Advanced RFI Detection, Alert and Analysis System Design and Monitoring Campaign Results

NAVITEC 2022

04 - 08 April 2022
ESA/ESTEC, Noordwijk, The Netherlands

Aiden Morrison(1), Nadezda Sokolova(1), Richard Swinden(2), Luciano Musumeci(2), Gianluca Caparra(2)

(1)SINTEF
Strindveien 4, 7034 Trondheim, Norway
Email:Aiden.Morrison@sintef.no, Nadia.Sokolova@sintef.no

(2)ESTEC
Keplerlaan 1, PO Box 299
NL-2200 AG Noordwijk, The Netherlands
Email: Richard.Swinden@esa.int, Luciano.Musumeci@esa.int, Gianluca.Caparra@esa.int

INTRODUCTION

The Advanced Radio Frequency Interference (RFI) Detection Analysis and Alerting System (ARFIDAAS) projects focus on providing Global Navigation Satellite System (GNSS) users and GNSS-based service providers with low latency notifications of the detection of Radio Frequency Interference (RFI) impacting their receiving equipment while also building a centralized database of activity from multiple sites for subsequent analysis and reporting. With some stations operating continuously since 2019, more than twenty terabytes of captured spectrum and generated analyses of GNSS RFI events have been collected. Within this paper the design and deployment of the system are presented along with discussions of information gathered during full-year monitoring periods from five selected stations within Scandinavia and Europe.

SYSTEM DESIGN

The ARFIDAAS hardware comprises a purpose built front-end which allows simultaneous coverage and capture of all present GNSS L-band signals from all operative constellations while also providing data streams specifically selected to aid in the tasks of detection and characterization of both unintentional RFI events and malicious jamming activity.

The signal handling sections of the front-end shown in Fig 1. are designed to tolerate the maximum signal power which can be represented by an active antenna when the five volts internal bias voltage optionally generated by the front-end is used to power the antenna low noise amplifier (LNA). Alternatively, the front-end can also tolerate high reverse biasing voltages as a precaution against being connected to an externally biased network without a DC-block. The onboard oscillator is an Oven Controlled Crystal Oscillator (OCXO) in order to provide a stable phase reference for RFI signal analysis, and is made available on an external SMA connection to optionally drive external equipment synchronously. Alternately, an external 10 MHz signal may be fed in to the front-end to drive it instead of the onboard oscillator. On the digital side of the design the system FPGA communicates via a USB3 first in first out (FIFO) from which command packets for configuration of the front-end parameters are received, while packets containing collected samples and metadata (e.g. bit bin populations, automatic gain control (AGC) parameters, measured in-band power meter outputs, current configuration parameters) are streamed to the host system. While both the original and second generation ARFIDAAS front-ends handle four bit quantization internally for AGC feedback, the output of the first generation system was limited to 3 bit quantization at 60 MHz complex for a total of 180 MB/second of data [1], while the second generation hardware is capable of 4 bit quantization at 75 MHz for 300 MB/second of data. The additional dynamic range is useful in situations where RFI sources can emerge from behind obstructing buildings or terrains at close range, allowing the system to avoid or minimize saturation while the AGCs adapt to the increased received power level.

Design elements of note which assist in the objective of RFI monitoring include the combined wide coverage and tight band selectivity provided by a dual SAW filter input configuration which excludes all non-GNSS bands prior to the mixing and down conversion stages where additional anti-aliasing filters are applied to the intermediate frequency data, and the inclusion of direct in-band RF power measurement sensors. In the case of the in-band power measurement sensors, this data stream allows the ARFIDAAS system to accurately assess relative changes in the local RF environment independent of the modulation of the encountered RFI signals, in contrast to solutions which rely only on C/N0 or AGC feedback monitoring based power level assessment.

