Cuprite Reference Manual V1.3

An RF tester for the *802.15.4 O-QPSK standard operating in the 2.4GHz band*, compatible with TLF3000.

July 16, 2021

1 Contents

2 Overview.

TLF3000 is a wideband, ultra-high dynamic range 2.4GHz software-defined receiver, signal analyzer and signal generator. It captures and analyzes the entire 2402-2480MHz band simultaneously. It can also generate arbitrary waveforms occupying the band 2395-2485MHz with a maximum peak level of 0 dBm. Additionally, it includes a CW signal generator covering 25MHz to 6GHz with an output level of -50dBm to -28dBm

Cuprite is a *802.15.4* O-QPSK application for the *TLF3000* software-defined receiver, signal analyzer and signal generator. The Cuprite application can:

1. Act as a signal generator, creating signals required for receiver testing including interfering and blocking signals. A variety of pulsed and continuous signals can be generated for measuring the receiver ED and AWGN may be added for LQI measurements.
2. Act as a signal analyzer, performing transmitter tests on conducted or off-air signals without knowledge of the payload or RF channel. Tests include EVM, power spectral density, carrier offset and drift, output power as well as symbol timing accuracy. The output of the carrier tracking loop is also available.
3. Monitor all 16 channels and either pipe the decoded packets directly into Wireshark for live protocol analysis or dump the packets to file. Data capture can be restricted to certain channels or by an RSSI threshold,

The application has been honed for speed. For example, EVM and spectral measurements are performed in parallel, exploiting the unique architecture of the *TLF3000*.

A key feature of the unit is its ability to perform C/I, receiver selectivity and intermodulation tests without the need for additional test equipment. This is possible due to *TLF3000's* ultra-linear wideband signal generator. This permits both wanted and interfering signals to be generated through the same signal path. The high linearity and low noise floor ensure that there is ample dynamic range to encompass both the wanted and interfering signals. Furthermore, high fidelity filtering of the interfering signals ensures that they are correctly bandlimited and that unwanted sidebands are not responsible for test failures; this is frequently overlooked when external test equipment is used to provide these signals. The single signal path also removes the need for time consuming and laborious calibration of signal combiners as well as eliminating the need to ensure that the injected interfering and wanted signals do not generate intermodulation products before arriving at the DUT.

Unique to *TLF3000* is a 25MHz to 6GHz signal generator. This enables the majority of the receiver blocking performance to be explored prior to committing the DUT for formal inspection at a test house with its associated costs.

3 Control.

3.1 Overview

The Cuprite application can be controlled directly from a host machine via USB or Ethernet. The control may be via a native command language or a comprehensive GUI. In addition, the signal generator can be stopped or started via hardware triggers.

3.2 Native language

The *TLF3000* supervisor program and Cuprite application can be controlled via a simple native language. The native language provides a convenient means of controlling Cuprite from high level host languages, such as Python. The native language exposes all the features supported by Cuprite.

The native language relies on three control channels:

1. Command Control channel. Transfers commands from the host to Cuprite.
2. Command Response channel. Contains the response from Cuprite for the command issued on the Command Control channel. There is one response for every command issued.
3. Data channel. Transfers asynchronous data from Cuprite to the host.

If a USB interface is used, then these three channels map to three USB endpoints. If an Ethernet interface is used, then the first two channels map to one TCP/IP socket whilst the data channel maps to a second TCP/IP socket.

It is possible to utilise both the USB and Ethernet interfaces simultaneously.

3.3 Cuprite GUI

A GUI is shipped with the Cuprite application. This permits the application to be controlled via a host running Windows, Linux or OS X. The GUI connects to the *TLF3000* either over USB or Ethernet. The GUI exposes the majority of the Cuprite functionality.

4 Operating Modes.

4.1 Overview

Cuprite has three operating modes:

1. Signal generator.
2. Signal analyzer.
3. Packet sniffer (Wireshark)

4.2 Signal Generator

The signal generator mode permits manual control over all the signal sources used for receiver testing. Any combination of the following signals can be generated simultaneously:

1. Packetized 802.15.4 O-QPSK signal with programmable contents
2. Continuously modulated or packetized O-QPSK signal
3. Up to 3 independent in-band CW signals, which may be pulsed
4. In-band AWGN source, which may be pulsed
5. Out-of-band CW signal.

All signal sources are fully parameterised.

4.3 Signal Analyzer

The signal analyzer mode monitors all 16 channels simultaneously. Any detected packets are captured and analyzed in accordance with the 802.15.4 specification. Tests include EVM, power spectral density, carrier offset and drift, output power as well as symbol timing accuracy.

The signal analyzer can process either conducted signals or monitor off-air traffic from live links.

The signal analyzer mode also permits the capture of raw IQ data, FM demodulated data, constellations plots or power profiles.

4.4 Packet Sniffer (Wireshark)

The packet sniffer mode monitors all 16 channels simultaneously Any packets which are detected are demodulated and the bit stream either piped directly into Wireshark for live protocol analysis, and/or saved to file. Capture can be restricted to certain RF channels or an RSSI threshold can be set. During capture, a spectrum display is available so that the prevailing RF environment can be monitored.

5 Launching the Cuprite GUI.

In order to communicate with the *TLF3000* unit, it is necessary to attach it to a host computer via USB or Ethernet (or both). An Ethernet connection is only possible if the host computer and *TLF3000* unit reside on the same subnet. The *TLF3000* IP address can be changed by connecting it to a host computer via USB and using the *Application Loader*.

To launch the Cuprite GUI it is first necessary to run *Application Loader*. This should result in the following screen being displayed:

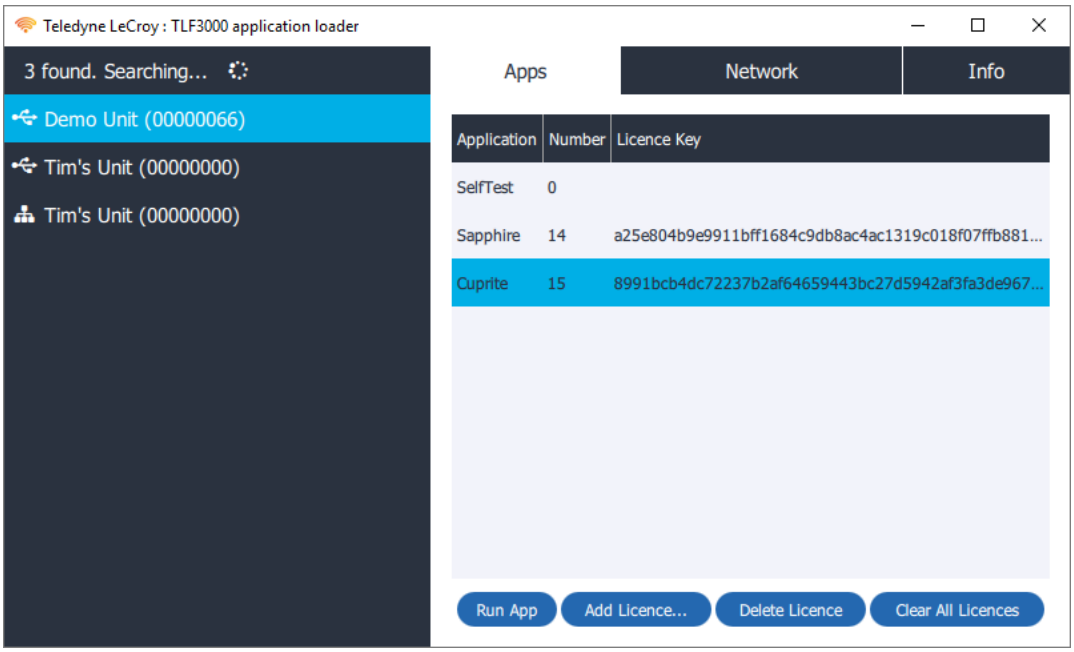


Figure 1: Application Loader main screen.

This screen indicates that the following *TLF3000* devices have been discovered:

1. Serial number 00000066 connected via USB (highlighted)
2. Serial number 00000000 connected via USB
3. Serial number 000000600connected via Ethernet (this device is shown twice)

The right hand side of the window has three tabs:

1. *Apps*. Shows which applications are licensed to run on this unit. It also permits the loading of new licence keys.
2. *Network*. Shows the current network settings and permits these to be modified.
3. *Info*. Provides more information about the unit and permits the unit's friendly name to be modified. It also provides a means of updating the firmware on the unit.

To launch the Cuprite application open the '*Apps'* tab and then either:

1. Double click on the Cuprite application
2. Highlight the Cuprite application and then click the '*Run App*' button.

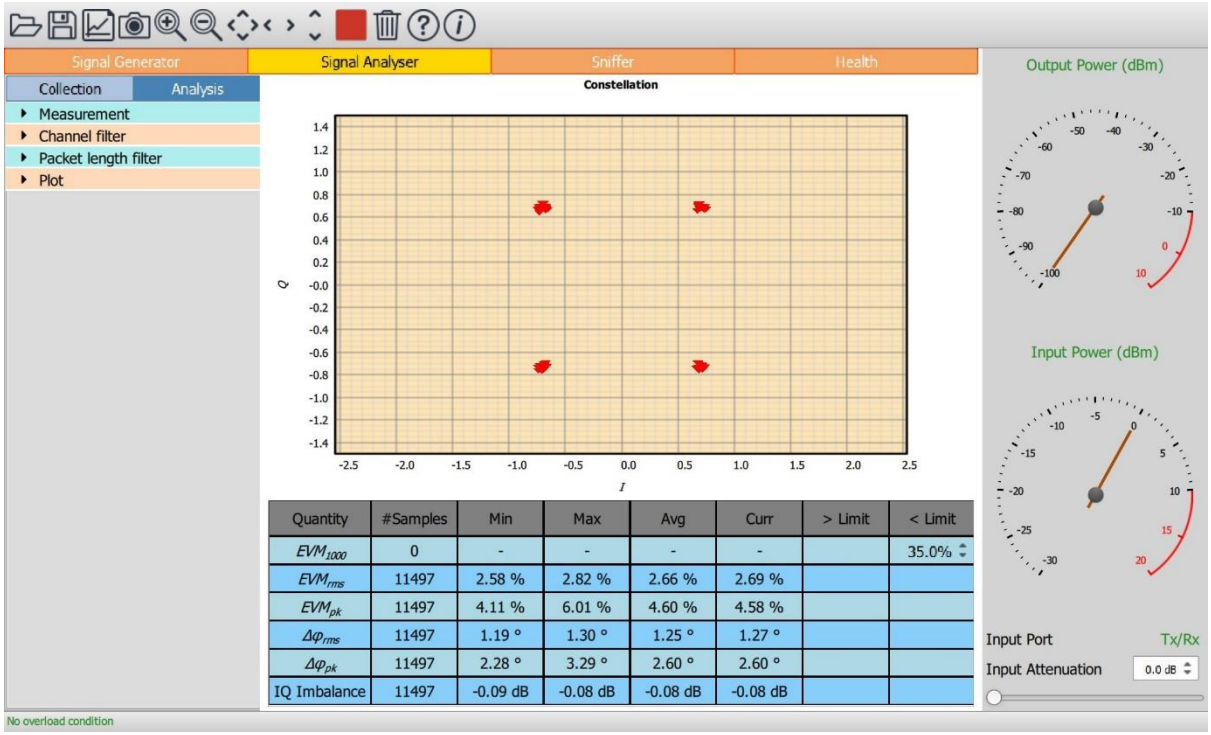
On launching the application, the searching cursor should stall, the fan on the *TLF3000* unit will start to spin and after a few seconds the Cuprite GUI will load.

6 Anatomy of the Cuprite GUI.

6.1 Overview

The Cuprite GUI is composed of the following elements:

1. A tool bar along the top of the window
2. A monitor panel to the right of the window
3. A status bar at the bottom of the window
4. Mode tabs located immediately underneath the tool bar
5. A mode control panel to the left of the window
6. A graphics area
7. A tabular results area below the graphics area (not present in signal generator mode)



Quantity	#Samples	Min	Max	Avg	Curr	> Limit	< Limit
EVM_{1000}	0	-	-	-	-		35.0%
EVM_{rms}	11497	2.58 %	2.82 %	2.66 %	2.69 %		
EVM_{pk}	11497	4.11 %	6.01 %	4.60 %	4.58 %		
$\Delta\varphi_{rms}$	11497	1.19 °	1.30 °	1.25 °	1.27 °		
$\Delta\varphi_{pk}$	11497	2.28 °	3.29 °	2.60 °	2.60 °		
IQ Imbalance	11497	-0.09 dB	-0.08 dB	-0.08 dB	-0.08 dB		

Figure 2: Cuprite GUI

6.2 Toolbar

The toolbar contains the following elements:

6.2.1 Open and save

Opens and loads a settings file. Settings are saved individually for each mode of operation. The appropriate settings file is automatically selected on the basis of the current mode tab.

Saves the settings or results. Settings are saved individually for each mode of operation. The choice as to whether settings or results are saved is determined by the file extension which is selected.

6.2.2 Screen capture

Saves the current graphics area as an image file. A variety of image file formats are supported.

Takes a screen shot of the GUI and saves as an image file. A variety of image file formats are supported.

6.2.3 Zooming

Activates the cross-hair cursor which permits zooming within in the graphics area. Depress the left mouse button whilst dragging the cursor to select the area to be displayed. Clicking the right mouse button within the graphics area will give a list of additional zoom options.

Zooms out within the graphics area. Clicking the right mouse button within the graphics area will give a list of additional zoom options.

Pans within the graphics area. Hold down the left mouse button and drag to pan anywhere within the graphics display.

Pans along the x-axis within the graphics area. Hold down the left mouse button and drag horizontally. This is particularly useful for examining long waveforms.

Pans along the y-axis within the graphics area. Hold down the left mouse button and drag vertically.

6.2.4 Run and clear

Causes the currently selected mode to run. ***NOTE: the signal generator will not output energy until this is clicked.***

Stops the currently selected mode running. A running operation will automatically be aborted if a different mode of operation is selected.

Clears the current results history. Not applicable in signal generator mode.

6.2.5 Help

Displays the online documentation in a pop-up window.

Displays version information.

6.3 Monitor panel

6.3.1 Overview

The purpose of the monitor panel is to permit the user to quickly ascertain whether:

1. There is RF energy being emitted from the unit
2. There is RF energy being received by the unit

Whenever the unit or DUT appears to be unable to receive, the monitor panel should always be the first item to examine. Many problems can be quickly resolved with the information that it displays.

The monitor panel also determines which RF port is being used and provides manual control of the receiver front-end attenuation.

6.3.2 Output power

The output power gauge shows the energy being emitted by the *TLF3000*. The gauge is only approximate and should not be used for accurate measurements.

The red arc indicates the overload region. If an overload does occur, this will be evident by the '*Output Power (dBm)*' label turning red and a warning message being displayed in the status bar.

The output power gauge only shows the energy being emitted within the 2.4GHz ISM band. Energy from the out-of-band CW blocker is not included, even if its frequency lies within the 2.4GHz ISM band.

6.3.3 Input power

The input power gauge shows the energy incident on the selected *TLF3000* input port. The gauge is only approximate and should not be used for accurate measurements.

The red arc indicates the overload region. If an overload does occur, this will be evident by the '*Input Power (dBm)*' label turning red and a warning message being displayed in the status bar. It may be possible to remove a receiver overload condition by:

1. Adding additional receiver front-end attenuation using the control at the bottom of the monitor panel.
2. Swapping to the '*Tx/Rx*' RF port if the '*Monitor In*' RF port is being used. It is also necessary to select which RF port is being used by setting the switch at the bottom of the monitor panel.

The input power gauge only shows energy within the 2.4GHz ISM band. F-bar filters at the front of the receiver chain ensure other energy is eliminated and cannot block the receiver.

6.3.4 Input port

The input port switch selects which of the two RF input ports will be used:

1. The '*Monitor In'* port is suitable for off-air monitoring and has a noise figure of 6dB. In benign environments no additional receiver front-end attenuation should be required. However, in environments with strong Wi-Fi activity, it may be necessary to add receiver front-end attenuation to prevent overload conditions.
2. The '*Tx/Rx*' port is suitable for conducted measurements. If the DUT is capable of outputting more than +10dBm, it may be necessary to add receiver front-end attenuation to prevent overloading the receiver.

6.3.5 Input attenuation

These controls are used to select the receiver front-end attenuation. The attenuation may be adjusted by:

1. Moving the slider
2. Using the up/down arrows on the spin box
3. Typing a numeric value into the spin box text area

The available attenuation range is 0 to 31.5dB in steps of 0.5dB.

6.4 Status bar

6.4.1 Overview

The status bar at the bottom of the window is divided into two areas:

1. Overload indicator
2. Error message text

6.4.2 Overload indicator

The overload indicator will turn red when an overload condition occurs on either the transmit output or the selected receiver input port. The text of the message will indicate where the overload condition is occurring.

6.4.3 Error message text

The error message text reflects the last error detected by the Cuprite application running on the *TLF3000* unit. This message is cleared when either the '*Run*' or '*Clear*' buttons are pressed, or when a different operating mode is selected.

6.5 Mode tabs

The operating mode is selected by the tabs immediately underneath the tool bar. The following operating modes can be selected:

1. Signal generator
2. Signal analyzer
3. Packet sniffer (Wireshark)

In addition, it is possible to display a page showing the health of the *TLF3000* unit.

Whenever a new mode of operation is selected, any currently running tests are aborted.

6.6 Mode control panel

For each operating mode, a mode control panel is displayed to the left of the window. This panel allows the user to define the parameters for the current operating mode. The contents of the mode control panel are mode-specific.

In the case of the signal analyzer, the mode control panel is divided into two tabs:

1. *Collection*. This tab contains parameters which determine what data will be collected and how it will be collected.
2. *Analysis*. This tab contains parameters which determine how results from the collected data will be displayed.

6.7 Graphics area

For the signal analyzer mode of operation, a graphical representation of the results are displayed in the graphics area. Which results are displayed and how they are displayed are determined by the settings in the '*Analysis*' tab on the mode control panel. The graphics area also displays any limits which may apply to the displayed quantity.

For the signal generator mode, the graphics area provides a visual indication of which signals have been programmed. Note that the graphics area only shows what has been programmed; to make the programmed signals appear at the transmitter port, the '*Play'* button within the tool bar must be activated.

For the packet sniffer (Wireshark) mode, the graphics display area shows a 100kHz resolution spectrum of the entire 2.4GHz band. The spectrum analyzer detector is run in a peak detect mode. This provides a visual indication of the prevailing RF environment, which can severely impact on which packets can be collected.

6.8 Tabular results area

In the signal analyzer mode the region below the graphics is used to display tabular results. Which results are displayed is determined by settings on the '*Analysis'* tab in the mode control panel. The results tables also contain test limits which can be adjusted by the user. Tests that fail the limits are highlighted. The contents of the graphics display area can also be controlled by highlighting rows within the results table.

In the packet sniffer (Wireshark) mode, the tabular results area shows how many packets have been received on each of the 16 channels.

The tabular results area is not used in signal generator mode.

7 Signal Generator Mode.

7.1 Overview

The signal generator is able to produce any combination of the following signals:

1. A packetized 802.15.4 O-QPSK test signal with programmable contents.
2. A continuously modulated or packetized O-QPSK interfering signal.
3. Up to 3 independent in-band CW signals, which may be pulsed.
4. An in-band AWGN source, which may be pulsed.
5. An out-of-band CW signal.

The mode control panel on the left hand side of the screen lists the signals which can be generated. The switch to the left of the signal name programs the signal on or off. Although a signal may be programmed on, no output is generated from the unit until the '*Play*' button in the tool bar is activated.

The top graph in the graphics window shows a symbolic representation of signals generated within the 2.4GHz ISM band. The graphics assume a resolution bandwidth of 100kHz, hence the displayed levels for modulated signals will be slightly lower than their programmed levels. The 802.15.4 channels are emphasised by coloured bars.

The bottom graph in the graphics window shows a symbolic representation of the signals generated between DC and 6GHz. The graphics assume a resolution bandwidth greater than the modulation bandwidth, hence all signals appear at their programmed levels.

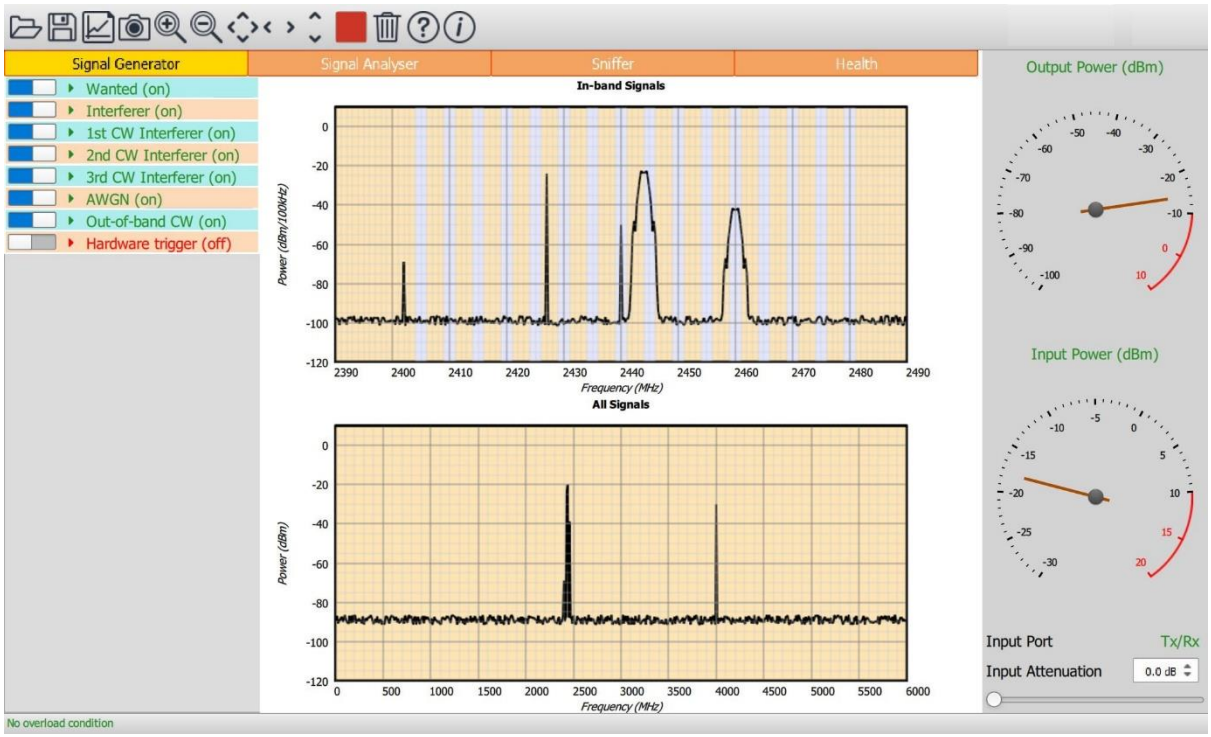


Figure 3: Cuprite GUI in signal generator mode.

