

WiMOD LR Base Plus Firmware

Feature Specification Version 1.1

Document ID: 4000/40140/0137

IMST GmbH

Carl-Friedrich-Gauß-Str. 2-4

47475 KAMP-LINTFORT

GERMANY



Document Information

File name	WiMOD_LR_Base_Plus_Feature_Spec.docx
Created	2018-06-05
Total pages	17

Revision History

Version	Note
0.1	Created, Initial Version
0.2	Draft Version Created For Review
0.3	Preliminary Version
1.0	First Release for iM282A
1.1	Listen Before Talk added

Aim of this Document

This document outlines the WiMOD LR Base Plus firmware features. This firmware is designed for the WiMOD LR radio module iM282A.

Table of Contents

1. OVERVIEW	4
2. FEATURES	5
2.1 Host Controller Interface	5
2.1.1 HCI Message Format	5
2.1.2 Destination Endpoint Identifier (Dst ID)	5
2.1.3 Message Identifier (Msg ID)	5
2.1.4 Payload Field	6
2.1.5 Communication over UART	6
2.1.6 Radio Wakeup from Power Saving	6
2.1.7 Host Controller Wakeup	7
2.2 Radio Link / Modem Service	7
2.2.1 Addressing Scheme	7
2.2.2 Groupcast Service	7
2.2.3 Broadcast Service	7
2.2.4 Unconfirmed Data Exchange	8
2.2.5 Confirmed Data Exchange	8
2.2.6 Radio Packet Format	8
2.2.7 Physical Radio Settings	9
2.2.8 AES Encryption & Decryption	10
2.2.9 Listen Before Talk	10
2.3 Radio Link Test	11
2.4 Sensor App	12
2.4.1 Digital Signal Output	12
2.4.2 Link Monitor	12
2.4.3 Ack Message	12
2.4.4 I/O Mapping	12
2.5 Remote Control App	13
2.5.1 I/O Mapping	13
2.6 Radio Packet Sniffer	13
2.7 Device Management	14
3. APPENDIX	15
3.1 List of Abbreviations	15

3.2	List of References	15
3.3	List of Figures	15
4.	IMPORTANT NOTICE	16
4.1	Disclaimer	16
4.2	Contact Information	16

1. Overview

The WiMOD LR Base Plus firmware provides LoRa modem functionalities which allows to implement proprietary and cost sensitive radio networks with typical topologies like peer-to-peer and star configurations. The embedded radio protocol stack offers unacknowledged and acknowledged radio packet exchange with optional encryption and automatic power saving for battery driven applications.

Besides the modem services the firmware includes some example features which are typical for the application area of these radio modules: a tiny sensor application which demonstrates a periodic sensor data transmission and a remote control with digital input/output via radio link.

Finally this software provides two analyzing tools, which are helpful in developing radio based applications:

- Radio Link Test application which allows to analyze the radio link quality for different radio settings by means of the typical metrics Packet RSSI, Packet SNR and Packet Error Rate
- Radio Packet Sniffer which forwards received radio packets

These embedded development tools and all the other features can be used in combination with WiMOD LR Studio which offers an easy to use configuration, logging capabilities and data visualisation.

