Leuze electronic

Leuze RFID systems

RFU 61 SL 100-EU
RFU 81 SL 100-EU
with IMRFU 1

Read /write devices according to
EPC 1 Gen 2, ISO 18000-6C

Description of commands and configuration

(direct communication via terminal software)

5
0
1
1
9
5
5
0

Version V 1.3

CONTENT

1 Command structure

For the data interface we use the Leuze standard with 9600 Bd, 1 Startbit, 8 Databits, none Parity, 1 Stoppbit. The data frame is the typically used type at Leuze electronic.

STX		CR LF

The data from and to the RFM is coded in ASCII-Hex and always read or written in complete data blocks. Applicable as data conternt are all characters of the ASCII table. Between receive data and send data to the RFU should be a delay of about 150 ms.

1.1 Commands without Data

Commands are recognized in Capital letters as well as in small letters

STX	Command	CR LF
02h	HEX-Character	0Dh 0Ah

Command: **R0**/**r1** (5230h) *Reset to factory settings* (0=IMRFU, 1=RFU)
Response: **Q2** (5132h) *Acknowledge, action performed*

Command: **H**/**h** (48h) *stop command & warm start IMRFU, setting stays*
Response: **Q2** (5132h) *Acknowledge, action performed*

Command: **V0**/**v1** (5630h) *get version of firmware*
Response: 1012031234IMRFU
with 10=year,12=month, 03=day,1234=Code, IMRFU=device type, for RFU FW/HW version

Command: **+** (2Bh) Sets Trigger (LED red =ON)

Command: **-** (2Dh) Stops Trigger (LED red = OFF*)*

For the commands 'N ', 'B','D' und 'W without write forward' it is **neccessary to have** a **READ** operation (via Trigger) **before and** the tag has to stay within the field! The smallest memory area is a single block with 2Byte, means always use a multiplier of 2Bytes.

1.2 Data output / response telegram of the devices

Data output after trigger (parameter setting via configuration: operation mode)
The devices deliver different data after a trigger:

EPC number (factory setting)

e.g. 0010000000C006003B4D530002007420000000000
This response contains the following informations (starting from left):

0	character, if there are more telegrams. (0 means only one telegram)
01	bank number
0000	byte address within bank
000C	number of bytes (12byte)
006003	transponder type, see table
B4D5	EPC-Length (2Byte)
3000	EPC-special data
2007420000000000	EPC number of the transponder

TID-number (Serial number)

e.g. 0020000000C006004E2006004016E43C700000000
This response contains the following informations (starting from left):

0	character, if there are more telegrams. (0 means only one telegram)
02	bank number
0000	byte address within bank
000C	number of bytes (12byte)
006004	transponder type, see table
E2006004016E43C700000000	TID –Number(8Byte) of transponder

User data (Bank 03), 2 to 20 byte possible (depends on transponder)

e.g. 003000400020060030000 (2 Byte, starting with Byte 04)
In this response are several informations included, too (starting from left):

0	character, if there are more telegrams. (0 means only one telegram)
03	Bank number
0004	Start-address withink bank
0002	number of byte
006003	transponder type, see table
0000	data in hexadecimal presentation (2 characters /byte)

Data output after Online-command (via terminal software)

Response after command Read Blocks N0100000004000000 (see.chapter 1.1)

e.g. 00100000004006003B4D53000 (4 Byte, starting with Byte 00)
In this response are several informations included, too (starting from left):

0	character, if there are more telegrams. (0 means only one telegram)
01	Bank number
0000	Start-address number
0004	number of byte
006003	transponder type, see table
B4D53000	data in hexadecimal presentation (2 characters /byte)

1.3 Commands with Data attached

Command Read Byte(s) N (4Eh) for Reading of 2 or more data Bytes, with one transponder in field

example: N0100000002000000 (Read Bank 01, from Byte 00, 2 Byte)

STX	**N**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**2**	**0**	**0**	**0**	**0**	**0**	**0**	CR	LF
02	4E	30	31	30	30	30	30	30	30	30	32	30	30	30	30	30	30	0D	0A
PRE	CMD	Bank		Start Address				No of Bytes				Transponder type						POST	

The structure of the response is described in chapter 1.2
Per Data byte an average response time of 15ms is typical.

