JOANNEUM RESEARCH DIGITAL

Institut für Informations- und Kommunikationstechnologien

Blind GNSS software receiver tool for field test assessment

Deliverable FR

Executive Summary

Authors:

Amir Tabatabaei
Dominik Dötterböck
Thomas Pany
Roman Lesjak
Thomas Prechtl

DIG.03-19.AF.002

Final Version 1.0 Oct-2022

IGASPIN

der Bundeswehr Universität München

JOANNEUM RESEARCH DIGITAL

ESA STUDY CONTRACT REPORT – SPECIMEN

ESA Contract No:	SUBJECT:	CONTRACTOR:
4000125806/18/NL/CRS	Blind GNSS software receiver tool for field test assessment Final Report	JOANNEUM RESEARCH

ESA CR( )No:	No. of Volumes: **1** This is Volume No: **1**	CONTRACTOR'S REFERENCE: *DIG*.03-19.AF.002

ABSTRACT:

This Report provides a complete description of all the work done during the study.

Names of authors (listed alphabetically):

Dominik Dötterböck, Roman Lesjak, Thomas Pany, Thomas Prechtl, Michael Schönhuber, Amir Tabatabaei

NAME OF ESA STUDY MANAGER:	ESA BUDGET HEADING:
Gianluca Caparra José Antonio García Molina	

Introduction, Background and Objectives

The project “BLIND” was lead by JOANNEUM RESEARCH with IGASPIN and Universität der Bundeswehr München as subcontracts and was contracted by ESA as answer of the proposal for the ITT ESA AO/1-9413/18/NL/CRS “Blind GNSS software receiver tool for field test assessment in harsh environments”.

The background of the ITT was exploiting navigation signals of opportunity (SoO) with unknown code chip sequences (or symbol sequences) in a GNSS software-defined receiver (SDR). An early assessment of new techniques (e.g., acquisition, tracking and positioning techniques) specifically designed for those signals without the need to have full access to the underlying code chip sequences (or symbol sequences – in case a navigaton message is present) was of interest.

The objectives of the activity were

- to design and develop a software tool to recover automatically unknown code chip sequences (or symbol sequences) from multiple GNSS SoOs and satellites based on low-noise signal recordings from high-gain antennas or arrays of antennas in order to enable the de-spreading and exploitation of those SoOs when received with commercial GNSS antennas;
- to design and develop a blind GNSS SDR concept demonstrator (referred to as “CD”) exploiting automatically the recovered code chip sequences (or symbol sequences). This includes the acquisition and tracking of the corresponding SoO from the signal recorded and the later derivation of a PVT solution;
- to design and implement in the concept demonstrator (CD) advanced techniques for the robust acquisition, tracking and positioning of the SoOs;
- to design and implement in the CD hybrid PVT solutions exploiting both the GPS/Galileo L1/E1 open signals (OS) and the SoOs from multiple GNSS satellites;
- to assess the performance of the CD with real field signals recorded.

State-of-the-Art

The project team decided to go for an antenna array as a high-gain antenna. This has the big advantage of having an omnidirectional high-gain antenna compared to dish antennas. With the focus on an antenna array in mind, an extensive state-of-the-art research was conducted with focus on low to medium-cost commerciall off-the-sheld components (COTS) and potential algorithms and signals to be used.

A market research on GNSS antennas covering the full GNSS L1/E1/G1 plus optionally L-band satellite communication signals was performed. The focus on the selection was a high passive gain, ideally going down to low elevations. Different antenna models (helical, patch, etc., active and passive) were evaluated and four models were bought to investigate them in detail and make practical experiments and test measurements. In the end, the Tallysman 33-VSE6137-01-WR was bought, which is a single frequency embedded antenna model (PCB version) of the VSP6XXX series.

Another market research was done for appropriate sampling platforms (software-defined radios, SDRs). In the end, the two platforms LimeSDR and BladeRF 2.0 xA4 were investigated in detail and the BladeRF 2.0 was chosen.

A state-of-the Art review was done to find an optimal way for the blind sequence generation (BSG). Instead of the traditional way of having a phased array with digital beamforming, a modern approach with some similarities to recent developments in LTE and 5G called “massive MIMO” was elaborated, where the open signals from GNSS are used to generate the phase coherence.

