Signal Analysis
for
Radio Monitoring

Edition 2013

Dipl.- Ing. Roland Proesch

Signal Analysis
for
Radio Monitoring

Edition 2013

Books on Demand GmbH

Description of techniques to analyse
unknown waveforms
with 160 pictures and 31 tables

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Email: roland@proesch.net
Production and publishing: Books on Demand GmbH, Norderstedt, Germany
Cover design: Anne Proesch
Printed in Germany

Web page: www.frequencymanager.de

ISBN 9783732242566

Acknowledgement:

Thanks for those persons who have supported me in the preparation of this book:

Aikaterini Daskalaki-Proesch

Disclaimer:

The information in this book have been collected over years. The main problem is that there are not many open sources to get information about this sensitive field. Although I tried to verify these information from different sources it may be that there are mistakes. Please do not hesitate to contact me if you discover any wrong description.

Content

1. List of Pictures

2. List of Tables

3. General

For years shortwave radio has been used for communication beyond the line of sight. With the introduction of worldwide satellite services in the geostationary or low earth orbits HF radio communication lost more and more in interest.

But with the introduction of new, sophisticated modems and digital broadcast services in high quality HF communication has seen a renewal during the last years.

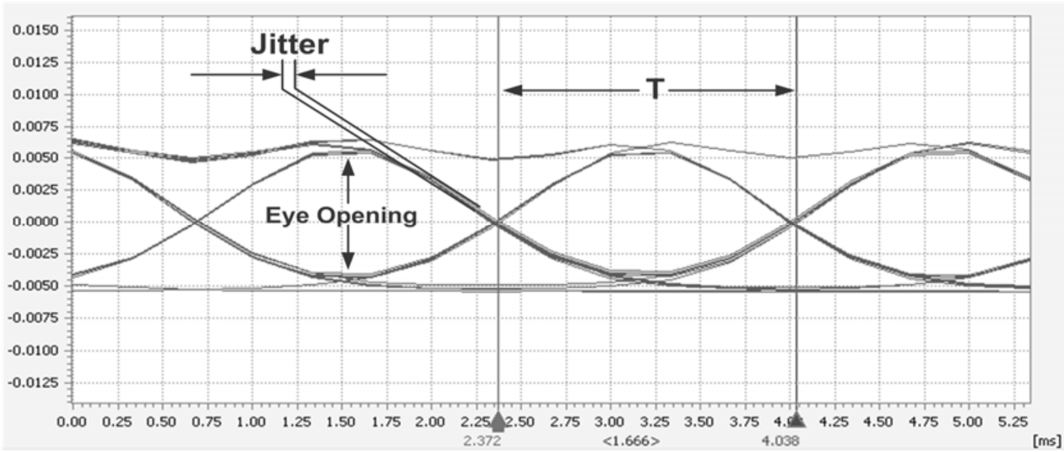
Shortwave radio, however, has some qualities that will ensure its attractiveness for some time. The most important one for commercial users is that there is no charge for using the ionosphere.
In the military context this translates to low cost, potentially global communication that has the important attributes of national ownership and military control.
And in comparison to satellite services shortwave communication is harder to disrupt.
The good old radio for shortwave has been perfected during the last years in several ways. Information data rates of a few tens of bits per second were increased to more than 19200 bit/s by sophisticated modem techniques and error correction. Algorithms were created to adapt transmission parameters to channel quality or initiate a change to a better channel. Passive and active channel analysis, i.e. sending and measuring test signals on assigned pool frequencies have been developed to solve problems of channel distortions.
There are new signals “on air” nearly every month. That makes it very difficult to keep track of them. And they often sound the same way.
This book shall give an introduction how to work with signals on shortwave and get that information which is necessary to identify the different waveforms. It will show some techniques for measurement the main parameter of digital signals.
It will also show some tools which I have used over the years to come to a result in a relative short time frame.
You are not bound to those tools described in this book. There are many others with a similar functionality which will do the job.

And please keep in mind:

Signal analysis is not an easy task!

If you are doing it only occasionally it will be difficult to come to satisfactory results. Signal analysis needs a constant practise.
And sometimes it may be a good idea not to choose an obvious way to do signal analysis.

Most signal analysis tasks are performed on recorded signals. For a successful work you will need good recordings. Information that is lost i.e. by noise can never be reconstructed.

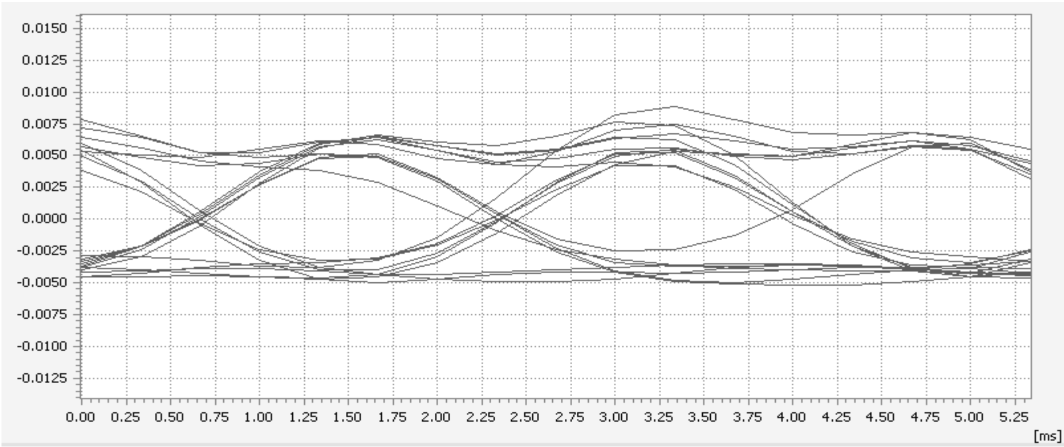


Picture 37: Measurement with eye diagram

The eye diagram can also be used to measure and calculate the baud rate of a signal. In this example the signal is a 2ASK with 600 Bd. The upper and lower lines are representing the binary 1 and binary 0. The transition between both is the change from 0 to 1 or 1 to 0. These transitions are related to the baud rate. The time distance of two cross points between two transition paths are a value for the bit width $\mathbf{T_B}$ in ms. 1000 ms divided by 1.66 ms is equal to the baud rate of the signal, in this case 600 Bd.