Command Write Byte(s) W (57h) **W0100040002000000xxxxxxxx**

STX	**W**	**0**	**1**	**0**	**0**	**0**	**4**	**0**	**0**	**0**	**2**	**0**	**0**	**0**	**0**	**0**	**0**	X	X	X	X	CR	LF
02	57	30	31	30	30	30	34	30	30	30	32	30	30	30	30	30	30	x	X	X	X	0D	0A
PRE	CMD	Bank		Start Address				No of Bytes				Transponder type						DATA1		DATA2		POST	

For writing always a complete Block (multiplier of 2 Byte) is transmitted, means. 4 digits(hex). The response with ‘write forward’ is'Q4', after trigger or '+' the data is written to the transponder and with ‘Q5' successful answered. Without 'Write forward'(default) a transponder must stay in the field and the response is 'Q5' directly.

Response Q4 / Q5 Q4 Command understood (see Messages)
Q5 Writing succesful
Q0 Writing failed

For any write operation it is neccessary to have ONLY ONE Transponder in the reading field of the reader.

Command Lock Bank B (42h) B01 Lock bank EPC
B02 Lock bank SNR(TID)
B03 Lock UserBank

Note: The activation of a Lockbit for a bank can only be set ONCE. A deactivation of this function is NOT possible. Locking a single byte within a bank is not available.

Command Diagnose D (44h) delivers informations of read quality, e.g. interferences, while setup, etc. The devices tries this No of reads and gives the valid responses back,

D19 gives 25 (19h) trials, time consumption ca. 3Sec
D32 gives 50 (32h) trials
D64 gives 100 (64h) trials

Command Set Output A (41h) A0FF On
A000 Off

This command sets the output permanent and gets no response! This will work only if the output is **not activated** automatically !! Reaction time 20 ms.

Command Switch Field ON/OFF F (46h) F1 Switch “ON“
F2 Switch“OFF“
F3 HF-Reset

With the F-command, the magnetic field of the RFU´s can be switched. The answer on this command is Q2, and the field is switched ON/OFF. The reaction time on F commands is 20 ms. The field is switched on automatically after a new trigger pulse.

1.4 Transponder(tag-) types within the telegram

Some commands and answers transmit the transponder type within the telegram. The RFU devices are able to read standard EPC1Gen2 types, to select some different types could be set.
See the following table for typical tag types but it will be not complete and values may vary or change.

N0	Description
000000	EPC1 Gen2 (12 /30characters Bank 01 from Byte 04, more banks possible (TID + USER)
006003	NXP G2XL: TID+EPC(30characters)
006004	NXP G2XM: TID+EPC(30characters)+USER(30charaters)
001093	Impinj Monza 3: TID+EPC(12charaters)
003412	Alian Higgs 3: TID+EPC(12characters)+USER(30characters

2 Configuration of the RFID-devices

With the Leuze RF-config-tool the parameter setting is very easy and transparent. All functions are displayed in menus and click buttons. Each RFU device is connected and configured via an IMRFU. But all devices can be activated and configured directly from a PLC or via standard terminal software, too. With the printed information below you can choose your preferred and easiest way. The used structure is always like described in paragraph 1.
Dependent on the function, one or two addresses can belong to one parameter. The factory setting is printed in bold letters.

Command Read configuration G **GFF00 (complete)**
Response 00xxxxxxx
G1000 (only addresses 00-0Fh)
. G01xx (only one address)

Command Configure C **C010199**
01 number of bytes in telegram
01 parameter address
99 configuration data

When using this command it is important to know that only the **start address** is to print and all data is transmitted serial to the configurations register. This allows either to send the configuration data with one string or address by address. Each valid address can be the start address. The change of configuration is answered by the 'Q1' response. The data for operation mode "Write" must be stored with this command beginning at the address 11h.

