MCU-RF

Demo software user guide for 80 bit product family

Table of Contents Page

1 Introduction 10

2 Installation 11

2.1 Hardware Installation of ADR2 Demo Reader 11
2.2 Software Installation 11

3 Schematics 12

4 Communication Ports 14

4.1 Com – Port search 14
4.1.1 Repeat Automatic Device Search 17
4.2 Manual Com-Port Connection 18

5 Applications for DST80 devices 19

5.1 Settings 19
5.2 Resonant Trimming 20
5.2.1 Resonant Trimming (Reader controlled) 21
5.2.2 Resonant Trimming Protocol overview 21
5.3 Passive Entry, Passive Start with a RAID / CRAID 26
5.4 Immobilizer Read Page (DST80) 29
5.4.1 Problems with DST80 Transponder Immobilizer function 30
5.4.2 Example: Read Page 3 command (DST80) 31
5.4.3 Example: Read Page 8 response (DST80) 32
5.5 Immobilizer Program Page (DST80) 33
5.5.1 Example: Program Page 8 command (DST80) 34
5.6 Immobilizer Lock Page (DST80) 35
5.6.1 Example: Lock Page 8 command (DST80) 36
5.7 Using the TPIC 84134 Antenna Extension Board 37

6 Serial protocol description 39

6.1 RS232 / USB settings 39
6.2 Setup protocol overview 39
6.3 Setup Protocol Responses 40
6.4 Setup Protocol Examples 40
6.4.1 “Get Version Information” 40
6.4.2 “Write BLC Timing Information” 41
6.5 Block Check Character 42
6.6 Immobilizer protocol downlink overview 43
6.7 Immobilizer protocol downlink command byte definition 44
6.8 Immobilizer protocol response overview 45
6.9 Specific Protocols 46
6.9.1 CRAID PEPS Telegram 46
6.9.2 CRAID PEPS Response / RKE Telegram 47
6.9.3 DST80 Immobilizer 48
6.9.4 AES Immobilizer 49
6.9.5 AES Immobilizer Response 50
6.9.6 AES PEPS Telegram 51
6.9.7 AES Burst Read / Anti-Collision AES Encryption 52
6.9.8 Trimming: Get Frequency (“Others”) 53
6.9.9 Trimming: Trim Byte (“Others”) 53
6.9.10 Trimming: Get Frequency (RAIDAES) 54
6.9.11 Trimming: Trim Byte (RAIDAES) 54
6.9.12 RF430F59xx UHF response 55
6.10 Command-Byte Structure 56
6.10.1 Advanced LF Reader Protocols 57
6.10.2 Advanced Command Byte Structure 64
6.11 UHF Passive Entry/ Passive Start / Remote Keyless Entry protocol 65

6.11.1 Communication Link Settings....65
6.11.2 Communication Protocol....65

Summary of Figures Page

Figure 1: Base Station Schematics **12**
Figure 2: Com Port Search **14**
Figure 3: Connected Hardware Tools **15**
Figure 4: Transponder Timing Settings **16**
Figure 5: New Automatic Device Search **17**
Figure 6: Toggle Manual Selection / Automatic Search of Com Port **18**
Figure 7: Access Settings Menu **19**
Figure 8: *Transfer Settings* and *Finished* **19**
Figure 9: Resonant Frequency Trimming **20**
Figure 10: Configure CRAID EEPROM **27**
Figure 11: Transponder: Read Page (DST80) **29**
Figure 12: Coding Configuration (DST80) **30**
Figure 13: Example: Program Page 8 (DST80) **33**
Figure 14: Example: Lock Page 8 (DST80) **35**
Figure 15: TPIC connection **37**
Figure 16: Antenna Extension Configuration **37**

About This Manual

This manual describes the modules and peripherals of the MCU-RF DST80 family of devices. Each description presents the module or peripheral in a general sense. Not all features and functions of all modules or peripherals may be present on all devices. In addition, modules or peripherals may differ in their exact implementation between device families, or may not be fully implemented on an individual device or device family.
Pin functions, internal signal connections, and operational parameters differ from device to device. The user should consult the device-specific data sheet for these details.
The LF communication scheme is described in a dedicated LF user guide.

Related Documentation from Texas Instruments

FCC Warning

This equipment is intended for use in a laboratory test environment only. It generates, uses, and can radiate radio frequency energy and has not been tested for compliance with the limits of computing devices pursuant to subpart J of part 15 of FCC rules, which are designed to provide reasonable protection against radio frequency interference. Operation of this equipment in other environments may cause interference with radio communications, in which case the user himself will be required to take whatever measures may be required to correct this interference.

Notational Conventions

Program examples, are shown in a special typeface.

Definitions

Base Station	Communication partner able to communicate by the use LF telegrams with a transponder
Immobilizer Mode	Short range LF communication between base station and transponder running without battery support on transponder side
Downlink	LF communication from the Base Station to the transponder
Charge Phase	LF energy transfer from the Base Station to the transponder; energy is stored in the charge capacitor for the uplink phase
Uplink, Response	LF communication from the transponder to the base station
RKE	Remote Keyless Entry: UHF communication from the key fob to the vehicle initiated by a push button press
PEPS	Passive Entry/ Passive Start: The Base Station sends a LF telegram which requests a UHF response from the Key Fob

1 Introduction

The RFID Demo software can be used to execute the main features of TI MCU-RF DST80 product portfolio. Resonant trimming, transponder communication and passive entry communication can be executed. The Demo software synchronizes its own settings with the device configuration as far as possible to achieve valid data communication and response analyzing. Some devices only offer partial functionality (e.g. smaller memory or trimming only). This is not considered in the demo software and needs to be managed by the user.

The tool doesn't require an installation run as long as Microsoft .NET Framework is installed on the computer. A com port or USB port is required to communicate with the demo hardware.

2 Installation

2.1 Hardware Installation of ADR2 Demo Reader

1. Connect the external USB Interface Board to the two designated sockets on the bottom-left side of the Base Station board. Make sure to connect the device in correct orientation – the Texas Instruments logo of the boards should point in the same direction!
2. Connect the Loop Antenna to the corresponding connectors in the top-right corner of the Base Station Board, labelled 1 to 6.
3. Connect the USB Interface Board to a PC using the Mini-USB Cable.
4. (Optional) Apply an additional power source to the power-connector of the Base Station (12V DC) to achieve an increased transmission range and/or drive a bigger antenna.

2.2 Software Installation

1. Go to the product page of the ADR2 Demo Reader: http://www.ti.com/tool/ri-acc-adr2-10
2. Download the RFID Demo Software
3. Extract the ZIP-file into a folder and execute the RFID Demo Software executable – no installation required.
4. To use DST80 functionality, no activation code is required. Just leave the textbox blank and click *OK*

3 Schematics

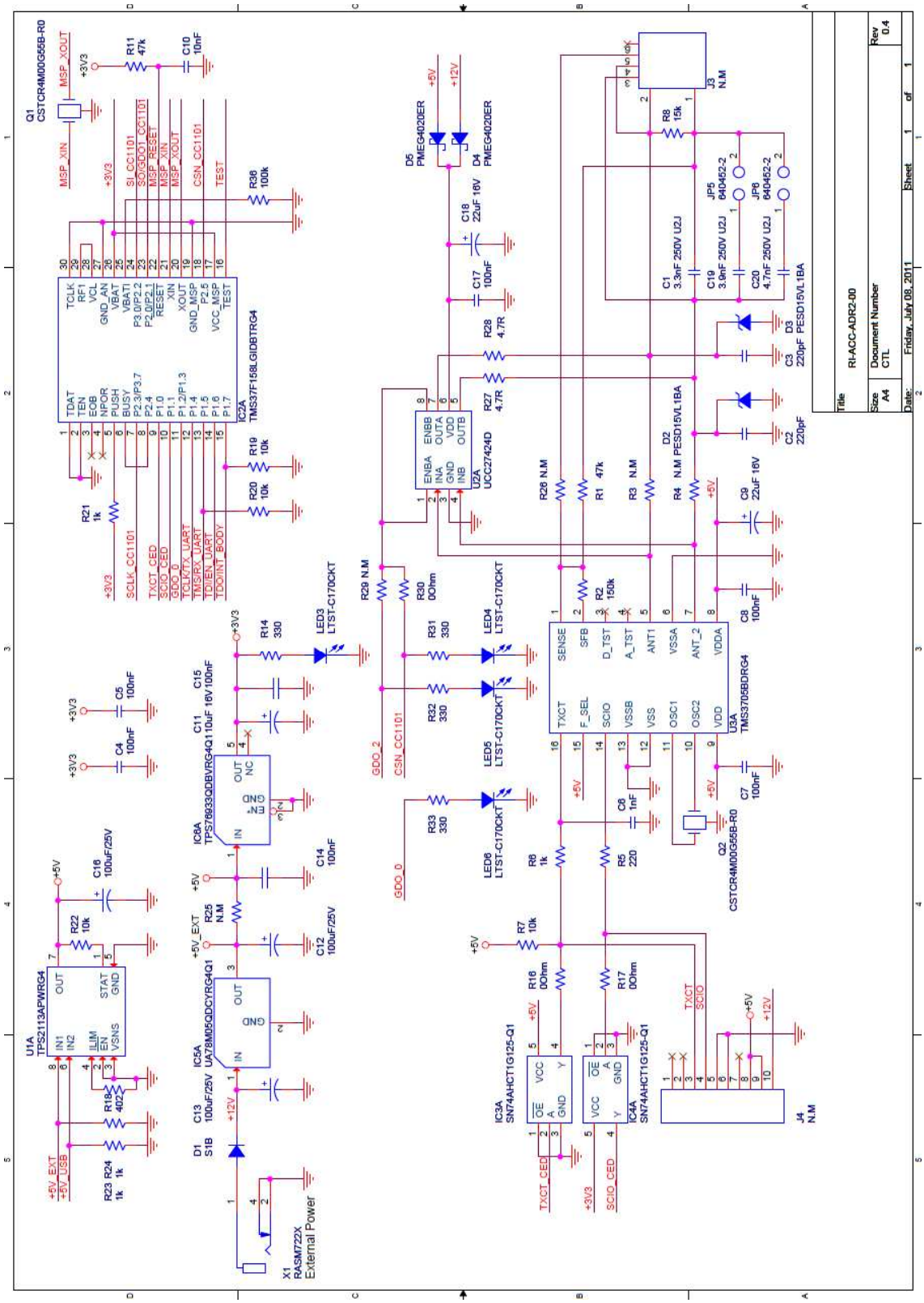


Figure 1: Base Station Schematics

4 Communication Ports

4.1 Com – Port search

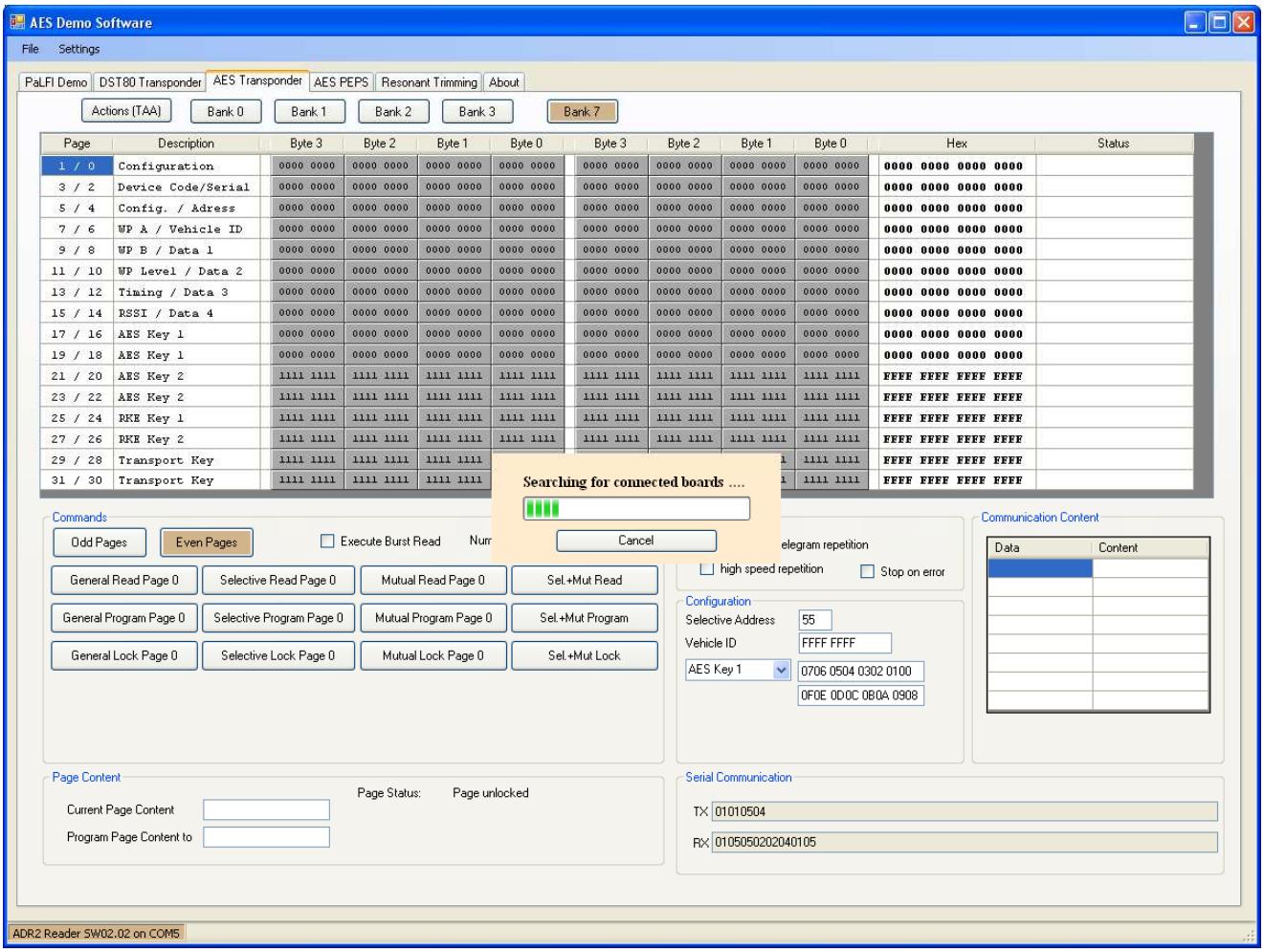


Figure 2: Com Port Search

After start-up of the AES Demo Software, it searches automatically for attached demo readers and probe test boxes.
The tool supports up to 3 Demo readers and 1 Probe Test box.