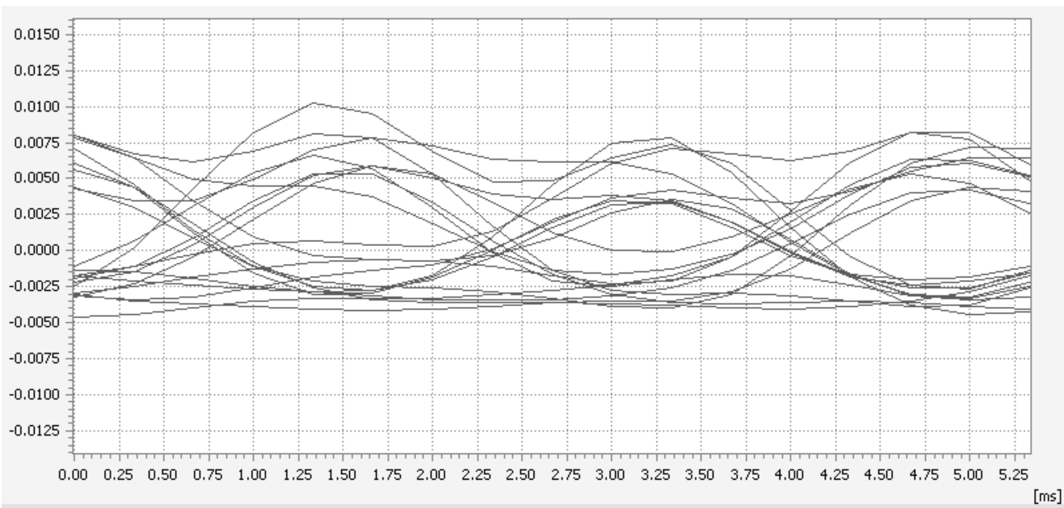
The thickness of the eye lines are an indicator for the jitter of a signal. The wider the lines are the more jitter between each bit is on the signal. Jitter is an indicator of timing errors during the transmission or reception.

The eye width or eye opening shows the additive noise on the signal. This is shown in the following two pictures:



Picture 38: Eye diagram with moderate noise

The eye can still be recognized.

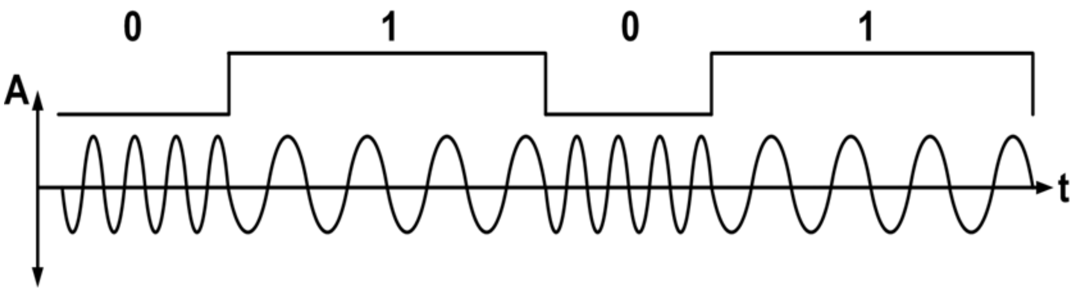


Picture 39: Eye diagram with more noise

In this case with a high amount of noise the eye width is very small.

Frequency Shift Keying (FSK)

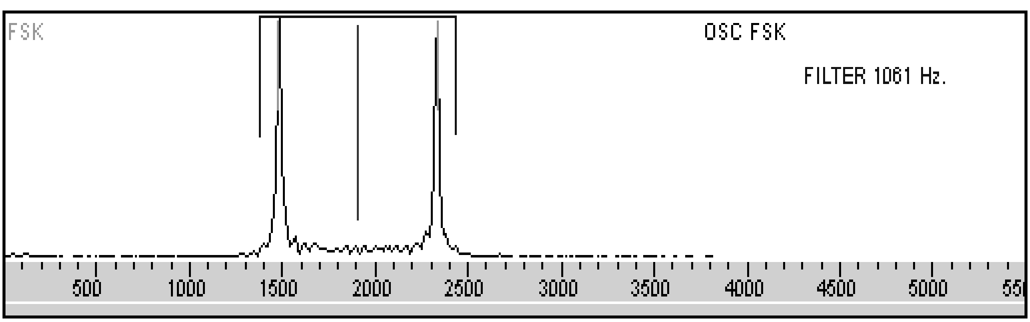
In frequency shift keying, the carrier frequency changes between discrete values. If only two frequencies are used then this will be called BFSK, for binary frequency shift keying. In the following picture the same data is represented, 0101.



Picture 40: Frequency Shift Keying (FSK)

Normally FSK is generated by **A**udio **F**requency **S**hift **K**eying (AFSK) switching between two tones which then can be used in single sideband (SSB) technique to modulate the transmitter. In relation to the incoming data for a 0 tone 1 is transmitted and for a 1 tone 2.

