RFI Monitoring in Support of Safety-Critical Multi-Band GNSS-based Systems

Aiden Morrison
SINTEF Digital
Trondheim, Norway
aiden.morrison@sintef.no

Nadezda Sokolova
SINTEF Digital
Trondheim, Norway
nadia.sokolova@sintef.no

Naveed Ahmed
Department of Engineering Cybernetics,
NTNU
Trondheim, Norway
naveed.ahmed@ntnu.no

***Abstract*—This paper discusses design details and field test verification results of a low-cost Radio Frequency Interference (RFI) event logger developed for monitoring the Global Navigation Satellite System (GNSS) L1 and L5 frequency bands for anomalous emissions that might disrupt or degrade Ground Based Augmentation System (GBAS) operation. On-going system evolution in support of simultaneous coverage of all present and upcoming L-band GNSS signals is also presented.**

Keywords—GNSS, Interference monitoring, Jamming

I. Introduction

Over the past several years the combination of ubiquitous, low-cost communications systems and satellite navigation has moved civil GNSS positioning and timing into use domains where there are stronger motivations for jamming attacks. In particular, widespread use in road-tolling/automotive insurance or asset-tracking/fleet-management systems, encourages attacks directed at GNSS. Jamming is not a selective process and it can affect multiple unintended targets in addition to the intended one.

As the infrastructure of some of the safety-critical GNSS-based systems such as GBAS must operate in close proximity to high traffic roads and airport parking, the risk of being affected is high [1]. This includes both the ground reference receivers and the airborne receivers during landing, roll-out and taxiing operations. As GNSS becomes more deeply embedded into societal infrastructure, we can expect to see more attacks of increased sophistication. Thorough evaluation of the operational environment is prerequisite to any system deployment. Monitoring and characterization of the threats that exist, and are likely to arise, is critical for effective protection.

While there are multiple options for Radio Frequency Interference (RFI) monitoring in the L-band, most of them cover only a small subsection of the L1 band, providing no observability for L2, L5, or even GLONASS L1. The RFI monitors with multi-band capabilities are typically high-end rack-mount solutions [2][3].

This paper focuses on the design of a low cost RFI monitor/event logger addressing the need for a cost-effective, easy to deploy, and mobile means of detecting and characterizing RFI events on the core GBAS Approach Service Types (GASTs) D and F (per definition used in the SESAR JU GBAS focused projects [4]) GNSS frequency bands: L1/E1 and L5/E5a.

Tests performed for system performance verification are also presented with the major focus on the results from field testing where multiple types of GNSS jammers including the wideband noise, CW, stepped CW/frequency hopping were used.

Additionally, the paper covers the on-going system evolution in support of simultaneous coverage of all present and upcoming L-band GNSS signals.

II. Low Cost RFI Monitor/Event Logger

The purpose of this section is to briefly describe the functionality and capabilities of the multi band RFI event datalogger, as well as system configuration steps taken to set the initial monitoring threshold.

A. Design

The RFI monitor/event logger is a low cost monitoring device designed to monitor the L1 and L5 bands for anomalous emissions that may disrupt or degrade normal operation of GNSS/GBAS receivers. It is a combination of a compact multi-channel digitizing L-band front-end with a compact low cost single board computer in a minimalistic enclosure. The design of the low cost datalogger supports easy deployment to available observation points and requires only a GNSS antenna connection plus a power connection, and functions autonomously without need of a screen or keyboard. Shown in Fig. 1 with an ruler for scale, the RFI event logger comprises a multi-channel RF front-end with energy monitoring, a control computer with push-button interface and removable storage.