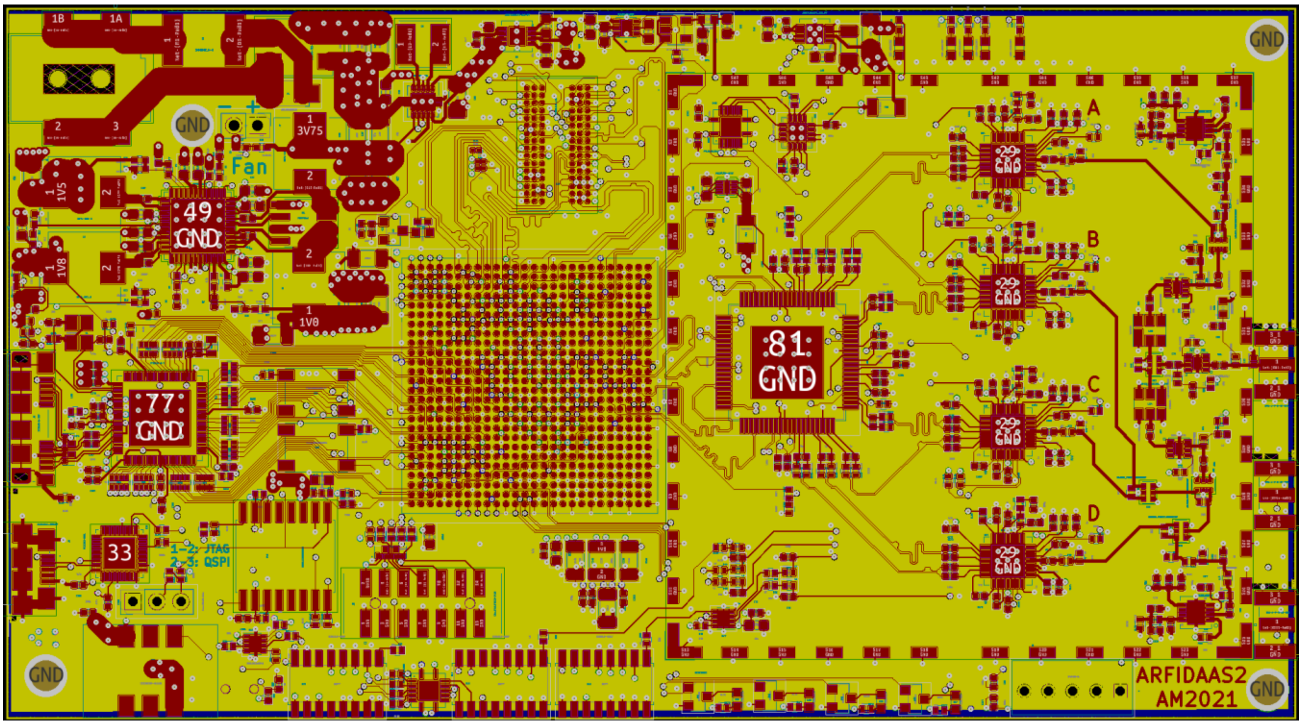

Fig. 1. ARFIDAAS second generation front-end printed circuit board (13.5 x 7.5 cm)

The software and cloud interfaced portions of the ARFIDAAS system design are shown in Fig 2. The software of the ARFIDAAS system is designed to provide essential event data to site operators at low latency as well as comprehensive information to shared cloud storage to enable both immediate reactions to RFI when necessary as well as complete event data for later centralized analysis. The detection software deployed on each node is configurable via a web interface to allow site operators to define the characteristics of the RFI that they wish the system to detect and report. Detection options include the length and intensity of RFI necessary to trigger a detection, the rate at which both in-band power and AGC thresholds are allowed to vary to account for factors such as thermal variation in the antenna LNA, duration of raw RF data to be collected during a detection event. Additional options include both the email addresses to be notified during detections, and the limitations to usable instantaneous and monthly upload bandwidth the system should respect.

After initial notification emails are sent with rapidly generated spectrogram and waterfall plot contents, a source classifier algorithm is run on the edge computer which attempts to categorize the detected event in to one of numerous categories (e.g. continuous wave, chirp, multilevel chirp, other wideband) and to extract the central features of the detected modulation. For example, when a chirp event is detected and classified, the total sweep range and sweep rate are also determined and noted. When the system is unable to determine a specific modulation type for the signal it will fall-back to generalized categorization including narrowband general, wideband general and baseline variation, the latter of which is an indication that anomalous power has been detected in band at or above the levels specified by the site operator, but that the event is either too weak, or too evenly spread over the band to be isolated. Once local event analysis has completed the collected package of raw IF data file, generated visualization pdfs, initial event report text file, event classifier results database file are collectively uploaded to centralized cloud storage. Data collected in the centralized cloud storage now totals nearly 20 TB of multi-band reference material making the ARFIDAAS database the largest known open access repository of raw GNSS RFI and jamming event data. The collection of this large volume of data sorted by site and date allows the production of detailed site report summaries, typically at time resolutions of one month or one year to allow characterization of the site RFI environment and to identify trends in the number and type of jamming devices encountered at each over time. By the end of the project in 2022 it is planned to provide site stakeholders and interested parties with monthly and annual reports for deployed stations as well as to allow machine learning based fingerprinting of detected jammers such that individual hardware devices can be recognized and their previous sightings over the whole catalogue of events can be reported.

