Signal quality monitoring for protection of GBAS users against evil waveforms

Christophe Macabiau, Eric Chatre

Signal Quality Monitoring for Protection of GBAS Users Against Evil Waveforms

Christophe MACABIAU, , *CNS Research Laboratory of the ENAC*
Eric CHATRE**,** *STNA*

BIOGRAPHY

Christophe Macabiau is in charge of the signal processing unit of the CNS Research Laboratory (URE-CNS) at the Ecole Nationale de l'Aviation Civile (ENAC) in Toulouse, France. After working in 1993 for the MLS Project Office in Ottawa, Canada, he received his Ph.D. from the Laboratoire de Traitement du Signal et des Télécommunications of the ENAC in 1997. He is currently working on the application of code and phase LADGPS positioning techniques to aeronautics.

Eric Chatre graduated as an electronics engineer in 1992 from the ENAC (Ecole Nationale de l'Aviation Civile), Toulouse, France. Since 1994, he has been working with the Service Technique de la Navigation Aérienne (STNA) in Toulouse. He is involved in GNSS standardization activities in ICAO GNSSP and EUROCAE, RTCA forums.

ABSTRACT

Several types of failures can occur in the GPS satellites that transmit the ranging signals to the users. Among them, a specific type of failure in the signal generation process aboard the satellite may result in an anomalous waveform being transmitted, called an 'evil waveform'. Evil waveforms are GPS signals that have a distorted PRN code modulation waveform. The main impact is a rupture of the symmetry of the cross-correlation peak inside the tracking channel, therefore inducing a different measurement error for two receivers that would not have the same architecture. As a consequence, there is a potential for evil waveforms to induce large tracking errors of differential systems if left undetected.

The aim of this paper is to analyze the performance of the latest proposed ground Signal Quality Monitoring (SQM) techniques, and to present a summary of the final recommendations adopted by ICAO GNSSPanel.

The paper starts with a description of the mathematical model of the evil waveform, and its predicted effect on the GPS receiver is presented.

Next, we discuss the rationale for the methodology employed to design the currently proposed ground Signal Quality Monitoring (SQM) techniques, and describe one of these techniques. Some theoretical and collected statistics of the test thresholds including measurement noise and multipath level used by this technique are then presented.

Then, we present simulation results showing the level of protection provided by this technique, depending on the airborne receiver architecture. Observed behaviors of real receivers tracking one of these evil waveforms is then shown.

We finally conclude with the actual recommendations formulated by the GNSSP.

I. INTRODUCTION

Several types of failures can occur in the GPS space segment designed to deliver the ranging signals to the users. Among the potential failures, a specific type of failure in the signal generation process aboard the satellite may result in an anomalous waveform being transmitted, called an 'evil waveform'. Such a failure was already observed in 1993 on an operating satellite, and an analysis of the causes of failures have led to the derivation of a mathematical model of these waveforms [Enge et al., 1999].

Evil waveforms are GPS signals that have a distorted PRN code modulation waveform. The deformation is modeled by a lead or a lag of the rising or falling edges of the modulation code, and/or by a second-order filtering of this waveform.

The main impact is a rupture of the symmetry of the cross-correlation peak inside the tracking channel, therefore inducing a different measurement error for two receivers that would not have the same loops architecture.

As a consequence, there is a potential for evil waveforms to induce large tracking errors of differential

systems. This potential danger pushed the Global Navigation Satellite System Panel (GNSSP) of the International Civil Aviation Organization (ICAO), and the RTCA SC-159, to propose sections in the standards that would guarantee the safe operation of differential GPS.

Several teams gathered their efforts to tackle that problem, and after insufficient initial results [Macabiau and Chatre, 2000], an example of adequate ground monitoring technique was proposed and constraints on the airborne receiver were proposed to make sure the differential tracking error does not exceed the required accuracy level.

II. EVIL WAVEFORM MODEL

The evil waveform is a GPS signal that has a distorted PRN code modulation waveform. The failure giving birth to an evil waveform occurs in the code modulation generation channel only, therefore the transmitted carrier is not affected. Two types of failure can occur that result in an evil waveform being radiated. A failure in the digital code chip generation module can alter the synchronization of some of the C/A code chip edges. A mismatch of the analog band-limiting filter can distort the physical waveform being transmitted.

As a consequence, the model proposed in [Enge et al., 1999] is a PRN signal affected by one or both of the following effects:

1. All the falling edges or all the rising edges of the code modulation are delayed or advanced by an amount of Δ seconds. If there is a lag, then Δ is positive, if there is a lead, Δ is negative. Δ is usually expressed in chips, as a multiple of the chip length T_c=1/1.023·10^6 s.
2. The modulation is filtered by a 2nd order filter characterized by two parameters:
   - $\sigma=\delta\omega_n$ where δ is the damping factor and $\omega_n/2\pi$ is the frequency.
   - $F_d = \frac{\omega_n}{2\pi}\sqrt{1-\delta^2}$ is the resonant frequency.

   Usually, σ and F_d are expressed in MHz.

Several types of threat models are considered:

- Threat model A: this type of evil waveform contains only the lead/lag effect. In that case, σ=0, F_d=0 and the accepted range of values for Δ is:
  $$-0.12\ T_c \le \Delta \le 0.12\ T_c.$$
- Threat model B: this type of evil waveform contains only the 2nd order filtering effect. Therefore, Δ=0 and the possible range of values for σ and F_d is:
  $$0.8\ MHz \le \sigma \le 8.8\ MHz,\quad 4\ MHz \le F_d \le 17\ MHz.$$
- Threat model C: this type of evil waveform contains both effects. The possible range of values is:
  $$-0.12\ T_c \le \Delta \le 0.12\ T_c,\ 0.8\ MHz \le \sigma \le 8.8\ MHz,\ 7.3\ MHz \le F_d \le 13\ MHz.$$

Model A evil waveforms add a periodic line spectrum to the nominal C/A code power spectrum density. This additive line spectrum has a $\sin(\pi f\Delta)/\pi f\Delta$ envelope.

Moreover, model A evil waveforms raise the DC component of the code modulation by an amount close to $\Delta/2$ due to the near balance of 0s and 1s in each C/A code. As indicated in [Enge et al., 1999], the cross-correlation between model A evil waveforms and a nominal C/A code shifts the top section of the triangle, and introduces a plateau of width Δ.