7.2 RF connections

The signal generator output is on the Tx/Rx port.

7.3 Programming the packetized 802.15.4 signal

7.3.1 Overview

The packetized 802.15.4 signal generated by Cuprite is heavily parametrised. Virtually any aspect of the packet generation can be controlled.

To turn the packetized 802.15.4 signal on or off, toggle the switch to the left of the 'Wanted' text.

To program the packetized 802.15.4 signal, expand the 'Wanted' signal menu by clicking on it:

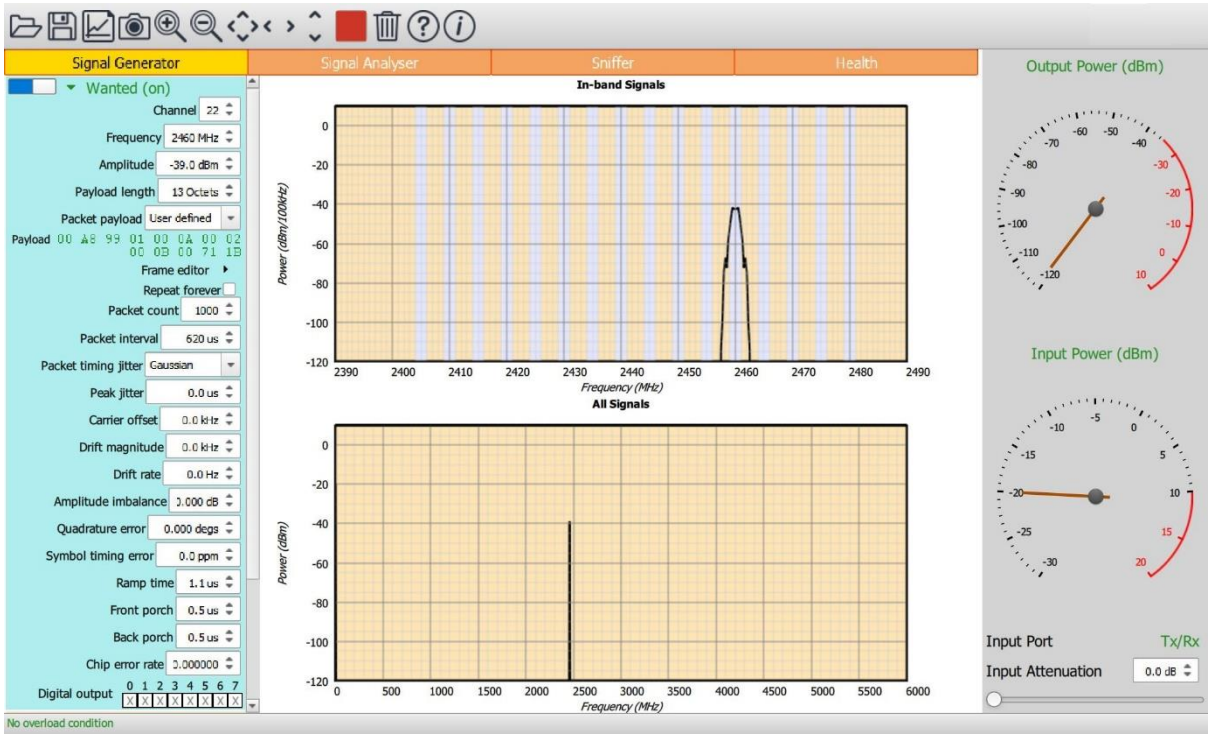


Figure 4: Programming the packetized 802.15.4 signal.

7.3.2 Carrier frequency

The frequency of the carrier can be set to anyone of the sixteen 802.15.4 channels either by:

1. Using the channel number spin box
2. Using the frequency spin box

As with all spin boxes, adjustment can be performed either by using the up/down arrows or by entering a numeric value into the text field.

7.3.3 Amplitude

The amplitude of the wanted signal can be adjusted from -120dBm to 0dBm. The total combined output power of the unit within the 2.4GHz ISM band is 0dBm. Therefore, if other signals are active,

the maximum output power for the wanted signal will be reduced to maintain the peak output power within the 0dBm limit.

7.3.4 Payload length

The payload length can be adjusted between 0 and 127 octets. This is the number of octets in the PHY PPDU after the PHR field. Altering the payload length may result in the packet interval changing to ensure that packets do not overlap in time.

7.3.5 Payload

The packet payload (ie the octets in the PHY PPDU subsequent to the PHR field) can be set to any one of the following (least significant bit first):

1. PRBS9 sequence
2. PRBS11 sequence
3. PRBS15 sequence
4. PRBS20 sequence
5. PRBS23 sequence
6. PRBS29 sequence
7. PRBS31 sequence
8. `11110000` repeated
9. `10101010` repeated
10. `11111111` repeated
11. `00000000` repeated
12. `00001111` repeated
13. `01010101` repeated
14. User defined

If the '*User defined*' option is selected, then the payload is shown below the packet payload selection box as a hex string in transmission order. This hex string can be edited directly.

To aid the entry of valid 802.15.4 packets, a frame editor is also available if the '*User defined*' option has been selected. If the '*Frame editor*' text is clicked, then the frame editor will open up in a new window. The operation of the frame editor is described in section 7.3.5.

7.3.6 Frame editor

7.3.6.1 Frame editor overview

Clicking on the '*Frame editor*' text will pop-up the 802.15.4 frame editor dialog. The frame editor initial shows an interpretation of the hex string in the payload field of the main window.

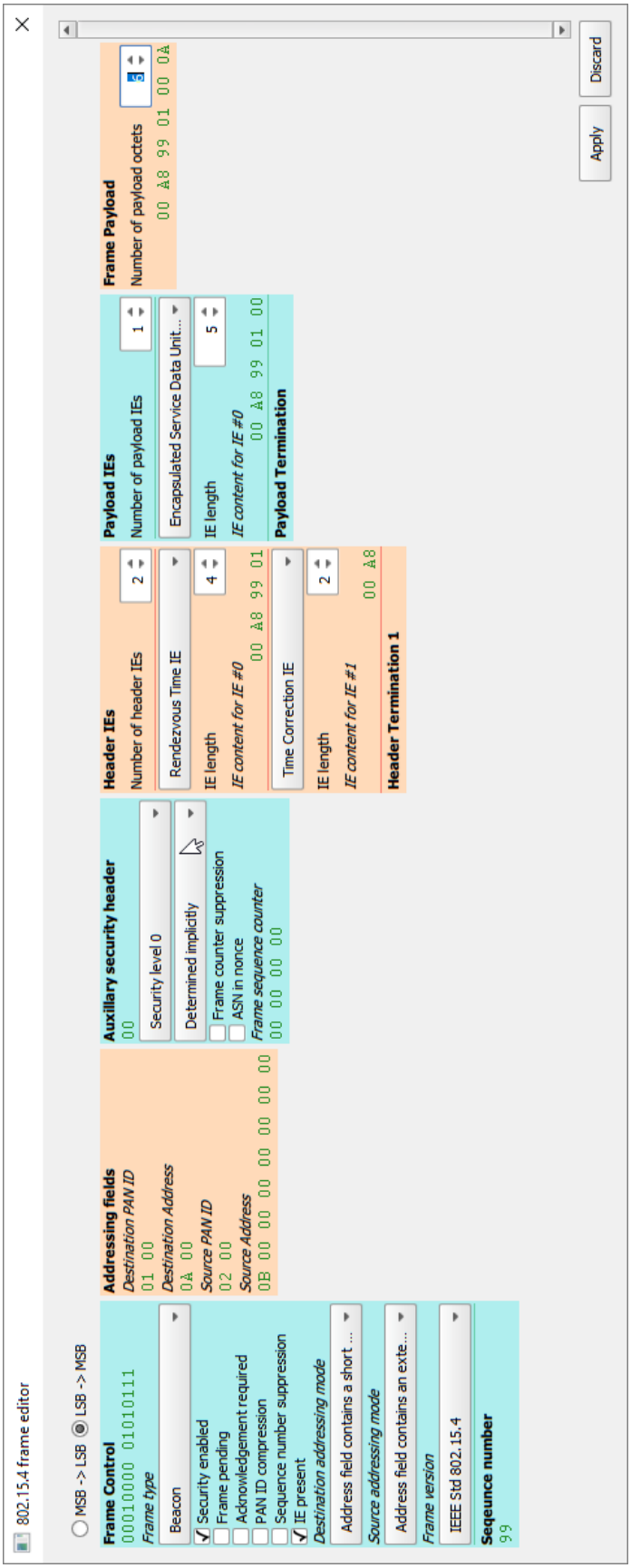


Figure 5: 802.15.4 frame editor.

At the top of the frame editor are two radio buttons labelled *'MSB -> LSB*' and '*LSB -> MSB*'. These determine how the data to be transmitted is displayed in the frame editor window. If '*LSB -> MSB*' is selected then all bit sequences and hex strings start with the LSB, ie transmission order. If '*MSB -> LSB*' is selected, then all bit sequences and hex strings start with the MSB.

The frame editor window is divided into six columns:

1. The left hand column contains the frame control field information and the sequence number (if present)
2. The second column contains addressing information
3. The third column contains information relating to the auxiliary security header field
4. The fourth column contains the header IEs
5. The fifth column contains the payload IEs
6. The sixth column contains the payload

Not all columns may necessarily be visible, depending on the settings within the frame control field. When columns are not required, remaining columns are shuffled to the left.

The FCS is not shown but is automatically calculated and appended. Only support for a 16bit FCS is currently provided.

It is possible to construct frames which are longer than the maximum 127 octets of the PHY PPDU payload. Such frames will be silently truncated to 127 octets.

7.3.6.2 Programming the frame control field

The frame control field is programmed using the controls in the first column, which is always visible. Each bit within the frame control field can be set either through an appropriately named checkbox or through a combo-box. The resulting bit sequence is displayed at the top of the column. Some checkboxes may be hidden when they are not required. For some combinations of frame type and frame version, certain bits in the frame control field may have fixed values. In this case, clicking the corresponding checkbox will have no effect.

The frame control field may also be programmed by directly typing over the bit sequence displayed at the top of the column.

7.3.6.3 Programming the sequence number

When a sequence number is required in the frame, it is shown at the bottom of the first column, below the frame control field. The sequence number is displayed as a hex string and can be edited directly by typing over the displayed digits.

7.3.6.4 Programming the addressing fields

The addressing fields relevant to the frame are displayed in the second column, when required. Each address is shown as a hex string. The addresses may be edited by directly typing over the hex strings.

7.3.6.5 Programming the auxiliary security header field

The auxiliary security header field column will be visible when the security enable bit in the frame control field is set.

The security control field is shown as a hex string at the top of the column. The bits within this field may be set using the combo-boxes and checkboxes below it. Alternatively, the security control field may be edited by typing directly over the hex string.

If a frame sequence counter and key ID are required, then these are shown as hex strings at the bottom of the column. These can be edited by directly typing over the hex strings.

7.3.6.6 Programming the header IEs

Whenever the IE present bit in the frame control field is set, the header IEs column will be visible. The number of header IEs in the frame is determined by the spin box at the top of the column. A maximum of 16 header IEs is supported.

The contents of each header IE are listed separately. For each header IE it is possible to select the header IE type through a combo box and the number of octets in the header IE content field via a spin box. If the contents field is of non-zero length, then the contents are displayed as a hex string which may be edited directly. No support is provided in the entry of valid header IE contents; it is the user's responsibility to ensure that the data entered here is valid.

If a header IE terminator is required, then this is indicated at the bottom of the header IEs' column, along with its type. The need for a header IE terminator is automatically calculated.

If the number of header IEs is set to zero, then the number of payload IEs will be forced to at least one.

7.3.6.7 Programming the payload IEs

Whenever the IE present bit in the frame control field is set, the payload IEs column will be visible. The number of payload IEs in the frame is determined by the spin box at the top of the column. A maximum of 16 payload IEs is supported.

The contents of each payload IE are listed separately. For each payload IE it is possible to select the payload IE type through a combo box and the number of octets in the payload IE content field via a spin box. If the contents field is of non-zero length, then the contents are displayed as a hex string which may be edited directly. No support is provided in the entry of valid payload IE contents; it is the user's responsibility to ensure that the data entered here is valid.

If a payload IE terminator is required, then this is indicated at the bottom of the payload IEs' column. The need for a payload IE terminator is automatically calculated.

If the number of payload IEs is forced to zero, then the number of header IEs will be forced to at least one.

7.3.6.8 Programming the payload

The right most column, which is always present, shows the frame payload. The spin box at the top of the column is used to determine the number of octets in the payload. The actual payload contents are displayed as a hex string at the bottom of the column. No support is provided for entering valid payload contents; it is the user's responsibility to ensure that the payload contents are valid. The payload data may be edited directly by typing over the hex string.

7.3.6.9 Frame editor dialog buttons

The buttons along the bottom of the frame editor dialog perform the following functions:

1. *Apply*. The contents of the frame editor are copied to the payload field of the main window and the frame editor window is closed.
2. *Discard*. The contents of the frame editor window are discarded, the payload field of the main window remains unchanged and the frame editor window is closed.

7.3.7 Packet count

The signal generator can be set to transmit 802.15.4 packets forever or a finite number of packets can be specified. The specification of a finite number of packets is useful if it is desired to measure the PER on a receiving DUT.

No packets are transmitted from the unit until either:

1. The '*Run'* button in the tool bar is pressed
2. The '*Run'* button in the tool bar is pressed and the signal generator is triggered by toggling lines on its digital interface

If a finite number of packets have been specified, then the signal generator will continue to run even after all the packets have been transmitted. To generate another sequence of packets it is necessary to either:

1. Stop the signal generator by activating the '*Stop'* button in the tool bar and then restarting the signal generator using the '*Run'* button
2. Toggling digital lines to stop the generator and then toggling digital lines to restart the signal generator

The minimum number of packets which can be set is 1. If not in repeat forever mode, the maximum number of packets which can be sent is 65535.

7.3.8 Packet interval

The minimum packet interval is dependent on both the payload length and the packet timing jitter. The maximum packet interval is 500ms.

The packet interval may change automatically if the payload length or packet timing jitter are modified. If this occurs, then the packet interval will be set to the lowest time interval which encompasses the entire packet, including ramp up/down times plus any potential timing jitter.

7.3.9 Packet timing jitter

The wanted 802.15.4 packets are normally transmitted at fixed intervals determined by the packet interval control. However, it is possible to add random timing jitter to the nominal transmission times. Two types of random timing jitter can be added:

1. Uniformly distributed jitter.
2. Gaussian distributed jitter (approximate).

For each distribution, the peak jitter can be specified. The maximum peak jitter which can be specified is 20ms.

7.3.10 Carrier frequency offset

The carrier frequency of the wanted 802.15.4 packetized signals may be offset. The maximum offset which can be selected is ±250kHz.

7.3.11 Carrier frequency drift

A sinusoidal carrier frequency drift can be applied to each packet. This drift is in addition to the carrier frequency offset. The carrier frequency drift is zero at the start of the packet and then follows a sinusoidal path with the peak value determined by the '*Drift magnitude*' spin box and the frequency of the sinusoid determined by the '*Drift rate*' spin box.

The maximum value of the drift magnitude is ±70kHz. The maximum value of the drift rate is 2440Hz.

7.3.12 Amplitude imbalance

An amplitude imbalance can be imposed between the I and Q channels of the O-QPSK modulator. The magnitude of the amplitude imbalance is expressed in dBs and is determined by the setting of the '*Amplitude imbalance*' spin box. The maximum imbalance which can be specified is 3dB.

7.3.13 Quadrature error

The angle between the I and Q channels in the O-QPSK modulator can be offset from 90° by using the '*Quadrature error*' spin box. The maximum phase error which can be specified is ±10°.

7.3.14 Symbol timing error

The symbol timing error within a packet can be set using the '*Symbol timing error*' spin box. This only alters the symbol timing error within a packet; the timing between packets is unaffected. The maximum symbol timing error which can be imposed is ±100ppm.

7.3.15 Ramp time

The time taken for the power to ramp up and down at the start and end of the packet can be controlled using the '*Ramp time*' spin box. The power ramp profile follows a Chebyshev window. The minimum ramp time is 1.1µs and the maximum ramp time is 10µs.

7.3.16 Front and back porch

After the power ramp, there is a period of unmodulated carrier prior to the commencement of the modulated packet preamble. This period is referred to as the front porch. After the last chip of the payload has been sent, there is a period of unmodulated carrier prior to the down ramp. This period is referred to as the back porch. The length of both the front and back porch may be set independently using the '*Front porch*' and '*Back porch'* spin boxes. The minimum lengths are 0µs and the maximum lengths are 25µs.

7.3.17 Chip error rate

By default, the wanted signal modulator faithfully outputs the chips as defined by the packet payload. However, it is possible to impose random chip errors on the stream entering the modulator. These errors are uncorrelated. The chip error rate can be specified using the '*Chip error rate*' spin box. The maximum chip error rate is 0.0625. The resolution of the chip error rate is 0.000001.

7.3.18 Digital output

To enable other test equipment to be synchronised with Cuprite's transmissions, it is possible to toggle digital output lines when a packet is being transmitted. The selected lines will be low between transmissions and go high during the transmission.

The *TLF3000* unit has 8 digital output lines. All lines are available for signalling packet transmission. Lines are selected by toggling '*X*' to '*1*' in the appropriate box.

If a digital output line is specified as monitoring both wanted signal transmissions and modulated interferer transmissions, then the state of the line is the logical OR of the two signals.

The IO voltage for the lines may be either:

1. An internal 3.3 V generated supply
2. An external supply in the range 0.8 V to 3.5 V

The selection of the IO voltage is performed under '*Hardware trigger*'

7.4 Programming the modulated interferer signal

7.4.1 Overview

Cuprite can generated either a continuous or packetized modulated interferer signal. The interferer signal is modulated using the 802.15.4 spreading codes and O-QPSK. This signal is required to perform receiver C/I and intermodulation tests. The modulated interferer may also be used to characterise the ED function of the receiver.

To turn the modulated interferer signal on or off, toggle the switch to the left of the '*Interferer*' text.

To program the modulated interferer signal, expand the '*Interferer*' signal menu by clicking on it:

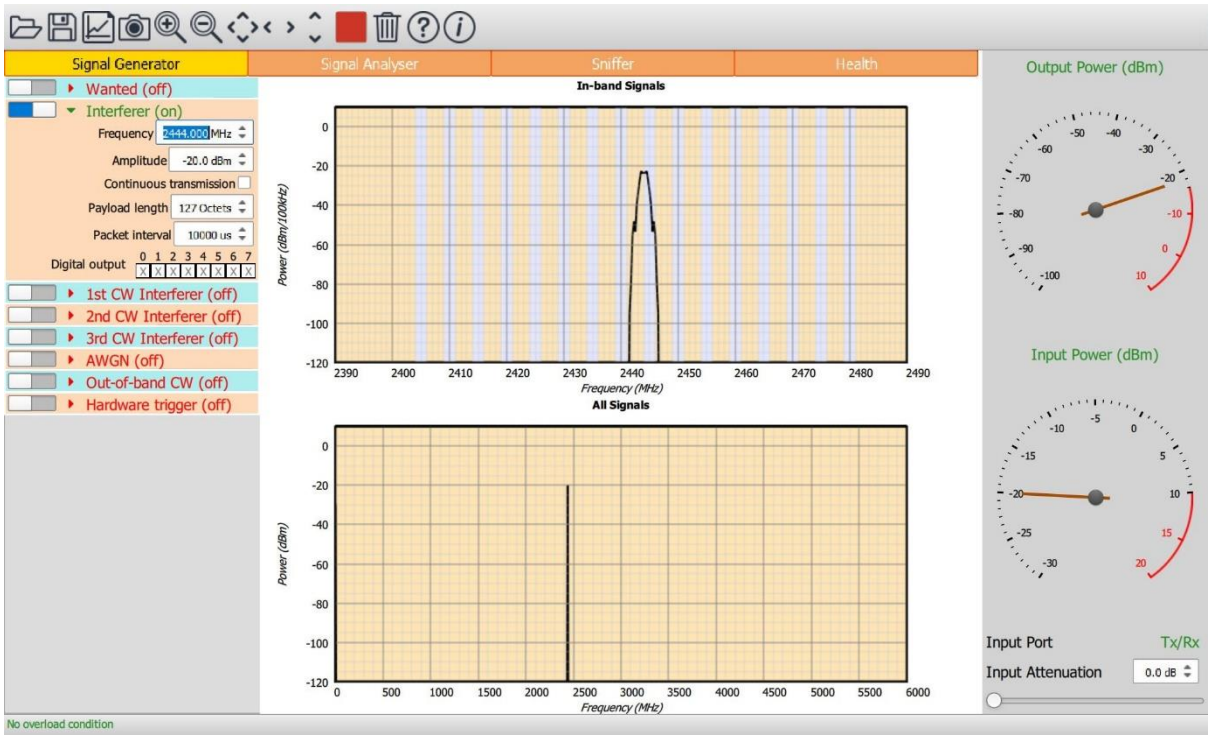


Figure 6: Programming the modulated interferer signal.

7.4.2 Carrier frequency

The frequency of the carrier can be set by using the '*Frequency*' spin box. The interferer signal is not constrained to the 802.15.4 channels. Its frequency may be set anywhere from 2395MHz to 2485MHz in steps of 1kHz,

7.4.3 Amplitude

The amplitude of the modulated interferer signal can be adjusted from -120dBm to 0dBm. The total combined output power of the unit within the 2.4GHz ISM band is 0dBm. Therefore, if other signals are active, the maximum output power for the modulated interferer signal will be reduced to maintain the peak output power within the 0dBm limit.

7.4.4 Continuous or packetized

The interferer signal can be either be continuous or packetized. If continuous is selected, then the transmission has a normal packet ramp up and preamble, but the packet "payload" is an infinitely long PRBS15 sequence. If the interferer is packetized, then the transmission is a standard 802.15.4 transmission with a section of a PRBS15 sequence in the PHY PPDU payload.

