® EM MICROELECTRONIC - MARIN SA

A COMPANY OF THE SWATCH GROUP

AppNote 406

Application Note 406

Title: **EM4150 Application Note**

Product Family: **RFID**

Part Number: EM4150
Keywords: 125KHz Read / Write. Contactless Identification Device
Date: 25 September 2002

TABLE OF CONTENT

1 Introduction

The EM4150 is a chip to be used in identification or data storage systems. Connected to a single coil and packed into a housing (plastic card or other) it represents a complete transponder which can be read or written by a base station via magnetic coupling. Due to the high integration level and the low power consumption the coil is the only external component which is necessary.

The EM4150 is designed to work with a carrier frequency of 115kHz to 135kHz. The bit period can be chosen to be 32 or 64 carrier frequency cycles which causes the data rate to be about 3.9kBaud or 1.95kBaud, allowing a full memory read cycle of 32 bit at 125kHz within 29.5ms or 59ms.

The chip contains all in all 1024 bit of EEPROM which is organized in 32 bit double words. Three of these double words have special functions, the rest is user memory. Beside that the chip contains two double words of laser programmed ROM. These are used for identification and serial number and can not be modified.

Due to the large temperature range and the on chip memory the typical application for the EM4150 is the ticketing or industrial data storage. Automotive immobilizer usage by means of a rolling code method is also feasible.

A brief summary of the chip is given below:

- 1kBit of E²PROM
- 32 bit of factory programmed serial number
- 32 bit of factory programmed device identification
- Read memory area defined by user
- Write inhibited memory area defined by user
- Read protected memory area defined by user
- Power check for E²PROM write operation
- Data transmission performed by amplitude modulation
- -40°C to +85°C temperature range
- Typical 125kHz carrier frequency
- Two data rate options can be chosen

2 General Operation

The transponder is interfaced with the base station via the magnetic coupling of two coils. Both coils are acting as a transformer with a very large air gap. The air gap is in typical applications that large that the coupling factor of both coils is below 5%.

The base station applies a 125kHz square wave signal to its antenna coil, which is connected with a capacitor to a series resonance circuit to increase the coil current and filter the harmonics of the square wave signal. The quality factor of this series resonance circuit is usually in the range of 10 to 15, limited by the tolerance of the electronic components and the data rate of the transponder.

This base station coil current induces an alternating voltage in the transponder coil. To increase this voltage the transponder coil is connected to an on-chip capacitor which forms a parallel resonant circuit. The coil voltage is rectified on the chip and supplies the circuit.

The writing from transponder to base station (reading the transponder) is done by internally modulating the quality factor of the transponder's parallel resonant circuit. Due to the magnetic coupling of both coils this quality factor change can be seen as voltage variation at the base station antenna coil.

The writing from the base station to the transponder is done by disrupting the carrier signal for a short period of time so that the transponder can "survive" due to its supply voltage capacitor. The disruption must be synchronized with the transponder clock. To achieve this the transponder is modulating the carrier signal with a so called listen window.

3 Internal structure

The EM4150 incorporates a full transponder circuit, except the coil, on a single chip. The two coil terminals are internally connected with a capacitor to achieve a parallel resonant circuit. The alternating voltage over this circuit is rectified by a full wave diode bridge and supplies the rest of the circuit. Another on chip capacitor is used to buffer this supply voltage during the modulation of the carrier frequency.

Two other blocks are using the coil interface as input: The clock extractor is generating the clock for all chip logic out of the 125kHz carrier signal. There is no internal oscillator on the chip, all timings are derived from the alternating voltage at the coil. This makes a larger tolerance for the carrier frequency possible which is usually the case for PLL based reader circuits. As there is no clock during the modulation of the carrier the "off" time of the carrier has to be measured by a monoflop.

The second block is the data extractor where the modulation of the carrier is compared and digitized. This data extractor is feeding the command decoder (during the first bit of the message) as well as the E²PROM depending on the sent command.