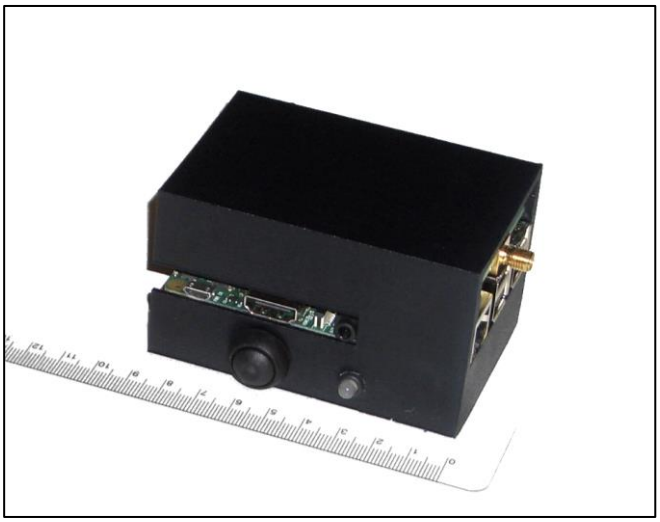

Fig. 1. Low Cost RFI Event Logger with ruler for scale.

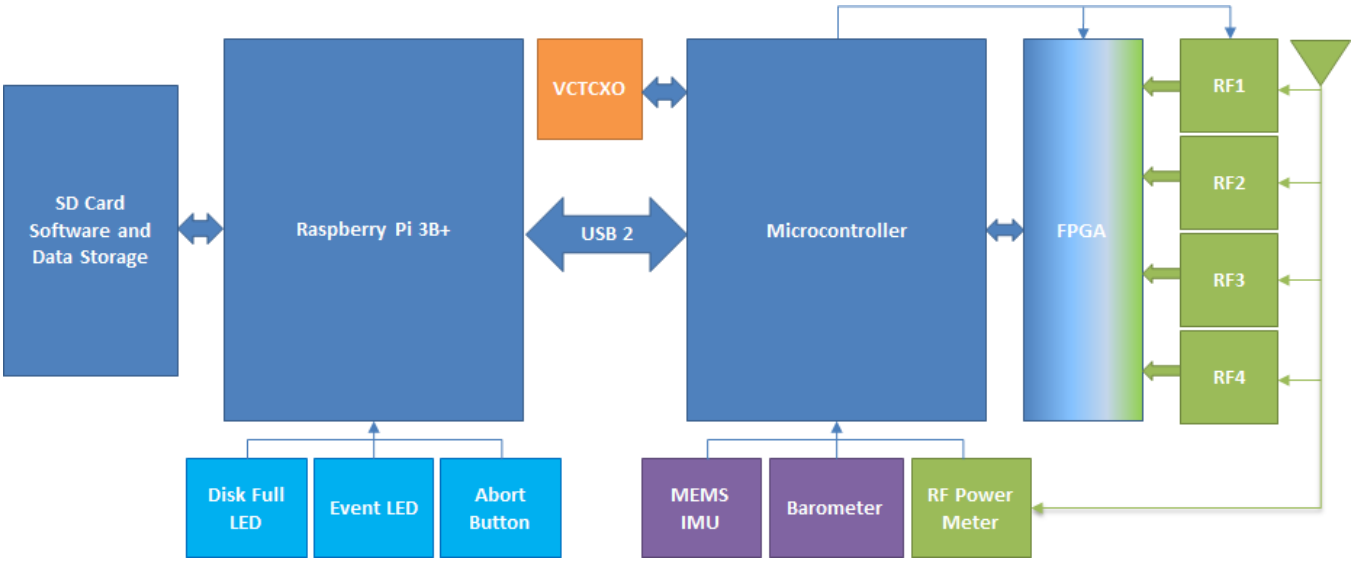

Fig. 2. Low Cost RFI monitoring system block diagram [5][6].

As indicated in Fig. 2 showing the basic structure of the unit, primary data flow goes from right to left, starting with the raw RF signal from the system antenna, passing through the FPGA and microcontroller firmware on the front-end module, before passing over a USB interface to the compute and storage module comprising a Raspberry Pi and SD card storage. RF elements are colour coded in green, with digital subsystems in dark blue. User interface elements are colour coded in light blue with the voltage feedback controlled TCXO in orange and peripheral MEMS sensors in purple. Since the raw files represent 21.6 or 24 MHz of spectrum, they are packed to 1-bit quantization during collection and storage after which they are unpacked to standard 8-bit integers for post-processing.

