BaSE: Development of a Galileo PRS Receiver

F. Schubert, J. Wendel
Astrium GmbH
Taufkirchen, Germany

M. Sgammini, A. Konovaltsev, M. Meurer
German Aerospace Center (DLR)
Oberpfaffenhofen, Germany

A. Rügamer, P. Neumaier, F. Garzia,
P. Sommer, G. Rohmer
Fraunhofer IIS
Nürnberg, Germany

S. Baumann
IABG mbH
Ottobrunn, Germany

***Abstract* — The paper presents the hardware architecture of the Galileo PRS receiver developed within the BaSE project, and describes the core technologies required for using the Galileo PRS service. The approaches for increasing the robustness against radio frequency interference by using single sideband tracking techniques, adaptive notch filtering and pulse blanking are described. The potential of utilizing the direction of arrival estimation and correlation function analysis for detecting spoofing and meaconing counterfeit signals is discussed. Further challenges addressed in the paper include handling of the wideband PRS signals with multi-peaked correlation functions in real-time.**

Keywords— Galileo PRS, interference mitigation, receiver platform, robust navigation, beamforming, security related applications, BOC tracking

I. INTRODUCTION

The increasing use of GNSS for military and security-related applications is generating a higher demand for robust positioning/navigation solutions. Galileo's Public Regulated Service (PRS) targets governmental and authorized users, e.g. defence, police, border control, emergency, armed forces, and Search and Rescue (SAR), as well as operators of critical infrastructures like telecommunication- and energy-networks and critical transports. Most of these "new" user communities do not have the same level of experience with security-related equipment as military users; therefore, a dedicated security-architecture has to be chosen to allow a user-friendly handling of PRS-receivers. The basic security framework for the handling of PRS receivers will be given by the Common Minimum Standards (CMS) and the subsequent Implementing Acts and related technical documents. The CMS are being ratified at the moment by the European Council and are expected to be published early 2014. The Implementing Acts and related technical documents will follow-on later.

The Public Regulated Service will be one of the first Galileo services to become available: First PRS signals are already transmitted by the four IOV satellites and dedicated PPTI (PRS Participants To IOV) trials are ongoing in various Member States. Full automated PRS will be supported when the two Galileo Security Monitoring Centers will become operational in 2016.

The PRS service features two encrypted signals on two frequency bands. A PRS receiver has to deliver robust, reliable, and continuous position information even under challenging reception conditions and also in jammed environments, requiring a considerable robustness against interference. Further, a protection against signal meaconing and spoofing has to be provided as well as means to control the use of GNSS signals within a local/regional area of operations. All these issues make PRS receiver development a very demanding task.

Within the BaSE (Bayerischer Sicherheitsempfänger) project, a consortium consisting of six Bavarian companies and research institutes was formed to investigate core technologies, acquire necessary know-how, and develop a high-end Galileo PRS receiver prototype. The project is co-financed and supported by the Bavarian Ministry of Economic Affairs.

The BaSE consortium has developed within the first BaSE (Bavarian security receiver) project in 2010-2012 key technologies for Galileo PRS receivers including a versatile receiver platform, the analysis of potential security module architectures and the first verification of functional implemented cryptographic functions. Moreover the focus of the first BaSE project was on tracking the ambiguous binary offset carrier (BOC) modulated signals with a double estimator (DE) correlator and to implement interferer mitigation by means of an adaptive 2x2 array processing [1].

In the successor project BaSE-II – timeframe 2012-2014 – the objective is now to finalize all essential components needed for a Galileo PRS receiver demonstrator and to integrate them on a functional level. In addition BaSE-II focuses more on interference mitigation on receiver level, like the detection of interference, the usage of adaptive filter algorithms for interference suppression, meaconing and spoofing detection based on correlation function analysis and spatial filtering. Moreover BaSE-II features a new robust BOC tracking algorithm combined with a single sideband tracking depending on the interference environment. Other non-technical goals of BaSE are the identification of national users and applications for Galileo PRS, the analysis of their specific requirements, the coordination with national and European PRS interfaces, projects, and developments as well as the elaboration and integration of a capable IT-security concept into the receiver

system, and aspects related to future standardization and certification of PRS receivers. Future integration of PRS receivers into the whole Galileo PRS-Management and Security infrastructure are further tasks performed within the BaSE project, as well as basic considerations on combined PRS/PMR (TETRA) and PRS/GPS PPS use. Further a preliminary key-loading and –management interface will be developed.

The paper is structured as follows: In the next Section, the signals employed for the Galileo PRS service are reviewed. Then, The BaSE receiver hardware is described, followed by a discussion of the signal processing techniques for BOC tracking and interference mitigation. Finally, conclusions are drawn.

II. GALILEO PRS SIGNALS

A. BOC Modulation

A simplified model of a BOC signal in baseband, ignoring effects of finite front-end bandwidth, front-end distortions and quantization, is given by following expression

$$s(t) = \frac{A}{\sqrt{2}} \cdot c(t-\tau) \cdot b(t-\tau) \cdot e^{j(\omega_{dop} t + \varphi)} + n(t)$$