After completion of the Com port search up to 3 found devices are displayed in the status line:

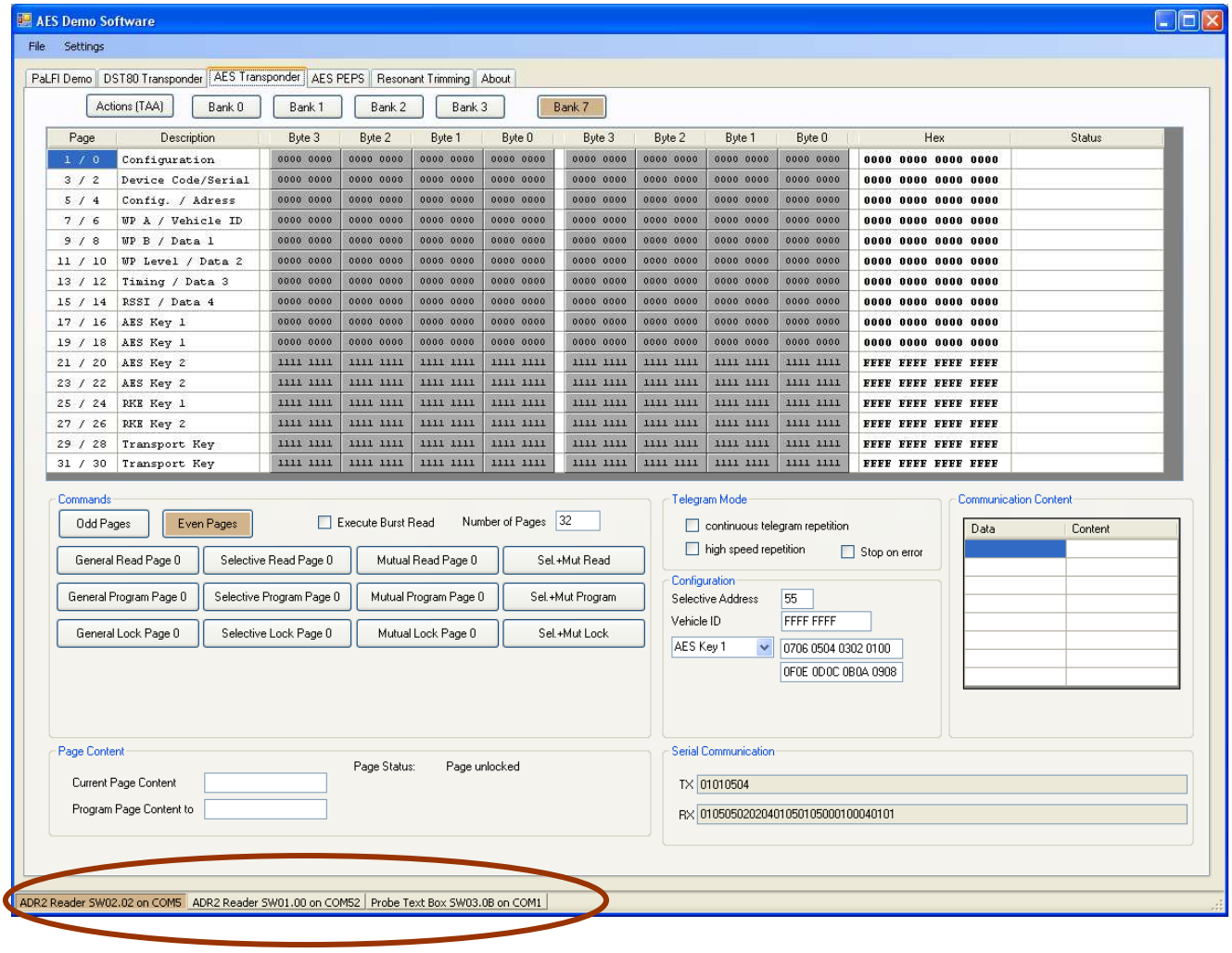


Figure 3: Connected Hardware Tools

The highlighted text indicates the currently used com port for communication. Each attached device is automatically initialized with the communication parameters valid for the currently used tab.
For example in the screen shot above the ADR2 Reader is initialized with the BLC LF communication parameters configured in the ‘Settings’ menu shown below:

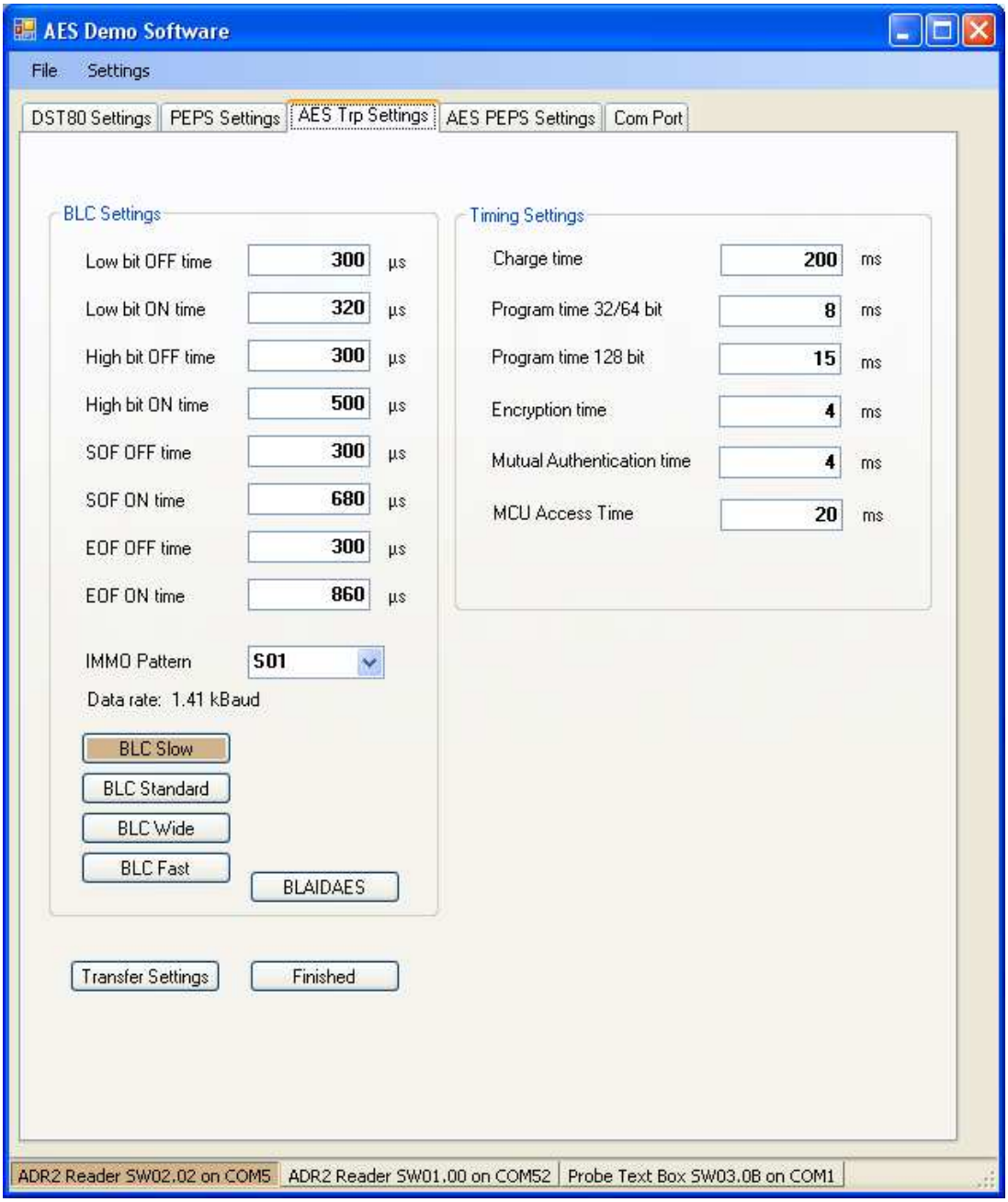


Figure 4: Transponder Timing Settings

4.1.1 Repeat Automatic Device Search

In some cases it might be desirable to repeat the Automatic Device Search. For example when a device is connected which supports no auto-detection (e.g. Probe Test Box) while the software is already running.

In that case, just click on the *Com Port Search* button in the status bar.

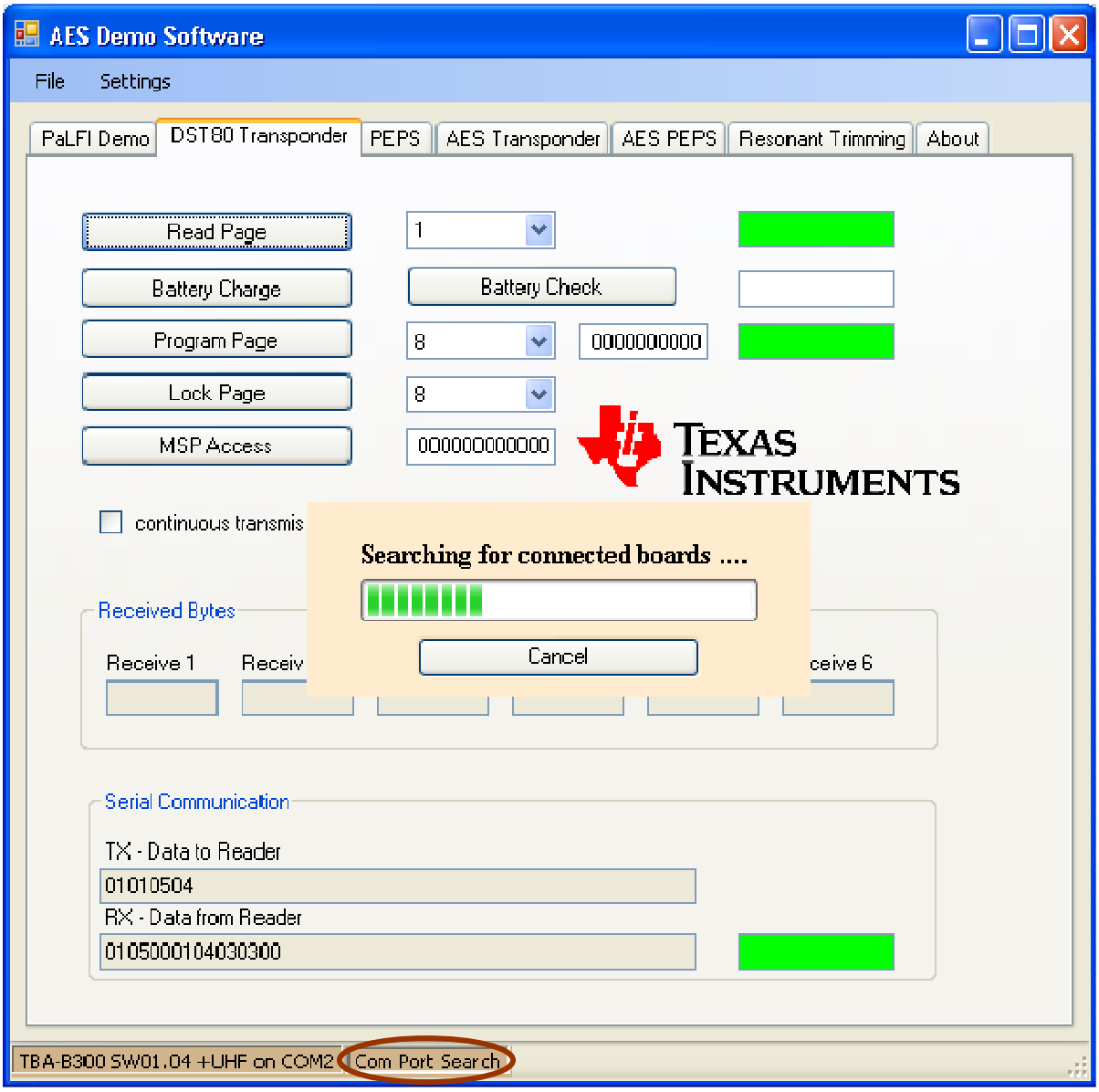


Figure 5: New Automatic Device Search

Note:

If the Automatic Com Port Search is deactivated (see chapter Manual Com-Port Connection) it will get reactivated by executing an Automatic Com Port Search.

4.2 Manual Com-Port Connection

If problems with the Automatic Com Port search are experienced or for other reasons a manual selection of the Com Port is desired, the Automatic Com Port Search should be deactivated and the corresponding Com Port should be chosen manually.

To do so following steps are required:

1. Activate the *Settings* tabs
2. Select the *Com Port* Tab Page
3. Uncheck *Automatic Search*
4. Select the Com Port which the device is connected to
5. To deactivate the *Settings* tabs and return to the last used tab click *Finished*

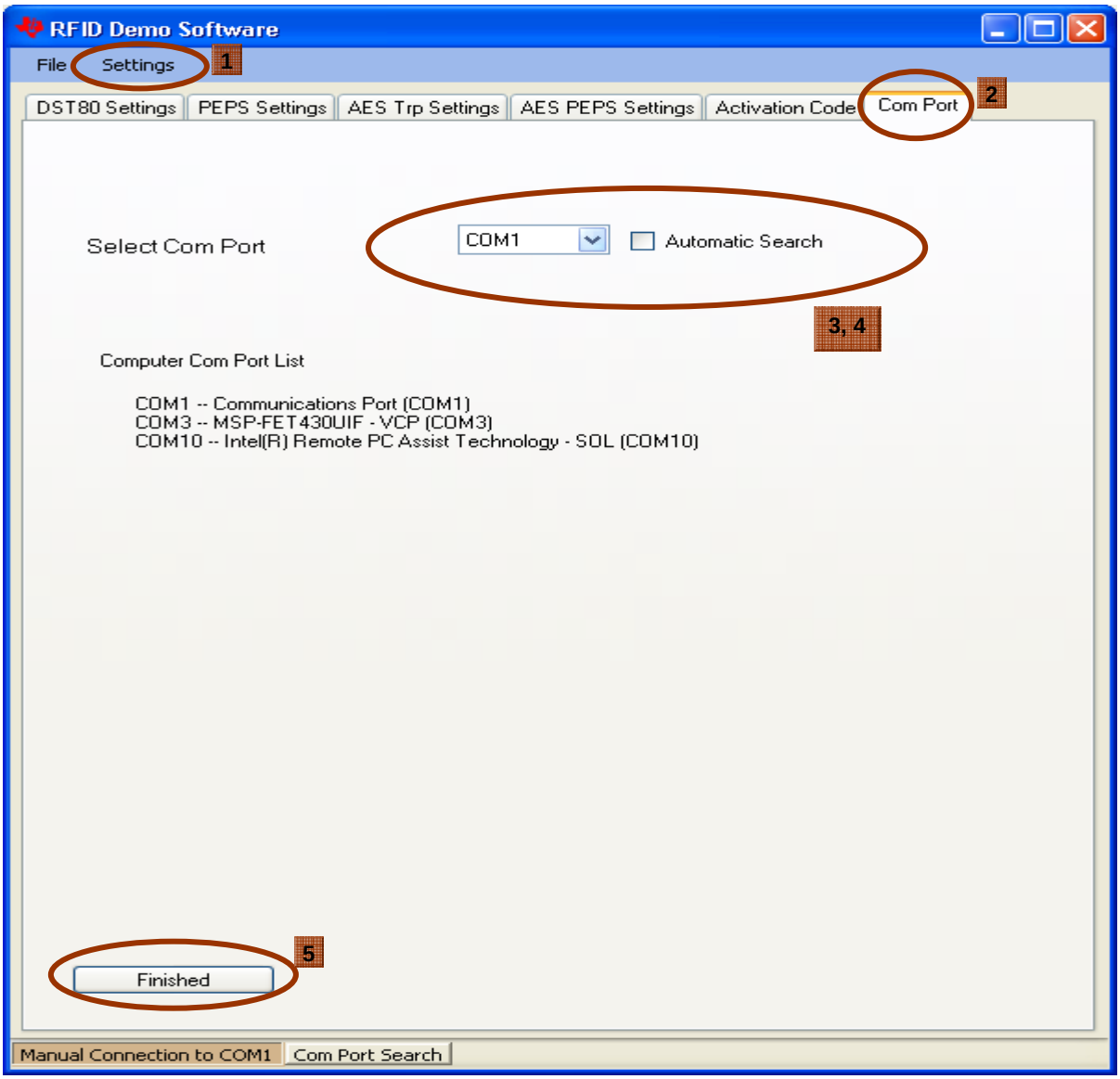


Figure 6: Toggle Manual Selection / Automatic Search of Com Port

5 Applications for DST80 devices

5.1 Settings

To configure bit timings, burst durations, com port connections and more the *Settings* tab page can be used. To access this tab page click on *Settings* as shown below:

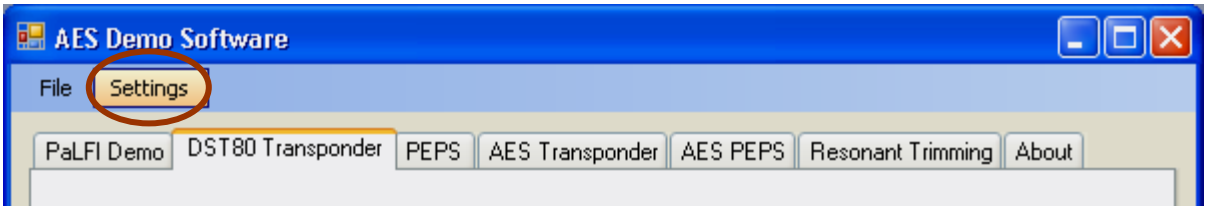


Figure 7: Access Settings Menu

On all *Settings* tab pages there are two buttons *Transfer Settings* and *Finished*.