For the use of the unknown satellite signals in a GNSS-SDR, a state-of-the Art review on different tracking strategies was performed. For the purpose of tracking the signals with Binary Offset Carrier (BOC) modulation, narrow correlator, bump jumping, Double Optimization Multi-correlator-based Estimator (DOME), and BPSK-like approaches were investigated.

System Design and Implementation

Based on the chosen components, a link budget calculation was done to recalculate the expected chip error rate (CER) based on the preliminary defined array size of 40 antennas, which was a compromise between maximum costs and achievable accuracy.

Over the course of the project, it was agreed with the Agency to focus on GPS M-Code on the L1 frequency as only signal of opportunity and to leave aside investigations on Galileo PRS signals, Beidou signals and other L-band satellite communication signals. For the exploitation of different frequency bands, only the antennas need to be replaced.

According to the consolidated project requirements, a system design was worked out for the concept demonstrator (CD), which is shown in the following figure. The system was designed and later tested in a way that the chip error rate is sufficiently low for the encrypted GPS M-Code signal.

According to the design, the components were bought and the CD was built, which will be explained in the following paragraphs.

The antenna platform (AP) has the task to collect the data from the 40 elements antenna array to estimate the chip sequences of unknown satellite signals. The antenna elements (Tallysman VSE6137) are connected to 20 dual-channel BladeRF2.0 xA4 SDR platforms.

The receiver platform (RP) has the task to collect data for the GNSS software-defined receiver (GNSS-SDR) to investigate the tracking of the Blind signals. It consists of 4 COTS multi-frequency GNSS antennas, 2 dual-channel BladeRF2.0 xA4 SDR platforms, one single-frequency GNSS antenna connected to a uBlox M8T mass-market receiver.

Each SDR of the AP and RP is connected to a low-cost Intel NUC recording PC for the temporal storage of the samples. The SDR platforms from the AP and RP get their stabilised 38.4 MHz base frequency from one shared GPS disciplined oscillator (GPSDO) for a stable sampling. The recording PCs are synchronised via GPS-based NTP server included in the AP and RP to guarantee a synchronised start of the sampling within less than one second.

