In-Lab Receiver Testing Based on Live Captured RFI Events for DFMC GBAS Development

Nadezda Sokolova[1,*,†], Aiden Morrison[1,†] and Adrian Winter[1,†]

[1]SINTEF Digital, SCT Dept., Strindveien 4, Trondheim, Norway, 7034

Abstract

As the Ground Based Augmentation Systems (GBAS) have to often operate in close proximity to high traffic roads, parking garages, and other transportation infrastructure, the chances of being affected by unintentional Radio Frequency Interference (RFI) from low-cost jamming devices and malfunctioning equipment are high. Multiple recent studies have indicated that interference levels in such environments are frequently exceeding the tolerable limits for safety-critical system/infrastructure operations. It is therefore important for GBAS to have effective RFI detection and mitigation mechanisms. This article presents sample results and analysis of GNSS receiver responses to different RFI signal types generated based on real life observations made as part of multi-dimensional parameter spaces extracted from a multi-site, multi-year monitoring campaign carried out in Europe and Scandinavia. The obtained results are discussed in light of RFI monitor design in support of the dual frequency multi constellation (DFMC) GBAS ground system providing initial recommendations for the potential monitoring scheme with respect to which observables should be used and how they interrelate over the various RFI signal types.

Keywords

GNSS, RFI, GBAS, Interference monitoring

1. Introduction

While GNSS signals used in aviation are located in a protected Aeronautical Radio-Navigation Signal (ARNS) frequency band, jamming affecting this band is occurring frequently as it has been shown by multiple projects including the EU H2020 STRIKE3 [1], ESA NAVISP-EL3 Advanced RFI Detection Analysis and Alerting System (ARFIDAAS) [2], as well as multiple other studies (see e.g. [3, 4]). Results show that the amount of observed interference frequently exceeds the tolerable limits for safety-critical infrastructure systems. It is also expected that the occurrence rate, complexity, as well as the range will increase due to growing financial and geopolitical incentives [5]. Low-cost GNSS receiver manufacturers already support dual- and multi-frequency solutions. With GNSS being deeply embedded in today's digital infrastructure and numerous applications, more jamming events targeting multiple GNSS frequencies at the same time are being observed, as well as more attacks of increased complexity [6, 7]. GBAS is a local area GNSS-based precision approach guidance system for the final approach phase. The system is intended to be used for safety-critical operations (e.g., zero-visibility operations including Autoland), and is therefore designed to support very stringent integrity, continuity and availability requirements. GBAS ground reference receivers have to operate in close proximity to high-traffic roads and airport parking so the chances of being affected by RFI are high [8, 9]. At the current moment, the GBAS Approach Service Types (GAST) utilizing the GPS L1 and L5, as well as the Galileo E1 and E5a frequencies is still under development [10]. As resilience against unintentional RFI (here we are excluding the case of state actor generated high power, wide range attacks) is an important aspect of system design, reaction strategies necessary to ensure continuity and availability of service relying on multiple frequencies (i.e., switching between modes based on different core frequencies), as well as RFI monitoring and detection algorithms need to be developed. Development of such algorithms

WIPHAL'25: Work-in-Progress in Hardware and Software for Location Computation June 10–12, 2025, Rome, Italy

*Corresponding author.

†These authors contributed equally.

nadia.sokolova@sintef.no (N. Sokolova); aiden.morrison@sintef.no (A. Morrison); adrian.winter@sintef.no (A. Winter)

0009-0005-9079-1380 (N. Sokolova); 0000-0002-0617-9959 (A. Morrison); 0009-0006-6008-6039 (A. Winter)

requires knowledge of the current RFI threat space and an understanding of receiver responses to various interference signal types and characteristics. Mapping the RFI threat space is a challenging task as it relies on long-term monitoring, characterization, and threat evolution analysis. Within the ESA funded NAVISP-EL3 program ARFIDAAS project, more than a decade of aggregated GNSS site monitoring was analyzed with raw data for over 50 thousand RFI events captured [7]. This extensive database of the captured RFI events allows one to extract the important parameters, parameter ranges, and characteristics of different interference signals observed in real life and use those to generate representative signal types and patterns for in-lab testing. This article presents sample results and analysis of two GNSS receiver responses (NovAtel OEM7 and Septentrio mosaic-T) to different RFI signal types generated considering multi-dimensional parameter spaces extracted from the ARFIDAAS event database. The focus is on the GPS L1 and L5, as well as the Galileo E1 and E5a signals that are the core ones used in the next generation dual frequency, multi-constellation (DFMC) GBAS. The obtained results are discussed in light of RFI monitor design in support of the DFMC GBAS ground system development providing initial recommendations for the potential monitoring scheme with respect to which observables should be used and how they interrelate over the various RFI signal types. Since GBAS ground reference receivers do not implement time-frequency adaprive processing, or other algorithmic RFI mitigation measures, these are disabled on the evaluated receivers during the tests presented here.