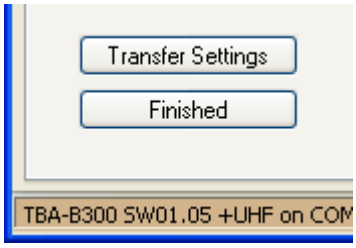


Figure 8: *Transfer Settings* and *Finished*

Transfer Settings transfers the currently displayed settings to the selected reader or the selected com port but stays on the *Settings* tab page.

Finished transfers the settings exactly like the *Transfer Settings* button but switches to the corresponding normal (non-settings) tab page or the tab page previously used.
For example if the *PEPS Settings* are currently configured and then the *Finished* button is pushed the program will switch to the *PEPS* tab page.

5.2 Resonant Trimming

The AES Demo Software supports Resonant Trimming for all devices through the Test Interface.

Requirements:

- Probe Test Box
  OR
- TBA-B300

To execute the resonant trimming procedure, following steps are required:

1. Connect the Reader / Probe Test Box to the PC and to the Test interface of the device.
2. Start the RFID Demo Software
3. Select tab “Resonant Trimming”
4. Select the device to be trimmed in the *Device Selection* combo box
5. Click on *Automatic Trim All*

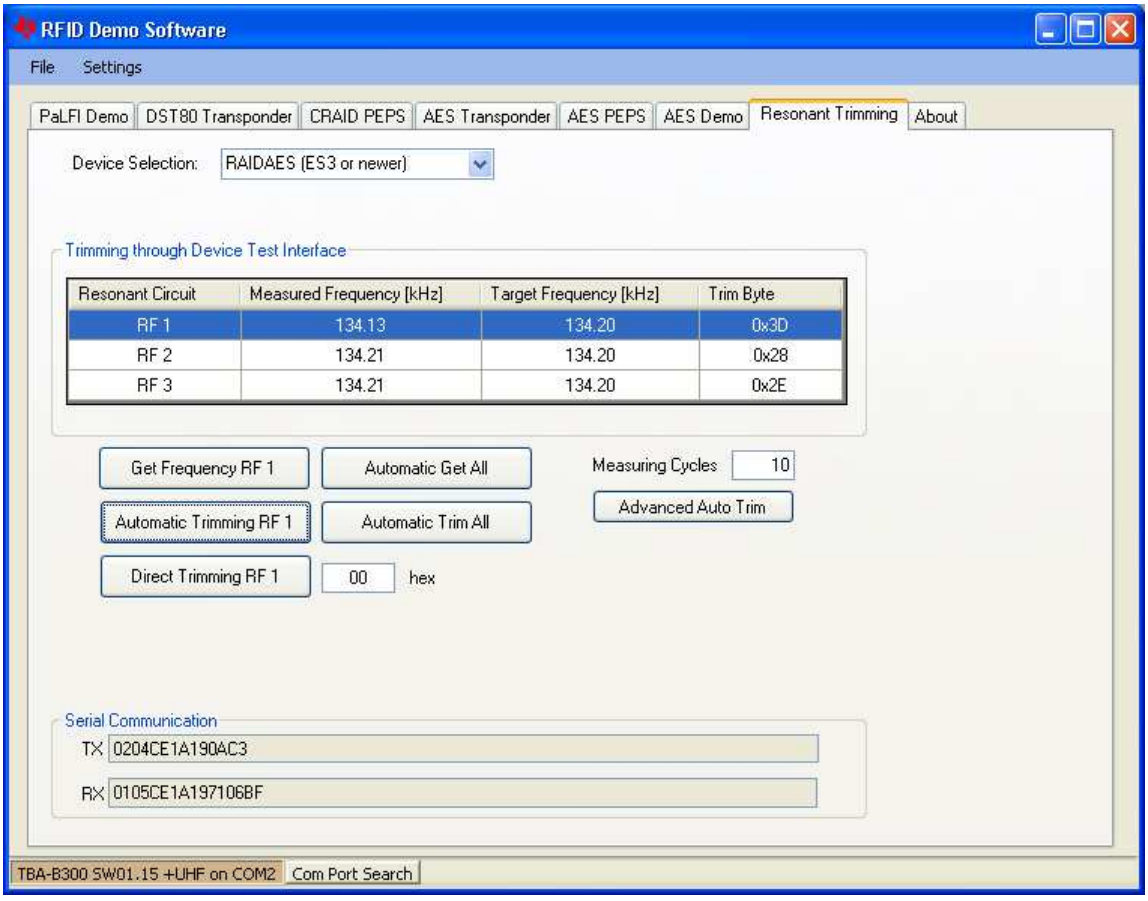


Figure 9: Resonant Frequency Trimming

The Demo Software will show the trimmed frequency in the field “Measured Frequency”. In case the resonant frequency couldn’t be trimmed to the target frequency a notice will be displayed providing further instructions.

5.2.1 Resonant Trimming (Reader controlled)

It's also possible to perform a reader controlled automatic trimming of all channels.

Requirements:
- TBA-B300

1. Connect the Base Station to the PC and to the Test interface of the device.
2. Start the RFID Demo Software
3. Select tab "Resonant Trimming"
4. Select the device to be trimmed in the *Device Selection* combo box
5. Click on *Advanced Automatic Trimming*
6. Wait until results are shown in the table above. The orange LED3 on the Base Station indicates trimming activity.

5.2.2 Resonant Trimming Protocol overview

The used protocol depends on the chosen device. There are following device types available:

1. *RAIDAES (ES3 and newer)*
   An AES device of the ES3 chip generation or newer.
2. *RAIDAES (ES2 and older)*
   An AES device of the ES2 chip generation or older.
3. *Others*
   Any other (no-AES) device (e.g. CRAID).

5.2.2.1 AES Trimming *Get Frequency* Protocol

For an AES device following protocol is used:

AES Trimming *Get Frequency* Protocol (All RAIDAES devices)

Start	Length	Device	Command	Channel	Plucks	Cycles	BCC
02	04	CE	1A	19	0	A	C3

Byte	Abbreviation	Content	Example Value	Explanation
1	Start	Start Mark	02	The startbyte is dependant on the Reader used: *ProbeTestBox:* Startbyte: 01 *TBA-B300:* Startbyte: 02
2	Length	Length	04	4 Byte are following, excluding BCC
3	Device	Device Code	CE	AES device
4	Command	Command to measure frequency	1A	Measure Frequency
5	Channel	Channel ID	19	Channel IDs are: *ES3 and newer:* RF1: 19 RF2: 1A RF3: 1B *ES2 and older:*

				RF1: 11 RF2: 12 RF3: 13
6	Plucks	Number of plucks during measurement	0	No plucks during measurement
6	Cycles	Number of measurement cycles	A	Ten measurement cycles
7	BCC	Block Check Character	C3	

5.2.2.2 AES Trimming *Get Frequency* Response Protocol

AES Trimming *Get Frequency* Response Protocol (All RAIDAES devices)

Start	Length	Device	Command	Channel	Freq LSB	Freq MSB	BCC
01	05	CE	1A	19	70	06	BE

Byte	Abbreviation	Content	Example Value	Explanation
1	Start	Start Mark	01	Always 01
2	Length	Length	05	5 Byte are following, excluding BCC
3	Device	Device Code	CE	AES device
4	Command	Command to measure frequency	1A	See following table
5	Channel	Channel ID	19	Channel IDs are: *ES3 and newer:* RF1: 19 RF2: 1A RF3: 1B *ES2 and older:* RF1: 11 RF2: 12 RF3: 13
6	Freq LSB	Least significant Byte of measured Frequency	70	Measured value: 0670h Or 1648d
7	Freq MSB	Most significant Byte of measured Frequency	06	Frequency= 10^7 / (measured value * 45.2112) = 134.21 kHz
8	BCC	Block Check Character	C3	

5.2.2.3 AES Trimming *Direct Trimming* Protocol

AES Trimming *Direct Trimming* Protocol (All RAIDAES devices)

Start	Length	Device	CMD	Channel	Trim Byte	BCC
02	04	CE	0D	01	3F	F9

Byte	Abbreviation	Content	Example Value	Explanation
1	Start	Start Mark	02	The startbyte is dependant on the Reader used: *ProbeTestBox:* Startbyte: 01 *TBA-B300:* Startbyte: 02
2	Length	Length	04	4 Byte are following, excluding BCC
3	Device	Device Code	CE	AES device
4	CMD	Command to program Trim Byte	0D	Measure Frequency
5	Channel	Channel ID	01	Channel IDs are: RF1: 01 RF2: 02 RF3: 03
6	Trim Byte	Trimming value which will be programmed to the Capacitive Trimming Array	3F	Value between 00h and 7Fh which determines the capacitance of the resonant capacitor
7	BCC	Block Check Character	C3	

5.2.2.4 AES Trimming *Direct Trimming* Response Protocol

AES Trimming *Direct Trimming* Response Protocol (All RAIDAES devices)

Start	Length	Device	CMD	Channel	BCC
01	03	CE	0D	01	C1

Byte	Abbreviation	Content	Example Value	Explanation
1	Start	Start Mark	01	Always 01h
2	Length	Length	03	3 Byte are following, excluding BCC
3	Device	Device Code	CE	AES device
4	CMD	Command to program Trim Byte	0D	Measure Frequency
5	Channel	Channel ID	01	Channel IDs (see 5.2.2.3)
7	BCC	Block Check Character	C3	

5.2.2.5 Default Trimming *Get Frequency* Protocol

Default Trimming *Get Frequency* Protocol (e.g. CRAID)

Start	Length	Device	Channel	CMD	Plucks	Cycles	BCC
02	05	7E	18	5AA1	0	A	92

Byte	Abbreviation	Content	Example Value	Explanation
1	Start	Start Mark	02	The startbyte is dependant on the Reader used: *ProbeTestBox:* Startbyte: 01 *TBA-B300:* Startbyte: 02
2	Length	Length	05	5 Byte are following, excluding BCC
3	Device	Device Code	7E	Non-AES TI device
4	Channel	Channel ID	18	Channel IDs are: RF1: 18 RF2: 28 RF3: 38
5	CMD	Command with Password	5AA1	Measure Frequency
6	Plucks	Number of plucks during measurement	0	No plucks during measurement Ten measurement cycles
6	Cycles	Number of measurement cycles	A	
8	BCC	Block Check Character	C3	

5.2.2.6 Default Trimming *Get Frequency* Response Protocol

Default Trimming *Get Frequency* Response Protocol (e.g. CRAID)

Start	Length	Device	Channel	Freq LSB	Freq MSB	BCC
01	04	7E	18	70	06	14

Byte	Abbreviation	Content	Example Value	Explanation
1	Start	Start Mark	01	Always 01h
2	Length	Length	04	5 Byte are following, w/o BCC
3	Device	Device Code	7E	Non-AES TI device
4	Channel	Channel ID	18	Channel IDs are: RF1: 18 RF2: 28 RF3: 38
6	Freq LSB	Least significant Byte of measured Frequency	70	Measured value: 0670h Or 1648d
7	Freq MSB	Most significant Byte of measured Frequency	06	Frequency= 10^7 / (measured value * 45.2112) = 134.21 kHz
8	BCC	Block Check Character	14	

5.2.2.7 Default Trimming *Direct Trimming* Protocol

Default Trimming *Direct Trimming* Protocol (Non-AES devices)

Start	Length	Device	Channel	Password	Trim Byte	BCC
02	04	7E	14	5A	41	75

Byte	Abbreviation	Content	Example Value	Explanation
1	Start	Start Mark	02	The startbyte is dependant on the Reader used: *ProbeTestBox:* Startbyte: 01 *TBA-B300:* Startbyte: 02
2	Length	Length	04	4 Byte are following, excluding BCC
3	Device	Device Code	7E	Non- AES TI device
4	Channel	Channel ID	14	Program TrimByte on Channel: RF1: 14 RF2: 24 RF3: 34
5	Password	Test Interface Access Password	5A	Always 5Ah
6	Trim Byte	Trimming value which will be programmed to the Capacitive Trimming Array	41	Value between 00h and 7Fh which determines the capacitance of the resonant capacitor
7	BCC	Block Check Character	75	

5.2.2.8 Default Trimming *Direct Trimming* Response Protocol

Default Trimming *Direct Trimming* Response Protocol (All RAIDAES devices)

Start	Length	Device	Channel	BCC
01	02	7E	14	68

Byte	Abbreviation	Content	Example Value	Explanation
1	Start	Start Mark	01	Always 01h
2	Length	Length	02	2 Byte are following, excluding BCC
3	Device	Device Code	7E	Non-AES TI device
5	Channel	Channel ID	14	Channel IDs (see 5.2.2.7)
7	BCC	Block Check Character	68	

5.3 Passive Entry, Passive Start with a RAID / CRAID

For a unidirectional PEPS communication, which means the Base Station will send a LF Wake Pattern, following requirements apply:

Requirements (unidirectional PEPS):
- ADR2 demo reader **OR** TBA-B300
- RAID / CRAID device with LF- Antenna

For a complete (bidirectional) PEPS communication, which means the Base Station will send a LF Wake Pattern and can receive the UHF response of the woken key fob, following requirements apply:

Requirements (complete PEPS):
- TBA-B300 with connected UHF- Module
- RAID / CRAID device with LF- Antenna and UHF- Module