The following picture shows the typical spectrum of an FSK with discrete frequencies at 1500 Hz and 2350 Hz which gives a shift of 850 Hz:



Picture 41: Spectrum of an FSK

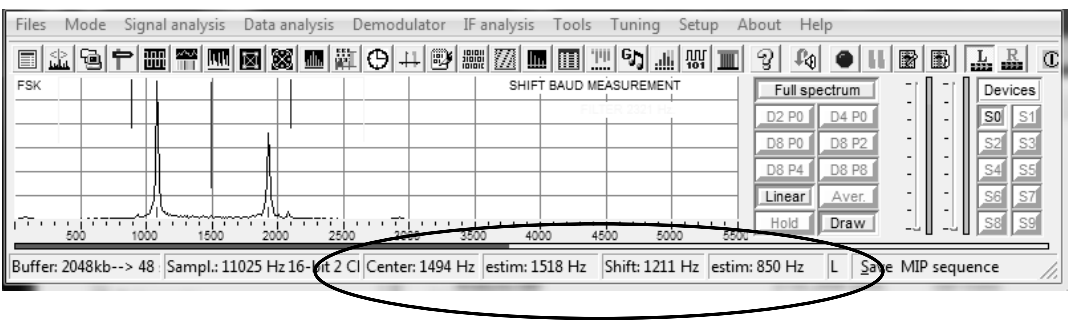
Analysis of a FSK

For a description of the waveform of a FSK signal the following parameter needs to be determined:

- Center frequency
- Mark frequency
- Space frequency
- Frequency shift
- Baud rate

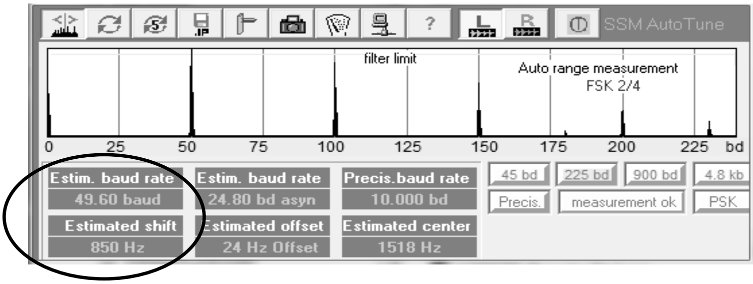
Automatic Detection of Center Frequency

In a first step it is important to determine the correct frequency of a FSK signal, especially when the reception is done with a receiver using a SSB demodulator. A decoder like C300 or C3P will do this automatically as shown in the next picture.



Picture 42: Automatic measurements

The software measures the two peaks in the spectrum, calculates the peak frequency and the center frequency. These values are also used for an automatic determination of the baud rate.

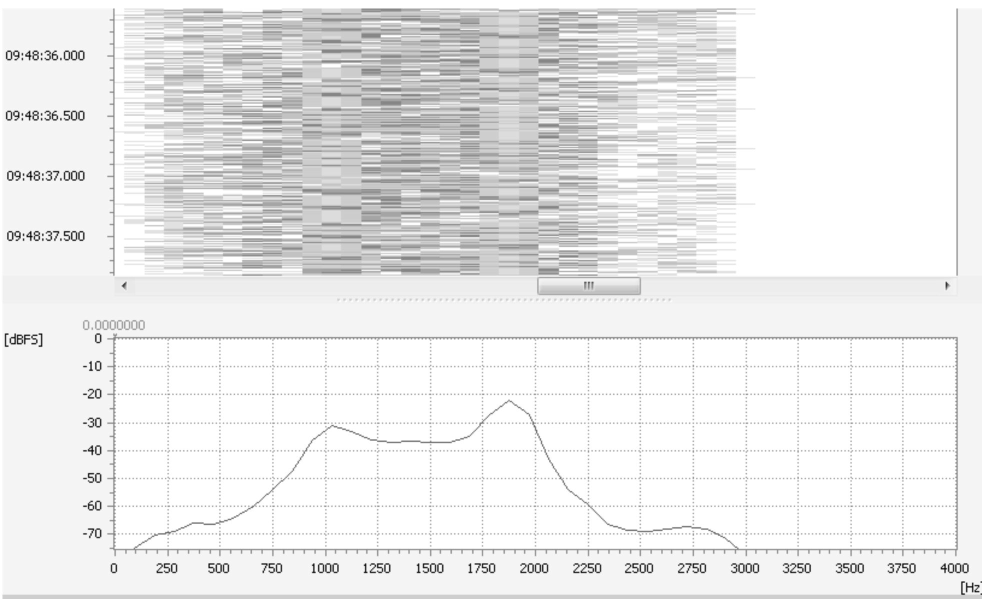


Picture 43: Automatic baud rate and shift measurement

Manual Detection of Center Frequency

<u>Frequency Resolution of FFT</u>

For the manual measurement the signal needs to be displayed correctly in a spectrum and/or a sonogram view. It is important to use a very high FFT resolution. With a low resolution the frequency distance between each FFT point is very high and results in a spectrum display with less information. The peaks are very wide. The following picture shows a FFT resolution of 256 points.



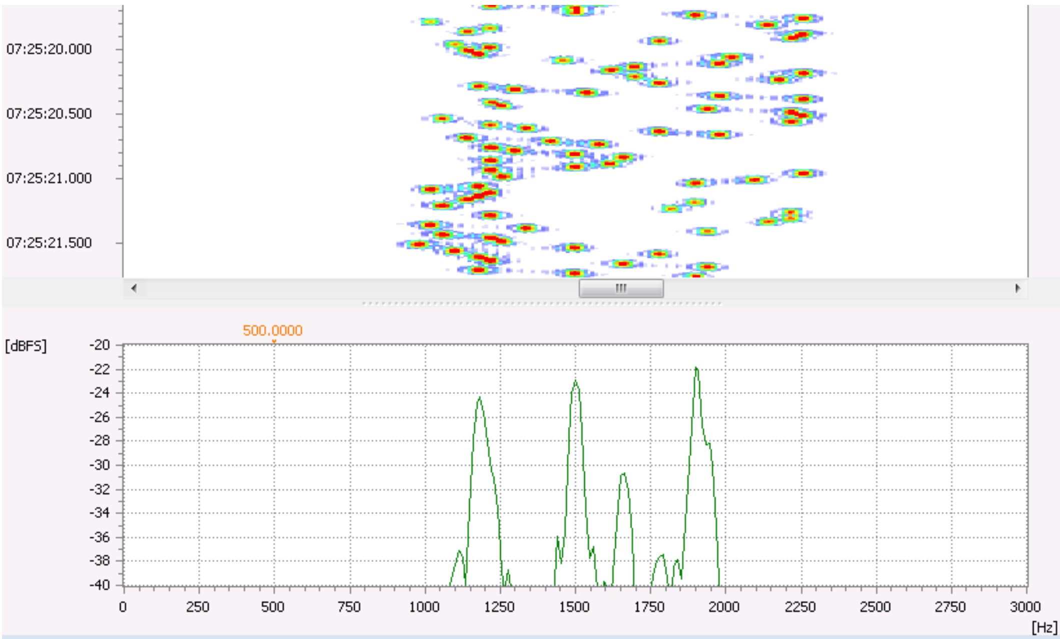
Picture 44: Spectrogram display with low FFT resolution

