SPECTRUMSENS

Detection, analysis, monitoring and action

CIBERTECCH companies

External and internal protection (RF - Data intelligence)

Jordi Garcia Castillón – info@jordigarcia.eu – Tel. (+34) 636714253

Summary

Development of a spectrum analyser thought especially for the business area (although it can be for domestic use) whose objective is to perform the permanent monitoring of the RF spectrum environment of the client to be informed and, if it is necessary, to protect potential interferences by malicious cybernetic attacks of its wireless environment.

The device will carry out a constant modular monitoring (usually within a range that will be between 30 kHz and 30 GHz, range and bands which could be defined according to the geographical environment where the device is used).

The main objective will be to carry out the pattern designing of the usual performance, especially in the spectrum bands that can have a direct impact on the performance of the devices and mechanisms of the wireless environment to be protected.

The main bands to be protected will be all those which are related to the devices that can work within the range of the ISM bands, bands for RFID uses, Wi-Fi bands, band for bluetooth uses and all those bands assigned to the mobile phone uses of usual use, among others.

In the case of detecting defects in the analysed spectrum, the device will be able to send a signal indicating the defect to be analysed. From this point on, the system will be scalable being able to incorporate the following:

- A system of registered data delivery to an external application or even to an application specifically designed for each client for the exclusive monitoring use.

- A system of answer by sending a far-reaching signal when it is potentially anomalous it tries to neutralize its effects (only active in those jurisdictions where this functionality is completely legal). In the case of those environments where the functionality is not legal it could be carried out an automation *shutdown* of all the devices which are working in the affected frequencies.

- A business layer given to the client which monitors for him/her its RF spectrum in 24 x 7 x 365 mode and, in case of any defect, it will warn the client and will act if it is necessary

All the aforementioned will be accompanied by an integral service layer which will include:

- Business in service layer (training, audit, implementations, alarm monitoring central of events and management of them, etc.)

- Business in personalised developments (IoT hardware, control software, etc.).

And with the optional parallel but integrated development of a platform of data intelligence based on the accumulation and analysis of data individualised for each client according to its security events (the RF environment and others) of the devices which result in an “IntelligenSys” platform self-managed by the client or managed externally as a service layer.

Here there is a summary of the solution offered to the recipient users indicate the following:

- Doubled-level security dome: internal and external

- Homogeneous base with high capacity of customization

- Multi-paradigm solution: hardware and software

- The base of the standardised hardware can be considered, as far as possible, as an open source for its constant investigation and development and, from this point, resulting in the associated services and the closed modular and personalised projects

TECHNICAL DEVELOPMENT

Technical development on which the whole modular development will be structured

SUMMARY

The general purpose of this development is to set the open base of a system that, subsequently, it could be modulated according to the specific needs of each user and adapting the frequency range or of frequencies to each specific area, as well as it specific development.

From this open base it can be developed a community, as well as a research and development system which results in a joint benefit for the general RF environment and that give specific solutions to specific cases and situations.

In this case, as an introductory example, it will work with a unique 700 MHz frequency and in a system that can work independently (*standalone* mode) and, from that base, it can be introduced layers of connected integration, as well as precision and specific development elements.

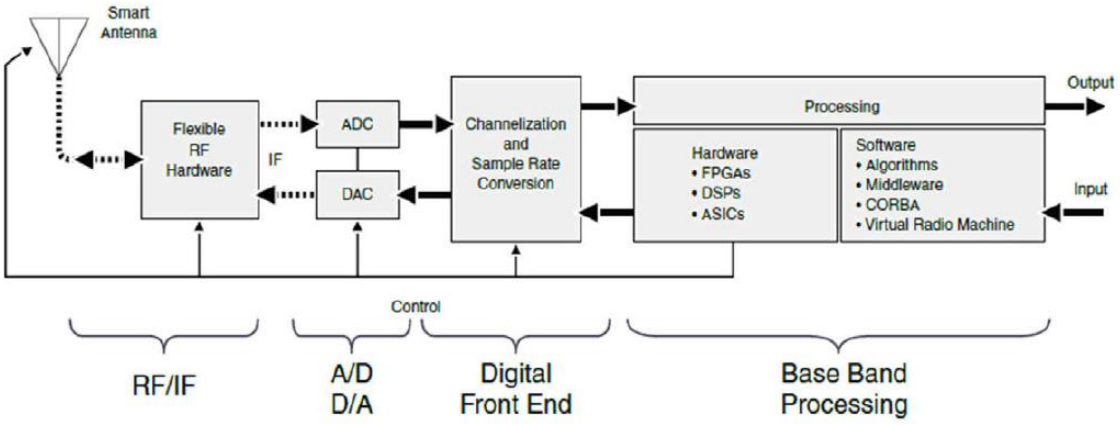
The objective of the development of the base is to establish it on open systems such as the microcontrollers / microprocessors as ARDUINO or RASPBERRY to mention two examples.