To perform a PEPS command some preparation is required if the RAID/CRAID EEPROM is not yet configured:
1. Connect the CRAID and the Base Station via the Test Interface
2. Activate the *PEPS* tab
3. Check the *Configure CRAID EEPROM* checkbox
4. Choose a configuration or just load the default values (by clicking on *Get AFE Defaults*)
5. Transmit settings by clicking on *Set AFE Configuration*. On success, the background of the button will become green. If preferred, the *Configure CRAID EEPROM* checkbox may be unchecked
6. Disconnect the device from Test Interface

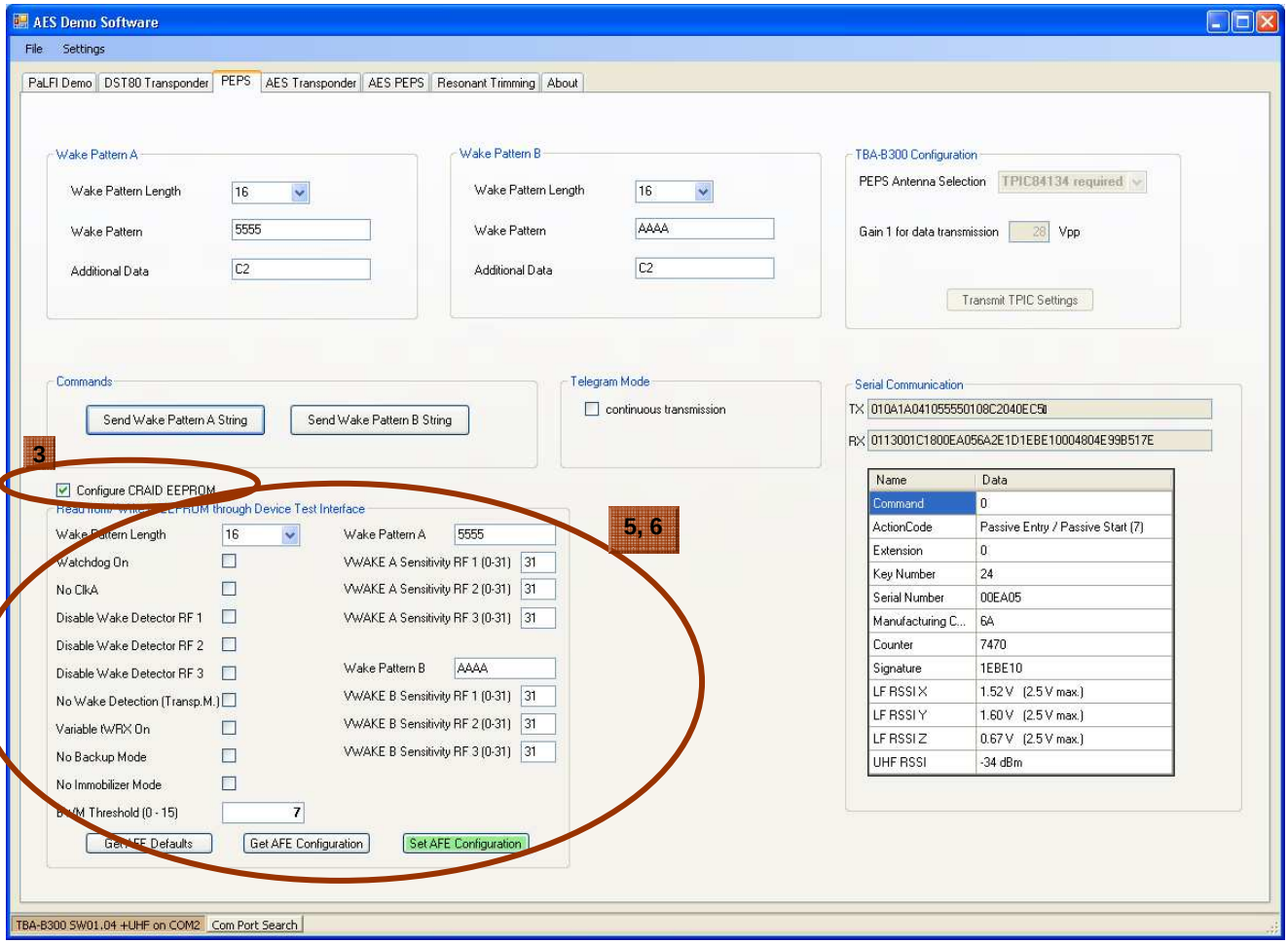
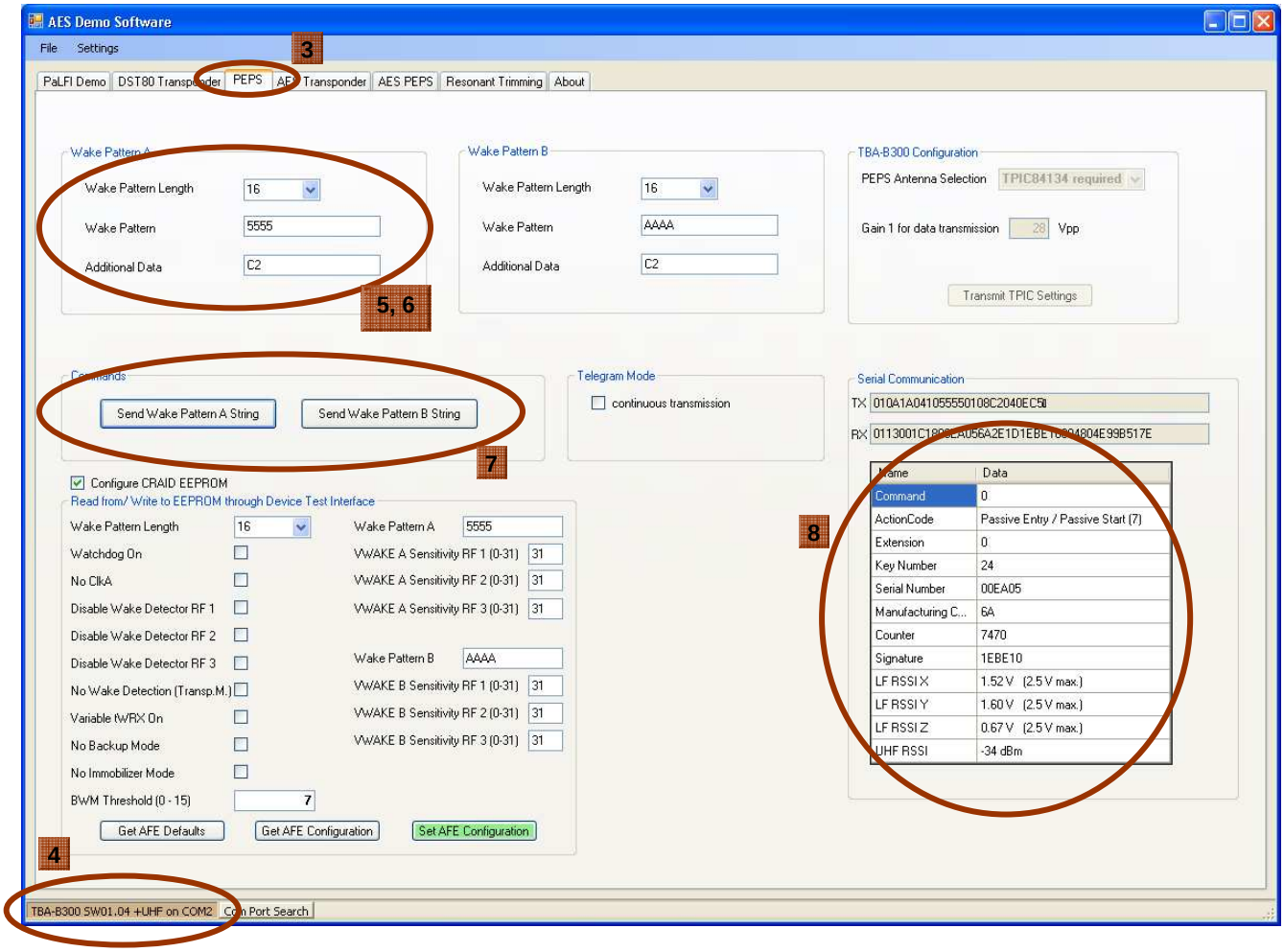


Figure 10: Configure CRAID EEPROM

With the configured EEPROM of the RAID / CRAID device it is now possible to execute the PEPS command.

1. Apply an adequate voltage source to the RAID / CRAID (e.g. a 3V coin cell)
2. Place the RAID / CRAID demo board somewhere in range of the stick antenna LF field, not too close to the UHF Module of the Base Station to prevent oversaturation.
3. Select the PEPS tab in the software.
4. Ensure the correct reader is selected – preferably with UHF Module to receive a response
5. Adjust *Wake Pattern Length* and *Wake Pattern* according to the configuration on the CRAID EEPROM
6. Eventually add an Additional Data string. Sending “C2” will cause the RAID / CRAID to measure the LF RSSI.
7. To execute the action click on *Send Wake Pattern String*
8. If a UHF response is obtained the content will be displayed



If problems with the LF RSSI measurement occur though “C2” is sent as *Additional Data*, consider configuration of *RSSI Burst Time* in the *PEPS Settings* tab page (*Settings* menu). During this power burst at the end of the LF transmission the RSSI value is measured.

5.4 Immobilizer Read Page (DST80)

To read a page of a DST80 transponder or a device using one, like the RAID / CRAID devices, follow those instructions:

1. If not done yet, power up the board, connect it to the PC, start the software and place the Transponder / LF- Antenna in the LF field of the readers Immobilizer Loop Antenna.
2. Activate the *DST80 Transponder* tab
3. Choose the page which should be read
4. Click on *Read Page*
5. After a successful read *CRC correct* should be displayed along with green highlighting
6. The data read out from the page will be displayed in the *Received Bytes* section

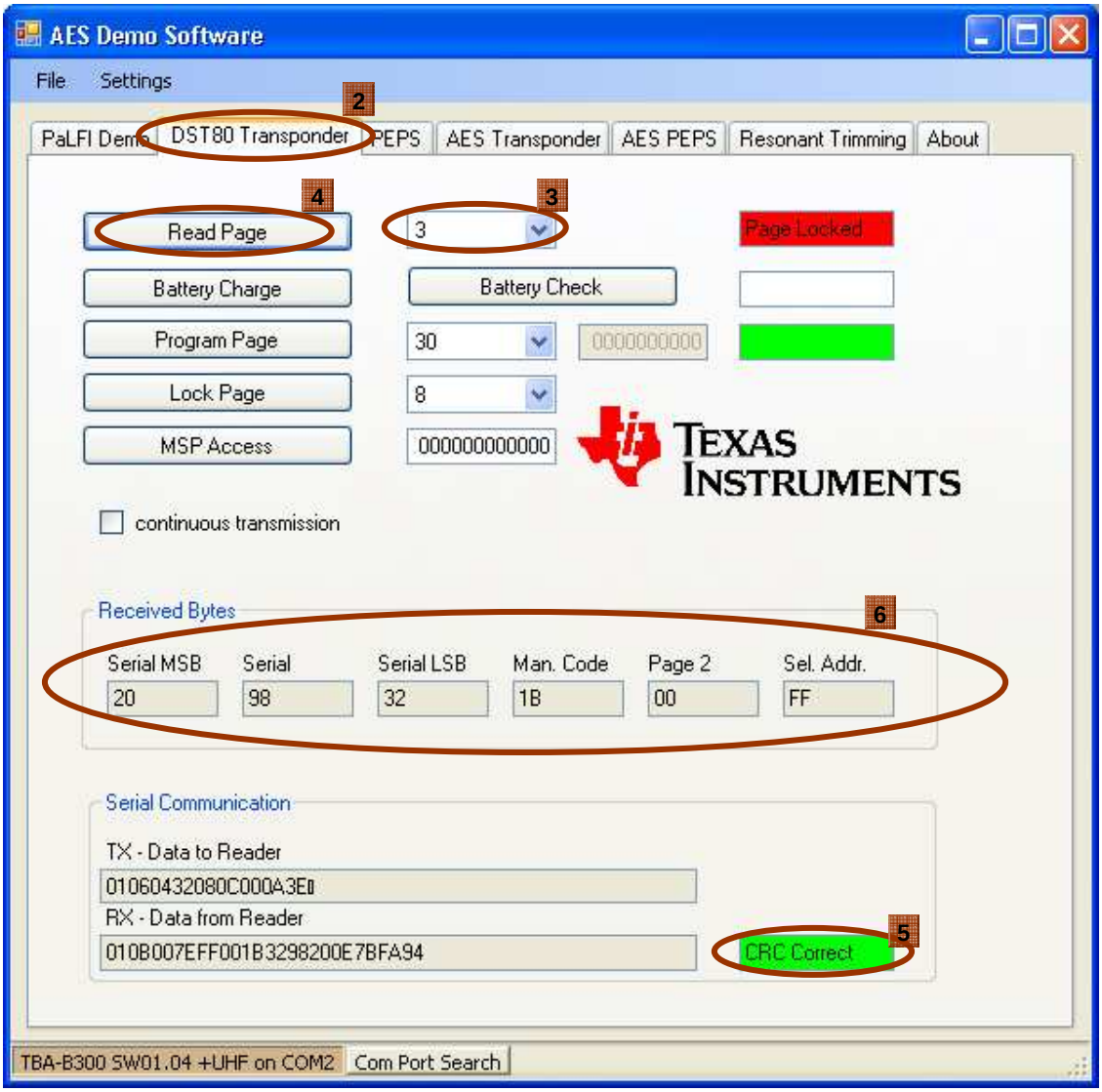


Figure 11: Transponder: Read Page (DST80)

5.4.1 Problems with DST80 Transponder Immobilizer function

When experiencing problems with the *DST80 Transponder* Immobilizer function ensure *Coding* is set to *PWM (Pulse Width Modulation).* This configuration is found in the *DST80 Settings* tab page.

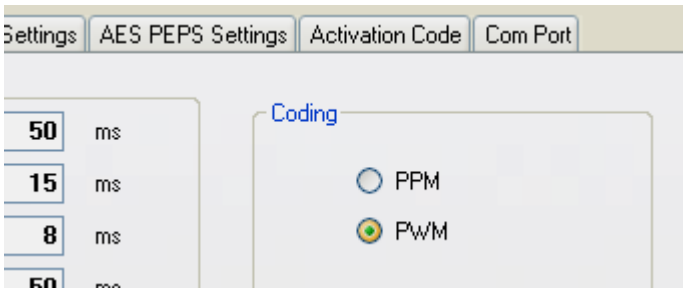


Figure 12: Coding Configuration (DST80)

In doubt, use default timing settings.