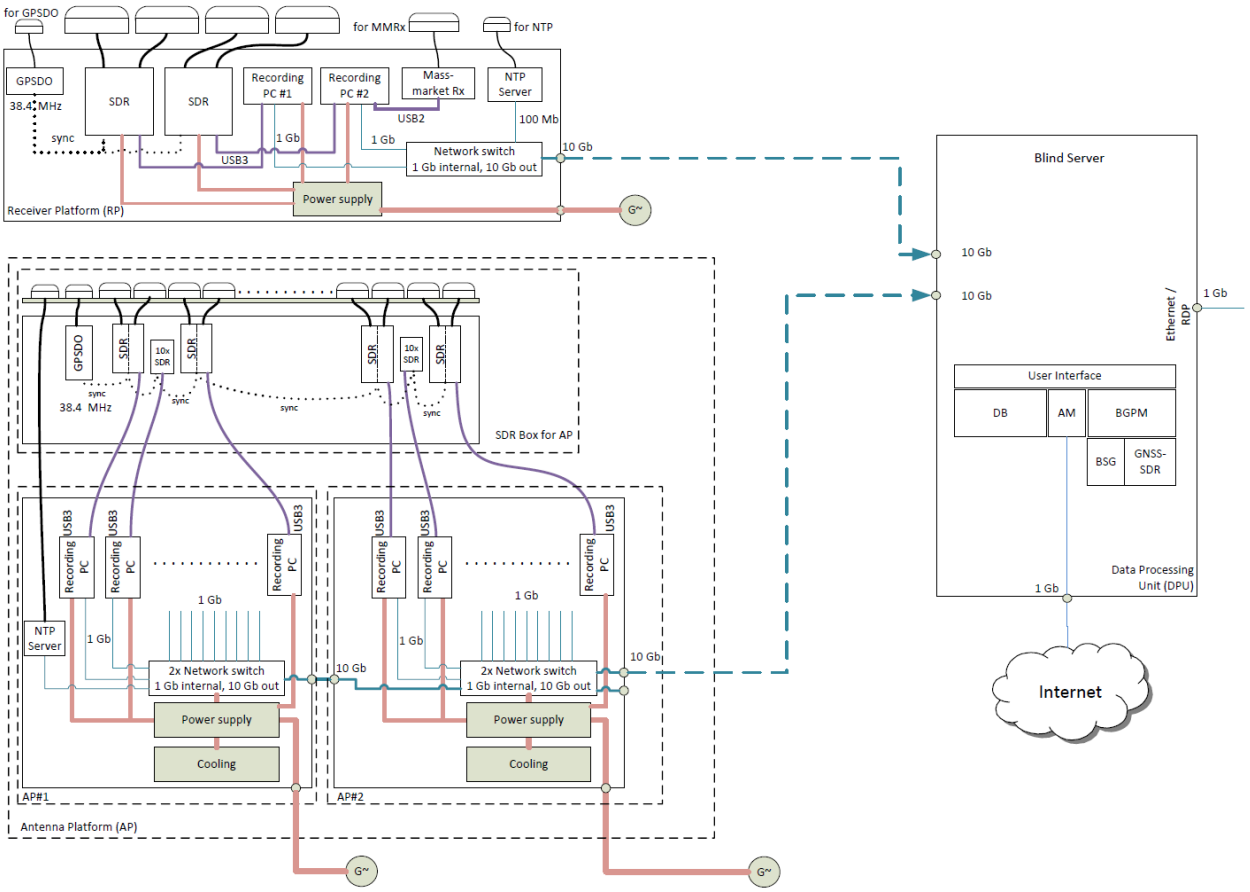

Figure: Design of the Concept Demonstrator

All the recording PCs are connected via 10G ethernet to a Data Processing Unit called Blind Server, which is an AMD Threadripper PC with 32 cores and 8 x 4 TB SATA SSDs in a Raid 0 configuration.

On the software side, a client-server communication was implemented between the Blind server and the recording PCs of AP and RP. On the Blind Server, a user interface allows the configuration of the measurement including the sampling settings, the measurement start time and duration, as well as the later processing settings for the BSG and the GNSS SDR. The user interface triggers the start of the sampling on the recording PCs and waits until the recording is finished. Afterwards, the copying of the data is started. As soon as all data is in the central database on the Blind Server, the BSG (MusNAT software from Uni-Bw München) starts combining the data streams of all 40 antenna elements of the AP. Therefore, first the data streams are exactly synchronised in software, the data is combind to maximize the gain for each satellite signal seperatly before estimating the chip sequences of the defined satellite signals. The BSG allows to configure the modulation scheme of the blind signal, the estimation of a phase offset between open and blind signal and various other parameters. When the BSG is finished, time-tagged chip sequences for each satellite exist and stored in separate files. As a next step, the GNSS-SDR (tailored IGASPIN SX3 version) starts processing the data of the RP to track both open signals from GPS L1 and Galileo E1B and blind signals using the chip sequences of the BSG in a combined PVT solution. The results of the PVT solution are the final results of the CD,

which can be analysed to investigate the potential of the CD. In addition, it is possible to use assistance data in the GNSS-SDR downloaded a-priori.

The following pictures show the implemented system.

Figure: Left: AP antenna array carrier. The low-loss antenna cables from the array are going to the sampling units. Upper right: plate with 40 antennas. Lower right: possibility to tilt unit.

