AND9319/D

DVK Use as a Sniffer Tool

ON Semiconductor®

www.onsemi.com

APPLICATION NOTE

Introduction

When dealing with RF systems it is often necessary to investigate the packet data transmitted by an existing device. If the parameters of the physical layer (frequency, datarate and modulation) are known, the ON Semiconductor DVK (DVK−2 as well as F143−MINI−DVK) can be used to investigate the packet data.

This document describes how to display the data transmitted by a given device using the ON Semiconductor DVK and the AX−RadioLAB software.

Setup

Create a new AX−RadioLAB Project. Make sure “RX continuous” mode is selected.

In the Kit Configuration panel: Select DVK−2 or F143−MINI−DVK according to your hardware. Make sure “Output on debug link” is enabled.

In the PHY panel: Configure the known physical parameters. Disable all encodings if unsure.

Finally the SYNC WORD or Start Frame Delimiter (SFD) has to be configured in the framing panel. It should be understood, that the receiver is continuously running and there is no triggering on RF energy. The receiver is thus continuously receiving random data from the noise except for the very moments when your device is transmitting. However, the received data is discarded by the receiver unless the configured SYNC WORD is matched. After matching the configured SYNC WORD a configurable number of data data bytes is received into the radio FIFO. The microcontroller will then display the data via the debug link interface.

If you happen to know the SYNC WORD transmitted by your device you can simply enter it into the SYNC WORD field of the framing panel and select the right length in the “Syncword length” field. Note that the representation of the SYNC WORD field in the framing panel is always MSB first. (The MSB first option in the framing panel only affects the fields after the SYNC WORD.)

If you don’t know the SYNC WORD used by your device it is recommended to trigger on the preamble. In most cases the device will transmit a series of 10101010 as a preamble. One option is to configure the matching of a 32 bit SYNC WORD of 55:55:55:55 or AA:AA:AA:AA. Those 32 bit sequences are unlikely to appear in the noise and thus the receiver will only trigger if preamble is received. The data received into the radio FIFO consists of more preamble bits appearing after the match, the transmitted SYNC WORD and the transmitted payload. The drawback is, that the exact trigger position inside the preamble is not well defined this way. Thus each received packet will be preceeded by an arbitrary number of preamble bits, which is inconvenient. A more clever approach is to configure matching a 32 bit SYNC WORD of 55:55:55:54 or AA:AA:AA:AB. (Try both!) Matching 0101…010100 or 1010…101011, i.e. the end of the preamble, will match a well defined point in the bit stream. This prevents each received packet from being displayed arbitrarily bit−shifted. However, the matching will eat one or more bits of the transmitted SYNC WORD (depending on the exact SYNC WORD). Thus the packet will not be displayed in a byte synchronized manner. The synchronization can be shifted by inspecting the received data and configuring the SYNC WORD field to match n more bit from the beginning of the received data. (At the expense of n bits of the 0101 sequence, since matching is restricted to 32 bit.) Note: The representation of the SYNC WORD in the framing panel is always MSB first. For dealing with the SYNC WORD as just described it is therefore convenient to represent the received data MSB first as well. This is achieved by checking “send MSB first” in the framing panel. Note: with zero a priori knowledge about the packet it may be impossible to determine the borders between preamble, SYNC WORD and actual packet.

Address matching and length byte should be disabled. MAC header length should be set to 0. The DATA field of the framing panel should contain N arbitrary bytes. This causes the receiver to receive fixed length packets of N bytes. CRC checking should be off.