If the packetized operation is selected, then the number of octets in the payload can be selected using the '*Payload length*' spin box and the interval between the start of packets by the '*Packet interval*' spin box. The payload length is restricted to 127 octets and the maximum packet interval to 500ms. The minimum packet interval is determined by the payload length; changing the payload length may alter the selected packet interval.

7.4.5 Digital output

To enable other test equipment to be synchronised with Cuprite's transmissions, it is possible to toggle digital output lines when the modulated interferer signal is being transmitted. The selected lines will be low prior to transmission and go high during the transmission.

The *TLF3000* unit has 8 digital output lines. All lines are available for signalling modulated interferer transmission. Lines are selected by toggling '*X*' to '*1*' in the appropriate box.

If a digital output line is specified as monitoring both wanted signal transmissions and modulated interferer transmissions, then the state of the line is the logical OR of the two signals.

The IO voltage for the lines may be either:

1. An internal 3.3 V generated supply
2. An external supply in the range 0.8 V to 3.5 V

The selection of the IO voltage is performed under '*Hardware trigger*'

7.5 Programming the in-band CW signals

7.5.1 Overview

Cuprite can generate up to 3 in-band (i.e. 2395MHz to 2485MHz) CW interferer signals. These signals are required to perform receiver intermodulation tests. The CW signals may also be used to characterise the ED function of a receiver.

To turn an in-band CW interferer signal on or off, toggle the switch to the left of the 'n^{th} *CW interferer*' text.

To program an in-band CW interferer signal, expand the 'n^{th} CW interferer' signal menu by clicking on it:

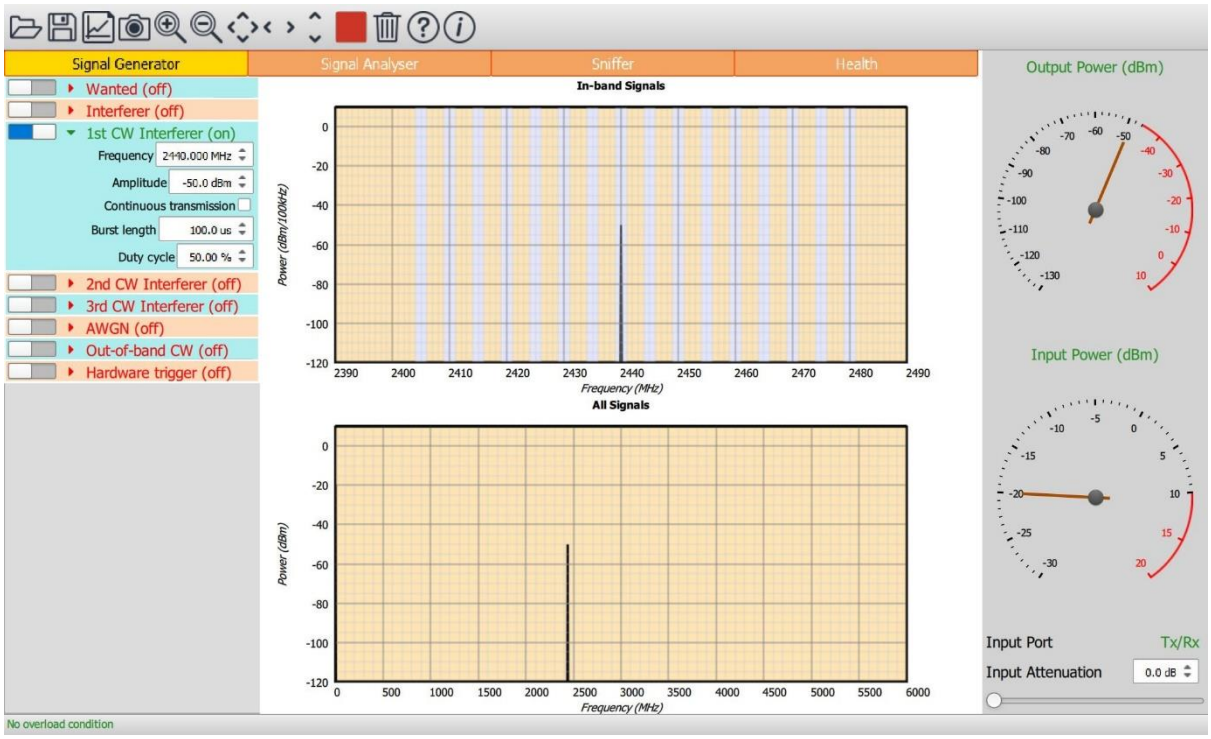


Figure 7: Programming an in-band CW interferer signal.

7.5.2 Frequency

The frequency of the CW signal can be set by using the '*Frequency'* spin box. The CW signal is not constrained to the 802.15.4 channels. Its frequency may be set anywhere from 2395MHz to 2485MHz in steps of 1kHz,

7.5.3 Amplitude

The amplitude of the in-band CW interferer signal can be adjusted from -120dBm to 0dBm. The total combined output power of the unit within the 2.4GHz ISM band is 0dBm. Therefore, if other signals are active, the maximum output power for the in-band CW interferer signal will be reduced to maintain the peak output power within the 0dBm limit.

7.5.4 Pulsed operation

Each CW signal can be independently set to either continuous or pulsed. If pulsed operation is selected, then the length of each pulse is set using the '*Burst length*' spin box. The minimum burst length is 0.1µs and the maximum burst length is 1.6s. The duty cycle of the signal is set using the '*Duty cycle*' spin box.

The commencement and cessation of each pulse is abrupt; there is no power ramp up or down. As a consequence, power may be splattered across the band at the start and end of each burst.

7.6 Programming the AWGN source

7.6.1 Overview

The AWGN source provides uniform output power from 2395MHz to 2485MHz. This source can be used to characterise the ED and LQI functions of a receiver. The AWGN source can be continuous or pulsed.

To turn the AWGN source on or off, toggle the switch to the left of the '*AWGN*' text.

To program the AWGN source, expand the '*AWGN*' signal menu by clicking on it:

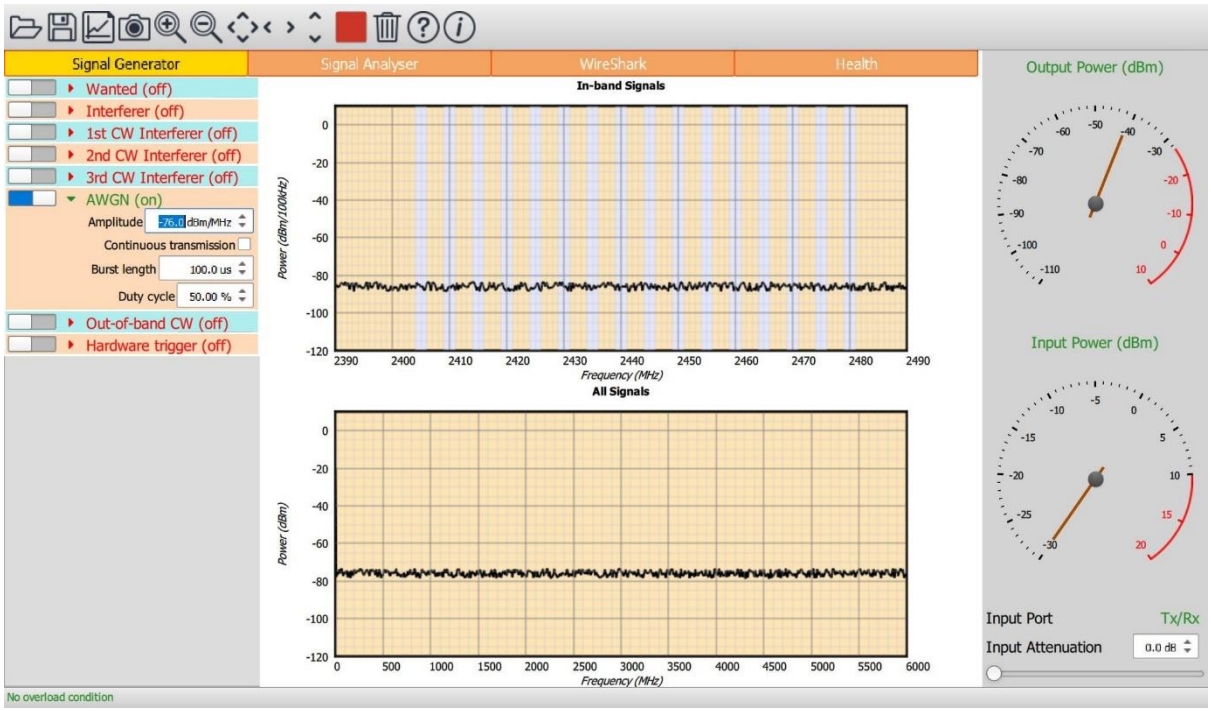


Figure 8: Programming the in-band AWGN source.

7.6.2 Amplitude

The amplitude of the AWGN source can be set in the range -162.1dBm/MHz to -39.1dBm/MHz. The total combined output power of the unit within the 2.4GHz ISM band is 0dBm. Therefore, if other signals are active, the maximum output power for the AWGN source will be reduced to maintain the peak output power within the 0dBm limit.

7.6.3 Pulsed operation

The AWGN source may be set to either continuous or pulsed. If pulsed operation is selected, then the length of each pulse is set using the '*Burst length*' spin box. The minimum burst length is 0.1µs and the maximum burst length is 1.6s. The duty cycle of the signal is set using the '*Duty cycle*' spin box.

7.7 Programming the out-of-band CW signal

Cuprite can generate an out-of-band CW interferer signal. This signal is required to perform receiver blocking tests.

To turn the out-of-band CW interferer signal on or off, toggle the switch to the left of the '*Out-of-band CW*' text.

To program the out-of-band CW interferer signal, expand the '*Out-of-band CW*' signal menu by clicking on it:

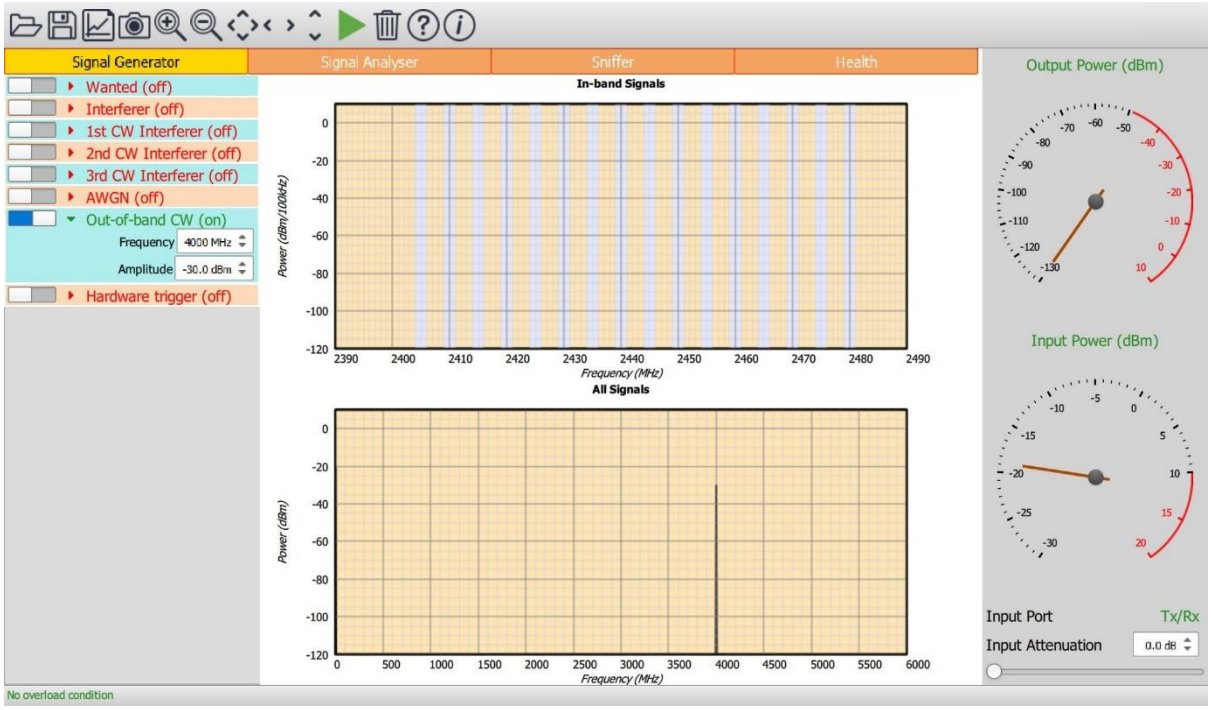


Figure 5: Programming the out-of-band CW interferer signal.

7.7.1 Frequency

The frequency of the out-of-band CW interferer signal can be set by using the frequency spin box. The frequency can be set to any integer MHz between 24MHz and 6GHz.

7.7.2 Amplitude

The amplitude of the out-of-band CW interferer signal can be adjusted from -50dBm to -28dBm.

The amplitude of the out-of-band CW interferer signal does not impact the maximum amplitude of the in-band signals. The energy of the out-of-band CW interferer signal is excluded from the power indicated by the '*Output power*' gauge in the monitor panel.

7.8 Hardware trigger

7.8.1 Overview

The signal generator output can be started or stopped by toggling the '*Play*' button on the toolbar. It is also possible to start or stop the signal generator by toggling digital input lines. This feature is useful if the signal generator must be synchronised with other test equipment.

To enable control of the signal generator from the digital input lines, toggle the switch to the left of the '*Hardware trigger*' text.

To program the hardware trigger feature, expand the '*Hardware trigger*' menu by clicking on it:

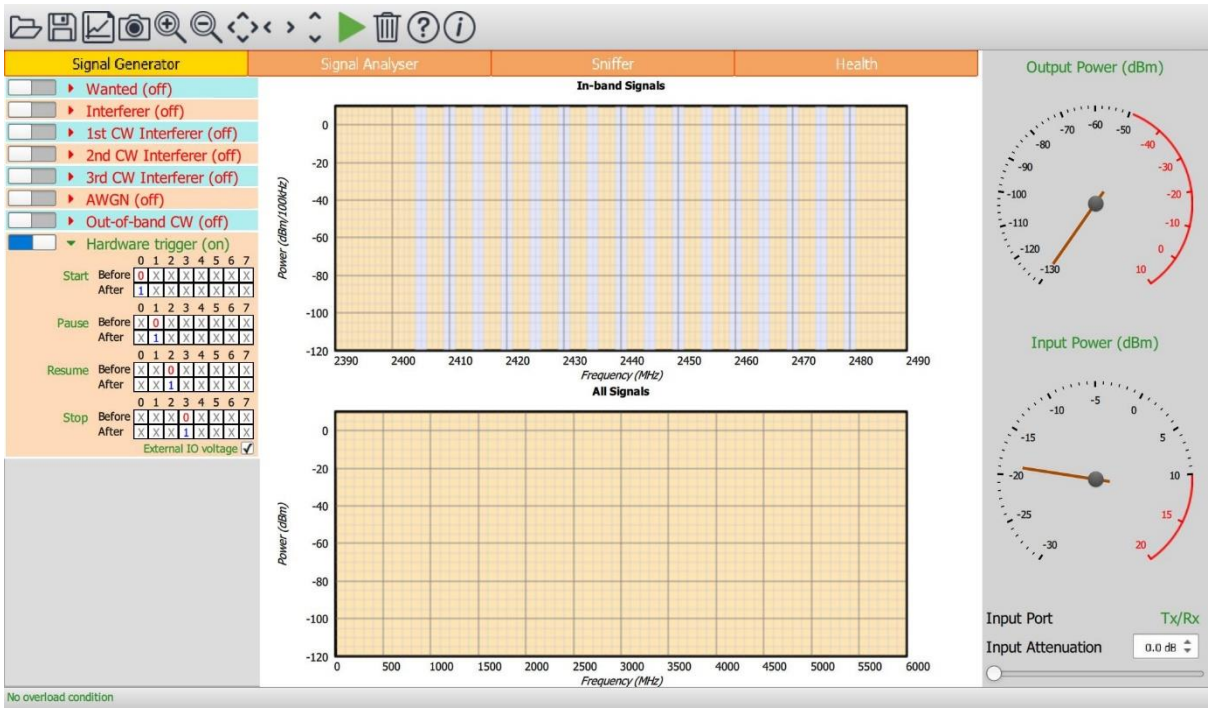


Figure 6: Programming the hardware trigger feature.

7.8.2 Starting the signal generator via digital input lines

The hardware trigger menu contains an item labelled '*Start'*, to the right of which is a table of two rows and 8 columns. Each column in the table represents a digital input line. The top row in the table indicates the state the digital input lines must be in prior to the signal generator starting. The bottom row in the table indicates the state the digital input lines must be in after the signal generator has started. A '*0*' indicates the corresponding line must be low, a '*1'* indicates the line must be high and an '*X*' indicates 'don't care'. If the digital input lines transition from a state which matches the '*before'* row to a state which matches the '*after'* row and the signal generator was in the stopped state, then the signal generator will be started.

When the digital signal generator is started, all the selected signals are turned on. The signal generator will then start to issue the specified number of 802.15.4 packets, if the '*Wanted*' signal has been selected.

7.8.3 Pausing the signal generator via digital input lines

The hardware trigger menu contains an item labelled '*Pause'*, to the right of which is a table of two rows and 8 columns. Each column in the table represents a digital input line. The top row in the table indicates the state the digital input lines must be in prior to the signal generator pausing. The bottom row in the table indicates the state the digital input lines must be in after the signal generator has paused. A '*0*' indicates the corresponding line must be low, a '*1*' indicates the line must be high and an '*X*' indicates 'don't care'. If the digital input lines transition from a state which

matches the '*before'* row to a state which matches the '*after'* row and the signal generator was in the running state, then the signal generator will be paused.

When the digital signal generator is paused, all the selected signals are turned off. If the '*Wanted*' signal has been selected, then the number of 802.15.4 packets already transmitted is remembered.

7.8.4 Resuming the signal generator via digital input lines

The hardware trigger menu contains an item labelled '*Resume'*, to the right of which is a table of two rows and 8 columns. Each column in the table represents a digital input line. The top row in the table indicates the state the digital input lines must be in prior to the signal generator resuming. The bottom row in the table indicates the state the digital input lines must be in after the signal generator has resumed. A '*0*' indicates the corresponding line must be low, a '1' indicates the line must be high and an '*X*' indicates 'don't care'. If the digital input lines transition from a state which matches the '*before'* row to a state which matches the '*after'* row and the signal generator was in the paused state, then the signal generator will resume operation..

When the digital signal generator resumes operation, all the selected signals are turned on. If the '*Wanted'* signal has been selected, then the signal generator will start transmitting the number of packetized 802.15.4 signals which were remaining when the previous '*Pause'* was issued.

7.8.5 Stopping the signal generator via digital input lines

The hardware trigger menu contains an item labelled '*Stop'*, to the right of which is a table of two rows and 8 columns. Each column in the table represents a digital input line. The top row in the table indicates the state the digital input lines must be in prior to the signal generator stopping. The bottom row in the table indicates the state the digital input lines must be in after the signal generator has stopped. A '*0*' indicates the corresponding line must be low, a '*1*' indicates the line must be high and an '*X*' indicates 'don't care'. If the digital input lines transition from a state which matches the '*before'* row to a state which matches the '*after'* row then the signal generator will stop, irrespective of the state it was previously in.

When the digital signal generator is stopped, all the selected signals are turned off. If the '*Wanted*' signal has been selected, then the number of 802.15.4 packets transmitted is reset to zero.

7.9 Saving and restoring settings

The current signal generator settings can be saved by clicking the '*Save'* button on the toolbar. Select the '*Signal generator settings (*.sgs)*' file type to save the current settings.

An existing signal generator settings file (*.sgs) can be opened using the '*Open'* button on the toolbar.

The signal generator settings file (*.sgs) is an XML file. It is not recommended that this file be edited manually. If it needs to be modified, open it from the signal generator, modify the required parameters and re-save.

8 Signal Analyzer Mode.

8.1 Overview

In signal analyzer mode, the Cuprite application is able to analyze incoming signals against the 802.15.4 specification. The application is able to analyze both conducted and off-air signals. All 16 802.15.4 channels are monitored simultaneously, hence there is no requirement to program the signal analyzer to look on a specified channel. The signal analyzer accumulates results separately for each channel and packet length. This permits the results to be filtered and displayed in a number of different ways.

The left hand mode control panel is divided into two separate tabs:

1. *Collection*. This tabs contains the parameters which define which signals will be collected and processed.
2. *Analysis*. This tabs contains the parameters which define how the captured results will be displayed.

The central graphics area is used to plot the results in a manner defined by the parameters under the analysis tab.

Below the '*Analysis'* tab is a results table which displays statistics of the test quantities. These results are filtered by the parameters set under the '*Analysis'* tab in the mode control panel. ***If no results are displayed this may be because the analysis filter settings are inconsistent with the packets being received.***

The receiver port and front-end attenuation are set using the controls in the monitor panel on the right hand side of the window.

Data collection is started/stopped by toggling the '*Play'* button in the toolbar.

The '*Clear'* button in the toolbar will discard all results which have been collected.

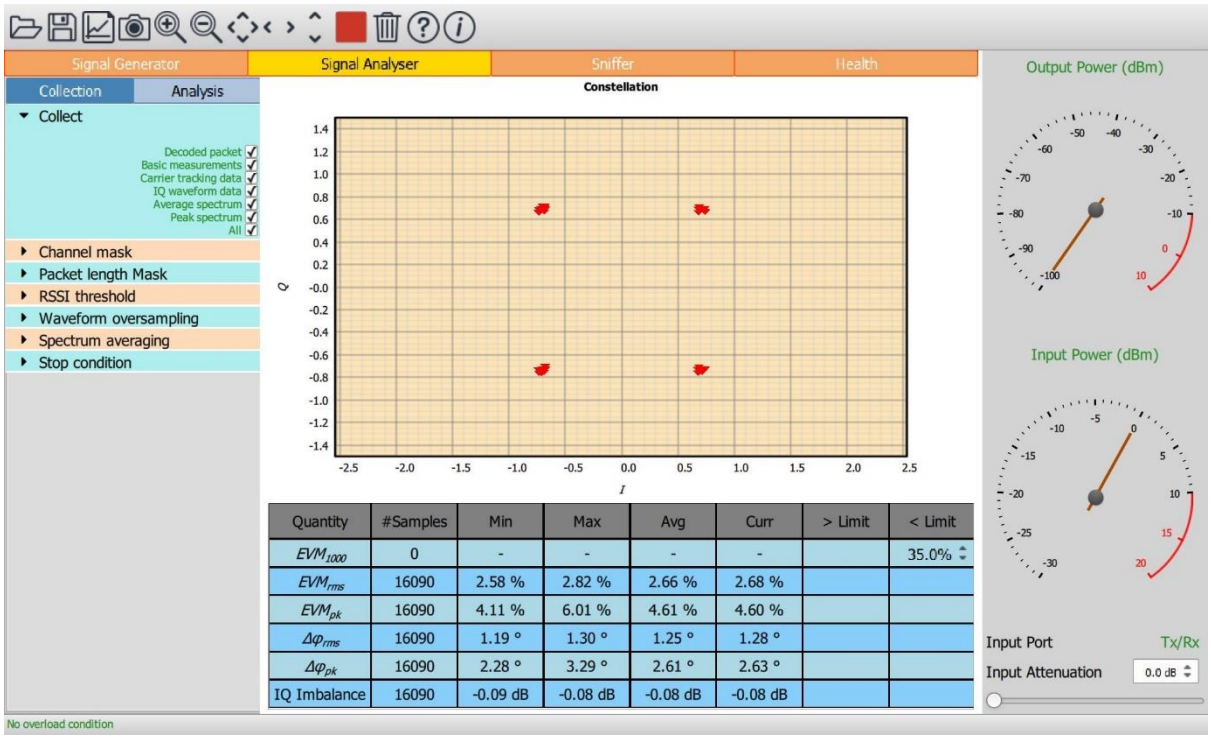


Figure 7: Cuprite GUI signal analyzer mode.