A block which is using the coil interface as output is the modulator which modulates the quality factor of the resonant circuit by clipping the coil voltage. This modulator is fed by the encoder which translates the serial NRZ data from the E²PROM into Manchester coded data.

The power control block supervises the supply voltage and generates a power on reset for a rising slope of the supply voltage. Furthermore it inhibits the writing E²PROM access below a certain voltage to avoid corrupted data.

The control logic finally is the central state machine for all logic operations of the transponder chip.

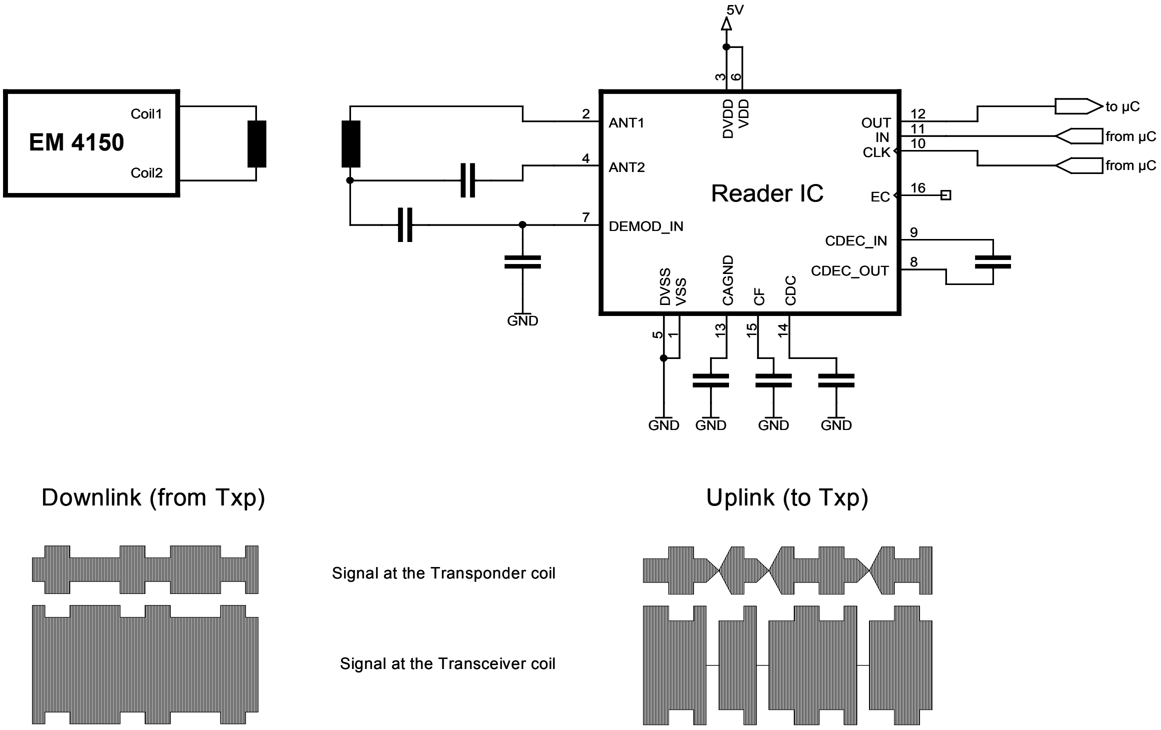


Figure 1: General system principle

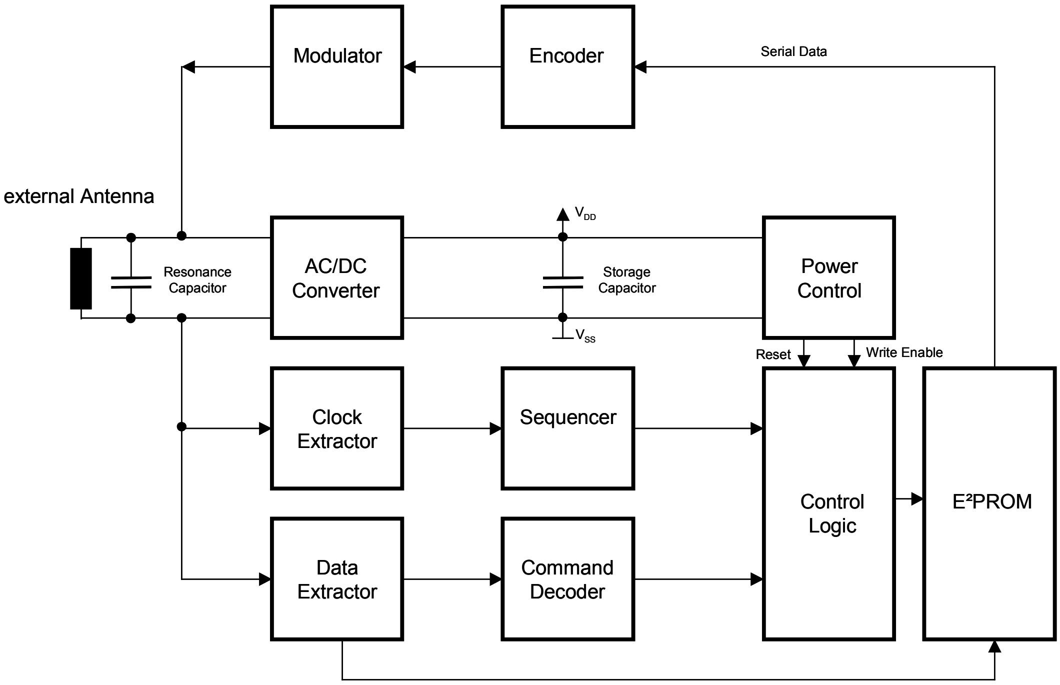