Model B evil waveforms raise all the frequency components of the code spectrum located around F_d,. As a result, the cross-correlation function is also filtered by the 2nd order filter.

Model C evil waveforms are a combination of the lead/lag effect with the 2nd order filtering effect.

III. IMPACT OF EVIL WAVEFORMS ON GPS RECEIVER

The tracking errors due to evil waveforms depend on the exact characteristics of a receiver. First, the incoming signal is amplified, down-converted, filtered and converted to digital samples by the RF front-end. Then, this signal is sent to the tracking loops that try to generate local replicas of the incoming carrier and code modulation.

The amount of distortion conveyed by the evil waveform entering the tracking loops is determined by the RF front-end filter, that rejects out-of-band frequency components. The Delay Lock Loop (DLL) is designed to track nominal C/A codes having near-triangular cross correlation function, and is therefore misleaded by the deformations on the correlation values.

Therefore, the main parameters are:

- the transfer function of the RF front-end pre-correlation filter (bandwidth and group delay variations)
- the DLL discriminator function (value of the spacing between correlator outputs, form of the combination of these outputs)

As these parameters may vary considerably from one receiver to the other, the differential tracking error may be severely affected by the evil waveform.

IV. EXAMPLE OF A SIGNAL QUALITY MONITORING TECHNIQUE

The techniques used to detect the presence of an evil waveform all attempt to check whether the cross-correlation function significantly departs from the nominal triangular shape.

The signal quality monitoring (SQM) technique which is analyzed here was proposed during a specific SQM meeting held in Stanford University in December 1999. The technique can only be implemented on receivers equipped with DLLs providing multiple correlator outputs. These outputs provide information about the possible deformation of the cross-correlation function. Several test

metrics are formed using these extra correlator outputs, and compared against test thresholds.

The test metrics are based on the following ratios:

$$\Delta_{\pm d} = \frac{I_{-d} - I_{+d}}{2I_P}, R_{\pm d} = \frac{I_{-d} + I_{+d}}{2I_p}, R_d = \frac{I_d}{I_p}$$

where

- d is the offset from the prompt code in chips
- I_d is the output of the d correlator on the I channel
- I_P is the output of the I prompt correlator

For the SQM presented here, we use the following test metrics, computed using the outputs presented in figure 1:

- $\Delta_{\pm 0.075} - \Delta_{\pm 0.05}$, $\Delta_{\pm 0.1} - \Delta_{\pm 0.05}$
- $R_{\pm 0.05}$, $R_{\pm 0.075}$, $R_{\pm 0.1}$
- $R_{-0.1}$, $R_{-0.075}$, $R_{-0.05}$, $R_{+0.05}$, $R_{+0.075}$, $R_{+0.1}$

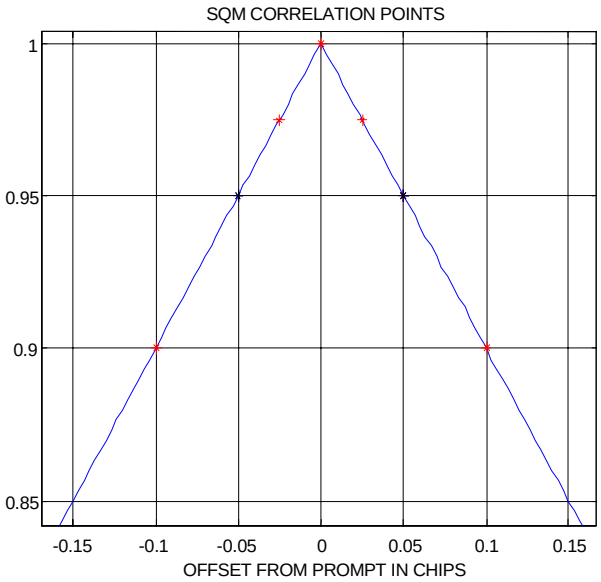

Figure 1: *Correlator outputs used for computation of SQM test metrics.*

To assess the performance of the SQM during simulations, we compare all these test criteria with thresholds called the Minimum Detectable Errors (MDEs).

The MDEs are computed so that both the false alarm rate and the probability of missed detection of a misleading information are met. A misleading information is defined as an undetected aircraft pseudorange differential error greater than the Maximum ERRor (MERR) that can be tolerated. Figure 2 shows the evolution of the MERR as a function of the elevation angle [Shively, 1999].

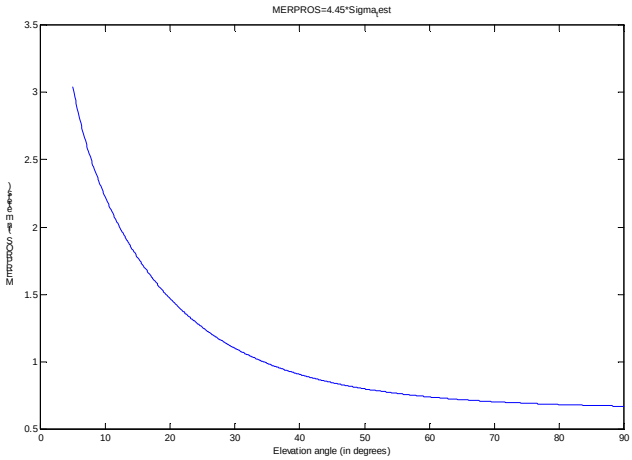

Figure 2: *Evolution of the MERR as a function of the elevation.*

To cope with that definition, the mathematical expression of the MDE is therefore

$$MDE = \left(K_{fa} + K_{md}\right)\sigma_{test}$$

where

- σ_{test} is the standard deviation of the test metric
- K_{fa} is the expansion factor required to guarantee a specific false alarm probability
- K_{md} is the expansion factor required to guarantee a specific missed detection rate

It is proposed in [Shively et al., 1999] that the probability of missed detection be set to 10^{-3}, inducing $K_{md}=3.09$, assuming the test metrics has a gaussian distribution. Similarly, a proposed allocation analysis in [Pullen and Van Dierendonck] concludes to a false alarm requirement of $1.5 \cdot 10^{-7}$ when using a total of 8 parallel test metrics on measurements coming from 6 satellites correlated over 100s. Therefore, $K_{fa}=5.26$, and

$$MDE = 8.35 \times \sigma_{test}$$

If no fault is detected by the SQM algorithm, then the pseudorange correction elaborated using the 0.1 Tc DLL measurement is sent to the airborne users.