8.2 RF connections

The signal analyzer can monitor signals on either the '*Tx/Rx*' port or the '*Monitor In*' port. See section 8.3.9 on setting the RF input port and section 8.3.10 on setting the receiver frontend attenuation.

8.3 Programming data collection

8.3.1 Overview

The data to be collected is determined the settings of the parameters under the '*Collection'* tab of the mode control panel on the left hand side of the window.

It is possible to select:

1. Which measurement data should be collected
2. Which RF channels are of interest
3. Which packet lengths are of interest
4. The minimum RSSI reading for collected packets
5. The oversampling rate for waveform data
6. The averaging time for spectral measurements
7. When the data analysis should terminate

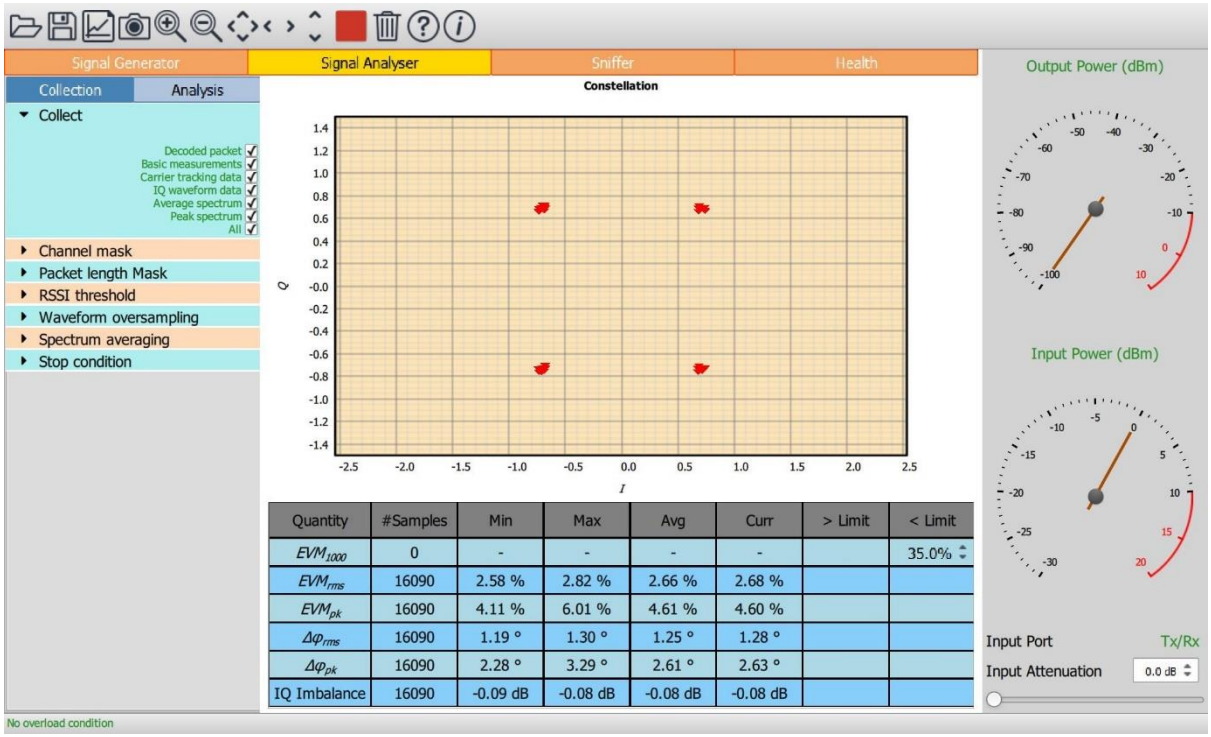
8.3.2 Programming the measurement data to be collected

The '*Collect'* menu permits the choice of the collected measurement data to be made. The following measurement data can be collected by the Cuprite application:

1. *Decoded packet data*. Any packet which is observed on anyone of the 16 RF channels is demodulated and the resulting bit stream passed back to the host. If this data is collected, then it is displayed alongside the IQ waveform data or FM demodulator data when these are plotted, otherwise it is unused in the Cuprite GUI.
2. *Basic measurements*. Basic measurements are returned for each packet which is analyzed. The basic measurement data consist of:
    a. Average power within the packet
    b. Peak power minus average power over the entire packet
    c. Initial carrier frequency offset at start of packet
    d. Lowest carrier frequency offset within packet
    e. Highest carrier frequency offset within packet
    f. Maximum carrier drift rate within packet
    g. Average symbol timing error within packet (if packet payload exceeds 64 octets and at least 32 packets have been observed)
    h. Average EVM over segments of 1000 chips (if packet length exceeds 1000 chips)
    i. Average EVM over packet
    j. Peak EVM over packet
    k. Average phase error over packet
    l. Peak phase error over packet
    m. IQ imbalance over packet
    n. IQ samples for each offset constellation point within the packet
3. *Carrier tracking data*. This data is extracted from the carrier tracking loop within the Cuprite demodulator. It can be plotted to show how the estimated carrier frequency varies throughout the packet,
4. *IQ waveform data*. Consists of normalized IQ samples commencing 40µs prior to the start of the packet and finishing 40µs after the end of the packet. The IQ waveform data can also be FM demodulated to enable the frequency deviation to be plotted vs time (ie an MSK interpretation of the 802.15.4 O-QPSK signal).
5. *Average spectrum*. This option returns a 100kHz resolution spectrum starting at 2395MHz and ending at 2485MHz with sampling points at approximately 50kHz intervals. The spectrum is generated using an accurate Gaussian filter and an rms detector. If this option is selected, then PSD measurements are also available.
6. *Peak spectrum*. This option returns the a 100kHz resolution spectrum starting at 2395MHz and ending at 2485MHz with sampling points at approximately 50kHz intervals. The spectrum is generated using an accurate Gaussian filter and a peak detector.

Each of the above options can be individually selected using the corresponding checkboxes.

The rate at which packets can be analyzed depends on how fast data can be streamed from the TLF3000 to the host. By minimising the measurement options selected, the rate at which packets can be analyzed can be dramatically increased and hence test time reduced. In particular, collecting IQ waveform data is particularly expensive. To carry out the tests set out in the 802.15.4 specification, only *Basic measurements* and *Average spectrum* need be selected, the remaining options only provide data useful during device characterisation.



Quantity	#Samples	Min	Max	Avg	Curr	> Limit	< Limit
EVM_{1000}	0	-	-	-	-		35.0%
EVM_{rms}	16090	2.58 %	2.82 %	2.66 %	2.68 %		
EVM_{pk}	16090	4.11 %	6.01 %	4.61 %	4.60 %		
$\Delta\varphi_{rms}$	16090	1.19 °	1.30 °	1.25 °	1.28 °		
$\Delta\varphi_{pk}$	16090	2.28 °	3.29 °	2.61 °	2.63 °		
IQ Imbalance	16090	-0.09 dB	-0.08 dB	-0.08 dB	-0.08 dB		

Figure 8: Specifying the measurement data to be collected.

8.3.3 Programming which RF channels to collect

The '*Channel mask*' menu permits the RF channels on which data is to be collected and processed to be defined. These are specified in terms of 802.15.4 RF channel numbers, starting at 11 (2405MHz) and ending at 26 (2480MHz).

The required RF channels can be selected by either:

1. Ticking the individual channel boxes
2. Using the quick channel group selection buttons:
    a. Clear all
    b. Select all
3. Entering a textual description

The textual description must be of the form:

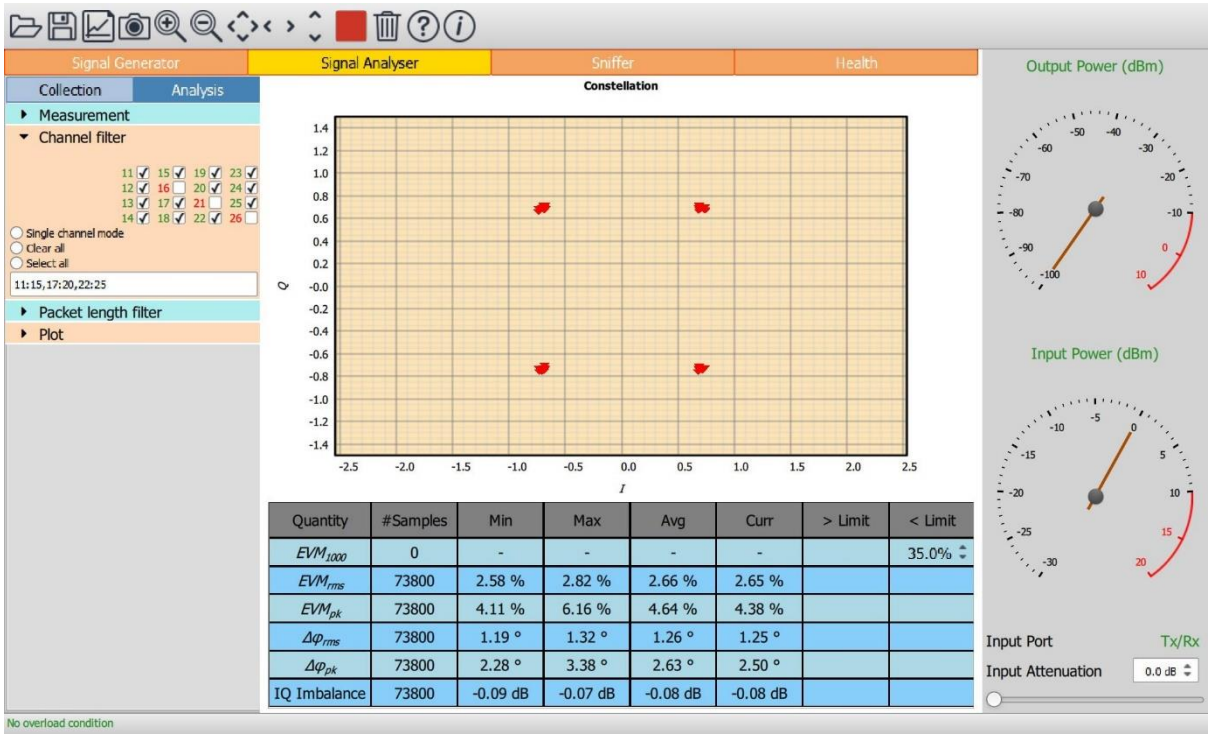
a_{start}:a_{step}: a_{stop}, b_{start}: b_{step}: b_{stop}, ...

This implies that all channels from a_{start} to a_{stop} in steps of a_{step} will be selected, plus all channels from b_{start} to b_{stop} in steps of b_{step}, etc.

If a_{step} is unity, then a_{start}:a_{step}: a_{stop} can be abbreviated to a_{start}: a_{stop}.

If a_{step} is equal to a_{stop} then a_{start}:a_{step}: a_{stop} can be abbreviated to a_{start}.

If the '*Single channel*' mode option is selected, then only one channel can be selected at any time.



Quantity	#Samples	Min	Max	Avg	Curr	> Limit	< Limit
EVM_{1000}	0	-	-	-	-		35.0%
EVM_{rms}	73800	2.58 %	2.82 %	2.66 %	2.65 %		
EVM_{pk}	73800	4.11 %	6.16 %	4.64 %	4.38 %		
$\Delta\varphi_{rms}$	73800	1.19 °	1.32 °	1.26 °	1.25 °		
$\Delta\varphi_{pk}$	73800	2.28 °	3.38 °	2.63 °	2.50 °		
IQ Imbalance	73800	-0.09 dB	-0.07 dB	-0.08 dB	-0.08 dB		

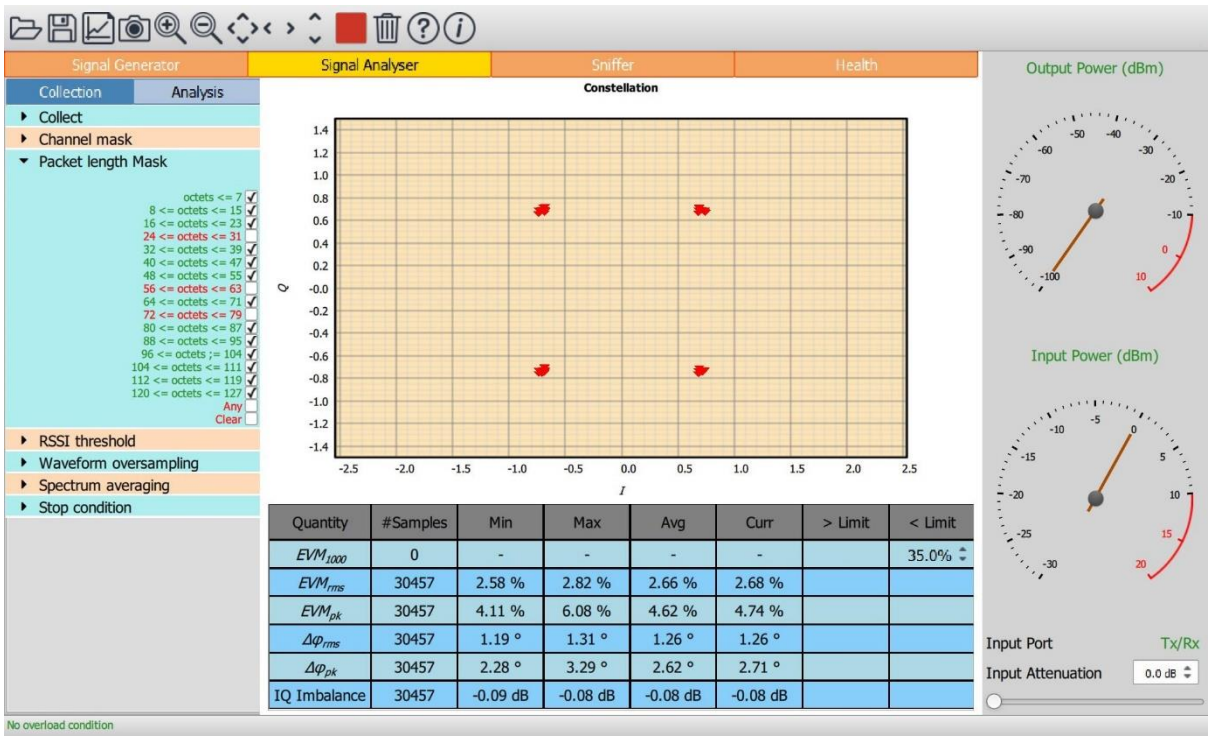
Figure 13: Programming which RF channels to collect.

8.3.4 Programming which packet lengths to collect

The '*Packet length mask*' menu permits the 802.15.4 packet lengths for which data is to be collected and processed to be defined.

Due to memory restrictions, individual packet lengths cannot be specified. Instead, the range of possible packet lengths is divided up into 16 groups, each group spanning 8 contiguous packet lengths. The packet length refers to the number of octets in the PHY PPDU payload, ie it excludes the SHR and PHR fields.

The required packet lengths are selected by ticking the corresponding boxes. If all packet lengths are of interest, then clicking the '*All*' box at the bottom of the menu will select all packet length groups.



Quantity	#Samples	Min	Max	Avg	Curr	> Limit	< Limit
EVM_{1000}	0	-	-	-	-		35.0%
EVM_{rms}	30457	2.58 %	2.82 %	2.66 %	2.68 %		
EVM_{pk}	30457	4.11 %	6.08 %	4.62 %	4.74 %		
$\Delta\varphi_{rms}$	30457	1.19 °	1.31 °	1.26 °	1.26 °		
$\Delta\varphi_{pk}$	30457	2.28 °	3.29 °	2.62 °	2.71 °		
IQ Imbalance	30457	-0.09 dB	-0.08 dB	-0.08 dB	-0.08 dB		

Figure 14: Programming which packet lengths to collect.

8.3.5 Programming the RSSI threshold

The '*RSSI threshold*' menu permits weak signal strength packets to be ignored. This feature is useful when there is prevailing 802.15.4 activity in the test area, since it allows the weak packets from distance devices to be ignored and only the strong packets from the nearby device under test to be analyzed.

The RSSI threshold for packets to be analyzed can be set anywhere from -120dBm to +20dBm in steps of 1dBm.

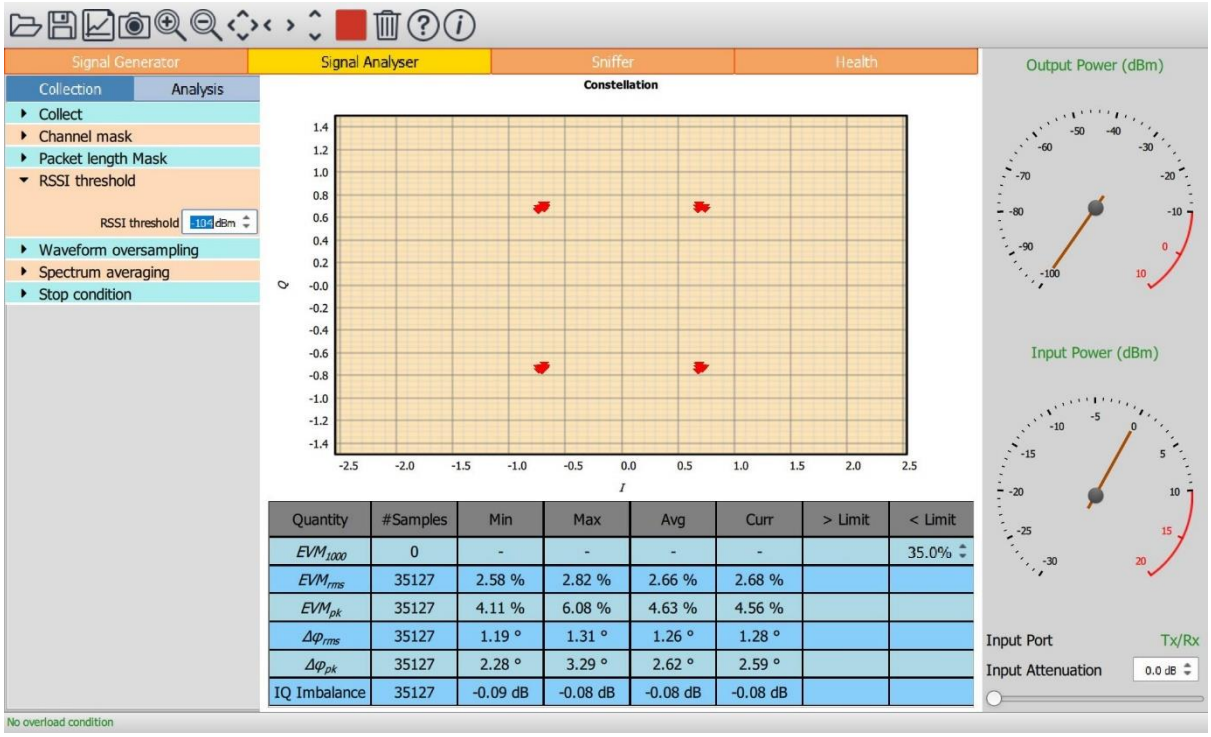
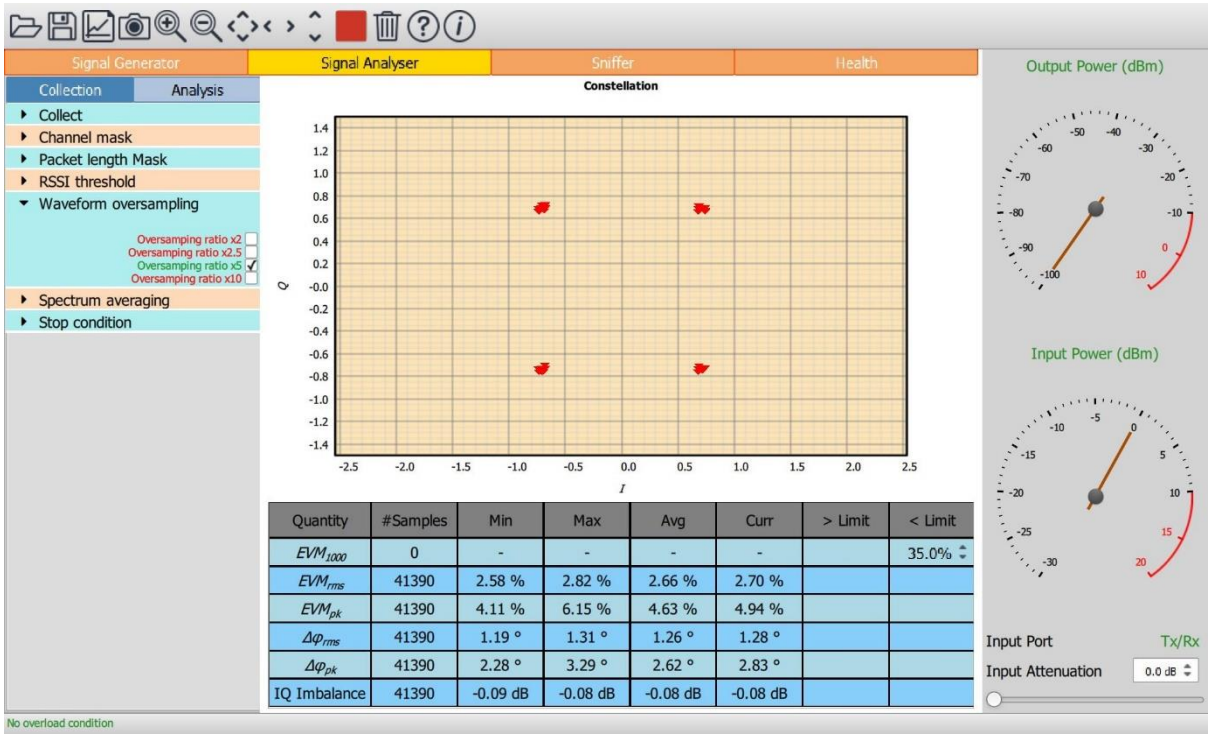


Figure 15: Programming the RSSI threshold.