Hereby, $c(t)$ denotes the PRN code with chip duration T_C and chip rate $1/T_C$, $b(t)$ is the bipolar rectangular subcarrier with sub-chip duration T_S and subcarrier frequency $1/(2T_S)$. A positive and a negative sub-chip together form one subcarrier period of duration $2T_S$, like a positive half-wave and a negative half wave form one period of a sinusoid. The Doppler frequency is denoted with ω_{dop}, the signal's phase with φ, A is an amplitude scaling factor, and $n(t)$ is additive white Gaussian noise. The navigation message data which additionally modulates this signal has been omitted, as it is in general not relevant for tracking considerations. A BOC signal is identified by the subcarrier and the PRN code rate. Both are expressed as multiples of 1.023 MHz, so a BOC signal with a subcarrier frequency of $m \cdot 1.023$ MHz and a code rate of $n \cdot 1.023$ MHz is referred to as BOC(m,n). If the transitions of the subcarrier are aligned with the transitions of the code chips, a sine-phased BOC signal results; if the subcarrier transitions are shifted by half a sub-chip duration $T_S/2$ w.r.t. the code chip transitions, a cosine phased BOC signal results, denoted with BOCc or BOCcos. The autocorrelation function (ACF) of a BOCcos(15,2.5) signal, which is used for the Galileo PRS service in E1, is shown in . The multiple positive and negative peaks are clearly visible. The code envelope, i.e. the ACF of the corresponding BPSK signal, is shown as well. An overview on the Galileo PRS Signals on E1 and E6 is given in Table 1.

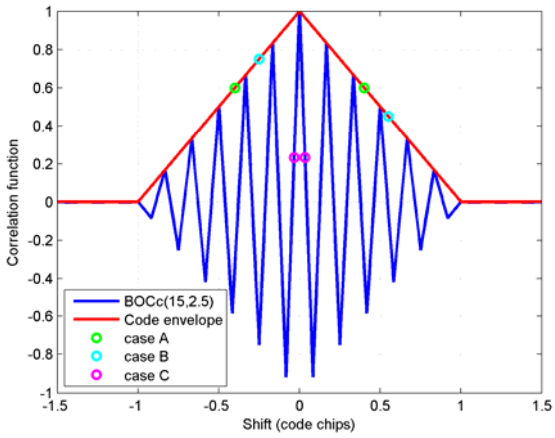


Fig. 1. BOCc(15,2.5) ACF and triangular ACF of the corresponding BPSK signal

TABLE I. GALILEO PRS SIGNALS

GNSS Signal	*Carrier Frequency (MHz)*	*Modulation*
Galileo E1A PRS	1575.42	BOCcos(15,2.5)
Galileo E6A PRS	1278.75	BOCcos(10,5)

III. BASE RECEIVER HARDWARE

A. Receiver Architecture

Fig. 2 shows the BaSE-II receiver block diagram. A 4-element dual-frequency (E1 and E6) array antenna is used to set the basis for protection against signal meaconing and spoofing with high interference mitigation capabilities. The BaSE-II receiver incorporates a calibration transmitter featuring the PRS signals for a receiver self-calibration. The analog signal conditioning (filtering, amplification, down-conversion) is done in separate quadruple radio frequency (RF) analog front-ends for E1 and E6, respectively. The analog-to-digital conversion (ADC) with digital signal conditioning is carried out in the successive digital front-ends. One digital front-end is used for the four E1 channels and one for the four E6 channels. All necessary clock signals (for the ADCs and the FPGAs) and local oscillator (LO) signals (for the analog mixer stages) are coherently derived and distributed on a dedicated clock and local oscillator generation module. Using an optical multi-gigabit transceiver link (MGT), the digital raw data from the digital front-ends are transferred to the pre-correlation interference mitigation module whose output is finally fed into the baseband receiver hardware, again using an optical MGT. All computationally demanding tasks like the acquisition and the correlators are implemented on the digital baseband FPGA. The tracking loops are closed in software running on a standard PC over a PCIe link where both the beamforming and the PVT with RAIM and spoofing detection are also implemented.

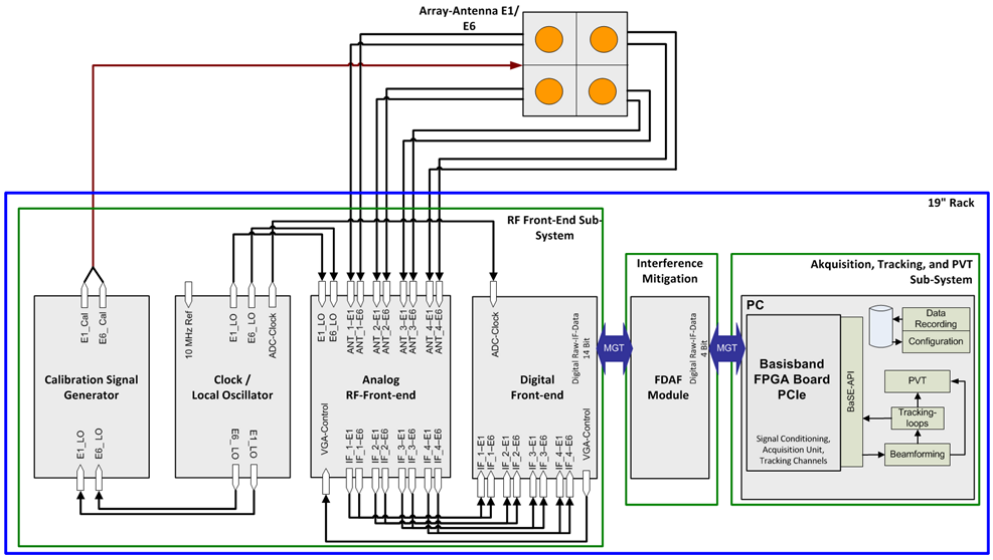


Fig. 2. Overall BaSE-II receiver block diagram

The hardware setup of the BaSE-II receiver is depicted in Fig. 3, excluding the antenna. The RF front-end sub-system is realized using 6 units of height modules. The interference mitigation module, as well as the baseband FPGA are installed within a standard 19" rack PC. An optical cable patch panel gives the possibility to include or exclude the interference mitigation module for different signal combinations. All these components are mounted in a 19" desk chassis using overall 12 units of height.

