The Journal of Navigation (2025), **78**:2-3 339–357
doi:10.1017/S0373463325101343

CAMBRIDGE UNIVERSITY PRESS

RESEARCH ARTICLE

Low-cost SDR-based GNSS signal recorder and replayer for equipment testing

Karolis Stankevičius and Rimvydas Aleksiejūnas

Institute of Applied Electrodynamics and Telecommunications, Vilnius University, Vilnius, Lithuania
Corresponding author: Rimvydas Aleksiejūnas; Email: rimvydas.aleksiejunas@ff.vu.lt

Received: 15 December 2022; **Revised:** 18 September 2025; **Accepted:** 10 October 2025; **First published online:** 07 November 2025

Keywords: BEIDOU; GALILEO; GLONASS; GNSS; GP; L1+L5; multi-band; record and replay; SDRS

Abstract
The need for Global Navigation Satellite System (GNSS) receiver testing increases with the advent of widespread Internet of Things (IoT) technologies and other electronic devices dependent on position determination. In this paper, a low-cost GNSS multiband L1+L5 signal recorder and replayer for equipment testing purposes is proposed. It is implemented using Software-Defined Radio (SDR) modules HackRF One with proper time and phase synchronisation. The recorder–replayer has been tested with GPS, GALILEO, BEIDOU and GLONASS satellites and several commercial GNSS receivers. Reduced GNSS signal bandwidth of approximately 10 MHz is sufficient for efficient reception of recorded signals. Performed tests with a driving car show applicability of this GNSS recorder–replayer in dynamic settings.

1. Introduction

Recent years have shown rapid growth in electronic devices requiring global position determination. As an example, in 2022, the number of connected Internet of Things (IoT) devices reached 14.4 billion globally and is projected to grow further (Hasan, 2022). To perform their functions, some of these devices need to know their location that can be achieved by integrating Global Navigation Satellite System (GNSS) receivers into IoT devices. However, usually, GNSS signals are very weak since transmit power varies from 20 to 265 W (Steigenberger et al., 2018) and orbit height varies from 20,000 to 23,000 km (Jeffrey, 2015). At the receiver, the signal power can be as low as -163 dBW, which is below the noise floor (China Satellite Navigation Office, 2019). In addition, GNSS radio signals in urban areas are degraded significantly due to multipath caused by buildings and other obstacles (Vagle et al., 2016). For these reasons, before electronic devices can be produced and sold at scale, they must be thoroughly tested to determine their GNSS capabilities.

To test an IoT device, one may use a GNSS simulator, which can record and playback GNSS radio signals. An example of such a device could be LabSat 3 Wideband (Racelogic, 2022) capable of recording and replaying up to 20 simultaneous GNSS signals in multiple bands, for example, L1 and L5. However, in general, GNSS simulators are expensive and the choice is limited. Therefore, manufacturing companies that develop GNSS-enabled devices have to find sufficient justification to make an investment into such devices for simulating GNSS signals. The high price of GNSS simulators is the reason for such companies to explore alternatives, like simply driving around the city with a device prototype and analysing logs, which is far from ideal.

Taking everything into account, there is a genuine need for a GNSS simulation solution that would be cheaper and not be reliant on prototypes of unknown capabilities. Currently, there are Software-Defined

© The Author(s), 2025. Published by Cambridge University Press on behalf of The Royal Institute of Navigation. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

https://doi.org/10.1017/S0373463325101343 Published online by Cambridge University Press

Radio (SDR)-based solutions, like a Software-Defined GPS Signal Simulator (Ebinuma, 2022), which can simulate only GPS L1 C/A signals or GNSS record–replay systems described by Chen et al. (2013), Di et al. (2012) and Hennigar (2014), which mostly perform simulations only of GPS L1 C/A signals (Di et al., 2012 is an exception). These simulators use hardware that, in total, cost as much if not more than commercial solutions, are mostly not portable (Hennigar, 2014 is an exception) and are almost 10 years old.

As of the writing of this paper, there is not a single SDR-based GNSS record–replay simulation solution that is capable of recording and replaying all L1 and L5 GNSS signals, and that is relatively cheap and portable. Therefore, the goal of this research is to create a GNSS L1+L5 record–replay simulator, which can simulate L1 and L5 signals, and is affordable and portable.

The paper is organised as follows. Section 2 details the problem description and reviews related published works. Section 3 introduces SDR implementation of a GNSS record–replay simulator with time and phase synchronisation techniques, Section 4 contains simulator test results in static and dynamic environments for GPS, GALILEO, BEIDOU and GLONASS satellites on L1+L5 bands, and finally, conclusions are drawn in Section 5.

2. Problem description and related work

2.1. Characteristics of GNSS radio signals

Currently, there are six different GNSS constellations, which can be used independently, and more than 20 different types of GNSS signals. All signals are transmitted between 1,164 and 1,610 MHz, and the aggregate of all constellations and signals constitute what is known as the global navigation satellite system. Radio frequency spectra of GNSS are illustrated in Figure 1. For GNSS signal spectra generation, the GNSS-matlab library (Pascual, 2022) was used. Most civilian signals are located in the L1 and L5 bands, and signals of these bands are used also in IoT applications. Therefore, for the purposes of this work, only the signals in the L1 and L5 bands will be discussed further.

The main characteristics of GNSS signals located in L1 and L5 bands can be found in GPS Directorate (2021a,c), European Union (2021), China Satellite Navigation Office (2017, 2018, 2019), Glonass, ICD (2008) and GPS Directorate (2021b). There are some specific details that need to be addressed to successfully record these signals. One such characteristic is related to GPS L1C, GALILEO E1 and BEIDOU B1C signals. All of these signals are rather complex, because they use TMBOC(6,1,1/11), CBOC(6,1,1/11) and QMBOC(6,1,3/44) modulations, respectively. These modulations are similar because they are essentially various possible combinations of Binary Offset Carrier BOC(1,1) and BOC(6,1) modulations, which allow distributing signal power over data and pilot components of the signal (Hein et al., 2006; Yao et al., 2010). Frequency spectra of the GPS L1C, GALILEO E1 and BEIDOU B1C signals are shown in Figure 1a.

Another signal to be discussed is GALILEO E5a. This signal is part of the GALILEO E5 signal, which uses altBOC(15,10) modulation. The spectrum of E5 signal is shown in Figure 1b together with the GPS L5 signal. From the figure, it is clear that the E5 main lobes are very similar to the main lobe of GPS L5 Binary Phase Shift Keying BPSK(10) modulation. This was done by design so that both E5 lobes can be received and processed independently as E5a and E5b signals. Receivers can even demodulate E5a as the BPSK(10) signal (Rodriguez, 2008).

The third signal which needs more attention is GLONASS L1 C/A, because unlike other GNSS systems, GLONASS uses the Frequency Division Multiple Access (FDMA) technique (GLONASS, ICD, 2008). This means that to transmit GNSS data, GLONASS uses 14 channels and each channel has its centre frequency defined by

$$f_{cp} = 1602 + 0.5625p \ \text{MHz} \tag{1}$$

where p is the channel number in the interval $-7 \leq p \leq 6$. The width of each channel is only 0.511 MHz and all 14 channels need 7.3125 MHz of bandwidth. The frequency spectrum of GLONASS L1 C/A is shown in Figure 1d.

https://doi.org/10.1017/S0373463325101343 Published online by Cambridge University Press

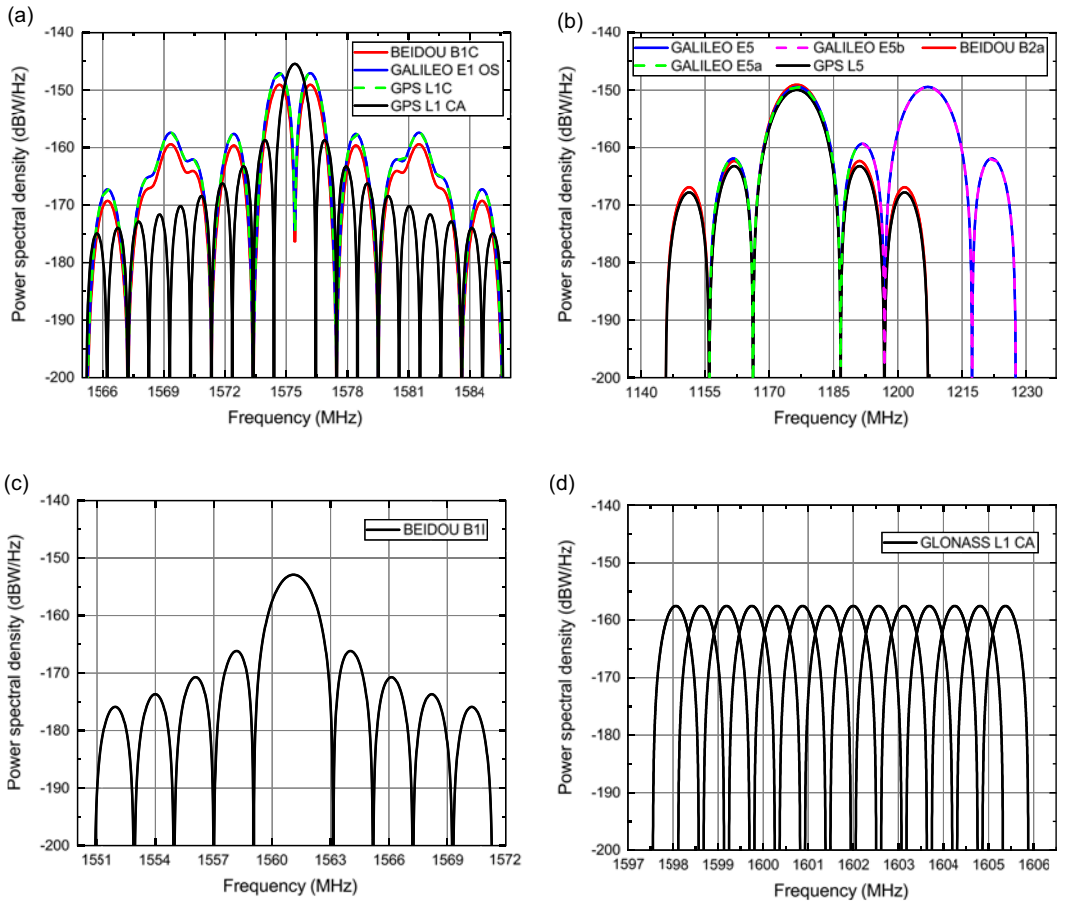


Figure 1. *GNSS signal spectra: (a) L1; (b) E5/L5; (c) B1I and (d) GLONASS L1.*

The remaining GNSS signals do not have any special characteristics that need to be known in advance before recording GNSS signals. It is enough to know the centre frequency and signal bandwidth to successfully record these signals. Note that GNSS signals are relatively weak and are below the noise floor (Borre et al., 2007). This means that looking at these signals with a spectrum analyser would show nothing at the GNSS centre frequencies. Therefore, it is important to use appropriate gain parameters in the SDR for recording and replaying GNSS signals.