Although there are different possible options (in the same way that there are different possibilities of subsequent connectivity to the display or warning platforms, as well as the networks: SIGFOX, LORA, etc.), in this case, it is specifically chosen Raspberry Pi, not only due to its low cost of development but also due to its capacity to work with a SDR system with an RTL-SDR receptor.

The base system (in general applied to the whole “IoT environment” and “classic ISM”) allows to obtain an autonomous system which is capable of detecting unwanted transmissions which are in the IEEE 802.11g/b/n/ac standard. In this case, due to the own restrictions of the used system, the frequency band that can be used will be those which are between 26 and 1766 MHz, but this base allows that you can work can by setting slight variations on any other band/s spectrum.

SDR (SOFTWARE-DEFINED RADIO)

One of the larger pillar of the base is the Software-Defined Radio (SDR) and we must understand it for this case according to its general outline:



Conceptually, we can say that a SDR has an RF section (antenna, filters, amplifiers, etc.), an ADC (analogue signal to digital signal converter) or a DAC (digital signal to analogue signal converter) and a *digital front end*.

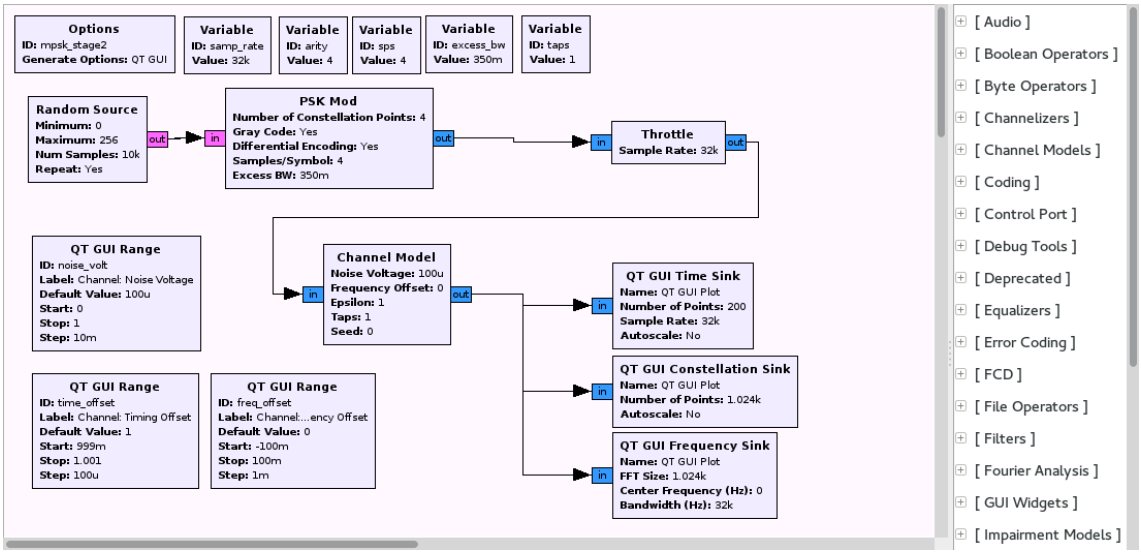
An SDR system offers clear advantages as they are the simplification of the development of processes of applications, as it allows to do it through code lines without having to perform physical modifications to the hardware. It also allows a flexible system when it is necessary to modify it. At the same time, it is easy to update and its cost is not high.

One of the essential aspects of the functioning of the SDR is in the conversion phase of the digital signal to analogue signal. This stage will be determining because the limits of the bandwidth that the system will have are set from it and that will be based on the popularly known as Nyquist Theorem.