5.4.2 Example: Read Page 3 command (DST80)

By clicking on *Read Page 3* the software sends via *Serial Communication* following telegram:
” 0106043208 0C 000AAC”. This data is assembled as follows:

Serial Communication Protocol

Start	Length	Cmd	PB1	No. TX bits	TX bits	PB2	No. RX bytes	BCC
01	06	04	32	08	0C	00	0A	AC

Byte	Abbreviation	Content	Example Value	Explanation
1	Start	Start Mark	01	
2	Length	Length	06	6 Byte transmission are following, excluding BCC
3	Cmd	Command	04	cf. section **6.7**
4	PB1	Data – Power Burst 1	32	50 ms Power Burst
5	No. TX bits	Data – Number of Transmit Bits	08	8 Bit to transmit to transponder
6	TX bits	Data – Transmit Bits	0C	see following table
7	PB2	Data – Power Burst 2	00	No second Power Burst
8	No. RX bytes	Data – Number of Receive Bytes	0A	10 Byte response expected from transponder
9	BCC	Block Check Character	AC	

LF Transmit Bits	hex	0C		
- Page - Command	hex	0C	0000 1100	
		Page	0000 11	Page 3
		Command	00	Read

5.4.3 Example: Read Page 8 response (DST80)

As response following telegram is received: “010B007E00123456789020EE2407”

Serial Communication Protocol

Start	Length	Cmd	TX bits	BCC
01	0B	007E	00123456789020EE24	07

Byte	Abbreviation	Content	Example Value	Explanation
1	Start	Start Mark	01	
2	Length	Length	0B	11 Byte are following, excluding BCC
3,4	Cmd	Command	007E	Transponder response
5 to 13	TX bits	LF transponder response	00123456789020EE24	See following table
14	BCC	Block Check Character	07	

LF Uplink Data	hex	00123456789020EE24		
- Page 2	hex	00		
- Page 8 content	hex	1234567890 *(Byte 0, Byte 1, Byte 2, Byte 3)*		
- Read Address - Read Address Extension	hex	20	0010 0000	
		Page	0010 00	Page 8
		Page locked	0	General access
		Programming	0	No Programming
- CRC check sum	hex	EE24		

5.5 Immobilizer Program Page (DST80)

To program a page of a DST80 transponder or a RAID / CRAID device, follow these instructions:

1. If not done yet, power up the board, connect it to the PC, start the software and place the Transponder / LF- Antenna in the LF field of the readers Immobilizer Loop Antenna.
2. Activate the *DST80 Transponder* tab
3. *Hint:* Read the page which shall be programmed first. This will help to find out if the page is eventually locked for write access. The lock-status will be displayed after a successful *Read page* command
4. Choose the page which shall be programmed
5. Enter the data which shall be programmed
   Programming configuration pages may differ from programming pages containing user defined data. Examples: Page 3 can't be programmed; Page 2 has partial write access; Page 30 has a configuration mask
6. Click on *Program Page*
7. The transponder answers with a *Read Page* command of the programmed page.

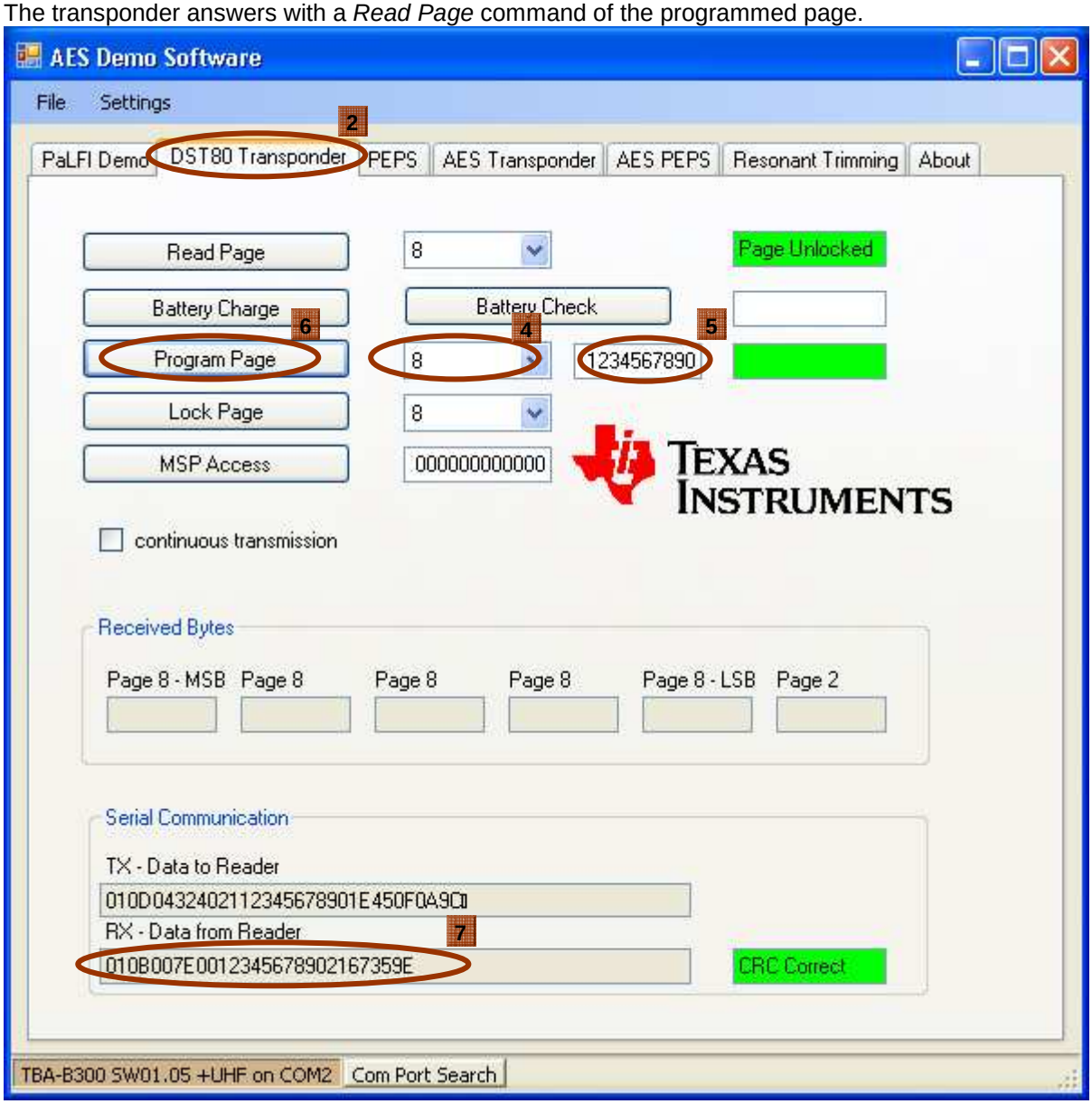


Figure 13: Example: Program Page 8 (DST80)

5.5.1 Example: Program Page 8 command (DST80)

By clicking on *Program Page (*Page *8* selected) the software sends via *Serial Communication* following telegram:
" 010D04324021123456789 01E45 0F0A 9C". This data is assembled as follows:

Serial Communication Protocol

Start	Length	Cmd	PB1	No. TX bits	TX bits	PB2	No. RX bytes	BCC
01	0D	04	32	40	21 1234567890 1E45	0F	0A	9C

Byte	Abbreviation	Content	Example Value	Explanation
1	Start	Start Mark	01	
2	Length	Length	0D	6 Byte transmission are following, excluding BCC
3	Cmd	Command	04	cf. Command Byte Definition **6.7**
4	PB1	Data – Power Burst 1	32	50 ms Power Burst
5	No. TX bits	Data – Number of Transmit Bits	40	8 Byte to transmit to transponder
6 - 13	TX bits	Data – Transmit Bits	21 12345 67890 1E45	see following table
14	PB2	Data – Power Burst 2	0F	No second Power Burst
15	No. RX bytes	Data – Number of Receive Bytes	0A	10 Byte response expected from transponder
16	BCC	Block Check Character	9C	

LF Transmit Bits	hex	2112345678901E45		
- Page - Command	hex	21	0010 0001	
		Page	0010 00	Page 8
		Command	01	Program
- Page Content	hex	1234567890		
- CRC check sum	hex	1E45		

Response will be similar to a *Read Page* response (c.f. **5.4.3**)

5.6 Immobilizer Lock Page (DST80)

To lock a page of a DST80 transponder or a RAID / CRAID device, follow these instructions:

1. If not done yet, power up the board, connect it to the PC, start the software and place the Transponder / LF- Antenna in the LF field of the readers Immobilizer Loop Antenna.
2. Activate the *DST80 Transponder* tab
3. Choose the page which shall be locked
4. Click on *Lock Page*
5. The transponder answers with a *Read Page* answer of the locked page viewable in the *RX – Data from Reader* textbox (5a). Additionally the new *Page Lock Status* which is *Paged Locked* after a successful lock command is executed will be displayed in the top right corner (5b).

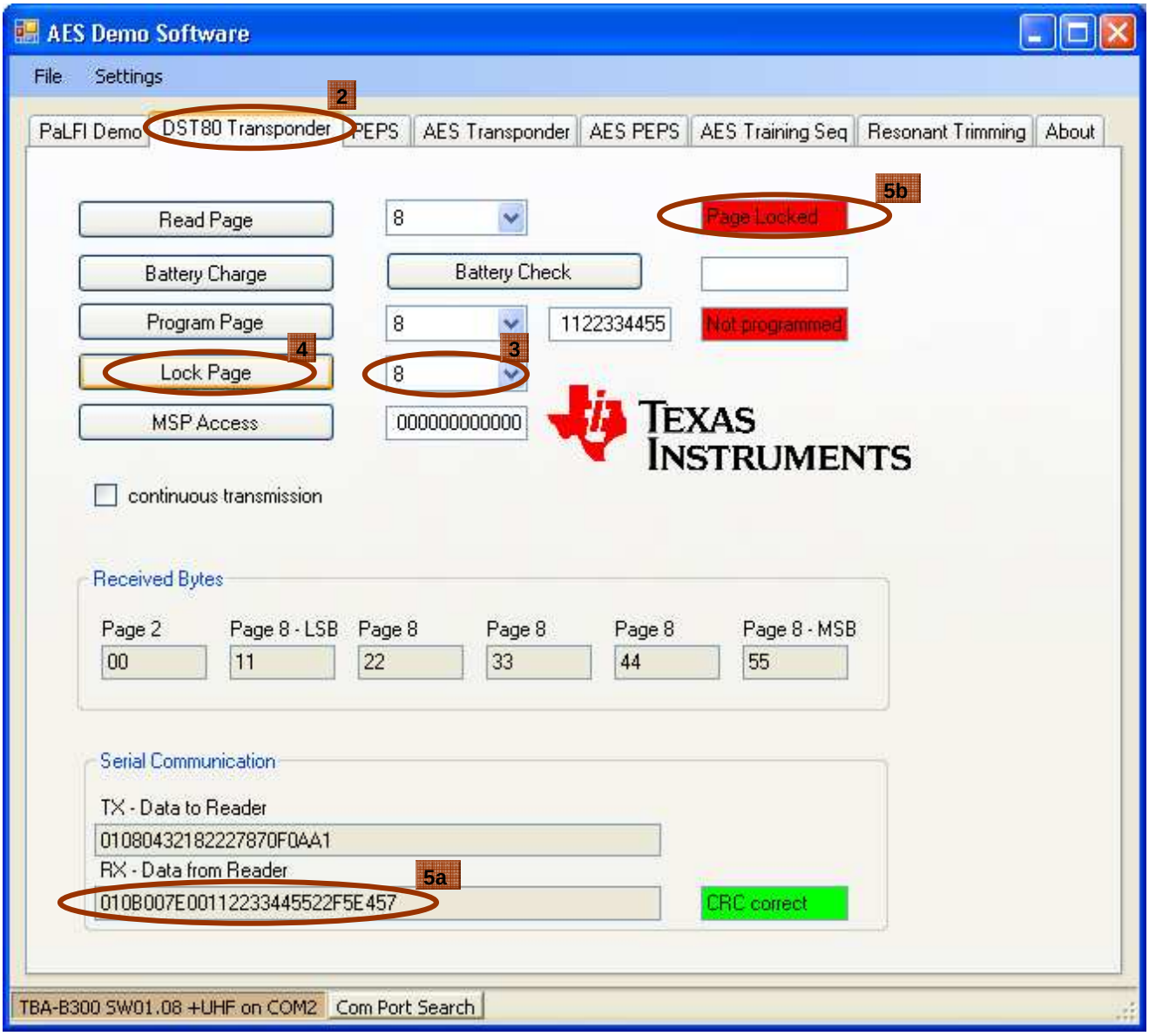


Figure 14: Example: Lock Page 8 (DST80)

5.6.1 Example: Lock Page 8 command (DST80)

By clicking on *Lock Page* the software sends via *Serial Communication* following telegram:
" 0108043218222787 0F0A A1". This data is assembled as follows:

Serial Communication Protocol

Start	Length	Cmd	PB1	No. TX bits	TX bits	PB2	No. RX bytes	BCC
01	08	04	32	18	222787	0F	0A	A1

Byte	Abbreviation	Content	Example Value	Explanation
1	Start	Start Mark	01	
2	Length	Length	08	6 Byte transmission are following, excluding BCC
3	Cmd	Command	04	cf. Command Byte Definition **6.7**
4	PB1	Data – Power Burst 1	32	50 ms Power Burst
5	No. TX bits	Data – Number of Transmit Bits	18	3 Byte to transmit to transponder
6, 7, 8	TX bits	Data – Transmit Bits	222787	see following table
9	PB2	Data – Power Burst 2	0F	No second Power Burst
10	No. RX bytes	Data – Number of Receive Bytes	0A	10 Byte response expected from transponder
11	BCC	Block Check Character	A1	

LF Transmit Bits	hex	222787		
- Page - Command	hex	22	0010 0010	
		Page	0010 00	Page 8
		Command	10	Lock
- CRC check sum	hex	2787		

Response will be similar to a *Read Page* response (c.f. **5.4.3**)

5.7 Using the TPIC 84134 Antenna Extension Board

Requirements:

- TBA-B300 Base Station
- TPIC 84134 Antenna Extension Board

To use the antenna extension board follow this instructions:

Ensure the TPIC 84134 is detected correctly to the reader and that both are detected by the AES Demo Software. This is indicated by the "+TPIC" addition after the reader name in the status bar.