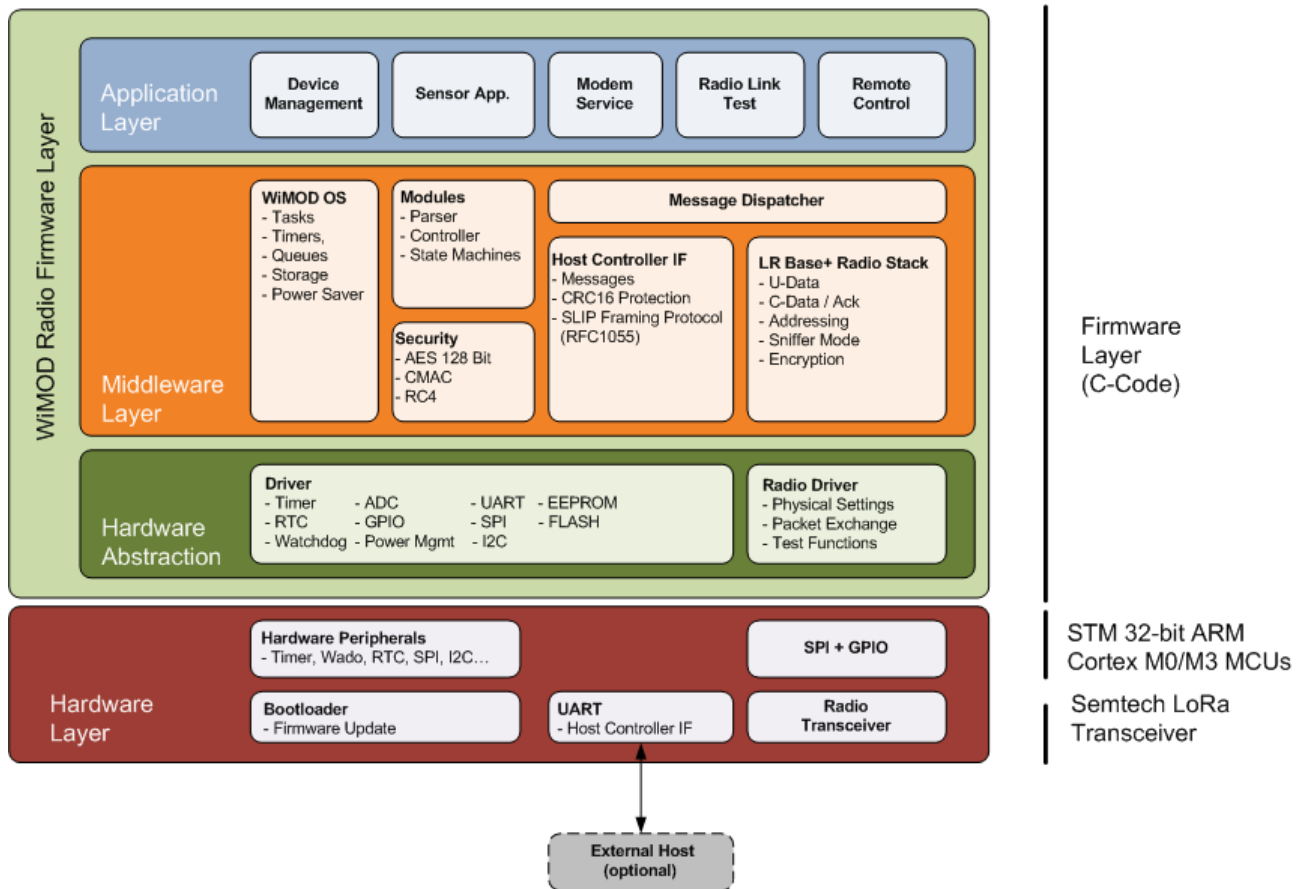


Fig. 1-1: WiMOD LR Base Plus Firmware Architecture



2. Features

2.1 Host Controller Interface

The host controller interface (HCI) offers access to the internal firmware services. The message based HCI protocol (see [1]) can be used for firmware configuration and radio communication. A simple UART interface (default settings: 115200 bps, 8N1) is used as physical interface and allows asynchronous message exchange in both directions: host controller to radio module and vice versa. The baudrate can be changed if needed.

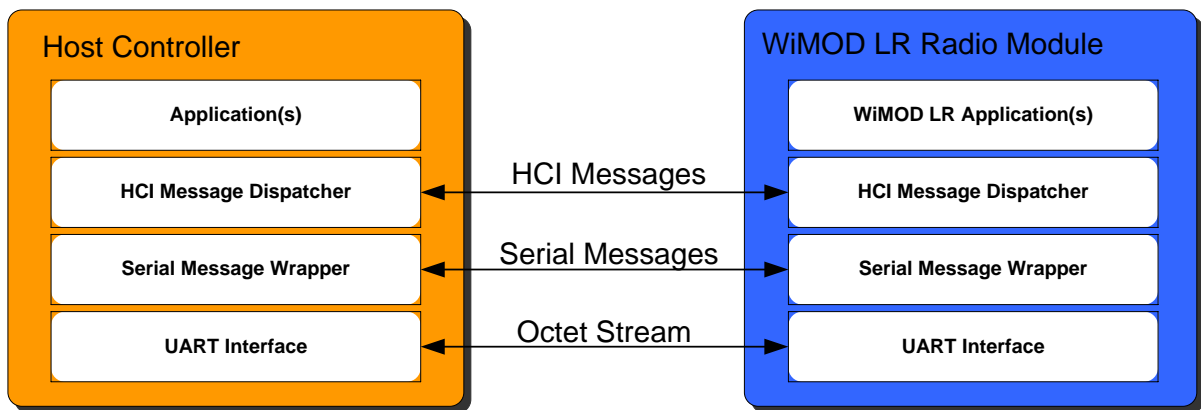


Fig. 2-1: Host Controller Communication

2.1.1 HCI Message Format

The following figure outlines the general message format which is used for communication purposes. A single HCI message consists of two header fields **Dst ID** and **Msg ID** and a **Payload Field** with variable length.