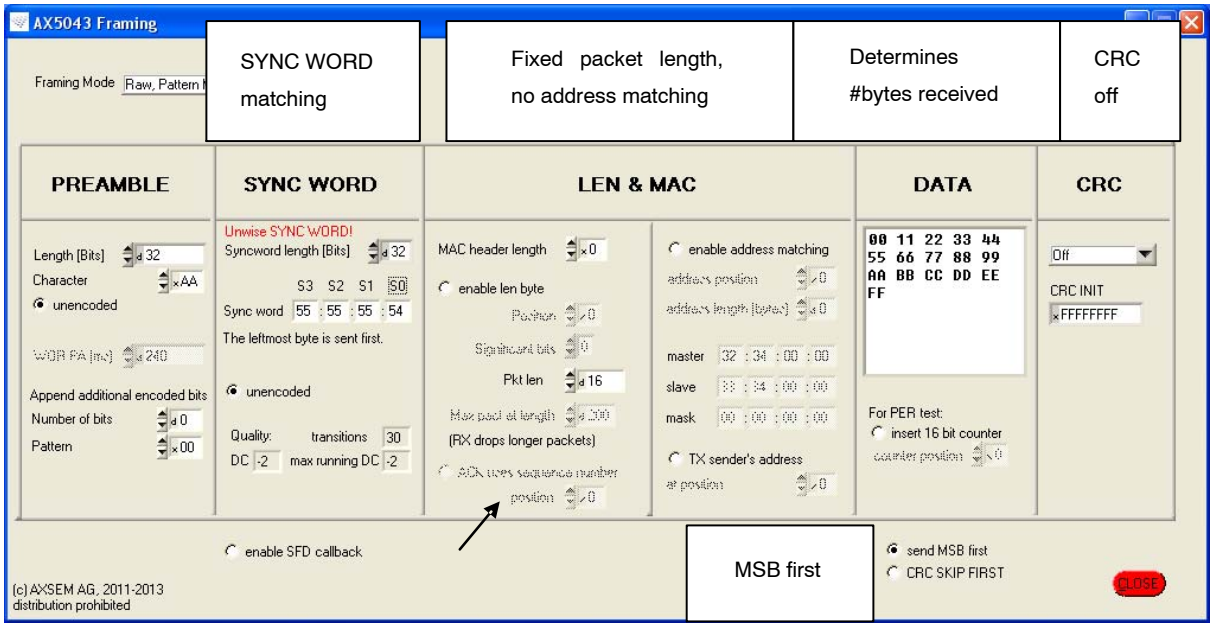

Figure 1.

NOTE: In AX−Gen2−RadioLAB for AX5051 (rather than AX−RadioLAB for AX5043) it is not possible to disable CRC checking in the framing panel. Therefore it is necessary to manually disable CRC checking in the code. After opening the AXCode::Blocks IDE (see below) open AX_Radio_Lab_output/config.c and change to body of th function axradio_framing_check_crc(const uint8_t __xdata *pkt, uint16_t cnt) to “return 1;”. Note that this change gets overwritten each time you save changes in the AX−RadioLAB GUI.

After configuring all parameters press the yellow “calculate registers”, then the orange “Save & Write Output” button in the AX−RadioLAB main panel. Then press the light green “Edit Slave” button. This opens the AXCode::Blocks IDE. Connect the F143−MINI−DVK or DVK2 with plugged in RF module to the computer. Compile and download the software onto the DVK using the “play” shaped “Debug / Continue” button in the IDE.

Enable the Debug Link window using the “Debugging Windows” button.

Received packet data should now appear in the Debug Link window. If nothing is received, try changing the SYNC WORD matching from 55:55:55:54 to AA:AA:AA:AB. And check the physical parameters. If your device transmits very short preambles only it may be necessary to decrease the “Syncword length”. Mind, that this will lead to more frequent spurious matches, however.

