POLITECNICO
MILANO 1863

SCUOLA DI INGEGNERIA INDUSTRIALE
E DELL'INFORMAZIONE

Executive Summary of the Thesis

SDR-based automatic RF component analyzer

Laurea Magistrale in Telecommunication Engineering - Ingegneria delle Telecomunicazioni

Author: Alessandro Andrea Vogrig

Advisor: Prof. Matteo Oldoni

Academic year: 2024-2025

1. Introduction

In modern engineering education, particularly in the field of telecommunications, practical experience is fundamental. Yet, the high cost and fragility of RF instrumentation often limit hands-on experimentation. This thesis addresses that gap by developing an affordable, open-source platform for RF signal generation and analysis using software-defined radio (SDR) components. The goal is to demonstrate that such platform can enable meaningful RF measurements with minimal budget requirements, making RF experimentation accessible to students and hobbyists.

The motivation for this work stemmed from the author's personal experience with the challenges of hands-on experimentation of concepts studied in theoretical university courses. This difficulty is objectively confirmed by the limited access to measurement instruments for hobbyists, students, and educators, primarily due to economic constraints and accessibility limitations: high-quality spectrum analysers and signal generators are often cost-prohibitive and delicate, limiting hands-on experimentation and independent learning. This work addresses this challenge by offering a modular, extensible system with a bill of materials of approximately €150, less than a tenth of the cost of many entry-level commercial solutions.

2. Structure

The work was divided in different phases, through which a deep understanding and characterization of the hardware was acquired and software methods to correct hardware impairments and to perform measurements were written in Matlab language.

3. Software-Defined Radios

SDRs represent a paradigm shift in radio technology, moving a substantial part of the signal processing chain from dedicated hardware to flexible software. This software-centric approach offers significant flexibility and reconfigurability in system design, reducing the complexity of the RF chain. SDR architectures can vary, including direct-IF or heterodyne configurations, and can be monolithic (single IC) or less integrated. The core principle of SDRs is the digitization of the RF signal as early as possible in the receiver chain (via Analog-to-Digital Converters - ADCs) and conversion from digital to analog in the transmitter chain (via Digital-to-Analog Converters - DACs). The performance of these converters, particularly their number of bits, dy-

Figure 1: A device under testing connected to the system hardware.

namic range, and sampling frequency, is critical for signal quality and achievable bandwidth. As an example, higher resolution ADCs and DACs lead to reduced quantization error and improved dynamic range.[1]

4. Hardware framework

The choice of hardware for this project was primarily driven by affordability and resilience, possibly maintaining an open hardware design. The primary goal was to create an instrument as affordable as possible while maintaining characteristics similar to the ones offered by commercial products. The Analog Devices Adalm Pluto and the ANT SDR E200 were considered, both being full duplex SDR transceivers with comparable RF performance. However, because of the relatively high cost of these solutions, they were set aside. The chosen solution combines the open hardware HackRF SDR[2] as the signal generator and a Nooelec Nesdr Smart V5[3] as the receiver. The combined cost of these two devices is significantly less, approximately one-third, of the other options considered. A key advantage of this two-device approach is the system's resilience to damage, particularly important for inexperienced users. The HackRF, that is the more expensive transmitter module, is robust enough to withstand issues like unterminated ports or total power reflection. In contrast, the Nooelec RTL-SDR, the receiver side, is inexpensive (around €25) and easily replaceable in case of damages. This means that if a user inadvertently applies excessive power to the receiver, only the cheaper

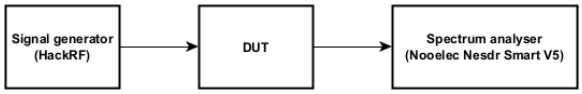

Figure 2: System intended connection diagram.

part needs replacement, avoiding the full system replacement cost that would be incurred with monolithic transceivers. One disadvantage of using two separate devices is that the receiver and transmitter operate under different, unsynchronized clock domains. However, this is not a significant limitation for the intended measurements, as generated and received signals can be frequency-aligned in software, and phase coherence is not a strict requirement for the types of analyses performed (e.g., vectorial signal analysis is not needed).