Analysis of MFSK signals

In this part we will determine the main parameter of a MFSK signal. These are:

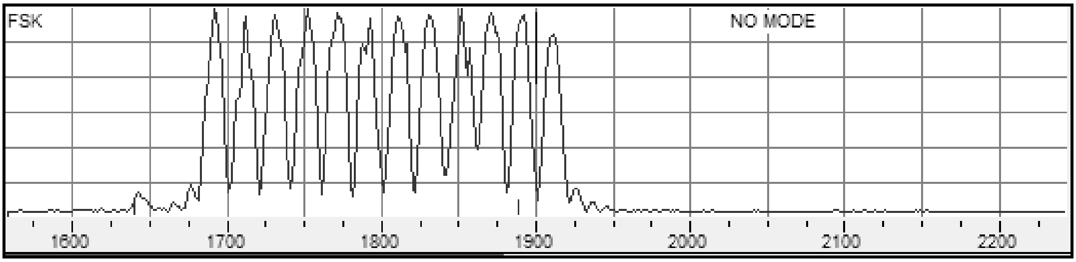
- Number of tones
- Tone duration
- Tone distance
- Baud rate

The following picture shows a typical MFSK signal in the spectrogram view.



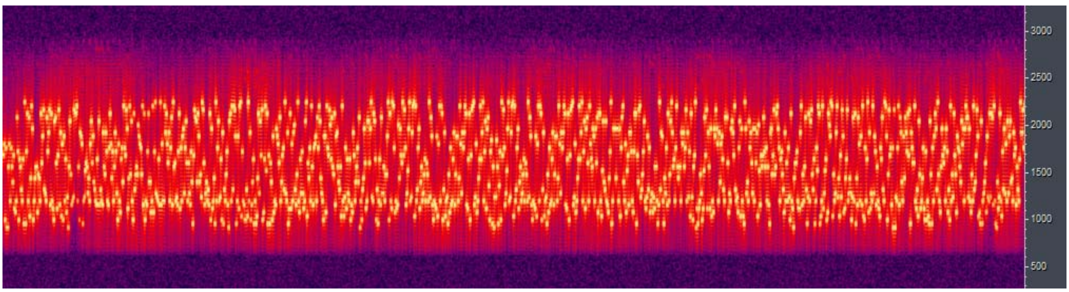
Picture 67: MFSK in the spectrogram view

In the first step we will determine the number of tones. The best tool for this is a spectrum analyser with a peak hold function. Each tone will be held in his highest amplitude. The measurement of number of tone is very easy: just count the number of them. In this example we can see the 12 tones of a PICCOLO signal. The procedure will be more difficult with a MFSK with a high number of tones.

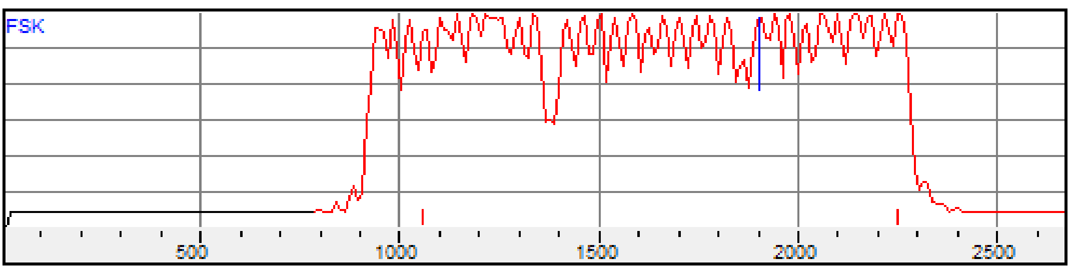


Picture 68: Number of tones of a MFSK

The procedure will be more difficult with a MFSK with a high number of tones like in the following picture.



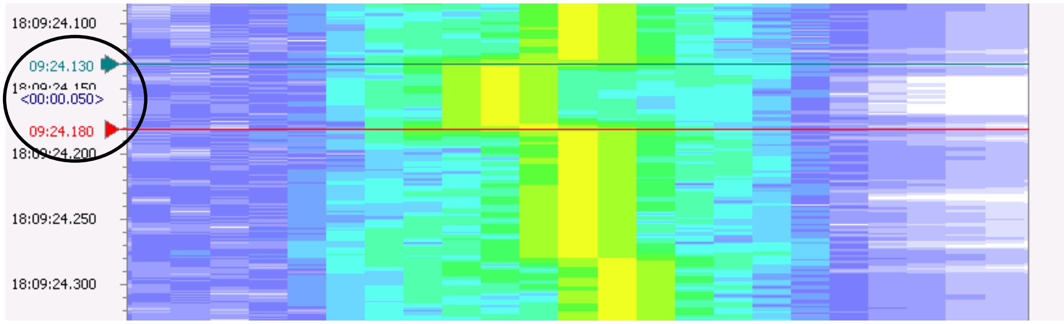
Picture 69: MFSK with 36 tones



Picture 70: Spectrum of a MFSK with 36 tones

But with the peak hold function this should also be possible as shown in the above example of a CIS 36 signal.

