right)_{min}$, can be studied in the $\frac{\sigma}{(f_d)^2}$ representation. Indeed, from this $\left(\frac{\sigma}{(f_d)^2}\right)_{min}$ the new representation is able to take into account most of the different threatening distortions even for high f_d where less σ are tested. This is supported by the fact that above this limit, distortions vary slowly as it can be sensed on Figure 5.

Area 2 could be reduced to the area between the 20 meters tracking error and the black line representing area 1 upper limits in the $\frac{\sigma}{(f_d)^2}$ representation (Figure 4). Nonetheless, to be conservative and simplify the TM definition, it is

decided to limit Area 2 to the blue rectangles. Finally, Area 2 limits are given by:

Galileo E1C

$$f_d = 3 \; to \; 19 \; MHz$$
$$\left(\frac{\sigma}{(f_d)^2}\right) = 0.07 \; to \; 5 \; nepers/s/Hz/MHz$$

Galileo E5a

$$f_d = 4 \; to \; 19 \; MHz$$
$$\left(\frac{\sigma}{(f_d)^2}\right) = 0.06 \; to \; 3.5 \; nepers/s/Hz/MHz$$

Number of tests to cover the entire proposed TM

It is noticeable that the proposed Threat Space, composed of both area 1 and 2, is wider (by a factor 100) than the GPS L1 C/A Threat Space defined by ICAO. The purpose of this part is to compare the Threat Space in terms of number of tests to consider to take into account all threatening distortions with a fair resolution. In this part, the term resolution is used to represent the capacity of a test to get the most of different distortions as possible in a given TS.

It is not possible to test all threatening distortions because there is an infinity of distortions in a Threat Space. Nevertheless, to work with the current TM, only a finite number of distortions are tested. We define two consecutive tested distortions as two distortions with the same f_d but consecutive σ values or with the same σ but two consecutive f_d. To assess losses caused by the quantification of the Threat Space, a parameter is introduced: the tracking error difference observed between two consecutive tested distortions. This parameter is called Δ_{err_dist} and is used to evaluate the correlation function shape difference between to tested distortions.

The concept is to consider that only low enough Δ_{err_dist} values are tolerable. Indeed, if these values are too large, it means that the quantification of the TS is too large, and that the correlation function shape varies dramatically between two consecutive tested distortions. The consequence is that some threatening distortions could be omitted. It is remarkable that Δ_{err_dist} does not reflect exactly the difference of correlation function shape between two tested distortions. To be rigorous, a metric based on all correlation function points should be evaluated. Nevertheless, in this document, only a general idea of the correlation function behavior is necessary to compare TM convenience.

The lower the value of Δ_{err_dist} is, the better the resolution is. In order to compare the convenience of the new proposed Threat Space relatively to the ICAO Threat Space used for GPS L1 C/A, the same Δ_{err_dist} order of magnitude has to be reached in both Threat Spaces. Due to the fact that the problem is on high σ values, only the resolution on σ is studied, it means for a fixed f_d.

The reference for the resolution is based on the GPS L1 C/A ICAO TM. As an example, it is decided to introduce the grid of tested distortions presented in Figure 6 for the ICAO Threat Space: $f_d = 4{:}\,1{:}\,17MHz$, $\sigma = 0.8{:}\,1{:}\,8.8Mnepers/s$. Figure 6 shows tested values.

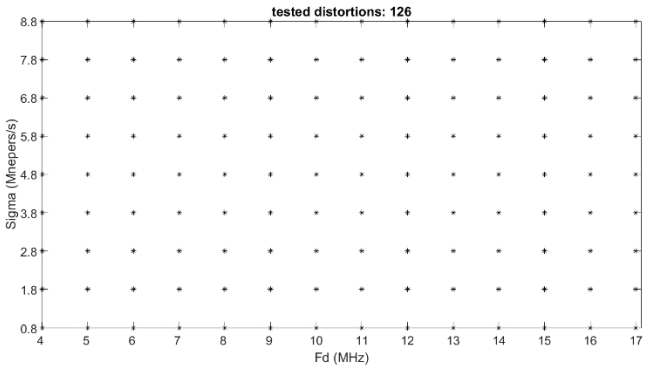

Figure 6. *Example of a Threat Space grid. (GPS L1 C/A ICAO TM)*

In this case 126 tests are realized to cover the Threat Space. For this particular case, Δ_{err_dist} values are given Figure 7. Different curves correspond to the 14 tested f_d. The abscissa gives the σ mean value of the two consecutive σ tested values at the origin of the Δ_{err_dist} computation. The maximum Δ_{err_dist} obtained with this sampling of the L1 C/A current TS is 2.8m. This is the approximate limit that has to be reached in the worst case for the sampling of the TS for the studied new signals.

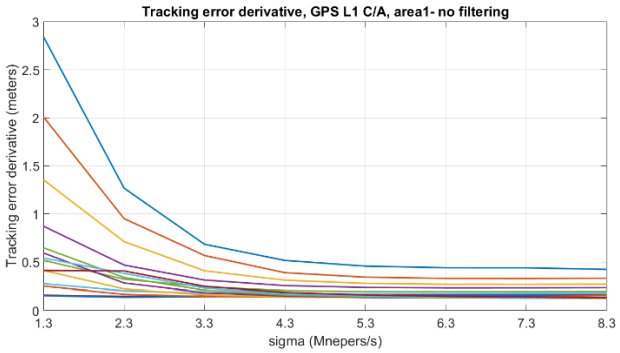

Figure 7. Δ_{err_dist} associated to the Threat Space grid from Figure 6. (GPS L1 C/A ICAO TM)

Area 1

Using the same grid for the area 1 of the Galileo E1C signal case, 513 tests are necessary to cover the whole area. This augmentation is due to the fact that higher values of f_d and σ are considered in area 1 of the proposed TM. Moreover for low f_d frequencies and low σ values a thinner grid has to be design to reach the same Δ_{err_dist} order of magnitude. The proposed grid is presented in Figure 8 and corresponds to 765 tests.