It must be noted that the fault-free standard deviation of the test metrics is highly dependent on the architecture of the ground station : environment, antenna, receivers, process adopted to output the corrections.

In the real implemented monitor, the test threshold T_{test} is determined as

$$T_{test} = K_{fa} \times \sigma_{test}$$

where

- σ_{test} is the standard deviation of the test metric
- K_{fa} is the expansion factor required to guarantee a specific false alarm probability

V. SETTING OF THE MDEs

The MDEs are test thresholds that are used to detect the presence of an hazardous evil waveform.

Therefore, setting the MDEs is a compromise to avoid that any small distortion on the received signal, such as nominal multipath, raises a false alarm, while providing the necessary protection for airborne users.

Various teams proposed to collect statistics for all the test metrics. This was initially done by Stanford University, then by the STNA. The data was collected using a Novatel Millenium receiver running a specific software providing 48 correlator outputs for I and Q in one channel. Meanwhile, Honeywell proposed some theoretical values of the standard deviations.

Figure 3 shows the theoretical standard deviation of test metric $\Delta_{\pm 0.1} - \Delta_{\pm 0.05}$ proposed by Honeywell as a function of the elevation angle of the satellite.

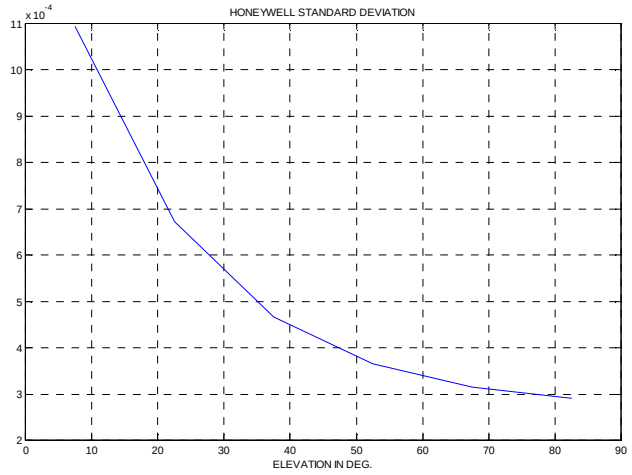

Figure 3: *Theoretical σ for test metric $\Delta_{\pm 0.1} - \Delta_{\pm 0.05}$.*

Figure 4 shows the σ collected by the STNA for PRN 15, with an antenna located on the STNA roof, for several days. The antenna is a Novatel L1/L2 antenna (ref 502, no choke ring). Figure 5 shows the σ collected by the STNA for PRN 15, with an antenna located on the roof of the shelter of the GBAS reference station at Blagnac airport, for several days. The antenna is a Novatel choke ring antenna (ref 501). The computed metrics were averaged over 100 s. Each line corresponds to one satellite pass.

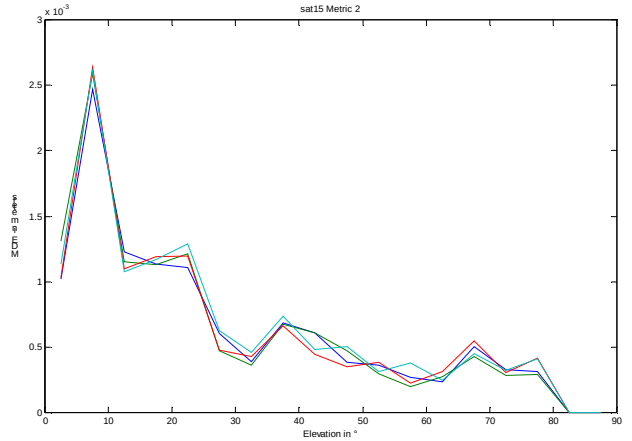

Figure 4: *Collected σ for test metric $\Delta_{\pm 0.1} - \Delta_{\pm 0.05}$ at the STNA roof for PRN 15.*

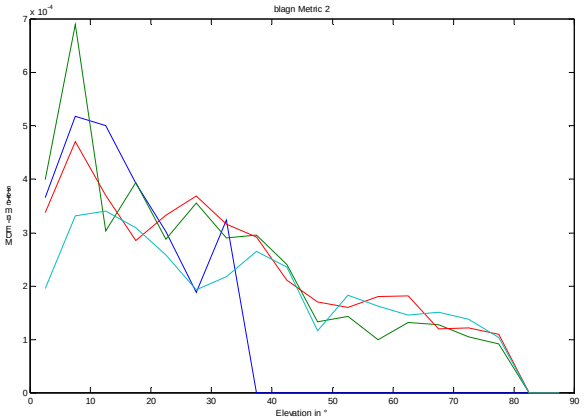

Figure 5: *Collected σ for test metric $\Delta_{\pm 0.1} - \Delta_{\pm 0.05}$ at BLAGNAC airport for PRN 15.*

Finally, figure 6 shows the σ collected by Stanford University for PRN 5 for different passes using a choke-ring antenna, located on the top of Durand Building.

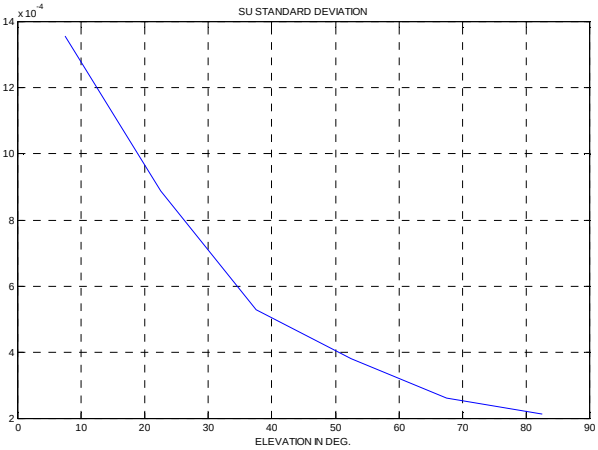

Figure 6: *Collected σ for test metric $\Delta_{\pm 0.1} - \Delta_{\pm 0.05}$ at Stanford University for PRN 5.*

MDE values observed in STNA are generally higher than the ones presented by Stanford. This is due to the high exposure to multipath in this test configuration (sub-optimal site and no built-in robustness in antenna).
The measurements collected in Blagnac Airport are a lot better and are in line with the initial values collected at Stanford.