B. Baseband Hardware

The block diagram of the BaSE-II baseband design is depicted in Fig. 4. Eight MGT are used to receive the filtered and preprocessed digital data stream with a total of 16.8 Gbit/s (4 Channels E1, 4 Channels E6 with 75 MSPS @ 14 bit I/Q each). A 6-out-of-14 bit multiplexer allows to select the 6 effective bits to be used for the further baseband processing. At this stage it is also possible to do a parallel snapshot of all either 4 E1 or 4 E6 signal to a so called covariance storage for the analysis of the different reception elements from the 2x2 beamforming antenna used.

Fig. 3. BaSE-II receiver without antenna

The 4 E1 signals, as well as the 4 E6 signals can be assigned to any of the available tracking channels at run-time. This can be done in software by setting the value of a dedicated multiplexer. The basic system configuration is characterized by 24 channels, 8 channels per correlator type. The 3 different correlator types are described below. In the default assignment each antenna is connected to each type of correlator.

The system is equipped also with a dedicated Hardware FFT acquisition module. The module is able to perform a parallel code phase search in the Fourier domain based on a 16K FFT. This enables a fast detection of the satellites of the L1/E1 bands with their respective code delays and Doppler frequencies. These Doppler results can have an accuracy of 2 Hz by using a pre-acquisition search step based on a novel patented algorithm [2]. This guarantees a faster and more reliable transition to the tracking.

The dedicated memories present in the FFT module can be used to make a snapshot from one of the 8 incoming signals. The antenna and the band can be selected at run-time. Up to 81,920 6-bit I/Q samples at 75 MHz sampling rate can be stored and sent to the PCIe interface for offline analysis. This corresponds to a 1.09 ms recorded signal with a frequency resolution of 915 Hz. This enables sophisticated spoofing detection methods, for example by monitoring the 2D-acquisiton search space, as well as interferer detection and characterization methods by employing short-time Fourier transforms (STFT).

There are two different baseband FPGA hardware designs: one experimental with three different types of correlators in parallel and one with 40 channels of the so called Astrium correlators only as described in the following.

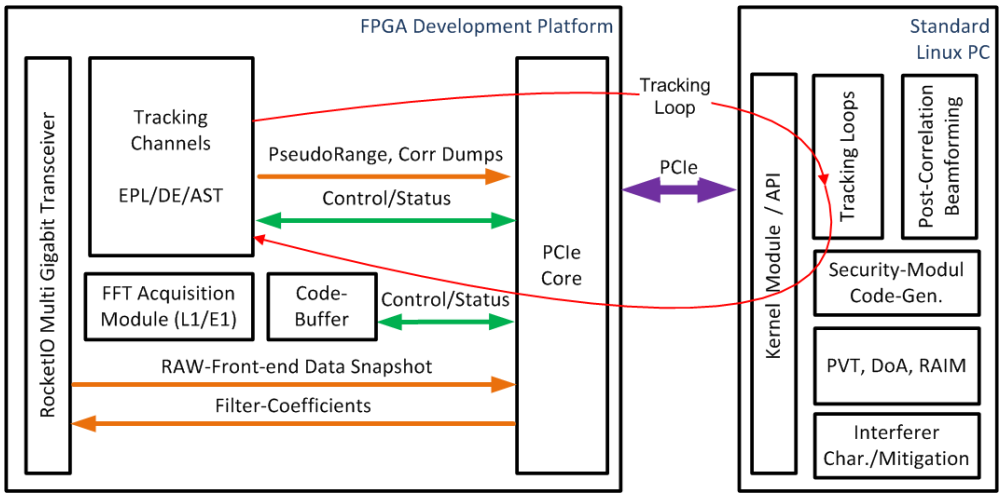


Fig. 4. BaSE-II receiver without antenna

C. Correlator Implementations

The first correlator type is a modified version of a conventional early-prompt-late tracking architecture, which can deal with BOC(1,1), but to track higher order BOC signals some additional algorithms in addition to bump-jumping have to be used to ensure to track really the right peak. This correlator module contains two independent loops: a phase locked loop (PLL) for carrier tracking and a delay locked loop (DLL) for the code tracking. Both Loops are independent and are controlled by numerically controlled oscillator (NCO).

The second correlator type is a modified version of the Double Estimator, which is currently used for test purposes only and will be removed in future. In this module, the multiplication with code replica and signal is separated in three entities instead of two. Next to a standard PLL, the code phase will be simultaneously but independently tracked by a DLL and a subcarrier locked loop (SLL). The function space is now two dimensional due the code and subcarrier delay. This approach is a powerful technique to avoid the subcarrier ambiguities.

The third correlator type is the so called “Astrium correlator”, which uses a PLL for carrier tracking and just one loop for coherent subcarrier and code tracking with five specific fixed subcarrier/code-relation replicas. Due the fixed alignment between subcarrier and code, one DLL is enough being still able to track the BOC signals without peak ambiguity. A brief description of this novel BOC tracking technique is given in Section IV A.

D. BaSE-API / Software-Assisted Hardware Receiver

Using an application programming interface (API) the baseband FPGA can be controlled via a high-speed PCIe interface and the tracking loops closed in software on a standard Linux-PC. This approach uses the advantages of the fast parallel FPGA processing while still providing the flexibility of a software receiver.