The next task is the measurement of the tone duration. This can be done in the sonogram with a very low FFT resolution. But as shown in the following picture this method is not very accurate and only practical for low baudrates. Due to the low frequency resolution it is very difficult to find the correct transition between tones.



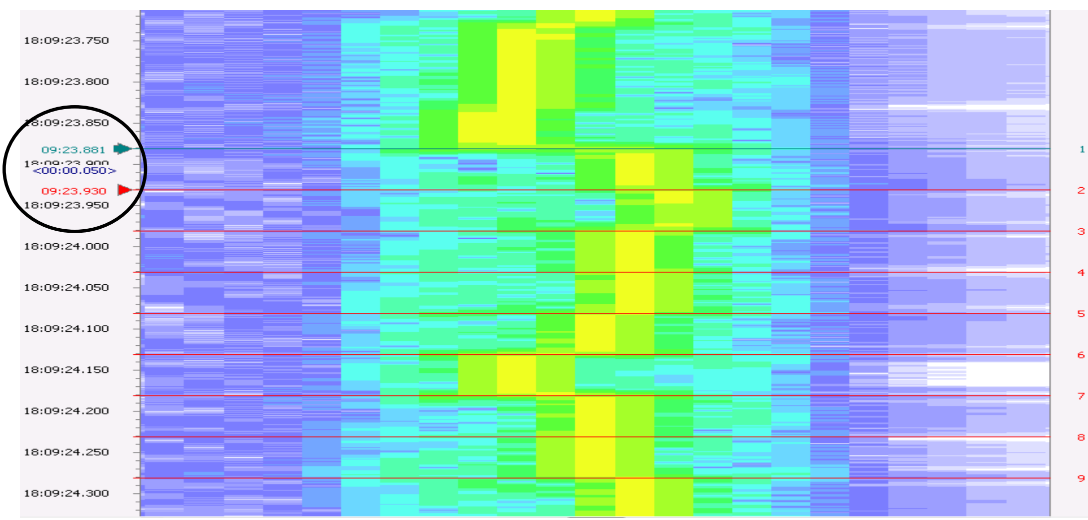
Picture 71: Measurement of tone duration of a MFSK

The smallest pulse corresponds to the time length of one bit. This time T_B is measured with a time cursor. The baud rate B is calculated by dividing one second or better 1000 ms through the time for one bit.

$$1000\ (\text{ms}) / T_B\ (\text{ms}) = B.$$

In this example it is 1000 ms/50 ms = 20 Bd.

If a harmonic cursor is available the correct setup can be proven by the exact match of the cursors to the changes between the different tones.

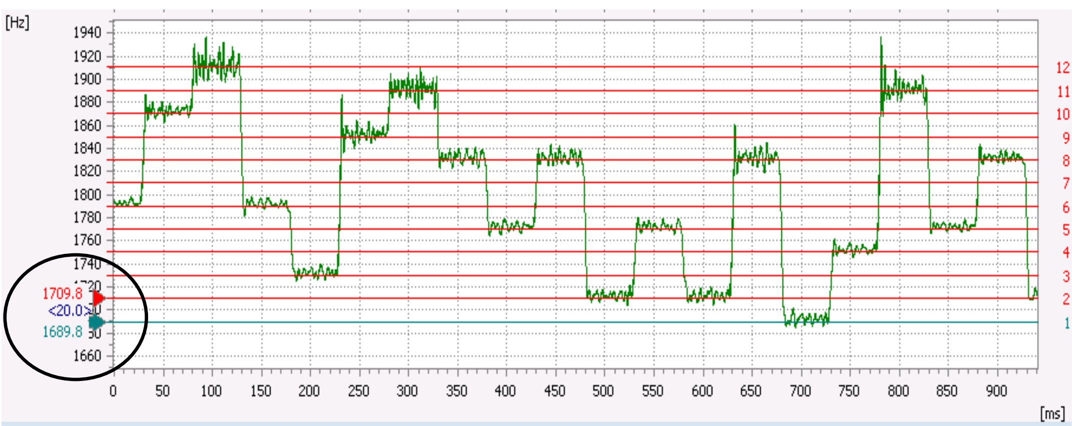


Picture 72: MFSK measurement with harmonic cursor

Another possibility to measure the duration of each tone is the usage of a MFSK demodulator or MFSK oscilloscope. Each tone is demodulated and shown as in the following picture. The duration can be measured with a time cursor. In this example the duration of one tone is 50 ms which corresponds to 20 Bd.

Picture 73: Tone duration measurement with MFSK oscilloscope

By placing a cursor of a harmonic cursor on each tone we can also determine the number of tones. It also will give us the distance of the tones which is 20 Hz in this example

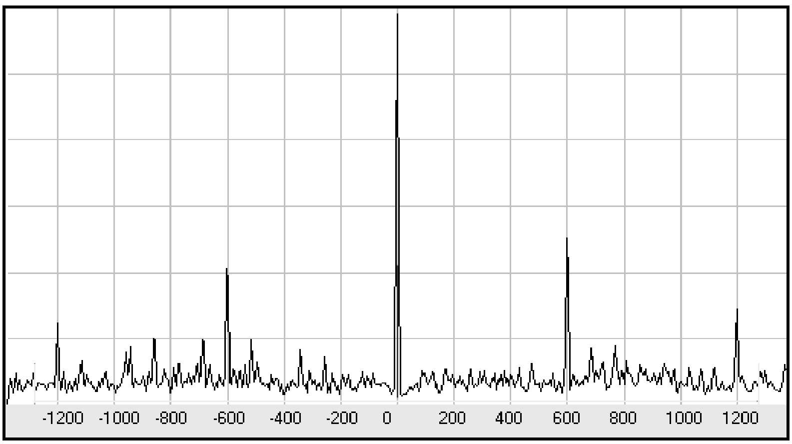


Picture 74: Determination of numbers of tones of a MFSK

From the above table can be seen that a PSK-2B has the same shifts as PSK-4A. Thus it may be difficult to recognize if in a PSK transmission it is a BPSK or a QPSK because the phase constellation looks the same way. But fortunalty there is another possibility to recognize the correct type.