2. Source of Data

2.1. ARFIDAAS Event Database

To support the in-lab testing carried out in this work, data captured by the ARFIDAAS GNSS RFI monitoring network was used as the basis. The network comprised 14 sites in Europe and Scandinavia, where each site is equipped with a low-cost monitoring unit supporting all navigation bands transmitted by GPS (L1, L2 and L5), Galileo (E1, E5a, E5b and E6), GLONASS (G1, G2 and G3) and Beidou (B1, B2 and B3). For more details about the monitoring unit design as well as event statistics and analysis see [4, 6, 7]. Each of the detected RFI events was passed through an automatic event classification algorithm [4] for identifying jamming signal type and its characteristics (center frequency, bandwidth and time modulation frequency, etc.). Classification results, site details, as well as the captured raw signal samples for all the detected events at each monitoring site where then stored in the cloud. The accumulated database includes more than 50 thousand RFI events captured across the ARFIDAAS monitoring network. As illustrated in Figure 1, for event classification within the ARFIDAAS system, fourteen RFI types across four main categories (narrowband, time-modulated, wideband, and environment baseline) were defined.

As presented in [10] where the developed automatic classification algorithm is described, the narrowband category includes RFI signals that evidence one or more narrowband signals. The time modulated category collects events which have signals where the power is concentrated in a specific region of the spectrum over each observation interval within the limits of the Fourier transform window width(s) used such as chirp signals where the power is swept over a range of frequencies but at each epoch it is concentrated at a specific frequency. Wideband events are in contrast those for which the RFI signal impacts one or more regions of the spectrum, but for which the signal cannot be isolated in frequency versus time, such as white noise sources. The fourth category called ‘environment baseline’ is a special case where the event has not measurably distorted the observed spectrum despite the in-band power meters and Automatic Gain Control (AGC) feedback detection criteria being met. As this increase in measured in band power without spectral profile distortion is what would be expected during a low power spoofing event, this category serves as an indication of potential spoofing/meaconing events. It is noted that at the current moment, the analysis results of this group of events are yet available, and will not be used as part of the work presented in this article leaving the focus purely on jamming.

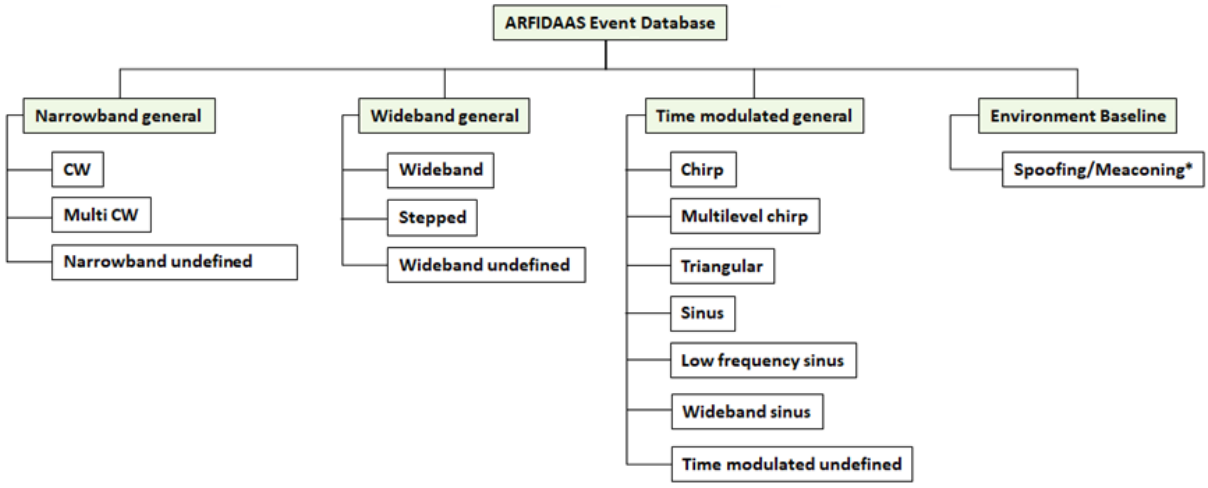

Figure 1: GNSS RFI event categories used in the ARFIDAAS system [10]. Categorization of events as spoofing/meaconing under the Environmental Baseline is indicative.