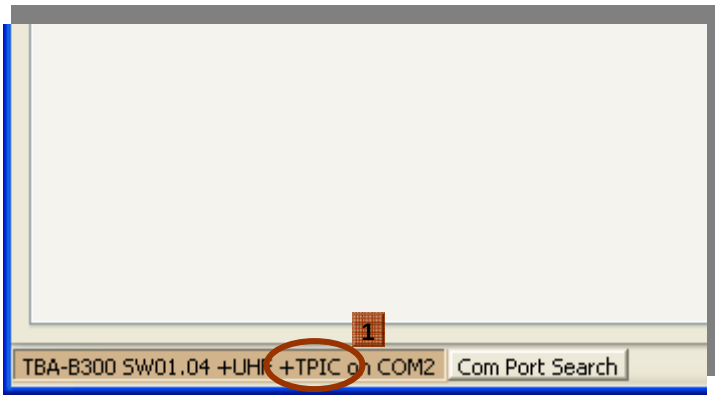


Figure 15: TPIC connection

1. Activate the *PEPS* or *AES PEPS* tab dependant on which device you use for PEPS communication (for details of PEPS communication refer to **5.2** for DST80 devices or to Error! Reference source not found. for AES devices)
2. Choose the output on which the antenna is connected which should be used.
   J1, J2 and J3 are the three standard TBA-B300 antenna outputs.
   Usually connected to J1 is the Immobilizer Antenna, to J2 the Stick Antenna while J3 remains unused.
   The **TPIC outputs** in the dropdown box are numbered accordingly to the output numbering on the board. By picking a single TPIC Output *Half Bridge Mode* will be activated, which is normal operation. If two TPIC outputs are selected *Full Bridge Mode* is activated. This means the outputs are sending the LF- transmission with a 180 degree phase shift on the second output. Wired correctly to an antenna this means twice the peak-to-peak voltage!
   By picking **Default Antenna** the Base Station is configured for behaviour as though the TPIC would not have been connected.
3. Choose the desired peak-to-peak voltage (Vpp) on a single output
4. Transmit the settings by clicking *Transmit TPIC Settings*

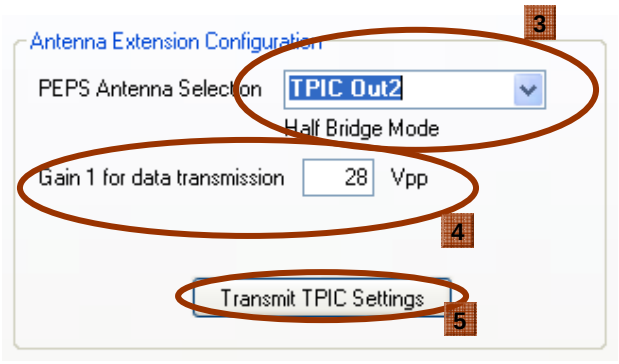


Figure 16: Antenna Extension Configuration

5. Execute a PEPS command as usual

6 Serial protocol description

6.1 RS232 / USB settings

The RI-ACC-ADR2-00 reader is designed for engineering purposes.
The data communication is performed via USB port but shows up as serial COM port on the PC side. The transmission parameters are 8 data bits, 1 stop bit, no parity and a speed of 9600 baud.
No hardware or software handshake is used. The protocol data consists only of the following ASCII characters ‘0’,’1’, …,‘9’, ‘A’,…,’F’.

The data communication between the PC and the reader is performed within a frame structure.

6.2 Setup protocol overview

To setup or request parameter, the following *Setup* protocol has to be sent from the PC to the reader.

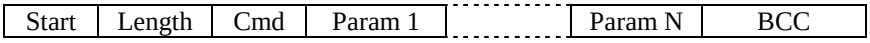
Start	Length	Cmd	Param1	.....	Param N	BCC

Block	Abbreviation	Content
1	Start	Start Mark
2	Length	Length (following number of bytes without BCC)
3	Cmd	Command
4 .. N	Para	Parameter
N+1	BCC	Block Check Character

Command ASCII	Description	N	Parameter	Parameter format
‘01’	Read PWM timings	8	ToffH, TonH, ToffL, TonL	2 byte for each in us
‘03’	Write PWM timings	8	ToffH, TonH, ToffL, TonL	2 byte for each in us
‘05’	Read Version Information	4	SW_major, SW_minor, HW_major, HW_minor	1 byte for each
‘07’	Set Mode Control bytes	2	MCW1, MCW2	1 byte for each
‘11’	Read PPM timings	8	Toff, TonH, TonSC, TonL	2 byte for each in us
‘13’	Write PPM timings	8	Toff, TonH, TonSC, TonL	2 byte for each in us
‘17’	Write BLC timings part I	12	T_{SOF_ON}, T_{SOF_OFF}, T_{LOW_ON}, T_{LOW_OFF}, T_{HIGH_ON}, T_{HIGH_OFF}	2 byte for each in us
‘1B’	Write BLC timings part II	10	T_{EOF_ON}, T_{EOF_OFF}, T_{WAKE_ON}, T_{WAKE_OFF}, PEPS_Pattern, Immo_Pattern	2 byte for each in us
‘19’	Read BLC timings part I	12	T_{SOF_ON}, T_{SOF_OFF}, T_{LOW_ON}, T_{LOW_OFF}, T_{HIGH_ON}, T_{HIGH_OFF}	2 byte for each in us
‘1D’	Read BLC timings part II	10	T_{EOF_ON}, T_{EOF_OFF}, T_{WAKE_ON}, T_{WAKE_OFF}, PEPS_Pattern, Immo_Pattern	2 byte for each in us
‘31’	Read Power Burst timings	14	Charge, Programtime 64bit, Programtime 128bit, Encryption time, Mutual Authentication Time, MCU Access Time (Supported only by TBA-B300 for AES Pairing Demo Mode).	2 byte for each, charge: 4 byte in ms
‘33’	Write Power Burst timings	14		

6.3 Setup Protocol Responses

Setup information from the Reader to the PC is transmitted using following *Setup Response* protocol.



Block	Abbreviation	Content
1	Start	Start Mark
2	Length	Length (following number of bytes without BCC)
3	Cmd	Command
4 .. N	Param	Setup Parameter
N+1	BCC	Block Check Character

6.4 Setup Protocol Examples

6.4.1 "Get Version Information"

Request:

Block	ASCII	Hex	Content	Description
1	'01'	30,31	Start Mark	Start of Protocol Frame
2	'01'	30,31	Length	1 byte follow excluding BCC
3	'05'	30,35	Command	Read Version Information
4	'04'	30,34	Block Check Character	BCC over previous blocks excluding Start Mark

Response:

Block	ASCII	Hex	Content	Description
1	'01'	30,31	Start Mark	Start of Protocol Frame
2	'05'	30,35	Length	5 bytes follow excluding BCC
3	'00'	30,30	Command	Normal mode: 00hex
4	'02'	30,32	Data	Software Version major
5	'03'	30,33	Data	Software Version minor
6	'04'	30,34	Data	Hardware Version major
7	'02'	30,32	Data	Hardware Version minor
8	'02'	30,32	Block Check Character	BCC over previous blocks excluding Start Mark

6.4.2 "Write BLC Timing Information"

Request: 010B1B035C012C04B000001001C7

Block	ASCII	Hex	Content	Description
1	'01'	30,31	Start Mark	Start of Protocol Frame
2	'0B'	30,42	Length	11 byte follow excluding BCC
3	'1B'	30,42	Command	Write BLC timings part II
4	'03'	30,33	EOF on time 0x035C	T_{EOF_ON} = 860µs
5	'5C'	35,43		
6	'01'	30,31	EOF off time 0x012C	T_{EOF_OFF} = 300µs
7	'2C'	32,43		
8	'04'	30,34	Wake on time 0x04B0	T_{WAKE_ON} = 1200µs
9	'B0'	42,30		
10	'00'	30,30	Wake off time 0x0000	T_{WAKEF_OFF} = 0µs
11	'00'	30,30		
12	'10'	31,30	PEPS Pattern	→ S10
13	'01'	30,31	Immo Pattern	→ S01
14	'C7'	43,37	Block Check Character	BCC over previous blocks excluding Start Mark

Response: 010B1D035C012C04B000001001C1

Block	ASCII	Hex	Content	Description
1	'01'	30,31	Start Mark	Start of Protocol Frame
2	'0B'	30,42	Length	11 byte follow excluding BCC
3	'1D'	30,42	Command	Read BLC timings part II
4	'03'	30,33	EOF on time 0x035C	T_{EOF_ON} = 860µs
5	'5C'	35,43		
6	'01'	30,31	EOF off time 0x012C	T_{EOF_OFF} = 300µs
7	'2C'	32,43		
8	'04'	30,34	Wake on time 0x04B0	T_{WAKE_ON} = 1200µs
9	'B0'	42,30		
10	'00'	30,30	Wake off time 0x0000	T_{WAKEF_OFF} = 0µs
11	'00'	30,30		
12	'10'	31,30	PEPS Pattern	→ S10
13	'01'	30,31	Immo Pattern	→ S01
14	'C1'	43,37	Block Check Character	BCC over previous blocks excluding Start Mark

6.5 Block Check Character

The *BCC* is the one-block value of the Longitudinal Redundancy Check calculation (Xor'ed blocks) of the preceding blocks. The BCC is calculated over all bytes of the incoming and outgoing data excluding the start byte. The BCC is always the last byte of the outgoing or incoming data. The user can calculate the BCC over the received data and compare it with the received BCC for error detection.

The sample code below shows a calculation routine for the Block Check Character which is calculated by the use of a Longitudinal Redundancy Check (LRC). It returns the BCC as a byte value.

```
public byte LRC_calc(byte[] bytes, int length)
{
        int lrc;

        lrc = bytes[0];
        for (int i = 1; i < length; i++)
        {
                lrc = lrc ^ bytes[i];
    }
    return (byte)(lrc);
}
```

6.6 Immobilizer protocol downlink overview

To initiate an action, following *Request* protocol has to be sent from the PC to the reader.

Start	Length	Cmd	PB1	No. TX bits	TX bits	PB2	No. RX bytes	BCC

Block	Abbreviation	Content
1	Start	Start Mark
2	Length	Length
3	Cmd	Command
4	PB1	Data - Power Burst 1
5	No. TX bits	Data - Number of Transmit Bits
4 .. N	TX bits	Data - Transmit Bits
N+1	PB2	Data - Power Burst 2
N+2	No. RX bytes	Data - Number of Receive Bytes
N+3	BCC	Block Check Character

Start Mark
The *Start Mark* identifies the beginning of the Request protocol. It is represented by the ASCII characters '01'.

Length
The *Length* indicates the number of the following Command and Data bytes (Power Burst 1, Number of Transmit Bits, Transmit Bits, Power Burst 2 and Number of Receive Bytes).

Command
The *Command* defines the mode in which the controller operates.

Data – Power Burst 1
The *Data – Power Burst 1* parameter specifies the duration of the transponder charge burst in milliseconds.

Data – Number TX Bits
The *Data – Number TX Bits* parameter specifies the amount of bits to be transferred to the transponder.

Data – Transmit Bits
The *Data – Transmit Bits* contains the information to be transferred to the transponder.

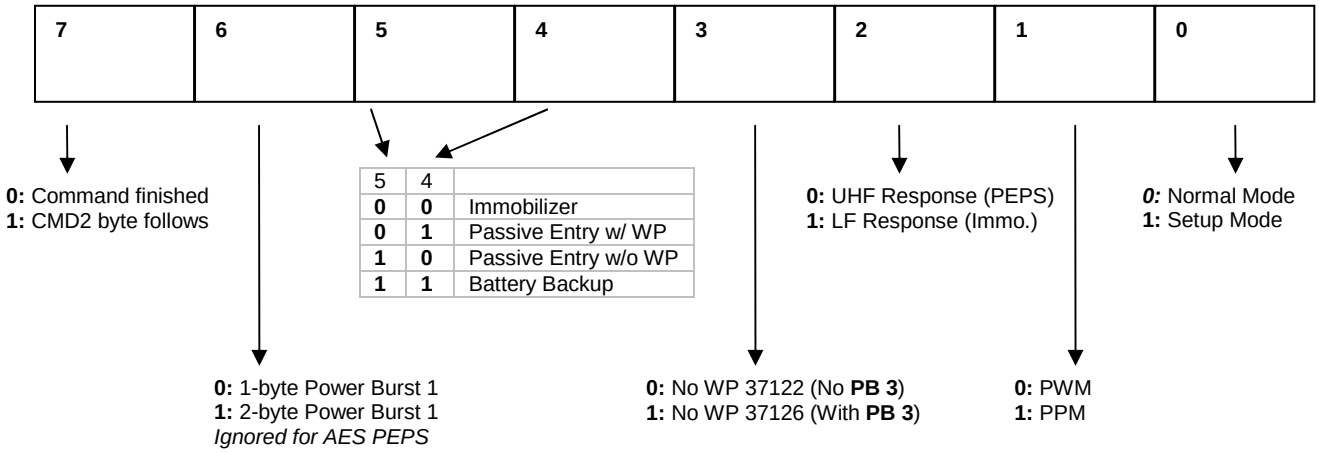
Data – Power Burst 2
The *Data – Power Burst 2* parameter specifies the duration of the transponder program or encrypt burst in milliseconds.

Data – Number RX Bytes
The *Data - Number RX Bytes* parameter specifies the expected amount of bytes responded by a transponder.

Block Check Character
See next section for detailed description of the Block Check Character

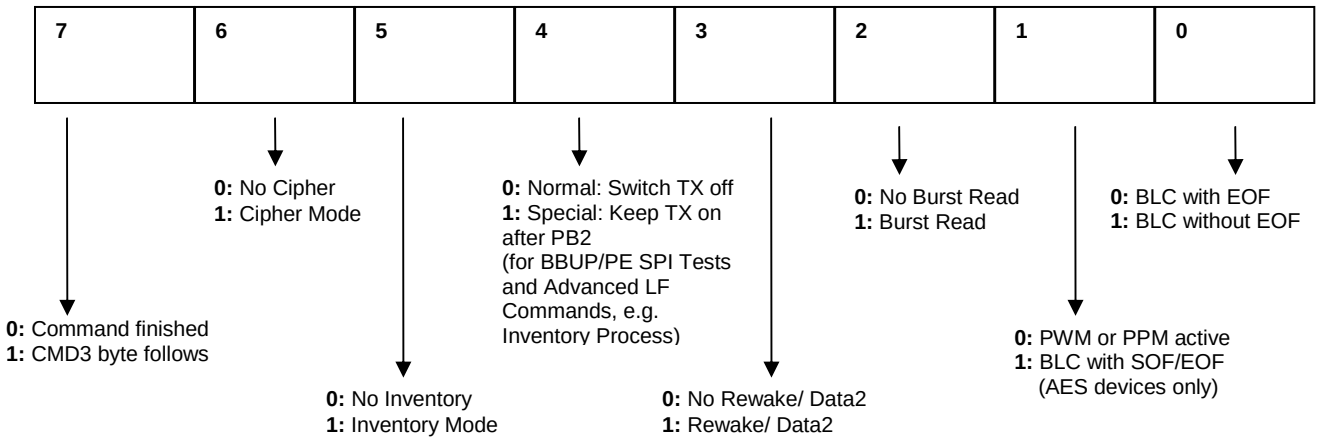
6.7 Immobilizer protocol downlink command byte definition

1st Byte CMD

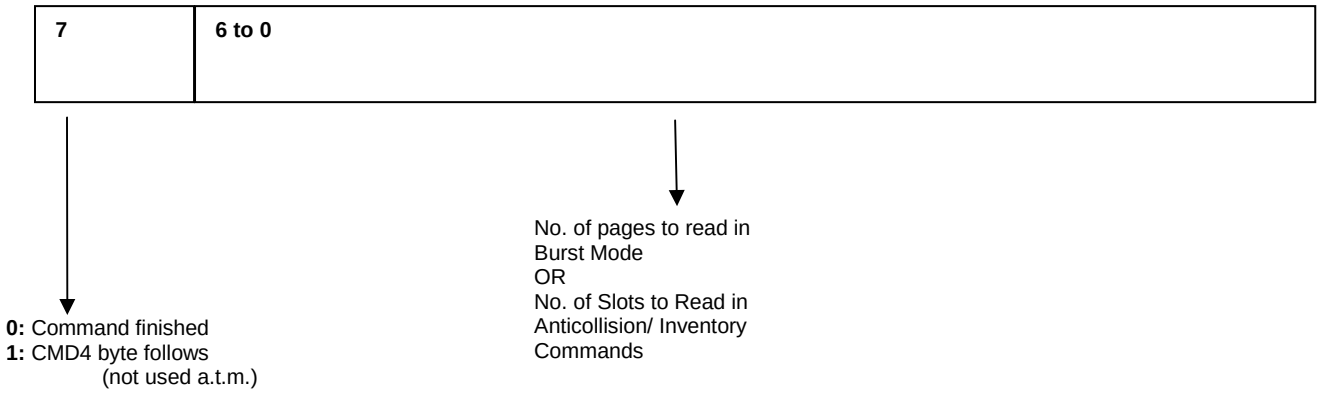


5	4	
0	0	Immobilizer
0	1	Passive Entry w/ WP
1	0	Passive Entry w/o WP
1	1	Battery Backup

2nd Byte CMD2



3rd Byte CMD3



6.8 Immobilizer protocol response overview

Data information from the Reader to the PC is transmitted using following *Response* protocol.