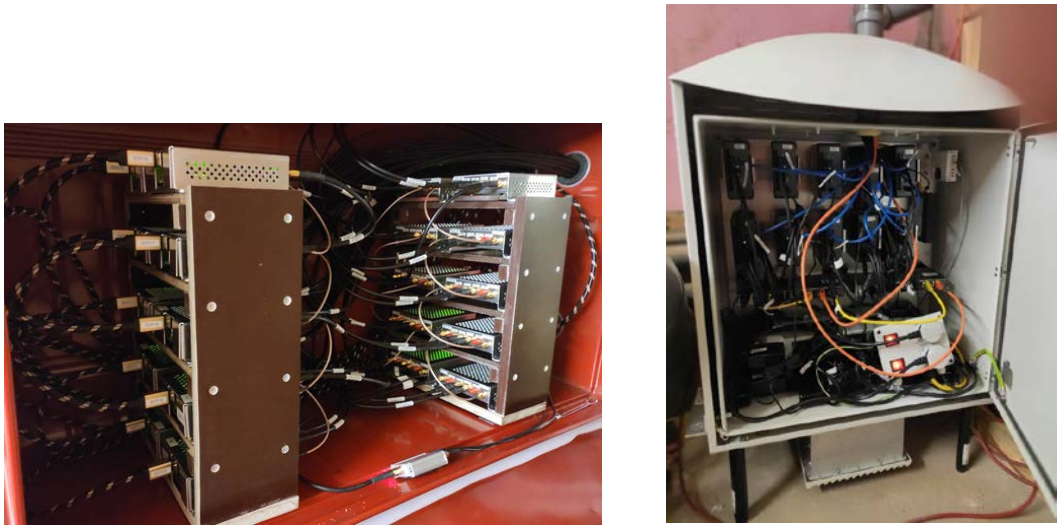

Figure: left: AP cabinet for SDRs. Right: AP cabinet for recording PCs.

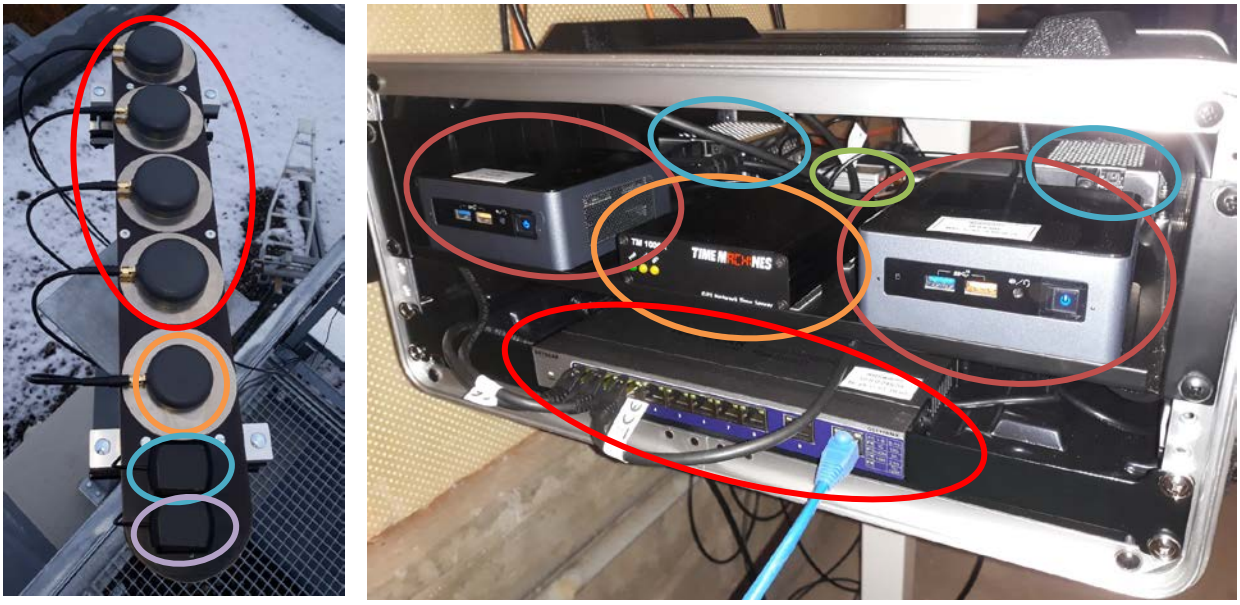

Figure: Receiver Platform: antennas (left) and recording flight case (right).
Antennas: red – RP antennas, orange – antenna for MM receiver, cyan – GPSDO antenna, purple: NTP antenna.
Flight case contents: red – network switch, brown – NUC PCs, orange – NTP server, green – GPSDO, cyan - SDRs

One major challenge during the implementation of the CD was the fact that the SDR platform was causing some electromagnetic interference (EMI), why the antennas needed to be separated from the SDR platforms and recording PCs. Hence, approaximately 12m low-loss RF cables were used to connect the antennas of the AP with the SDR boards.