Table 1
RFI parameter ranges for the Time-modulated general event category.

Time-modulated general						
Parameter range	Linear chirp	Multilevel chirp	Sinusoidal	Low frequency sinusoidal	Time-modulated undefined	Triangular
Bandwidth (MHz)	0.17 – 35.57	0.17 – 34.7	0.17 – 16.5	0.2 – 2.4	0.17 – 28.46	0.34 – 28.1
Repeat rate (kHz)	0.68 – 573.6	0.11 - 1294	4 - 556	0.7 - 4	0.23 – 555	0.29 - 319
Power (dB)	2 – 37.93	2 – 34.2	2 - 11	2 - 4	2 – 37.9	2 – 28

Table 2
RFI parameter ranges for the Narrowband general event category.

Narrowband general		
Parameter range	CW	Multi CW
Centre frequency (MHz)	1555 - 1615	-
Power (dB)	2 – 20	2 - 23
Number of CWs	-	2 – 15
Spacing between tones (MHz)	-	0.17 – 17.7

2.2. Parameter Set Extraction

The event classification results accumulated across sites and over time allows one to study the observed jamming signal characteristics, define key parameter sets for each of the main signal categories, as well as define parameter ranges based on real life observations. Tables 1-3 show parameter ranges for the three of the most frequently observed categories [6], namely the time modulated, wideband and narrowband jamming signal types. In total, there are eleven RFI signal categories covered of the thirteen listed in Figure 1. excluding the environment baseline category. While the ARFIDAAS system classifier was developed to identify each of these types, some were not observed in the wild by the monitoring network leading to Tables 1-3 having the indicated subset of signal types present. Another important detail to note here is that the extracted parameter sets and ranges include all observations made by the ARFIDAAS network also considering the non-standard events that were classified as a particular type while not matching the standard characteristics. Figure 2 shows examples of such events. In both cases, the automatic classification algorithm placed the event in a particular category, however each of the events was on closer inspection not a clear match to the expected signal structure.

Event shown in Figure 2 (a) for example was classified as multilevel chirp, and while there are some features in it resembling one, it is difficult to say why such a signal structure would be used to jam GNSS

Table 3
RFI parameter ranges for the Wideband general event category.

Wideband general			
Parameter range	Wideband	Wideband Stepped	Wideband (sinusoidal)
Bandwidth (MHz)	0.17 - 29.2	0.17 – 25.2	0.17 – 24.51
Power (dB)	2 – 28.8	2 – 24.7	2 - 21
Repeat rate/burst length (kHz)	-	-	0.17 – 634

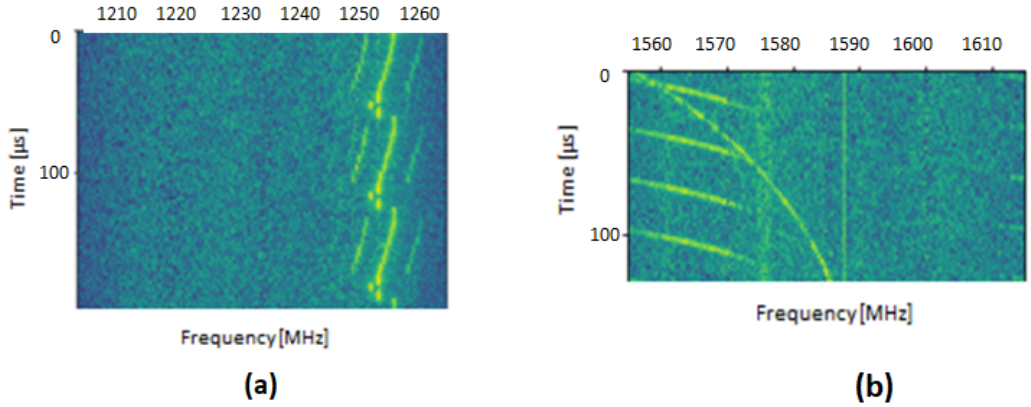

Figure 2: (a) A detected potentially unintentionally generated RFI event in the GLONASS G2 band classified as a multilevel chirp. (b): A detected RFI event comprised of a weak CW, an exponential and linear chirp signals in the same band classified as a time-modulated undefined.

as it might not be as efficient as a less complex signal modulation. For this reason, and based on the fact that the center of the RFI is located several MHz above the band center of GLONASS G2, it is believed that this signal is unintentionally generated. The example shown in Figure 2 (b) is a special case as it contains three distinct perturbing signals at power levels low enough that the main lobes of the GPS and Galileo L1/E1 signals are still visible. While the weak CW signal is of no note, the simultaneous occurrence of two distinct time modulated signals is. In addition to the traditional linear chirp signal, an exponentially swept signal is present.