5. Receiver characterization

The Nooelec Nesdr Smart V5 was selected as the receiver device. It is based on the Realtek RTL2832U chipset, originally designed for DVB-T TV reception. A fundamental discovery in 2012 by researchers (including Steve Markgraf, Antti Palosaari, and others) revealed that the demodulator and decoding stages of the RTL2832U could be bypassed, allowing direct access to the Analog-to-Digital Converter (ADC) data via a USB interface. This breakthrough significantly reduced the cost of SDR devices[4].
The RTL2832U chip[5] functions as a low-IF or baseband ADC. The other critical component is the Rafael Micro R820T tuner IC[6], which includes a mixer, PLL, IF filtering, and gain adjustment circuitry. The Nooelec Nesdr incorporates a 28.8MHz temperature-compensated crystal oscillator that provides the clock for both the RTL2832U and R820T chips.
The RTL2832U's internal block diagram reveals a 7-bit ADC sampling at 28.8MHz. The device performs I/Q demodulation in the digital domain, minimizing I/Q imbalance issues. A resampler block downsamples the 28.8MHz ADC output to 2.4Msamples/s, averaging out noise and compensating for the modest ADC resolution, thereby improving the signal-to-noise ratio.
The MATLAB RTL-SDR Toolbox[7] exposes limited tunable parameters: tuned center frequency, sample rate, IF gain, and AGC enable.

The AGC cannot be used in this application as it would invalidate the calibrated power reading. Experimental characterization confirmed that a sampling rate of 2.4 Msamples/s provides the best performance, yielding a maximum instantaneous input bandwidth of 2.4 MHz. Higher sampling rates, above 2.4 Msamples/s, up to 3.2 Msamples/s, lead to instability, loss of responsivity, and require hard resets. Lower rates also exhibited a worse noise floor and higher spurious content.
The frequency response of the Nooelec SDR was extensively characterized using a Rohde & Schwarz SMA100B CW signal generator over the SDR's operational frequency range of 26MHz-1766MHz. The frequency response generally shows a relatively flat profile with a slow decay as frequency increases (approximately 10dB difference between 200MHz and 1600MHz). Slight oscillatory behavior, likely due to cable resonances or impedance mismatches, was observed but deemed negligible (approximately 1dB in amplitude). Sharp dips and jumps around 250MHz were attributed to reconfigurations of the RF filters within the tuner chip. An abrupt attenuation was observed at 1600MHz, which is expected given the R820T tuner's design limit of 1400MHz. Through experimental testing, an improvement in frequency response characteristics was observed by cooling the SDR with ice. Gain linearity tests, performed at different power levels, showed consistent frequency response curves, with slightly increased attenuation towards the higher frequency range as the gain is increased, nonetheless indicating acceptable linearity.
Using a Keysight N5227B vector network analyzer (VNA), it was possible to measure the S_{11} parameter, discovering a generally poor input matching and an unexpected impedance dependence from the tuner gain configuration, further justifying the variances found in the aforementioned tests.
As a final test, the input third-order intercept point (IIP_3) of the devices was checked: the results showed that before reaching any measurable nonlinearity in the analog chain, the ADC saturates.

6. Transmitter

HackRF One, an open-source Software-Defined Radio platform, was chosen as the signal generator due to its capabilities and cost-effectiveness. It operates as a half-duplex transceiver, meaning it cannot transmit and receive simultaneously using the same RF path.
HackRF One is developed by Great Scott Gadgets. It differs from monolithic SDR transceivers (like those using the Analog Devices AD9363) by employing a less integrated architecture, involving distinct stages for digital-to-analog conversion and RF modulation and upconversion, providing flexibility in signal generation. This design choice contributes to its affordability and robustness.
A new HackRF interface for MATLAB was developed and publicly released. This interface was specifically designed to overcome limitations found in existing, unmaintained community-developed libraries, thereby enabling other developers to more easily integrate the HackRF into their MATLAB code. This new interface simplifies the control and utilization of the HackRF for signal generation within the MATLAB environment.
The HackRF is capable of outputting signals with a wider bandwidth than the maximum acquired by the Nooelec RTL-SDR (2.4MHz). It was observed that, lacking the HackRF on samples interpolation, a high sampling rate should be used with the generated signal to properly exploit the DAC dynamics and minimize signal artifacts. Through experimental testing, it was determined that the maximum stable sampling rate achievable using the HackRF and MATLAB is 12.5Msamples/s.
The thesis focused also on the baseband filters included in the MAX2837 modulator chip[8], as proper baseband filtering has proven to be crucial for shaping the generated signal and minimizing unwanted spurious emissions.
During testing, a notable variation was observed in the performance of different HackRF units: one board, for instance, exhibited significantly higher intermodulation distortion and local oscillator leakage, which degraded the quality of the transmitted signal. These discrepancies likely stem from the use of substandard or out-of-spec components, which are sometimes used in unofficial builds found on Eastern