8.3.6 Programming the waveform oversampling rate

The '*Waveform oversampling*' menu controls the density of IQ samples which are returned if the '*IQ samples*' measurement option has been selected under the '*Collect'* menu. The IQ samples can either be displayed directly or FM demodulated to show a frequency deviation vs time plot (ie an MSK interpretation of the 802.15.4 O-QPSK signal).

Internally each chip is oversampled by a factor of 10, ie a sampling rate of 20MSps. This sampling rate is required for accurate timing recovery and EVM calculations. In order to reduce the quantity of data transferred to the host, it is possible to reduce the 10x oversampling rate to 5x, 2.5x or 2x. This in turn reduces the resolution of the plotted IQ sample data and FM demodulated data.



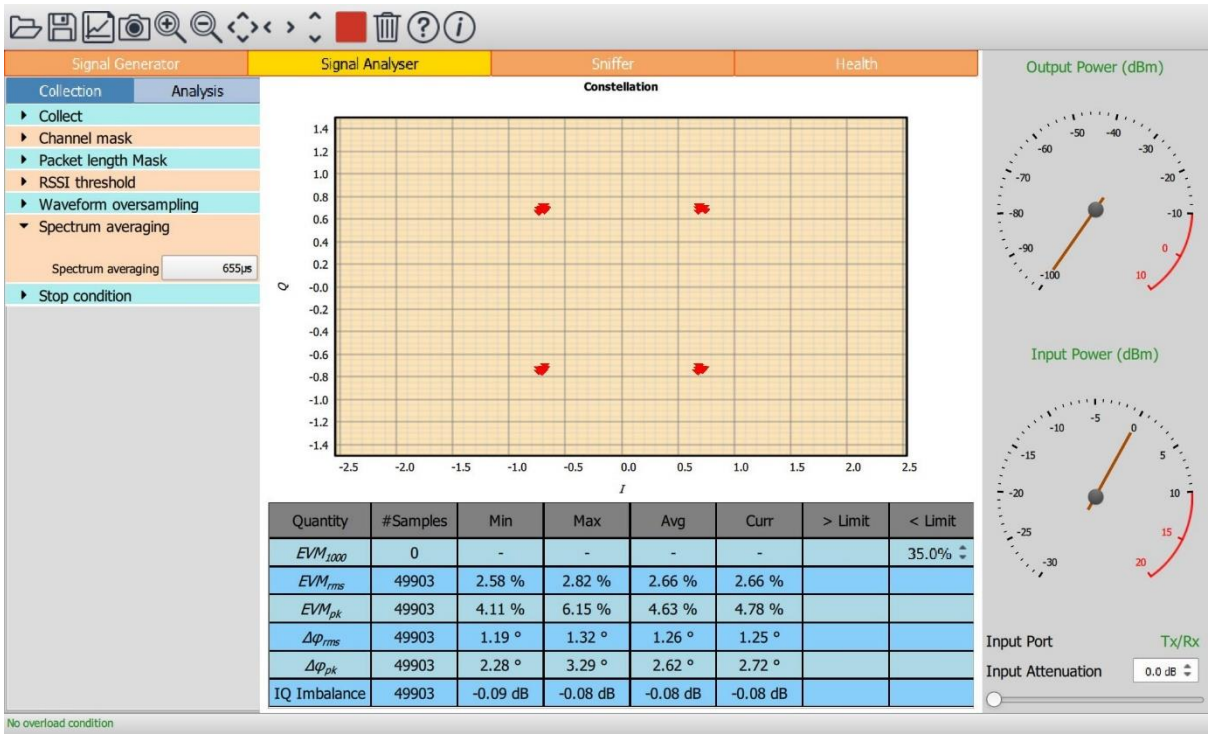
Quantity	#Samples	Min	Max	Avg	Curr	> Limit	< Limit
EVM_{1000}	0	-	-	-	-		35.0%
EVM_{rms}	41390	2.58 %	2.82 %	2.66 %	2.70 %		
EVM_{pk}	41390	4.11 %	6.15 %	4.63 %	4.94 %		
$\Delta\varphi_{rms}$	41390	1.19 °	1.31 °	1.26 °	1.28 °		
$\Delta\varphi_{pk}$	41390	2.28 °	3.29 °	2.62 °	2.83 °		
IQ Imbalance	41390	-0.09 dB	-0.08 dB	-0.08 dB	-0.08 dB		

Figure 16: Programming the waveform oversampling rate.

8.3.7 Programming the spectrum averaging period

The '*Spectrum averaging*' menu permits control of the averaging time and peak hold time for the spectrum analyzer function. The same time interval is used for both averaging and peak hold. The time interval can be varied from 10µs to 6hours. All data received during the averaging interval is processed; there are no dead periods. The shorter interval is useful for capturing artefacts during power ramp up or down whilst the longer intervals can be used to capture infrequent spurious events.

The spectrum analyzer is triggered by the packet synchroniser. Hence the spectrum analyzer will not start until after the SHR has been received. As a consequence, the ramp up of the first packet will not be included in the analysis. To ensure that the packet ramp is analyzed, it is necessary to set the spectrum averaging time to include the SHR of the subsequent packet. It is therefore recommended that the spectrum averaging period is set to at least the packet repetition interval of the device under test.



Quantity	#Samples	Min	Max	Avg	Curr	> Limit	< Limit
EVM_{1000}	0	-	-	-	-		35.0%
EVM_{rms}	49903	2.58 %	2.82 %	2.66 %	2.66 %		
EVM_{pk}	49903	4.11 %	6.15 %	4.63 %	4.78 %		
$\Delta\varphi_{rms}$	49903	1.19 °	1.32 °	1.26 °	1.25 °		
$\Delta\varphi_{pk}$	49903	2.28 °	3.29 °	2.62 °	2.72 °		
IQ Imbalance	49903	-0.09 dB	-0.08 dB	-0.08 dB	-0.08 dB		

Figure 17: Programming the spectrum averaging period

8.3.8 Programming the termination criterion

Once the signal analyzer has been started by toggling the '*Play'* button in the toolbar, it will continue to collect, process and display data until either:

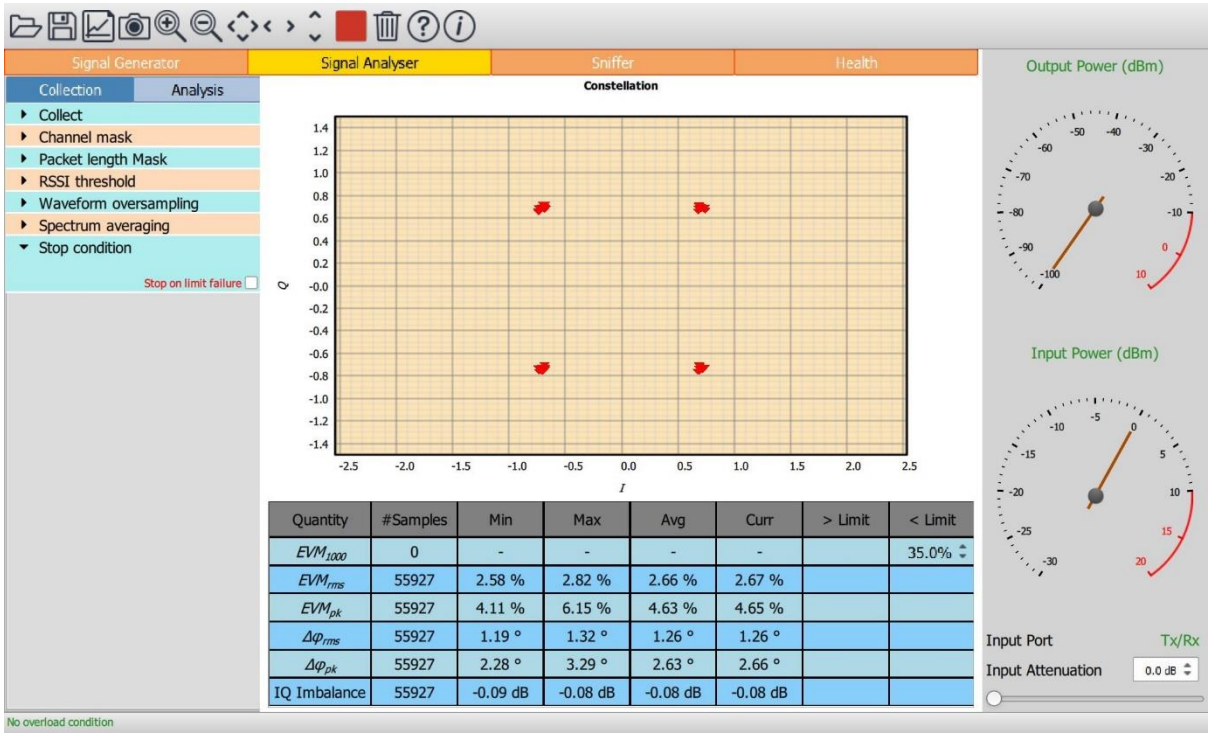
1. The '*Stop'* button in the toolbar is toggled
2. The stop condition has been set to '*Stop on test failure'* and a test limit is failed

The '*Stop on test failure*' condition is set by the single checkbox under the '*Stop condition'* menu.

The test limits are shown in the results table. The penultimate column of the results table displays the lower limit and the final column the upper limit. They can be altered by changing the values in the spin boxes, either by using the up/down arrows or by entering numeric text directly.

When a limit fail is detected, and the stop condition has been set to 'Stop on test failure', then the GUI will automatically alter its graphics and tabular display to reflect the quantity that failed. It is possible that a rogue packet will fail more than one test limit, so the data displayed may only partially reflect the reason why the packet failed.

If '*Decoded packet data'*, '*IQ waveform data'* or *'Carrier tracking data*' collection has been enabled under the '*Collect'* menu, then these data all refer to the packet which failed. This provides an invaluable mechanism for catching rogue packets, particularly when monitoring links off-air, and then determining where in the packet the problem occurred.



Quantity	#Samples	Min	Max	Avg	Curr	> Limit	< Limit
EVM_{1000}	0	-	-	-	-		35.0%
EVM_{rms}	55927	2.58 %	2.82 %	2.66 %	2.67 %		
EVM_{pk}	55927	4.11 %	6.15 %	4.63 %	4.65 %		
$\Delta\varphi_{rms}$	55927	1.19 °	1.32 °	1.26 °	1.26 °		
$\Delta\varphi_{pk}$	55927	2.28 °	3.29 °	2.63 °	2.66 °		
IQ Imbalance	55927	-0.09 dB	-0.08 dB	-0.08 dB	-0.08 dB		

Figure 9: Programming the termination criterion.

8.3.9 Selecting the RF input port

The signal analyzer can monitor signals on either the '*Monitor In*' RF port or the '*Tx/Rx*' RF port. The selection of which port is used is made by clicking the port displayed towards the bottom of the monitor panel.

The '*Monitor In*' port is designed for monitoring signals off-air. The '*Tx/Rx'* port is designed for conducted measurements.

If the monitor panel shows a lack of RF input energy, check that the DUT is connected to the same RF port as selected by the label at the bottom of the monitor panel.

8.3.10 Adjusting the RF frontend attenuation

The RF frontend attenuation is set via either:

1. The slider at the bottom of the monitor panel
2. The spin box at the bottom of the monitor panel

The RF frontend attenuation can be set between 0 and 31.5dB in steps of 0.5dB.

To set the RF attenuation, the '*Input Power*' gauge on the monitor panel must be examined. This shows both the current input signal level (the position of the needle) and the point at which saturation of the *TLF3000* receiver will occur (the red arc). The RF attenuation should be adjusted such that the input signal level is just below the saturation level.

If too little attenuation is applied, then there is a danger that the *TLF3000* receiver will be overloaded. An overload condition on the receiver is indicated by:

1. The needle on the '*Input Power*' gauge on the monitor panel entering the region of the red arc (the input power measurement is only approximate so this is only a rough guide)
2. The title of the '*Input Power*' gauge on the monitor panel turning red
3. The text '*Rx overload*' appearing in red within the status bar at the bottom of the window

If too much attenuation is applied, then the test results may become unreliable. If too much attenuation is applied, then the signal to be analyzed will be pushed down towards the *TLF3000* receiver noise floor and the accuracy of the test results will be compromised.

8.4 Controlling data analysis and presentation

8.4.1 Overview

The Cuprite application accumulates results independently for each:

1. 802.15.4 RF channel
2. Packet length group

The '*Analysis'* tab in the mode control panel determines how these results are filtered and displayed. ***If no results are displayed, then it is possible that the current analysis filter does not correspond to any of the packets which have been collected.***

The '*Measurement'* menu under the '*Analysis'* tab determines which group of measurements will be displayed.

The displayed results are filtered according to the settings of the '*Channel'* and '*Packet length*' menus.

The graphics area shows a plot of one of the test quantities. This may be selected either through the '*Plot'* menu or by highlighting a row in the results table. The '*Plot'* menu also defines the format of the plot.

The results table shows the filtered results for the selected measurement group. It also contains the test limits.

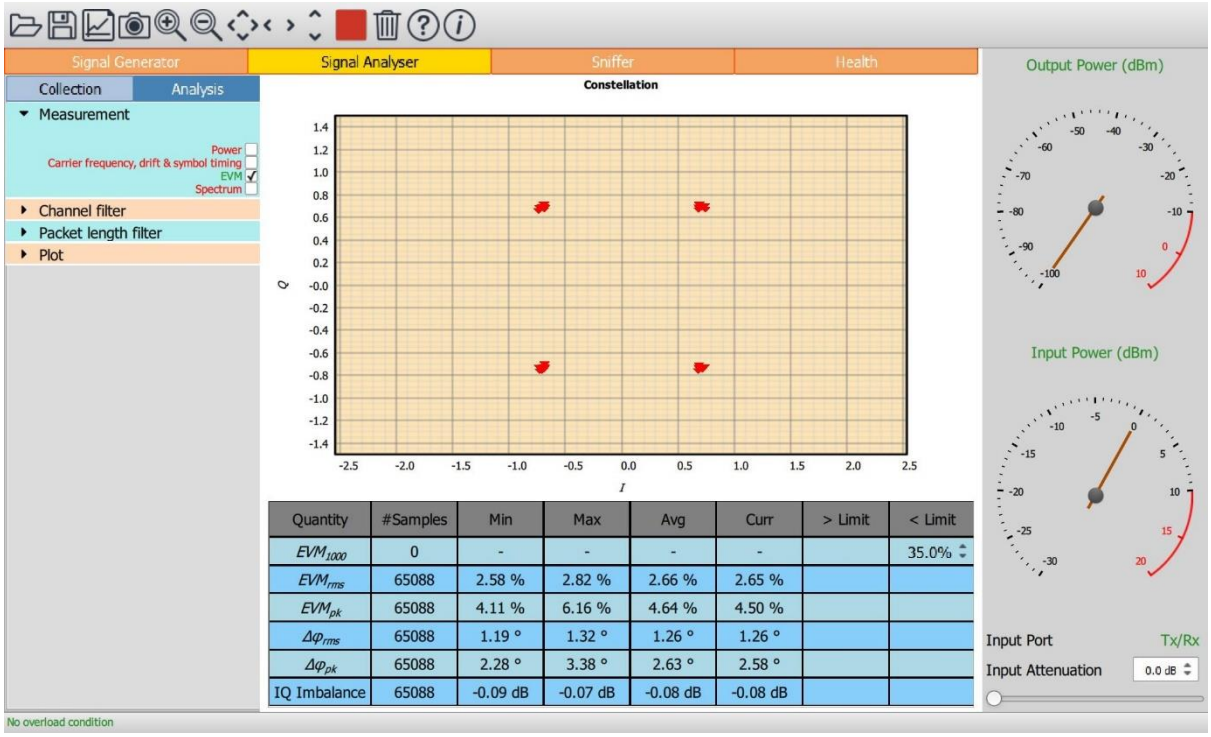
8.4.2 Selecting the measurement group to display

Cuprite divides the 802.15.4 RF PHY transmitter test measurements into five groups:

1. Power measurements, which include:
    a. Average power over a packet, P_{avg}
    b. Peak power minus average power over a packet, P_{pk} - P_{avg}
2. Carrier frequency, drift and symbol timing measurements, which include:
    a. Initial carrier frequency estimated from the packet preamble, *Initial* F_c
    b. Minimum carrier frequency over the packet estimated from the carrier tracking loop, *Min* F_c
    c. Maximum carrier frequency over the packet estimated from the carrier tracking loop, *Max* F_c
    d. Maximum drift rate within the packet, estimated from the carrier tracking loop, *Drift rate*
    e. Average symbol timing error within a packet(only available on packets with a PHY PPDU payload exceeding 64 octets and after 32 packets have been received), *Symbol timing*
3. EVM measurements, which include:
    a. EVM over 1000 chips averaged over each 1000 chip segment within the packet (only available if at least 1000 chips are present in the packet), EVM_{1000}
    b. Average EVM over the entire packet, EVM_{avg}
    c. Peak EVM over the entire packet, EVM_{pk}
    d. Average phase error at each constellation point over the entire packet, $\Delta\varphi_{avg}$
    e. Peak phase error at each constellation point over the entire packet, $\Delta\varphi_{pk}$
    f. IQ imbalance averaged over the entire packet, *IQ imbalance*
4. Spectrum measurements, which include:
    a. The absolute transmitter PSD measurement, as defined in the 802.15.4 specification, PSD_{abs}
    b. The relative transmitter PSD measurement, as defined in the 802.15.4 specification, PSD_{rel}

The Cuprite GUI displays the results from just one of these measurement groups at any one time. The selection of which measurement group to display is accomplished through the '*Measurement*' menu under the '*Analysis*' tab.

If no results are displayed, then it is possible that no packets have been received or that the analysis measurement group selected is incompatible with the choice of collected measurement data.



Quantity	#Samples	Min	Max	Avg	Curr	> Limit	< Limit
EVM_{1000}	0	-	-	-	-		35.0%
EVM_{rms}	65088	2.58 %	2.82 %	2.66 %	2.65 %		
EVM_{pk}	65088	4.11 %	6.16 %	4.64 %	4.50 %		
$\Delta\varphi_{rms}$	65088	1.19 °	1.32 °	1.26 °	1.26 °		
$\Delta\varphi_{pk}$	65088	2.28 °	3.38 °	2.63 °	2.58 °		
IQ Imbalance	65088	-0.09 dB	-0.07 dB	-0.08 dB	-0.08 dB		

Figure 10: Selecting the measurement group to display.

8.4.3 Filtering the displayed results by RF channel

The displayed results can be filtered by RF channel number. This facility may be useful when monitoring a live link and it is suspected that there is a problem with packet transfer on a particular RF channel. It also provides a simple means of comparing test results on different RF channels.

The RF channels used to filter the results are selected via the '*Channel filter*' menu under the '*Analysis*' tab. The channels are number according to the 802.15.4 specification, starting at channel 11 (2405MHz) and ending at channel 26 (2480MHz),

The required RF channels can be selected by either:

1. Ticking the individual channel boxes
2. Using the quick channel group selection buttons:
    a. Clear all
    b. Select all
3. Entering a textual description

The textual description must be of the form:

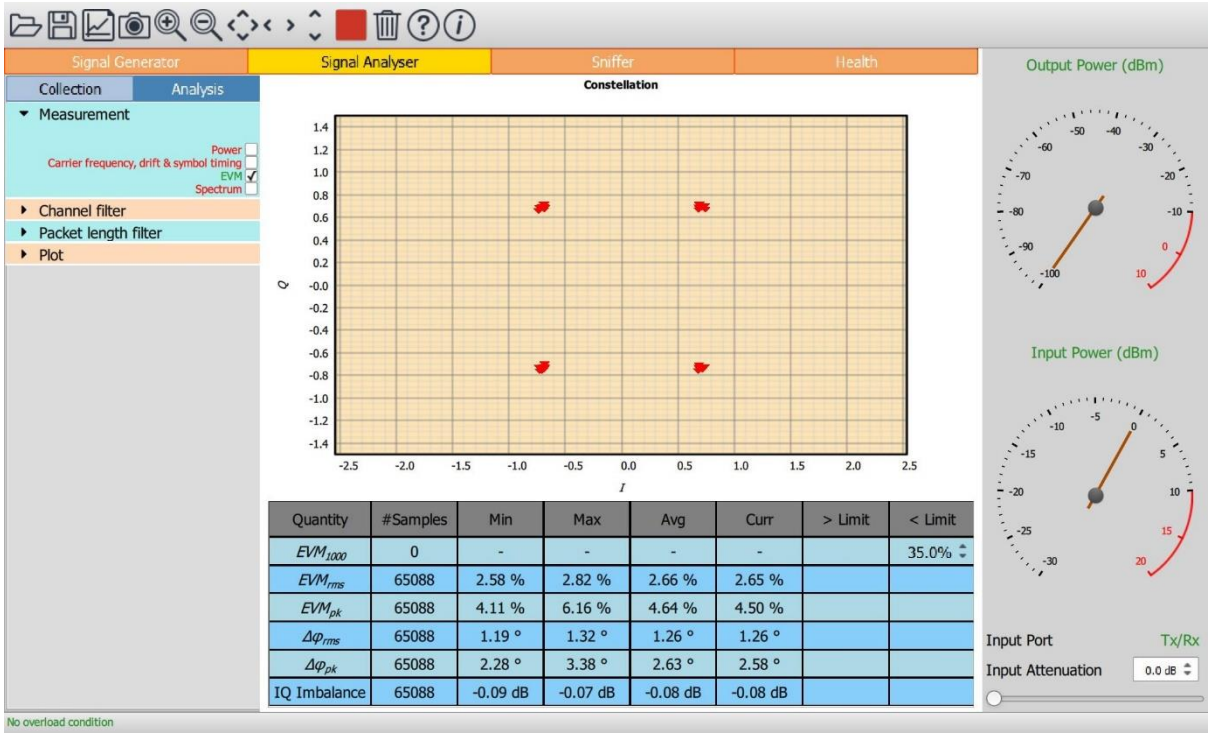
a_{start}:a_{step}: a_{stop}, b_{start}: b_{step}: b_{stop}, …

This implies that all channels from a_{start} to a_{stop} in steps of a_{step} will be selected, plus all channels from b_{start} to b_{stop} in steps of b_{step}, etc.