Another challenge was how to make the CD also work for satellites with a low elevation angle because GNSS antennas usually have less gain at lower elevation to decrease multipath effects. Therefore, a mechanical possibility of the AP was implemented to tilt the AP by up to 50 degrees. This allows to compensate for the decreased gain but not for the higher attenuation due to the longer path through the atmosphere.

Performed Tests and Achieved Results

During the implementation process, numerous (unit) tests in the lab and real world were performed to investigate the correct behaviour of the different components of the CD. As soon as the CD was completed, data analysis based on simulated data streams coming from a GNSS simulator (generation of IQ files for the 40 antennas) were performed. As soon as the system was working as expected, the testing was continued recording the signals in-space – in particular the GPS M-Code with GPS C/A-code as open signal. To veryfiy the CD in general, and the BSG in particular, cross-checking against signals acquired by a 2.4 m dish antenna was done proving that the finally obtained measurements match the expectations. Numerous iterations were performed to continuously improve the quality of the tracking in the GNSS SDR by tailoring the settings to the chosen sampling platform.

Within the next figures, exemplary results are presented.

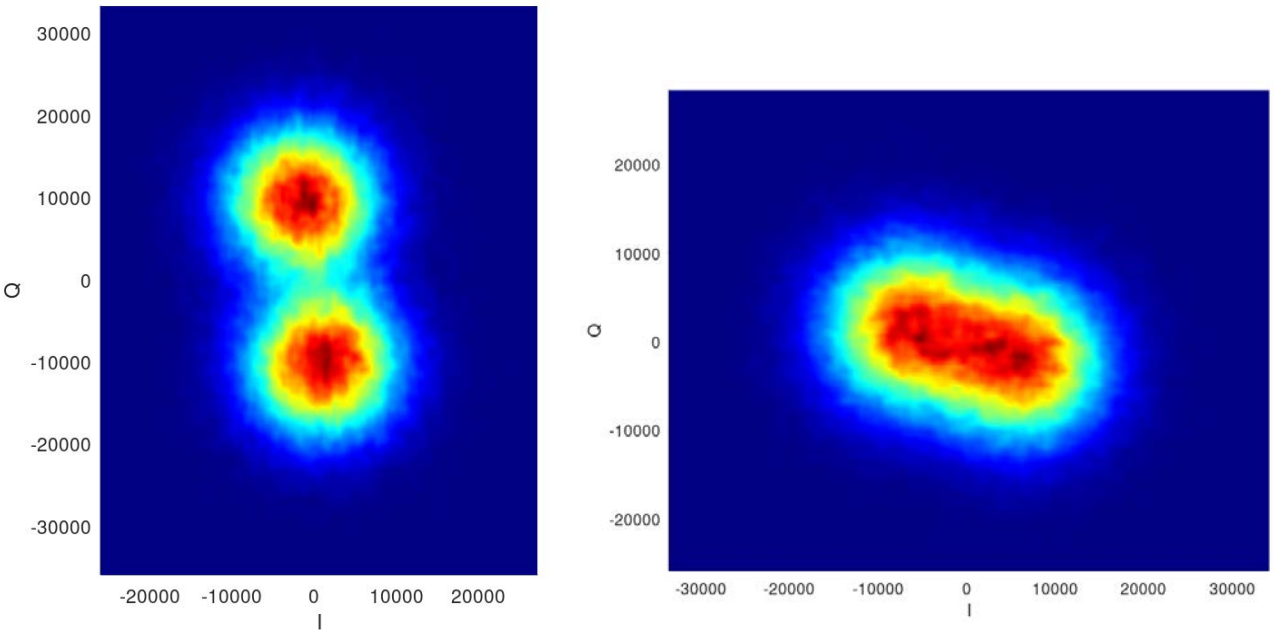

Figure: View of the I/Q histograms for PRN 18 (left) and PRN23 (right) showing the binary modulation of the GPS M-code, after beamforming using all 40 antenne elements of the AP