External modules, e.g. beamforming, tracking or a code provider can register with the receiver stub by calling register_*cb functions of the API. These callback functions will be executed when a certain event occurs. With this architecture, flexibility is guaranteed by modularity. Low latency hardware access and a fast event handling provide a robust tracking performance.

For example, the code provider is responsible to generate the PRS codes for a channel. Such a functional Galileo PRS software security module is developed by the BaSE consortium member Siemens. It must register itself with the receiver stub. Once this is done, the receiver informs the code provider whenever a new code block is required by a channel. The data exchanged between the receiver stub and the code provider is described in an appropriate structure. This structure contains all necessary information to initialize the provider and continuously retrieve new code blocks. If the relevant flag is set, the code provider uses the data fields GalileoWeekNr and GalileoTow to initialize itself with a correct reference to time. After the initialization the code provider will write subsequent code blocks to memory. From this location, the chips will be written into the hardware using a DMA transfer.

IV. Signal Processing

A. Novel BOC Tracking Algorithm

In the BaSE-II receiver, a novel BOC tracking technique is used, referred to in the following as "Astrium correlator". A block diagram of this technique is shown in Fig. 5.

This architecture also consists of two loops. The first loop is a PLL for carrier tracking. The second loop is closed by tracking the subcarrier. This is achieved using a NCO which in total generates five replicas, denoted with PE, PL, PP, EP, and LP.

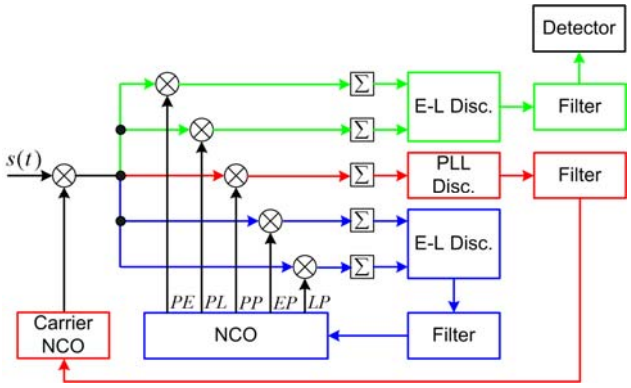


Fig. 5. Astrium Correlator block diagram

These replicas are composed as follows:

PP	Prompt subcarrier, prompt code
EP	Early subcarrier, prompt code
LP	Late subcarrier, prompt code
PE	Prompt subcarrier, early code
PL	Prompt subcarrier, late code

Ignoring the tracking jitter, the PP replica consists of subcarrier and PRN code, both aligned with the subcarrier and code of the received signal $s(t)$. For the EP replica, the subcarrier is advanced by $1/2 \cdot \Delta T_{EL,S}$ compared to a subcarrier aligned with the subcarrier of the received signal, while the code is still aligned with the code of the received signal. For the PE replica, the code is advanced by $1/2 \cdot \Delta T_{EL,C}$ compared to a code aligned with the code of the received signal, while the subcarrier is still aligned with the subcarrier of the received signal. The construction of the LP and PL replicas is obviously achieved by delaying subcarrier and code, respectively, compared to the received signal.

Multiplying the received digital baseband signal with the PP replica performs a wipe-off of code and subcarrier, so that only the carrier remains. After the integrate and dump operation, a PLL discriminator or FLL discriminator is used to estimate the carrier tracking error, which is fed to the PLL/FLL loop filter in order to generate the steering command for the carrier NCO. Multiplying the signal generated by this carrier NCO with the received signal performs a carrier wipe-off, so that without carrier tracking error after this multiplication, only code and subcarrier remain.

Multiplying the received digital baseband signal after carrier wipe-off with the EP and LP replicas performs a code wipe-off, so that the resulting two signals can be used in an Early-Late discriminator to estimate the subcarrier tracking error. Different types of Early-Late discriminators can be used, including Early-Late power, and Early-Late power envelope. The discriminator output is fed to a loop filter, which generates the steering command for the NCO generating the five replicas described previously, hereby closing the subcarrier loop.

Multiplying the received digital baseband signal after carrier wipe-off with the PE and PL replicas performs a subcarrier wipe-off, so that the resulting two signals can be fed in an Early-Late discriminator of any type. The output of this discriminator is lowpass filtered and fed to a detector. Given that the subcarrier tracking is locked on the main peak, the signal arriving at the detector is zero-mean. Given that a sidepeak is tracked, the mean of the signal arriving at the detector significantly deviates from zero, and the sign indicates whether the false lock is to a sidepeak left or right from the main peak. This allows to identify the false lock, and a correction can be performed so that the subcarrier loop transfers lock from the sidepeak to the neighbouring peak towards the main peak, until a zero mean detector input signal results, indicating the desired lock to the main peak.

This tracking algorithm fully exploits the subcarrier accuracy, and allows for a reliable, fast and robust detection and correction of false locks to side peaks. A detailed analysis of this BOC tracking approach can be found in [3].

B. Interferer Mitigation in the Digital Front-End

The digital front-end performs the analog to digital conversion, followed by a first signal conditioning, the interference mitigation modules, and the high speed multi gigabit transceiver (MGT) interface for the transmission of the raw IF samples. Its block diagram is shown in Fig. 6.

Two interference mitigation methods are applied right to the 2x14 bit raw samples of the analog digital converter (ADC): pulse blanking and digital filtering.

The digital filtering is realized with configurable complex FIR and IIR filters. In an undisturbed environment, the complex FIR filters are configured as standard digital anti-aliasing filters. If a wideband interference is detected, the complex FIR filter can be configured to suppress one of the two BOCc mainlobes, so that the receiver can still track the non-affected one. Moreover, this configurable filter could also be used to intentionally suppress the Galileo OS and GPS C/A signals in a high-pass / band-pass configuration.