2.2. Software-defined radio and synchronisation

Software-defined radios represent systems in which all signal processing is performed by the software. They are composed of analogue front-end, which is a configurable analogue transceiver, and an analogue-to-digital/digital-to-analogue converter (Krueckemeier et al., 2019). The front-end converts a specific part of the spectrum to a lower frequency band, where it can be converted to the digital domain. The digital receiver then performs all the necessary digital signal processing. Therefore, SDR systems provide a great degree of flexibility.

An SDR system can record any part of spectrum, which is within its operational limits and GNSS signals are no exception. However, to successfully record these signals, more than one SDR is needed, because there are four centre frequencies around which L1 and L5 signals are located. This means that four separate SDR devices must work as a phase-coherent transceiver, which simultaneously and

https://doi.org/10.1017/S0373463325101343 Published online by Cambridge University Press

synchronously receives or transmits signals at the aforementioned four centre frequencies. The need for such an operation arises from the fact that L1 and L5 signals coming from the same satellite are synchronised, their code delay is approximately the same since both signal travel the same path, the relative speed is the same and Doppler shifts are proportional with a known factor (Leclère et al., 2018). Additionally, GNSS receiver manufacturers can use acquisition information gathered by acquiring the L1 signal for L5 acquisition as an optimisation and cost-cutting measure, which leads to operational mode when, without L1 signals and their synchronisation to L5, L5 signals cannot be detected.

To realise a phase-coherent transceiver from separate SDRs, the time, frequency and phase synchronisation in hardware and software must be achieved. Usually, SDR systems have 10 MHz frequency reference signal input and output, as well as 1 Pulse Per Second (1 PPS) signal input for synchronisation; however, synchronisation using these inputs and outputs without additional efforts is not sufficient for application, which requires channel coherence (Krueckemeier et al., 2019).

There are three possible ways to distribute the 10 MHz reference signal in the whole system. In the reference clock sharing topology, a common reference signal is distributed to all SDRs and every SDR generates its own Local Oscillator (LO) signal using Phase Lock Loop (PLL) (Tröster-Schmid and Bednorz, 2016). In practice, this approach produces tens of degrees of phase drift due to reference signal drift and several degrees of phase drift due to noise caused by PLL (Baker and Avenell, 2019).

Another possible approach is the daisy chain topology, when the reference signal is used only for the first SDR in the chain, and after PLL generates the LO signal of that SDR, the LO signal is used internally and also exported to the next SDR in the chain, which in turn exports this signal to the subsequent SDR (Tröster-Schmid and Bednorz, 2016). This is a simpler and commonly used approach, allowing several degrees of phase drift per daisy chain stage and several decimal parts of degree phase drift due to LO output and input circuits (Baker and Avenell, 2019).

The last possible topology is the star distribution, in which case, the LO signal of the first SDR is exported to all remaining SDRs via a splitter. This topology is superior to the previous two, because it provides a stable phase relationship between all devices in the system, since phase noise in all channels becomes correlated in time (Tröster-Schmid and Bednorz, 2016). Such a configuration is used in large or phase sensitive applications (Baker and Avenell, 2019).

After reference signal distribution is done, time synchronisation must be addressed. Without it, all previous efforts do not make much difference, because recorded basebands are misaligned in time. Time synchronisation can be achieved by using 1 PPS input if the SDR has it. Using this signal, all SDRs in the system can have a synchronous start and stop, and also the internal components of each SDR can be triggered synchronously system-wide. Synchronous start and stop is sufficient to solve time misalignment (Jepson, 2019; Tröster-Schmid and Bednorz, 2016).

However, not all SDRs have 1 PPS input. In such a case, time alignment can be done in the software. A noise source has to be connected to radio frequency inputs of each SDR and by estimating cross-correlation between signal streams, the time and phase alignment can be achieved (Laakso et al., 2021). Alignment is done by shifting maxima of cross-correlation functions to the same time moment. The same time shifts can be applied to recorded baseband signals.

Finally, after reference signal distribution and time alignment are completed, phase alignment must be performed. Even if phase drift is minimised and a stable phase relation between SDRs is established, phase differences between SDRs at the beginning are unknown and random due to PLL behaviour and distribution equipment (Tröster-Schmid and Bednorz, 2016; Laakso et al., 2021). Phase alignment can be accomplished in software and must be done every time the SDRs are started. For phase alignment, the noise source is used as well. Phase correction coefficient α_n is calculated for all SDRs $n = 1, \ldots, N$ using

$$\alpha_n = \frac{\langle x_n{}^*, r\rangle}{|\langle x_n{}^*, r\rangle|} \tag{2}$$

where x_n is a complex baseband signal of the nth SDR, r is the baseband values of the reference SDR, a star symbol denotes complex conjugate, $\langle \cdot, \cdot \rangle$ is a dot product and $|\cdot|$ is a modulus operation. Coefficient α_n

https://doi.org/10.1017/S0373463325101343 Published online by Cambridge University Press

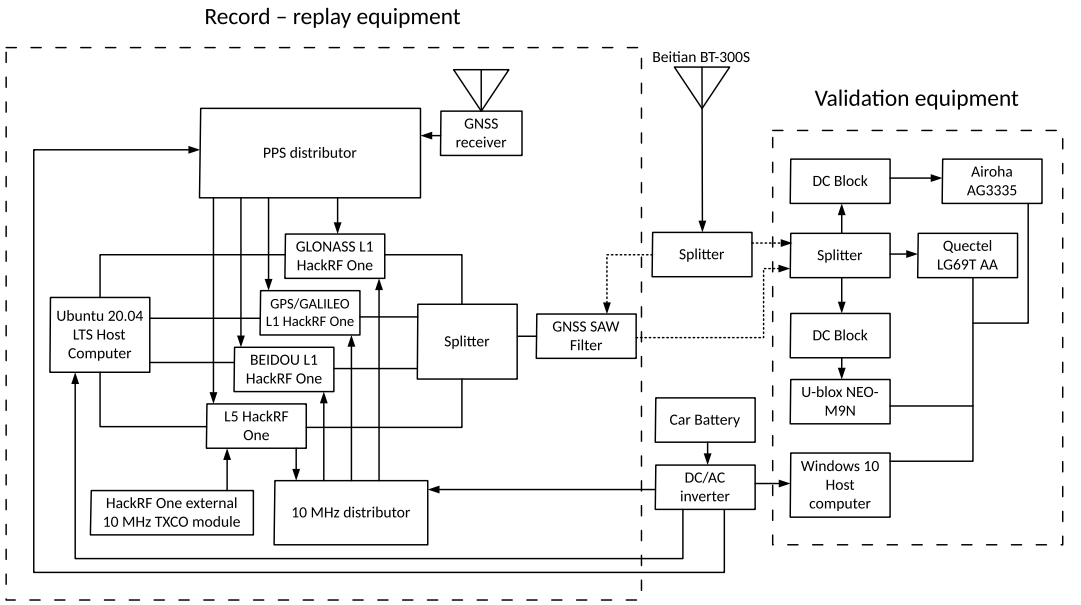


Figure 2. *Block diagram of GNSS record–replay simulator and validation equipment.*

should be calculated over a few frames to reduce the noise (Laakso et al., 2021). After correction coefficients are applied, it is assumed that the SDRs are coherent until the next restart. Note that the noise source should not be connected after alignment procedures are completed, because it will significantly reduce the signal-to-noise ratio (Laakso et al., 2021).

3. Experimental setup

All necessary equipment for GNSS L1+L5 recording and replaying, as well as for validation of records with necessary connections, are shown as a block diagram in Figure 2. This diagram constitutes the GNSS L1+L5 record–replay simulator and can be split into two parts along the main GNSS L1+L5 antenna Beitian BT-300S. All equipment to the left of this antenna is necessary for successful record–replay operation, while everything on the right side is for validation. Physical record–replay equipment is shown in Figure 3 and are discussed in the following subsections.

It was observed that the temperature of the GNSS simulator must be stable and constant during record and playback procedures. Otherwise, it will be impossible to replay records even after a few hours due to ambient temperature fluctuations. To solve this issue, all internal components are placed into a thermal insulated box with a heating wire mounted on the walls, as can be seen in Figure 3b. There is also an air circulation fan (marked 8 in Figure 3b), which forces air to move diagonally towards the SDR rack in a closed box.

To maintain the temperature in this setup, first, the temperature inside the box is raised above the ambient temperature to the point at which there is a natural tendency for the temperature to drop if the heating wire is turned off and SDRs do not transmit or receive signals. At this temperature, when inside of the box heats up due to tasks being performed, all the heat is dissipated via holes in the cover of the box. If more heat is dissipated than SDRs can provide and the temperature drops below the preset operating temperature, the heating wire turns on to provide additional heat. To achieve temperature stabilisation, the whole system must be in such a state that heat added to the system by SDRs and other equipment is equal to the heat lost by the system.