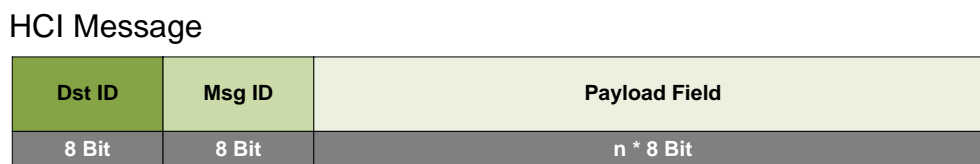


Fig. 2-2: HCI Message Format

2.1.2 Destination Endpoint Identifier (Dst ID)

This field is used to address one of the embedded application layer modules e.g Modem Service, Device Management, Radio Link Test, etc.

2.1.3 Message Identifier (Msg ID)

This field identifies a specific type of message and is used to trigger a corresponding service function or to indicate a service response or event when sent to the host controller.

2.1.4 Payload Field

The Payload Field has variable length and transports message depending parameters. The maximum size of this field is 300 Bytes.

2.1.5 Communication over UART

The standard host controller communication interface is a UART interface. The WiMOD LR HCI Protocol uses a SLIP (RFC1055) framing protocol when transmitted over asynchronous serial interfaces (UART).

All messages are protected by means of a 16-Bit CCITT CRC to support for bit error detection which is helpful in noisy environments and in case of battery powered devices when supply voltages are getting low.

The following figure shows the relationship between a single HCI message and the resulting SLIP message which may include some additional stuffing octets (SLIP ESC) to mark the special reserved SLIP END octets which might occur within a HCI message.