Answer Q1 (see Chapter 3. messages)

structure: C [no of bytes][record address] [data]

The number of data must fit a byte length (2 characters / byte), if not you receive an error message (E02). The data is always in hexadecimal presentation. If you communicate via **field bus** with the RFU all characters of the command are to handle as a separate **ASCII character** in the transmission.

For operation mode "Write" the data has to be stored **before** in the same way (C11xxxx). The memory area for the data to write is 11h to 30h (32 Byte)
Example: C041187654321 stores write data (4Byte) starting address 11h.

Structure of the configuration parameters

Address	Level	Parameter/Function
00	01	Baudrate RS232
01	30	Functions Register 1
02	10	Functions Register 2
03	10	Triggermode / Output
04	01	Trigger pulse time (ms) Highbyte
05	2C	Trigger pulse time (ms) Lowbyte
06	01	Output pulse time (ms) Highbyte
07	2C	Output pulse time (ms) Lowbyte
08	1B	Power level RFU
09	01	Memory Bank No
0A	00	Start address Highbyte
0B	00	Start address Lowbyte
0C	00	Number of blocks Highbyte
0D	0C	Number of blocks Lowbyte
0E	00	Tagtype Highbyte
0F	00	Tagtype
10	00	Tagtype Lowbyte
11-30	00	*Write mode: Data to Write (max 32Byte)*

Very important are the two functions registers, where the function of the device is seet. But all parameters are described in the following chapters.

2.4 Configuration Baudrate Address 00h

Bit	Level	Hex	Description
0	1	**01**	Baudrate 9600Bd (Factory set)
1	0	02	Baudrate 19200Bd
2	0	04	Baudrate 38400Bd
4 + 1	0	12	Baudrate 115200Bd

The set information is calculated with the Bit row. Plese note Bit 7 is MSP.
Factory set: 01h

2.2 Configuration Functions Register 1 Address 01h

Bit	Function	Level	Description
0	Operation mode	**0**	Operation mode Read
		1	Operation mode Write
1	Verification	**0**	Nur Schnittstellenquittung nach Schreiben
		1	Zusätzliche Kontrollesung
2	Reserved	**0**	
3	Reserved	**0**	
4	Trigger	0	Permanent ready for read
		1	Read on trigger puls
5	Read mode	0	Permanent Read and data output
		1	Singleshot (read once while in field)
6	Write forward	**0**	Not active, for Write command a transponder must be within the reader field !
		1	Active, after write command data is written in the next transponder entering the field
7	Reserved	**0**	reserved

factory set: 30h

The operation mode defines, what function a trigger pulse (or '+') causes.
The factory setting is "Read", that means after a trigger the EPC no. is read (addresses 0A-0Ch). The response is the same as after a "N" command: state, bank no, Byte no, No of byte, tag type, data.
With operation mode "Write" the stored data (address C11 following) is written into every tag after trigger, answer is "Q5".or “Q0” and “^” in case of failure.

2.3 Configuration Functions Register 2 Address 02h

Bit	Function	Level	Description
0	Data 1	**0**	READ, configured Address only
		1	READ, configured + EPC-Bank
1	Data 2	**0**	READ, configured Address only
		1	READ, configured + TID-Bank
2	CRC	**0**	NO CRC check
3	Reserved	**0**	
4	Output switch	0	Not used
		1	Automatical activated, Address 03h
5	Gate-Mode	**0**	Stand alone
		1	Reader address in telegram
6	Location info	**0**	1= for telegram W / N Bank and Start address out of config, not in telegram
7	Tag Type info	**0**	1=for telegram W / N type info out of config, not in telegram

factory setting: 10h

Important note:
Some functions refer to others, some are mutually exclusive! Below the most important reliances of configuration settings with this affections are listed:

Write forward = "Active" (Adr. 01, Bit 6)	Trigger **active** (Adr.01, Bit 4)
Read mode = "permanent read" (Adr. 01,Bit 5)	Trigger = **not** active (Adr. 01, Bit 4), write forward = **not active** (Adr.01, Bit 6)

If any of these points is not or in parts only taken notice of, the device gives back an error "E10" for invalid configuration and nothing is changed.