The area 1 can be decomposed in three tested zones:

- Zone1 to study low f_d. The grid consists on $f_d = 1{:}\,1{:}\,4MHz$, $\sigma = 1{:}\,0.2{:}\,26Mnepers/s$.
- Zone2 to study low σ. The grid consists on $f_d = 1{:}\,1{:}\,19MHz$, $\sigma = 0.05{:}\,0.1{:}\,1Mnepers/s$. It is

noticeable that distortions with σ lower than 0.05 $Mnepers/s$ cannot be studied without increasing dramatically the number of tests. This is why this lower bound of 0.05 $Mnepers/s$ is set.

- Zone3 to study the rest of the Threat Space. The grid consists on $f_d = 1{:}\,4{:}\,19MHz$, $\sigma = 1{:}\,1{:}\,26Mnepers/s$.

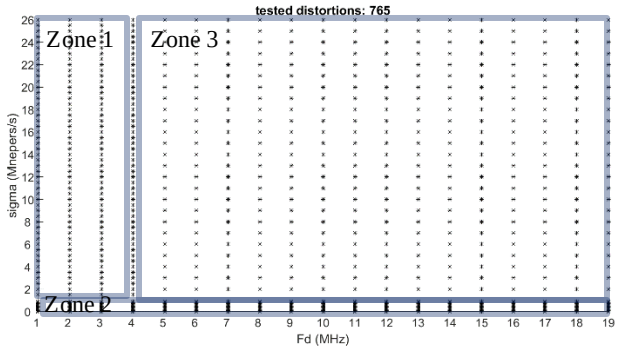

Figure 8. *Example of a Threat Space grid. (Galileo E1C, area1 of the proposed TM)*

Δ_{err_dist} associated to zone 1 are presented Figure 9. Δ_{err_dist} associated to zone 2 are presented Figure 10. Δ_{err_dist} associated to zone 3 are presented Figure 11.

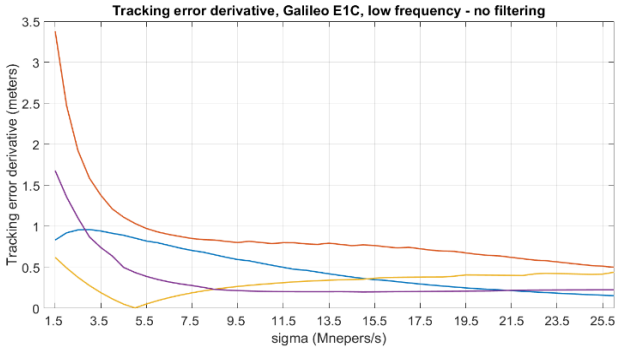

Figure 9. Δ_{err_dist} *associated to zone1 Threat Space grid from Figure 8. (Galileo E1C, area1 of the proposed TM)*

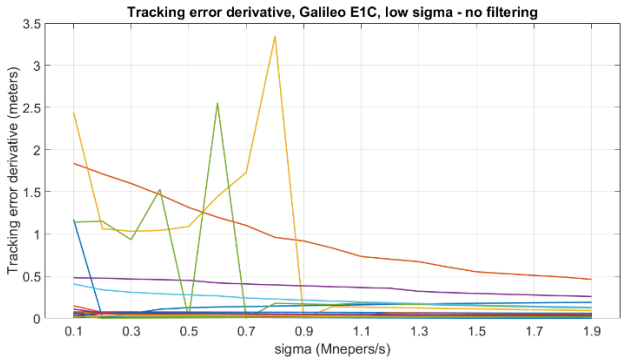

Figure 10. Δ_{err_dist} *associated to zone2 Threat Space grid from Figure 8. (Galileo E1C, area1 of the proposed TM)*

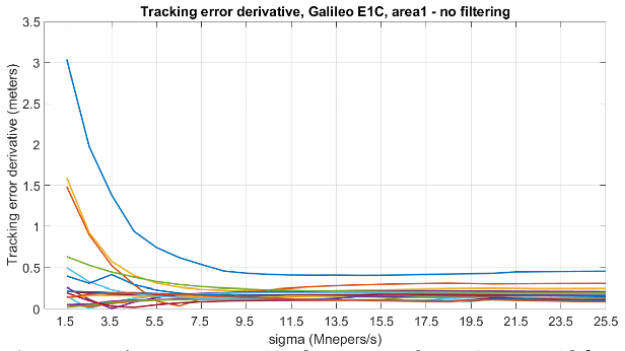

Figure 11. Δ_{err_dist} *associated to zone3 Threat Space grid from Figure 8. (Galileo E1C, area1 of the proposed TM)*

With the grid proposed for the area 1 of Galileo E1C signal, Δ_{err_dist} are comparable to values obtained with the grid proposed as an example for the GPS L1 C/A ICAO TM (Figure 6). Consequently, on Galileo E1C area 1 this new grid can be adopted to obtain approximatively the same resolution. The number of tested values is multiplied by a factor 6.1 ($\approx {}^{765}/_{126}$).