Gloablly, it was agreed that there is a good consistency between the theoretical and observed statistics of all the test metrics.

The adopted standard deviations for all the test metrics at 5° for the simulations were:

Test metric	$\Delta_{\pm 0.075} - \Delta_{\pm 0.05}$	$\Delta_{\pm 0.1} - \Delta_{\pm 0.05}$	$R_{\pm 0.05}$
σ	**$6.21 \cdot 10^{-4}$**	**$1.34 \cdot 10^{-3}$**	**$8.50 \cdot 10^{-4}$**
Test metric	$R_{\pm 0.075}$	$R_{\pm 0.1}$	$R_{-0.1}$
σ	**$1.40 \cdot 10^{-3}$**	**$1.79 \cdot 10^{-3}$**	**$1.02 \cdot 10^{-3}$**

Test metric	$R_{-0.075}$	$R_{-0.05}$	$R_{+0.05}$
σ	**$1.02 \cdot 10^{-3}$**	**$8.69 \cdot 10^{-4}$**	**$8.8 \cdot 10^{-4}$**
Test metric	$R_{+0.075}$	$R_{+0.1}$	
σ	**$1.96 \cdot 10^{-3}$**	**$3.01 \cdot 10^{-3}$**	

VI. RESULTS IN THE BASELINE CASE

The results presented in this section are the worst-case airborne differential tracking errors for one particular threat model. These worst case errors are computed in the following way:

- For each parameter value in the threat model
  - Compute multiple correlator output.
  - Compute each test metric.
  - If the magnitude of any of the test metric is larger than the corresponding MDE, then the anomaly is detected, and the pseudorange correction is not transmitted
  - If not, then the pseudorange correction is transmitted
    - For each RF filter bandwidth
      - For each chip spacing
        - Compute the tracking error
        - Compute the differential tracking error using the received correction
        - Determine the magnitude of the maximum differential tracking error observed up to now
      - End;
    - End;
  - End;
- End;
- Plot the magnitude of the maximum differential tracking error for all the evil waveforms in the threat model.

These values are all computed assuming the satellite has a 5° elevation angle. The corresponding airborne MERR at 5° is 3.5 m. In each case, the ground filter is a 6th order Butterworth filter with double sided bandwidth BW2=16 MHz. The MDEs were artificially increased by 20 % to take into account any error in the setting of the MDE values. In addition, we assumed that the test metrics were actually averaged over 3 receivers before being compared to the test thresholds.

The initial propositions of constraints for the airborne users would only allow receivers with the pairs of double sided bandwidth and chip spacings presented in table 1.

Region	3dB Pre-correlation Bandwidth, BW2	Average Correlator Spacing
1	0<BW≤7 MHz	0.045-1.1
2	7<BW≤16 MHz	0.045-0.21
3	16<BW≤20 MHz	0.045-0.12

Table 1: *Initial proposition of constraints on allowed receiver designs.*

Figures 7, 8 and 9 show the final airborne differential tracking error for Early minus Late DLLs.

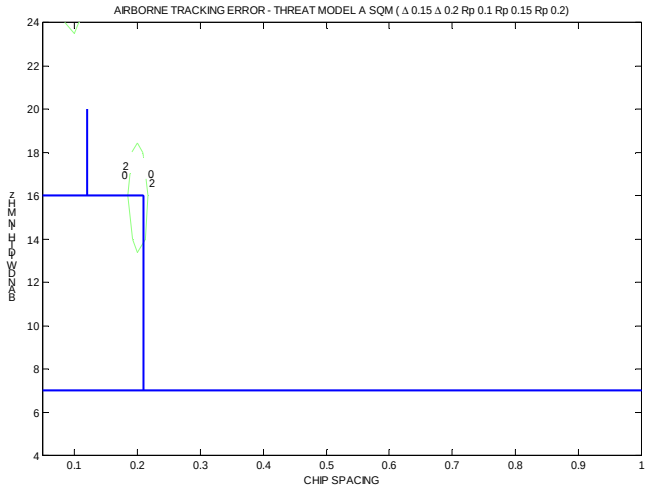

Figure 7: *Airborne differential tracking error for E-L DLLs for threat model A.*

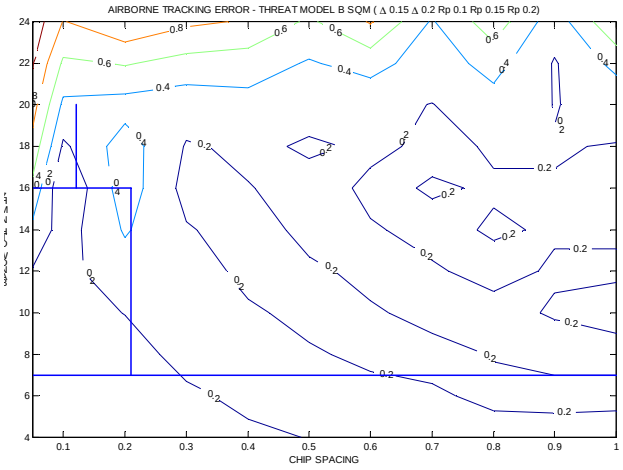

Figure 8: *Airborne differential tracking error for E-L DLLs for threat model B.*

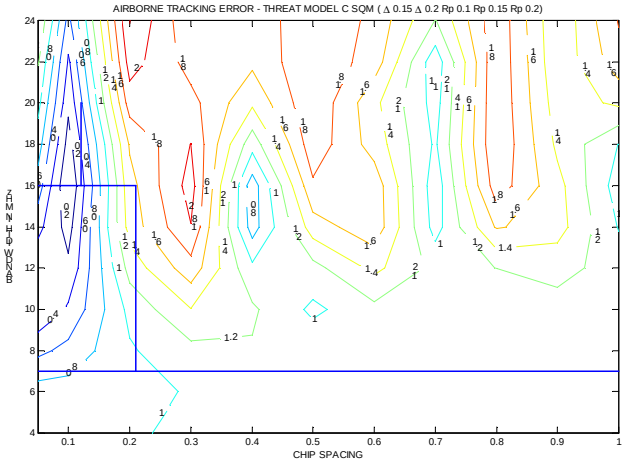

Figure 9: *Airborne differential tracking error for E-L DLLs for threat model C.*

Another type of DLL discriminator function was investigated called Double Delta. The discriminator

function of this DLL is $2\Delta_{d/2} - \Delta_d$ Figures 10, 11 and 12 show the final airborne differential tracking error for Double Delta DLLs. The tracking error is plotted as a function of the narrowest correlator pair.

