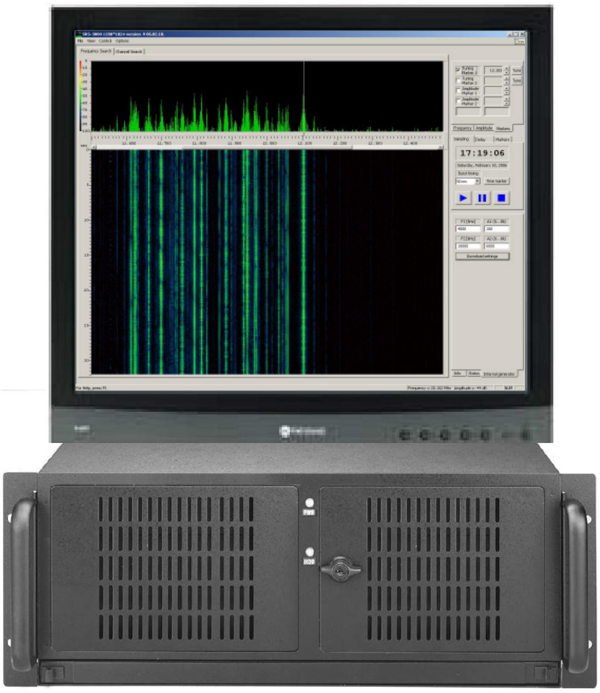
Spectrum Scanning Principles



CONTENT

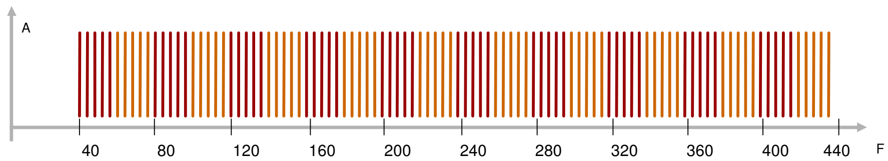
Introduction

In modern spectrum search and monitoring missions is one of most required task to provide up to date spectrum estimation about what is going in the air. The higher level system components have to control other monitoring or jamming parts of the SIGINT/COMINT/EW components of the system based on that spectrum information. In the case of communication system a cognitive radio should have relevant information about spectrum occupancy to organize its own communication to the useable part of the spectrum. In the following parts of this document we describe some basic principles of spectrum scanning which process is used to collect information about the spectrum.

Scanning requirements

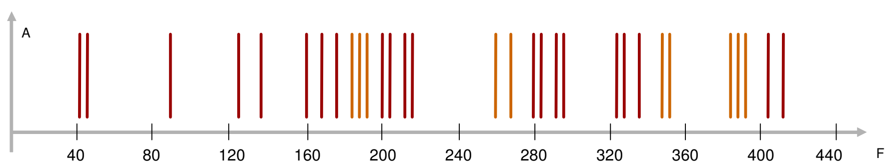
Search scanning

In the case of search or band scanning we have complete frequency band defined with its start and stop frequency or center and span frequency. The task of the scanning receiver in this mode is the scanning the band continuously with a given resolution and report the power level estimation in the resolution bandwidth. If partial bands of the receiver input frequency range is defined the task could be derivated to some band scanning tasks.



Random scanning

In random or memory scanning mode the receiver has to scan a given frequency list defined in any memory store resource of the receiver system. In this case the frequency values could be spread out randomly in the reception band of the receiver. The task of the receiver is visit all of the frequency value given in the memory list and report the reception level at the particular frequency in the defined receiving bandwidth.



Definition of scanning speed

For search scanning

In search scanning mode the receiver is span trough a defined frequency band, so it is possible to define that how much time is required for span trough this frequency band. The scanning speed could be expressed in Frequency/Time format and usually normalized to 1sec to be comparable to others.
However as we will see later, for exact definition we need to define the resolution of the power estimation of the frequency band the receiver is developed. So the exact definition of the scanning speed is Frequency band spanned/Time required @ Frequency resolution.

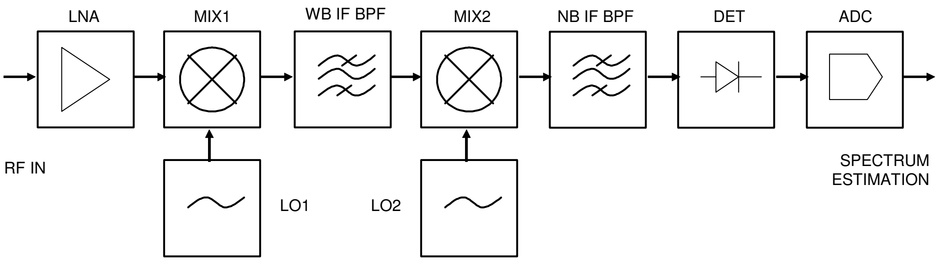
For random scanning

In the random scanning mode of operation the frequency band which should be covered is not a continuous band, instead of the frequencies spread out randomly. In that case it is more useful to define the time which is required to implement one power level measurement at a given frequency in the reception band of the receiver.
In practical reasons it is used to define the number of channels could be measured during a given time period which should be normalized to 1sec again for comparability reasons. So the definition is Number of channels measured / Time required.
As we can determine the total number of channels in search scanning mode too as the span bandwidth divided by the resolution bandwidth, we are able to express speed of the search receivers in Number of channels / Time format. In that case the resolution bandwidth is under taking into account in the calculation.