If a_{step} is unity, then a_{start}:a_{step}: a_{stop} can be abbreviated to a_{start}: a_{stop}.

If a_{step} is equal to a_{stop} then a_{start}:a_{step}: a_{stop} can be abbreviated to a_{start}.

If the '*Single channel*' mode option is selected, then only one channel can be selected at any time.



Quantity	#Samples	Min	Max	Avg	Curr	> Limit	< Limit
EVM_{1000}	0	-	-	-	-		35.0%
EVM_{rms}	65088	2.58 %	2.82 %	2.66 %	2.65 %		
EVM_{pk}	65088	4.11 %	6.16 %	4.64 %	4.50 %		
$\Delta\varphi_{rms}$	65088	1.19 °	1.32 °	1.26 °	1.26 °		
$\Delta\varphi_{pk}$	65088	2.28 °	3.38 °	2.63 °	2.58 °		
IQ Imbalance	65088	-0.09 dB	-0.07 dB	-0.08 dB	-0.08 dB		

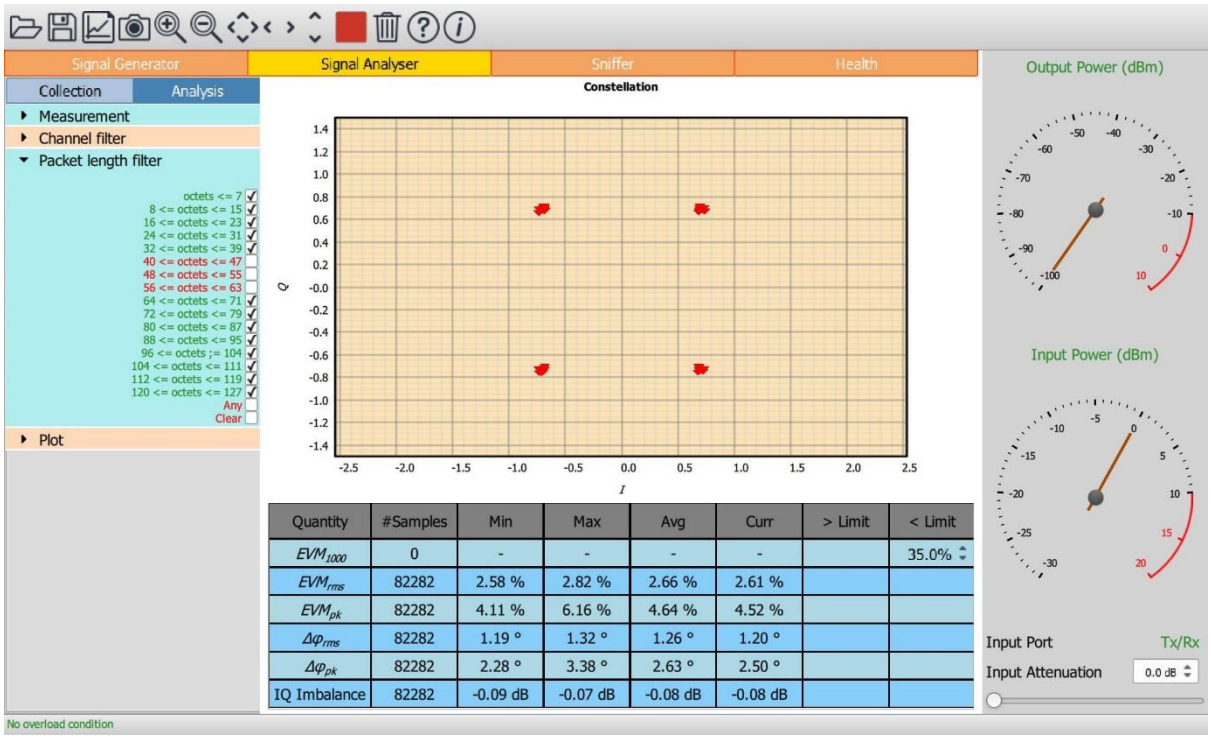
Figure 20: Filtering displayed results by RF channel.

8.4.4 Filtering the displayed results by packet length

The displayed results can be filtered by packet length. This provides a simple facility for monitoring transmitter quality as a function of packet length.

Due to memory restrictions, individual packet lengths cannot be specified. Instead, the range of possible packet lengths is divided up into 16 groups, each group spanning 8 contiguous packet lengths. The packet length refers to the number of octets in the PHY PPDU payload, ie it excludes the SHR and PHR fields.

The packet length filtering is specified via the '*Packet length filter*' menu under the '*Analysis'* tab. The required packet lengths are selected by ticking the corresponding boxes. If all packet lengths are of interest, then clicking the '*All'* box at the bottom of the menu will select all packet length groups.



Quantity	#Samples	Min	Max	Avg	Curr	> Limit	< Limit
EVM_{1000}	0	-	-	-	-		35.0%
EVM_{rms}	82282	2.58 %	2.82 %	2.66 %	2.61 %		
EVM_{pk}	82282	4.11 %	6.16 %	4.64 %	4.52 %		
$\Delta\varphi_{rms}$	82282	1.19 °	1.32 °	1.26 °	1.20 °		
$\Delta\varphi_{pk}$	82282	2.28 °	3.38 °	2.63 °	2.50 °		
IQ Imbalance	82282	-0.09 dB	-0.07 dB	-0.08 dB	-0.08 dB		

Figure 11: Filtering displayed result by packet length.

8.4.5 Understanding the results table

The results table contains a summary of the results obtained from the selected measurement group when filtered by the selected RF channel and packet length.

The first column in the table contains the names of the measurements which belong to the currently selected measurement group (see section 8.4.2).

The second column in the table contains the number of independent measurements (usually equivalent to the number of packets) which have contributed to the results for each measured quantity.

The third and fourth columns contain the minimum and maximum values which have been observed for each measured quantity.

The fifth column contains the average value of the measured quantity over all packets. If the units of the measured quantity are dBm or dB, then the average is the average of the dB values, not an average of the powers or linear ratios.

The last measured value is displayed in the sixth column.

For quantities with 802.15.4 specification test limits, the lower limit is contained in column seven and the upper limit in column eight.

Quantity	#Samples	Min	Max	Avg	Curr	> Limit	< Limit
EVM_{1000}	532	2.71 %	2.94 %	2.80 %	2.80 %		35.0%
EVM_{rms}	266	2.71 %	2.88 %	2.78 %	2.80 %		
EVM_{pk}	266	4.33 %	5.84 %	4.67 %	4.68 %		
$\Delta\varphi_{rms}$	266	1.24 °	1.33 °	1.29 °	1.31 °		
$\Delta\varphi_{pk}$	266	2.38 °	2.93 °	2.64 °	2.67 °		
IQ Imbalance	266	-0.07 dB	-0.06 dB	-0.06 dB	-0.06 dB		

Figure 12: The results table.

When the selected filters include more than one RF channel or packet length group, then the displayed values of minimum, maximum and average are the minimum, maximum and average over all packets which satisfy the selected filtering parameters.

If no measurement is available, then the symbol '-' is used to fill the corresponding table cell.

If a cell exceeds one of its test limits, then that cell is highlighted in red.

It is possible to select a row in the table by clicking on it. Once a row has been selected, the corresponding quantity will be plotted in the graphics areas. The format of the plot is controlled by the '*Plot*' menu under the '*Analysis*' tab.

8.4.6 Controlling the graphical data

8.4.6.1 Overview

The graphical data being displayed is controlled by the '*Plot*' menu under the '*Analysis*' tab. The contents of the plot menu will vary depending on which measurement group has been selected under the '*Measurement*' menu. Only those quantities relevant to the currently selected measurement group will be available for selection.

At the top of the '*Plot*' menu are a number of checkboxes. Selecting one of these checkboxes will result in one of the following graphical displays:

1. Offset constellation plot
2. EVM vs time throughout the packet
3. Phase error at offset constellation points vs time throughout the packet
4. Output of the carrier tracking loop vs time throughout the packet
5. Peak and average spectra used to perform the PSD measurements
6. Power profile of the packet
7. IQ samples
8. FM demodulation of the IQ samples (ie an MSK interpretation of the O-QPSK signal)

The final checkbox is labelled '*Other*'. If this is selected, then two combo boxes will be made visible.

The left hand combo box lists all the quantities which are measured for the current measurement group (which is selected under the '*Measurement*' menu of the '*Analysis*' tab). These are the same

quantities as displayed in the first column of the results table. The quantity to be plotted can be selected either through the combo box or by highlighting the appropriate row in the results table.

The right had combo box under the '*Plot'* menu determines how the measured quantity is to be plotted. Options may include:

1. vs channel
2. vs packet length group
3. as a histogram

The screen update period can also be altered via the '*Plot'* menu.

8.4.6.2 Offset constellation plot

The offset constellation plot can be selected from the '*Plot'* meu when the '*EVM'* measurement group has been selected under the '*Measurement'* menu. In order to view an offset constellation plot, '*Basic measurements*' must have been selected under the '*Collect'* menu.

The offset constellation plot shows a point for every pair of chips within the packet. The I samples are offset to align with the Q samples. The power in the constellation is normalized to unity.

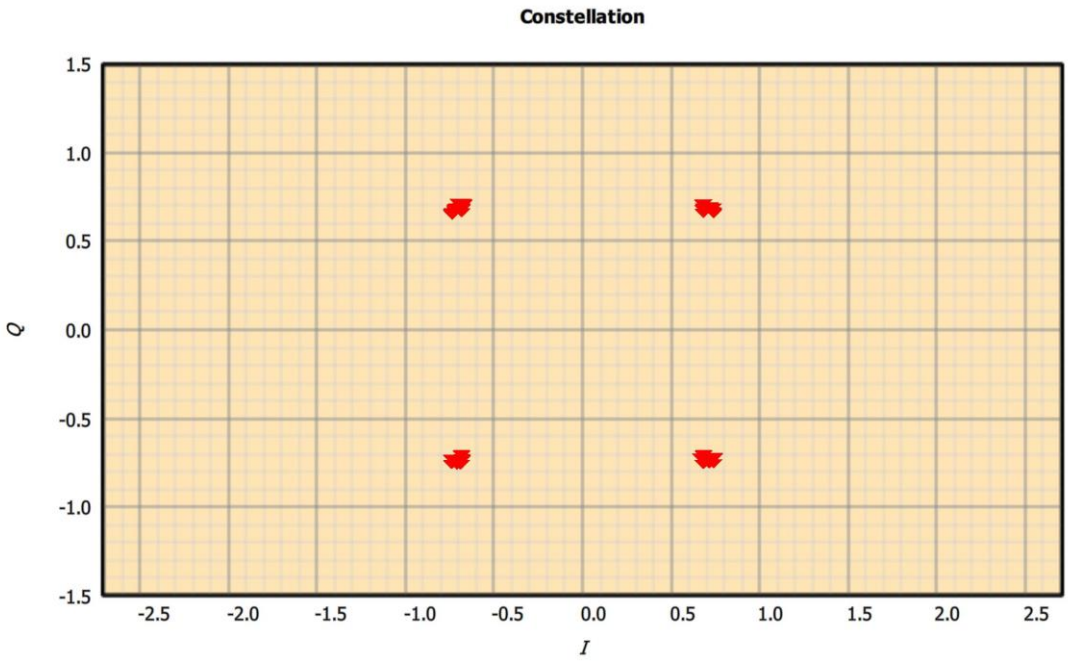


Figure23: Offset constellation plot

8.4.6.3 EVM vs time

The EVM vs time plot can be selected from the '*Plot'* meu when the '*EVM'* measurement group has been selected under the '*Measurement'* menu. In order to view an EVM vs time plot, '*Basic measurements*' must have been selected under the '*Collect'* menu.

The EVM vs time plot shows the EVM vs time throughout the packet. Each point plotted corresponds to a pair of chips. The EVM is measured as a percentage.

The EVM vs time plot will show patterns related to the packet contents. This is due to the band limiting of the signal by the Cuprite analyzer. See section 8.8 for further discussion.

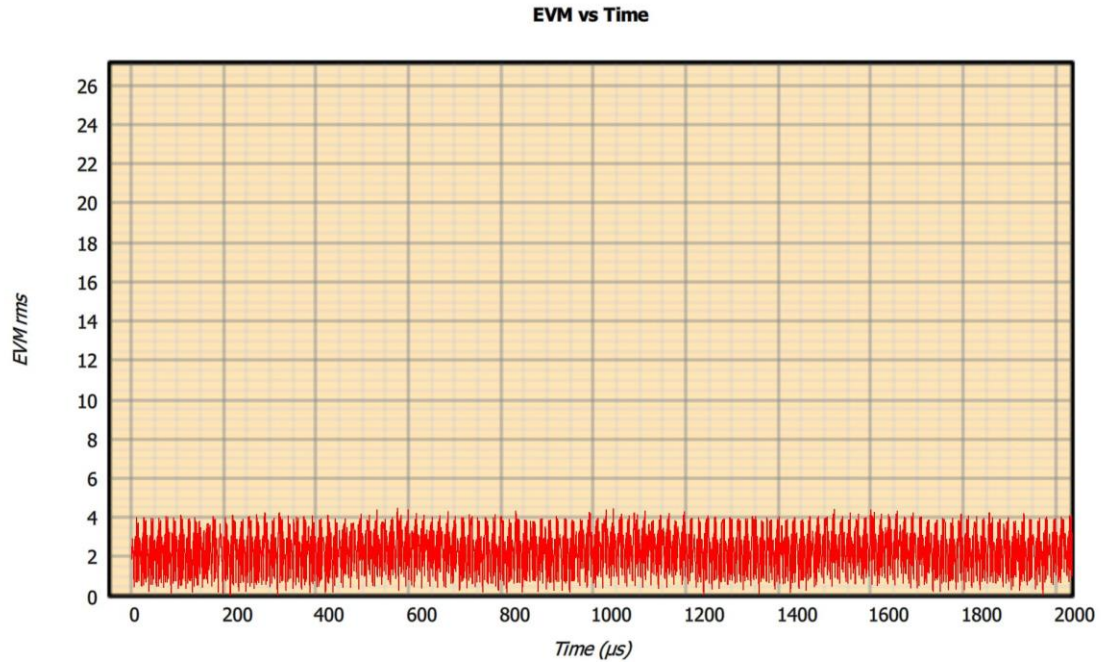


Figure 24: EVM vs time plot

8.4.6.4 Phase error vs time

The phase error vs time plot can be selected from the '*Plot'* meu when the '*EVM'* measurement group has been selected under the '*Measurement'* menu. In order to view a phase error vs time plot, '*Basic measurements*' must have been selected under the '*Collect'* menu.

The phase error vs time plot shows the phase error at each offset constellation point vs time throughout the packet. Each point plotted corresponds to a pair of chips.

The phase error vs time plot will show patterns related to the packet contents. This is due to the band limiting of the signal by the Cuprite analyzer. See section 8.8 for further discussion.

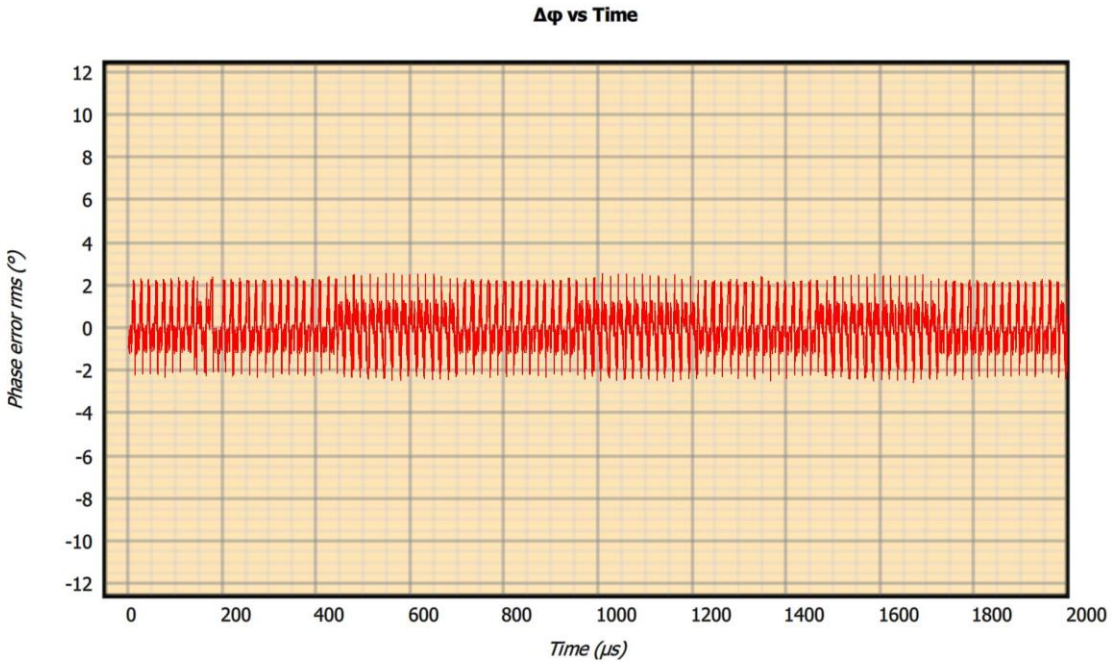


Figure 25: Phase error vs time plot.

8.4.6.5 Carrier tracking loop

The carrier tracking loop plot can be selected from the '*Plot'* meu when the '*carrier frequency, drift and symbol timing'* measurement group has been selected under the '*Measurement'* menu. In order to view a carrier tracking loop plot, '*Carrier tracking data*' must have been selected under the '*Collect'* menu.

The carrier tracking loop plot shows the estimated carrier frequency vs time throughout the packet. This information is extracted from the Cuprite demodulator carrier tracking loop.

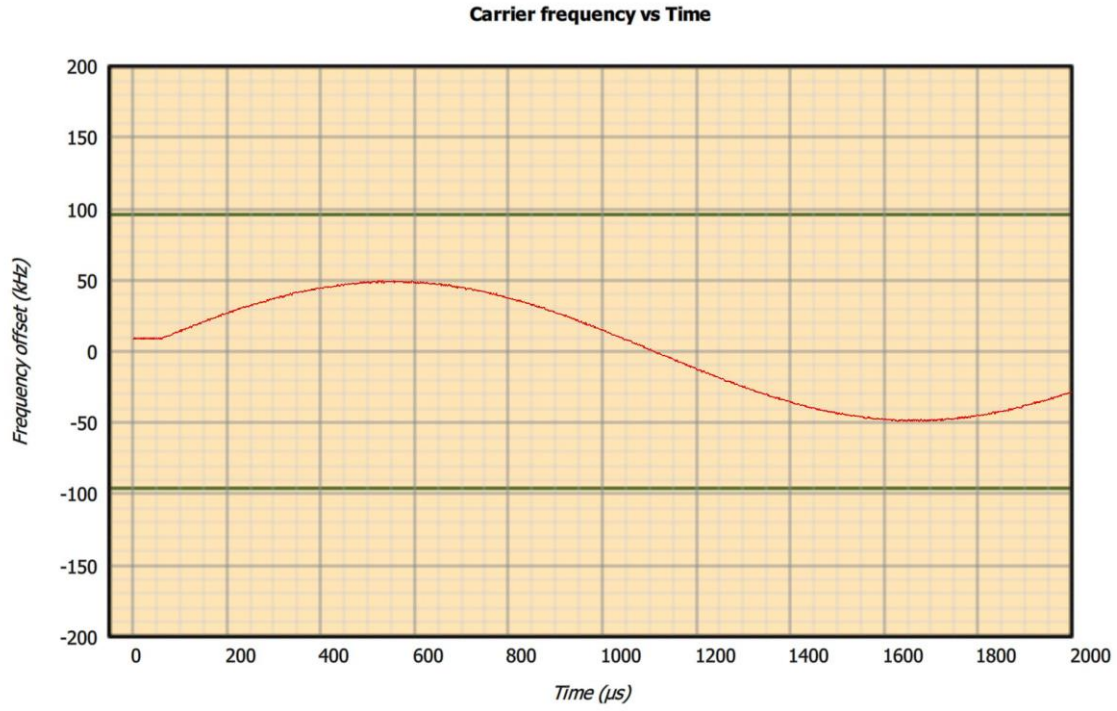


Figure 26: Carrier tracking loop plot.

8.4.6.6 Peak and average spectra

The peak and average spectra plot can be selected from the '*Plot'* meu when the '*Spectrum'* measurement group has been selected under the '*Measurement'* menu. In order to view a peak and average spectra plot, one or both of '*Average spectrum'* and '*Peak spectrum*' must have been selected under the '*Collect'* menu.

The red line on the plot shows the average spectrum (when available) and the blue line the peak spectrum (when available). The dark green line corresponds to the absolute PSD limit whilst the pale green line corresponds to the relative PSD limit. These limit lines are automatically updated when the received signal's channel or power changes. The average spectrum is only available if the '*Average spectrum*' measurement data option has been selected under the '*Collect'* menu. The peak spectrum is only available if the '*Peak spectrum'* measurement data option has been selected under the '*Collect'* menu.