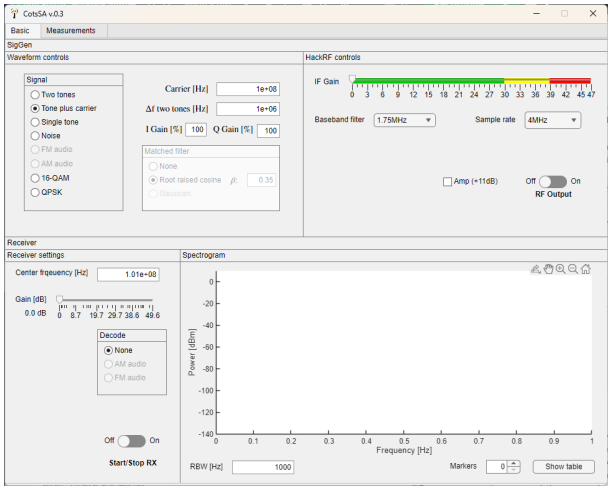

Figure 3: CotsA program interface.

markets to reduce cost. This underlines a key challenge when working with open hardware: while the design might be sound, the actual performance is only as good as the components used and the care taken in manufacturing.

7. Software

A key component of this project is the custom software developed in MATLAB, called CotsA (from "Component Off The Shelf Analyser"). The software is designed with a modular, object-oriented framework to allow users to easily add new functionalities[9]. It enables signal generation, data acquisition, power-corrected spectral analysis, and various analysis routines such as two-tone intermodulation tests[10], digital modulation analysis (e.g., 16-QAM and QPSK) and 1dB compression point automatic assessment.
As mentioned, a significant contribution of this thesis is the development of a new HackRF interface for MATLAB.
The developed software also includes scripts to control complex instruments like arbitrary waveform generators and continuous wave (CW) generators via the VISA interface. This code was used as a base for a quick-start guide for future users of the instruments.
The software prioritizes ease of use, utilizing readily available MATLAB toolboxes while maintaining a compatibility towards free languages like Python. To overcome limitations of the MATLAB, several workarounds were put in place. All design files and code are released as open source on a public GitHub repository, encouraging further adoption and development.

8. Conclusions and future developments

The system was tested using a component with known characteristics, the Qorvo TQP369184 amplifier, to compare the obtained results against the manufacturer datasheet. The system showed promising results: it measured an amplifier gain of 21 dB, only 0.8 dB off the datasheet's declared value; a P_{1dB} of 15.5 dBm, which matches the manufacturer's stated 16 dBm; and an IIP3 of 23 dBm, just 2.5 dB off the specified value.
The thesis successfully demonstrated the feasibility of using low-cost, off-the-shelf SDR hardware to create an effective and affordable platform for RF component analysis. The in-depth characterization of the selected SDRs provides valuable insights into their performance and limitations, paving the way for powerful RF measurements in budget-constrained environments. The developed modular software further enhances the utility of the system, offering a flexible and expandable tool for signal analysis and testing.
Future improvements of this work should focus on addressing the instabilities observed at the edges of the receiver's frequency range, further optimizing the software for performance, adding support for additional SDR platforms, such as Adalm Pluto, and extending the available measurement suite[11]. The open-source nature of the project encourages community contributions and further development, ensuring its continued evolution and wider applicability.

References

[1] M.N.O. Sadiku and C.M. Akujuobi. Software-defined radio: a brief overview. *IEEE Potentials*, 23(4):14–15, 2004.

[2] Michael Ossmann. The hackrf one project.

[3] Nooelec. *NESDR SMArt RTL-SDR v5 Datasheet - Revision 1*. Nooelec, 4-2045 Niagara Falls Blvd, Wheatfield, NY, USA, 1 edition, 10 2022.

[4] The Osmocom project. The rtl-sdr project, 2025.

[5] Realtek Semiconductor Corp. *RTL2832U DVB-T COFDM Demodulator+USB2.0 datasheet*. Realtek Semiconductor Corp., Taiwan, 1.4 edition, 11 2010.

[6] Rafael Microelectronics inc. *R820T High Performance Low Power Advanced Digital TV Silicon Tuner Datasheet*. Rafael Microelectronics inc., Taiwan, 10 2011.

[7] The MathWorks Inc. Rtl-sdr support from communications toolbox, 2025.

[8] Maxim Integrated. *MAX2837 2.3GHz to 2.7GHz Wireless Broadband RF Transceiver Datasheet*. Analog Devices, Sunnyvale, California, USA, 2015.

[9] Erich Gamma, Richard Helm, Ralph Johnson, and John Vlissides. *Design Patterns: Elements of Reusable Object-Oriented Software*. Addison-Wesley, 1994.

[10] Ken Kundert. Accurate and rapid measurement of ip2 and ip3. *The Designer's Guide Community*, 13, 2002.

[11] DL2ALF, DL8AAU, and DF9IC. Canfi, (c)heap (a)utomatic (n)oise (f)igure (i)ndicator with dvb-t stick, 12 2015.