Validation of GNSS records is performed using Airoha AG3335, Quectel LG69T AA and u-blox NEO-M9N GNSS receivers. The signal from the antenna or from SDRs is delivered by a three-way

https://doi.org/10.1017/S0373463325101343 Published online by Cambridge University Press

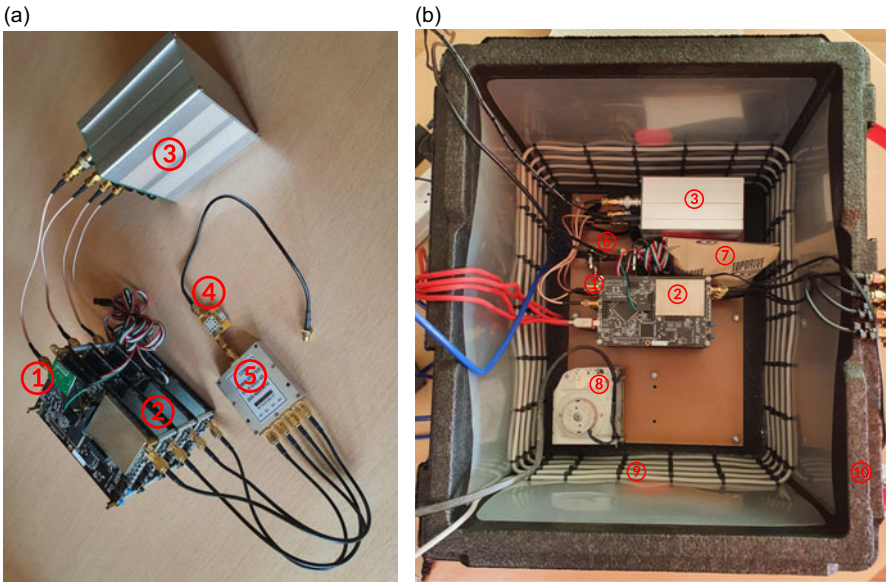


Figure 3. *Components of GNSS record–replay simulator (a) outside and (b) inside of thermal insulated box: 1 – external 10 MHz oscillator module; 2 – rack of HackRF One SDRs; 3 – 10 MHz distributor; 4 – Surface Acoustic Wave (SAW) GNSS band filter; 5 – four-way splitter; 6 – 1 PPS distributor; 7 – dehumidifier; 8 – air circulation fan; 9 – heating wire and 10 – thermal insulated box.*

splitter. It is necessary to use a DC block for two of the three receivers, because these receivers have DC voltage for active antennae. The third receiver is used as a power source for the main antenna. All GNSS receivers are controlled via a Microsoft Windows host computer, since the receiver software only works on this operating system.

All equipment is powered by a separate car battery (not the one needed for the car to run) and a DC/AC inverter. This is necessary to prolong operational time beyond what laptop batteries can provide to power PPS and 10 MHz distributors and, most importantly, for the SDR host computer to work without power limitations in performance mode.

3.1. HackRF One software-defined radios

At the very centre of developed GNSS L1+L5 record–replay simulator are software-defined radios. To record all GNSS L1 and L5 signals, four HackRF One SDRs were used. HackRF One was chosen because it can work in a frequency range from 1 to 6 GHz, has a bandwidth of 20 MHz, can both transmit and receive radio signals, has many power gain control options, has hardware support for 10 MHz frequency synchronisation and 1 PPS time synchronisation, has 8 bit resolution, and is also relatively cheap (Ossmann, 2022). Note that 8 bit resolution is an advantage because larger sample resolution can cause instability issues and recorded files will be excessively large requiring massive storage. Actually, in commercial applications like LabSat 3 Wideband, no more than 3 bit resolution is used (Racelogic, 2022), while many standard receivers support only 2 bits, and in some cases, only 1 bit is enough (Hegarty, 2011). The rack of four HackRF One SDRs used in the simulator is shown in Figure 3a. An input GNSS SAW filter is necessary for recording and replaying GNSS signals. It also acts as a DC block and is connected to a four-way splitter as shown in Figure 3a.

An alternative SDR could be USRP B210, which has all of the HackRF One features, but is more expensive and has 12 bit resolution. An attempt was made to record and replay GNSS signals using USRP B210, but when recording two channels simultaneously at different centre frequencies, USRP SDR causes

https://doi.org/10.1017/S0373463325101343 Published online by Cambridge University Press

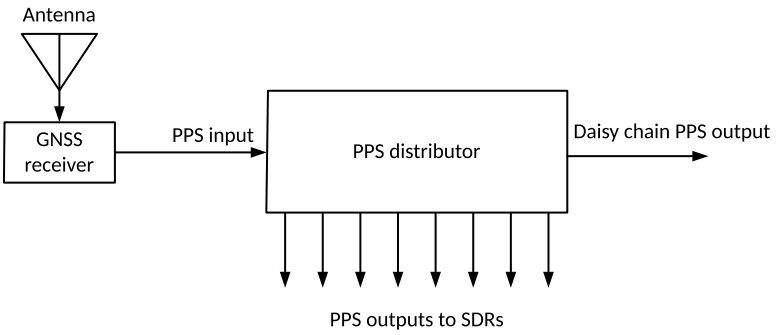


Figure 4. *Block diagram of PPS distributor.*

a linear time-dependent phase difference between the basebands. It was not completely possible to remove this phase artefact, which destroys phase synchronisation between L1 and L5 signals.

3.2. SDR host computer

The SDR host computer is no less important than the SDRs themselves. In this work, the Asus ROG Strix SCAR II GL504GM with Intel Core i7-8750H processor, 1 TB Kingston A2000 NVME SSD disk, 32 GB DDR4 2666 CL19 RAM and Ubuntu 20.04 LTS operating system was used. It is important that the host computer would have enough USB ports for each SDR, because every SDR must be connected directly to the host computer without any hubs to avoid limiting of the bandwidth. The Linux operating system is preferred, because it does not load the computer significantly, supports all the necessary software and allows forcing the computer to work in performance mode simply via a terminal. Note that the performance mode is absolutely necessary, because SDRs load the USB controller and CPU, and if the CPU is not in performance mode, after some time during a sustained load, there will be drops in performance, which could cause overflows or underflows affecting L1 and L5 synchronisation.

3.3. PPS distributor for time synchronisation

To record and replay GNSS signals, SDRs must be synchronised in time. According to Bartolucci et al. (2016), a HackRF One time synchronisation error of less than one sampling period can be achieved. HackRF One can be synchronised by using an external 1 PPS signal or by using one of the SDRs as a trigger source.

In practice, it was observed that using one of the SDRs as a source is not reliable and using the external 1 PPS signal produced by a standard GNSS receiver is better. However, to use an external signal safely and reliably, a PSS signal distributor is necessary. Following Kutkov (2021), the PPS distributor was designed and built for the GNSS L1+L5 record–replay simulator. A block diagram of the developed distributor is shown in Figure 4. This device works by using a GNSS receiver or any other external 1 PPS source, then this signal is buffered so as not to overload the source. The buffered signal is then distributed to three other buffers: one for daisy chain output, another for LED indication and the third for eight parallel outputs connected to the SDRs. This PPS distributor supports both TTL and CMOS voltage levels (depending on jumper configuration) and can be powered via a micro-USB port. Note that the hardware time synchronisation feature is only available in firmware release 2021.03.1 or newer of the HackRF One SDR.

3.4. Common oscillator distribution scheme for frequency synchronisation

To achieve frequency synchronisation, which in turn has an effect on phase synchronisation, the star topology is used, as shown in Figure 5. First, an external 10 MHz oscillator module is used to improve

https://doi.org/10.1017/S0373463325101343 Published online by Cambridge University Press

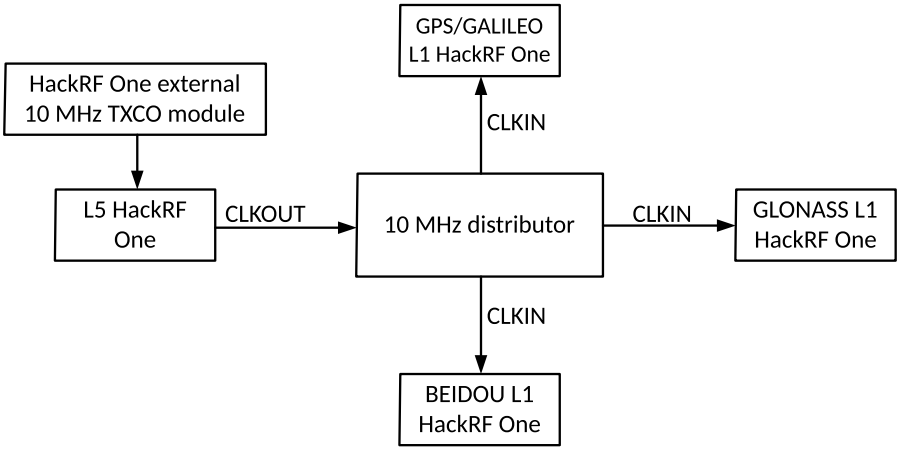


Figure 5. *Block diagram of common oscillator distribution.*

the frequency stability of HackRF One which records and replays L5 signals. Then, the reference signal of L5 HackRF One, generated by an on-board Si5351C clock generator, is exported via a CLKOUT output to a 10 MHz amplifier–distributor box. From the distributor box, local oscillator signals are delivered to the three remaining SDRs.

Since the 10 MHz distributor has a built-in OCXO, it was attempted to realise the reference clock sharing topology, but the achieved synchronisation was worse and had a significant effect on GNSS L1 and L5 signals, because, when replaying the record, L5 signals would sometimes randomly disappear after a few minutes into playback. Such behaviour was not observed using the star topology described above.