B. System Configuration

The event logger functions by using an integrated RF power meter as shown in Fig. 2 to continuously measure and characterize the background RF environment at the given installation location. A more detailed hardware design description and presentation of the additional system functionalities in support of synchronizing side channel information from non-RF sensors to be used for mobile monitoring (IMU, barometer, etc.), can be found in [4].

Online calibration allows the system to adapt to differences in the gain and loss characteristics of the antennas and signal distribution networks at each install site, as well as normal variations in the gain level of the antenna or other system components due to factors such as daily temperature trends. When the monitoring software running on Raspberry Pi 3B+ host computer detects power level deviations of sufficient magnitude and duration are present, the L1/E1 and L5/E5a signals are logged to disk in a packed format.

C. Approach to Data Analysis and Result Visualization

During post-processing the data is visualized in the form of a 'waterfall' plot for each of the L1 and L5 bands whereby color represents intensity of observed RF energy at each frequency level, and time scrolls vertically over each of the 90 second length event logs generated. Fig. 3 shows waterfall plot examples of the GPS L1 and L5 bands in the absence of interference. These plots show the stability in the spectral density over long periods covering both the L1 and L5 bands. An example of the total in-band power during these interference free periods is shown in Fig. 4. There is an almost smooth variation of around 2 dBm in the power levels except for the two spikes that last only a single epoch. As these spikes appear outside the L1 and L5 spectra, they are believed to be caused by adjacent band signals and are removed by setting the detection period for triggering an alarm to 3 seconds.

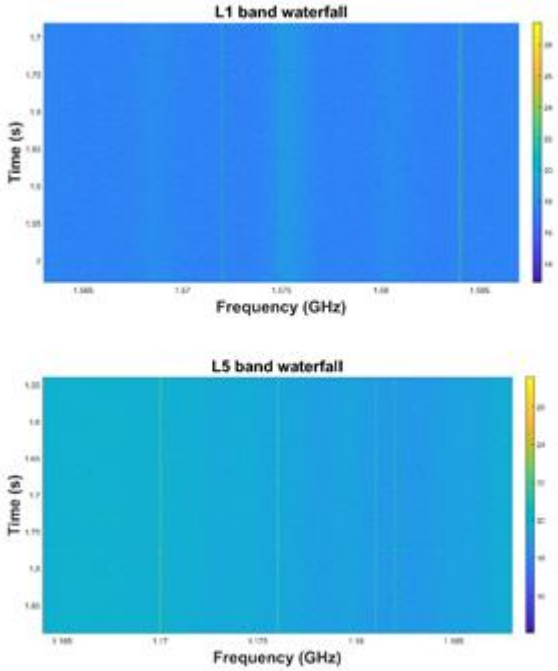

Fig. 3. Waterfall plot examples for the L1 band (top), and the L5 band (bottom) under nominal conditions.

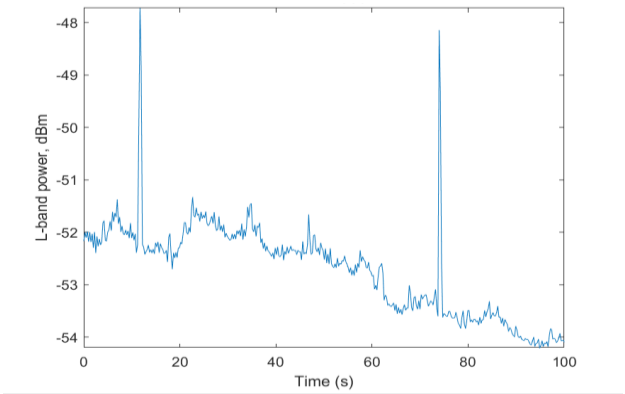

Fig. 4. Power level in interference free conditions. The observed spikes are believed to be caused by adjacent band signals as they are absent from the L1 and L5 spectra.

The weak tones present in the nominal spectra are due to residual DC imbalance and coupling within the low cost front-end, design imperfections that are minor nuisances in this application as they disappear in the presence of an external signal over the noise floor.