In such theorem it is established the condition that must be fulfilled in the signal sampling so that such signal can be recovered without any loss:

$$f_s > 2 * f_{max} = 2 * B$$

To control a radio system and to perform the signal processing it will be used the GNU radio software based on blocks. Here you can see a graphic representation:

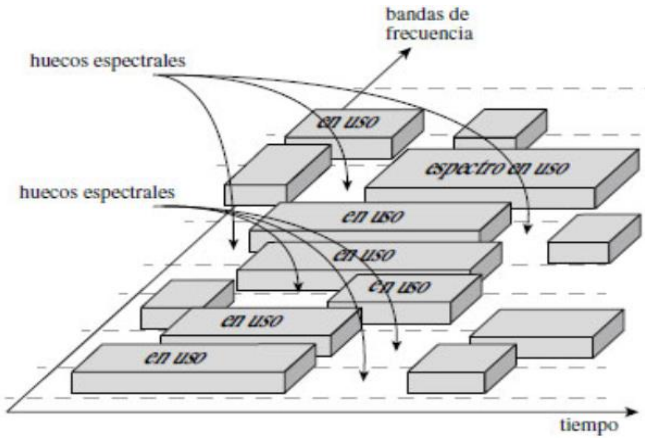


Nowadays it can be said that the SDR systems have a high level of implementation in business and also in military area. The applications can be different, its development and use are in currently expanding, the development of low cost solutions listed in this text contribute to expand it and they can reach all the levels of the society for its use (reducing the "*commoditization*" by means of the service layer, layer that guarantees the specificity and the constant evolution of the business attached to it).

The expansion of the SDR systems and its evolution must be taken to work in the reach and development of higher layers of active response. Among these layers it can be found the action of "attack against attack" (like the one which is set in this system when the legislation allows it), but a less "aggressive" option is in the cognitive radio, as it want and allows to avoid mostly the intentional aggression systems or interferences and situations of saturation or general collapse.

The cognitive radio does not have the function to neutralise an attack launching another attack, but which wants to avoid the attack by means of a tactical movement to other non-attacked, interfered or busy frequencies. In fact, we could face a situation where all the frequencies are being attacked, in that case, the best thing would be (provided that the legislation of the place allows it) a hybrid solution which will be implementation combined with a system of cognitive radio with a *jamming* system intended to perform functions of *anti-jamming, a shutdown or a solid global "caged"*.

Here you can see a graphic example of a system of cognitive radio scheme:



Graphic:

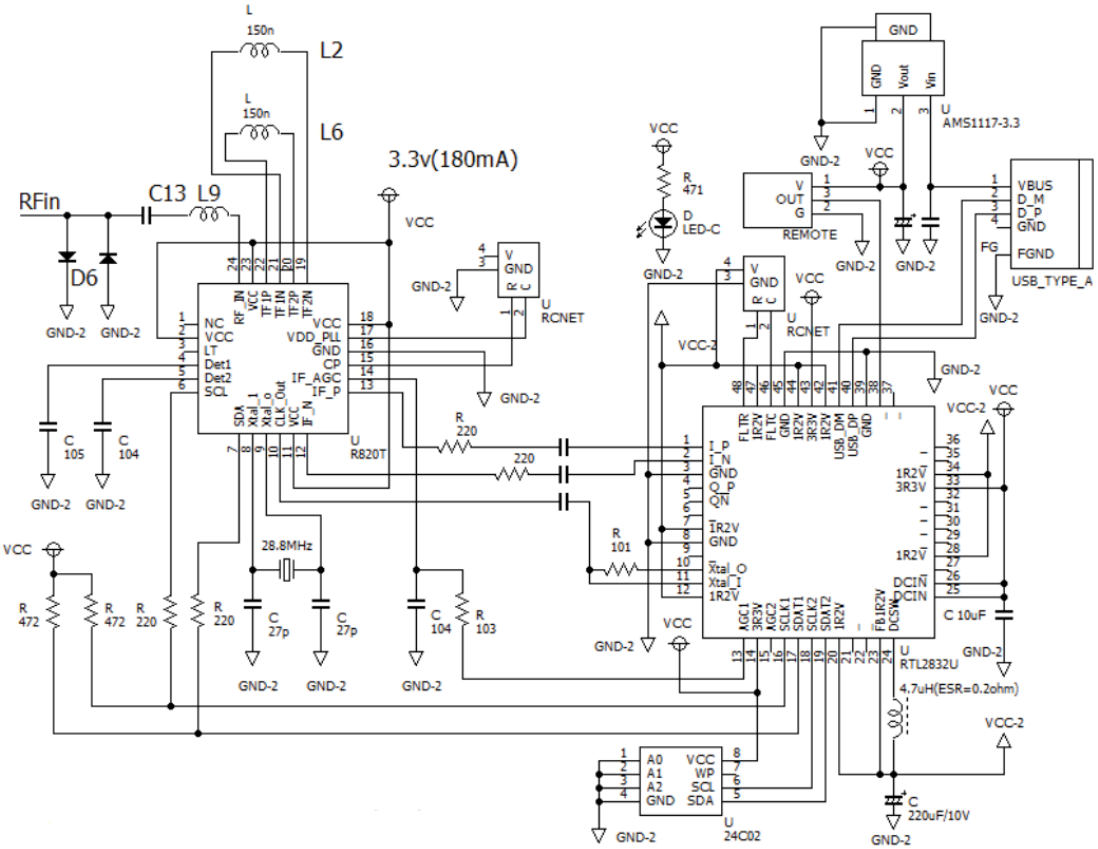
Huecos espectrales: Spectral spaces

Bandas de frecuencia: frequency bands

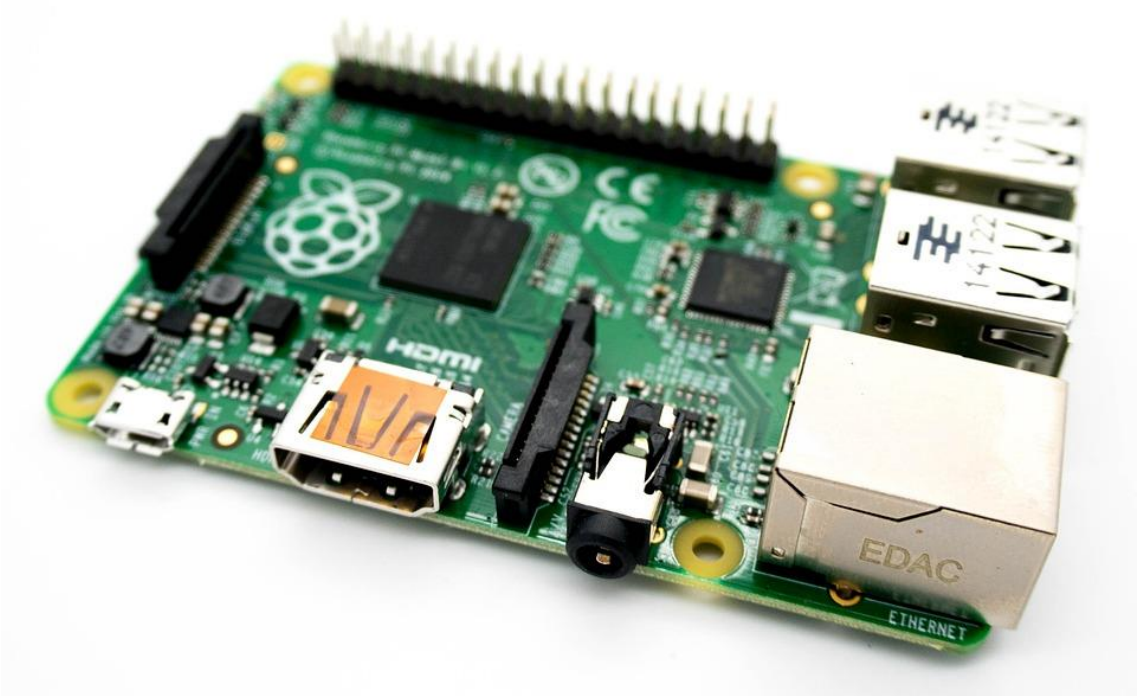
En uso: in use

Espectro en uso: spectrum in use

And all of that starting from an RTL-SDR electrical general scheme:



For this base development, as it was aforementioned a Raspberry Pi will control the RTL-SDR receptor and will perform the signal processing which will be received. It concretely will be the 3 model version B):



These are some of the main technical specifications of this version and model:

Processor:

Chipset Broadcom BCM2387

1.2 GHz of four ARM Cortex-A53 cores

GPU:

Dual Core VideoCore IV ® Multimedia CoProcessor. Gives Open GL ES 2.0, hardware-accelerated OpenVG and 1080p30 H.264 high profile decoding

1 Gpixel / s, 1.5Gtexel / s or 24 GFLOPs with texture filtering and the DMA infrastructure

RAM:

1GB LPDDR2

Connectivity:

Ethernet socket Ethernet 10/100 BaseT

802.11 b / g / n wireless LAN and Bluetooth 4.1 (Classic Bluetooth and LE)

Video output

HDMI rev 1.3 and 1.4

RCA composite (PAL and NTSC)

Audio output

Audio output 3.5 mm jack

USB 4 x USB 2.0 Connector

GPIO Connector

2.54 mm 40-plugs (100 thousand inch) of expansion: 2x20 strip

Provide 27 GPIO pins, as well as 3.3 V, +5 V and GND supply lines

Camera Connector of 15 pins MIPI Camera Serial Interface (CSI-2)

Display screen. Connector of the Display Serial Interface (DSI). Connector of 15 lines flat Flex cable with two data lines and a clock lane

Slot of memory card “push/pull” microSD

The system which will be used for this base development will be the S.O Raspbian Jessie Lite. This operative system has its base on Linux Debian. In this case, it will not have a graphic interface and it will be directly executed on a microSD card without the need of a hard disk.