The same principle can be applied on Galileo E5a signal. However, with this signal, it is not necessary to define different zones. One of the consequence is that less tests have to be realized.
The proposed grid presented in Figure 12 has been created using the following parameters:
$f_d = 3{:}\,1{:}\,19MHz$, $\sigma = 0.05{:}\,4{:}\,24Mnepers/s$.

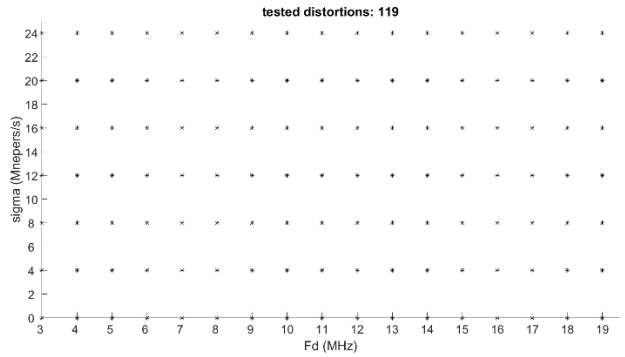

Figure 12. *Example of a Threat Space grid. (Galileo E5a, area1 of the proposed TM)*

Associated $\Delta_{err\ dist}$ are presented Figure 13:

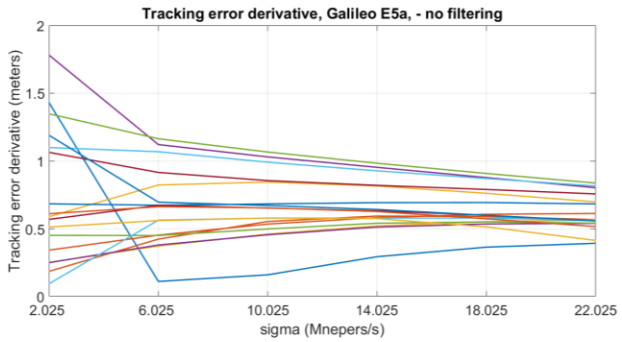

Figure 13. Δ_{err_dist} *associated to the Threat Space grid from Figure 12. (Galileo E5a, area1 of the proposed TM)*

It gives that the number of simulations to cover Galileo E5a area 1 has to be multiplied by 1 ($\approx {}^{119}/_{126}$) compared to the number of simulations necessary to cover the GPS L1 C/A ICAO TM with the same resolution.

Area 2

To these tested distortions, distortions in the area 2 of the TS, have to be added. In this area, with the same mesh ($f_d = 3:1:19MHz$, $\left(\frac{\sigma}{(f_d)^2}\right) = 0.07:1:5Mnepers/MHz/MHz/s$), Δ_{err_dist} are higher for high frequencies because a lot of σ values are omitted in the $\frac{\sigma}{(f_d)^2}$ representation. This is why it is necessary to reduce the mesh in area 2 to reach the same resolution as in area 1. Regarding the Galileo E1C signal, it is decided to use a mesh 20 times thinner for area 2 as illustrated in Figure 14. The plot on the top corresponds to the Threat Space grid in the $\frac{\sigma}{(f_d)^2}$ representation whereas the plot on the bottom is given in the σ representation.

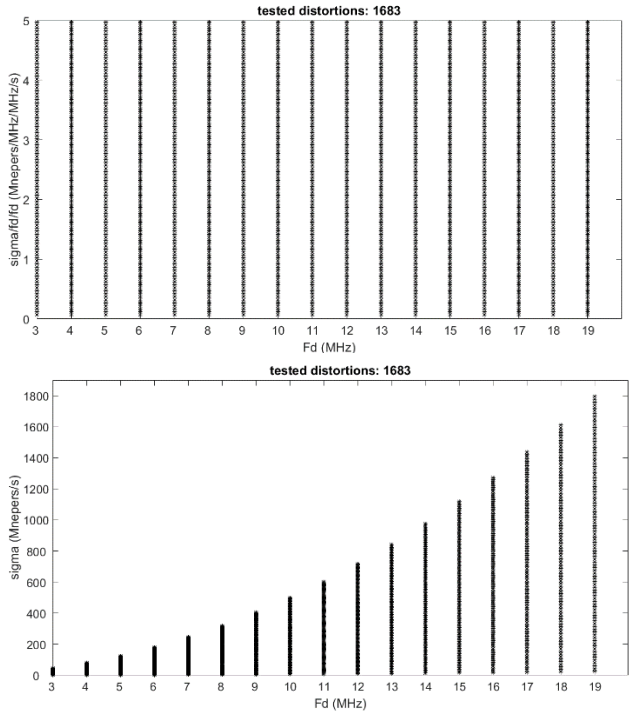

Figure 14. *Example of a Threat Space grid. (Galileo E1C, area2 of the proposed TM). On the top in the* $\frac{\sigma}{(f_d)^2}$ *representation, on the bottom in the* $\boldsymbol{\sigma}$ *representation.*

In this condition, Δ_{err_dist} is given Figure 15. Different curves correspond to the 17 tested f_d (from 3 MHz to 19 MHz). The abscissa gives the $\frac{\sigma}{(f_d)^2}$ mean value of the two consecutive $\frac{\sigma}{(f_d)^2}$ tested values at the origin of the Δ_{err_dist} computation.