If a narrow band interferer is detected, a complex IIR notch filter can be applied directly after the previous described FIR filter. The reason to use a second digital filter is twofold: First a notch filter (in this case of 2nd order) has a significant smaller

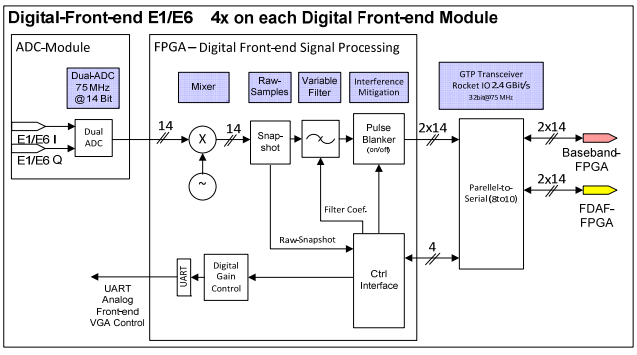


Fig. 6. Digital front-end block diagram

bandwidth as a FIR filter even with a much higher order. Secondly having a second independent filters gives the interferer mitigation methods of the receiver much more flexibility in its reactions.

To be able to detect and characterize an interference source, a snapshot of the raw samples coming from the ADC can be taken and transferred to the baseband receiver PC. There the complete computational power of a standard Linux-PC can be used for interference mitigation. Appropriate filters are designed adaptive to the interference source detected and uploaded to the configurable FIR and IIR filters. It is important that the samples before the digital filtering are used to be able to check if an interference source is still present.

In order to obtain the configuration parameters for the FIR and IIR filters, an analysis of the ADC sample spectrum is performed. The FIR filter is used to suppress a sideband of the BOC signal, if this is corrupted by interferers that cannot be mitigated with a Notch filtering. The Notch filters are particularly efficient to mitigate CW interferers, and are implemented as IIR filters. An IIR filter is described by the difference equation

$$y_n = \sum_{k=0}^{M} a_k \cdot x_{n-k} + \sum_{k=1}^{N} b_k \cdot y_{n-k}$$

which considers for the calculation of the filter output of the current epoch also filter outputs from previous epochs, weighted by the feedback filter coefficients b_k. Many design approaches of IIR filters are inspired by analogue filter implementations, and are therefore not suitable to derive a filter for complex baseband signals, given that a non-symmetric transfer function shall be implemented. One possibility to implement a complex first order IIR notch filter is outlined in the following: The transfer function of such a filter in z-domain is given by

$$\frac{Y(z)}{X(z)} = \frac{1 - z_0 z^{-1}}{1 - k_\alpha z_0 z^{-1}}.$$

Hereby, z_0 is the notch frequency in z-domain, which is given by $z_0 = e^{j2\pi f_{notch} T_S}$, where f_{notch} is the desired notch frequency and $T_S = 1/F_S$. Obviously, the enumerator of transfer function becomes zero for $z = z_0$, creating the notch at the desired frequency. The denominator shows almost the same frequency dependence as the enumerator, thereby assuring a flat pass-band. However, for stability reasons, the so-called pole contraction factor $k_\alpha < 1$ assures that the enumerator does not become zero at the notch frequency, too, because this pole could give rise to instabilities. The choice of k_α allows the regulation of the notch width and is a trade-off between interference attenuation and GNSS signal degradation. In order to obtain a difference equation suitable for implementation, the above transfer function is rearranged giving

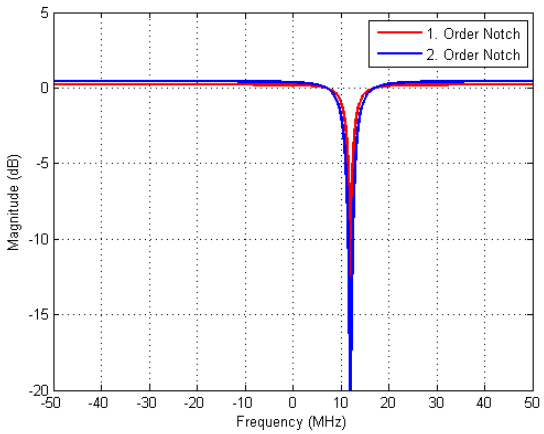


Fig. 7. Transfer function magnitude of 1st and 2nd order notch filter

$$Y(z) = X(z) - z_0 z^{-1} X(z) + k_\alpha z_0 z^{-1} Y(z),$$

and transformation to discrete time yields

$$y_n = x_n - e^{j2\pi f_{notch} T_S} x_{n-1} + k_\alpha e^{j2\pi f_{notch} T_S} y_{n-1}.$$

A second order notch filter is obtained by squaring the transfer function of a first order notch filter, yielding finally following difference equation:

$$\begin{aligned} y_n = x_n &- 2e^{j2\pi f_{notch} T_S} x_{n-1} + e^{j4\pi f_{notch} T_S} x_{n-2} \\ &+ 2k_\alpha e^{j2\pi f_{notch} T_S} y_{n-1} - k_\alpha^2 e^{j4\pi f_{notch} T_S} y_{n-2} \end{aligned}$$

For illustration, the magnitude of the transfer functions of first and second order notch filters is shown in Fig. 7.

Finally the filtered output of the digital front-end is streamed using RocketIO multi gigabit transceivers (MGT) to either the dedicated interference mitigation FPGA module or directly to the baseband hardware.