Always referring to the base development, this will be performed by means of the activation of the SSH server to create a tunnel for the remote management from another computer.

To perform the testing phase and filtering for the observation of the area of the spectrum which will be constantly analysed and in real time it will be used SIMULINK / MATLAB.

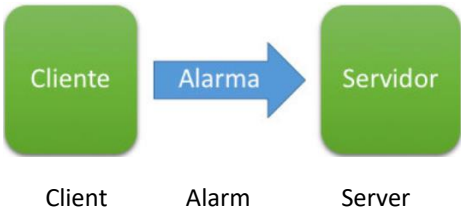
The main programming here considered is performed in C. All of this through the packing with CMake.

It will be used the “rtl-sdr.c” programmes by Osmocom and also the “rtl_power” programme also programmed in C. The first one will result adapted and the second will be in charged to perform the measuring of spectrum bandwidth.

Although there some several different options to use in the sending and display of the warnings que which can occur (and in each specific the best one will be able to be analysed for each specific situation) in this base development it will be performed by means of the Node.js *framework*.

Specifically, it will developed a client application which will be executed on the Raspberry Pi connected to a network and a small server into a host with has Internet connection and that has a fixed IP.

The connection between the client and the server will be performed by means of the use of a TCP socket. A brief summary of the architecture of this network layer would be as the following:



VALIDATION ENVIRONMENTS

To validate the application of this base system it must to be mentioned the example in 2 different situations, with some specific features regarding the RF reception signals se and which answer to 2 common situations for all the companies, matters, etc.:

A) Environment 1: device working in a “semitransparent” environment. This is in a space or external element or in any building with a light cover but which allow the input and output of the RF signals with a good signal level. In this case, common in most of the offices, industrial buildings, homes, etc.

B) Environment 2: device working in a “dull” environment. This is in a building with structural elements which do not completely the connectivity but which reduce it to the maximum, in hidden environments, etc.

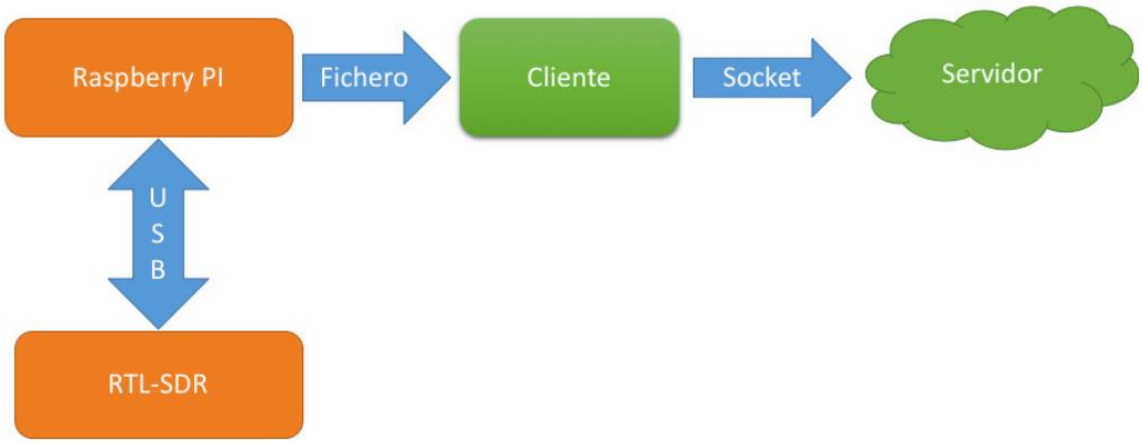
In both cases:

1- The monitoring will be constantly performed on the 700 MHz band and it be carried out the verification of the alarm emission.

2- The device works independently by an external battery.

3- The aim of the device is to receive the signal or signals (this would be extensible to all the frequency ranges you want) which are being sent between a within range, to monitor it/them and send warning signals when the existing emissions change the power according to some indicated percentage parameters or when they receive new emissions within the range (being able to set exclusion bands with the purpose of avoiding false positives). The system can use the automatic learning to “learn” and “evolve” by themselves about the signals of the regular environment which will be in charge to analyse it along its useful life.

Global scheme of the hardware-based system:



Graphic:

Fichero: file

Cliente: client

Servidor: server