During abnormal RFI containing events (such as that shown in Fig. 9) the spectrum often changes rapidly with time (vertically) and loses the normally 'smooth' variation in power level (color) with both time and frequency. By viewing these generated waterfall plots the data can be classified by the user into categories such as narrowband interference, wideband interference, near-band interference, or false alarms. To aid in the analysis of collected RFI candidate events, the total L-band power level is measured by a sensor on board the front-end module and embedded in the data stream of RF samples for later analysis and plotting.

III. Verification

To assess the system performance, a number of simulations in controlled lab environment, and tests using live signals were performed. This section describes the verification tests done, and features the results obtained during field testing using live signals.

A. Simulated Signal Tests

To verify the sensitivity and triggering criteria of the L-band power monitoring hardware and algorithm, a simulated GNSS signal was generated and combined with a controlled RFI signal via conducted emissions to the RFI event logger as shown in Fig.5.

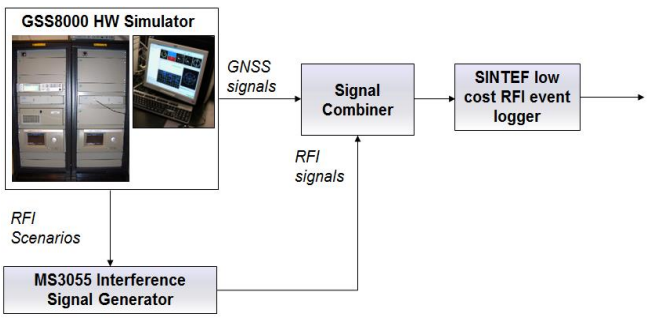

Fig.5. Equipment test set up for low cost RFI event logger in-lab verification.

In this verification exercise, the simulated GNSS signal was started first, after which the RFI event logger was activated and allowed to characterize the simulated baseline environment for a period of several minutes. After this initialization period has passed, a low intensity RFI event was simulated triggering the RFI event logger to record the affected signal spectrum to disk, which was later post-processed. This testing ensured that the monitoring algorithms and hardware were functioning as intended before the system was deployed to remote locations for data collection campaigns, or live signal tests.

B. Live Signal Tests

Verification outside of the laboratory was conducted using car-borne jammers. Due to the emission of a jamming signal in the protected spectrum necessary to conduct this type of live signal verification, this test was conducted in conjunction with the Norwegian communications authority (Nkom) and the defense research institute (FFI). In the test setup used, the jammers were deployed both statically as well as in vehicles which were driven past the testing location on a side-road, passing at variable short distances to simulate the passage of vehicle borne jammers past a static GBAS ground installation or other static GNSS-based infrastructure. Multiple jammer types were used including wideband noise, CW, stepped CW/frequency hopping to provide representation for each of the commonly encountered RFI types emitted by so called 'personal privacy device' jammers.

Despite such jammers being marketed to unsuspecting users as being 'personal' or somehow limited in range to the vehicle carrying it, the power output of at least one of the example jammers was in the vicinity of 1 Watt. To limit the disruption to other users, the tests were conducted in a valley well outside of the local urban centres, and in coordination with the Norwegian Public Road Authorities (NPRA).

It is noted that while jammers used in the tests covered different frequency band combinations (e.g. L1 only, L1/L2, L1/L2/L5), due to the design constraints of the low cost RFI monitor to capture events only on the L1 and/or L5 bands due to these being the signals used by GAST F GBAS, the results presented in the next section cover only the interference events observed by the unit.

C. Results

The datasets recorded during multiple drive by events, described in the previous subsection, were analysed using the waterfall plots.

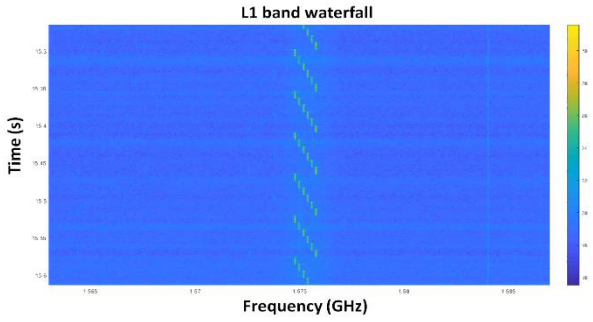

Fig. 6. Waterfall plot for the test using a dynamic stepped CW jammer, L1 band.