Recognition of Absolute (PSK-A) and Differential PSK (PSK-B)

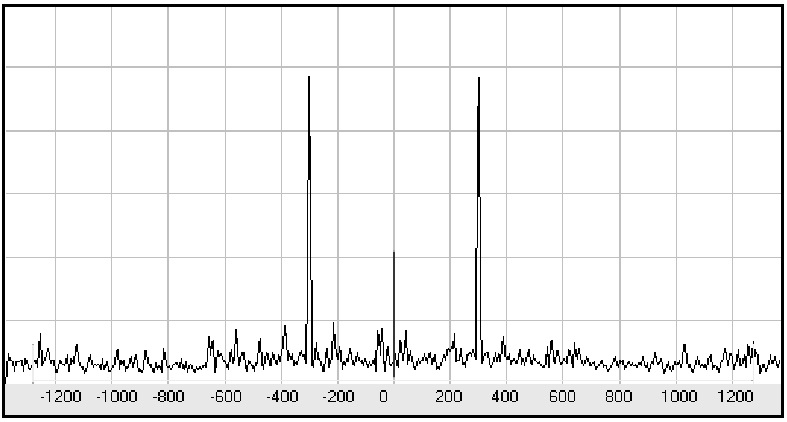
The main difference between a PSK-A and a PSK-B can be seen when using the squaring method for measurement of the exact center frequency. The following picture shows a QPSK-A with a 2 times squaring:



Picture 104: Double squaring of a QPSK-A

As we can see from the squaring result a QPSK-A is showing 3 peaks. The center peak is related to the center frequency. On the left and right side there are peaks related to the symbolrate of the signal. With the CODE300-32 phase tools the symbolrate is shown. In this example it is 600 Bd.

The following picture shows the spectrum of a QPSK-B after 2 times squaring.



Picture 105: Double squaring of a QPSK-B

As we can see that there is no center peak but two peak in a distance of 300 Hz to the center. The distance between both peaks correlates with the symbol rate.

Note: This is true for the CODE300-32. There are other spectrum analyzers with the possiblity of squaring. If the display is not corrected according the function of squaring you will need to mulitply the frequncy distance with the squaring number. For BPSK is it x2, for QPSK x4 and for 8PSK x8.
So the symbol rate is calculated:

Measured frequency distance x squaring number = symbolrate.

__PSK Types and their Behaviour__

<u>PSK2-A</u>

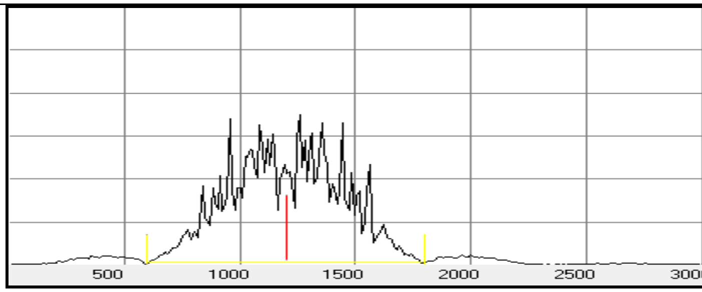
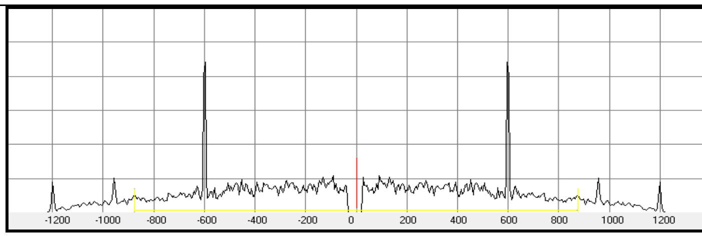
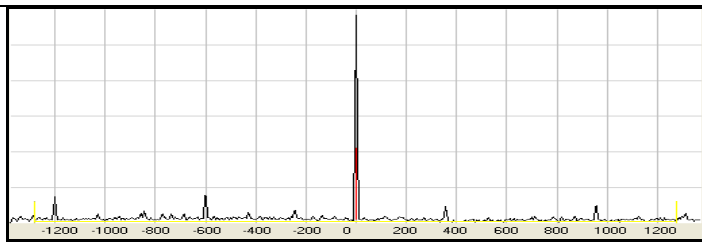
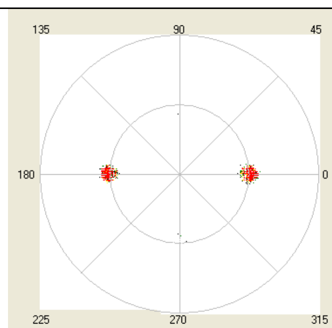
<table>
<tr><td>PSK-2A
Spectrum</td><td>
</td></tr>
<tr><td>PSK2-A
Envelope</td><td>
</td></tr>
<tr><td>PSK2-A 1x
Squaring</td><td>
</td></tr>
<tr><td>PSK2-A Phase
Constellation</td><td>
</td></tr>
</table>