Start	Length	Cmd	RX bytes	BCC

Block	Abbreviation	Content
1	Start	Start Mark
2	Length	Length
3	Cmd	Command
4 .. N	RX bytes	Data - Receive Bytes
N+1	BCC	Block Check Character

Start Mark
The *Start Mark* identifies the beginning of the Response protocol. It is represented by the ASCII characters '01'.

Length
The *Length* indicates the number of the following Command and Data blocks.

Command
The *Command* defines the mode in which the controller operates.

Data – Receive Bytes
The *Data –Receive Bytes* consists of the data information transferred by a transponder beginning with the transponder Start Byte.

BCC
See section 6.5 for details.

6.9 Specific Protocols

6.9.1 CRAID PEPS Telegram

Start	Len	Cmd	Wake_Dur	Wake_Len	Wake_Pat	
	DD_Burst	TX_Data	Data	Final_Burst	RX_Bytes	BCC

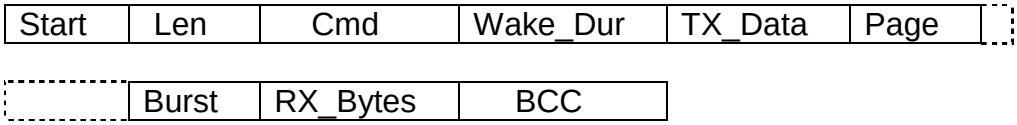
Abbreviation	Content	Example	Explanation
Start	Start	01	Start of Telegram
Len	Length	0A	Following Bytes in Telegram (in Byte excluding BCC)
Cmd	Command	1A	q.v. Command Bytes
Wake_Dur	Wake Burst Duration	04	4ms Wake Burst
Wake_Len	Wake Pattern Length	10	Bit Count of WP. (Hex! Here 16 Bits)
Wake_Pat	Wake Pattern	5555	
DD_Burst	Data Delay Burst	01	1ms Burst between Wake Pattern and Data
TX_Data	Amount of Data (TX)	08	8 Bits of Data following
Data	Transmitted Data	C2	Data to transmit If C2 is transmitted as Data, the CRAID will measure the 3D-LF RSSI and include it in its response
Final_Burst	Add Power Burst	04	4ms Burst after Data to measure the LF RSSI
RX_Bytes	Number Rx Bytes	00	No LF response expected
BCC	Block Check Char	C1	BCC over Message

6.9.2 CRAID PEPS Response / RKE Telegram

Start	Len	PID	Status	Key #	Serial #	ManuC	
	Counter	Signature		LF RSSI	UHF RSSI	BCC	

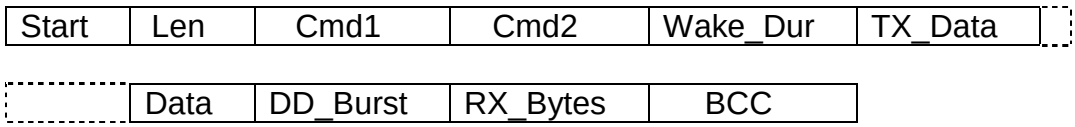
Abbreviation	Content	Example	Explanation
Start	Start	01	Start of Telegram
Len	Length	10	Following Bytes in Telegram (in Byte excluding BCC)
PID	Protocol Identifier	00	RKE Protocol ID: 00h
Status	Status Byte	11	Bit7: Extension Bit Bit6- Bit2: Action Code Bit1- Bit0: Reader Command
Key #	Key Number	11	Key Number 11h <=> Key Number 17d
Serial #	Serial Number	69E517	
ManuC	Manufacturer Code	94	
Counter	16 Bit Counter	1162	
Signature	24 Bit Signature	9D482B	
LF RSSI	3D- LF RSSI Data	6F4937	Byte2: X-Axis LF- RSSI in range from 00h to FFh Byte1: Y-Axis LF- RSSI in range from 00h to FFh Byte0: Z-Axis LF- RSSI in range from 00h to FFh
UHF RSSI	UHF RSSI Data	69	RSSI value of UHF transmission
BCC	Block Check Char	1A	BCC over Message

6.9.3 DST80 Immobilizer



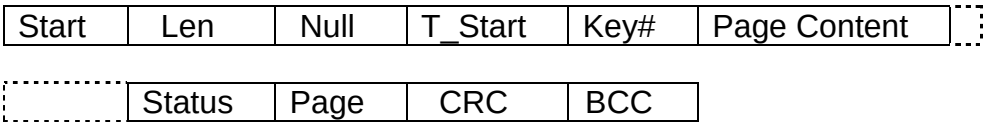
Abbreviation	Content	Example	Explanation
Start	Start	01	Start of Telegram
Len	Length	06	Following Bytes in Telegram (in Byte excluding BCC)
Cmd	Command	04	q.v. Command Bytes
Wake_Dur	Wake Burst Duration	A0	160ms Wake Burst
TX_Data	Amount of Data (TX)	08	8 Bits of Data following
Page	Page Select	0C	Page index to read from Transponder Page 1: 04 Page 2: 08 Page 3: 0C etc.
Burst	Data Delay Burst	00	No Burst before transmitting data
RX_Bytes	Number Rx Bytes	0A	Amount of Bytes demanded as response
BCC	Block Check Char	AC	BCC over Message

6.9.4 AES Immobilizer



Abbreviation	Content	Example	Explanation
Start	Start	01	Start of Telegram
Len	Length	08	Following Bytes in Telegram (in Byte excluding BCC)
Cmd1	Command Byte 1	84	q.v. Command Bytes
Cmd2	Command Byte 2	02	BLC Mode
Wake_Dur	Wake Burst Duration	0F	15ms Wake Burst
TX_Data	Amount of Data (TX)	10	Transmit following 2Bytes to Transponder
Data	Transmitted Data	F003	“Read Page 3”
DD_Burst	Data Delay Burst	00	No second power burst
RX_Bytes	Number Rx Bytes	0A	Amount of Bytes demanded as response
BCC	Block Check Char	68	BCC over Message

6.9.5 AES Immobilizer Response



Abbreviation	Content	Example	Explanation
Start	Start	01	Start of serial Telegram
Len	Length	0B	Following Bytes in Telegram (in Byte excluding BCC)
Null	Null Byte	00	
T_Start	Transponder Start byte	7E	Start of transponder telegram
Key#	Key Number	01	
Page Content	Page Content Data	1518B2E1	Page Content, starting with the LSB
Status	Status bits (Read Address)	F3	Bit6-Bit4: Bank; Bit3: Mutual Access; Bit2: LF Access; Bit1: Programming locked; Bit0: Command executed;
Page	Page Number (R.Ad. Extension)	00	Bit6-Bit0: Page Number;
CRC	BCC	D0EA	Transponder telegram BCC
BCC	Block Check Char	E3	BCC of serial Telegram

6.9.6 AES PEPS Telegram

Start	Len	Cmd1	Cmd2	Wake_Dur	Wake_Len	Wake_Pat	
	DD_Burst	TX_Data		Data	Final_Burst	RX_Bytes	BCC

Abbreviation	Content	Example	Explanation
Start	Start	01	Start of Telegram
Len	Length	09	Following Bytes in Telegram (in Byte excluding BCC)
Cmd1	Command Byte 1	90	q.v. Command Bytes
Cmd2	Command Byte 2	42	q.v. Command Bytes
Wake_Dur	Wake Burst Duration	00	No Wake Burst (additional to WakeB. configured in BLC Timings)
Wake_Len	Wake Pattern Length	04	Bit Count of Wake Pattern
Wake_Pat	Wake Pattern	08	“1” (nibbles read backwards)
DD_Burst	Data Delay Burst	00	No Burst after Wake Pattern
TX_Data	Amount of Data (TX)	00	No Data transmitted
Data	Actual Data		No Data transmitted
Final_Burst	Add Power Burst	04	4ms Burst at end of transmission
RX_Bytes	Number Rx Bytes	0A	Amount of Bytes demanded as response
BCC	Block Check Char	D9	BCC over Message

6.9.7 AES Burst Read / Anti-Collision AES Encryption

Start	Len	Cmd1	Cmd2	Cmd3	Charge	TX_Data	
	Address + Extension	Data			Final_Burst	RX_Bytes	BCC

Abbreviation	Content	Example	Explanation
Start	Start	01	Start of Telegram
Len	Length	11	Following Bytes in Telegram (in Byte excluding BCC)
Cmd1	Command Byte 1	84	q.v. Command Bytes
Cmd2	Command Byte 2	86	BLC Burst Mode
Cmd3	Command Byte 3	04	Number of Pages to Read / Highest Key Slot Number
Charge	Charge Time [ms]	96	150 ms Charge Time
TX_Data	Amount of Data (TX)	50	Amount of following bits to transmit to transponder (80 Bit)
Address + Extension	AES Write Address	FB32	AES Transponder Command
Data	Burst Start Page / Challenge + Reader Signature	0E0D0C0B 302013FD	Challenge and Reader Signature for AES Encryption (Anti-Collision)
Final_Burst	Add Power Burst	04	4ms Burst at end of transmission
RX_Bytes	Number Rx Bytes	0A	Number of Bytes demanded as response
BCC	Block Check Char	E0	BCC over Message

6.9.8 Trimming: Get Frequency (“Others”)

Start	Len	Device	Channel	Password	Plucks & LQ	
	Cycles	BCC				

Abbreviation	Content	Example	Explanation
Start	Probe Test Start	02	Start of Telegram
Len	Length	05	Following Bytes in Telegram (in Byte excluding BCC)
Device	Device ID	7E	
Channel	Channel ID	18	0x18: Measure RF1 0x28: Measure RF2 0x38: Measure RF3
Password	Password	5A	Password to unlock Probe Test Mode
Plucks & LQ	Number of Plucks and L & Q Info	A1	Bit7-Bit4: Num Plucks\ Bit3-Bit0: L & Q Info
Cycles	Number of Cycles	0A	Number of measure clock cycles per pluck
BCC	Block Check Char	92	BCC over Message

6.9.9 Trimming: Trim Byte (“Others”)

Start	Len	Device	Channel	Password	Trim Byte	BCC

Abbreviation	Content	Example	Explanation
Start	Probe Test Start	02	Start of Telegram
Len	Length	04	Following Bytes in Telegram (in Byte excluding BCC)
Device	Device ID	7E	
Channel	Channel ID	14	0x14: Trim Byte RF1 0x24: Trim Byte RF2 0x34: Trim Byte RF3
Password	Password	5A	Password to unlock Probe Test Mode
Trim Byte	Trim Byte	3C	
BCC	Block Check Char	08	BCC over Message

6.9.10 Trimming: Get Frequency (RAIDAES)

Start	Len	Device	Mode	Channel	Plucks & Cycles	BCC

Abbreviation	Content	Example	Explanation
Start	Probe Test Start	02	Start of Telegram
Len	Length	04	Following Bytes in Telegram (in Byte excluding BCC)
Device	Device ID	CE	
Mode	Mode Byte	1A	Mode: Measure Frequency
Channel	Channel ID	11	**ES3 or newer:** 0x19: Measure RF1 0x1A: Measure RF2 0x1B: Measure RF3 **ES2 or older:** 0x11: Measure RF1 0x12: Measure RF2 0x13: Measure RF3
Plucks & Cycles	Number of Plucks and Cycles	0A	Bit7-Bit4: Plucks Bit3-Bit0: Cycles
BCC	Block Check Char	92	BCC over Message

6.9.11 Trimming: Trim Byte (RAIDAES)

Start	Len	Device	Channel	Password	Trim Byte	BCC

Abbreviation	Content	Example	Explanation
Start	Probe Test Start	02	Start of Telegram
Len	Length	04	Following Bytes in Telegram (in Byte excluding BCC)
Device	Device ID	CE	
Mode	Mode Byte	0D	Mode: Program Trim Byte
Channel	Channel ID	01	0x01: Program RF1 0x02: Program RF2 0x04: Program RF3
Trim Byte	Trim Byte	3D	Byte to program to EEPROM
BCC	Block Check Char	FB	BCC over Message

6.9.12 RF430F59xx UHF response

Start	Len	Cmd	Voltage	Temp	LF RSSI	LF Wake	
	UHF RSSI	UHF LQI	LF RSSI	UHF RSSI	EOL		

Abbreviation	Content	Example	Explanation
Start	Start	01	Start of Telegram
Len	Length	13	Following Bytes in Telegram (in Byte excluding BCC)
Cmd	Command	01	In a response always Null- Byte
Voltage	Voltage	32393334	4 Bytes representing voltage ASCII encoded (e.g. 2934=2.934V)
Temp	Temperature	323538	3 Bytes representing voltage ASCII encoded (e.g. 258=25.8ºC)
LF RSSI	3D- LF RSSI Data	868272	3 Bytes representing RSSI values at channels RF1, RF2, RF3; HEX encoded Byte2: RF1 Byte1: RF2 Byte0: RF3
LF Wake	LF Wake Up	01	Shows which wake up occurred 0…7 switches 0..7 8 Wake A 9 Wake B
UHF RSSI	UHF RSSI Data	05	RSSI value of UHF transmission
UHF LQI	UHF LQI	05	RSSI value of UHF transmission
EOL	End of Message	0D	Carriage return to indicate end of message

6.10 Command-Byte Structure

	Command1	Command2	Command3
Bit 0	1: Setup Mode 0: Normal Mode	1: No BLC EOF 0: BLC EOF (Normal)	Amount of Pages to read in Burst Read Mode
Bit 1	1: PPM 0: PWM	1: BLC Mode 0: Default Modulation	
Bit 2	1: LF Response 0: UHF Response	1: Burst Read-Mode 0: Single Read Mode	
Bit 3	1: No WP for 37126 0: No WP for 37122	1: Dummy Bit 0:	
Bit 4	Select Mode (Bit5Bit4) 00: Immobilizer Mode (Loop Ant.) 01: PEPS Mode (Stick Antenna) 10: PE no Wake Pattern x22/x26 11: Battery Backup Mode (Loop A.)	1: Special: Keep TX on 0: Normal: Switch TX off	
Bit 5		1: Inventory 0:	
Bit 6	1: Two-Byte Power Burst 0: One-Byte Power Burst	1: Cipher 0:	
Bit 7	1: Byte follows (Command2-Byte) 0: End of Command	1: Byte follows (Cmd3) 0: End of command	1: Byte follows (not used) 0: End of command

6.10.1 Advanced LF Reader Protocols

With the TBA-B300 Base Station the Advanced LF Reader Protocols are introduced. They are designed to enable the Base Station to do more work on its own, like doing a complete Pairing Process, rather than just executing single actions.