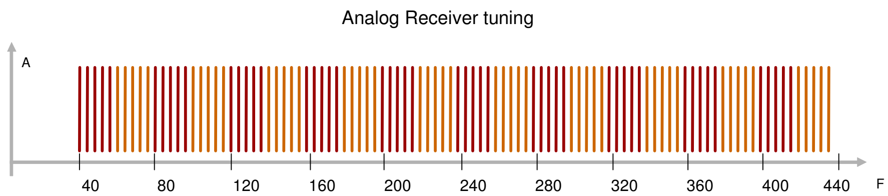
Implementation of scanning receivers

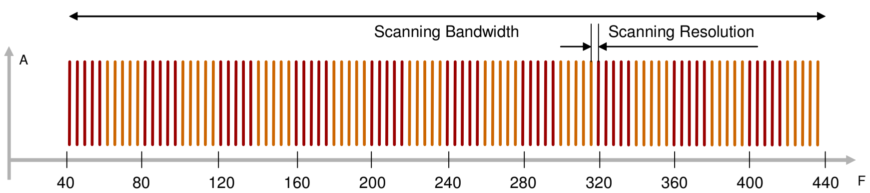
Tuned receiver implementation

The traditional way for implementing a scanning receiver is using a digitally controllable receiver to tune the required frequency value and measure the RF level on that frequency. As we use a traditional analog receiver processing the receiver is based two or more heterodyne frequency conversion and filtering. The final resolution bandwidth is determined by the last narrow-band IF filter.



The final IF filter is followed by a power detector and its signal is digitized by an analog to digital converter and reported to the higher level systems.
To perform a search scanning with this kind of receivers we have to select the IF bandwidth as the resolution is required and we have to tune the receiver to every individual frequency in the search bandwidth.



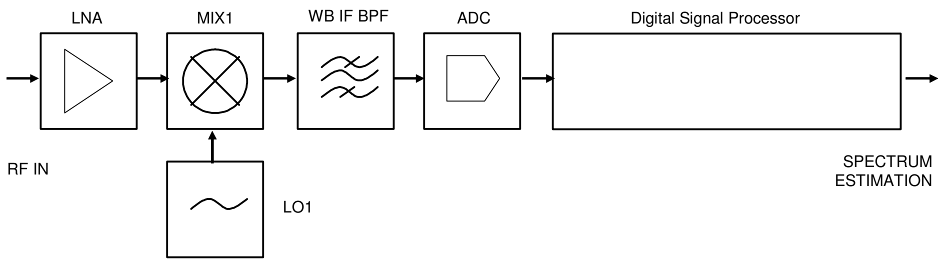


Spectrum estimation

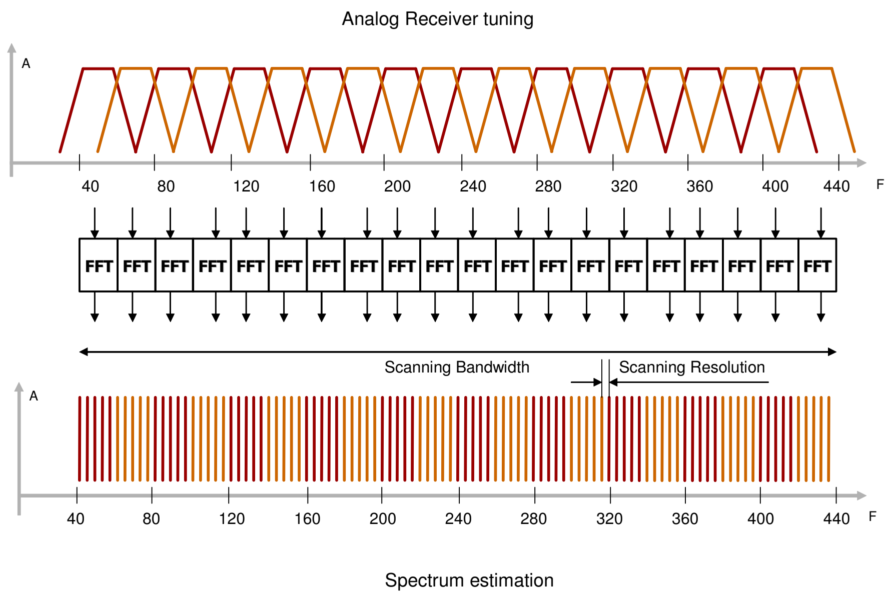
The scan speed is limited by the tuning speed of the local synthesizers, the transient time of the narrowband IF filter and conversion speed of the ADC.