Table 14: Characteristics of a PSK2-A

PSK2-B

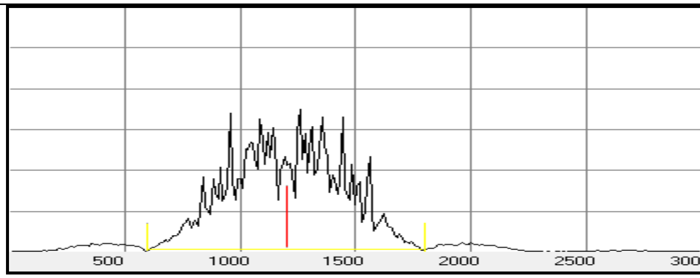
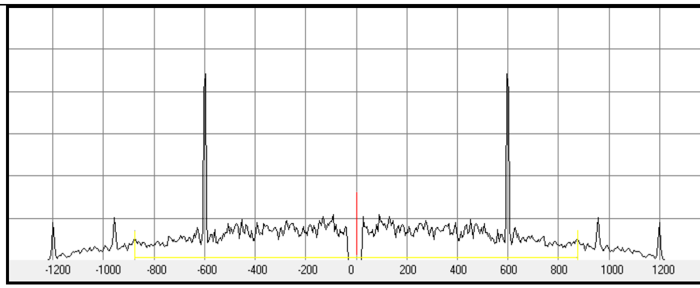
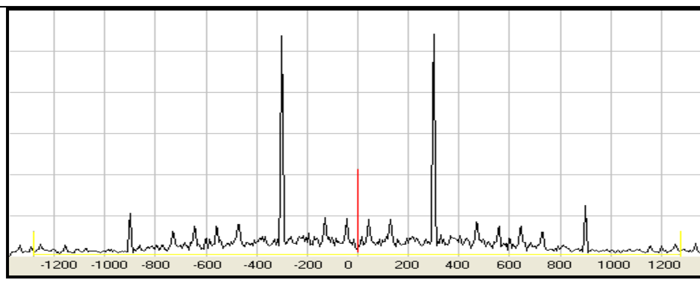
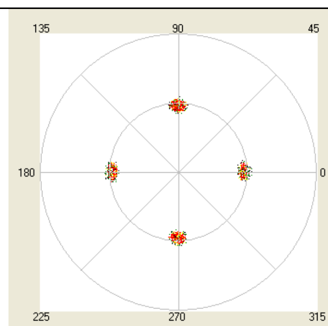
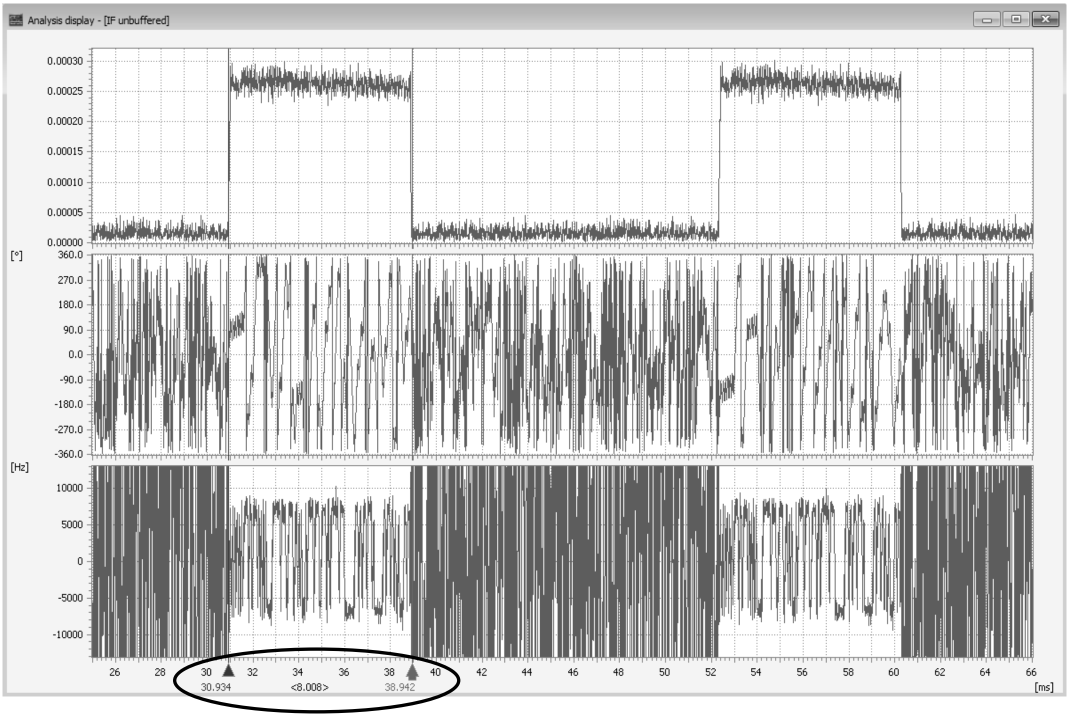
PSK2-B **Spectrum**	
PSK2-B **Envelope**	
PSK2-B **1 x Squaring**	
PSK2-B **Phase** **Constellation**	

Table 15: Characteristics of a PSK2-B

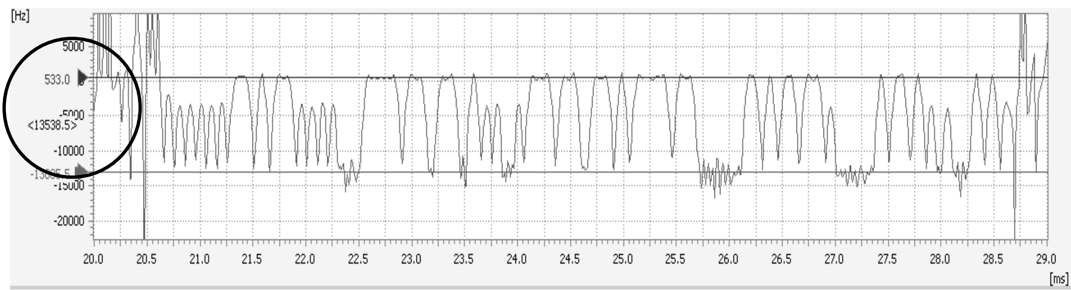
The magnitude window shows the signal each time it is repeated by the replay software. In the frequency window the signal contents can be recognized. In one step the duration of one hop can be determined by measuring the length of the hop with two cursors. This is shown in the following picture.



Picture 133: Measurement of the duration of one frequency hop

In this case a hop duration of 8 ms which gives a hopping rate of 125 hops per second. In the next step one hop is displayed and shows the data contest. The frequency display shows a FSK from which a shift of 13500 Hz can be determined.