This exponentially swept form was not observed during the first two years of the ARFIDAAS network operation and therefore was not defined as a separate signal type, however, by the end of the fourth year of operation this signal type was present with some regularity at multiple sites. While such a scenario containing multiple different RFI types plus a novel modulation which the classifier was not designed to isolate represents a significant challenge to classification, the classifier successfully categorized this event as a form of time-modulated interference. The identified parameter ranges as shown in Tables 1-3 have been used to define the limits of the simulation space. In this paper, we focus on a selected subset of results from the category of time-modulated (single linear, single exponential, and linear in combination with exponential chirp simultaneously as shown in Figure 2 (right)). The motivation for focusing on the dual signal case comes from a concern that this newly observed RFI combination may have been selected by malicious actors due to particularly disruptive impacts to GNSS signal tracking. In order to establish a baseline for comparison, it was decided to also test the traditional linear chirp impacts over their observed parameter space as linear chirp is by far the most frequently observed time-modulated RFI type in the wild. A particular note is that these evaluations focus on threshold impact power levels to stimulate disrupted tracking behavior in the receivers while allowing them to maintain signal lock so as to still provide observables/measurements for analysis. Since the GNSS receiver devices under test (DUT) must be run in real-time and require both initial acquisition time as well as a reset interval to ensure independence between test cycles, the number of simulation cycles and therefore the granularity of the 3D simulation space had to be constrained. With each simulation cycle desired to produce 60 seconds of RFI impacted output data, a single simulation cycle requires 5 minutes.

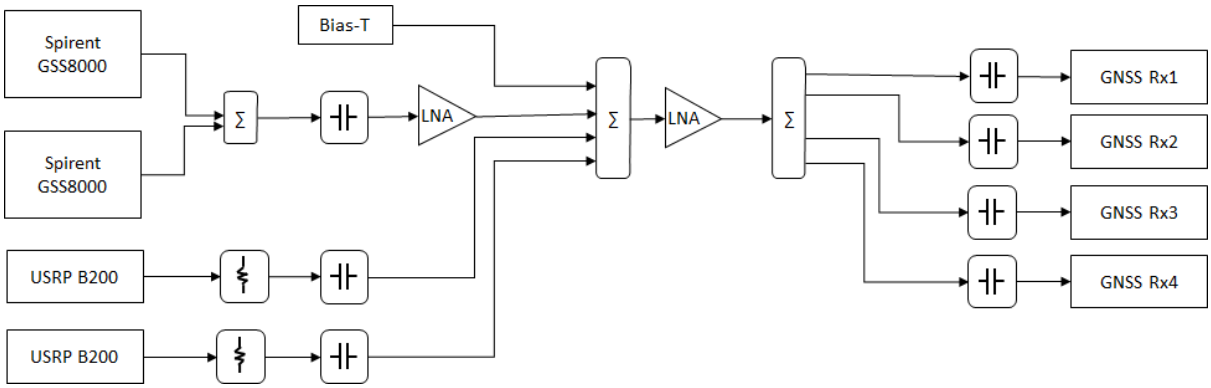

Figure 3: Schematic overview of the simulation equipment setup for dual frequency operation. Use of two USRPs allows for dual frequency, multi-source RFI generation.

Given a simulation grid of 13 bandwidth steps, 17 repeat rate steps, and 8 different power levels the aggregate simulation cycle reaches 2.5 days for a single scenario such as linear chirp, exponential chirp or the combined dual chirp. The amount of time is tripled in the case when the performance is evaluated on two frequency bands individually and combined (i.e. L1, L5, and L1 + L5).

3. Simulation Setup

To generate the jamming signal types observed live, the equipment setup illustrated in Figure 3 was used. A HW GNSS Spirent GSS800 simulator was supplemented by two Ettus Research universal software radio peripheral (USRP) B200 units for jamming signal generation. The USRP radios used have an adjustable transmit power gain between 0 and 89 dB, where a gain setting of 15 dB corresponds to an increase in total received power in band of 1 dB at each of the connected receivers. The supported signal bandwidth can go up to 50/55 MHz. When two jamming signals are simulated in the same frequency band, this setup allows for digital adjustment of the power level between signal components sent by the same radio. While this test bench equipment setup allows for the evaluation of four receivers simultaneously, the results in this paper focus on observations made from two geodetic grade receivers (NovAtel OEM7 and Septentrio mosaic-T). To confirm the capability to produce complex combined signal events prior to running a large number of simulations, the equipment setup was thoroughly tested to ensure that the interference signals were generated correctly. For this purpose, the ARFIDAAS front-end was used to capture and analyze the combined signal outputs.