3.5. Software phase correction for phase synchronisation

While using HackRF One, the only possible way to achieve phase synchronisation is via software. The software is implemented in Python and it works by reading a part of the GNSS record and calculating the necessary phase corrections to eliminate the phase difference between signals. When reading signals, the first 5 s are skipped, because HackRF PLL stabilises only after approximately 5 s from the time when the SDR has started. After skipping the initial interval, only 30 s are read. This limitation is caused by random access memory and, as a result, the minimum necessary amount of RAM for this software to work is 32 GB.

After records are loaded as complex samples into memory, necessary phase corrections are calculated in two ways: (i) by calculating phase difference using one second worth of samples for each second in 30 s and averaging 30 calculations, and (ii) by calculating phase difference using all samples in 30 s. The final results are compared by the user and should not be different by more than 0.01 degree. All of this is necessary to confirm that recorded signals fit the initial assumptions.

There are two initial assumptions. The first assumption is that the recorded signals are comparable to the output of noise generator, because GNSS signals are below the noise floor and no other signals are supposed to be in L1 and L5 bands. This assumption is necessary, because a noise source is needed for phase synchronisation (Laakso et al., 2021), and if the assumption is not violated, there is no need for a special phase synchronisation procedure like in KerberosSDR (KrakenRF Inc, 2022). The second assumption is that phase correction is a single complex number that can be applied to the whole record. If this assumption is invalid, the final results produced by two different ways of phase correction calculations will differ by more than 0.01 degree. These assumptions can be violated by choosing very large values for gain parameters of the HackRF One SDR. The correct gain values should be determined by trial and error.

https://doi.org/10.1017/S0373463325101343 Published online by Cambridge University Press

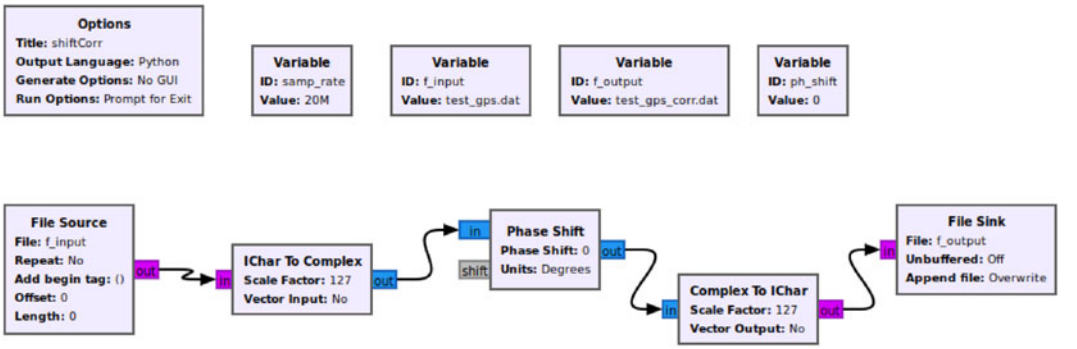


Figure 6. *Functional blocks in GNU Radio environment for applying phase correction.*

Furthermore, in written software, GNSS L5 recording is used as a reference, and phase correction is calculated in such a way that phase difference between the GNSS L5 record and any other record would be zero degrees.

Since GNSS records can be rather long, the calculated phase corrections are applied using GNU Radio software as shown in Figure 6. GNU Radio generates the constructed flow diagram as a Python script, which can be used inside other external Python scripts (GNU Radio Website, 2022). By doing this, the main script calculates corrections and then starts the GNU Radio script for each record to apply calculated corrections.

3.6. Synchronisation and sampling rate

GNSS L1 and L5 signals are transmitted on different centre frequencies using different modulations and different bandwidths. Therefore, in theory, different GNSS signals could be recorded using different sampling rates. This would be beneficial to the whole system, because multiple SDRs could be connected to the same USB port via a hub, less storage would be used by records and overall load on the host computer would be reduced.

However, despite extensive efforts, L1 and L5 signals were not successfully recorded and replayed in a multi-sampling rate system. None of the L1+L5 capable receivers used in experiments were able to detect both L1 and L5 signals. However, this does not mean that no signals can be recorded using different sampling rates for different centre frequencies. If the goal is to record only L1 signals, there are no issues in using different sampling rates. All receivers were able to detect L1 signals transmitted on all centre frequencies. Problems would begin only when an attempt to record multiple bands is made.

The most likely explanation for such a behaviour is that when recording GNSS signals using different sampling rates, synchronisation between signals is destroyed. This is not an issue for L1, because receivers do not use acquisition results from GPS L1 signals to acquire, for example, GALILEO L1 signals. No synchronisation between GPS and GALILEO could even be expected, because these signals are transmitted from different satellites.

Unfortunately, the situation for L1 and L5 bands is different, because these signals are transmitted by the same satellites; therefore, these signals are expected to be synchronised and receivers use acquisition results from L1 signals to acquire L5 signals (Leclère et al., 2018).

The fact that GNSS receivers heavily rely on L1 signal for L5 reception is clearly seen in the subsequent results, which are discussed below. Note that commercially available solutions do not use different sampling rates for multiple bands as well. For example, LabSat 3 Wideband can record three different bands, but all of them are recorded using the same bandwidth and, therefore, the same sampling rate (Racelogic, 2022). However, this creates situations where more bandwidth is recorded than needed and the system is stressed more than necessary. In the case of LabSat 3 Wideband, this problem is solved by reducing the resolution from 3 bits to 1 bit.

https://doi.org/10.1017/S0373463325101343 Published online by Cambridge University Press

To record multiple GNSS signals in the same band, different sampling rates for different centre frequencies can be used, because the loss of synchronisation is not important. However, to record multiple GNSS bands, the same sampling rate must be used for all centre frequencies to maintain synchronisation.

Since the HackRF One SDR does not have a possibility to adjust the resolution, the only possible optimisation for the system is to record GNSS signals with reduced bandwidth, which is achieved by reducing the sampling rate to the same value as the desired bandwidth. This was investigated and results are discussed in the following section.

4. Results and discussion

While investigating the quality of GNSS recordings and the possibilities of stability improvement for the proposed GNSS L1+L5 record–replay simulator, the dependencies of average carrier-to-noise ratio C/N_0 and the number of visible satellites on GNSS record bandwidth were measured. The reason for choosing these two particular parameters is that they directly reflect the quality of GNSS signals and they are mutually complementary, because it was observed during experimentation that large values of C/N_0 can be measured when the number of visible satellites is too small for positioning and, vice versa, large number of visible satellites are possible when C/N_0 is too small for reception. The bandwidth is an important factor, since it directly affects the reception quality, as insufficient bandwidth may cause data loss, but smaller bandwidth means lower sampling rate and smaller load on host computer resulting in better stability of the recording system.

In the following subsections, measurement results are analysed for the all-system GNSS case over the whole L1 and L5 bands, and also for each main GNSS system separately.

4.1. All-system GNSS L1+L5 band measurements

For the all-system GNSS L1 band, the dependency of C/N_0 on GNSS L1 recording bandwidth is shown in Figure 7a and the number of visible satellites in Figure 7b. As can be seen from these figures, dependencies vary significantly when comparing receiver to receiver. However, all curves show similar behaviour after crossing below 4 MHz since at smaller bandwidths, a sharp drop in both average carrier-to-noise ratio and the number of visible satellites is observed.

Regardless of the sharp decline in measured values, all receivers are able to determine the position even at 1 MHz record bandwidth, because C/N_0 and the number of satellites are sufficient. The u-blox NEO-M9N receiver is able to determine the position even at 0.5 MHz bandwidth. Although the absolute values are different comparing receiver to receiver, the general behaviour of the curves is very similar. Therefore, it is likely that other receivers will show the same behaviour.

For the all-system GNSS L5 case, the dependency of C/N_0 on GNSS L5 recording bandwidth is shown in Figure 7c and the dependency of the number of visible satellites on bandwidth is shown in Figure 7d. For L5 measurements, only the Airoha AG3335 and Quectel LG69T AA GNSS receivers were used, because u-blox NEO-M9N is L1 only. From these results one can see that while the number of visible satellites dependencies show similar behaviour, the C/N_0 curves are very different. These differences are the result of implementation differences between receivers, which are not disclosed in the documentation. Overall, any GNSS L5 signal can be recorded using as little as 6 MHz of bandwidth, because only after crossing below this limit, a sharp decline in measured values begins.