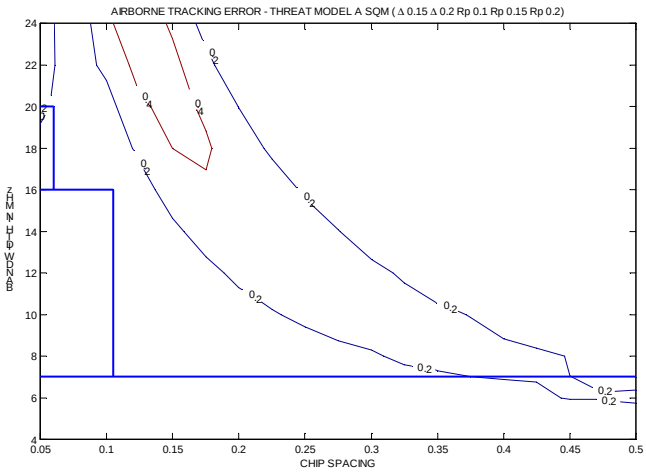

Figure 10: *Airborne differential tracking error for ΔΔ DLLs for threat model A.*

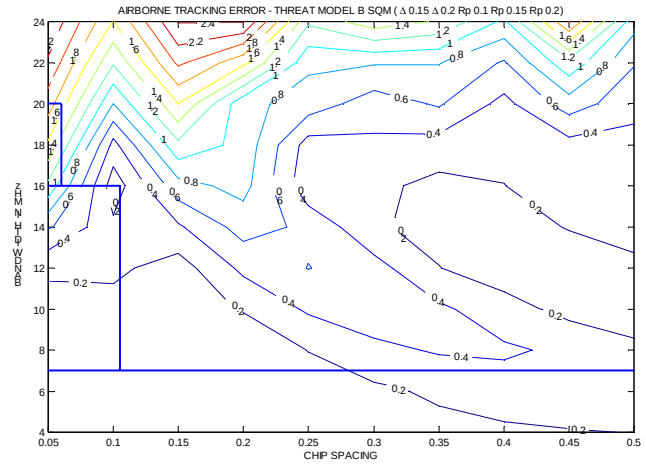

Figure 11: *Airborne differential tracking error for ΔΔ DLLs for threat model B.*

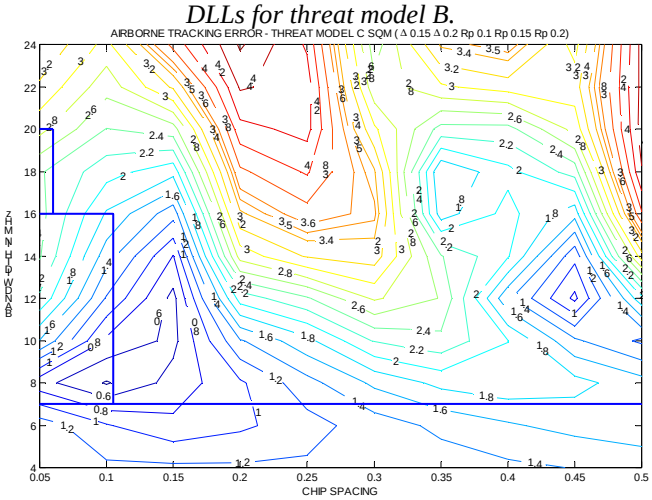

Figure 12: *Airborne differential tracking error for ΔΔ DLLs for threat model C.*

Additional simulations were run to determine the suitability of these constraints for higher elevation satellites. Indeed, as the elevation angle increases, the errors affecting the test metrics are reduced, allowing a better detection of anomalous signals. However, as shown in figure 2, the maximum tolerated error (MERR) decreases with the elevation angle. Therefore, it was necessary to test the protection provided by this SQM for satellites at all elevation angles. It was shown that all E-L correlators were properly protected with the initial constraints, while double delta receivers were not protected for large bandwidth receivers.

Similar simulations were run by other teams, and all results were extremely consistent. Therefore, we decided to reshape the constraint areas to fit the results.

VII. INFLUENCE OF RF/IF FILTER GROUP DELAY

Early in the process of the definition of the constraints, it was anticipated that the group delay variation of both the ground and the airborne receiver filters would influence the effect of the evil waveforms on the tracking error. These variations are brought by the antenna and by the RF front-end filters. It was considered a reasonable assumption that the ground reference station does not bring any significant group delay variation because of its large bandwidth and the likely use of SAW filters. Therefore, it was decided to limit the variation of the group delay of all the filters applied to the signal by the airborne receiver to 150 ns.

In order to check the validity of this constraint, we have implemented a filter that would have the magnitude response of a Butterworth 6 filter, with a maximum group delay variation of 150 ns.

The filter of the airborne receiver is modified from the transfer function of a 6th order Butterworth filter. The final magnitude response is kept equal to the response of the butter filter, while the phase response is adapted such that the maximum differential group delay variation reaches 150 ns at the corner frequency for all the simulated bandwidths. Filtering of the signal is performed in the frequency domain using the modified filter and the obtained filter output is converted back to the time domain.

This adaptation is illustrated in the following figures.