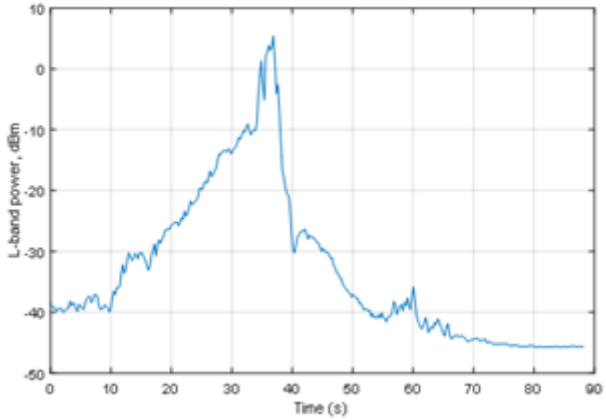

Fig. 7. Power level plotted as a function of time. Field test using a dynamic stepped CW jammer, L1 band. Note that on this scale the adjacent band pulses of 3 dB magnitude are not significant.

Fig. 6 shows an example of a frequency hopping continuous wave jammer spectral waterfall output, while the resulting in band power profile is given in Fig. 7.

Another example of a detected event is illustrated in Fig. 8 and Fig. 9, where the RFI datalogger captured a jamming signal impacting both the L1 and L5 frequency bands. The power levels observed during this even at the input of the integrated RF power meter are shown in Fig. 6. Unlike Fig. 4, the duration of the power excursion is longer than the 3 seconds that is set as the detection period for an alarm. The waterfall plots for the duration of jamming on GPS L1 and L5 signals show that majority of the band is affected by the suspected wideband pulse jammer. However, this is a rather critical situation that could be detrimental to the national infrastructure relying on L1/L5 E1/E5 GNSS.

In this particular case, L1/E1 and L5/E5a were all simultaneously impacted by interference. Since the jammer spectrum shown in Fig. 9 covers the entirety of the L1/E1 main lobes including the AltBOC components, unlike the jammer captured in Fig. 6, there will be little advantage to the use of Galileo E1 in this scenario relative to the use of legacy GPS L1.

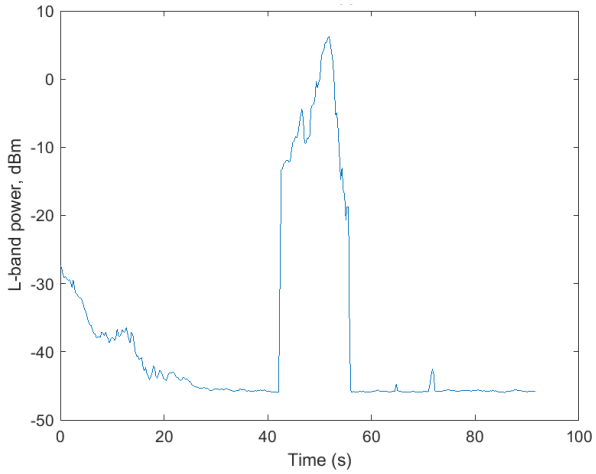

Fig. 8. Power level variation during an observed wideband pulse jammer event, L1 band.

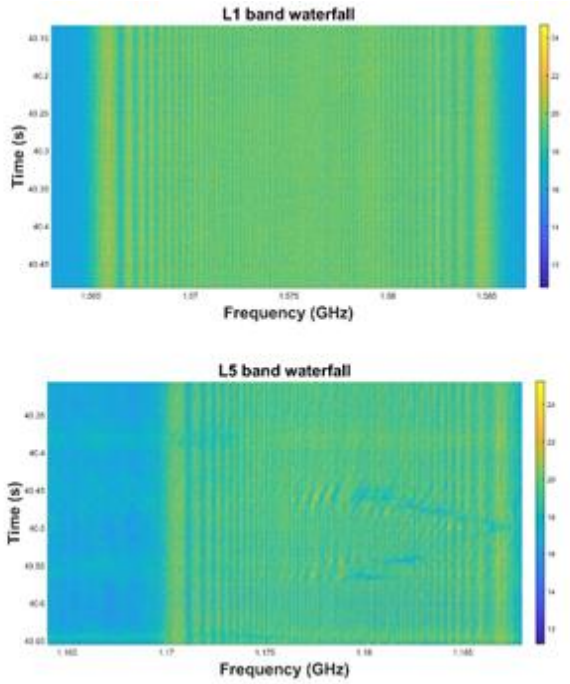

Fig. 9. Waterfall plots of the L1 band (top), and the L5 band (bottom) during a wideband pulse jammer event.