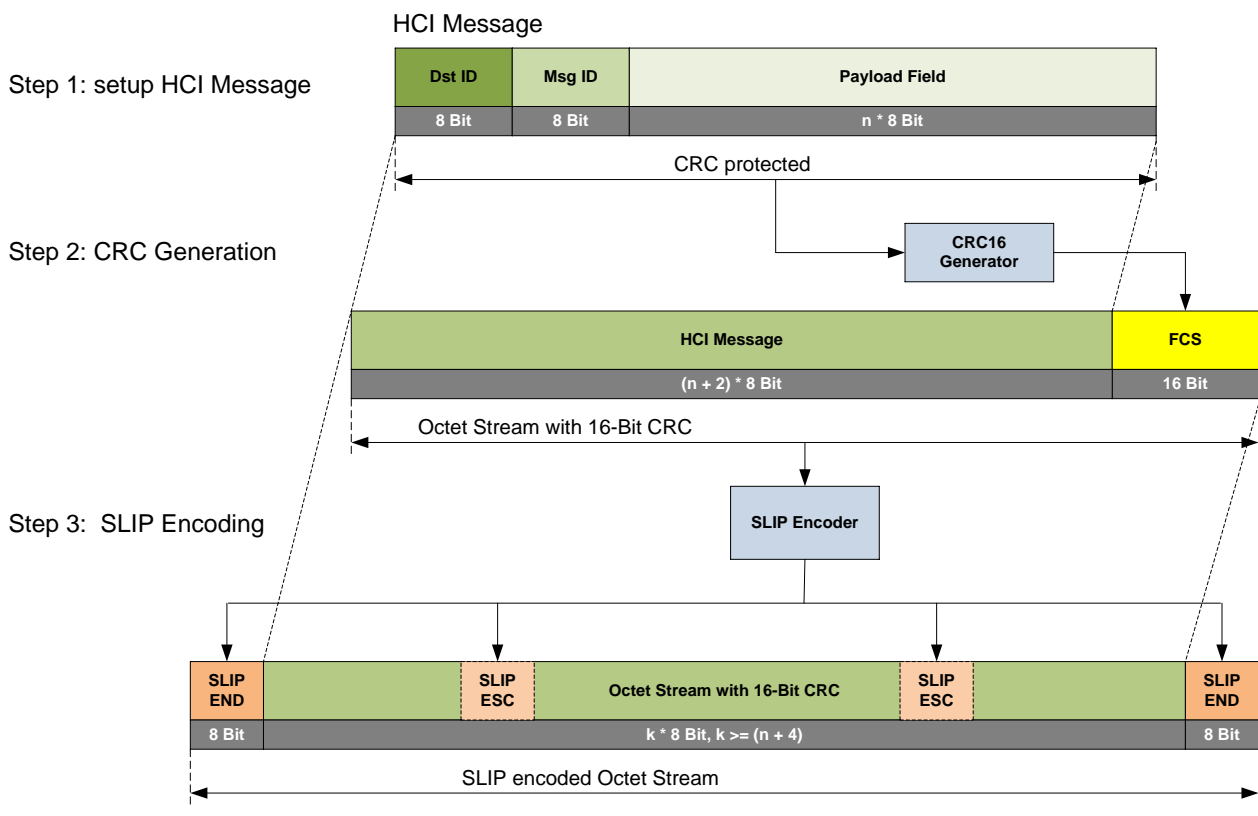


Fig. 2-3: Communication over UART

2.1.6 Radio Wakeup from Power Saving

The host controller interface is designed to support the automatic power saving feature. When ever possible the firmware will enter the lowest power consumption state. Reception of HCI messages requires a short wakeup phase to stabilize the internal clocks and baudrate generator. The embedded STM32 microcontroller requires ~3ms until the clock system is stable enough for



proper character decoding. For radio wakeup a host controller can simply send about 30 additional **SLIP END** (0xC0) characters @115200bps (~3ms) prior to any HCI message. The corresponding signal change on the UART RX input pin will generate an interrupt which reactivates the embedded firmware.

2.1.7 Host Controller Wakeup

In case a host controller requires power saving too it is possible to configure the number of **SLIP END** (0xC0) wakeup characters in the opposite direction for wakeup purpose. Depending on the microcontroller type it might be necessary to change the UART RX input pin to standard input pin mode during runtime to detect a falling / rising signal edge while the controller remains in a power saving state.

2.2 Radio Link / Modem Service

The modem service can be used to send radio messages from one radio device to another or to a group of other radio devices in an easy to use way. This feature has no limits regarding the network topology and offers full flexibility via configuration of addresses, radio modes and other typical radio settings.

2.2.1 Addressing Scheme

Each radio device has its own configurable **16-Bit Device Address** and **8-Bit Group Address** which can be used for explicit addressing. On transmitter side both address fields must be passed as **Destination Address** in combination with the application payload from the host controller to send a message via radio. Every radio message contains the **Destination Address**, **Source Address**, some radio protocol information and the actual application payload. The receiver of a radio message compares the **Destination Address** of the radio message with its own configured **Device Address** and **Group Address**. In case of a successful address match, the received message will be forwarded via HCI to the connected host controller. Otherwise the message will be discarded.

2.2.2 Groupcast Service

Beside explicit addressing of single radio devices it is possible to address a group of devices. In this case the host controller must select the specific **8-Bit Group Address** and must set the **Destination Address** to the reserved **BROADCAST_DEVICE_ADDRESS**.

2.2.3 Broadcast Service

In case a message should be processed by all devices in range independent of the assigned group and device address, the reserved **BROADCAST_GROUP_ADDRESS** and **BROADCAST_DEVICE_ADDRESS** must be used in combination.

2.2.4 Unconfirmed Data Exchange

This service can be used to exchange radio messages in an unreliable way, i.e. the corresponding **U-Data** radio message is sent once from the transmitting device to any receiver in range. No acknowledgement message is sent from a receiver back to the sender to confirm the received radio message.

This service is suitable whenever no acknowledgement is needed at all, the application wants to control the acknowledgement on its own or if a message is addressed to multiple receivers (Groupcast or Broadcast) due to collision of the resulting acknowledgement messages.

2.2.5 Confirmed Data Exchange

An application which needs a simple confirmation of a transmitted radio message can use this service. In this case the receiver swaps the **Destination** and **Source Address** of the received **C-Data** radio message and sends back an acknowledge message which can carry a few bytes of piggybacked application payload. This application payload must be stored in the radio module prior to the reception of the **C-Data** radio message.

The original transmitter device on the other side opens a reception window automatically and waits for an acknowledgement from the peer device. On successful reception an acknowledge indication message will be forwarded to the connected host controller. Otherwise an acknowledge timeout error will be sent.

2.2.6 Radio Packet Format

The following figure outlines the relationship between a HCI message (see [1]), sent from the host controller and the radio message, sent from the radio module. Please note, that every radio packet starts with an additional preamble and modulation depending header which are not displayed here. Furthermore every radio packet includes a checksum for bit error detection on receiver side.