While this test bench equipment setup allows for the evaluation of four receivers simultaneously, the results in this paper focus on observations made from two geodetic grade receivers (NovAtel OEM7 and Septentrio mosaic-T). To confirm the capability to produce complex combined signal events prior to running a large number of simulations, the equipment setup was thoroughly tested to ensure that the interference signals were generated correctly. For this purpose, the ARFIDAAS front-end was used to capture and analyze the combined signal outputs.

4. RFI Monitoring in GBAS

GBAS development must be carried out in accordance with rigorous standards therefore system evolution process is complex and time demanding with dual frequency architecture still in development phase. Design of an appropriate RFI monitoring scheme for a dual frequency system is therefore still a topic for investigation. While there is no dedicated RFI monitor, interference detection in GBAS ground reference receivers is typically carried out by monitoring the variation of the Carrier-to-Noise density ratio (C/N0) or various metrics derived from it in the form of the required low signal power monitor. While other signal/measurement quality monitors might be triggered by RFI, their purpose is to ensure integrity of service in the presence of other specific threats, so while the faulty measurements/ranging sources

will be excluded ensuring required performance, this information is typically not used for flagging the presence of RFI. This misattribution could lead to incorrect assumptions about the environment at given sites and otherwise lead to overlooking mitigation options such as berms and fences which would potentially resolve the RFI. Although the use of the Automatic Gain Control (AGC) outputs and histograms of analogue-to-digital converter (ADC) bins for RFI monitoring have been demonstrated to be very effective and sensitive, their availability is not guaranteed. While any receiver that utilizes multi-bit sample quantization would be expected to contain an AGC if not a histogram engine, these measurements are not always output by the receiver/visible to the user. With specific consideration of GBAS, currently there is no certified dual frequency GBAS ground receiver available, while the available certified single frequency GBAS receivers do not output either of these metrics. In this work we have therefore focused on the known available/supported measurements. It is also noted that while additional RFI suppression measures are desirable (e.g. use of the Controlled Reception Pattern Antennas), their use in GBAS may introduce calibration errors that will degrade system integrity and availability even if these measures will reduce the system's vulnerability against RFI.

5. Results and Analysis

As mentioned above, the results presented in this article focus on a sub-set of interference signal types, namely single linear, single exponential, and linear in combination with exponential chirp simultaneously. In the case of a single signal, the identified parameter set space is covered for the considered signal type. The dual signal case covered in this article is represented by the combination of a variable exponential chirp signal, meaning that for this signal type in each test a different sub-set of parameters is used, while the modulation parameter set for the linear chirp signal is kept the same at 200 kHz repeat rate and 20 MHz bandwidth. The power level of both signals is varied with constant relative offset. Since the primary interest of this study is the relative impact of the various jamming signal modulations over their parameter space, the results are presented to emphasize trends and not the absolute performance. High level and expected results include the observations that different receivers respond differently to the generated RFI types and regions of the parameter space. Due to reasonably expected differences in the C/N0 estimators and the tracking loop designs and parameters implemented in the receivers, their responses to various parameter combinations were notably different. In GBAS, this factor is taken into account by characterizing the performance of a specific certified receiver model when designing fault monitoring algorithms. One observation of note is that the impact of certain RFI modulation and parameter combinations result in differentially observable effects between the C/N0 degradation and the carrier phase uncertainty amplification. This is illustrated in Figures 4 and 5in the case of a single linear chirp signal where the NovAtel OEM7 receiver reports a near random but low loss of signal power for all RFI parameters for both GPS L1 C/A and Galileo E1 signals, but high noise in the carrier phase measurements in response to lower sweep bandwidths and lower repeat rates for GPS L1 C/A, while Galileo E1 is sensitive to bandwidth, but insensitive to the repeat rate. This scenario has the interference signal power level injected which raises the received total power in band by 1 dB. This is a very low power RFI signal, so the observation is of note in that even a very weak RFI signal causes both observable degradation as well as noticeable differential observable behavior. The same behavior trend has been observed when higher linear chirp signal power was considered though with a more frequent and longer lasting loss of observables starting with frequent cycle slipping and progressing to complete loss of lock.