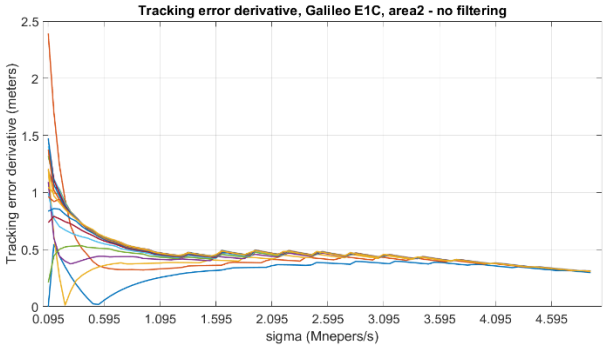

Figure 15. Δ_{err_dist} *associated to the Threat Space grid from Figure 10. (Galileo E1C, area2 of the proposed TM)*

From Figure 15 it can be seen that with the thinner mesh ($\left(\frac{\sigma}{(f_d)^2}\right) = 0.07:0.05:5Mnepers/MHz/MHz/s$), the maximum value of Δ_{err_dist} has the same order of magnitude than in the GPS L1 C/A ICAO TM case. It means that approximatively the same resolution is obtained if the number of tested values in area 2 is multiplied by 13.4 ($= {}^{1683}/_{126}$) compared to the number of tests necessary to cover the actual ICAO TM.

The same concept can be applied on Galileo E5a. Figure 16 represents Δ_{err_dist} values for $f_d = 4:1:19\,MHz$. At each f_d value corresponds one curve. It is decided to use a mesh 15 times thinner than for area 1 ($\left(\frac{\sigma}{(f_d)^2}\right) = 0.06:0.075:3.5Mnepers/MHz/MHz/s$).

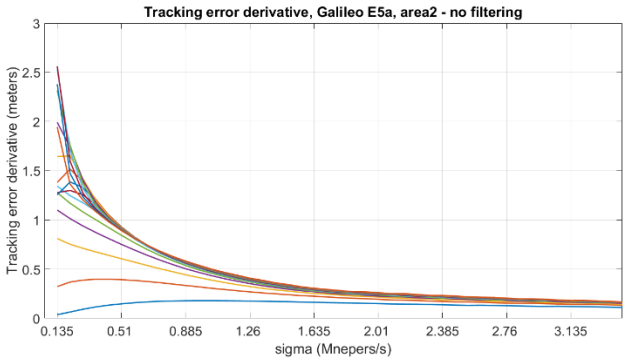

Figure 16. Δ_{err_dist} *values (Galileo E5a, area2 of the proposed TM)*

As observed for Galileo E1C, for this grid, Δ_{err_dist} have the same order of magnitude than in the GPS L1 C/A ICAO TM case. It means that approximatively the same resolution is obtained if the number of tested values in Galileo E5a area 2 is multiplied by 6.7 ($= {}^{840}/_{126}$) compared to the number of tests necessary to cover the current ICAO TM.

To conclude, it has been seen in this section that longer simulations are required to cover the wide proposed Threat Model. However to obtain approximatively the resolution with which the Threat model is examined in the GPS L1 C/A ICAO TM case, the number of simulations can be limited to:

- $13.4 + 6.1 = 19.5$ times the number of simulation compared to the actual TM for Galileo E1C.
- $6.7 + 1 = 7.7$ times the number of simulation compared to the actual TM for Galileo E5a.

These two values are reasonable to deal with the problem of signal distortions.

Conclusion about the conservative TM-B

This TM is conservative because it includes all dangerous signal distortions. The problem is that this TM has to take into account very high σ values. A solution is proposed to limit the number of distortions to test. This solution consists in the separation of the Threat Space in two areas:

- *Area 1*: This area resides on the σ in ordinate and f_d in abscise. This representation is equivalent to the classical ICAO TM-B distortion representation. This area is necessary to take into account low $\frac{\sigma}{(f_d)^2}$ signal distortion behaviors. Indeed, in this area, distortions vary rapidly and the $\frac{\sigma}{(f_d)^2}$ representation may let dangerous untested distortions with high f_d.
- *Area 2*: This area consists on $\frac{\sigma}{(f_d)^2}$ in ordinate and f_d in abscise. This area is the complementary of area 1

Based on distortions of the correlation function and their impact on differential user and on the reference ground station, the boundaries of the two areas were identified. An important remark is that Area 2 is dependent on the reference station capability to detect bias. Results given in this document are established for a reference with a minimum detectable bias equal to 20m. If performances of the reference station are better, the area 2 could be smaller. Parameters presented here are fairly conservative.

		Galileo E1C	*Galileo E5a*
Area 1	f_{d_min}	$1\ MHz$	$3\ MHz$
	f_{d_max}	$19\ MHz$	$19\ MHz$
	σ_{min}	$0\ Mnepers/s$	$0\ Mnepers/s$
	σ_{max}	$26\ Mnepers/s$	$24\ Mnepers/s$
Area2	f_{d_min}	$3\ MHz$	$4\ MHz$
	f_{d_max}	$19\ MHz$	$19\ MHz$
	$\left(\frac{\sigma}{(f_d)^2}\right)_{min}$	$0.07\ nepers/s/Hz/MHz$	$0.06\ nepers/s/Hz/MHz$
	$\left(\frac{\sigma}{(f_d)^2}\right)_{max}$	$5\ nepers/s/Hz/MHz$	$3.5\ nepers/s/Hz/MHz$

Table 2. *proposed TM-B parameters range for different signals using two representations*

It is noticeable that more signal distortions have to be tested in comparison to the actual ICAO GPS L1 C/A TM. Indeed, to run through the proposed TM, the number of tests have to be increased by a factor 20.