C. Interferer Mitigation FPGA Module

Besides the interference mitigation technique based on adaptive Notch Filtering, the robustness of the receiver can be furthermore increased by implementing an advanced signal processing algorithm. It extends the capability of the receiver to counteract, under particular circumstances, non-stationary radio frequency interference (RFI). The price to be paid is an increase in the computational complexity of the system.

The mitigation is based on the frequency domain adaptive filtering (FDAF) approach described in [1],[4]. This technique is implemented at the digital IF level directly after the A/D converter, allowing the realization of tracking channels with moderate number of input signal bits.

FDAF is based on Fast-Fourier Transform (FFT). It is especially capable of detecting and mitigating narrowband RFI sources [5] and is effectively implemented for block processing in real time.

The working principle is illustrated in Fig. 8. It consists in nulling out those frequency bins exceeding a threshold previously fixed, in other terms in the excision of the bins that

with a certain probability contain the interference energy. In the frequency domain, the contribution of the thermal noise is a constant which is generally estimated with a bias and an estimation variance. This variance could hide the spectral components of an interfering signal. The estimation variance represents a very relevant aspect for the detection techniques: the lower the estimation variance, the lower the false alarm probability (P_{FA}) and higher the detection probability (P_D).

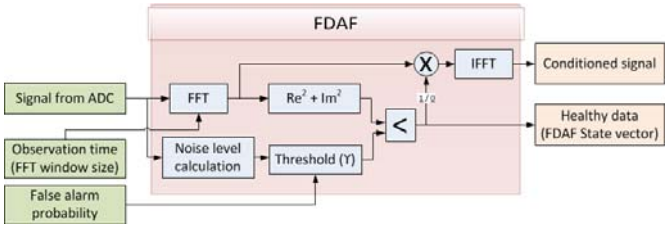


Fig. 8. FDAF Architecture

According to [6] fixing the desired P_{FA}, the corresponding threshold Υ is given by:

$$\gamma = \sigma^2 \ln\left(\frac{N/2-1}{P_{FA}}\right)$$

Where σ^2 is the variance of the received signal and N is the FFT length, in this case equal to 1024 samples.

Once the threshold Υ is fixed, the corresponding P_D depends on the Probability Density Function (PDF) of the RFI. If the PDF of the interfering signal is known, the P_D can be determined by integrating it over the interval [P_{FA}, ∞]; in other case P_D shall be determined numerically via Monte-Carlo simulations.

One of the major issues of FDAF is the spectral leakage effect, which spreads Fourier components that are not harmonic to the fundamental frequency over the adjacent frequency bins. This reduces drastically the selectivity in frequency of the algorithm and leads to the excision of a wider portion of the spectrum than strictly needed.

To overcome this problem the signal being processed by the Fourier transform shall be firstly multiplied by a scaling window.

A rich selection of windowing functions can be found in the literature; here 17 different scaling windows made available by MatLab R2011a have been used.

The windows have been evaluated in terms of reduction of the leakage effect, or in other words in terms of improvement in the interference mitigation capability. At this scope it has been used as test signal a sine wave with frequency f_i falling between two adjacent harmonic to the fundamental frequency.

A subset of 4 out of 17 windows has been selected. The selection was based valuating the best responding windows for different size of nulled bandwidth, varying from 1 to 6 frequency bins around f_i.

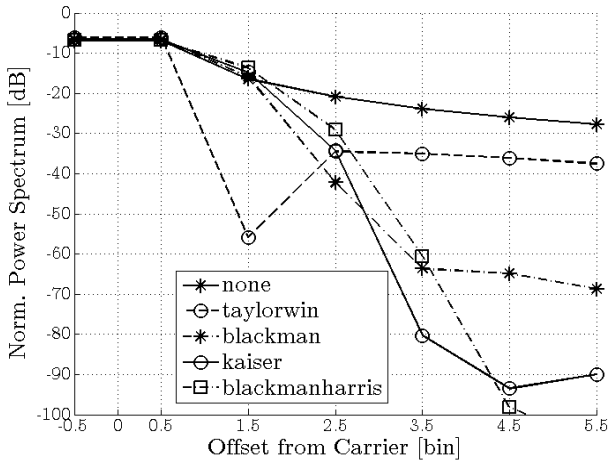


Fig. 9. Single-side FFT spectrum of a sine wave signal after windowing

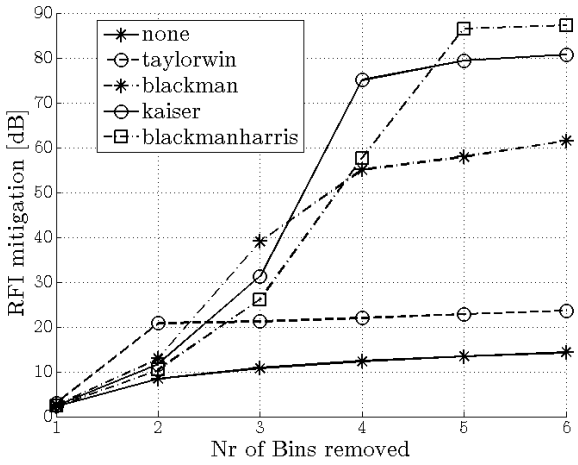


Fig. 10. Mitigation capability of a sine wave signal after windowing

In Fig. 9. the single side spectra after windowing and FFT for the selected scaling windows ('none' indicates that no scaling window is used) are shown. The sharper the spectrum, the better the FDAF performance, since the interferer power will be confined in a smaller portion of spectrum.

Fig .10 shows the cumulative RFI attenuation capability as a function of the number of bins around the sinus carrier frequency f_i considered for excision.