The same general observation holds when considering the exponential chirp signal as it impacts the GPS L5 tracking by the same receiver. Figure 6 shows the C/N0 degradation and the carrier phase measurement uncertainty observed in a scenario with a higher level of in band power (7 dB). Here the C/N0 degradation is sensitive to only the bandwidth of the exponential chirp, while carrier phase uncertainty is particularly sensitive to only a small region of the bandwidth and the repeat rate parameter space. While it is believed that the enhanced sensitivity of the L5 signal tracking to certain repeat rates of the exponential chirp RFI is related to the symbol rate of the signal, the same cannot be said

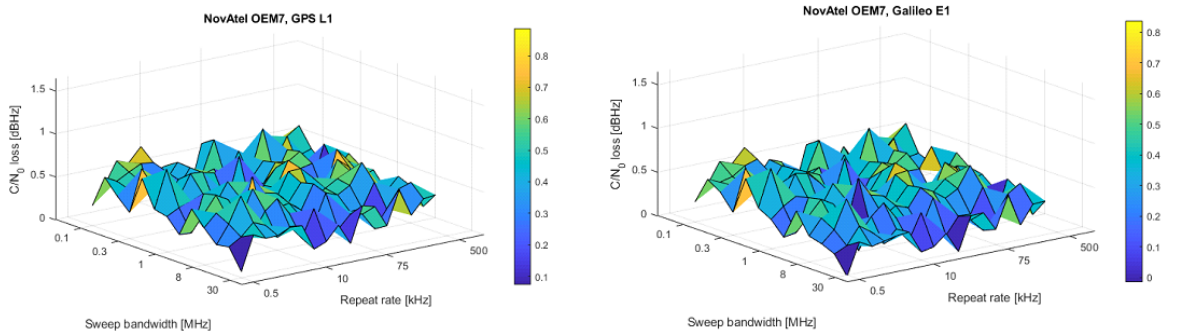

Figure 4: NovAtel OEM7 receiver C/N0 loss in the presence of a linear chirp interference signal. Power +1 dB.

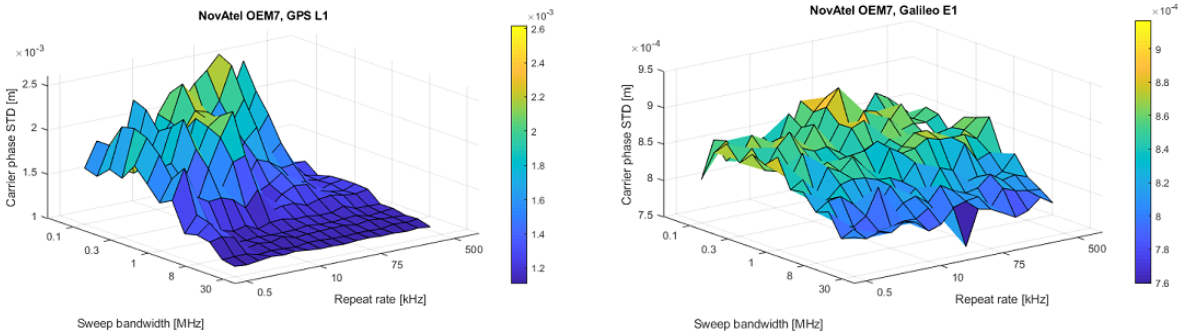

Figure 5: NovAtel OEM7 receiver carrier phase uncertainty in the presence of a linear chirp interference signal. Power +1 dB.

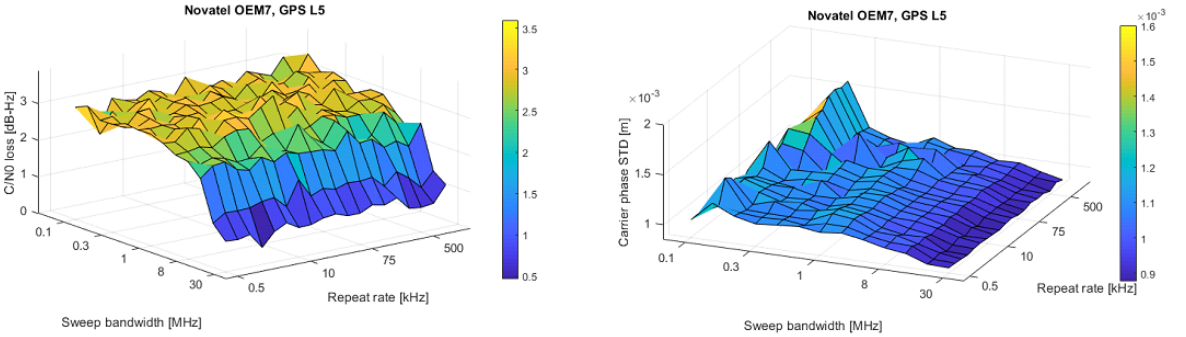

Figure 6: NovAtel OEM7 receiver C/N0 loss and carrier phase uncertainty in the presence of an exponential chirp interference signal. Power +7 dB.