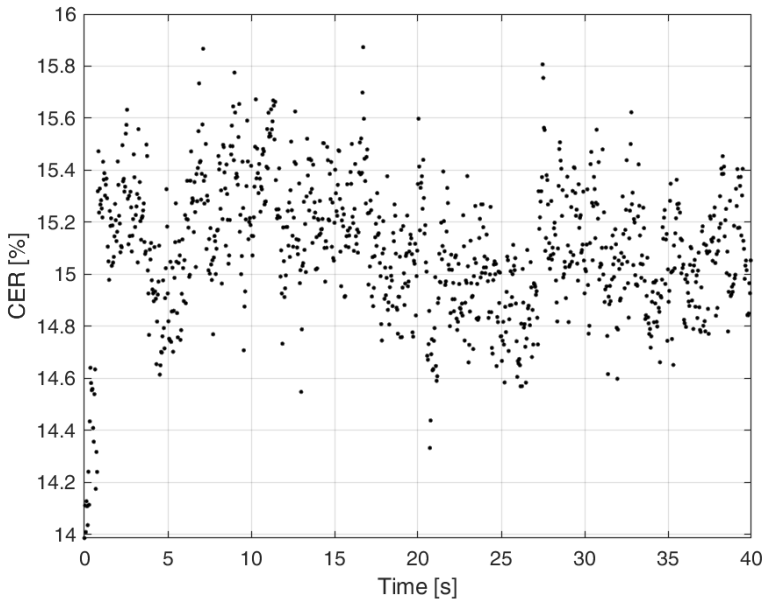

Figure: Chip Error Rate of GPS PRN 18 M-Code. Estimation by comparison with dish antenna measurements.