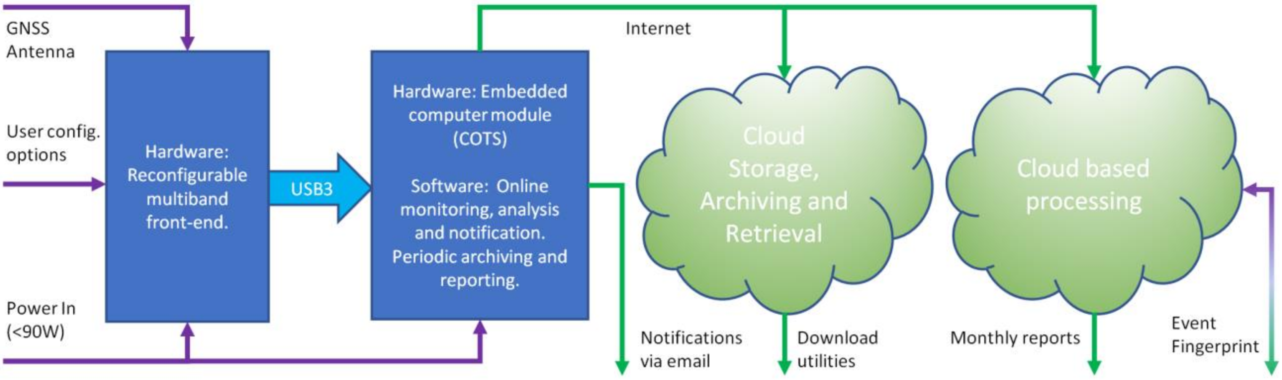

Fig. 2. ARFIDAAS high level functional diagram showing interfaces

THE DEPLOYED NETWORK

As of the writing of this paper there are eleven deployed ARFIDAAS monitoring stations throughout Scandinavia and Europe, with plans for an additional six units to be deployed within 2022 per Fig 3. The ARFIDAAS network is hosted primarily by cooperating research institutions and companies with active research or development projects utilizing GNSS signals. Typically, the ARFIDAAS system is connected to an existing GNSS multiband antenna via a signal splitter shared with receivers and equipment operated by the host. In order to support the use of dissimilar antennas and RF feed networks between the different host locations, the ARFIDAAS hardware front-end was designed to support a very wide signal power range, and to tolerate reverse biasing from DC injection on existing networks. Similarly, to allow the ARFIDAAS systems to integrate in to available installations several configurable aspects of the ARFIDAAS configuration software are used to suit the given site.

Fig. 3. The ARFIDAAS network (presently deployed systems in green, expected deployment sites in blue, and the number of systems indicated in brackets)

First, detection is based on deviation from a moving average power level rather than a static threshold of signal amplitude, which eliminates the need for calibration while also tolerating gain variation within the antenna and signal propagation network that can arise from temperature variation. Second, the centre frequencies, Intermediate Frequency (IF) bandwidths, and sampling rate parameters can each be adjusted to tailor the amount of captured spectrum to the signal bands and bandwidths supported by the connected antenna. Third, the system software allows for some masking of nuisance events either in terms of reporting, uploading, or both in cases where sites are found to suffer from the presence of a persistent yet unstable in power co-authorized user that would otherwise cause frequent nuisance detections. Fourth, the spectral shape of the 'environment baseline' is noted and deviations from this are used determine which region of the band is affected. If no substantial change in band shape is detected the event is considered to be an environment baseline event. Examples of sources that can cause such nuisance detections include Radio Detection And Ranging (RADAR) installations, amateur radio, amateur television, and malfunctioning Wi-Fi routers [2][3].

FULL YEAR DATASETS

For the remainder of this paper, we will focus on data from five of the sets within the overall network, specifically the three sites located in Trondheim (Norway), the Asker site (Norway), and the Amsterdam site (Netherlands). These sites are selected as they have been in continuous operation for over a year. The data from four of the five sites covers the calendar year 2020, while the Trondheim C site starts in April 2020 and runs through March 2021 as this latter site was not installed until March of 2020. As a design trade-off in the ARFIDAAS system between notification latency to site operators and fine-grained RFI event analysis, the classification and characteristic information presented below is formed in a separate processing step executed after notification emails have been sent, but before data is uploaded to centralized cloud storage. Information about each event's RFI modulation, bandwidth, centre frequency, power level and sweep rate where applicable is written in to an h5 database file [4], which is then uploaded to cloud storage along with the raw IF sample data and initial reporting documents previously emailed to site stakeholders. The reports below are formed using an aggregation of the full years-worth of h5 database files from each site.

TYPE DISTRIBUTIONS

When the event parameters are aggregated over whole year periods, site-specific RFI environment features become visible. In Fig. 4 and Fig 8. we can see that the Amsterdam site and the Trondheim C site respectively are dominated by Narrowband events such as continuous wave (CW) and Multi CW sources. In comparison, the Asker site in Fig. 5 experiences primarily wideband sources while Trondheim and Trondheim B in Fig. 6 and Fig. 7 respectively experience mostly time-modulated RFI sources.