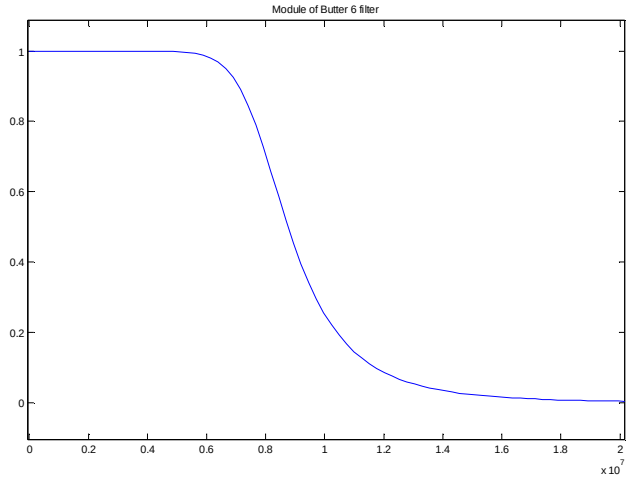

Figure 13: *Magnitude response of original Butter 6 filter*

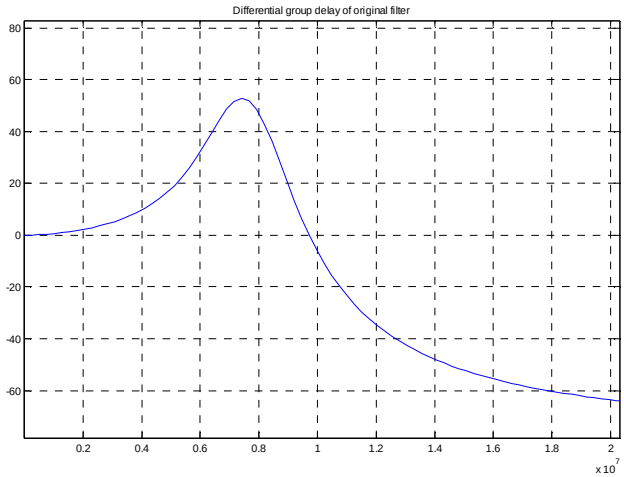

Figure 14: *Differential group delay response of original Butter 6 filter*

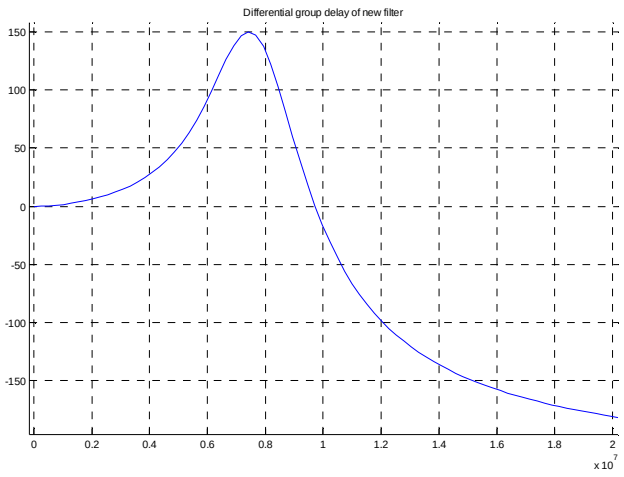

Figure 15: *Differential group delay response of modified filter*

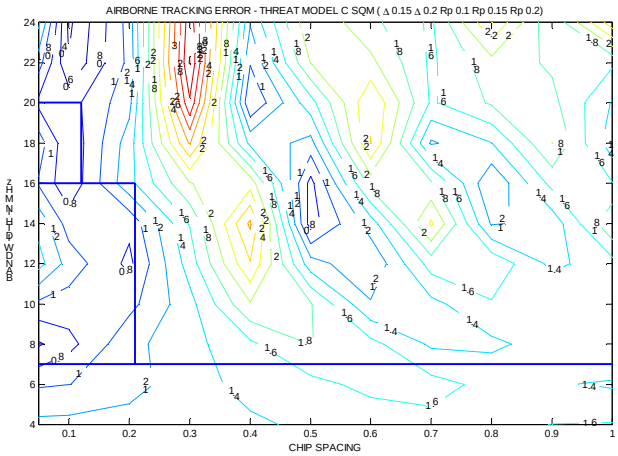

Figure 15: *Airborne differential tracking error for threat model C.*

For E-L airborne receivers, the results presented above show that the proposed requirements for regions 2 and 3 are appropriate. The maximum error is slightly increased (relative to the baseline case) but still meets the 3.5 m requirement.

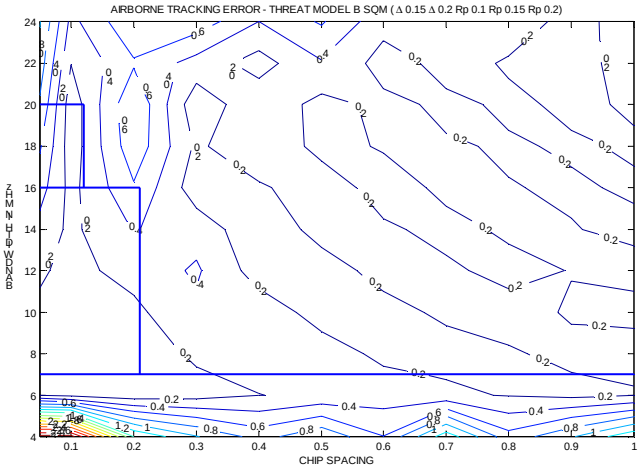

Figure 16: *Airborne differential tracking error for threat model B, airborne filter = butter 9.*

For region 1, it was shown that unacceptable airborne differential errors are obtained for high order Butterworth filters (larger or equal than 9), as illustrated in figure 16. The absence of requirement in terms of differential group delay is therefore not acceptable. It was recommended that a 600 ns differential group delay requirement is added for region 1. This value corresponds to the maximum differential group delay for a 7th order Butterworth filter with BW2=4 Mhz.

VIII. TEST ON REAL RECEIVERS

In order to test the validity of the results obtained with the simulation software, we decided to build a test bench that would allow to test the behaviour of real receivers submitted to evil waveforms. In order to build this test bench very quickly, we tried to use an already

existing GPS signal generator that would simply transmit classical signals to an RF module designed to generate evil waveforms from this input. The quickest way to do that was to build a filter generating a model B evil waveform at L1.

The RF filter is designed to generate an evil waveform with the following parameters : Δ=0, Fd=7 MHz, σ=0.8 MHz..

The following figures present the theoretical transfer function and group delay of the low-pass equivalent filter of the final RF filter.