The window coefficients can be stored in form of a 5-bits array on the FPGA ROM. More than one windowing function can be stored on the ROM allowing an online selection of the desired window.

The conditioned time signal is obtained via an Inverse FFT of the altered spectrum. Two overlapping windowing functions and two FDAF units are needed in order to reduce amplitude distortion caused by each single scaling window (see Fig. 11).

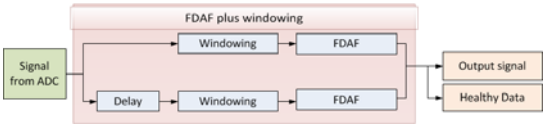


Fig. 11. Mitigation schema using FDAF plus windowing

D. Interferer Mitigation with Adaptive Antenna Array

The utilization of antenna arrays and the associated signal processing techniques in the BaSE receiver enables mitigation of radio frequency interference in the spatial domain. The mitigation of interfering signals is achieved by controlling the reception pattern of the antenna array and adaptive adjustment according to changing signal conditions. The methods for interference mitigation in time and frequency domains described above can be further used in the combination with the adaptive antenna leading to enhanced overall mitigation performance.

The adaptation of the array reception pattern is based on continuous estimation of the statistics of the array signals, such as the array covariance matrix $\mathbf{R}_{xx}$. In a GNSS receiver, there are principally two options for collecting the required signal statistics: before and after the de-spreading operation. In the first case, the useful signals are buried into the noise and the signal statistics is determined either by noise and/or radio interference. After de-speading, i.e. after the PRN code correlation, the estimated statistics is determined by the tracked satellite signal and, if present, multipath echoes.

The two main goals of using adaptive antenna array in the BaSE receiver prototype are (see Fig. 12):

- Before de-spreading, the main focus is on mitigation of radio frequency interference (RFI). The placement of the RFI mitigation before PRN code correlation allows to design the signal processing blocks for a nominal signal dynamic range that is dominated by the receiver thermal noise, which enables practical fixed-point realizations with low bit widths. The signal acquisition, one of the most vulnerable stages of the entire signal processing chain, is additionally assisted by producing antenna gain for the GNSS signal. This is achieved by adding the spatial dimension into the acquisition search space and using switched antenna beams each covering a given spatial search bin (see Fig. 13).

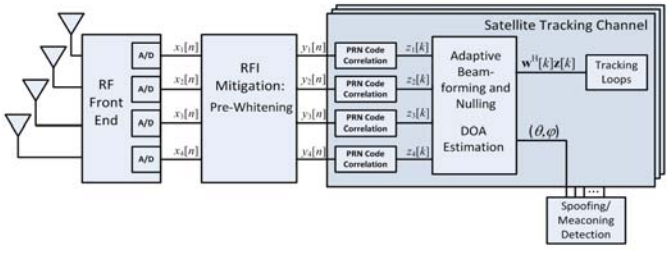


Fig. 12. Adaptive antenna signal processing in BaSE receiver prototype

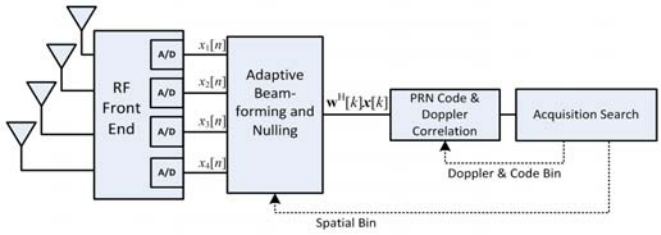


Fig. 13. Use of antenna array in signal acquisition stage

- After de-spreading, the antenna pattern is optimized for the reception of the GNSS signal in term of signal-to-noise-plus-interference ratio (SNIR).

The radio interference mitigation before the PRN code correlation is performed with help of a pre-whitening technique based on the eigenvalue decomposition of the estimated array covariance matrix and an orthogonal projection [7]:

$$\hat{\mathbf{R}}_{xx} = \begin{bmatrix}\hat{\mathbf{U}}_I & \hat{\mathbf{U}}_n\end{bmatrix}\left(\begin{bmatrix}\mathbf{\Lambda}_I & 0\\ 0 & 0\end{bmatrix} + \sigma_n^2\mathbf{I}_M\right)\begin{bmatrix}\hat{\mathbf{U}}_I^{\mathrm{H}}\\ \hat{\mathbf{U}}_n^{\mathrm{H}}\end{bmatrix}$$

$$\mathbf{y} = \mathbf{P}_I^{\perp}\mathbf{x}, \quad \mathbf{P}_I^{\perp} \approx \hat{\mathbf{U}}_n\hat{\mathbf{U}}_n^{\mathbf{H}}.$$

For the adaptive beamforming after PRN code correlation, the following options are available:

- Eigenbeamforming [7]:
  $\mathbf{w} = P\{\hat{\mathbf{R}}_{xx}\}$, where $P\{\hat{\mathbf{R}}_{xx}\}$ denotes the principal eigenvector of matrix $\hat{\mathbf{R}}_{xx}$.
- Minimum mean squared error (MMSE) beamforming [8],[9]:
  $\mathbf{w} = \arg\min_{\mathbf{w}}\left[\left|r - \mathbf{w}^{\mathrm{H}}\mathbf{y}\right|^2\right]$
- Deterministic beam-steering into a direction of the GNSS signal, (θ,φ), given by the scan θ, and azimuth φ, in the antenna local Cartesian coordinate system:
  $\mathbf{w} = a(\theta,\varphi)$
  where $a(\theta,\varphi)$ stands for the array steering vector consisting of the complex values of the reception patterns of the array elements in the direction (θ,φ).