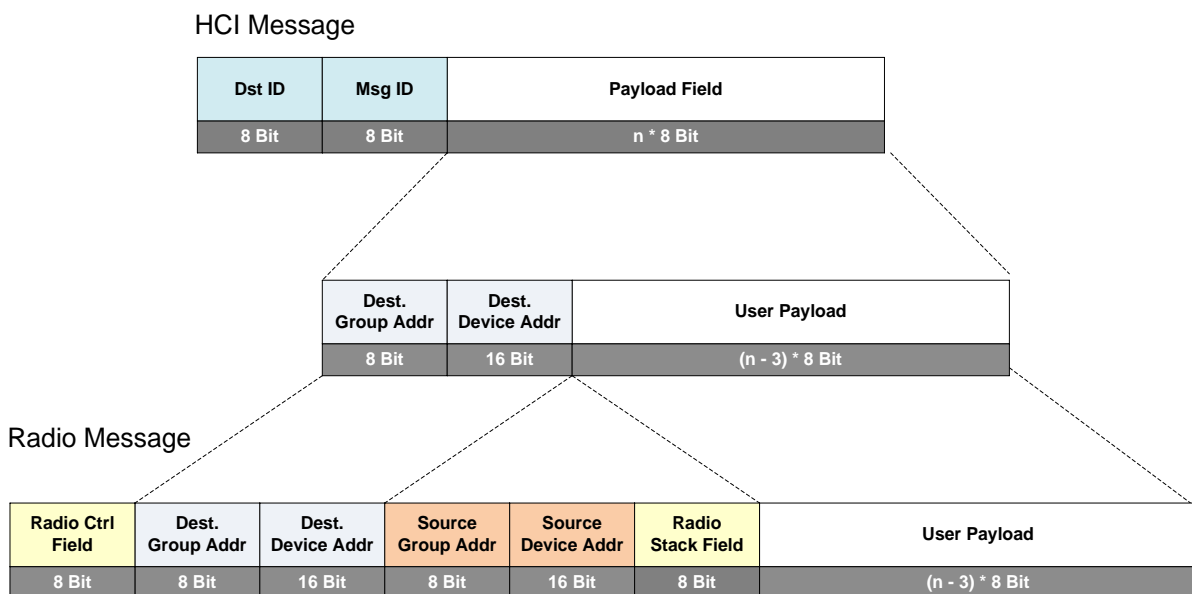


Fig. 2-4: Tx Radio Message and HCI Message (not encrypted format)

The next figure outlines the relationship between the radio message, received on the radio module and the forwarded HCI message.

Radio Message

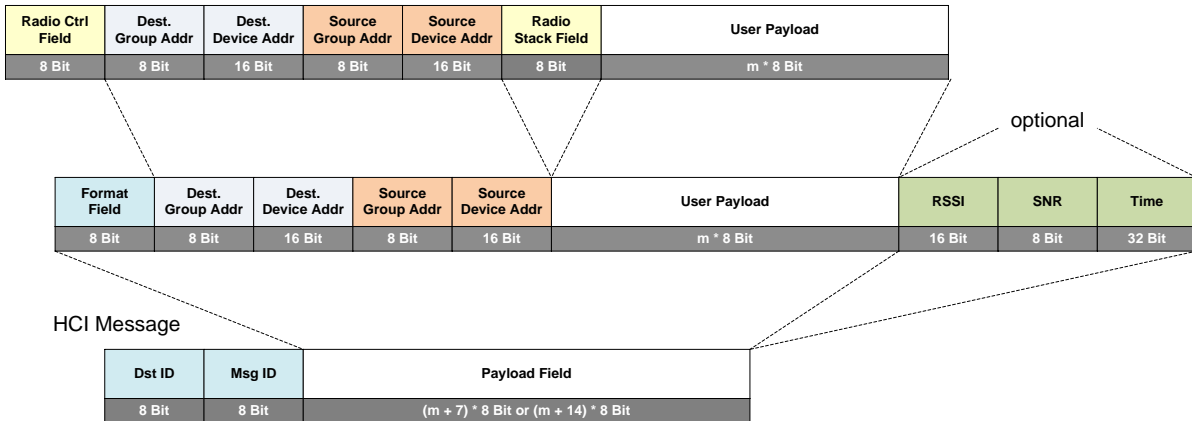


Fig. 2-5: Rx Radio Message and HCI Message (not encrypted format)

2.2.7 Physical Radio Settings

The physical radio settings e.g. frequency, modulation, power level, spreading factor etc. which will be used for radio communication are adjustable through the [Device Management](#) configuration service.

2.2.8 AES Encryption & Decryption

The **U-Data** and **C-Data** radio packets can be encrypted if needed. The packet encryption and required AES key can be configured through the *Device Management* configuration service. The used encryption scheme is based on the generic algorithm described in IEEE 24 802.15.4/2006 Annex B [IEEE802154] using AES with a key length of 128 bits.