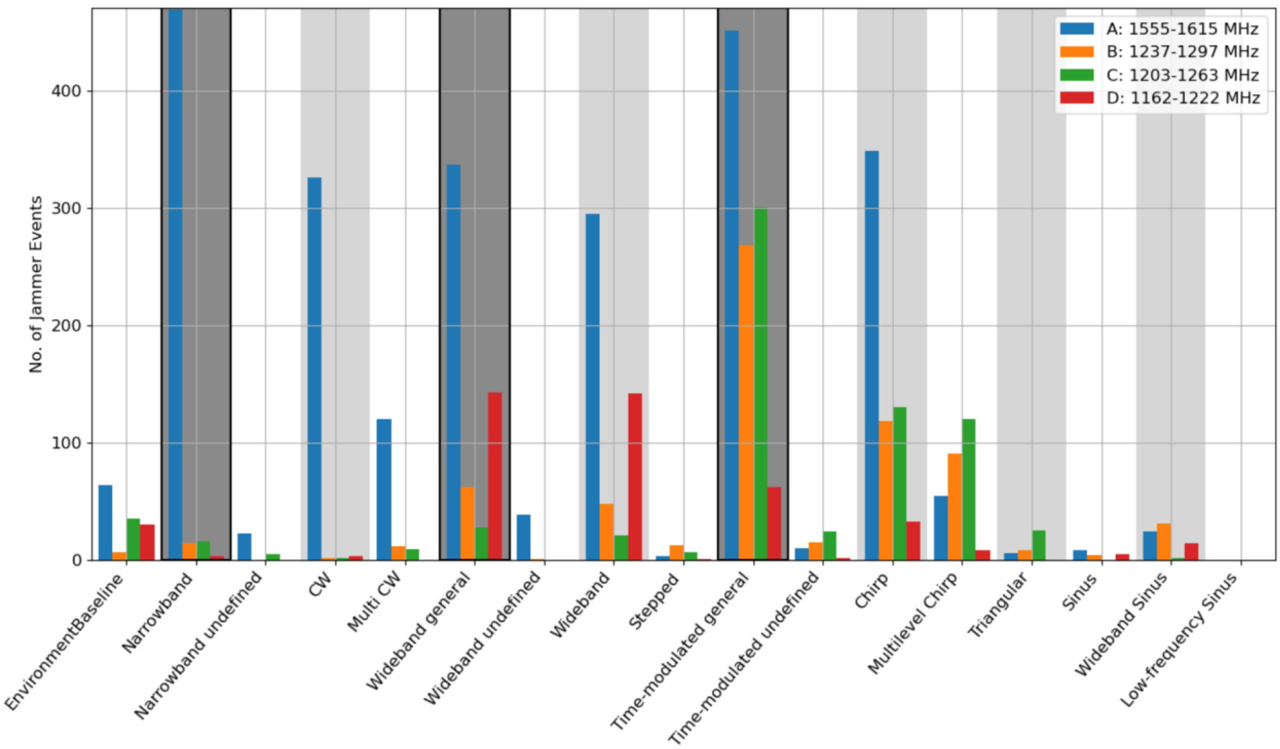

Fig. 4. Amsterdam, 2291 events from 1 January 2020 through 31 December 2020

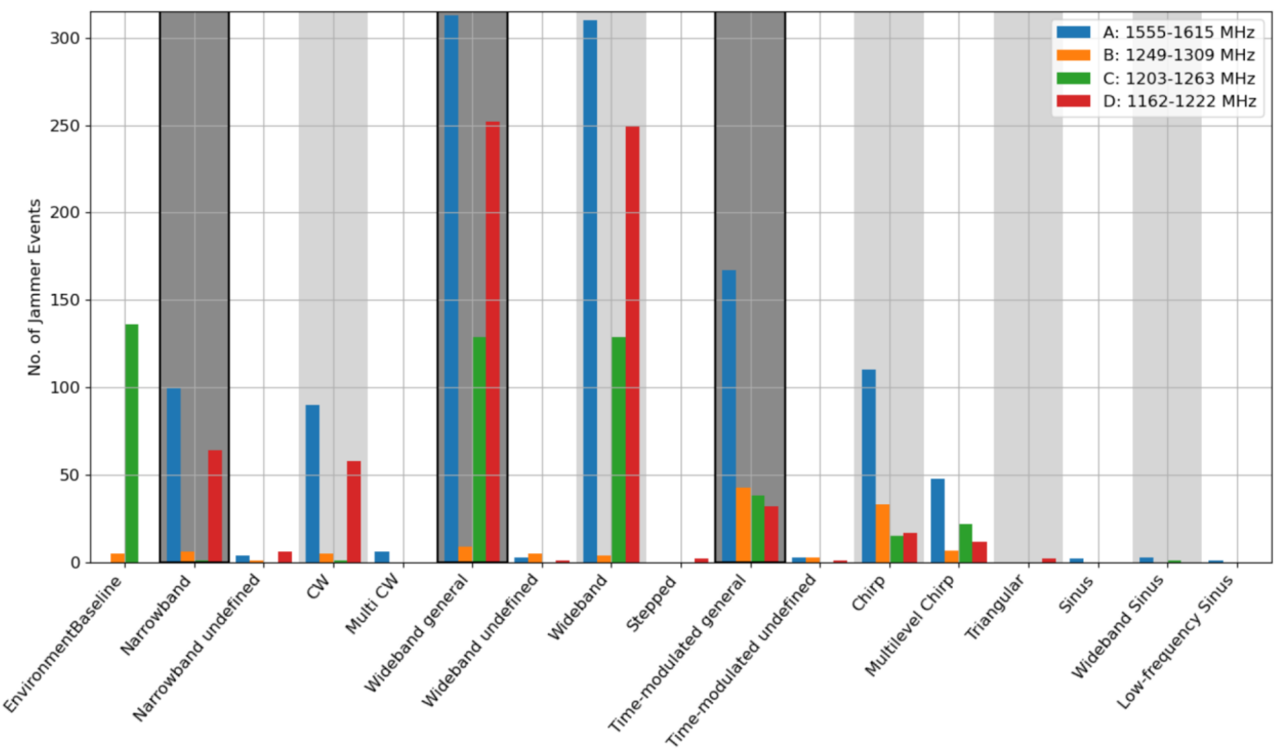

Fig. 5. Asker, 1295 events from 1 January 2020 through 31 December 2020

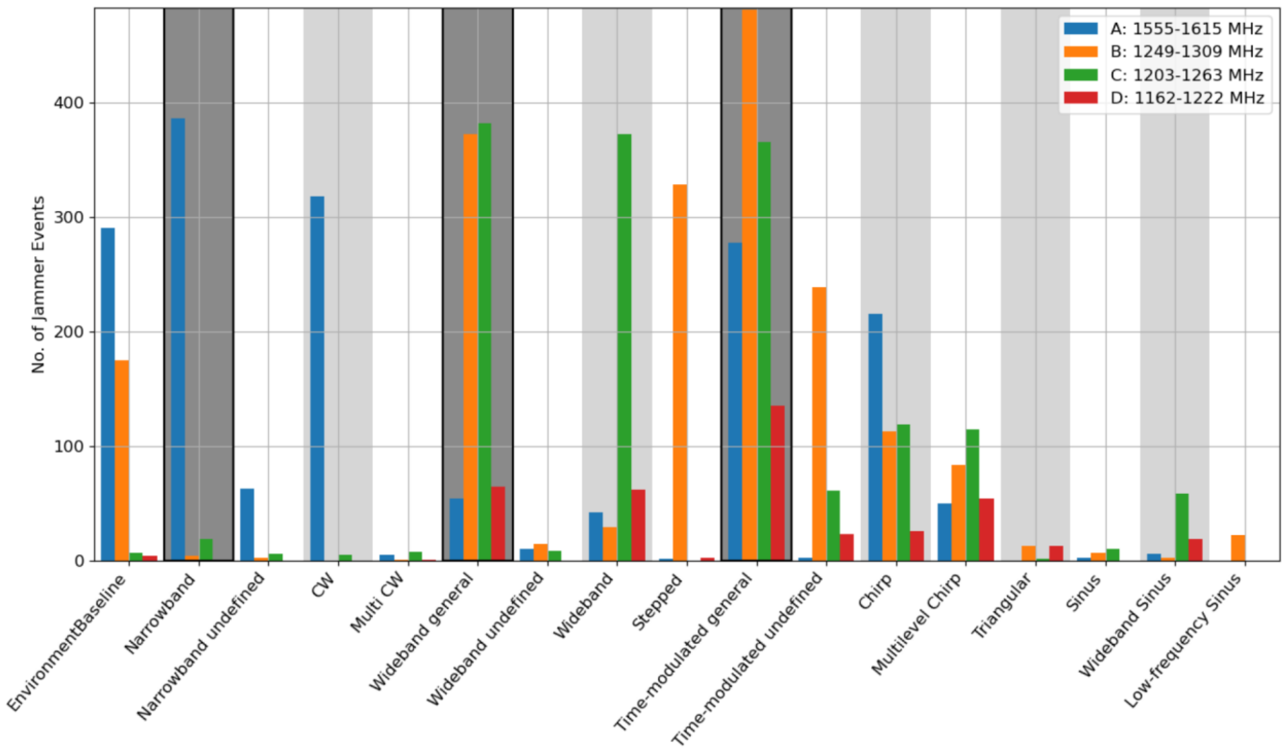

Fig. 6. Trondheim, 3021 events from 1 January 2020 through 31 December 2020

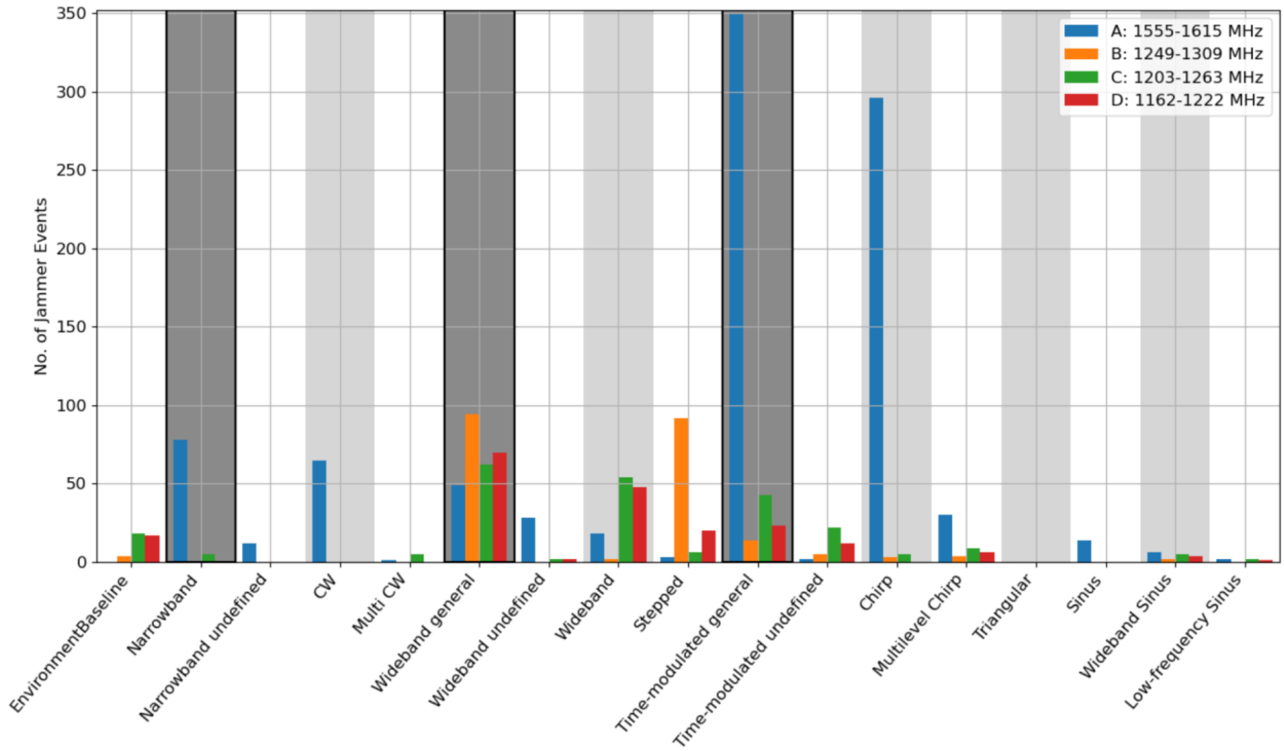

Fig. 7. Trondheim B, 827 events from 1 January 2020 through 31 December 2020

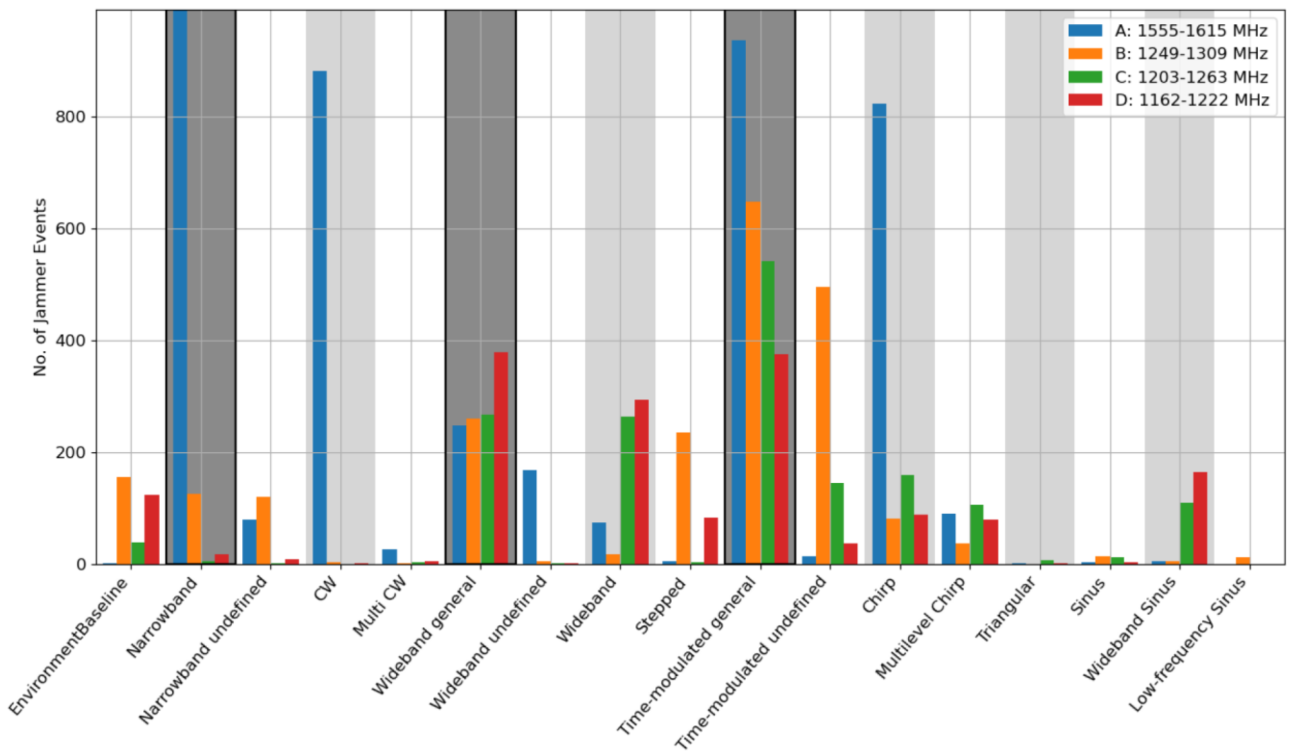

Fig. 8. Trondheim C, 5110 events from 1 April 2020 through 31 March 2021

When tabulating the site characteristics in Table 1, it is apparent that all of the sites except one experience tens of seconds per day of RFI on average, and that the E1/L1 band is typically the band that experiences the