The array weights in the signal acquisition stage (see Fig. 13) are calculated using the linearly-constrained minimum variance (LCMV) approach as described in [10].

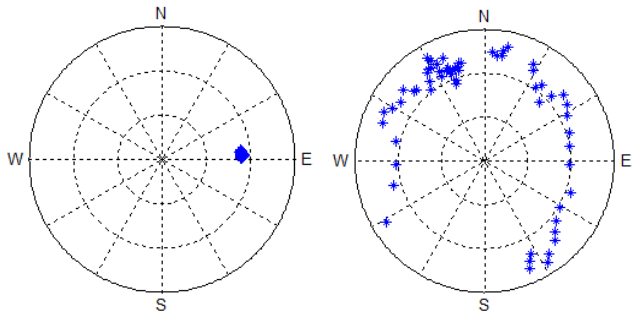
E. Detection and Mitigation of Spoofing / Meaconing

The use of adaptive antenna array technology allows for distinguishing between the authentic and counterfeit GNSS signals in the spatial domain. The detection of the spoofed GNSS signals is based on measuring directions of arrival (DOAs) of all incoming signals with a suitable direction finding method. The estimated DOAs of the authentic signals should be consistent with the geometry of the satellites

constellation that is observed at the user location. In contrast to that, because the spoofed signals are transmitted from a single source the corresponding DOA observations should be closely grouped together in the spatial domain. In view of this, the detection of spoofing and meaconing can be based on the observation of the cross-correlation factors between pairs of individual DOA measurements where such a factor, c_{ij}, for the cross-correlation between the *i*-th and *j*-th measured DOAs is calculated as

$$c_{ij} = \left\langle \hat{\mathbf{e}}_i, \hat{\mathbf{e}}_j \right\rangle$$

where $\hat{\mathbf{e}}_n$ is a unit directional cosine vector corresponding to the *n*-the DOA measurement, (θ, φ), defined as $\hat{\mathbf{e}}_n = \left[\sin\hat{\theta}_n \cos\hat{\varphi}_n, \sin\hat{\theta}_n \sin\hat{\varphi}_n, \cos\hat{\theta}_n\right]^{\mathrm{T}}$. In Fig. 14 exemplary results obtained for the detection of the direction to the repeater of GPS signals simulating a meaconing attack are presented. More details about this spoofing/meaconing detection technique can be found in [11].



a) static user b) dynamic user

Fig. 14. Estimated direction to the repeater of GPS signals

The detected direction of arrival of the spoofed signal can be further used for constraining the beamforming process and placing a spatial null to mitigate the interference.

V. CONCLUSION

The BaSE project enhances the competitiveness of German industry in the field of high-performance satellite navigation and security systems, will allow for an early testing of the integration of PRS-receivers into the Galileo PRS-Management/Security-architecture, and provides the basis for future security-certification of PRS receivers. The close link between research institutes, industrial partners and certification organizations will enable a fast and effective migration from prototypes into products.

ACKNOWLEDGMENT

The BaSE consortium would like to thank the Bavarian Ministry of Economic Affairs, Infrastructure, Transport and Technology for their co-funding and support.

REFERENCES

[1] A. Ruegamer, et al. "A Bavarian Initiative Towards a Robust Galileo PRS Receiver," Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011), Portland, OR, September 2011, pp. 3668-3678.

[2] I. Suberviola, S. Köhler, J. Mendizabal, G. Rohmer, "Doppler Search as Pre-acquisition Step," Proceedings of the 22nd International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2009), Savannah, GA, September 2009, pp. 2646-2652.

[3] F. Schubert, J. Wendel, "BOC Tracking Using Phase and Sub-Carrier Locked Loops", 6th European Workshop on GNSS Signals and Signal Processing, december 5-6, 2013, Neubiberg, Germany.

[4] G.X. Gao et al., "DME/TACAN interference mitigation for GNSS: algorithmsand flight test results", GPS Solutions, Nov. 2012.

[5] M. Cuntz et al., "Field Test: Jamming the DLR Adaptive Antenna Receiver", Proceedings of ION GNSS 2011, 19.-23. Sept. 2011, Portland, Oregon, USA.

[6] J Steven M. Kay, "Fundamentals of statistical signal processing, Volume II, Detection Theory", 1998, pp.279-283.

[7] M. Sgammini, F. Antreich, L. Kurz, M. Meurer, and T. G. Noll, "Blind Adaptive Beamformer Based on Orthogonal Projections for GNSS," in Proceedings of ION GNSS 2012, Sept. 2012, Nashville, TN, USA.

[8] A. Konovaltsev, F. Antreich, and A. Hornbostel, "Performance assessment of antenna array algorithms for multipath and interferers mitigation," in 2nd Workshop on GNSS Signals & Signal Processing - GNSS SIGNALS'2007, 2007.

[9] J. Litva and T. Lo, Digital Beamforming in Wireless Communications. Artech House, 1996.

[10] C. Haettich, M. Cuntz, A. Konovaltsev, G. Kappen, M. Meurer, "Robust Multi-Antenna Acquisition in Time, Frequency and Space for a Digital Beamforming Receiver," in Proc. ION GNSS 2011, 2011, Portland, Oregon, USA.

[11] A. Konovaltsev, M. Cuntz, C. Haettich, and M. Meurer, "Autonomous Spoofing Detection and Mitigation in a GNSS Receiver with an Adaptive Antenna Array," in Proc. ION GNSS+ 2013, Nashville, TN, USA.