Picture 134: Expanded display of one hop



Picture 135: Shift measurement of one hop

In a last step the baud rate of the FSK will be measured. This procedure was described in the FSK section before.

Picture 136: Baud rate measurement of one hop

The duration of one bit is 0.05 ms which can be calculated to 1000 ms / 0.05 ms = 20000 Bd.

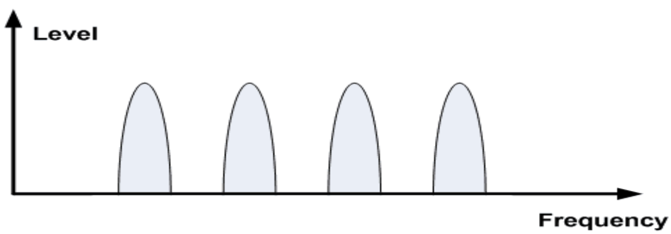
Incremental Frequency Keying (IFK)

In an incremental frequency keying the data is not represented by the frequency of each tone, but by the frequency difference between one tone and the next. IFK consequently provides complete independence of tuning and tolerance of drift. IFK also makes the management of tone sets possible in order to reduce inter-symbol interference, and reduces the effect of systematic errors, such as those produced by in-band carriers.

Channel access methods

Frequency-Division Multiple Access (FDMA)

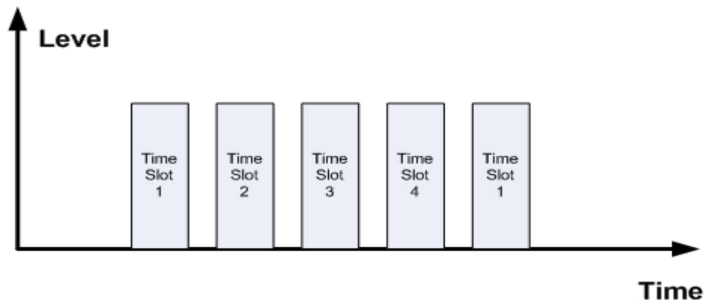
FDMA, or frequency-division multiple access, is the oldest and most important of the three main ways for multiple radio transmitters to share the radio spectrum. The other two methods are Time Division Multiple Access (TDMA), and Code Division Multiple Access (CDMA).
In FDMA, each transmitter is assigned a distinct frequency channel so that receivers can discriminate among them by tuning to the desired channel.
TDMA and CDMA are always used in combination with FDMA, i.e., a given frequency channel may be used for either TDMA or CDMA independently of signals on other frequency channels.



Picture 159: Principle of FDMA

Time Division Multiple Access (TDMA)

Time Division Multiple Access (TDMA) is a technology for shared medium (usually radio) networks. It allows several users to share the same frequency by dividing it into different time slots.
The users transmit in rapid succession, one after the other, each using their own timeslot. This allows multiple users to share the same transmission medium (e.g. radio frequency) whilst using only the part of its bandwidth they require. TDMA is used extensively in satellite systems, local area networks, physical security systems, and combat-net radio systems.



Picture 160: Principle of TDMA

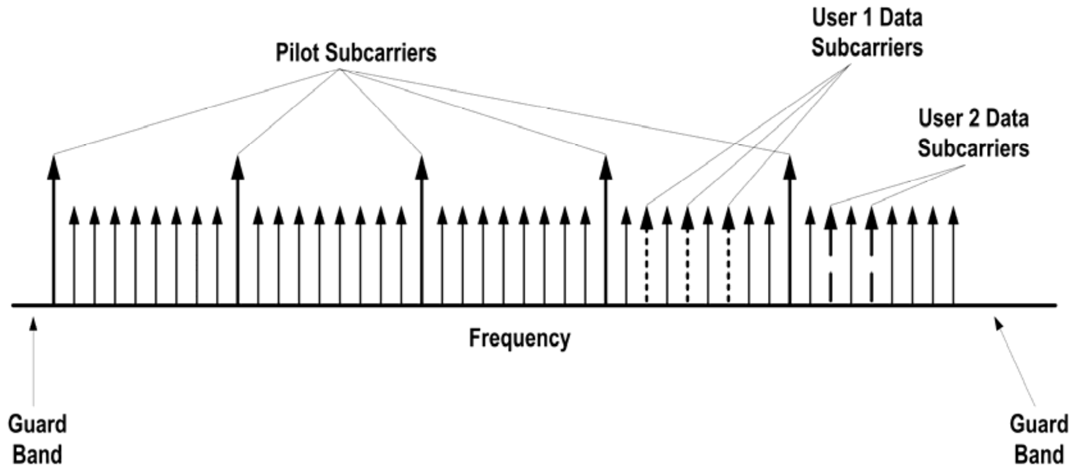
Code Division Multiple Access (CDMA)

Generically (as a multiplexing scheme), code division multiple access (CDMA) is any use of any form of spread spectrum by multiple transmitters to send to the same receiver on the same frequency channel at the same time without harmful interference.
One important application of CDMA is the Global Positioning System, GPS.

CDMA's main advantage over TDMA and FDMA is that the number of available CDMA codes is essentially infinite. This makes CDMA ideally suited to large numbers of transmitters each generating a relatively small amount of traffic at irregular intervals, as it avoids the overhead of continually allocating and de-allocating a limited number of orthogonal time slots or frequency channels to individual transmitters. CDMA transmitters simply send when they have something to say, and go off the air when nothing is to transmit.

Orthogonal Frequency Multiple Access (OFDMA)

Orthogonal Frequency Division Multiple Access (OFDMA) is a multi-user version of the OFDM digital modulation scheme. Multiple access is achieved in OFDMA by assigning subsets of subcarriers to individual users as shown in the picture below. This allows simultaneous low data rate transmission from several users. OFDMA can also be described as a combination of frequency domain and time domain multiple access, where the resources are partitioned in the time-frequency space, and slots are assigned along the OFDM symbol index as well as OFDM sub-carrier index.



Picture 161: Principle of OFDMA