Due to the BOC structure of Galileo signals they are less susceptible to narrowband jamming events within the main lobe of the GPS L1 BPSK1 signal, but suffer equivalently in the presence of wide-band noise. For comparison the power spectral density of GPS and Galileo signals in the L1 and L5 bands are shown in Fig.10.

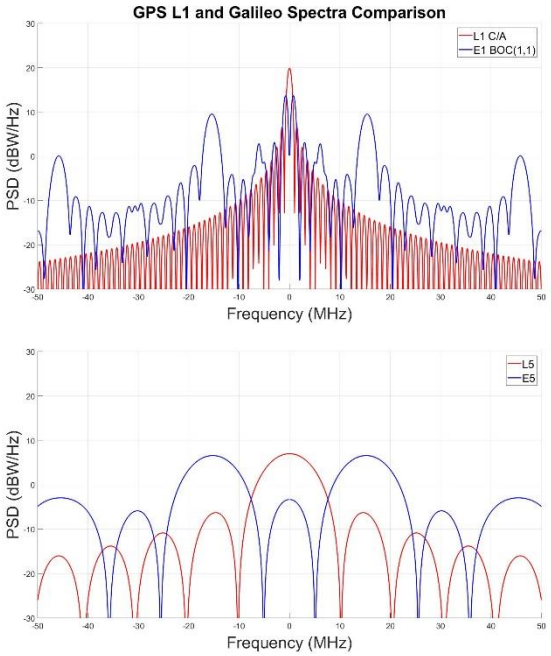

Fig.10. Comparison of GNSS Signals Spectra.

An interesting signal characteristic of the jammer shown in Fig. 9 is that its L1 component is well aligned to the nominal GPS/Galileo L1 centre frequency while its L5/E5a band emissions seem biased high by approximately 4-5 MHz. It is unclear if this is intentional on the part of the jammer designers to attempt to also partially cover E5b, or if it is simply a design choice.

The presence of strong RFI causes the RF signal chain to operate outside its nominal operating range. In conventional receivers, this would impact the functionality of the Automatic Gain Control (AGC) in the front end that normally only accounts for the thermal noise, as in normal situations the individual GNSS signals are buried under the noise floor. In the presence of RFI, the high-power signals would tend to saturate the Variable Gain Amplifier (VGA) present in the closed loop design of the AGC, hence, the AGC would be unable to adjust for the signal dynamics. In the current low cost design, however, this is not the case due to omission of the AGC as we are using single bit quantization. This trades the drawback of VGA saturation for one of zero dynamic quantization range, resulting in aliasing in the presence of in-band signals.

The aggregate power level recorded by the RFI datalogger for the same RFI emitter, but statically positioned at a substantial distance from the RFI monitor is shown in Fig. 10. The signal levels swing up to 7 dBm with abrupt "pulsating" variation observed due to unknown factors in the channel/environment between the emitter and receiving antenna. In this scenario the magnitude of the in-band power level is comparable to the 3dB out of band 'spikes' discussed earlier per Fig. 10. In the first half of Fig. 10 the distant jammer is active and dominates the in-band power estimate, while in the latter half it has been deactivated and only background variation including a single 3dB out of band emission spike remain. The waterfall plots, shown in Fig. 11, indicate that despite the distant placement of the jammer both the L5 and L1 bands are still substantially affected by the emitted RFI.

The plots show that the L5 band is not as adversely affected as the L1 band. In such cases, the receiver might be able to acquire/track the satellites with reduced stability.