for the L1 and E1 signal responses to the same RFI type. As shown in Figure 7 illustrating the results captured by the Septentrio mosaic-T receiver from the combined simultaneous linear and exponential chirp signals, the C/N0 loss and the carrier phase noise responses of the L1 and E1 signals match in their trends over the parameter space and the peak disruptions correspond to the parameter set where the quasi-constant frequency portion of the exponential sweep overlays a modulation main lobe. These sensitivities manifest regardless of the presence of the simultaneous linear chirp signal, meaning they are the function of the exponential chirp and not the combination of the two signal types. The same general observation holds when considering the exponential chirp signal as it impacts the GPS L5 tracking by the same receiver. Figure 6 shows the C/N0 degradation and the carrier phase measurement uncertainty observed in a scenario with a higher level of in band power (7 dB). Here the C/N0 degradation is sensitive to only the bandwidth of the exponential chirp, while carrier phase uncertainty is particularly sensitive

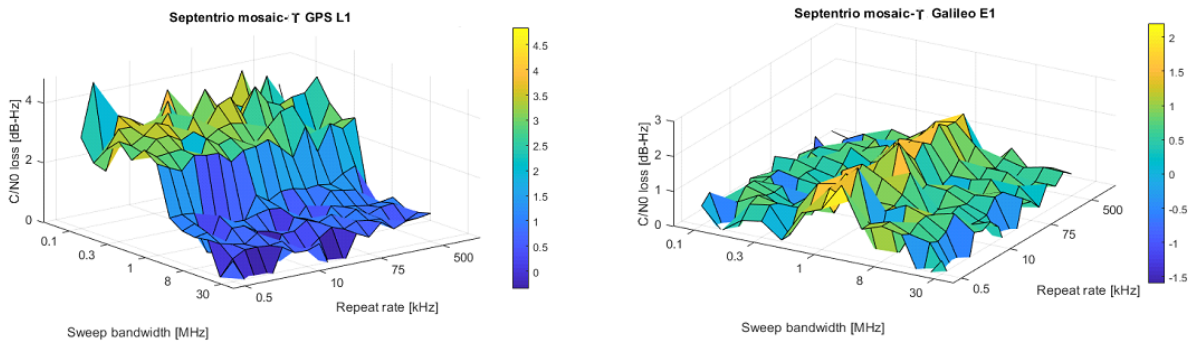

Figure 7: Septentrio mosaic-T receiver C/N0 loss in the presence of a variable exponential and a static linear chirp signals. Power +10 dB.

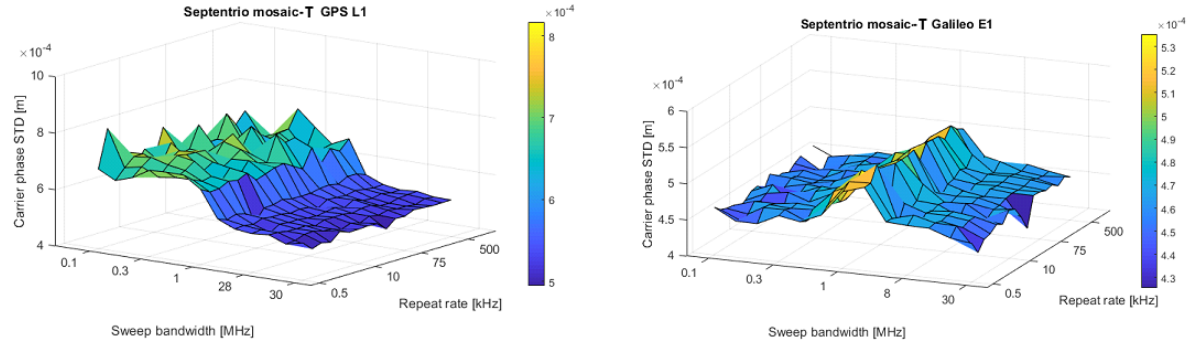

Figure 8: Septentrio mosaic-T receiver carrier phase uncertainty in the presence of a variable exponential and a static linear chirp signals. Power +10 dB.

to only a small region of the bandwidth and the repeat rate parameter space. While it is believed that the enhanced sensitivity of the L5 signal tracking to certain repeat rates of the exponential chirp RFI is related to the symbol rate of the signal, the same cannot be said for the L1 and E1 signal responses to the same RFI type. As shown in Figure 8 illustrating the results captured by the Septentrio mosaic-T receiver from the combined simultaneous linear and exponential chirp signals, the C/N0 loss and the carrier phase noise responses of the L1 and E1 signals match in their trends over the parameter space and the peak disruptions correspond to the parameter set where the quasi-constant frequency portion of the exponential sweep overlays a modulation main lobe. These sensitivities manifest regardless of the presence of the simultaneous linear chirp signal, meaning they are the function of the exponential chirp and not the combination of the two signal types.