RFU 61 max. 1 transponder, factory set
RFU 81 max. 1 transponder, factory set

2.4 Configuration Trigger / Output Address 03h

Value	Description
00	READ/ Write as long Higlevel on Input, Output NoRead
01	Read/ write pos. slope + time, Output NoRead
02	Read/write neg. slope + time, Output NoRead
10	READ/Write as long Higlevel on Input,Output GoodRead
11	Read/ write pos. Slope + time, output GoodRead
12	Read/write neg. slope + time, output GoodRead

Factory set = *10h*

2.5 Configuration Trigger puls time Addresses 04/05h

This is the time after the trigger puls in a range from 30 to 4000 ms. The chosen value is in hexadecimal numeric system. *Factory setting: 012Ch*

Examples

300 ms	*012Ch*
500 ms	*01F4h*
1000 ms	*03E8h*
2000 ms	*07D0h*

2.6 Configuration Output pulse time Addresses 06 / 07h

The activation time for "Good read" or "No read" is set between 30 and 9000 ms. The value is in hexadecimal numeric system. *Factory setting :12Ch*.

Examples

50 ms	*0032h*
300ms	*012Ch*
500 ms	*01F4h*
1000 ms	*03E8h*
2000 ms	*07D0h*

2.7 Configuration ERP power of RFU Address 08h

For adjusting the device to the application / range the output power (ERP) can be set in this address. In factory set for all devices work is max. power. The possible power levels are differing depending on the used device. Please refer to the according manual.

RFU61		**RFU81**	
P-Level (h)	ERP mW	P-Level (h)	ERP mW
0A	10	00	100
0D	20	01	250
0F	32	02	500
11	50	03	750
14	100	04	1000
16	158	05	1250
17	200	06	1500
18	250	07	1750
19	316	08	2000
1B	max	**09**	Max

2.8 Configuration Memory bank Address 09h

The frequency band UHF uses up to 3 banks (Transponder chip dependent)
01 : EPC Bank; 02 TID (Serial number) ; 03 USER Bank
Factory set 01h

2.9 Configuration Start address Read / Write Addresses 0A/0Bh

Start address Read (after Trigger) *factory setting : 00 (0000h),*
After a trigger (or '+') from this address on the data is read / wrote from / to the transponder. The possible byte number depends on the tag type.

2.10 Configuration Read / Write number of Blocks Address 0C/0Dh

This is the number of data blocks read / wrote on one operation after a trigger (or '+'). Please use values as a multiplier of 2Byte
factory setting : 000Ch gives 12 Data block range 02-20h

2.11 Configuration Transponder type Addresses 0E-10h

Defines the transponder type for read/ write access. The value 000000h Allows access to all EPC1Gen2 types. A different value works like a filter and only same types allow address then.
Factory set: 000000h

2.12 Configuration Write data(max 32Byte) Adresses 11 to 30h

In the operation mode "Write" this data will be written to the tag after a trigger. The data to write must be stored **before** starting with C-command. All tags get the same information. *factory setting : 000000….h*

3 Response codes and Error messages

For receiving some information after commands we have several codes and messages implemented in the firmware of the devices.

Response codes

Sign for a response is the letter `Q`. A response with 'Q' makes shure the command was understood from the device. The telegram looks like usual.

STX	**Q**	Code	CR LF

The table shows the meaning of the Code:

Code	Description/meaning
´Q0´	Command could not be performed
´Q1´	Command executed
´Q2´	Action performed
´Q4´	Write Command understood
´Q5´	Write Block successful

Error messages

An error occurs, if a command or string is not complete or send with false characters.The letter `E`is the sign for errors. The errors in detail

Code	Meaning
E01	Invalid command
E02	Invalid parameter
E04	Data Frame error
E08	CRC Error
E10	Controvert configuration settings (e.g.Trigger and permanent reading)

If an „E08“ message occurs the CRC was activated. For Reset please use the Command „R0“ and D2h via interface.