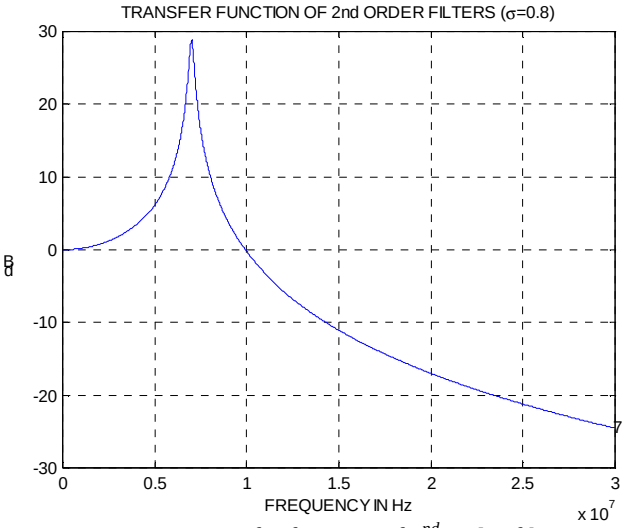

Figure 17: *Transfer function of 2nd order filter.*

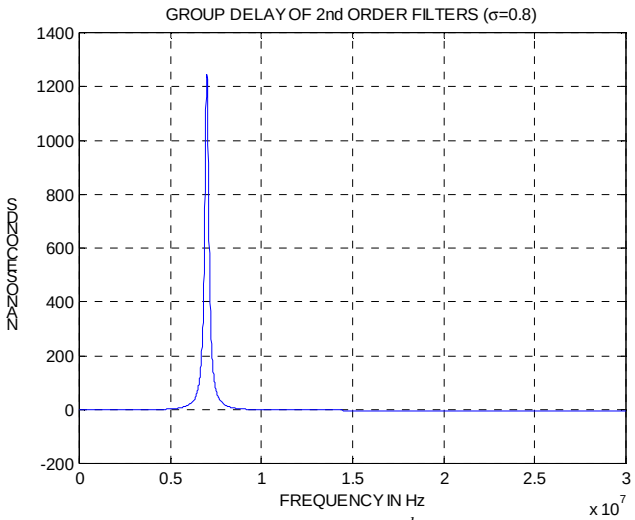

Figure 18: *Group delay of 2nd order filter.*

The filter is implemented using a waveguide to limit the signal losses, as shown in figure 19.

Figure 19: *Evil filter* .

The GPS signal generator is configured to deliver satellite signals for a primary and a secondary antenna that are both omni-directional antennas located at the exact same fixed position. The signals for each of the antennas are available on two different ports. The front panel output delivers signals with the preset power level while the back-end output delivers a signal which is 60 dB higher than the front panel output.

The back-end secondary output signal is sent to the EVIL filter, then to a 20dB attenuator, and finally to the 3dB coupler, where it is added to the signal delivered by the front panel primary output.

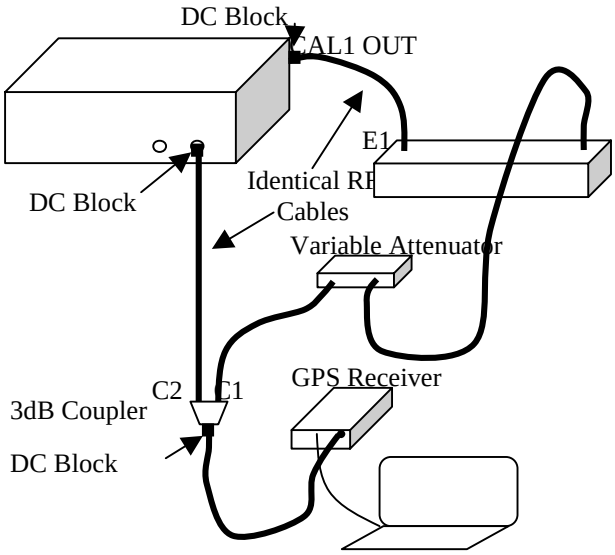

Figure 20: Test *set-up* .

The scenario that is run is designed such the generator delivers a signal for 9 satellites. Among these 9 satellites, 2 of them have the exact same ephemeris data. These satellites are PRN 18 and PRN 32. As soon as the scenario is launched, the transmission of all satellite signals on the primary channel is turned off, except for PRN 18 signal. Similarly, only the transmission of PRN 18 signal is interrupted on the secondary output, and all the other signals are sent.

Therefore, the receiver gets the sum of two signals :

- the attenuated and filtered PRN 18 signal
- the nominal signals from the other satellites, including PRN 32.

The estimation of the measurement error due to the EVIL filter is achieved by subtracting the measurements made on PRN 32 to the measurements made on PRN 18. This can only be done once the systematic propagation errors are calibrated. These errors are the differential propagation delay between CAL1 OUT-C1 and A2-C2, as well as the propagation delay offset at the signal generator output between CAL1 OUT and A2.

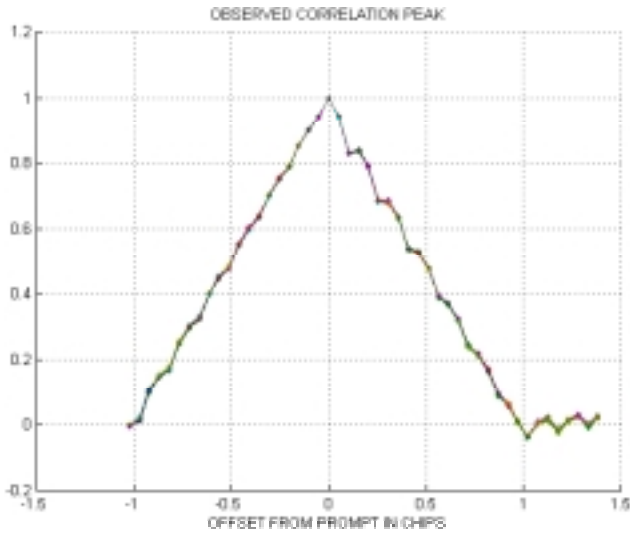

Figure 21: *Observed correlation peak* .