6.10.1.1 Get Pairing Data

Start	Len	Cmd	BCC

Byte #	Abbreviation	Content	Example	Explanation
1	Start	Advanced Start	03	Start of Telegram
2	Len	Length	01	Following Bytes in Telegram (in Byte excluding BCC)
3	Cmd	Advanced Command Byte	00	Get Pairing Data
4	BCC	Block Check Char	01	BCC over Message

The Base Station will respond with a *Get Pairing Data Response*.

6.10.1.2 Get Pairing Data Response

Start	Len	Cmd	AES Key	Vehicle ID	Paired Keys	Auth. Conf.	BCC

Byte #	Abbreviation	Content	Example	Explanation
1	Start	Advanced Start	03	Start of Telegram
2	Len	Length	01	Following Bytes in Telegram (in Byte excluding BCC)
3	Cmd	Advanced Command Byte	40	Get Pairing Data Response
4 to 19	AES Key	16 Byte AES Key 1	0F0E0D0C 0B0A0908 07060504 03020100	The Key which is programmed as AES Key 1 to the devices. Used for Encryption/ Authentication
20 to 23	Vehicle ID	4Byte Vehicle ID	ADFEADFA	
24	Paired Keys	Number of Paired Keys	02	Number of Keys paired by the Base Station
25	Auth. Conf.	Configuration of Authentication	04	Authentication con figuration byte of Bank7, Page 5. Contains Round Adder value and Challenge/ Signature lengths
26	BCC	Block Check		BCC over Message

Char

If there are paired keys the Base Station will send a *Get Key Data Response* for every paired key after this telegram.

6.10.1.3 Get Key Data Response

Start	Len	Cmd	Man.C.	Serial	SelAdr	Key#	Suc	BCC

Byte #	Abbreviation	Content	Example	Explanation
1	Start	Advanced Start	03	Start of Telegram
2	Len	Length	08	Following Bytes in Telegram (in Byte excluding BCC)
3	Cmd	Advanced Command Byte	41	Get Key Data Response
4	Man.C.	Manufacturer Code	0A	
5 to 7	Serial	Serial Number	0693CE	
8	SelAdr	Selective Address	02	
9	Key#	Key Number	02	
10	Suc	Success-Flag	01	01: true; Key is paired otherwise, pairing failed
11	BCC	Block Check Char	B3	BCC over Message

6.10.1.4 Sequential Pairing

Start	Len	Cmd	BCC

Byte #	Abbreviation	Content	Example	Explanation
1	Start	Advanced Start	03	Start of Telegram
2	Len	Length	01	Following Bytes in Telegram (in Byte excluding BCC)
3	Cmd	Advanced Command Byte	03	Sequential Pairing: The Base Station will start a Pairing Process for a single AES device in the Immobilizer Antennas LF field
4	BCC	Block Check Char	02	BCC over Message

After Pairing Process is done the Base Station will response with a *Get Pairing Data Response*.

6.10.1.5 Inventory Pairing

Start	Len	Cmd	BCC

Byte #	Abbreviation	Content	Example	Explanation
1	Start	Advanced Start	03	Start of Telegram
2	Len	Length	01	Following Bytes in Telegram (in Byte excluding BCC)
3	Cmd	Advanced Command Byte	04	Inventory Pairing: The Base Station will start a Inventory Pairing Process for all AES devices in the Immobilizer Antennas LF field
4	BCC	Block Check Char	05	BCC over Message

After Pairing Process is done the Base Station will response with a *Get Pairing Data Response*.

6.10.1.6 Mutual Authentication

Start	Len	Cmd	BCC

Byte #	Abbreviation	Content	Example	Explanation
1	Start	Advanced Start	03	Start of Telegram
2	Len	Length	01	Following Bytes in Telegram (in Byte excluding BCC)
3	Cmd	Advanced Command Byte	05	Mutual Authentication: The Base Station sends a Mutual Authentication downlink telegram using the Pairing Data. A paired AES transponder in the LF field will authenticate itself. (Only one transponder at a time may be in the LF field!)
4	BCC	Block Check Char	04	BCC over Message

After Authentication is evaluated the Base Station will response with an *Authentication Result Response*.

6.10.1.7 Authentication Result Response

Start	Len	Cmd	Serial	Result	BCC

Byte #	Abbreviation	Content	Example	Explanation
1	Start	Advanced Start	03	Start of Telegram
2	Len	Length	05	Following Bytes in Telegram (in Byte excluding BCC)

3	Cmd	Advanced Command Byte	42	Authentication Result Response
4 to 6	Serial	Serial Number	0693CE	Serial Number of Key which authenticated correctly
7	Result	Result	01	01: true; authentication successful, otherwise authentication failed
8	BCC	Block Check Char	1D	BCC over Message

6.10.1.8 Mutual Authentication with Anticollision

Start	Len	Cmd	BCC

Byte #	Abbreviation	Content	Example	Explanation
1	Start	Advanced Start	03	Start of Telegram
2	Len	Length	01	Following Bytes in Telegram (in Byte excluding BCC)
3	Cmd	Advanced Command Byte	06	Mutual Authentication with Anticollision: Identical to Mutual Authentication, but more paired AES devices may be in the LF field at a time.
4	BCC	Block Check Char	07	BCC over Message

After Authentication is evaluated the Base Station will response with an *Authentication Result Response*. If more than one device authenticated successfully, the device with the lowest *Key Number* will be listed in the *Authentication Result Response*.

6.10.1.9 PEPS Configuration

Start	Len	Cmd	BCC

Byte #	Abbreviation	Content	Example	Explanation
1	Start	Advanced Start	03	Start of Telegram
2	Len	Length	01	Following Bytes in Telegram (in Byte excluding BCC)
3	Cmd	Advanced Command Byte	10	PEPS Configuration: The Base Station will automatically program all relevant pages on Bank 7 to configure the reception of Wake Pattern A. (Pages 7, 11 and 13)
4	BCC	Block Check Char	04	BCC over Message

Instead of an USB response, the Base Station will show the success of this task through blink codes: green LED4 means successful, red LED2 means failure.

6.10.1.10 PEPS Telegram

Start	Len	Cmd	WakeLen	WakeP	DatLen	Data	BCC

Byte #	Abbreviation	Content	Example	Explanation
1	Start	Advanced Start	03	Start of Telegram
2	Len	Length	07	Following Bytes in Telegram (in Byte excluding BCC)
3	Cmd	Advanced Command Byte	11	PEPS Telegram: A PEPS telegram will be sent with the specified Wake Pattern and Additional Data
4	WakeLen	Length of Wake Pattern	03	Length of Wake Pattern in **nibbles**
5 to 7	WakeP	Wake Pattern	000123	Field contains Wake Pattern is always padded left with 0's. In this example the Wake Pattern would be: 0x123 (12 bit)
8	DatLen	Length of Additional Data	01	Length of Additional Data, sent after Data Delay Burst. Length in **bytes**
9 to 9+N	Data	Additional Data	C2	Contains Additional Data
9+N+1	BCC	Block Check Char		BCC over Message

If BCC is correct and telegram was sent, the green LED4 will flash up. No USB response is sent.
Since there is no LF response on a PEPS telegram it's recommended to observe the WAKE pin on the AES device to check if device was woken by the PEPS telegram.

6.10.1.11 Automatic Trimming

The Base Station will trim the capacitive trimming arrays to meet the desired resonant frequency on selected channels.

Start	Len	Cmd	Device	Frequency	Config	BCC

Byte #	Abbreviation	Content	Example	Explanation
1	Start	Advanced Start	03	Start of Telegram
2	Len	Length	06	Following Bytes in Telegram (in Byte excluding BCC)
3	Cmd	Advanced Command Byte	20	Automatic Trimming

4	Device	Device ID	7E	Known device IDs are: 7E: CRAID/ DST80 devices CE: RAIDAES/ AES devices
5 to 7	Frequency	Target resonant frequency of resonant circuit	020C38	This is an integer value in hex-notation and represents the resonant frequency in hertz. Example: 134.2d [kHz] = 134200d [Hz] = 020C38h [Hz]
8	Config	Configuration Byte	32	MSNibble: number of channels LSNibble: number of iterations The example value means there are three channels to be trimmed and the trimming process will be executed twice. (It's recommended to execute the trimming process at least twice to minimize the side effects which occur when the resonant circuits influence each other)
9	BCC	Block Check Char	5C	BCC over Message

While the Base Station is in the trimming process the yellow LED1 will be on and the orange LED3 will toggle at every single trimming step. After trimming is done all LEDs will lapse, except the green LED4. An *Automatic Trimming Response* will be sent to the PC.

6.10.1.12 Automatic Trimming Response

After *Automatic Trimming* process is done, the Base Station will uplink the trimming results to the PC.

Start	Len	Cmd	Frequencies	BCC

Byte #	Abbreviation	Content	Example	Explanation
1	Start	Advanced Start	03	Start of Telegram
2	Len	Length	0D	Following Bytes in Telegram (in Byte excluding BCC)
3	Cmd	Advanced Command Byte	60	Automatic Trimming Response
4 + ((n-1)*4) to 7 + ((n-1)*4)	Frequency n (In this Example: Frequencies 1 to 3)	Resulting resonant frequency of channel n	40020C45 64020C45 58020BF4	This is the Trim Byte with an integer value in hex-notation and represents the best Trim Byte value and the resonant frequency in hertz. Example: With Trim Byte 0x40 this frequency was measured: 020C45h [Hz] => 134.213d [kHz] On second channel with Trim Byte 0x64 also 134.2 kHz were measured The resulting resonant frequencies of all channels are attached one after another, each with a four byte length. The number of channels can be derived from the length byte. In this example three channels were trimmed.
4 + (n*4)	BCC	Block Check Char	EC	BCC over Message

6.10.2 Advanced Command Byte Structure

	Command
Bit0	Command ID See corresponding command.
Bit1	
Bit2	
Bit3	
Bit4	
Bit5	
Bit6	1: Response (Base Station answers) 0: Request (Base Station is asked to do something)
Bit7	1: Byte follows (Not used yet) 0: End of Command

6.11 UHF Passive Entry/ Passive Start / Remote Keyless Entry protocol

6.11.1 Communication Link Settings

- Carrier frequency: 868.34 MHz
- FSK deviation: 20.6 kHz
- Modulation: GFSK
- Data rate: 38.4kBaud
- Receiver bandwidth: 101.6 kHz
- Transmitter output power: -5 dBm
- Manchester coding: disabled
- Data whitening: disabled
- Automatic Frequency compensation: enabled
- Forward Error Correction: disabled

6.11.2 Communication Protocol

- Total length: 24 bytes

- Preamble length: 4 bytes
- Sync word: 2 bytes (D391hex)
- Data length: 16 bytes
  - Protocol Identifier 8 bit

  - Key number 8 bit
  - Serial number 24 bit
  - Manufacturer Code 8 bit
  - Counter Value 16 bit
  - Signature 24 bit
  - Dummy Byte 8 bit

  - Dummy Bits 2 bit
  - LF RSSI RF3 10 bit; Is set to zero in RKE-Mode
  - LF RSSI RF2 10 bit; Is set to zero in RKE-Mode
  - LF RSSI RF1 10 bit; Is set to zero in RKE-Mode
- UHF RSSI, LQI, CRC: 2 bytes

Revision History

NOTE: Page numbers for previous revisions may differ from page numbers in the current version.

Rev.	Version	SCN	Description of Change	Date	By
0	0	-	New Issue	09/21/2011	J. Austen

IMPORTANT NOTICE

Texas Instruments Incorporated and its subsidiaries (TI) reserve the right to make corrections, modifications, enhancements, improvements, and other changes to its products and services at any time and to discontinue any product or service without notice. Customers should obtain the latest relevant information before placing orders and should verify that such information is current and complete. All products are sold subject to TI's terms and conditions of sale supplied at the time of order acknowledgment.

TI warrants performance of its hardware products to the specifications applicable at the time of sale in accordance with TI's standard warranty. Testing and other quality control techniques are used to the extent TI deems necessary to support this warranty. Except where mandated by government requirements, testing of all parameters of each product is not necessarily performed.

TI assumes no liability for applications assistance or customer product design. Customers are responsible for their products and applications using TI components. To minimize the risks associated with customer products and applications, customers should provide adequate design and operating safeguards. TI does not warrant or represent that any license, either express or implied, is granted under any TI patent right, copyright, mask work right, or other TI intellectual property right relating to any combination, machine, or process in which TI products or services are used. Information published by TI regarding third-party products or services does not constitute a license from TI to use such products or services or a warranty or endorsement thereof. Use of such information may require a license from a third party under the patents or other intellectual property of the third party, or a license from TI under the patents or other intellectual property of TI.

Reproduction of TI information in TI data books or data sheets is permissible only if reproduction is without alteration and is accompanied by all associated warranties, conditions, limitations, and notices. Reproduction of this information with alteration is an unfair and deceptive business practice. TI is not responsible or liable for such altered documentation. Information of third parties may be subject to additional restrictions.

Resale of TI products or services with statements different from or beyond the parameters stated by TI for that product or service voids all express and any implied warranties for the associated TI product or service and is an unfair and deceptive business practice. TI is not responsible or liable for any such statements.

TI products are not authorized for use in safety-critical applications (such as life support) where a failure of the TI product would reasonably be expected to cause severe personal injury or death, unless officers of the parties have executed an agreement specifically governing such use. Buyers represent that they have all necessary expertise in the safety and regulatory ramifications of their applications, and acknowledge and agree that they are solely responsible for all legal, regulatory and safety-related requirements concerning their products and any use of TI products in such safety-critical applications, notwithstanding any applications-related information or support that may be provided by TI. Further, Buyers must fully indemnify TI and its representatives against any damages arising out of the use of TI products in such safety-critical applications.

TI products are neither designed nor intended for use in military/aerospace applications or environments unless the TI products are specifically designated by TI as military-grade or "enhanced plastic." Only products designated by TI as military-grade meet military specifications. Buyers acknowledge and agree that any such use of TI products which TI has not designated as military-grade is solely at the Buyer's risk, and that they are solely responsible for compliance with all legal and regulatory requirements in connection with such use.

TI products are neither designed nor intended for use in automotive applications or environments unless the specific TI products are designated by TI as compliant with ISO/TS 16949 requirements. Buyers acknowledge and agree that, if they use any non-designated products in automotive applications, TI will not be responsible for any failure to meet such requirements.

Following are URLs where you can obtain information on other Texas Instruments products and application solutions:

Products	
Amplifiers	amplifier.ti.com
Data Converters	dataconverter.ti.com
DLP® Products	www.dlp.com
DSP	dsp.ti.com
Clocks and Timers	www.ti.com/clocks
Interface	interface.ti.com
Logic	logic.ti.com
Power Mgmt	power.ti.com
Microcontrollers	microcontroller.ti.com
MCU RF / RFID	http://www.ti.com/rfid/
RF/IF and ZigBee® Solutions	www.ti.com/lprf

Applications	
Audio	www.ti.com/audio
Automotive	www.ti.com/automotive
Broadband	www.ti.com/broadband
Digital Control	www.ti.com/digitalcontrol
Medical	www.ti.com/medical
Military	www.ti.com/military
Optical Networking	www.ti.com/opticalnetwork
Security	www.ti.com/security
Telephony	www.ti.com/telephony
Video & Imaging	www.ti.com/video
Wireless	www.ti.com/wireless

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265