Encrypted radio packets are transmitted with the following radio packet format:

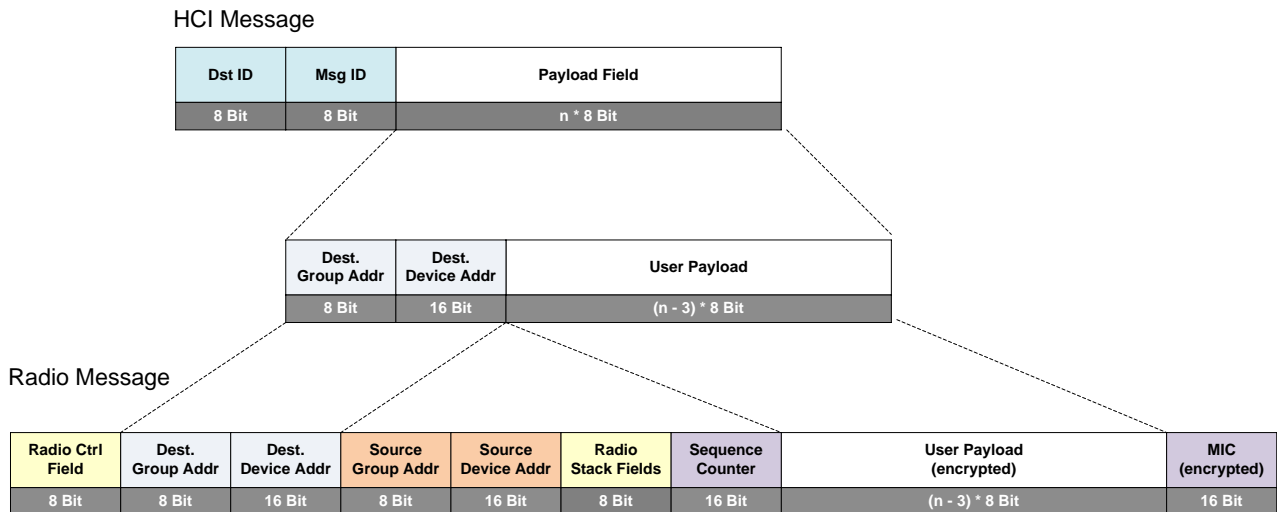


Fig. 2-6: Encrypted Radio Message Format

The user payload and attached message integrity code (MIC) field are encrypted using an AES 128-Bit Counter Mode which turns a block cipher into a stream cipher.

2.2.9 Listen Before Talk

The Listen Before Talk (LBT) procedure can be activated for every unconfirmed and confirmed radio message.

If LBT is activated, the radio will measure and test the RSSI for the configured RF channel. The measured RSSI value will be compared against a configurable LBT threshold. In case of a "Media Busy" detection the radio module will not transmit the radio message, indeed a HCI Tx Indication message with "Media Busy" status will be sent to the initiating host controller.

2.3 Radio Link Test

This feature can be used to analyze the radio link quality and range with different physical radio settings. The test itself is based on packet counting. A primary radio device connected to a host transmits a series of test packets to secondary device which answers with a corresponding response message. The response message includes the number of received test messages and the received RSSI and SNR values. Finally the primary device sends a status message to the host which has to evaluate these results. It is recommended to use this feature in combination with the WiMOD LR Studio which provides a simple configuration and visualization GUI for this purpose. The GUI shows the link test results like packet error rate, RSSI values and allows to capture those results via log files.

The following figure outlines the radio link test message flow in more detail:

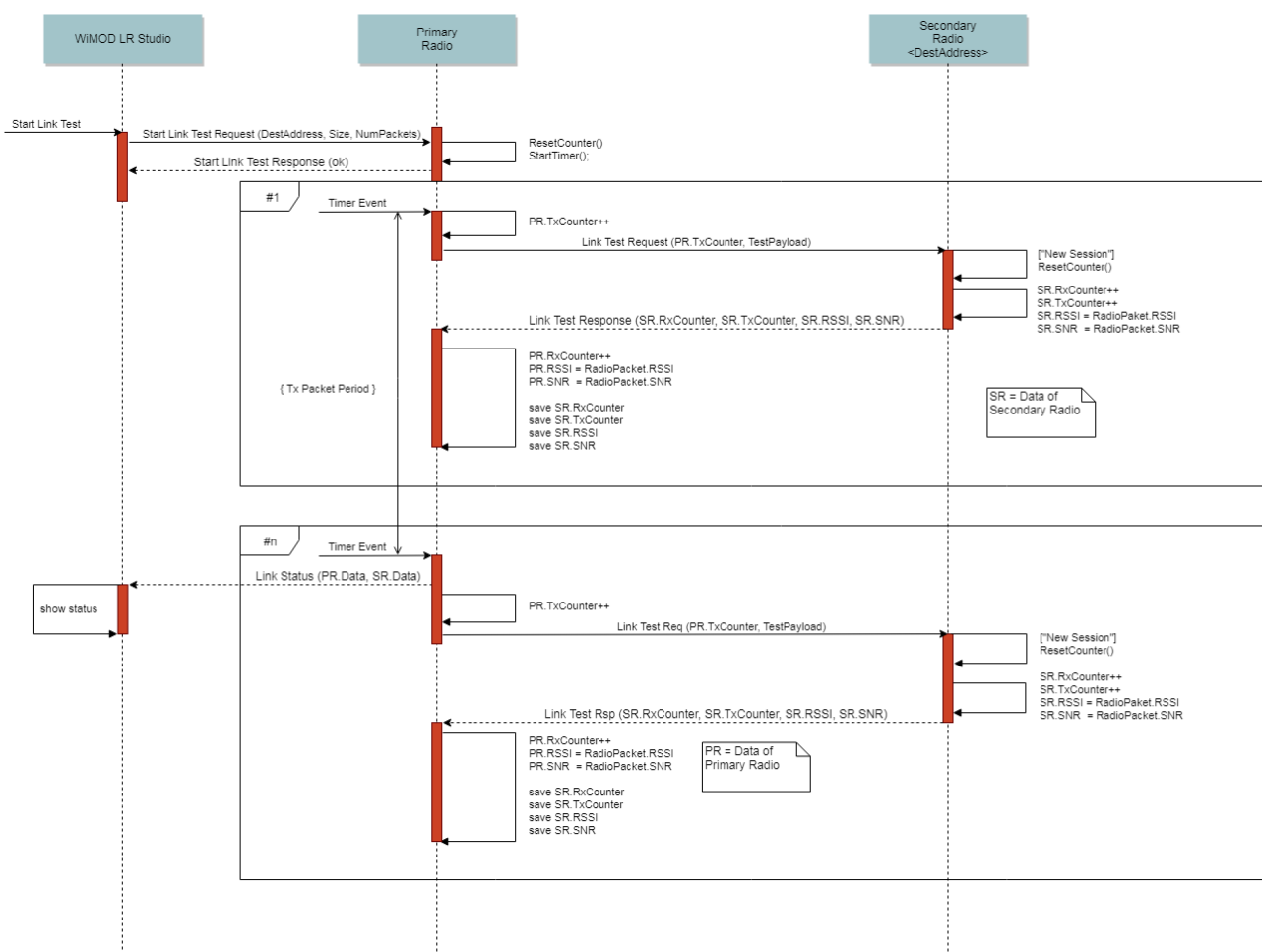


Fig. 2-7: Radio Link Test

2.4 Sensor App

The Sensor App is a typical application which demonstrates the functionality of a wireless sensor. This application samples some typical sensor data e.g.: analog voltage via ADC, digital inputs, internal battery state, etc. and transmits this data in a periodically manner to a receiver node in range. The transmit period and receiver destination address are configurable. The receiver will forward the data via HCI message to a connected host controller.

2.4.1 Digital Signal Output

On receiver side it is possible to output one digital input signal of a specific digital input pin of the transmitter side.

2.4.2 Link Monitor

An additional digital output can be configured to operate as link monitor i.e. the output indicates if the RF link between sensor and receiver operates well. The link monitor sets an output pin and starts a timer when ever a sensor packet will be received. If no further packet will be received the timer expires and the output will be reset. The link timeout can be configured and should be aligned with the data transmit period (e.g.: timer timeout > 3.5 * transmit period).

2.4.3 Ack Message

An Ack Message can be enabled which will be transmitted back, from the receiver to the sensor on every received sensor data packet. The Ack Message includes the digital input state of all three digital input pins of the receiver. These input states are visible on digital output pins on the sensor side.

2.4.4 I/O Mapping

The following table lists the input and output signals which are used for this application:

Function	iM282A Modul Pin	WiMOD Demoboard	
		Function	Header Connection
Inputs			
Enable Data Transmission	15	DIP SWITCH #1	X5.3 – X5.4
Digital Input #1	13	Pushbutton #1	X5.7 – X5.8
Digital Input #2	12	Pushbutton #2	X5.9 – X5.10
Digital Input #3	14	Pushbutton #3	X5.1 – X5.2
Analog Input #1	29	Potentiometer	X5.11 – X5.18
Outputs			
Received Digital Input #1 Signal	8	LED #1 (Red)	X5.17 / X5.19 – X5.14
Link Monitor State	9	LED #4 (Orange)	X6.7 – X5.12

2.5 Remote Control App

The Remote Control App simply transmits a specific radio message whenever a certain input pin detects a falling edge. The receiver node can be configured to send a HCI message to a connected host and/or to toggle a specific output pin.