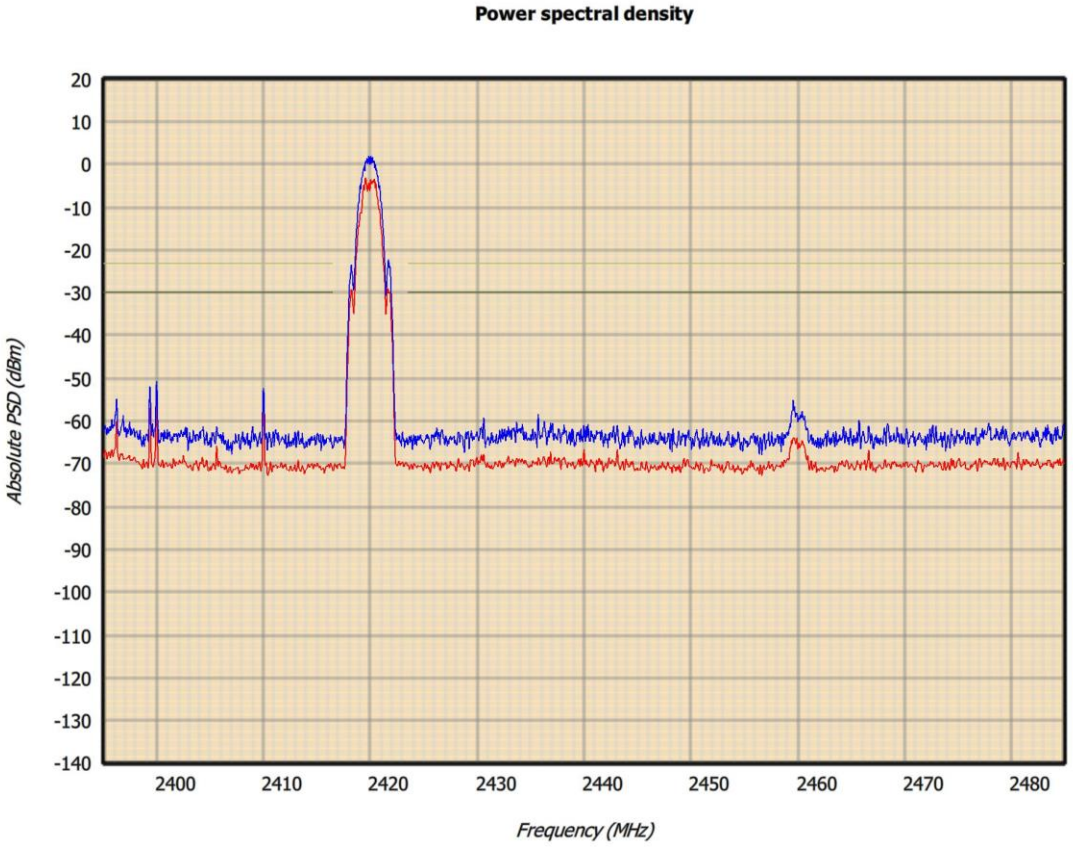


Figure 27: Peak and average spectra plot.

8.4.6.7 Power profile

The power profile plot can be selected from the '*Plot'* meu when the '*Power'* measurement group has been selected under the '*Measurement'* menu. In order to view a power profile plot, '*IQ waveform data*' must have been selected under the '*Collect'* menu.

The power profile plot shows the packet power in dBm as a function of time. The plot starts 40µs prior to the first chip and finishes 40µs after the last chip. This enables the power ramp up and down to be examined in detail.

The time resolution of the power profile plot is determined by the '*Waveform oversampling*' menu under the '*Collect'* tab.

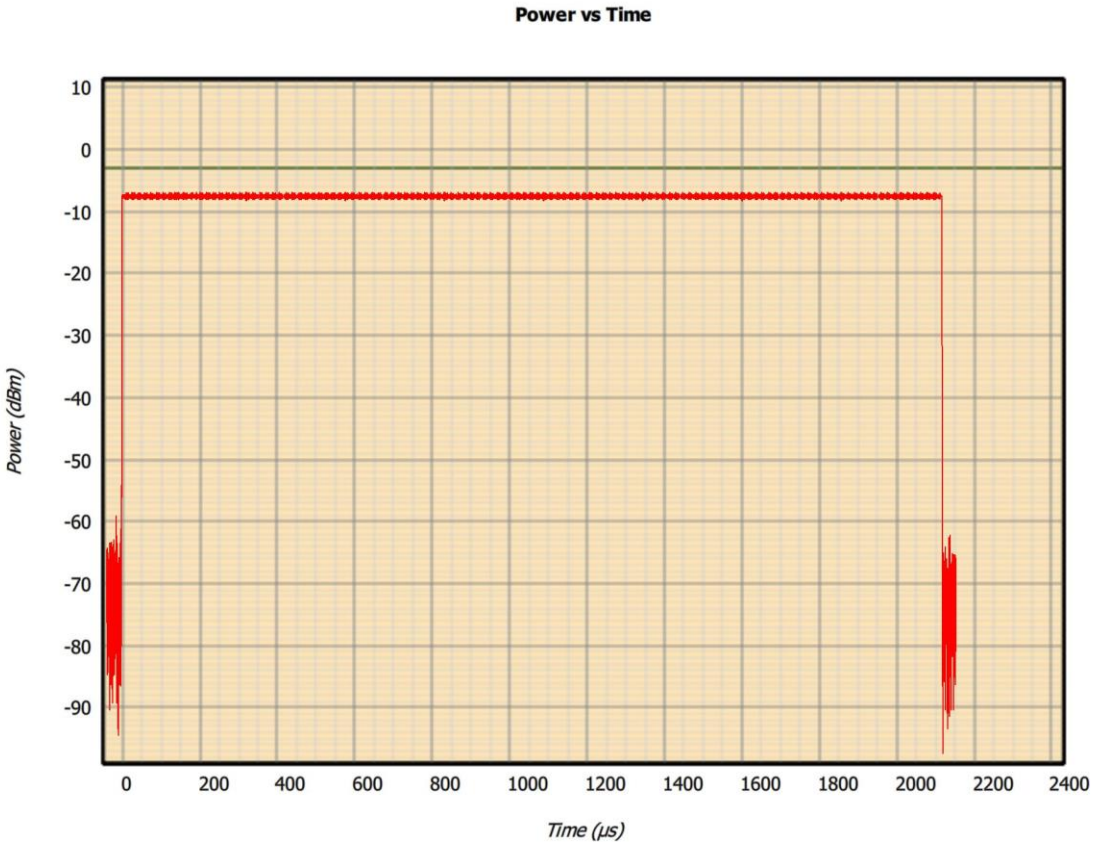


Figure 28: Power profile plot.

8.4.6.8 IQ Samples

The IQ samples plot can be selected from the '*Plot'* meu. This option is always available, irrespective of which measurement group has been selected under the '*Measurement'* menu. In order to view an IQ samples plot, '*IQ waveform data*' must have been selected under the '*Collect'* menu.

The I data is plotted in red and the Q data plotted in blue. The time resolution of the IQ samples plot is determined by the '*Waveform oversampling*' menu under the '*Collect'* tab. The IQ data are normalized to unity power.

If '*Decoded packet*' data has been selected under the '*Collect'* menu, then it is also possible to display the decode bit stream alongside the IQ data. In order to make the decoded packet data visible, it may be necessary to zoom in on the plot. When the plot is zoomed in sufficiently, the values of the individual symbols will be displayed at the top of the plot. Each symbol is displayed as a hex character in a box spanning the length of the symbol. The color of the boxes alternates between symbols. If the plot is zoomed in further, then the value of each chip is displayed at the top of the plot. Each chip is displayed as either 0 or 1 in a box which spans the length of the chip. The color of the boxes alternates between chips. The alternating colors change between successive symbols so that the symbol boundaries can readily be found.

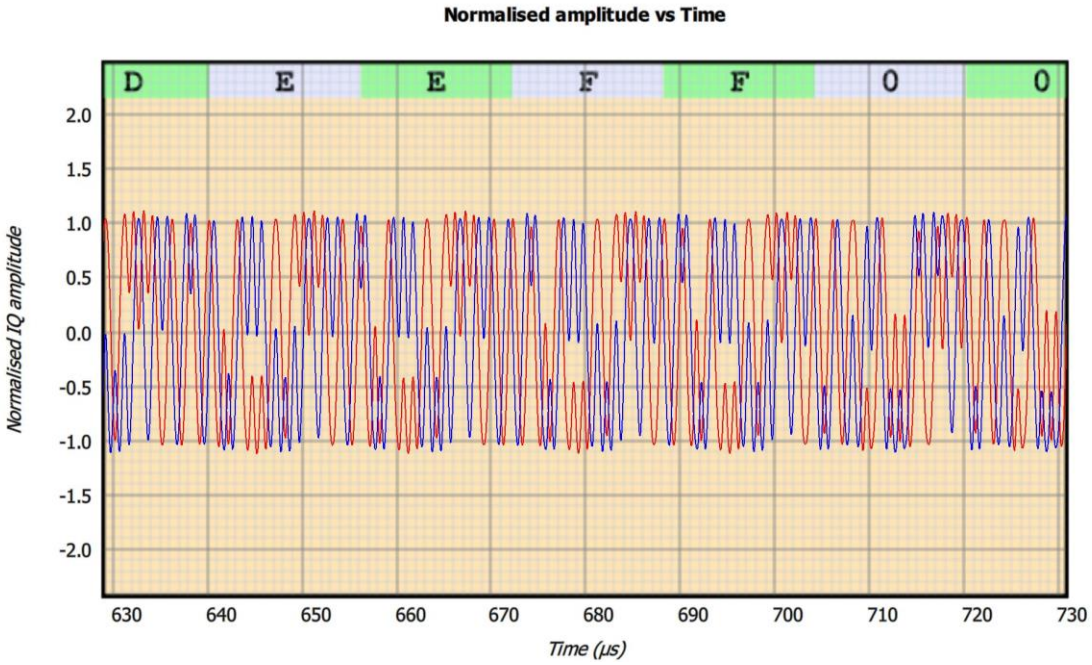


Figure 29: IQ sample plot.

8.4.6.9 FM demodulation

The FM demodulation plot can be selected from the '*Plot'* meu. This option is always available, irrespective of which measurement group has been selected under the '*Measurement'* menu. In order to view an FM demodulation plot, '*IQ waveform data*' must have been selected under the '*Collect'* menu.

The time resolution of the FM demodulation plot is determined by the '*Waveform oversampling*' menu under the '*Collect'* tab.

The FM demodulation data is useful in understanding how the 802.15.4 O-QPSK modulation can be interpreted as an MSK signal.

If '*Decoded packet*' data has been selected under the '*Collect'* menu, then it is also possible to display the decode bit stream alongside the frequency deviation data. In order to make the decoded packet data visible, it may be necessary to zoom in on the plot. When the plot is zoomed in sufficiently, the values of the individual symbols will be displayed at the top of the plot. Each symbol is displayed as a hex character in a box spanning the length of the symbol. The color of the boxes alternates between symbols. If the plot is zoomed in further, then the value of each chip is displayed at the top of the plot. Each chip is displayed as either 0 or 1 in a box which spans the length of the chip. The color of the boxes alternates between chips. The alternating colors change between successive symbols so that the symbol boundaries can readily be found.

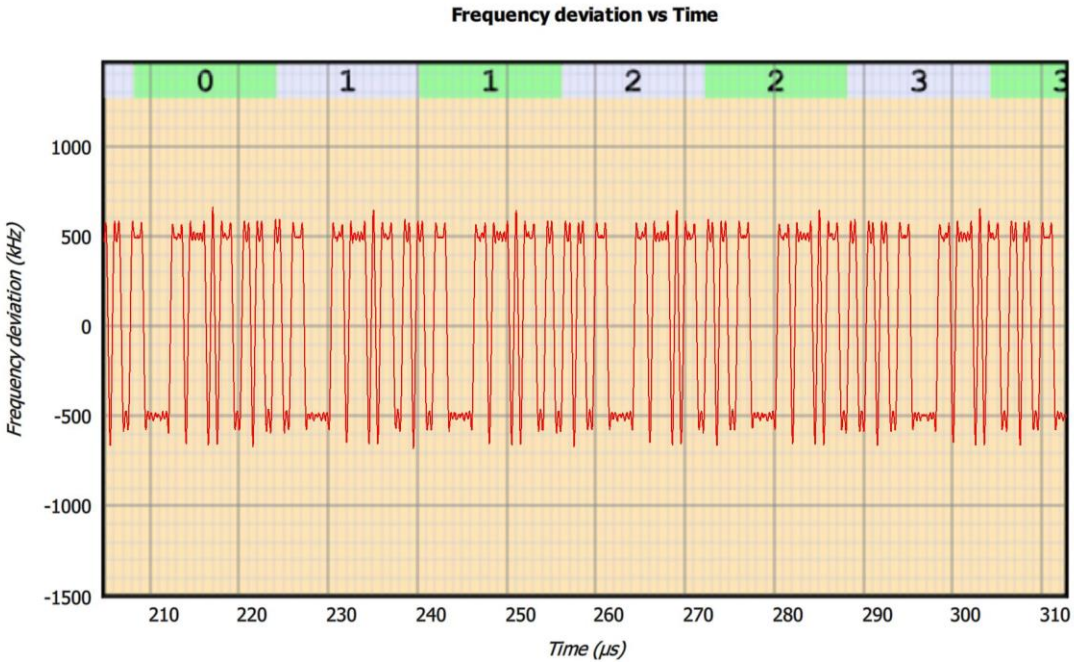


Figure 29: FM demodulation plot.

8.4.6.10 vs channel:

Select the appropriate measurement group for the quantity to be plotted from the '*Measurement*' menu. Check the '*Other*' box in the '*Plot*' menu. Either select the quantity to be plotted from the left-hand combo box in the '*Plot*' menu or by clicking on the quantity in the results table. Select '*vs Channel*' from the right-hand combo box in the '*Plot*' menu.

The quantity to be plotted is shown as a function of the RF channel number. For each RF channel the following quantities are displayed:

1. minimum observed value (bottom of pink bar)
2. average value (red line)
3. maximum observed value (top of green bar)

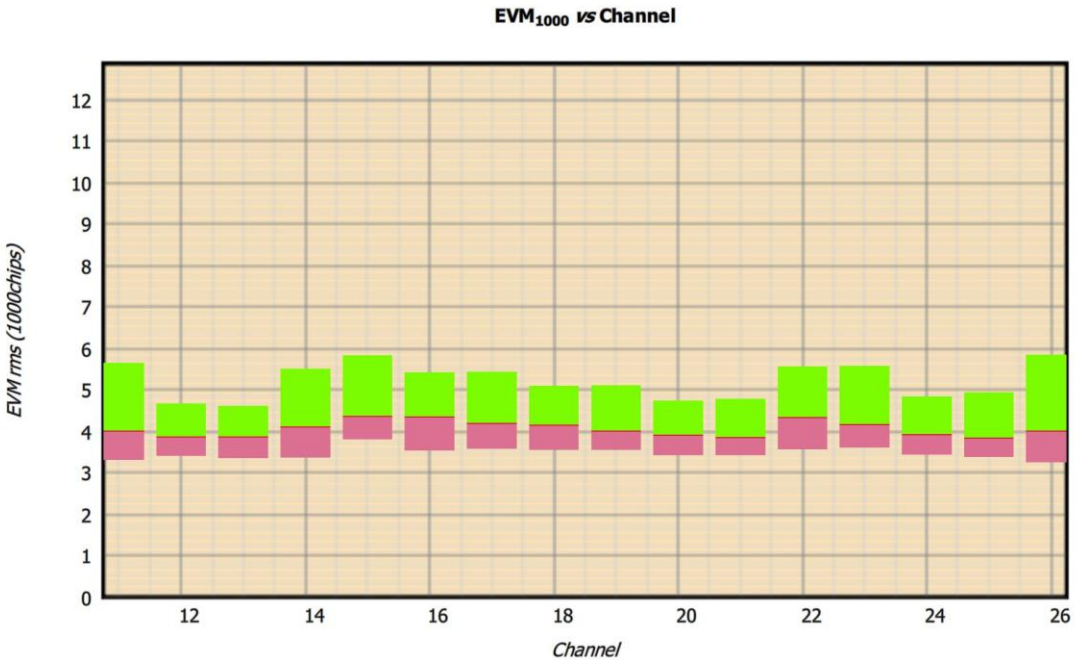


Figure 30: Results vs channel

8.4.6.11 vs packet length group:

Select the appropriate measurement group for the quantity to be plotted from the '*Measurement*' menu. Check the '*Other*' box in the '*Plot*' menu. Either select the quantity to be plotted from the left-hand combo box in the 'Plot' menu or by clicking on the quantity in the results table. Select '*vs Packet length*' from the right-hand combo box in the '*Plot*' menu.

The quantity to be plotted is shown as a function of the packet length group. For each packet length group the following quantities are displayed:

1. minimum observed value (bottom of pink bar)
2. average value (red line)
3. maximum observed value (top of green bar)

Figure 131: Results vs packet length group.

8.4.6.12 Histogram

Select the appropriate measurement group for the quantity to be plotted from the '*Measurement*' menu. Check the '*Other*' box in the '*Plot*' menu. Either select the quantity to be plotted from the left-hand combo box in the '*Plot*' menu or by clicking on the quantity in the results table. Select '*Histogram*' from the right-hand combo box in the '*Plot*' menu.

A histogram of the selected quantity is displayed.

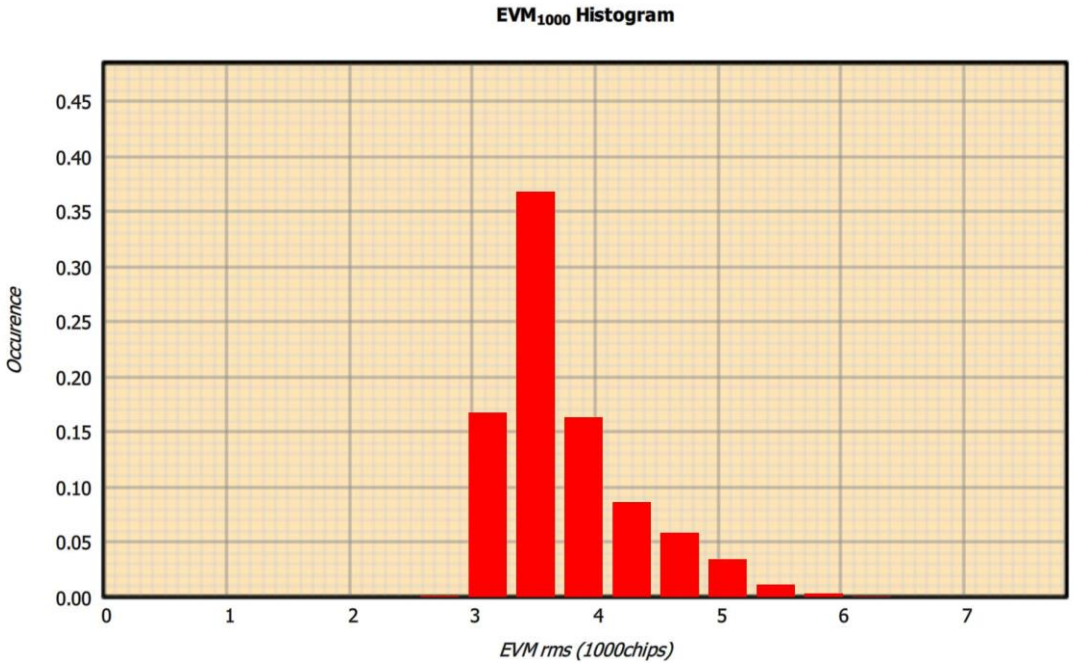


Figure 32: Results plotted as a histogram.

8.4.7 Screen update period

The '*Plot*' menu contains a slider which can be used to alter the rate at which the results table and graphics are updated.

The fastest update period possible is around 50ms, typically limited by the host screen refresh rate. However, if substantial processing is required by Cuprite – for example, the transfer of raw IQ data at 10x oversampling rate for a 127 octet packet – then the specified update rate may not be achievable.

The slowest update rate is 2 seconds. This gives the user time to assimilate the displayed results and waveform data before the next update.

8.5 Adjusting test limits

The test limits are shown in the results table. The penultimate column of the results table displays the lower limit and the final column the upper limit. They can be altered by changing the values in the spin boxes, either by using the up/down arrows or by entering numeric text directly.

8.6 Saving and restoring settings

The current collection, analysis and limit settings can be saved by clicking the '*Save'* button on the toolbar. Select the '*Signal analysis settings (*.sas)*' file type to save the current settings.

An existing signal analysis settings file (*.sas) can be opened using the '*Open'* button on the toolbar.

The signal analysis settings file (*.sas) is an XML file. It is not recommended that this file be edited manually. If it needs to be modified, open it from the signal analyzer, modify the required parameters and re-save.

8.7 Saving current results table and graphics

The current graph and results table can be saved as an image by clicking the '*Graph'* button on the toolbar. The range of possible graphics formats includes:

1. Windows bitmap files (*.bmp)
2. Joint photographic expert group files (*.jpg)
3. Portable network graphics files (*.png)
4. Portable bitmap files (*.pbm)
5. Portable graymap files (*.pgm)
6. Portable pixmap files (*.ppm)
7. X11 bitmap files (*.xbm)
8. X11 pixmap files (*.xpm)

8.8 Notes on EVM measurements

According to the 802.15.4 specification, the EVM measurements must be made using a reference receiver which performs carrier lock, symbol timing recovery and amplitude adjustment whilst making the measurements. Test equipment manufacturers normally emphasise the quality of their reference receivers by quoting the minimum EVM that they can measure. This may typically be around 0.2%. In order to achieve such EVMs, the manufacturers must necessarily employ very wide bandwidth receivers in order to analyze the far our sidebands of the transmission. This is clearly not how a real 802.15.4 receiver would function, and hence the quoted EVM accuracy figures are utterly meaningless.

The TLF300 attempts to more accurately model a real life 802.15.4 receiver. In particular, the signal is bandlimited prior to analysis. The shape of the channel filter used is shown below. The use of this representative channel filter limits the minimum EVM which can be achieved to 1.5%, considerably large than the 0.2% quoted by manufacturers with unrepresentative receivers, but still a small fraction of the 35% permitted by the 802.15.4 specification.

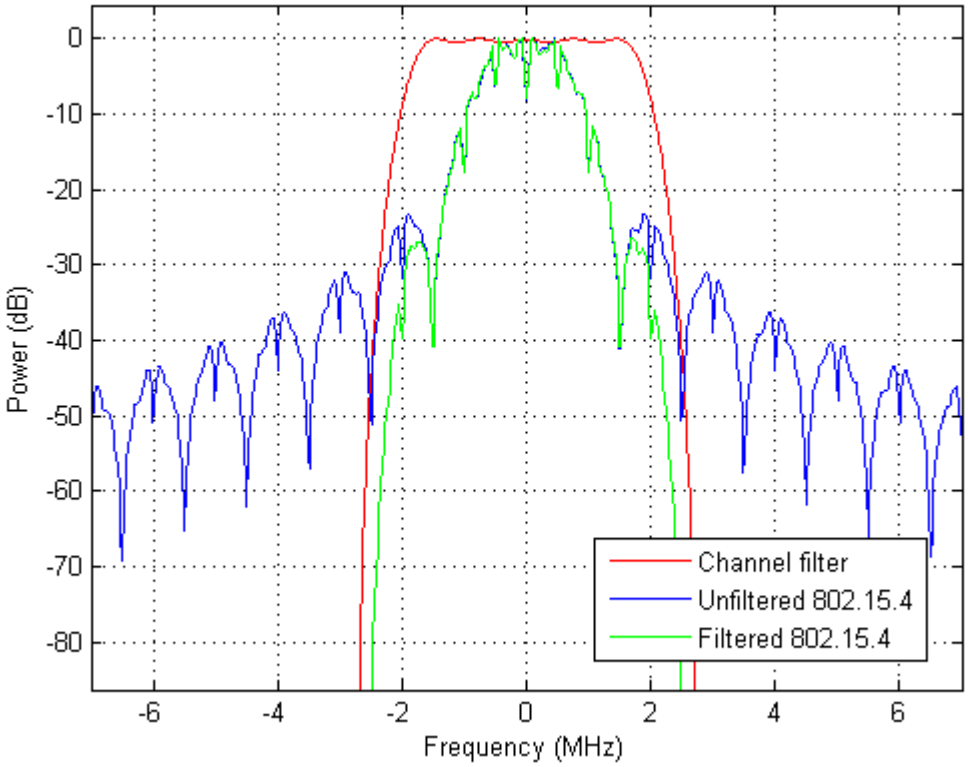


Figure 33: Cuprite demodulator channel filter.