4 Transponder specific information (Tag Info)

4.1 Memoryorganisation 96Bit (TID + EPC bank)

(TID, EPC12 Byte(+CRC)/ 30 Byte, 2 Byte per block)

Bank	Byte	Description
0	00-03h	Password, no Access
1	10-1Eh	Enhanced EPC-Bank, chip dependent
	04h – 0Fh	EPC-Bank
	00h - 03h	EPC-Bank (CRC, PC)
2	00-07h	TID (SNR), Read Only

This types have the TID and EPC bank and some are used as a Read Only (RO) type. The EPC bank can be blocked via command. Then the information is fixed.
The following Chips use this organisation:

Manufactorer	Type-No.
Impinj Monza 3	001 093
NXP G2XL	006 004

4.2 Memory organisation 512Bit (TID+EPC+USER Bank)

(TID, EPC 12Byte (+CRC)/ 30Byte, USER 30Byte, 2 Byte)

Bank	Block	Description
0	00-03h	Password, no Access
1	10-1Eh	Enhanced EPC-Bank, chip dependent
	04h – 0Fh	EPC-Bank
	00h - 03h	EPC-Bank (CRC, PC)
2	00-07h	TID(SNR), Read Only
3	00-3Fh	User bank

The EPC bank and the USER bank can be locked via command. Then the information is fixed.
The following Chips use this organisation:

Manufactorer	Type-No.
Alien Higgs 3	003 412
NXP G2XM	006 003

4.3 Not supported Transponderchips

Still new transponder are devellopped for this frequency and will appear on the markets.. Because of this it may occure there is no function with the firmware in your device. Please ask for actual versions if neccessary.

Former versions of the EPC chips were not supported, like EPC1Gen1 and EPC1Gen0.

5 ASCII-Table

HEX	DEC	CTRL	ABV	ENGLISH	GERMAN
00	0	^@	NUL	NULL	Null
01	1	^A	SOH	START OF HEADING	Kopfzeilenbeginn
02	2	^B	STX	START OF TEXT	Textanfangszeichen
03	3	^C	ETX	END OF TEXT	Textendezeichen
04	4	^D	EOT	END OF TRANSMISSION	Ende der Übertragung
05	5	^E	ENQ	ENQUIRY	Aufforderung zur Datenübertragung
06	6	^F	ACK	ACKNOWLEDGE	Positive Rückmeldung
07	7	^G	BEL	BELL	Klingelzeichen
08	8	^H	BS	BACKSPACE	Rückwärtsschritt
09	9	^I	HT	HORIZONTAL TABULATOR	Horizontal Tabulator
0A	10	^J	LF	LINE FEED	Zeilenvorschub
0B	11	^K	VT	VERTICAL TABULATOR	Vertikal Tabulator
0C	12	^L	FF	FORM FEED	Seitenvorschub
0D	13	^M	CR	CARRIAGE RETURN	Wagenrücklauf
0E	14	^N	SO	SHIFT OUT	Dauerumschaltungszeichen
0F	15	^O	SI	SHIFT IN	Rückschaltungszeichen
10	16	^P	DLE	DATA LINK ESCAPE	Datenübertragungsumschaltung
11	17	^Q	DC1	DEVICE CONTROL 1 (X-ON)	Gerätesteuerzeichen 1
12	18	^R	DC2	DEVICE CONTROL 2 (TAPE)	Gerätesteuerzeichen 2
13	19	^S	DC3	DEVICE CONTROL 3 (X-OFF)	Gerätesteuerzeichen 3
14	20	^T	DC4	DEVICE CONTROL 4	Gerätesteuerzeichen 4
15	21	^U	NAK	NEGATIVE (/Tape) ACKNOWLEDGE	Negative Rückmeldung
16	22	^V	SYN	SYNCRONOUS IDLE	Synchronisierung
17	23	^W	ETB	END OF TRANSMISSION BLOCK	Ende des Datenübertragungsblocks
18	24	^X	CAN	CANCEL	Ungültig
19	25	^Y	EM	END OF MEDIUM	Ende der Aufzeichnung
1A	26	^Z	SUB	SUBSTITUTE	Substitution
1B	27	^[	ESC	ESCAPE	Umschaltung
1C	28	^\	FS	FILE SEPARATOR	Hauptgruppentrennzeichen
1D	29	^]	GS	GROUP SEPARATOR	Gruppentrennzeichen
1E	30	^^	RS	RECORD SEPARATOR	Untergruppentrennzeichen
1F	31	^_	US	UNIT SEPARATOR	Teilgruppentrennzeichen
20	32		SP	SPACE	Leerzeichen
21	33		!	EXCLAMATION POINT	Ausrufungszeichen
22	34		"	QUOTATION MARK	Anführungszeichen
23	35		#	NUMBER SIGN	Nummerzeichen
24	36		$	DOLLAR SIGN	Dollarzeichen
25	37		%	PERCENT SIGN	Prozentzeichen
26	38		&	AMPERSAND	Kommerzielles UND-Zeichen
27	39		'	APOSTROPHE	Apostroph
28	40		(	OPENING PARENTHESIS	runde Klammer (offen)
29	41		)	CLOSING PARENTHESIS	runde Klammer (geschlossen)
2A	42		*	ASTERISK	Stern
2B	43		+	PLUS	Pluszeichen
2C	44		,	COMMA	Komma
2D	45		-	HYPHEN (MINUS)	Bindestrich (Minuszeichen)
2E	46		.	PERIOD (DECIMAL)	Punkt
2F	47		/	SLANT	Schrägstrich (rechts)
30	48		0		
31	49		1		
32	50		2		
33	51		3		
34	52		4		
35	53		5		
36	54		6		
37	55		7		
38	56		8		
39	57		9		
3A	58		:	COLON	Doppelpunkt
3B	59		;	SEMI-COLON	Semikolen
3C	60		<	LESS THEN	Kleiner als
3D	61		=	EQUALS	Gleichheitszeichen
3E	62		>	GREATER THEN	Größer als
3F	63		?	QUESTION MARK	Fragezeichen
40	64		@	COMMERCIAL AT	Kommerzielles a-Zeichen