2.5.1 I/O Mapping

The following table lists the input and output signals which are used for this application:

Function	iM282A Modul Pin	WiMOD Demoboard	
		Function	Header Connection
Inputs			
Digital Input #1	13	Pushbutton #1	X5.7 – X5.8
Outputs			
Remote Control Message Received Toggle Event	8	LED #1 (Red)	X5.17 – X5.18

Note: Pushbutton #1 must be explicitly configured for Remote Control functionality via Radio Settings to avoid conflicts with other features.

2.6 Radio Packet Sniffer

The firmware supports a special radio mode called *Sniffer* mode. While operating in *Sniffer* mode the firmware simply forwards every received radio packet without address filtering and interpretation in raw format to the connected host controller.

This feature is suitable in development of own applications when monitoring of radio traffic is required. In combination with the WiMOD LR Studio it is possible to visualize and to log those received radio messages for further analysis.

2.7 Device Management

The so called Device Management provides general services for module configuration, module identification, and everything which is not related to the data exchange via radio link. The following services are available:

- Ping message for simple HCI communication test
- Device Reset
- Device Information
- Firmware Information
- Radio Stack Configuration
- System Status
- RTC Synchronisation
- Alarm Configuration
- Device HCI Settings
- Bootloader activation for firmware update over serial interface

3. Appendix

3.1 List of Abbreviations

CCITT	Comité Consultatif International Télégraphique et Téléphonique
CRC	Cyclic Redundancy Check
HCI	Host Controller Interface
LR	Long Range
LoRa	Long Range
RTC	Real Time Clock
RSSI	Received Signal Strength Indicator
SLIP	Serial Line Internet Protocol (RFC1055)
SNR	Signal to Noise Ratio
UART	Universal Asynchronous Receiver/Transmitter
WiMOD	Wireless Module by IMST

3.2 List of References

[1] WiMOD_LR_Base_Plus_HCI_Spec.pdf

3.3 List of Figures

Fig. 1-1: WiMOD LR Base Plus Firmware Architecture	4
Fig. 2-1: Host Controller Communication	5
Fig. 2-2: HCI Message Format	5
Fig. 2-3: Communication over UART	6
Fig. 2-4: Tx Radio Message and HCI Message (not encrypted format)	8
Fig. 2-5: Rx Radio Message and HCI Message (not encrypted format)	9
Fig. 2-6: Encrypted Radio Message Format	10
Fig. 2-7: Radio Link Test	11

4. Important Notice

4.1 Disclaimer

IMST GmbH points out that all information in this document is given on an “as is” basis. No guarantee, neither explicit nor implicit is given for the correctness at the time of publication. IMST GmbH reserves all rights to make corrections, modifications, enhancements, and other changes to its products and services at any time and to discontinue any product or service without prior notice. It is recommended for customers to refer to the latest relevant information before placing orders and to verify that such information is current and complete. All products are sold and delivered subject to “General Terms and Conditions” of IMST GmbH, supplied at the time of order acknowledgment.

IMST GmbH assumes no liability for the use of its products and does not grant any licenses for its patent rights or for any other of its intellectual property rights or third-party rights. It is the customer’s duty to bear responsibility for compliance of systems or units in which products from IMST GmbH are integrated with applicable legal regulations. Customers should provide adequate design and operating safeguards to minimize the risks associated with customer products and applications. The products are not approved for use in life supporting systems or other systems whose malfunction could result in personal injury to the user. Customers using the products within such applications do so at their own risk.

Any reproduction of information in datasheets of IMST GmbH is permissible only if reproduction is without alteration and is accompanied by all given associated warranties, conditions, limitations, and notices. Any resale of IMST GmbH products or services with statements different from or beyond the parameters stated by IMST GmbH for that product/solution or service is not allowed and voids all express and any implied warranties. The limitations on liability in favor of IMST GmbH shall also affect its employees, executive personnel and bodies in the same way. IMST GmbH is not responsible or liable for any such wrong statements.

Copyright © 2018, IMST GmbH

4.2 Contact Information

IMST GmbH

Carl-Friedrich-Gauss-Str. 2-4
47475 Kamp-Lintfort
Germany

T +49 2842 981 0

F +49 2842 981 299

E wimod@imst.de

I www.wireless-solutions.de