most interference. The exception to this latter point is that of site Trondheim which encountered E6 band RFI more frequently than the other bands. Despite being in the same city, Trondheim B and Trondheim C do not have unobstructed lines of sight to the RADAR station which is believed to be a substantial contributor to the E6 events noted at the Trondheim station.

Table 1. Site activity summary over full year

Site name	Number of events	Most impacted band	Likelihood of jamming at site		Dominant RFI family
Amsterdam	2291	E1/L1	0.025 %	22 s / day	Narrowband
Asker	1295	E1/L1	0.016 %	14 s / day	Wideband
Trondheim	3021	E6	0.024 %	21 s / day	Time-modulated
Trondheim B	827	E1/L1	0.009 %	8 s / day	Time-modulated
Trondheim C	5110	E1/L1	0.042 %	36 s / day	Narrowband

LESSONS LEARNED REGARDING SITE CHARACTERIZATION

One of the most interesting observations gathered from the full year datasets was that the relative likelihood of different GNSS carriers being impacted at a given station shows extreme variability even at the level of full-month observation periods, suggesting that for accurate site characterization a minimum measurement campaign of several months may be necessary. As shown in Fig.9 and Fig.10, when the data from one station was analysed to indicate the relative levels of RFI encountered on the E1 versus E5 carriers to help decide if E5 would be a suitable fallback when E1 encounters jamming, it was noticed that in July 2020 the occurrence rate of E5A jamming was actually higher than that of E1 jamming, despite the full-year occurrence rate of E1 being approximately 4.5x higher than that of E5A.