Figure 2: Bloc schematic

3.1 *Memory organization*

The memory of the EM4150 is organized in 32 bit double words.

Starting with word 0 the first three double words have a special function. The first double word is the password which can not be read but written. It is needed to login to the chip and perform certain protected functions.

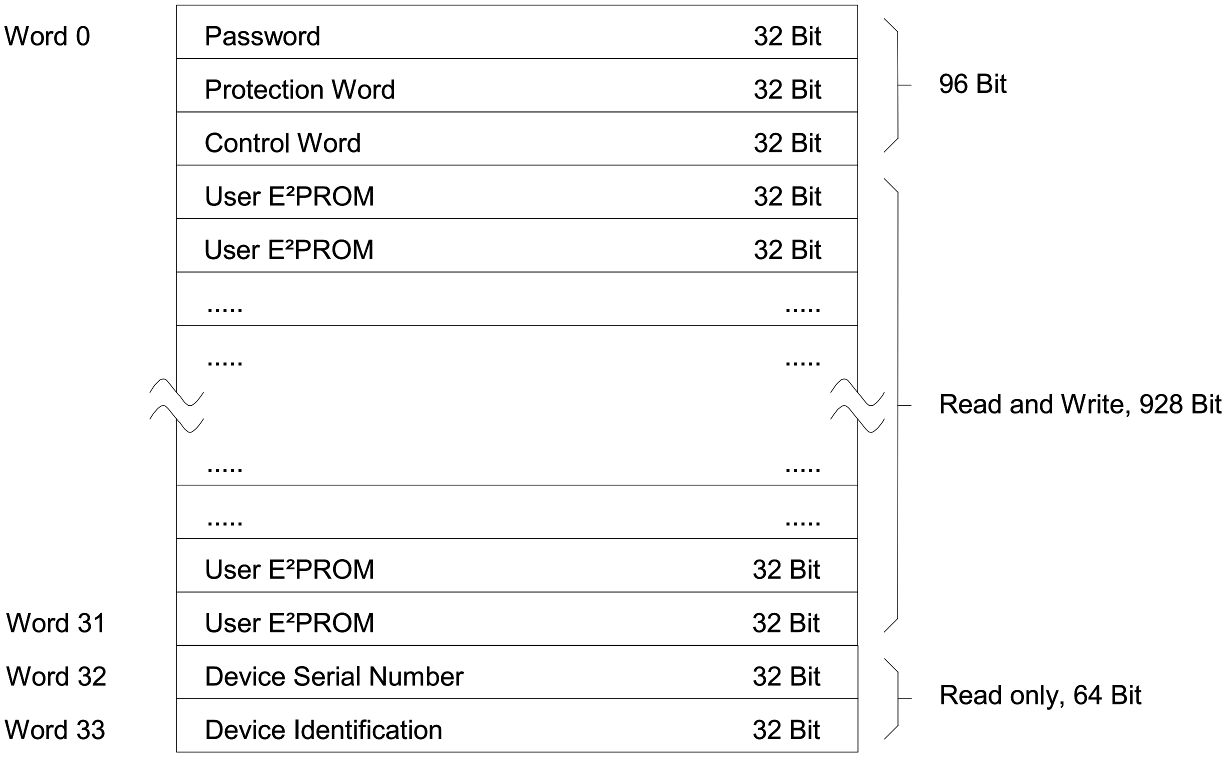
The protection word is the next double word and it contains the addresses of the first and last double word of protected or inhibited memory. By pointing on the first and last double word of a memory area this memory in between can be read protected. The same can be done with a second memory block which is write inhibited.