6. Conclusions

Based on the analyzed results presented in this article, initial recommendations for the DFMC GBAS monitoring scheme based on observables available within GBAS implementations include the need to monitor for the impacts of RFI separately on each individual signal modulation even in cases where those modulations are spectrally overlapped as indications are that subtle interactions of signal parameters and tracking strategies can lead to substantial differences in impact. Further, it is believed that the use of existing monitors to isolate the RFI impact would imply further work due to the lack of uniformity in the impact over the parameter space on the observables generated. This variable impact leads to triggering of different monitors for different RFI modulations and varied parameters within a modulation. For this reason, monitoring of RFI directly via automatic gain control feedback or other novel monitoring is desirable though acknowledged to require new outputs be made available. While the authors still believe that the exponential chirp signal is tuned to defeat certain types of RFI mitigations as previously

discussed in [7], in the context of this study where all receiver level RFI mitigations are disabled we can observe that the combination of linear and exponential chirps has no additive effects on the receivers beyond the impacts of the individual RFI signals. Comparing the impacts of the two signal types individually, the exponential chirp signal achieves higher phase stability impacts at lower relative power levels for the L1 and E1 signals.

7. Acknowledgments

The authors would like to thank the European Space Agency (NAVISP program) for funding the development of the ARFIDAAS system used for live data capture, as well as the Norwegian Council of Research (project number 344275) and HEU/EUSPA EDGAR project (project number 101130407) for funding the in-lab simulation environment development and data analysis.

Declaration on Generative AI

The author(s) have not employed any Generative AI tools.

References

[1] S. Thombre, M. Bhuiyan, P. Eliardsson, B. Gabrielsson, M. Pattinson, M. Dumville, D. Fryganiotis, S. Hill, V. Manikundalam, M. Poeloeskey, S. Lee, L. Ruotsalainen, S. Soderholm, H. Kuusniemi, GNSS threat monitoring and reporting: Past, present, and a proposed future, Journal of Navigation 71 (2018) 513–529. doi:10.1017/S0373463317000911.

[2] ESA NAVISP3, Advanced RFI Detection Analysis and Alert System (ARFIDAAS) project, 2019. URL: https://navisp.esa.int/project/details/135/show.

[3] N. Gerrard, A. Rødningsby, A. Morrison, N. Sokolova, C. Rost, GNSS RFI Monitoring and Classification on Norwegian Highways – An Authority Perspective, , in: proceedings of the 34th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2020+), St. Louis, Missouri, USA, 2021.

[4] N. Gerrard, A. Morrison, N. Sokolova, C. Rost, Exploration of Unintentional GNSS RFI Sources: Causes, Occurrence Rates, and Predicted Future Impact, in: proceedings of the 35th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2022), Denver, CO, USA, 2022.

[5] EUROCONTROL, Aviation Intelligence Unit, Does RFI to satellite navigation pose an increasing threat to network efficiency, cost-effectiveness and ultimately safety?, Think Paper #9, 2021. URL: https://www.eurocontrol.int/publication/eurocontrol-think-paper-9-radio-frequency-interference-satellite-navigation-active.

[6] N. Sokolova, A. Morrison, A. Diez, Characterization of the GNSS RFI Threat to DFMC GBAS Signal Bands, Sensors 22 (2022) 8587. doi:10.3390/s22228587.

[7] A. Morrison, N. Sokolova, A. Diez, The Evolving GNSS RFI Threat Space, in: proceedings of the 36th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2023), Denver, CO, USA, 2023.

[8] J. Warburton, C. Tedeschi, GPS Privacy Jammers and RFI at Newark: Navigation Team AJP-652 Results, in: proceedings of the 12th International GBAS Working Group Meeting (I-GWG-12), Atlantic City, NJ, USA, 2011.

[9] RNT Foundation, GPS Jammer Delays Flights in France, 2017. URL: https://rntfnd.org/2017/09/15/gpsjammer-delays-flights-in-france/.

[10] A. Diez, A. Morrison, N. Sokolova, Automatic classification of RFI events from a multi-band multi-site GNSS monitoring network, in: proceedings of the 35th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2023), Denver, CO, USA, 2022.