Digital receiver implementation

In digital receivers usually the incoming RF or the wide-band IF signal is digitized and the final bandwidth of the receiver is given by the digitally implemented filter. AS the signal already is represented in digitally the final power estimation of the given frequency components is available in digital form.



To perform the scanning with this kind of receivers we have to tune the analog front-end to the required frequency band, sample the spectrum with the wide-band analog to digital converter, calculate the power level of each frequency component and present them to the higher level system components.



In that case the frequency tinning of the analog receiver front-end is required less time. On the other hand the frequency resolution of the tuning components (local oscillators) of the receiver could be higher. As the frequency tuning speed of a phase locked loop (PLL) based local oscillator is inverse proportional with the frequency step the tuning speed of wide-bandwidth, high-step local oscillator is higher than the low-bandwidth fine tuning PLL based local oscillators of the tuned receiver implementation. The power spectrum estimation could be done with fine-tuned, high-speed algorithms with dedicated hardware support on general propose processor (GPP) or digital signal processor (DSP). In that way we win the time for narrow-band filter transient and AD conversion time too.
That is why the wide-band digitally implemented receiver can reach significantly higher scan speed than the tuned receiver version.

Search scanning example

Problem definition

Let us define a simple example for EW/SIGINT operations like the following. We have to search the VHF band from 40MHz to 440MHz with 25KHz channel resolution as this a common channel spacing in that frequency band.
This task means 400MHz full span bandwidth, and based on the 25KHz resolution the total number of channels are: 400MHz/0.025MHz=16000.

Tuned receiver results

The commercially available low-grade receivers do not offer more than 40channels/sec scan speed. [1], [2] Using such kind of receiver the total time to require to scan this band is 16000ch/40ch/sec=400sec. Based on that value the scanning speed is 400MHz/400sec=1MHz/sec@25KHz resolution.
In the market we can fine professional-grade high speed scanning receivers based on advanced, combined architecture with up to 1000channels/sec scan speed. [3] With this kind of receiver we need 16000ch/1000ch/sec=16sec to scan the full frequency band. It means scanning speed of 400MHz/16sec=25MHz/sec@25KHz resolution.

Digital receiver results

If we use advanced digital receiver architecture with 20MHz of instantaneous bandwidth and 1ms synthesizer tuning time for the local oscillators of the font-end tuner [4] we are able to reach the following results.
To cover the full 400MHz span the analog front-end tuner should be tuned to 400MHz/20MHz=20 times which means 20ms full scan time for the receiver. To generate the 25KHz resolution in the 20MHz bandwidth we need to perform 20MHz/0.025MHz=800points FFT which takes less than 100microseconds for the Intel Pentium 4 GPP. [5] As we see the speed is limited by the tuning speed of the analog front-end. But the scanning speed is 400MHz/20ms=0.4GHz/0.02sec=20GHz/sec@25KHz resolution. Calculating back this value to channels it means 16000channel/0.02sec=800000channels/sec equivalent scanning speed.

Memory scanning example

Problem definition

Let use the assumption that we have 100 different hot frequencies stored in the memory channel store in the receiver. The frequencies randomly placed in the 40MHz to 440MHz VHF range.

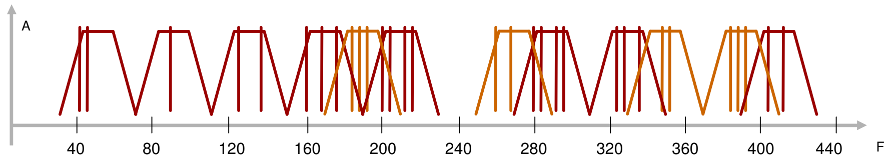
Tuned receiver results

Based on the receiver parameters used above we could calculate that a commercial low-grade tuned receiver is able to scan these 100 channel during 100channles/40channel/sec=2.5sec.

The professional-grade tuner receiver spent 100channles/1000channel/sec=0.1sec with this task.

Digital receiver results

In the case of using wide-band digital receiver first we have to determine that which bands should be captured based on the frequency list.



After that we have to calculate the power spectrum estimation for that frequency bands, find the signal value for the channel frequencies stored by the channel memory and report it to the higher system level. As we did not defined the exact frequency values let use the worst case situation that we have at least one channel in each instantaneous frequency band so we have to capture and calculate all of hem. In that case we need the same 20millisec to find the signal levels of the channels in the memory store.

Conclusions

It could be seen from the results above that based on tuned receiver architecture we need 400sec time to visit a given frequency again. This time far enough to send out any voice message at VHF without high risk of the interception of the transmission. If we use professional receiver the 16sec time means moderate increasing the interception probability, but using a digital transmission method lot of information could be send out during that time. The professional, high-speed, wide-bandwidth digital scanning receiver provides exceptional interception probability against time and frequency agile signals.
In the case of memory scanning the tuned receiver speeds up as the number of channels decease, but the exceptional speed of digital scanners provide more than enough performance against tuned receiver structure.