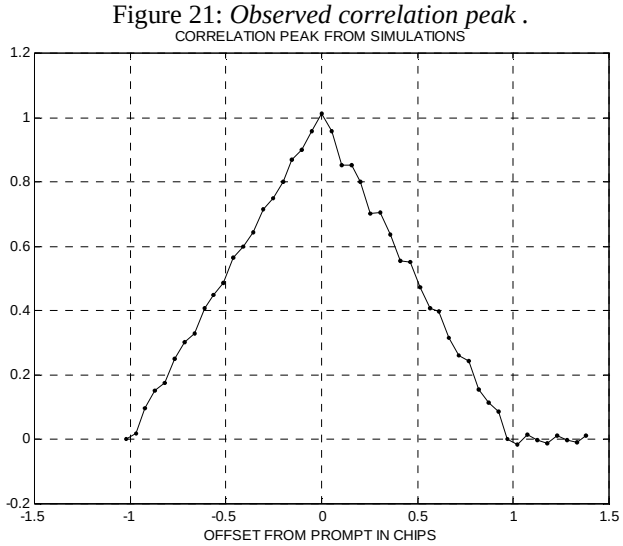

Figure 22: *Simulated correlation peak* .

Real receivers can indeed acquire and lock on the evil waveform generated by our set-up.

The measurement errors induced by the generated evil waveform that we have extracted from the raw measurements range from –1.6 m to 4.2 m depending on the receiver.

The comparison between the observed and the predicted errors is summarized in the following table:

	Butter 6	Cheby 6	**SAW FIR 300**	OBSER-VED
Millenium 0.1	2.2 m	2.3 m	**2.2 m**	2.33 m
Millenium 1	2.8 m	4.6 m	**1.2 m**	1.93 m
Millenium 0.05	2.6 m	2.4 m	**3.2 m**	4.16 m
GPSCard MET (0.2-0.4)	0.1 m	0.6 m	**0.0 m**	-1.31 m
Topstar EL 0.1	1.0 m	0.8 m	**-0.8 m**	-1.40 m
Topstar EL 0.2	0.1 m	0.6 m	**-0.7 m**	-1.38 m
Topstar EL 0.4	-0.2 m	-0.3 m	**-0.8 m**	-1.56 m
Topstar EL 0.8	-0.1 m	0.3 m	**-0.7 m**	-1.17 m
Topstar ΔΔ 0.1-0.2	0.1 m	0.8 m	**-0.3 m**	-1.15 m
Topstar ΔΔ 0.2-0.4	0.7 m	0.9 m	**0.1 m**	-1.25 m
Topstar ΔΔ 0.4-0.8	-0.7 m	-0.7 m	**-0.1 m**	-1.61 m
MEAN OF ERROR	1.0 m	1.3 m	**0.5 m**	
STD OF ERROR	1.0 m	1.3 m	**0.8 m**	
MAX |ERROR|	2.4 m	2.7 m	**1.5 m**	
MEAN |ERROR|	1.3 m	1.7 m	**0.9 m**	

The measurement errors predicted using our simulation software highly depend on the nature of the assumed RF/IF front-end filter, inducing a dispersion of about 1.5 m across the different filters. The best-fitting filter is a 300 pt FIR filter, that matches all the observed measurement errors with an average estimation error of 0.9 m, which is quite good. A better fit with the observed values could probably be obtained with improved models of these filters, provided by manufacturers.

IX. CONCLUSION

The investigations presented in this paper have required significant effort on a short period of time in order to support the finalization of ICAO and RTCA standards in a timely fashion. The successful outcome was possible thanks to efficient and fruitful cooperation with Stanford University GPS Lab, Honeywell, Raytheon, Sextant and AJ Systems.

The final recommendations included in the SARPS material are the following ones:

In order for the ground monitor to protect users against the different threat models described above, it is necessary to assume that aircraft receivers have some specific characteristics. If no such constraints were assumed, the complexity of the ground monitor would be un-necessarily high. Future evolutions in the technology may lead to improved detection capability in the aircraft receiver and may alleviate the current constraints.

For double delta correlators, the aircraft receivers shall track the strongest correlation peak over the full code sequence for every ranging source used in the navigation

solution to avoid potential false locks created by such discrimination functions.

For aircraft receivers using Double Delta correlators and tracking GPS satellites, the pre-correlation bandwidth of the installation, the correlator spacing, and the differential group delay are within the ranges as defined in the following table:

GPS Tracking Constraints for Early-Late Correlators

Region	3 dB Pre-correlation bandwidth, BW	Average Correlator Spacing (chips)	Differential Group Delay
1	2<BW≤7	0.045-1.1	≤ 600 ns
2	7<BW≤16	0.045-0.21	≤ 150 nsec
3	16<BW≤20	0.045-0.12	≤ 150 nsec
4	20<BW≤24	0.08-0.12	≤ 150 nsec

For aircraft receivers using Double Delta correlators and tracking GPS satellites, the pre-correlation bandwidth of the installation, the correlator spacing, and the differential group delay are within the ranges as defined in the following table:

GPS Tracking Constraints for Double-Delta Correlators

Region	3 dB Pre-correlation bandwidth, BW	Average Correlator Spacing range (chips)	Differential Group Delay
1	2<BW≤7	0.045-0.6	≤ 600 ns
2	7<BW≤14	0.045-0.24	≤ 150 nsec
3	14<BW≤16	0.07-0.24	≤ 150 nsec

REFERENCES

[Enge et al., 1999] P. ENGE, E. PHELTS and A. MITELMAN, « Detecting Anomalous Signals from GPS Satellites », Global Navigation Satellite System Panel meeting, Toulouse October 18-29 1999, working paper 19.

[Macabiau and Chatre, 2000] C.Macabiau and E. Chatre, « Impact of Evil Waveforms on GBAS Performance », IEEE PLANS 2000, San Diego

[Pullen and Van Dierendonck, 2000], S. Pullen and A.J. Van Dierendonck, « Proposed Reallocation of LAAS SQM Fault-free Alarm Probability and Resulting MDE Reductions (Rev.1) », January 24, 2000.

[Shively, 1999] C. SHIVELY, « Derivation of Acceptable Error Limits for Satellite Signal Faults in LAAS », ION GPS-1999.

[Shively et al., 1999] C. SHIVELY, M. BRENNER and P. KLINE, « Multiple Ground Tests Protecting Against Satellite Correlation Symmetry Faults in LAAS (Revision 3)», RTCA SC-159, 1999.