The EVM measurement is also affected by the signal-to-noise ratio. It is important to adjust the receiver frontend attenuator such that the input signal is just below the level at which the receiver will saturate. See section 8.3.10. The signal-to-noise ration can also be affected by pick-up of other 2.4GHz ISM band transmissions, in particular WiFi. Many devices under test are unscreened PCBs which can act as superb antennas for other 2.4GHz transmissions. A tell-tale sign of unwanted pick-up is burst of constellation points which are misplaced. This is particularly obvious when viewing the EVM vs time plot.

It should be noted that the band limiting of the Cuprite signal generator plus the band limiting of the Cuprite demodulator results in an overall EVM measurement of around 2.7% when the two are connected back-to-back. This is figure is also typical of the measurements to be expected from a real 802.15.4 transmitter.

In summary, the band limiting of the signal performed by the Cuprite demodulator is in accordance with the 802.15.4 specification and real 802.15.4 receivers. As a consequence, the minimum EVM measurement is limited to 1.5%. A typical 802.15.4 transmitter yields an EVM measurement of 2.7%.

9 Packet sniffer (Wireshark) mode.

9.1 Overview

The packet sniffer mode monitors all 16 channels simultaneously Any packets which are detected are demodulated and the bit stream either piped directly into Wireshark for live protocol analysis, and/or saved to file in pcap-ng format. Capture can be restricted to certain RF channels, or an RSSI threshold can be set. During capture, a spectrum display is available so that the prevailing RF environment can be monitored.

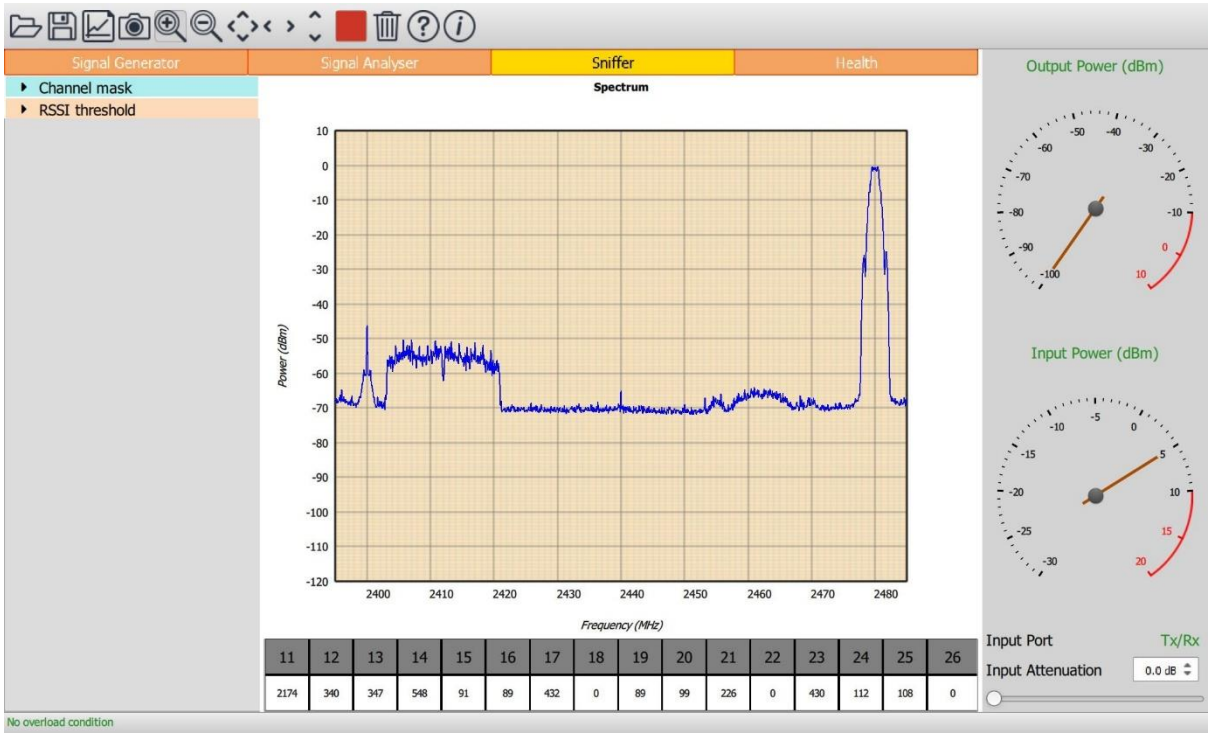


Figure 34: Cuprite packet sniffer mode.

9.2 Pre-requisites

Wireshark 2.4.2 or later must be installed on the host computer. The Wireshark executable must be located at:

C:\Program Files\Wireshark\Wireshark.exe

9.3 RF connections

The packet sniffer can monitor signals on either the '*Tx/Rx'* port or the '*Monitor In*' port. See section 8.3.9 on setting the RF input port and section 8.3.10 on setting the RF frontend attenuator. It is important that the RF frontend attenuator is set correctly to maximize sensitive and prevent RF overload.

9.4 Programming the packet sniffer

9.4.1 Programming which RF channels to collect

The '*Channel mask*' menu permits selection of the RF channels on which data is to be collected. These are specified in terms of 802.15.4 RF channel numbers, starting at 11 (2405MHz) and ending at 26 (2480MHz).

The required RF channels can be selected by either:

1. Ticking the individual channel boxes
2. Using the quick channel group selection buttons:
    a. Clear all
    b. Select all
3. Entering a textual description

The textual description must be of the form:

a_{start}:a_{step}: a_{stop}, b_{start}: b_{step}: b_{stop}, ...

This implies that all channels from a_{start} to a_{stop} in steps of a_{step} will be selected, plus all channels from b_{start} to b_{stop} in steps of b_{step}, etc.

If a_{step} is unity, then a_{start}:a_{step}: a_{stop} can be abbreviated to a_{start}: a_{stop}.

If a_{step} is equal to a_{stop} then a_{start}:a_{step}: a_{stop} can be abbreviated to a_{start}.

If the '*Single channel*' mode option is selected, then only one channel can be selected at any time.

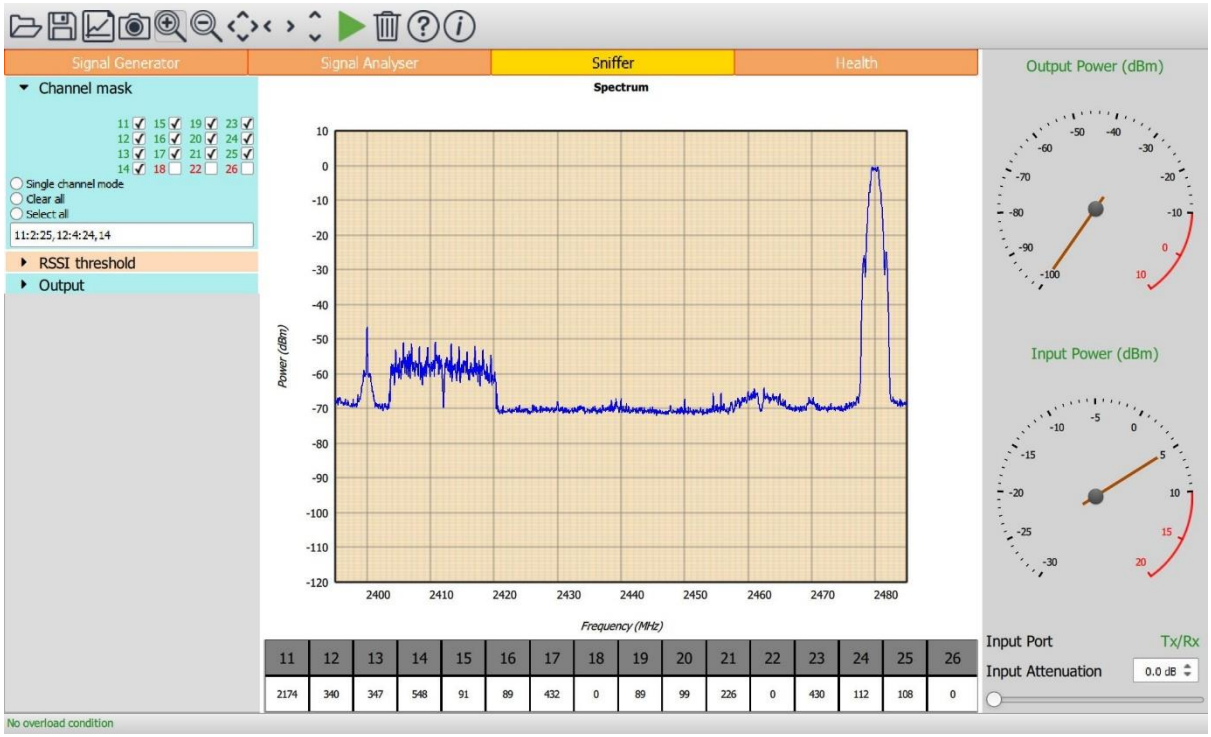


Figure 35: Programming which RF channels to sniff.

9.4.2 Programming the detection thresholds

The TLF3000 permits detection thresholds to be set for:

1. *RSSI threshold*. This permits weak signal strength packets to be ignored.
2. *Synchronizer threshold*. This permits signals which are corrupted by noise or interference to be ignored.

The '*RSSI threshold*' permits weak signal strength packets to be ignored. This feature is useful when there is prevailing 802.15.4 activity in the test area, since it allows the weak packets from distance devices to be ignored and only the strong packets from the nearby devices under test to be collected.

The RSSI threshold for packets to be collected can be set anywhere from -120dBm to +20dBm in steps of 1dBm.

The '*Synchroniser threshold*' permits signals whose packet preamble correlates poorly to be ignored. This feature is useful for maximizing sensitivity whilst minimizing false detections.

The synchronizer threshold can be set anywhere from 900 to 1500. The higher the value, the more stringent the correlation criterion. If the threshold is reduced, then the sniffer will become more sensitive, however, there is also a risk of synchronizing on noise or interference and hence false detections can be generated. Conversely, if the threshold is set too high, the sniffer will cease generating false detections but some wanted packets may be discarded. The default value is 1140.

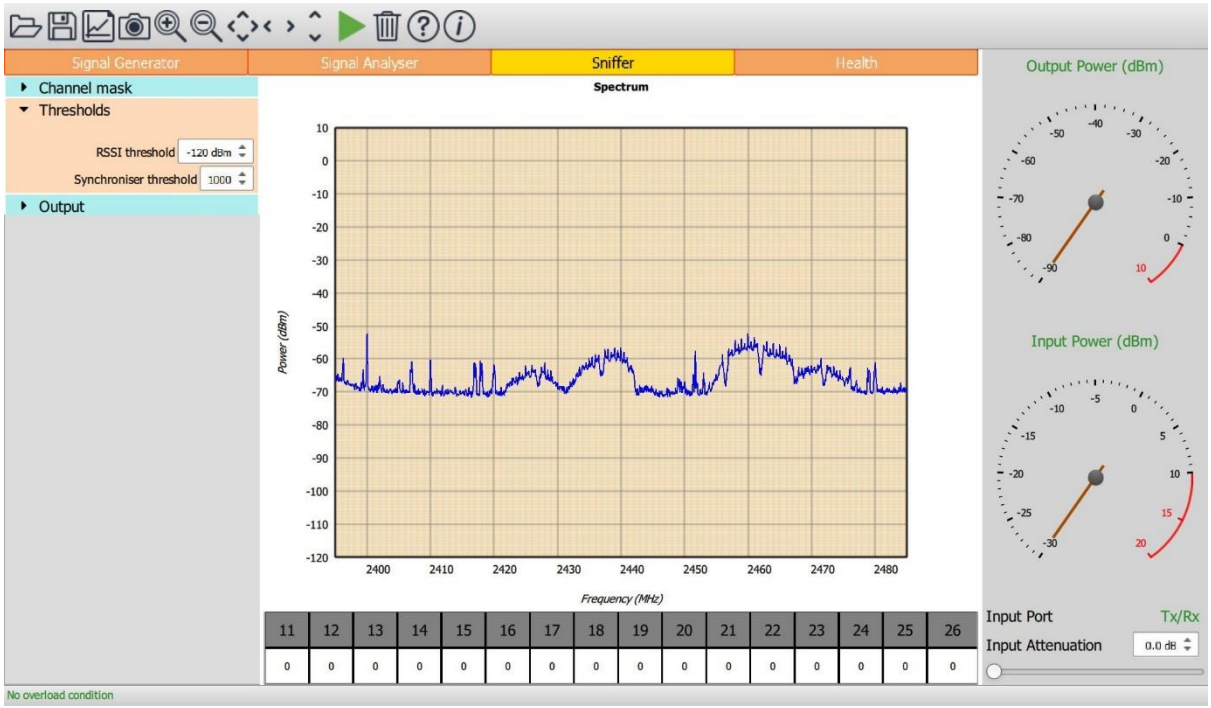


Figure 36 Programming the sniffer detection thresholds.

9.4.3 Programming the data sink

The '*Output'* menu dictates where the decoded packets are sent and in what format.

Two options are available for the output format:

1. *ZEPv2*. The packets are sent as Zigbee Encapsulated Protocol version 2. They are encapsulated as IPv4 packets and the Wireshark link layer header type of DLT_IPV4 is used.
2. *DLT_IEEE802_15_4*. The packets are sent using the Wireshark link layer header type of DLT_IEEE802_15_4.

Two options are available for the packet sink:

1. *Live capture & decode*. The packets will be piped into Wireshark which will perform real-time protocol analysis.
2. *Stream packets to file*. The packets will be written to file in pcap-ng format.

One for both of these options may be selected.

If the '*Stream packets to file*' option is selected, then a text input box will be made visible to receive the output file name. The name can either be typed directly into this box or pasted in. A '*Browse'* button is also provided to locate the path to the output file.

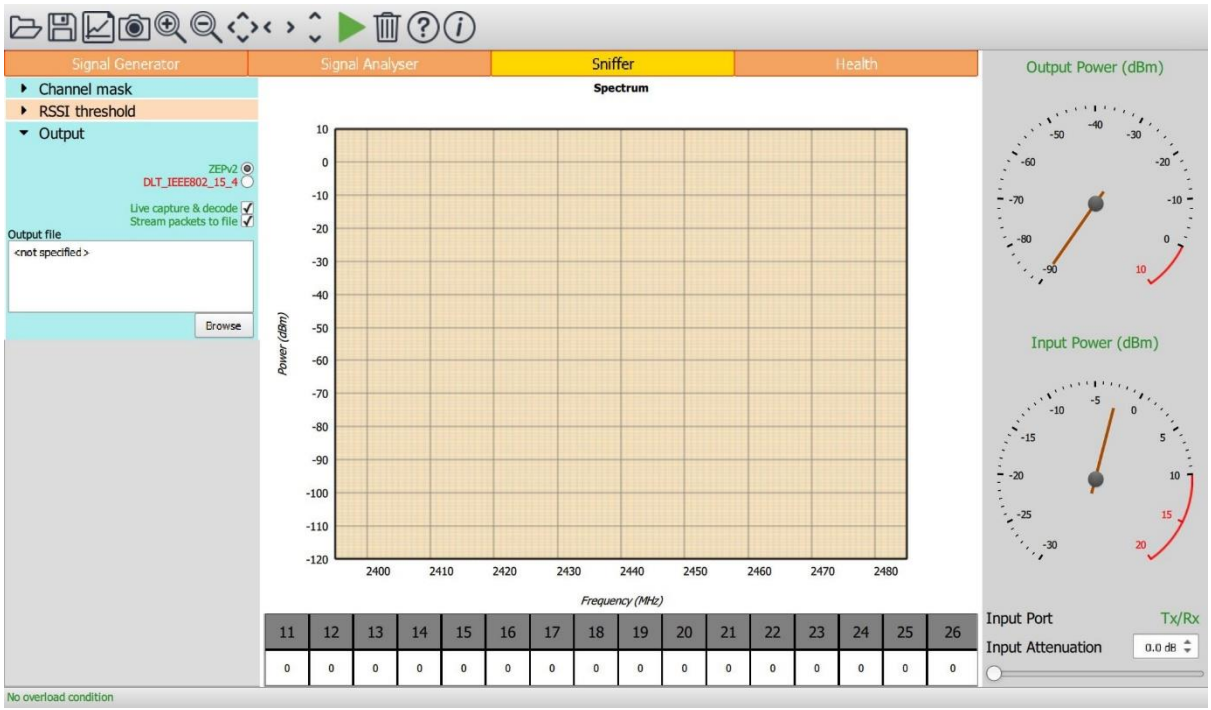


Figure 37: Programming the packet data sink

9.5 Controlling the packet sniffer

9.5.1 Starting the packet sniffer

The packet sniffer is started by clicking the '*Play*' button on the toolbar. If '*Live capture & decode*' has been selected in the '*Output*' menu, then an attempt will be made to launch Wireshark.

It may take a few seconds to launch Wireshark. If the '*Stream packets to file*' option has also be selected in the '*Output*' menu, then packets will be streamed to file whilst Wireshark is launching. However, no packets can be streamed to Wireshark until it has successfully launched. As a consequence, the capture file may contain more packets than displayed in Wireshark

9.5.2 Controlling sniffing from the Cuprite GUI

Sniffing can be controlled using the '*Play*' button in the Cuprite GUI toolbar.

If capture is halted from the Cuprite GUI, then:

1. If packets are being streamed to Wireshark, then this streaming will stop. However, Wireshark will remain active and the pipe between Cuprite and Wireshark will remain open. Wireshark is unaware that the capture has been paused and continues to wait for further packets.
2. If packets are being written to file, then the file will be closed.

If capture is restarted from the Cuprite GUI then:

1. If Wireshark is already open, and the '*Live capture & decode*' option is currently selected, then the packets will be streamed to Wireshark. Provided Wireshark is still in the run state, it will receive and process the packets as if part of the previous capture. If on restarting the capture from the Cuprite GUI Wireshark is in the stopped state, then a window will popup requesting the user to restart Wireshark capture using the '*Start*' option under the Wireshark '*Capture*' menu.
2. If the '*Stream packets to file*' option is currently selected, then an attempt will be made to open the specified output file. If the file exists, the user will be prompted as to whether the contents of the file should be overridden, or whether a new section should be appended to the existing file. Once the file has been opened, packets will be streamed into it.

9.5.3 Controlling sniffing from Wireshark

Once Wireshark has been launched, packet capture can be controlled directly from Wireshark. Under the Wireshark capture menu, the following options will function:

1. Start
2. Stop
3. Restart

9.6 Output file format

When streaming decoded packets to file, they are saved in pcap-ng format.

If capture is stopped and then restarted, the user is given the option of either overriding the existing file or appending a new section to the end of the file.

If the DLT_IEEE802_15_4 format has been selected, then sixteen different interfaces are defined in the pcap-ng output file. Each interface corresponds to one of the 16 RF channels. For each interface, the *if_name* field is set to the 802.15.4 channel number and the *if_description* field is set to the frequency of the RF channel in MHz.

If the ZEPv2 format has been selected, then a single interface block is created. Both the channel field and the LQI field in the ZEPv2 header are populated. The LQI field contains a unsigned integer representing the LQI. The CRC/LQI mode flag is set to zero, corresponding to the TI CC24xx mode of operation. The first octet of the FCS at the end of the packet is replaced with a signed value representing the RSSI in units of dBm. The MSB of the second octet of the FCS indicates whether the FCS in the received packet was correct. The lowest 7 LSB of the second octet of the FCS are replaced with the LQI. The highest observable value of LQI is around 110. The lowest value of LQI at which packets can still be detected is around 50.

The timestamp resolution in the interface header blocks is set to 100ns.

Each received packet is placed in an Enhanced Packet block. These contain a 2988 custom option with private enterprise number (PEN) of 50894. This field contains the RSSI of the packet in units of dBm.

9.7 Graphical display and tabular results area

Whilst packet capture is in progress, the graphics area shows a spectrum of the 2.4GHz ISM band. The spectrum is 100kHz resolution and uses a peak detector. The spectrum display provides the user with a visual indication of the prevailing RF conditions. This can be important in understanding why some packets may not have been captured.

The tabular results area contains 16 boxes labelled by channel number. These boxes indicate the number of packets which have been received on each RF channel. These boxes are reset at the start of each new capture. The number of packets reported in the Cuprite GUI may be slightly larger than that reported by Wireshark if the packet sniffer is controlled using the Wireshark capture menu. This discrepancy arises since the Cuprite GUI may have already posted several packets into the output pipe before the Wireshark application closes the pipe. The packets residing in the pipe at the time of closure have been counted by the Cuprite GUI but not read by the Wireshark application.

9.8 Saving and restoring settings

The settings can be saved by clicking the ‘S*a*ve’ button on the toolbar. Select the ‘*Wireshark settings (*.wss)’* file type to save the current settings.

An existing packet sniffer settings file (*.wss) can be opened using the ‘*Open’* button on the toolbar.

The packet sniffer settings file (*.aas) is an XML file. It is not recommended that this file be edited manually. If it needs to be modified, open it from the packet sniffer mode, modify the required parameters and re-save.

9.9 Saving current results table and graphics

The current graph and results table can be saved as an image by clicking the '*Graph*' button on the toolbar. The range of possible graphics formats includes:

1. Windows bitmap files (*.bmp)
2. Joint photographic expert group files (*.jpg)
3. Portable network graphics files (*.png)
4. Portable bitmap files (*.pbm)
5. Portable graymap files (*.pgm)
6. Portable pixmap files (*.ppm)
7. X11 bitmap files (*.xbm)
8. X11 pixmap files (*.xpm)