This observation implicitly raises the point that individual site statistics are heavily influenced by a small number of jamming devices which tend to revisit the site, which is conceptually consistent with vehicle borne personal privacy devices (PPDs) operated by individuals with daily routines, or the presence of fixed emission sources in range of the monitoring station. Even comparing sites within the same city such as Trondheim, Trondheim B, and Trondheim C do not show similar activity levels suggesting that RFI environments are very specific to a given location.

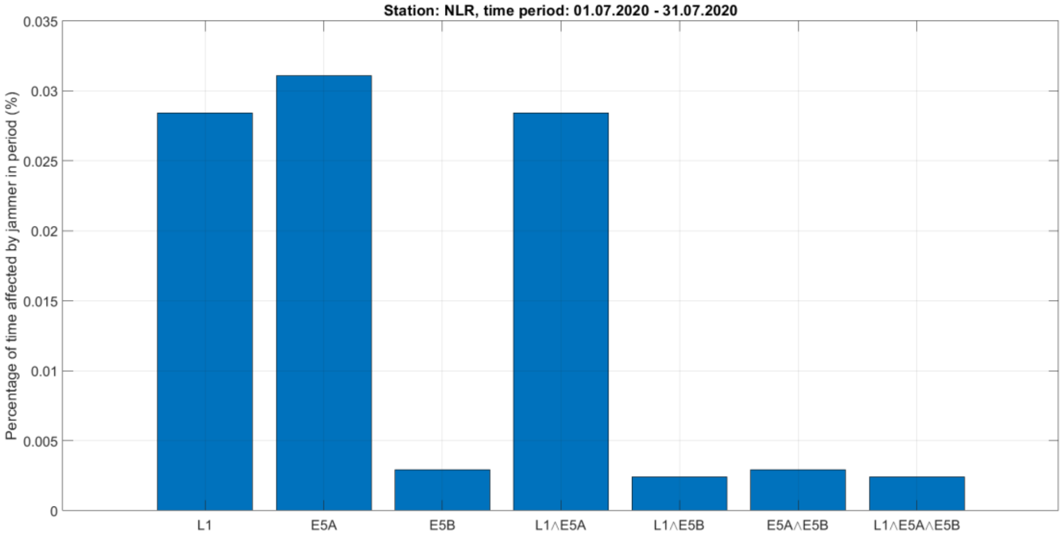

Fig. 9. Amsterdam site, E1 vs E5 likelihood comparison for July 2020

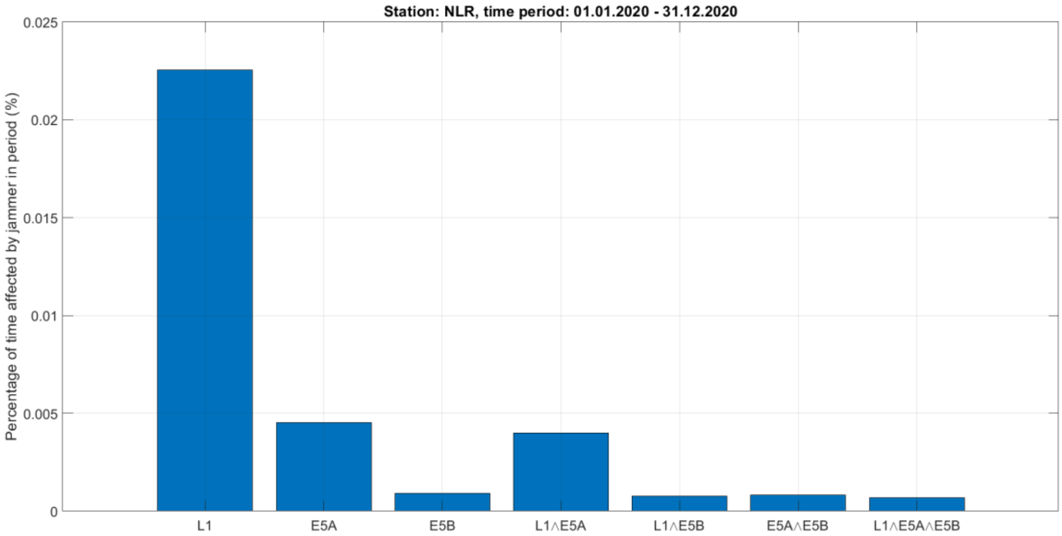

Fig. 10. Amsterdam site, E1 vs E5 likelihood comparison for calendar year 2020

SPECTRAL OCCUPANCY DISTRIBUTIONS

A secondary interesting observation was that for all of the five sites considered, the category of narrowband noise is dominated by activity within the E1/L1 bands of the monitoring stations with three of the five stations showing one or more orders of magnitude more activity on the E1/L1 band than the others. The current working theory of the authors for this disparity is that the vast majority of these narrowband detections are emissions from low-cost active E1/L1 GNSS receiver devices which have become self-resonant or otherwise leak energy in this band. When considering the distribution of narrowband (dot only) sources versus spectrum location in Fig.11, and the categorization in Fig. 8, we can see that the Trondheim C station observes vastly more narrowband RFI in the E1/L1 band than others. If this phenomenon were unrelated to the specific E1/L1 frequency band and were instead uniformly distributed over the L-band then we would expect to see approximately two times more events over the other three bands (with overlap taken in to account) than on E1/L1, but this is obviously not the case. While it is conceptually uncomfortable to consider that GNSS receivers may be a large source of GNSS RFI, this might also imply that as low-cost multi-frequency GNSS receivers proliferate that we should expect the prevalence of narrow-band RFI in each of the other bands to increase over time. We hope to test this assumption via future comparison with subsequent full-years of data to determine if there is a positive trend in narrowband RFI in the E5 band.