4.2. GPS L1+L5 band measurements

In the case of GPS L1 (Figure 8a and b), the situation is very different compared with GNSS L1. There is almost no dependency on the recording bandwidth for the number of visible satellites and only some variation for C/N_0. The drop in values occurs only after crossing below the 4 MHz bandwidth.

https://doi.org/10.1017/S0373463325101343 Published online by Cambridge University Press

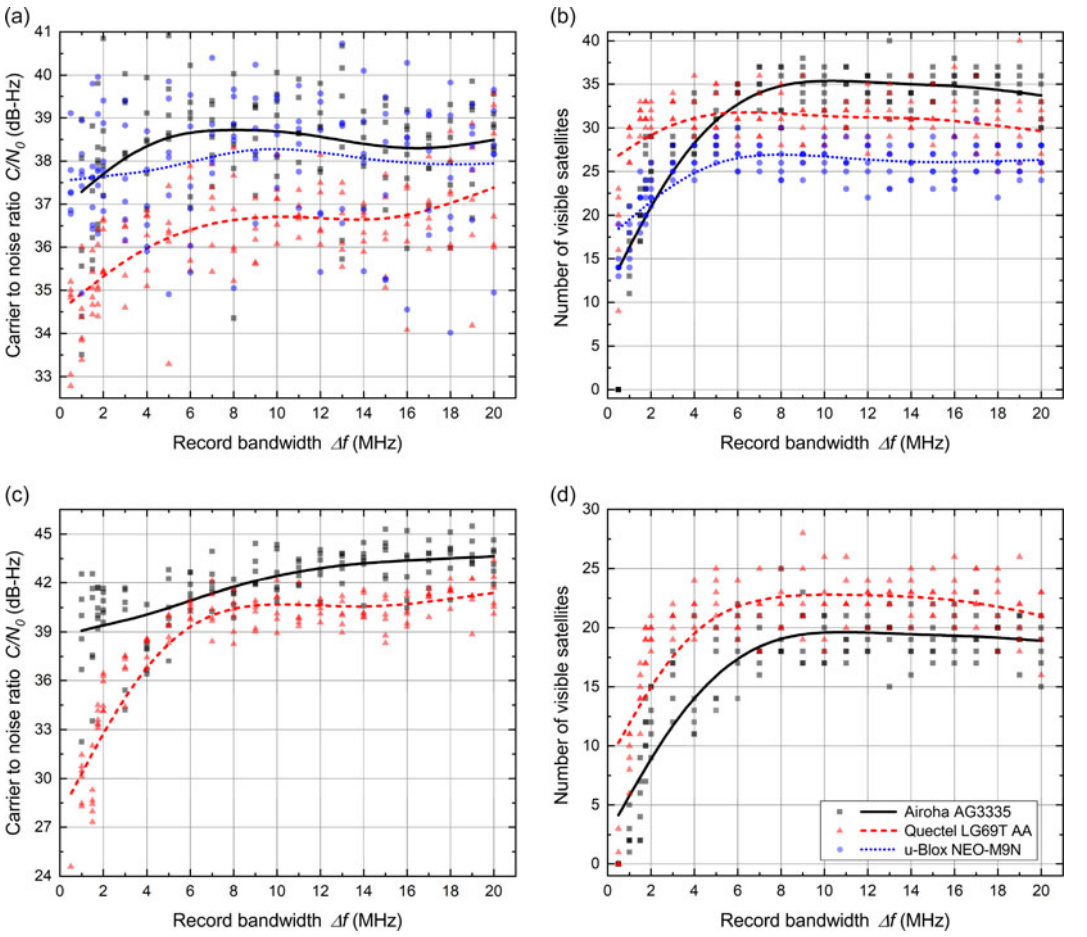


Figure 7. *Dependency of carrier-to-noise ratio (left column) and the number of visible satellites (right column) on the GNSS record bandwidth over L1 (top row) and L5 (bottom row) bands for three GNSS receivers shown in the common legend. Points are measured values and lines correspond to statistically averaged results.*

This result is not very surprising, because even if one needs approximately 15 MHz bandwidth to fully record GPS TMBOC(6,1,1/11) signal, only pilot signals are located between 4 and 15 MHz. These pilot signals use BOC(6,1) modulation and they do not carry any information, and are mostly used for channel state estimation. After crossing below the 4 MHz limit, data loss occurs and GPS L1C data signals, which use BOC(1,1) modulation, no longer can be fully recorded; however, GPS L1 C/A signals need only 2 MHz due to BPSK(1) modulation, therefore, even at 1 MHz bandwidth, GPS satellites are still visible by all receivers with sufficient signal quality for navigation.

Considering the GPS L5 case (Figure 8c and d), the curve behaviour is similar to the L5 all-system GNSS case, except for the fact that according to the dependency of the number of visible satellites, only 4 MHz of bandwidth is needed before a sharp drop in values occurs and, according to the C/N_0 dependency, 6 MHz of bandwidth is needed. Unfortunately, such behaviour cannot be explained by signal structures and modulations, because GPS uses BPSK(10). This means that to record this signal without data loss, one needs 20.46 MHz of bandwidth and after crossing 20 MHz, the situation should be similar to what was observed in GPS L1 after crossing 4 MHz.

The most likely explanation is that, as observed with BPSK(1) and 1 MHz of bandwidth, similar behaviour should be possible in the case of BPSK(10) and 10 MHz of bandwidth. Further reduction of

https://doi.org/10.1017/S0373463325101343 Published online by Cambridge University Press

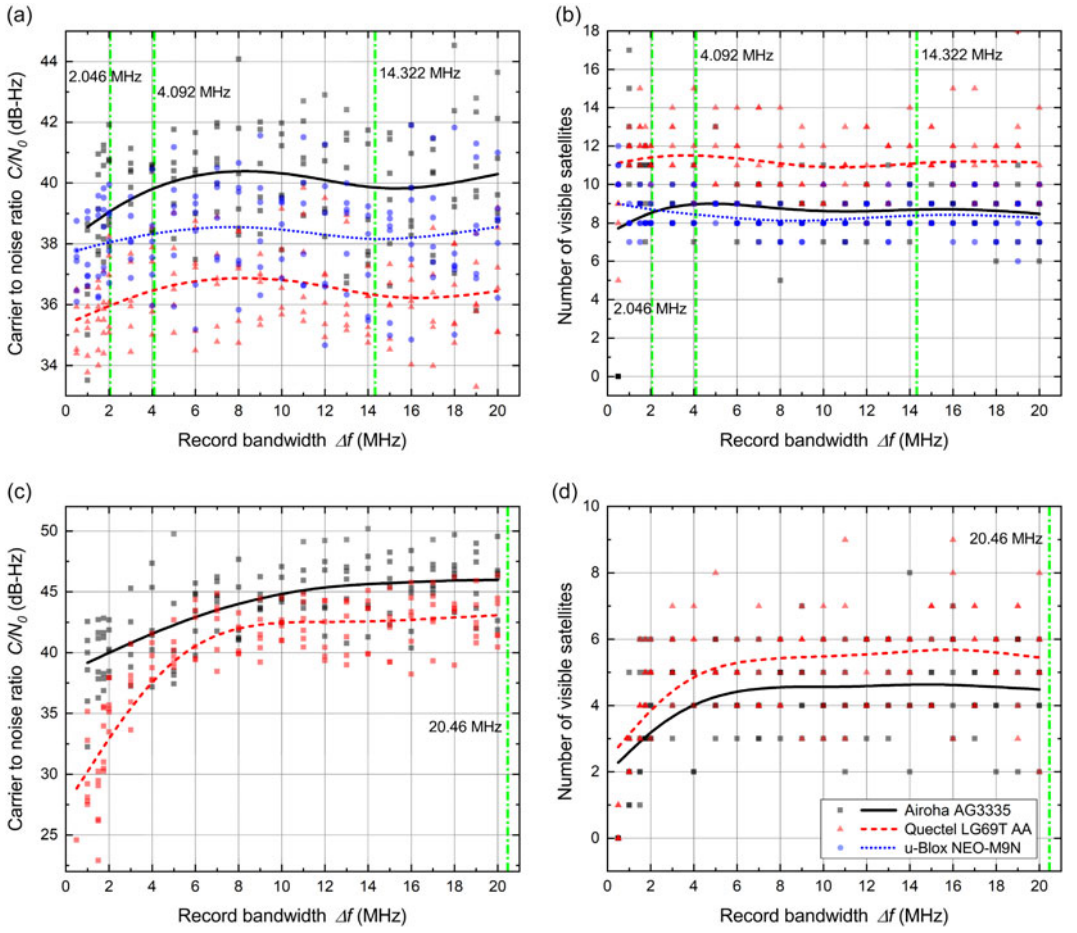


Figure 8. *Dependency of carrier-to-noise ratio (left column) and the number of visible satellites (right column) on the GPS record's bandwidth over L1 (top row) and L5 (bottom row) bands for three GNSS receivers shown in the common legend. Points are measured values and lines correspond to statistically averaged results. Vertical green lines in this and the following figures indicate typical bandwidths of L1 and L5 signal modulations.*

bandwidth is possible due to utilisation of L1 acquisition results in L5 acquisition. This cannot be confirmed due to the scarcity of documentation from the manufacturers.

4.3. GALILEO L1+L5 band measurements

The situation regarding GALILEO L1 (Figure 9a and b) is very similar to the GPS case, because GALILEO E1 signals use CBOC(6,1,1/11), which is similar to TMBOC(6,1,1/11); however, data are carried by both BOC(1,1) and BOC(6,1). Despite this, there is almost no change in the C/N_0 dependency and even an improvement with shrinking bandwidth in the number of satellites dependency is observed in the region from 4 to 15 MHz. Most likely, this behaviour is observed due to the fact that the majority of signal power is allocated to BOC(1,1) (European Union, 2021). Also, as with the GPS case, one can observe a decline of values after the bandwidth becomes smaller than 4 MHz, and the decline is sharper than in the GPS case, because GALILEO does not have BPSK(1) signals.

https://doi.org/10.1017/S0373463325101343 Published online by Cambridge University Press