Figure 6 gives the two areas in the σ (left plot) and in the $\frac{\sigma}{(f_d)^2}$ (right plot) representations for Galileo E5a signal:

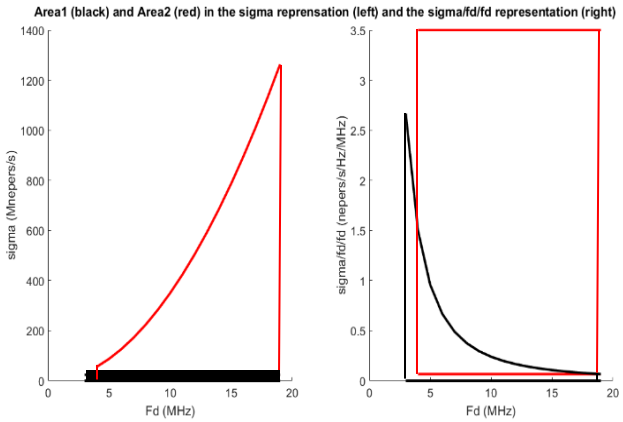

Figure 17. *Area 1 (black) and area 2 (red) in the $\frac{\sigma}{(f_d)^2}$ representation (left) and in the σ representation (right) for Galileo E5a signal.*

TM-A DISTORTION (DIGITAL DISTORTION)

As presented in the introduction Threat Model A consists of the normal C/A code signal except that all the positive chips have a falling edge that leads or lags relative to the nominal end-time for that chip.

Threat Model A for GPS L1 C/A has a single parameter Δ, which is the lead ($\Delta < 0$) or lag ($\Delta > 0$) expressed in fractions of a chip. The range for this parameter is $-0.12 \leq \Delta \leq 0.12$.

In this part, the TM-A is extended to Galileo E5a and Galileo E1C signals. It is recalled that the reasoning developed in this paper is based on the assumption that the same kind of failure appears on GPS L1 C/A, Galileo E1C and Galileo E5a signals.

The extension to the BPSK(10) (Galileo E5a) is simpler than to the CBOC (Galileo E1C) signal. That is why two digital TMs are proposed for the CBOC modulation: one conservative TM and one simplified TM. The simplest remaining CBOC TM-A presented in the last sub-part is based on a strong assumption: the CBOC digital signal is directly generated as the components product.

Galileo E5a

It is proposed to extend the range of Δ (in chip unit) compared to GPS L1 C/A TM-A for three reasons:

- Currently, the range of Δ considered in the ICAO model ($-0.12 \leq \Delta \leq 0.12$ chips) is justified by the fact that larger values of Δ are detectable by multi-correlator techniques [6]. If access to multiple correlator values is reduced on E5a because of a lower

sampling of the correlation function, then the range for Δ should be higher. [7]

- Regarding the impact on the receiver, the correlator spacing of the E5a tracking pair should be around 1chip whereas on GPS L1 C/A this value is around 0.1chip. Δ values currently in use for the GPS L1 C/A TM-A correspond to a flat zone at the top of the correlation function which is slightly larger than the 0.1chip correlator spacing. The same principle is envisaged for the Galileo E5a case.
- When converting Δ in seconds (rather than chip unit), the same order of magnitude should be envisaged.

To be conservative, it is proposed to take:

$$-1.2\ E5a\ chips \leq \Delta \leq 1.2\ E5a\ chips$$

Galileo E1C

As introduced previously, the CBOC(6,1,$^1/_{11}$) signal TM-A is more difficult to design because of the presence of sub-carriers. The presence of several components in the signal entails a multiplication of TM-A possibilities. Payload knowledge could help to make choices among the large number of conceivable TM-A. However, the lack of information about a payload miss-functioning prevents the selection. In this section, only most likely digital distortions are presented.

The following scheme presents the Galileo E1 signal generation [8]. Only the bottom part (highlighted green box) is of interest in the E1C component generation.

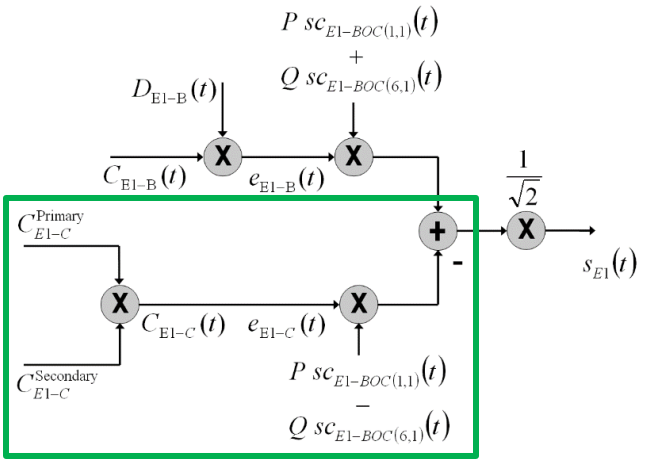

Figure 18. *Galileo E1 signal generation block scheme [8]*

Digital distortion 1: A lead/lag on every signal falling transitions after modulation. It is possible to imagine that only BOC(6,1) or BOC(1,1) transitions are affected by this lead/lag but because the distortion is applied after modulation, it is most likely that a delay will appear on every transitions.