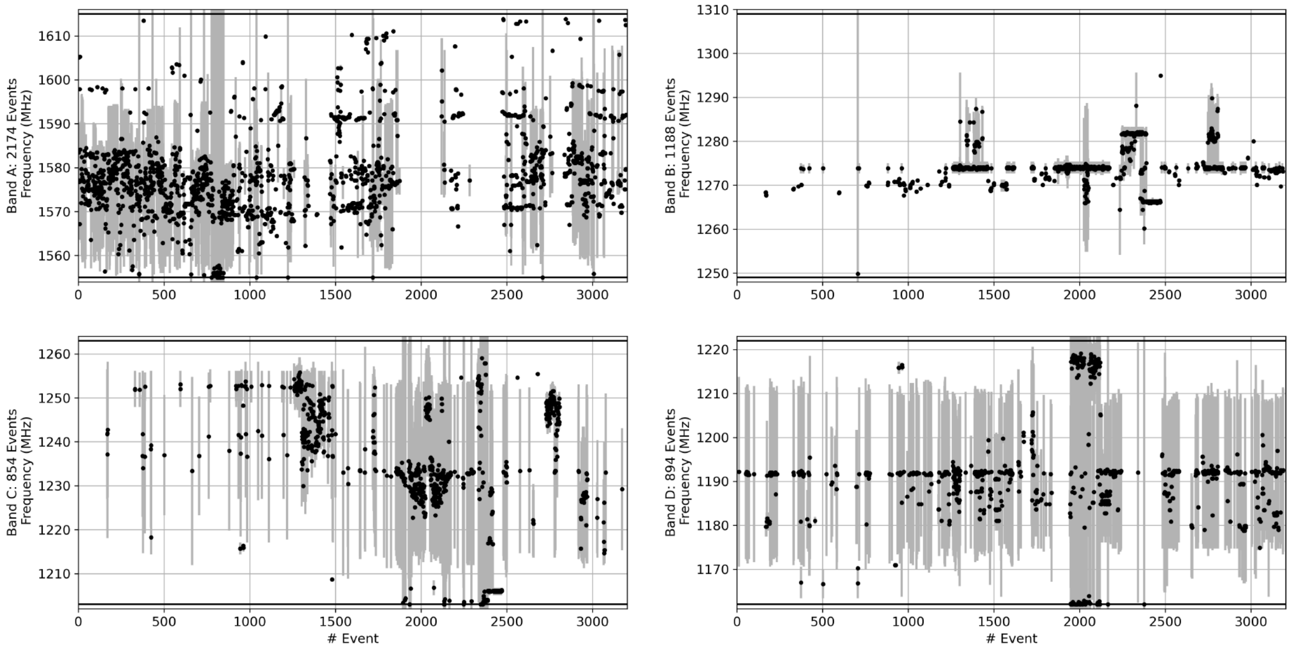

Fig. 11. Trondheim C site, event centre and span scatterplot 1 April 2020 through 31 March 2021

FUTURE WORK

In addition to revisiting the band occupancy of narrowband sources with future full year data sets, and the aforementioned attempt to use fingerprinting to identify individual jammers the authors are also considering future options to assist with RFI enforcement work. At present it is believed that traditional monitoring and reporting stations are too limited in terms of detection range to feasibly serve as a primary tool for apprehension of illegal jamming devices. While the fingerprinting techniques may allow prediction of user behaviour accurate enough to allow pre-positioning of enforcement teams, the authors are also considering alternative technologies for real-time long-range source localization.

DATA AVAILABILITY

The ARFIDAAS RFI library is available to interested research and corporate parties free of charge beyond the provision of storage media and/or payment for download bandwidth from the cloud storage solution. To obtain data access please contact one of the authors.

ACKNOWLEDGEMENTS

The authors would like to thank the hosts of the ARFIDAAS systems for their assistance.

REFERENCES

[1]. Morrison A., Sokolova N., Håkegård J. E., Bryne T. H. and L. Ruotsalainen, "A Multi-Site Quad-Band Radio Frequency Interference Monitoring Alerting and Reporting System," in proc. of the 2020 European Navigation Conference (ENC GNSS), 22-25 Nov. 2020, Dresden, Germany.

[2]. Morrison A., N. Sokolova, N. Gerrard, A. Rødningsby and C. Rost, "RFI Considerations for Utility of the Galileo E6 Signal," in proc. of the 34th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2021), 20-24 Sept. 2021, St. Louis, Missouri, US.

[3]. Nkom, "Varsel om vedtak med pålegg om retting," case 2108815-3, Trondheim, Norway, 17 December 2021.

[4]. The HDF Group, "HDF5 User's Guide", release 1.10 available at: https://support.hdfgroup.org/HDF5/doc/H5.intro.html, last accessed December 2021.