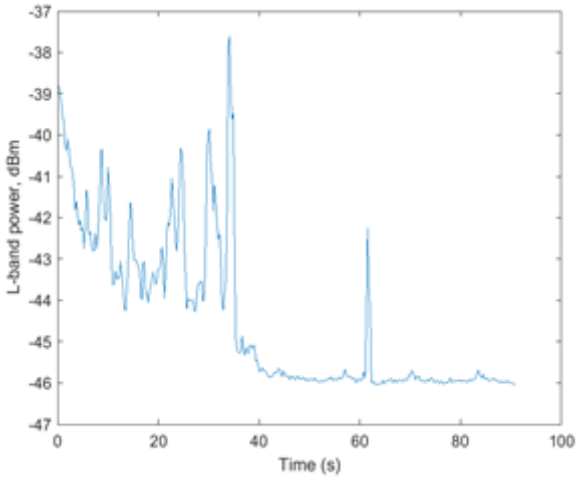

Fig. 11. Power level during a wideband pulse jammer event.

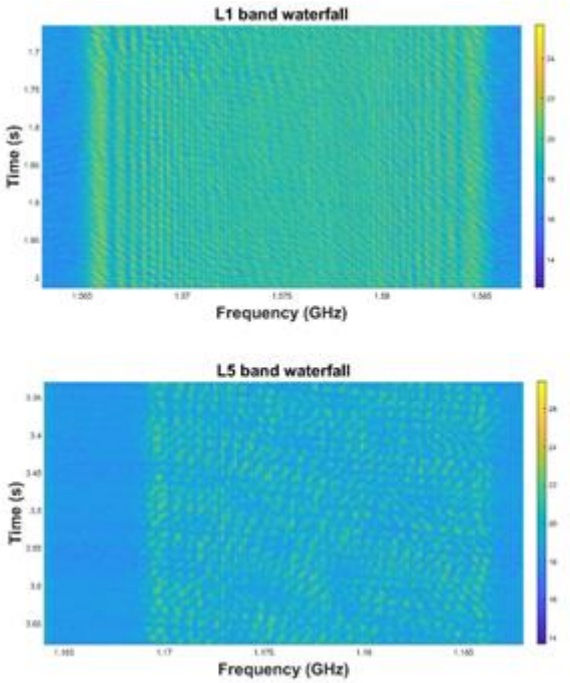

Fig. 12. Waterfall plots of the L1 band (top), and the L5 band (bottom) during a wideband pulse jammer event.

D. Single Bit Quantization

The current design of the low cost RFI event monitor/logger supports single bit quantization of the down converted signals that originate from the mixers. On the circuit board level, it is accomplished by connecting the MAXIM MAX2120 down converter's differential outputs to the differential I/O cell of the FPGA that is configured as a pair of input pins. The FPGA performs the quantization by assigning positive/negative state based on the difference of the signals at the differential inputs of the FPGA. This configuration simplifies the design to a greater extent excluding an external Analog to Digital Converter (ADC) and AGC between the analog and digital part of the front end that saves the cost, complexity and board space. Ideally, the transmission of signals on balanced/differential traces provides resistance to electromagnetic interference (EMI), but limitations of the board power supply design have allowed coupling of weak tones from the digital section to affect the noise floor of the nominal spectrum.

In the context of RFI characterization, the use of single bit quantization is undesirable, as the RFI signals can have a very large dynamic range relative to the normally received GNSS signals, which individually are below the thermal noise floor, and in aggregate only manifest as a small local increase of the spectral energy density. While single bit quantization is sufficient for the tracking of nominal GNSS signals due to the de-spreading process, the limited dynamic range makes analysis and characterization of the capture RFI events problematic.

IV. Future System Evolution

To address the limitations of the existing monitoring solution, a new version is under development that will

improve the system parameters, though at a higher size power and cost level. In particular:

RF architecture changes

To mitigate the occurrence rate of false alarms due to adjacent band signals, the evolved system will divide the RF chain in to high and low bands with independent RF power meters. Band selectivity will be achieved through the use of commercially available SAW filters, and though this will limit the meaningful tuning range of the individual RF channels it will dramatically reduce the sensitivity of the existing solution to emissions in the 1300-1550 MHz range.