The third double word is called control word and it controls the behavior of the chip after the power on reset is released. Between listen windows a memory area is continuously transmitted whose first and last memory address is determined by the control word. Furthermore the password function and the read-after-write functionality is controlled by this word.

The following 29 double words are called user memory and can be used to store any data. It can be protected against unintentional reading writing or both.

The last two double words are laser programmed ROM, they are factory programmed and can not be written. They contain the serial number and the device identification.

All in all the EM4150 contains 1088 bit of memory. 928 bit of it can be used to store any data.



Word 0	Password	32 Bit	96 Bit
	Protection Word	32 Bit	
	Control Word	32 Bit	
	User E^{2}PROM	32 Bit	Read and Write, 928 Bit
	User E^{2}PROM	32 Bit	
	.....	.....	
	.....	.....	
	.....	.....	
	.....	.....	
	User E^{2}PROM	32 Bit	
Word 31	User E^{2}PROM	32 Bit	
Word 32	Device Serial Number	32 Bit	Read only, 64 Bit
Word 33	Device Identification	32 Bit	

Figure 3 : Memory organization

4 Mode of operation

After entering a magnetic field of sufficient strength and the internal power on reset is released the chip enters the standard read mode. During this mode a memory area defined by the control word is transmitted continuously. Each double word is separated by a single listen window, the first word (the start of the block) is headed by a double listen window.

This sequence can be interrupted during every listen window by switching into the receive mode.

As every transmitted double word from the transponder memory is separated by at least a single listen window the transponder can be switched to read mode every 11.5ms if the opt32 is chosen.

If the receive mode is not used and the first word read (FWR) and the last word read (LWR) are set appropriate the transponder behaves like a read only transponder with the exception that listen windows are transmitted between the data words.

It can be seen that every command and the power up reset leads back to the standard read mode. This is also true for misunderstood, corrupted or wrong commands.