The impact on the signal and on the correlation function of such a signal deformation are shown respectively on the top and on the bottom for $\Delta = 0.05\ chip$ (In blue the undistorted signal, in red the distorted signal):

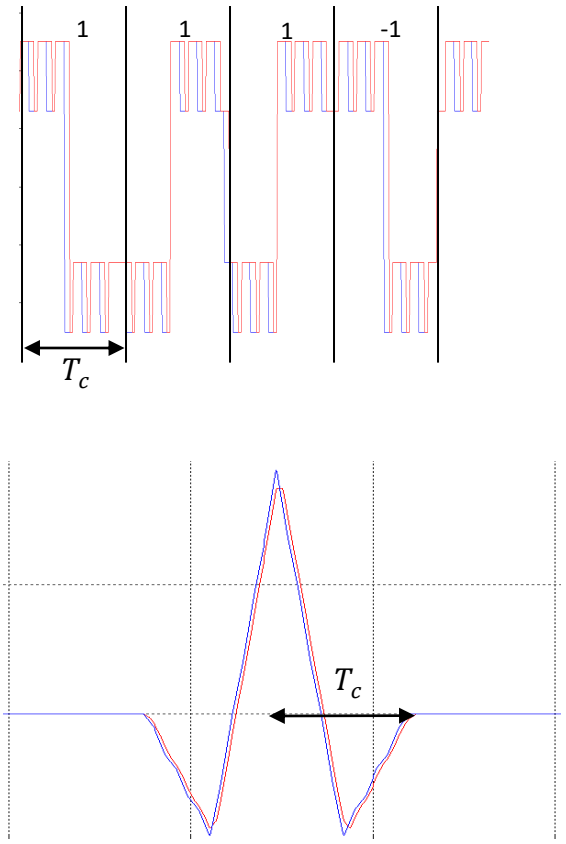

Figure 19. *Impact of the digital distortion 5 on the signal (top), and on the correlation function (bottom).*

Digital distortion 2: A lead/lag on the BOC(1,1) sub-carrier or/and on the BOC(6,1) sub-carrier falling transitions at the signal square wave generator level (before modulation). This distortion was introduced by Stanford in [1] for BOC(1,1) signal. In Figure 9, the lag on BOC(1,1) and BOC(6,1) transitions is similar. To be conservative and take into account most of possible cases, two independents parameters are defined:

- Δ_{11} : the lead/lag parameter on BOC(1,1) sub-carrier component (before modulation).
- Δ_{61} : the lead/lag parameter on BOC(6,1) sub-carrier component (before modulation).

The impact on the signal and on the correlation function of such a signal deformation are shown respectively on the top and on the bottom for $\Delta = 0.05\ chip$ (In blue the undistorted signal, in red the distorted signal):

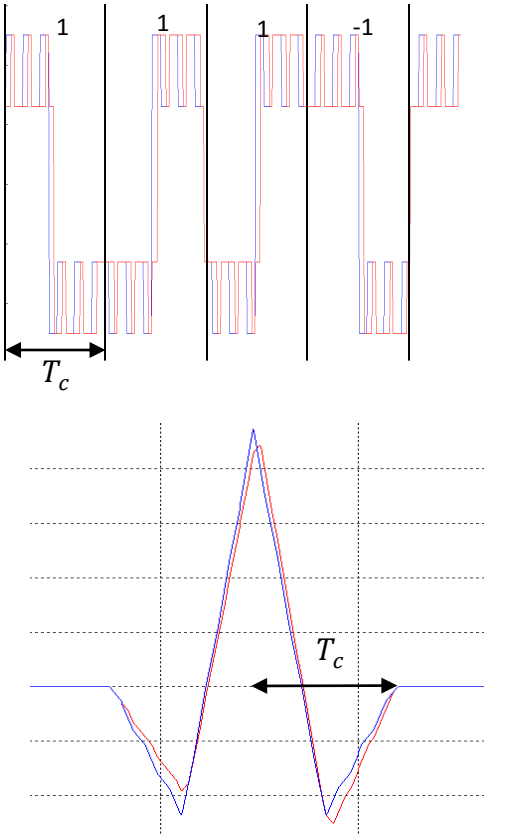

Figure 20. *Impact of the digital distortion 4 on the signal (top), and on the correlation function (bottom).*

In red, the signal generation component where the distortion 1 appears and in orange where distortion 2 appears:

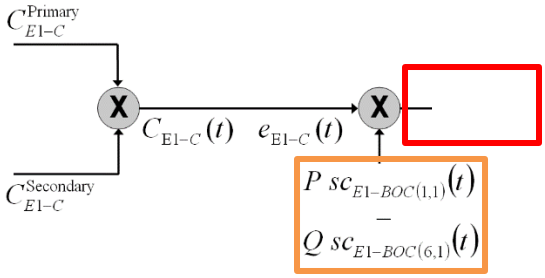

Figure 21. *Galileo E1C signal generation and digital distortions*

Parameters values

Two TM-A are proposed to take into account digital distortions for the new Galileo E1C signal:

- *TM-A1*: A lead/lag (Δ) on every signal falling transitions after modulation. Only one parameter is necessary. (digital distortion 1).
- *TM-A2*: A lead/lag on the BOC(6,1) (Δ_{61}) and on the BOC(1,1) (Δ_{11}) sub-carrier falling transitions at signal square wave generator level (before modulation). Two parameters are necessary. (digital distortion 2)

Δ parameters range can be fixed observing the signal. Indeed, it is visible that with BOC signals, from a certain value of Δ, the signal keep the same shape. Indeed, from a certain value of Δ, sub-chips are disappearing. Following illustrations show this concept for different distortions:

1) TM-A1 with $\Delta = 1.08\ chips$
2) TM-A2 with $\Delta_{11} = 0.5\ chips$ (Δ_{61} not considered)
3) TM-A2 with $\Delta_{61} = 0\ .08\ chips$ (Δ_{11} not considered)

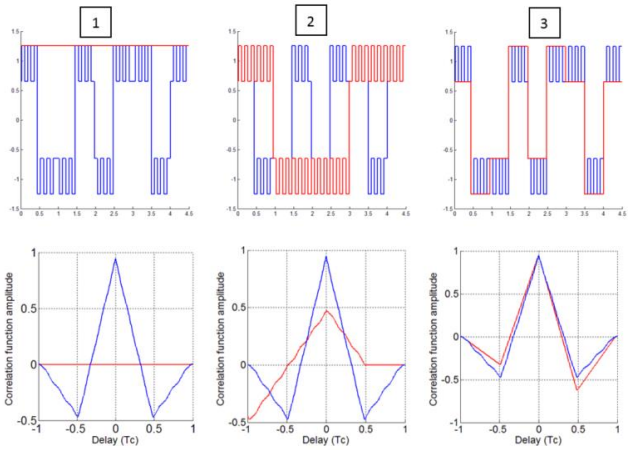

Figure 22. *CBOC signal affected by different digital distortions on the top and associated correlation function on the bottom.*

In the three cases, choosing higher values of Δ doesn't bring any change on the signal. These limits can be considered as physical limitations.

These principles are based on a reasoning without considering several TM-A combinations or simultaneous effect of Δ_{11} and Δ_{61}. Nevertheless, these limits seem reasonable.

However, it is noticeable that some of these high Δ parameter's distortions can be easily detectable. As it could be done to limit TM-B parameter ranges in the conservative proposed TM-B; Δ parameter ranges could be limited by the reference capability to detect large absolute bias. In this report, it is decided to hold that the reference is able to detect tracking bias larger than 20 meters to define TM-A limits.

Using this condition of 20 meters, Δ and Δ_{11} can be decreased to 0.12 chip and 0.10 chip respectively. The reference tracking error function of delta values are presented Figure 12. Reference configuration was applied to establish these plots.

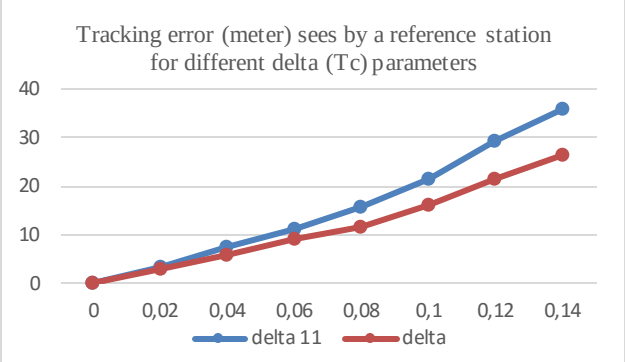

Figure 23. *Tracking error for TM-A1 and TM-A2 and different delta values (Δ and Δ_{11}).*

By consequence, for TM-A1, following parameter values are envisaged:

$$-0.12\ chips \leq \Delta \leq 0.12\ chips$$

And for TM-A2,

$$-0.1\ chips \leq \Delta_{11} \leq 0.1\ chips$$
$$-0.08\ chips \leq \Delta_{61} \leq 0.08\ chips$$

Simplified TM-A

Based on the current GPS L1 C/A digital TM, it is clear that the distortion is applied after the signal modulation with the PRN code. No information about the Galileo E1C signal generation is available. The answer to the question below could be helpful to choose one of the TM-A:

Are the three signal components (BOC(1,1), BOC(6,1), PRN) generated independently (TM-A2) or is the digital signal directly generated as the product of the components (TM-A1)?

Here, the assumption is made that the digital signal is directly generated as the components product. It entails that only TM-A1 is conserved.

Proposed TM

TM-A1: A lead/lag (Δ) on every signal falling transitions after modulation. Only one parameter is necessary (digital distortion 1). The retained parameter range is:

$$-0.12\ chips \leq \Delta \leq 0.12\ chips$$

Conclusion on TM-A

Galileo E1c

- *TM-A1*: lead/lag at every signal falling transitions after modulation: Δ.
- *TM-A2*: lead/lag on the BOC(6,1) (Δ_{61}) and on the BOC(1,1) (Δ_{11}) sub-carrier falling transitions at signal square wave generator level: Δ_{61} on the BOC(6,1) sub-carrier, Δ_{11} on the BOC(1,1) sub-carrier.

CONSERVATIVE TM	SIMPLIFIED TM
$-12.3\ ns \leq \Delta \leq 12.3\ ns$	$-12.3\ ns \leq \Delta \leq 12.3\ ns$
$-10.3\ ns \leq \Delta_{11} \leq 10.3\ ns$	/
$-8.2\ ns \leq \Delta_{61} \leq 8.2\ ns$	/

Table 3. *Digital parameter proposed range for Galileo E1C*

Galileo E5a

TM-A: lead/lag at every signal falling transitions after modulation: Δ.

$$-12.3\ ns \leq \Delta \leq 12.3\ ns$$

It is noteworthy that all these limits could be reduced if the reference station is able to detect smaller bias than 20 meters.

TM-C

In the current ICAO TM, the TM-C is a TM-A and TM-B combination. Parameter ranges choose for TM-C are smaller than individual parameter ranges for TM-A and TM-B.
To be conservative and without more knowledge, the proposed TM-C takes parameter ranges established for the TM-A and the TM-B.