Quantization and bandwidth changes

To expand the aliasing free dynamic range and aggregate spectral coverage of the collected signal samples in support of analysis and classification of detected RFI events, the bit depth of the quantization will be extended to 4 bits I and Q, while the sampling rates will be increased to approximately 55 MHz. This is intended to allow simultaneous coverage of all current L-band GNSS signals, including E6 and the overlaid B3 signal.

Compute Platform and storage changes

Since the evolved system will require aggregate bandwidth up to 220 MByte per second, the supporting compute platform will be based on a quad core ARM cpu with support for USB3 and PCIexpress based solid state storage devices.

Detection approach changes

To further mitigate the system false alarm rate while providing additional user adjustable parameters for event detection, the following strategy used for triggering the system will be adapted:

- The first stage of the detection process will still be based on aggregate RF power exceeding a threshold for a defined hold off period, but there will also be options to trigger on the upper or lower L-band power, or only when both are simultaneously elevated.
- The second detection stage will incorporate the use of the now necessary automatic gain control feedback signal to determine which if any tuners are experiencing measurable disruption. The combination of the first and second stage of detection along with the modified filtering architecture will serve to limit the amount of data which must be logged to only include those bands with activity if desired.
- The third stage of the updated detection approach will leverage the increased CPU power, optional network connectivity, and storage bandwidth to locally pre-process the collected data to further eliminate false alarms, and pre-screen collected data before bandwidth is consumed by its transfer to a remote system for final analysis, or in standalone mode to limit disk usage to only 'valid' events.

V. CONCLUSIONS

This paper presented a brief design review of a low cost RFI event monitor/datalogger and discussed the tests performed in order to verify its performance.

The results of the field validation activities have shown that as expected so called 'personal privacy devices' can severely disrupt the operation of GNSS receivers even at distances far beyond their stated 'in car' jamming ranges, making them a threat to safety of life systems such as GBAS that must position their antennas near busy roadways.

The results have also demonstrated that even a low-cost single bit front-end is sufficient for detection and high-level analysis of events in terms of their spectral coverage and characteristics.

Based on these activities and the results produced during their execution, several additional desirable design features were identified as necessary for future applications that will also monitor E5b, L2, and E6, such as extension to quad band operation from dual as well as the desire to better suppress the influence of adjacent band emissions, and to increase sample bit depth and dynamic range to facilitate additional analysis.

ACKNOWLEDGMENT

The authors would like to acknowledge the SESAR 2020 PJ14.03.01-GBAS project under which the design and verification activities of the discussed system were funded.

REFERENCES

[1] Warburton, J., C. Tedeschi, “GPS Privacy Jammers and RFI at Newark: Navigation Team AJP-652 Results,” 12th Int'l. GBAS Working Group Meeting (I-GWG-12), Atlantic City, NJ, Nov. 17, 2011.

[2] PXI Systems—National Instruments. Available online: http://www.ni.com/en-no/shop/pxi.html (accessed on 11 January 2019).

[3] SX3 GNSS Software Receiver. Available online: https://www.ifen.com/products/sx3-gnss-softwarereceiver/ (accessed on 11 January 2019).

[4] SESAR JU, PJ15.3.7 – MFMC GBAS, D04 - System Architecture, Requirements Definition and Safety Aspects, 2016.

[5] Morrison A., N. Sokolova and J. Curran (2018), Design of a Multiband Global Navigation Satellite System Radio Frequency Interference Monitoring Front-End with Synchronized Secondary Sensors, *SENSORS 2018*, 18(8):2594, doi:10.3390/s18082594.

[6] Curran, J.T.; Morrison, A.; Sokolova, N. Dual-Frequency Positioning via Time-Multiplexing of Single-Frequency Resources. In Proceedings of the ION GNSS+ 2017, Portland, OR, USA, 25–29 September 2017.

[7] IS-GPS-200 Revision F, IS-IRN-200F-001, Navstar GPS Space Segment/User Segment Interfaces, 21 September 2011

[8] Galileo OS SIS ICD Issue 1 Revision 1 September 2010e

[9] Fabio, D,; *GNSS Interference Threats and Countermeasures*, Artech House, 2015 pp 109-111.