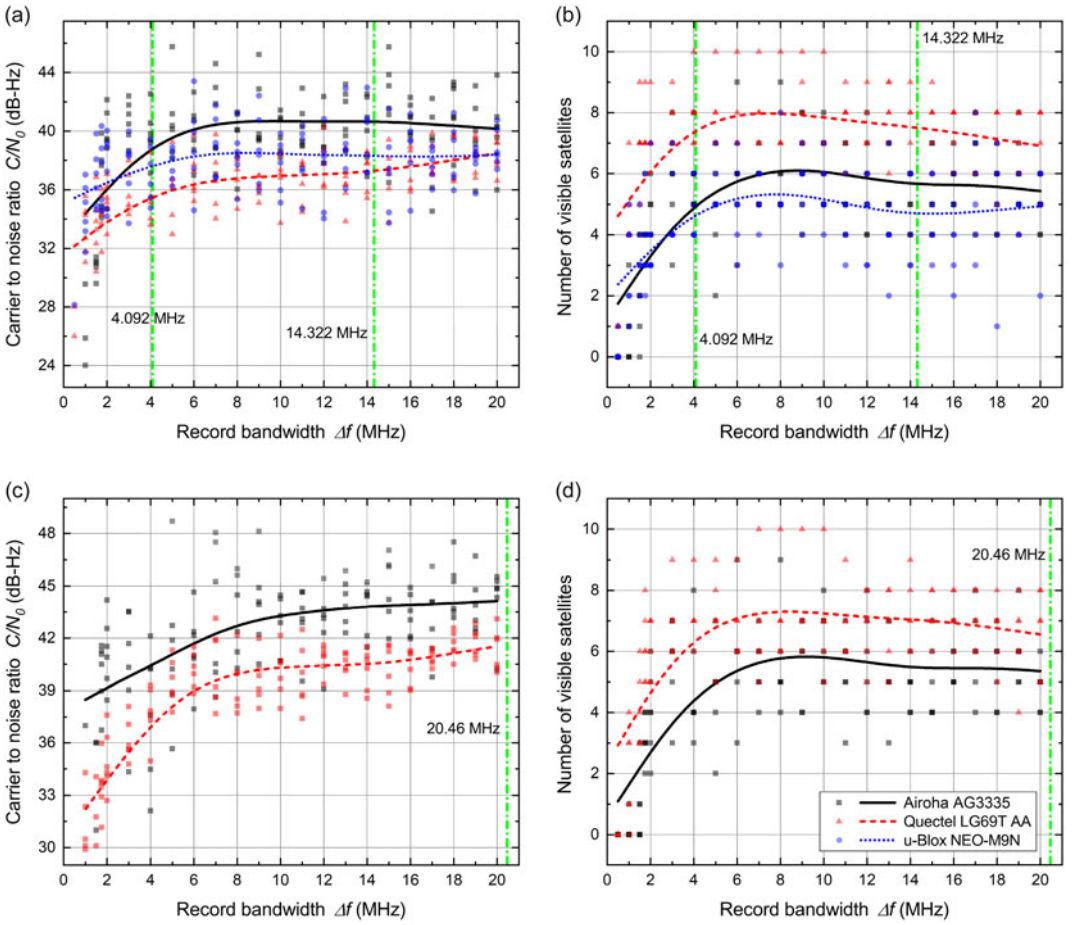


Figure 9. *Dependency of carrier-to-noise ratio (left column) and the number of visible satellites (right column) on the GALILEO record's bandwidth over L1 (top row) and L5 (bottom row) bands for three GNSS receivers shown in the common legend. Points are measured values and lines correspond to statistically averaged results.*

GALILEO L5 (Figure 9c and d) dependencies are similar to the all-system GNSS case. A sharp drop in values starts at 6 MHz that is less than 30% of the necessary bandwidth to demodulate GALILEO E5a signal. However, since its main lobe can be compared with and demodulated as BPSK(10) (European Union, 2021), the measured curves follow similar behaviour to those observed in the GPS case.

4.4. BEIDOU L1+L5 band measurements

The L1 band curves of the BEIDOU system (Figure 10a and b) show dependency on both the bandwidth and receiver type. For Quectel LG69T AA and u-Blox NEO-M9N receivers, the observed curve behaviour is similar to the GPS case. This is because BEIDOU B1C uses QMBOC(6,1,4/33), which is similar to TMBOC(6,1,1/11), and also BOC(6,1) is used only for pilot signals. In addition to that, BEIDOU transmits a B1I signal, which uses BPSK(2) modulation. What is interesting in this case, is that, just as BOC(1,1), BPSK(2) needs 4.092 MHz of bandwidth, but unlike BOC(1,1) and much more like BPSK(1), the drop of C/N_0 values starts only when the record bandwidth is reduced below 4 MHz, but it is significantly less sharp than in the GALILEO case. It is likely that BPSK(2) has a similar effect on this dependency as BPSK(1) in the GPS case.

https://doi.org/10.1017/S0373463325101343 Published online by Cambridge University Press

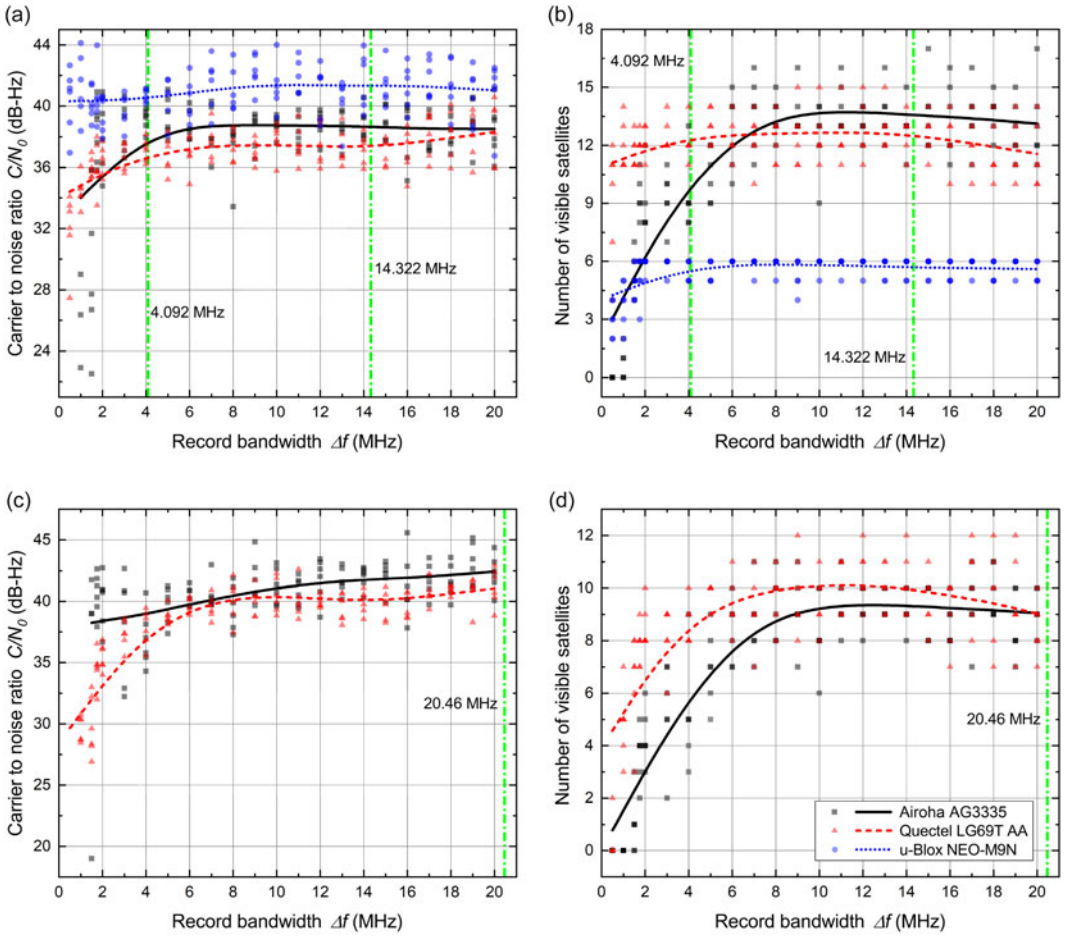


Figure 10. *Dependency of carrier-to-noise ratio (left column) and the number of visible satellites (right column) on the BEIDOU record's bandwidth over L1 (top row) and L5 (bottom row) bands for three GNSS receivers shown in the common legend. Points are measured values and lines correspond to statistically averaged results.*

However, the Airoha AG3335 receiver shows a very different behaviour. It can be observed from Figure 10b that a significant drop in the number of satellites begins after crossing below 6 MHz, which is similar to what is observed in the L5 cases. However, even if the bandwidth is limited to 4 MHz, the receiver is still able to see approximately nine satellites, which is sufficient for navigation. Therefore, bandwidth can be reduced to as little as 4 MHz, which agrees with other receiver results.

The BEIDOU L5 band behaviour (Figure 10c and d) is similar to the GPS and GALILEO systems. A sharp decline in measured characteristics is observed after crossing below 6 MHz, because, as the GPS, the BEIDOU B2a signal uses BPSK(10) modulation and, as noted before, receivers use information acquired via L1 for L5 signal processing.

Overall, it could be noted that the number of visible satellites is a superior parameter, because it is less affected by GNSS receiver differences and reports similar dependencies across all GNSS systems. However, this parameter can lead one to believe that Quectel LG69T AA is a superior receiver since it can detect more GNSS satellites at all tested bandwidths for almost each GNSS system. Such an assumption could not be true, because it was observed that without L1, Quectel LG69T AA cannot detect a single L5 satellite and L1 has to be present all the time, while Airoha AG3335 only needs L1 at

https://doi.org/10.1017/S0373463325101343 Published online by Cambridge University Press

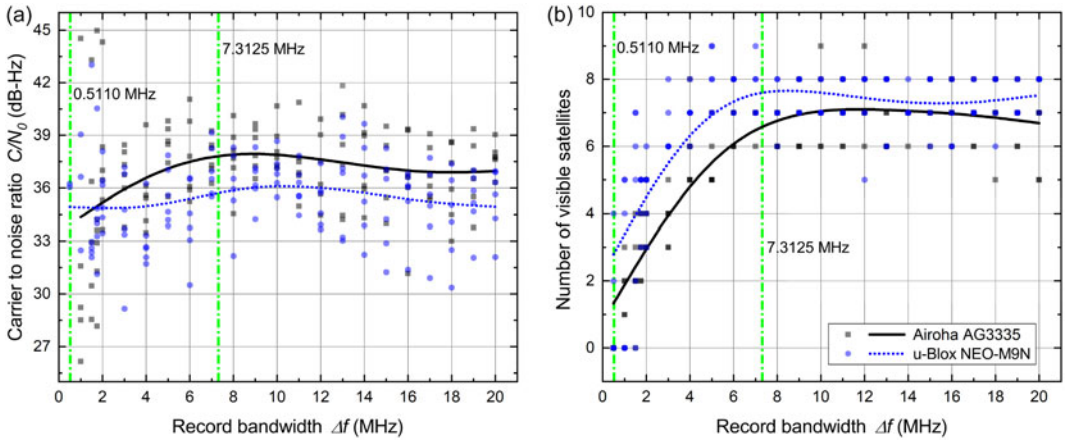


Figure 11. *Dependency of (a) carrier-to-noise ratio and (b) the number of visible satellites on the GLONASS record's bandwidth over L1 band for two GNSS receivers shown in the common legend. Points are measured values and lines correspond to statistically averaged results.*

the beginning and, after satellites are detected, L1 is no longer needed for L5 tracking and thus L5 can be used independently. However, as far as L1 is concerned, Quectel LG69T AA detects more satellites, because in our testing, it only worked with GPS, GALILEO and BEIDOU systems, but the total number of visible satellites is comparable to other receivers, as seen in Figure 7b.