HEX	DEC	CTRL	ABV	ENGLISH	GERMAN
41	65		A		
42	66		B		
43	67		C		
44	68		D		
45	69		E		
46	70		F		
47	71		G		
48	72		H		
49	73		I		
4A	74		J		
4B	75		K		
4C	76		L		
4D	77		M		
4E	78		N		
4F	79		O		
50	80		P		
51	81		Q		
52	82		R		
53	83		S		
54	84		T		
55	85		U		
56	86		V		
57	87		W		
58	88		X		
59	89		Y		
5A	90		Z		
5B	91		[	OPENING BRACKET	eckige Klammer (offen)
5C	92		\	REVERSE SLANT	Schrägstrich (links)
5D	93		]	CLOSING BRACKET	eckige Klammer (geschlossen)
5E	94		^	CIRCUMFLEX	Zirkumflex
5F	95		—	UNDERSCORE	Unterstrich
60	96		`	GRAVE ACCENT	Gravis
61	97		a		
62	98		b		
63	99		c		
64	100		d		
65	101		e		
66	102		f		
67	103		g		
68	104		h		
69	105		i		
6A	106		j		
6B	107		k		
6C	108		l		
6D	109		m		
6E	110		n		
6F	111		o		
70	112		p		
71	113		q		
72	114		r		
73	115		s		
74	116		t		
75	117		u		
76	118		v		
77	119		w		
78	120		x		
79	121		y		
7A	122		z		
7B	123		{	OPENING BRACE	geschweifte Klammer (offen)
7C	124		|	VERTICAL LINE	Vertikalstrich
7D	125		}	CLOSING BRACE	geschweifte Klammer (geschlossen)
7E	126		~	TILDE	Tilde
7F	127		DEL	DELETE (RUBOUT)	Löschen

Leuze electronic GmbH+Co.KG
Postbox 1111
In der Braike 1
D-73277 Owen / Teck
Tel +49 (07021) 573-0
Fax +49 (07021) 573199
E-mail: info@leuze.de
http://www.leuze.de

State 11 / 2011
document UM_RFU-commands_en_50119550