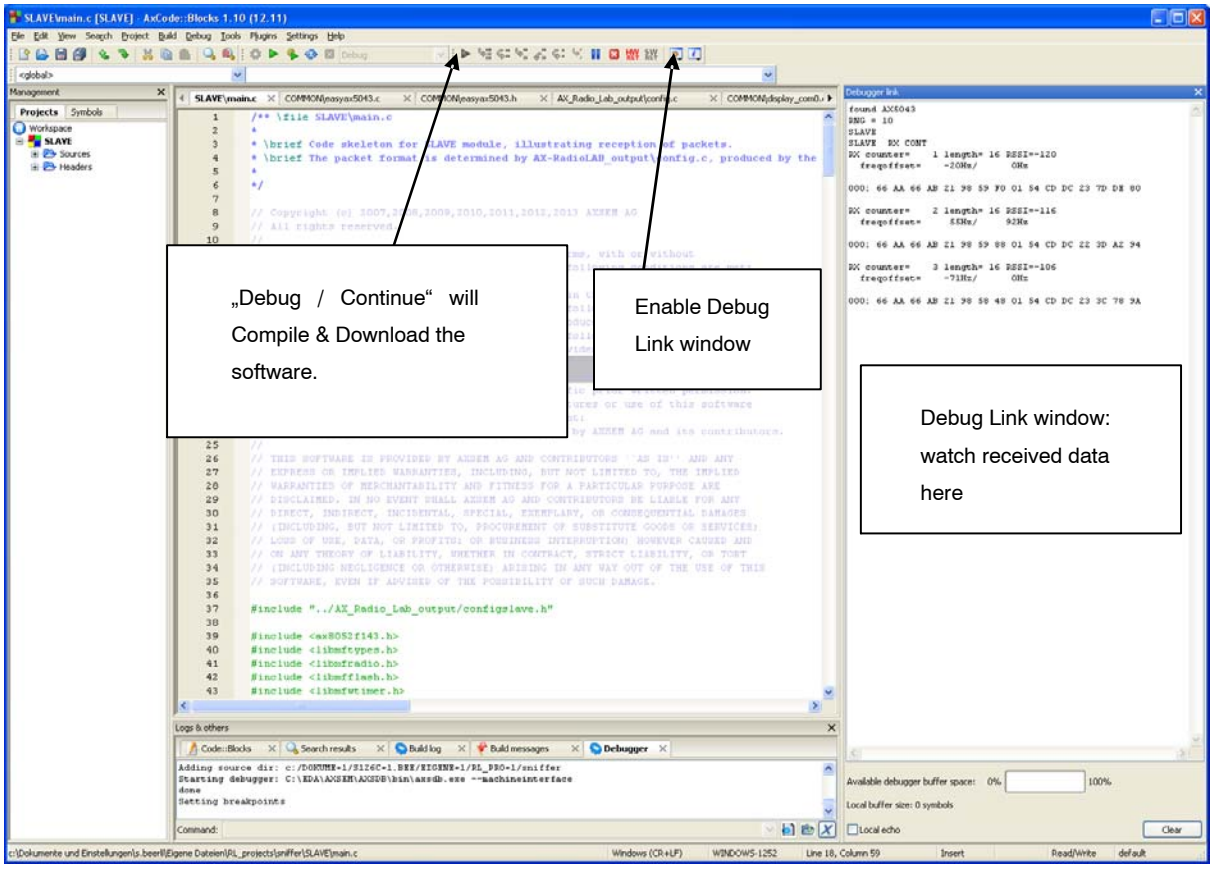

Figure 2.

NOTE: The frequency offset and RSSI values displayed are unreliable, since they are measured at the end of received data, which may be in the noise behind the transmitted packet.

Untriggered Dumping of Received Data in BER Test Mode

The RX 1010 function of the AX−RadioLAB Basic & Regulatory Tests features (also known as BER test mode) offers an alternative way of dumping received data.

In order to use this feature it is necessary to create an AX−RadioLAB project and set up the parameters in the Kit Configuration and PHY panels as described above. Parameters in the framing panel are unimportant here.

Press the yellow “calculate registers”, then the orange “Save & Write Output” button in the AX−RadioLAB main panel. Then press the pink “Basic & Regulatory Tests” button and adjust “BER digits” to a practical value, e.g. 3 for datarates of 1 kbps, 4 for 10 kbps and 5 for 100 kbps. Lower values give faster updates. Press the “RX 1010” button. Finally press the light green “Edit TESTS” button to open the AXCode::Blocks IDE. Replace the line “#undef DUMP_PACKET” in main.c by “#define DUMP_PACKET”.

Compile & download the firmware and open the Debug Link window as described in the previous chapter. The Debug Link window should now periodically display the BER value (which is meaningful only if a continuous 1010 bit stream is applied to at the antenna) together with the received data.

Note: In this mode the radio chip periodically acquires the signal strength (AGC value) and then freezes the AGC for receiving a block of 1000, 10000 or 100000 bits. Note, that this mode is intended for continuous data. It is not well suited for dumping packet data. Applying packet data will usually cause the AGC to settle and freeze in the gap between packets. The packet will then overload the receiver stage.

PUBLICATION ORDERING INFORMATION

LITERATURE FULFILLMENT:
Literature Distribution Center for ON Semiconductor
19521 E. 32nd Pkwy, Aurora, Colorado 80011 USA
Phone: 303−675−2175 or 800−344−3860 Toll Free USA/Canada
Fax: 303−675−2176 or 800−344−3867 Toll Free USA/Canada
Email: orderlit@onsemi.com

N. American Technical Support: 800−282−9855 Toll Free USA/Canada
Europe, Middle East and Africa Technical Support:
Phone: 421 33 790 2910
Japan Customer Focus Center
Phone: 81−3−5817−1050

ON Semiconductor Website: **www.onsemi.com**

Order Literature: http://www.onsemi.com/orderlit

For additional information, please contact your local Sales Representative