4.5. GLONASS L1 band measurements

Since GLONASS uses FDMA instead of CDMA, this causes very different behaviour of the C/N_0 curves compared with the other GNSS systems, as seen in Figure 11a. There are only small variations over the whole measured bandwidth, which are likely caused by reception conditions, since there was a 4 hour difference between measurements from 2 to 20 MHz bandwidths. The explanation for non-dependent behaviour is the fact that as a FDMA system, GLONASS needs almost 8 MHz of bandwidth for its 14 channels, but each channel transmits only a BPSK(0.5) modulated signal that needs only 0.511 MHz of bandwidth.

The effects of FDMA are clearly visible in Figure 11b. There is no dependency on record bandwidth while the bandwidth stays above 8 MHz. After moving below this limit, the number of visible satellites starts to gradually decrease until only one satellite is visible at 0.5 MHz, since only one GLONASS FDMA channel can fit in 0.5 MHz. Notice that if the bandwidth is limited to 6 MHz as in the all-system GNSS case, there are still more than six available GLONASS satellites, which is sufficient for determination of the position using GLONASS signals alone.

4.6. Dynamic testing of GNSS L1+L5 record–replay simulator

After determining that the proposed GNSS L1+L5 record–replay simulator can record GNSS signals in a stationary configuration and the simulator can be optimised by reducing sampling rate without significant decrease in signal quality, dynamic testing was performed. In these tests, GNSS signals were recorded, while driving a car. All equipment was put in the trunk of the car with the antenna mounted on the rooftop. Signals were recorded by a simulator and, at the same time, logged by Airoha AG3335, Quectel LG69T AA and u-blox NEO-M9N GNSS receivers. After completing the route shown in Figure 12, GNSS records were transmitted to receivers and results were logged to files. After this, the

https://doi.org/10.1017/S0373463325101343 Published online by Cambridge University Press

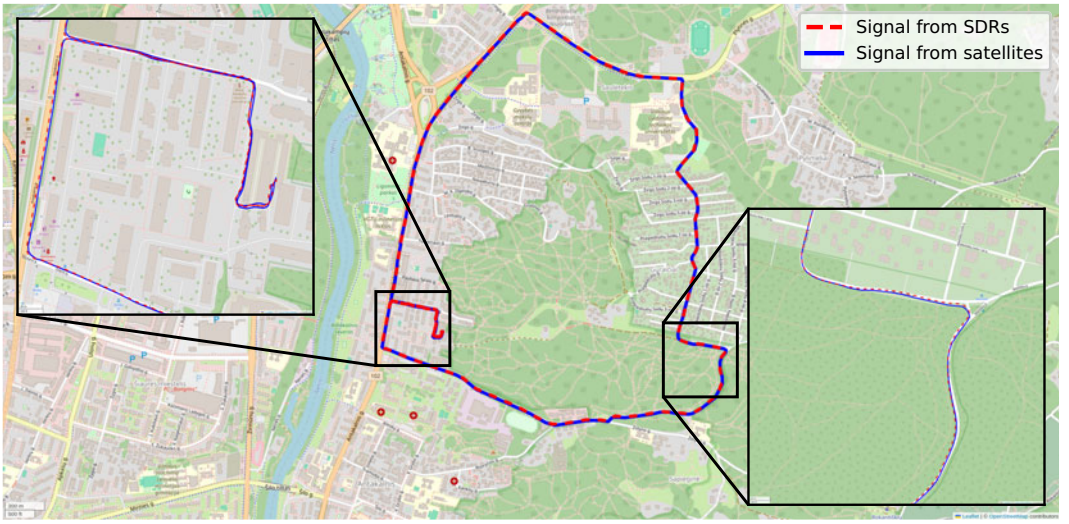


Figure 12. *Route of dynamic testing as logged by Airoha AG3335 GNSS receiver for signals obtained directly from satellite and recorded by SDRs.*

logs were compared to evaluate if the recorded signals produce the same results as the signals directly from the satellites in the dynamic configuration.

To evaluate if bandwidth reduction is a viable optimisation not only in the stationary, but also in the dynamic mode, the sampling rate for all signals was set to 10 MHz. Such a sampling rate is sufficient for L1; however, is close to the 6 MHz limit for the L5 signal. Selecting a lower sampling rate reduces the load on host computer and allows to collect more GNSS recording data.

All GNSS receivers produced similar results; therefore, only results obtained from Airoha AG3335 receiver are presented in this paper. As shown in Figure 12, the GNSS receiver produces very similar trajectory results for both the direct satellite signal and that recorded using SDRs. The differences occur only at small radius corners as shown in the zoomed-in portions of the map, but these differences are the result of nearby buildings and vegetation, which block a clear line of sight between satellites and antenna or introduce reflections, therefore degrading record quality.

Both L1 and L5 signals were successfully recorded and detected by the GNSS receiver when replaying them. This is clearly evident in C/N_0 and the number of visible satellites dependencies over time (Figure 13a and b). There are only small differences related to signal origin: in the case of direct satellite reception, C/N_0 dependencies report higher values by less than 1 dB in the L1 case and by less than 2 dB in the L5 case compared with signals from SDRs. However, the behaviour of dependencies is the same regardless of signal origin.

Some differences can be observed in the number of visible satellites dependencies as well, SDR-based dependencies reporting smaller overall number of satellites compared with direct satellite reception in the L1 case, while a similar number is reported for L5. Also, the origin of the signals cannot be determined from the behaviour of the curves.

Since Airoha AG3335 needs the L1 signal only in the beginning, the L5-only mode was tested using this receiver together with a 10 MHz sampling rate for L5 recording. This test could not be performed with the Quectel LG69T AA receiver, because it needs L1 to be present all the time and the u-blox NEO-M9N receiver is not suitable for this test, because it only works with L1 signals. The L5-only mode test is performed by first replaying both L1 and L5 signals, and then, after the receiver has detected L5 signals, L1-replaying SDRs are reset to stop L1 playback.

From the results presented in Figure 13a and b, it is clear that even in the L5-only mode, the Airoha AG3335 GNSS receiver is able to detect a sufficient number of satellites for positioning. In this case, the

https://doi.org/10.1017/S0373463325101343 Published online by Cambridge University Press

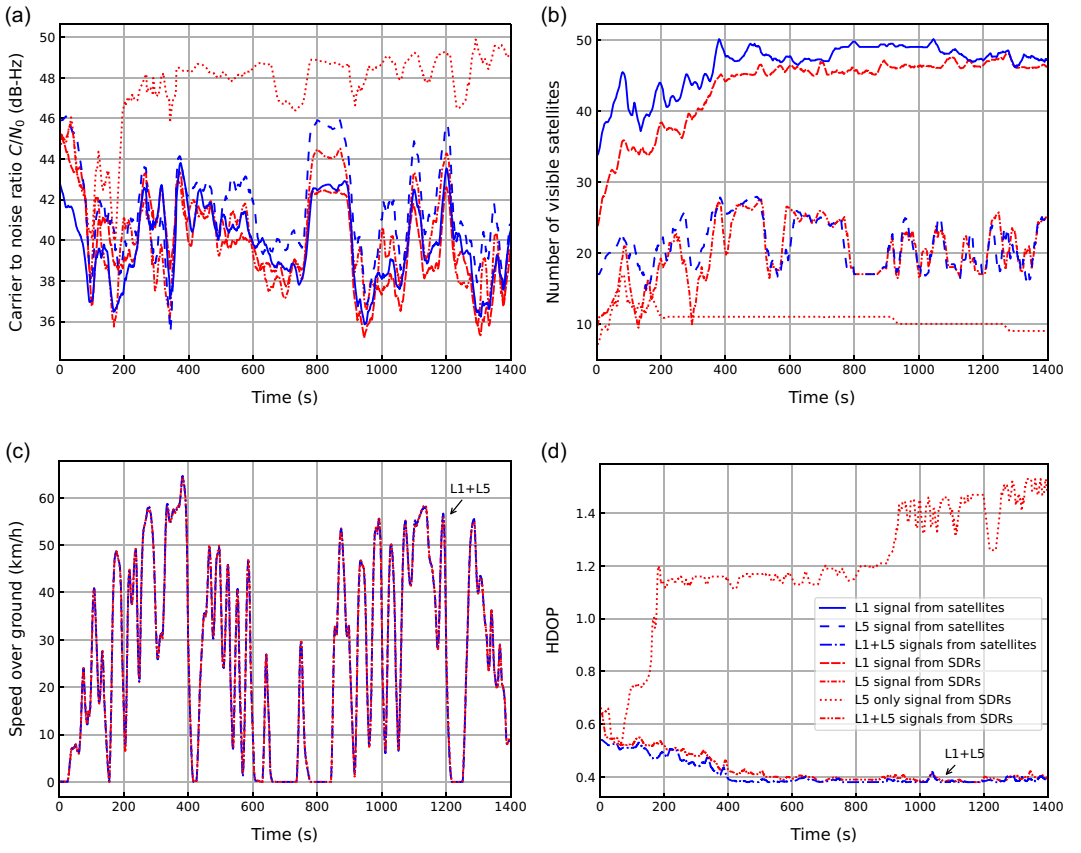


Figure 13. *Dependency over time of (a) carrier-to-noise ratio, (b) the number of visible satellites, (c) receiver speed over ground and (d) HDOP for L1, L5 and L1+L5 signals received directly from satellites and replayed by SDRs as shown in the common legend. Data logged using Airoha AG3335 GNSS receiver.*

number of visible satellites is significantly lower compared with signals directly from satellites or L5 record playback with available L1 signal, since in the L5-only mode, the receiver is unable to detect new satellites without L1, which was used for detection at the beginning of the test.