Proposed parameters are summarized in table 4:

		Galileo E1C	*Galileo E5a*
Area 1	f_{d_min}	1 MHz	3 MHz
	f_{d_max}	19 MHz	19 MHz
	σ_{min}	0 $Mnepers/s$	0 $Mnepers/s$
	σ_{max}	26 $Mnepers/s$	24 $Mnepers/s$
Area 2	f_{d_min}	3 MHz	4 MHz
	f_{d_max}	19 MHz	19 MHz
	$\left(\frac{\sigma}{(f_d)^2}\right)_{min}$	0.07 $nepers/s/Hz/MHz$	0.06 $nepers/s/Hz/MHz$
	$\left(\frac{\sigma}{(f_d)^2}\right)_{max}$	5 $nepers/s/Hz/MHz$	3.5 $nepers/s/Hz/MHz$
	$\Delta_{min} = -\Delta_{max}$	0.12 $chips$	1.2 $chips$
Not in the simplified TM	$\Delta_{11min} = -\Delta_{11max}$	0.1 $chips$	/
	$\Delta_{61min} = -\Delta_{61max}$	0.08 $chips$	/

Table 4. *TM-C parameters range estimated for Galileo E1C and Galileo E5a signals.*

CONCLUSION AND FUTURE WORKS

This document proposes two threats models: one for Galileo E5a and one for Galileo E1C signals. These TMs are based on current ICAO threats established for the GPS L1 C/A signal. It is clear that the ICAO TM main drawback is still present in this approach: only a model is considered with its miss-modelling and the impossibility to take into account all possible signal distortions. Moreover, applying it directly to Galileo signals means that there is an acknowledgement that the Galileo payload would not provide different distortions, which is very unsure. This question of TM legitimacy is raised for example in [9] but this was not the subject of this report. It was shown that second orders distortions with high damping factors are not included in the current ICAO TM-B whereas these distortions can be critical. Regarding TM-A, digital failures proposed for Galileo E1C are disputable in that sense that tens of different digital failures are thinkable. Nevertheless, most relevant distortions were kept.

The approach to limit the TM-B is based on keeping only signal distortions with:

- An impact higher than $\Delta_{err\_max} = 1m$ for differential users in a specific receiver configuration range. This value is fixed by requirement.
- An impact smaller than 20 meters on a reference station's absolute pseudorange measurement, using an E-L discriminator with a correlator equal to 0.1 chip and an equivalent RF filter modelled by a 6-order Butterworth with a 24 MHz bandwidth.

It is assumed that distortions which do not satisfy the first point are not a threat for a differential user whereas distortions which do not satisfy the second point will be detected by a separate monitor implemented the reference station.

These new TMs are interesting because they take into account all possible threats for reference/user configurations exposed in this document. Even if large values of σ have to be considered, the range of distortion to test can be greatly reduced using the $\sigma/(f_d)^2$ representation.

An estimation of the required quantization of the proposed Threat Space for TM-B has been assessed. It gives a number of possible distortions that is approximately 20 times for Galileo E1C and 8 times for Galileo E5a higher than the number of distortions in the current GPS L1 C/A Treat Space.

Regarding the TM-A, the procedure is easier and it is still possible to find acceptable parameter ranges only using receiver considerations. Far more TM-A could be envisaged but without prior knowledge on the satellite payload, the two TM-A proposed for Galileo E1C signals are the easiest to conceive. The simplified TM-A is established from the assumption that the signal is generated as the product of signal components. If this assumption cannot be verified, the conservative TM should be adopted, meaning one TM-A1 with one parameter plus one TM-A2 with two parameters.

The proposed methodology could be applied to other signal modulation (modernized GPS, GLONASS, Beidou, etc …).

Once the threat model is established, new SQM algorithms can be studied to protect a Civil Aviation user from the defined threats.

REFERENCES

[1] R.E. Phelts, D.M. Akos, Effects of Signal Deformations on Modernized GNSS Signals, *Journal of Global Positioning Systems, Vol. 5 No. 1-2*, Hong Kong, China, 2006.

[2] Fontanella D.,PaonniM.,Eissfeller B., "A Novel Evil Waveforms Threat Model for New Generation GNSS signals: Theoretical Analysis and Performance," *Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC), 2010 5th ESA Workshop* on , vol., no., pp.1,8, 8-10 Dec. 2010

[3] International Standards and Recommended Practices. Annex 10 to. ICAO. 6th Edition. July 2006.

[4] A.M. Mitelman, Signal Quality Monitoring for GPS Augmentation Systems, Ph.D. Thesis, 2004, Stanford University, Stanford, CA.

[5] Enge, P. K., Phelts, R. E., Mitelman, A. M., "Detecting Anomalous signals from GPS Stallites," ICAO, GNSS/P, Toulouse, France, 1999.

[6] R.E. Phelts, Multicorrelator Techniques for Robust Mitigation of Threats to GPS Signal Quality, Ph.D. Thesis, 2001, Stanford University, Stanford, CA.

[7] Thevenon, P., Julien, O. Adaptation of the ICAO Signal Distortion Threat Model to the GPS L5 signal. Deliverable for WP1 of the contract with Cap Gemini, 2014

[8] Navipedia (Website), J.A Ávila Rodríguez, Galileo Signal Plan, 2011

[9] Pullen, S., "Providing Integrity for Satellite Navigation: Lessons Learned (Thus Far) from the Financial Collapse of 2008 - 2009," *Proceedings of the 22nd International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2009)*, Savannah, GA, September 2009, pp. 1305-1316.