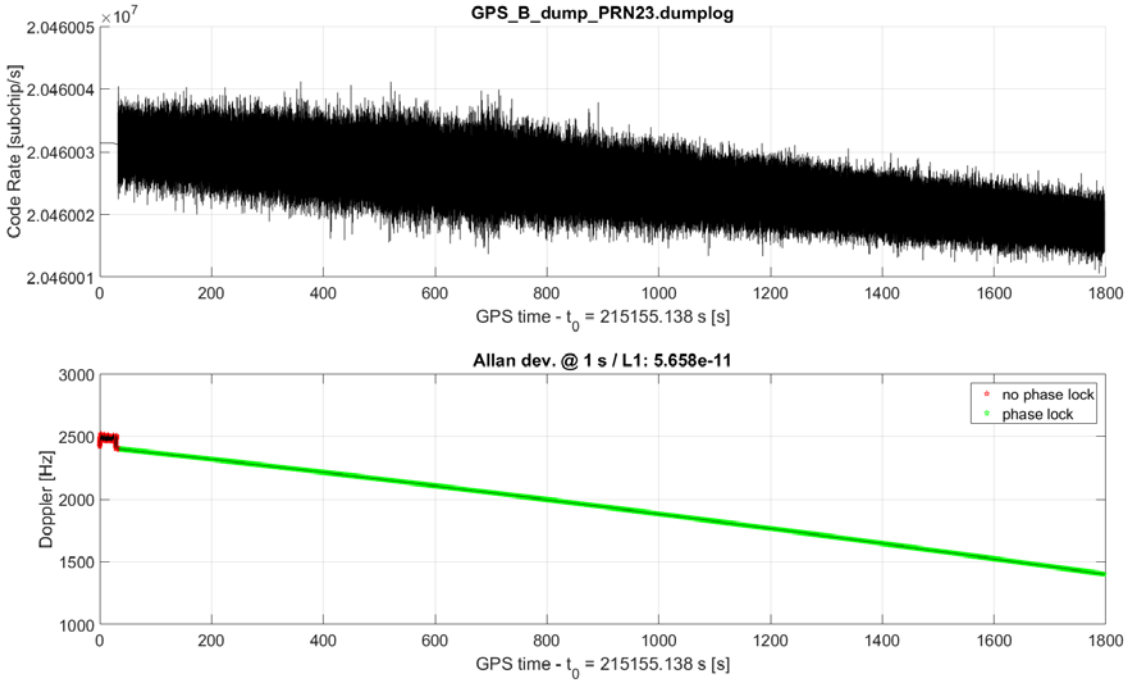

Figure: Code rate and Doppler of the blind tracking for M-code of GPS PRN23

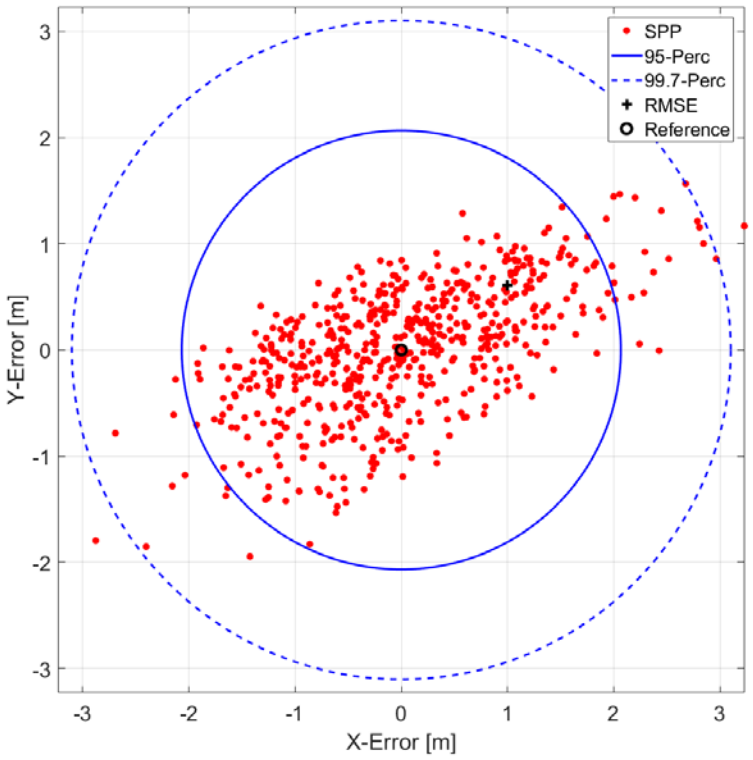

Figure: 2D position accuracy of a PVT solution combining GPS C/A measurements and M-Code observations from PRN18 + PRN23

Conclusions, Lessons Learnt and Merits

Within this project a concept demonstrator for blind GNSS signal processing including chip estimation with a loosely synchronized antenna array has been designed, build, and verified including using the estimated chips within another GNSS receiver to acquire and track the blind signals. The used hardware was based on COTS components. The resulting antenna array is for sure one of the largest arrays ever built for GNSS. The system was designed in a way that the chip error rate is sufficiently low for the encrypted GNSS services of GPS when the satellites are above a certain minimum elevation. The GNSS receiver using the chip sequences can acquire and track those blind signals implementing the tracking loop features necessary for higher order BOC signals. The algorithms and software were verified with simulated signals and performs almost perfectly to the expectations. The full system was verified by making use of a 2.4 m dish antenna to cross-check the estimated chip sequences but also by proving that the finally obtained tracking results match the expectations. The hardware setup is comparable complex, and a number of iterations were necessary until it performed as desired. A considerable limitation within the project was the limited number of test signals/satellites. During the testing phase, only two satellites broadcast the M-code over Europe (PRN18 + 23), hence the obtained results seem limited. The system can however also be configured for other GNSS systems with no or little effort. Possible future navigation satellite systems in LEO can most likely also be handled by the system, if they broadcast in the L1 frequency band. If different frequency bands are used, the antennas need to be replaced. The results obtained for the GPS C/A +M-code signals reported are encouraging that also for other satellite systems reliable chip estimation can be performed and those signals can be acquired and tracked, e.g. for deeper understanding of higher order BOC modulation schemes.

The lessons learnt of this project are varios; in such big systems, electromagnetic interference always has to be taken into consideration. In addition, also the use of COTS products can be quite challenging, but also allows the implementation of cost-efficient systems. The investigations within the system also showed that also encrypted systems are not 100 percent safe against attacks when potentally having such a system with real-time capability (which is not the case here).

Besides the direct results of the project (the working CD), the project team grew together to build a team of harmonizing experts for future challenging activities. Apart of this project, a few high-quality publications with a related topic could be published, also addressing other GNSS signals beside GPS M-code.

JOANNEUM RESEARCH
Forschungsgesellschaft mbH

Leonhardstraße 59
8010 Graz

Tel. +43 316 876-0
Fax +43 316 876-1181

pr@joanneum.at
www.joanneum.at

oef mfg 12 008