A low number of visible satellites has a significant effect on the Horizontal Dilution of Precision (HDOP) dependency on time (Figure 13d), because over time, HDOP only worsens in the L5-only case, while for direct satellite reception and L1+L5 record playback, HDOP improves with a rising number of satellites and remains below 0.6 all the time. This is not surprising, because in the L5-only mode, the number of visible satellites is close to theoretical minimum necessary for trilateration.

The speed over ground reported by the GNSS receiver is the same in all three cases of signal reception, as shown in Figure 13c. Since the L5 signal has a limited bandwidth, it was important to test if driving at higher speeds would have any kind of impact. During additional testing, GNSS signals were recorded while driving at speeds up to 130 km/h and no differences were observed in the L1+L5 record playback compared with driving at lower speeds.

Note that L5 recording used in L5-only testing was conducted using only 10 MHz bandwidth. This is more than two times less than necessary for the BPSK(10) modulated signal. Therefore, L5-only testing is very important, because it proves that the band-limited L5 record can be used in standalone mode without L1 signals. Of course, L5-only testing results are significantly worse due to the low number of

https://doi.org/10.1017/S0373463325101343 Published online by Cambridge University Press

visible satellites, because the GNSS receiver cannot detect new satellites without the presence of L1 signal.

5. Conclusions

In this work, GNSS signal characterisation and SDR synchronisation analysis allowed to determine the initial configuration of the hardware and software necessary for successful operation of an SDR-based GNSS L5+L1 record–replay simulator. Final fine-tuning was performed via trial and error due to peculiarities of the selected hardware. Since the generic SDR based simulation approach imposes a large load on the SDR host computer, potential ways to increase system stability were explored. One of the possible optimisations is recording of GNSS signals using a lower than necessary sampling rate. The results show that any GNSS L1 signal can be successfully recorded using a sampling rate as low as 6 MHz. Carrier-to-noise ratio and the number of visible satellites starts to decrease significantly only when the sampling rate becomes lower than 4 MHz. In the case of L5, any GNSS L5 signal can be recorded using a sampling rate of 6 MHz, although GPS L5 can be recorded using only 4 MHz. Regardless of the absolute lower limits of sampling rate, it is important that all recorded signals use the same sampling rate in case L1 and L5 are recorded simultaneously. If this condition is not satisfied, GNSS receivers do not recognise L5 signals, but only L1. Multiple sampling rates are only viable when signals are recorded in the same band.

Acknowledgements. This research was partially supported by Teltonika company group.

Competing interests. The authors declare none.

References

Baker, D. and Avenell, B. (2019). RF System Synchronization – LO's. https://www.gnuradio.org/grcon/grcon19/presentations/Phase_Synchronization_Techniques/Dan Accessed 14 December 2022.

Bartolucci, M., del Peral-Rosado, J. A., Estatuet-Castillo, R., Garcia-Molina, J. A., Crisci, M., and Corazza, G. E. (2016). Synchronisation of Low-Cost Open Source SDRs for Navigation Applications. 2016 8th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC), IEEE, 1–7.

Borre, K., Akos, D. M., Bertelsen, N., Rinder, P. and Jensen, S. H. (2007). *A Software-Defined GPS and Galileo Receiver: A Single-Frequency Approach*. Springer Science & Business Media.

Chen, J., Zhang, S., Wang, H. and Zhang, X. (2013). Practicing a Record-and-Replay System on USRP. Proceedings of the Second Workshop on Software Radio Implementation Forum, 61–64.

China Satellite Navigation Office (2017). BeiDou Navigation Satellite System Signal in Space Interface Control Document Open Service Signal B2a (Version 1.0).

China Satellite Navigation Office (2018). BeiDou Navigation Satellite System Signal in Space Interface Control Document Open Service Signal B1C (Version 1.0).

China Satellite Navigation Office (2019). BeiDou Navigation Satellite System Signal in Space Interface Control Document Open Service Signal B1I (Version 3.0).

Di, R., Peng, S., Taylor, S., and Morton, Y. (2012). A USRP-based GNSS and Interference Signal Generator and Playback System. Proceedings of the 2012 IEEE/ION Position, Location and Navigation Symposium, IEEE, 470–478.

Ebinuma, T. (2022). Software-Defined GPS Signal Simulator. https://github.com/osqzss/gps-sdr-sim. Accessed 14 December 2022.

European Union (2021). European GNSS (Galileo) Open Service: Signal in Space Interface Control Document. Office for Official Publications of the European Communities.

Glonass, ICD (2008). Glonass Interface Control Document. Russian Institute of Space Device Engineering.

GNU Radio Website (2022). GNU Radio. https://www.gnuradio.org/. Accessed 14 December 2022.

GPS Directorate (2021a). IS-GPS-200M, Navstar GPS Space Segment/User Segment Interfaces.

GPS Directorate (2021b). IS-GPS-750H, Navstar GPS Space Segment/User Segment L5 interfaces.

GPS Directorate (2021c). IS-GPS-800H, Navstar GPS Space Segment/User Segment L1C interfaces.

Hasan, M. (2022). State of IoT 2022: Number of Connected IoT Devices Growing 18% to 14.4 Billion Globally. https://iot-analytics.com/number-connected-iot-devices/. Accessed 14 December 2022.

Hegarty, C. J. (2011). Analytical Model for GNSS Receiver Implementation Losses. *Navigation*, **58**(1), 29–44.

https://doi.org/10.1017/S0373463325101343 Published online by Cambridge University Press

Hein, G. W., Avila-Rodriguez, J.-A., Wallner, S., Pratt, A. R., Owen, J., Issler, J.-L., Betz, J. W., Hegarty, C. J., Lenahan, L. S., Rushanan, J. J., et al. (2006). MBOC: The New Optimized Spreading Modulation Recommended for GALILEO L1 OS and GPS L1C. Proceedings of the 2006 IEEE/ION Position, Location and Navigation Symposium, IEEE, 883–892.

Hennigar, A. (2014). Analysis of Record and Playback Errors of GPS Signals Caused by the USRP. Ph.D. thesis, Auburn University.

Jeffrey, C. (2015). *An Introduction to GNSS: GPS, GLONASS, Galileo and Other Global Navigation Satellite Systems*. NovAtel.

Jepson, D. (2019). RF System Synchronization — Baseband. https://www.gnuradio.org/grcon/grcon19/presentations/Synchronization_Core_Concepts_and_Applications/Daniel Accessed 14 December 2022.

KrakenRF Inc (2022). KerberosSDR Quickstart Guide. https://www.rtl-sdr.com/ksdr/. Accessed 14 December 2022.

Krueckemeier, M., Schwartau, F., Monka-Ewe, C. and Technische, J. S. (2019). Synchronization of Multiple USRP SDRs for Coherent Receiver Applications. 2019 Sixth International Conference on Software Defined Systems (SDS), IEEE, 11–16.

Kutkov, O. (2021). 1PPS Distribution Circuit. https://olegkutkov.me/2021/02/28/1pps-distribution-circuit/. Accessed 14 December 2022.

Laakso, M., Rajamäki, R., Wichman, R. and Koivunen, V. (2021). Phase-Coherent Multichannel SDR-Sparse Array Beamforming. 2020 28th European Signal Processing Conference (EUSIPCO), IEEE, 1856–1860.

Leclère, J., Landry, R., and Botteron, C. (2018). Comparison of L1 and L5 Bands GNSS Signals Acquisition. *Sensors*, **18**(9), 2779.

Ossmann, M. (2022). Hack RF. https://greatscottgadgets.com/hackrf/. Accessed 14 December 2022.

Pascual, D. (2022). danipascual/GNSS-matlab, GitHub. https://github.com/danipascual/GNSS-matlab. Accessed 14 December 2022.

Racelogic (2022). LabSat 3 Wideband. https://www.labsat.co.uk/index.php/en/products/labsat-3-wideband. Accessed 14 December 2022.

Rodriguez, J. A. A. (2008). On Generalized Signal Waveforms for Satellite Navigation. Ph.D. thesis, Universitätsbibliothek der Universität der Bundeswehr München.

Steigenberger, P., Thoelert, S. and Montenbruck, O. (2018). GNSS Satellite Transmit Power and its Impact on Orbit Determination. *Journal of Geodesy*, **92**(6), 609–624.

Tröster-Schmid, C. and Bednorz, T. (2016). *Generating Multiple Phase Coherent Signals–Aligned in Phase and Time*. Rohde & Schwarz GmbH & Co. KG, München.

Vagle, N., Broumandan, A., Jafarnia-Jahromi, A. and Lachapelle, G. (2016). Performance Analysis of GNSS Multipath Mitigation Using Antenna Arrays. *The Journal of Global Positioning Systems*, **14**(1), 1–15.

Yao, Z., Lu, M. and Feng, Z. (2010). Quadrature Multiplexed BOC Modulation for Interoperable GNSS Signals. *Electronics Letters*, **46**(17), 1234–1236.

Cite this article: Stankevičius, K. and Aleksiejūnas, R. (2025). Low-cost SDR-based GNSS signal recorder and replayer for equipment testing. *The Journal of Navigation* **78**: 2-3, 339–357. https://doi.org/10.1017/S0373463325101343

https://doi.org/10.1017/S0373463325101343 Published online by Cambridge University Press