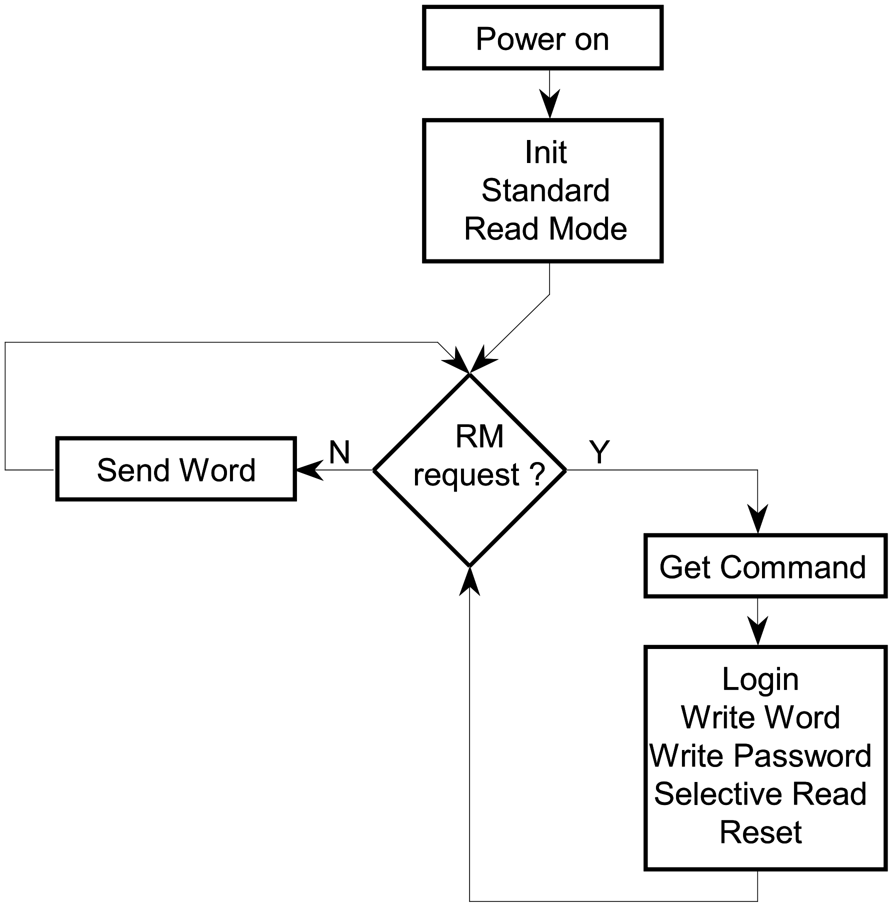


Figure 4: Mode of operation

4.1 *Timing*

The timings below are calculated with the opt32 option, which is 32 clocks per bit or 256µs at 125kHz.

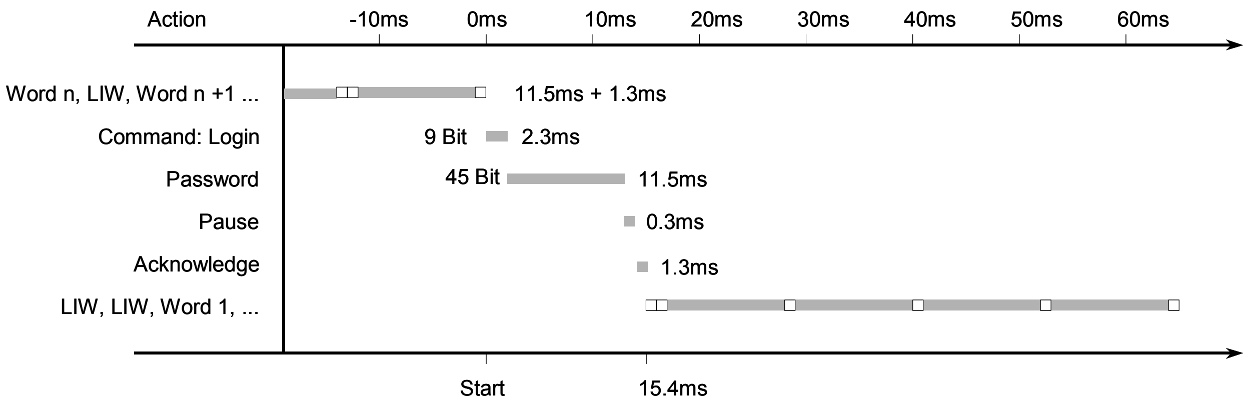


Figure 5: ***Login timing***

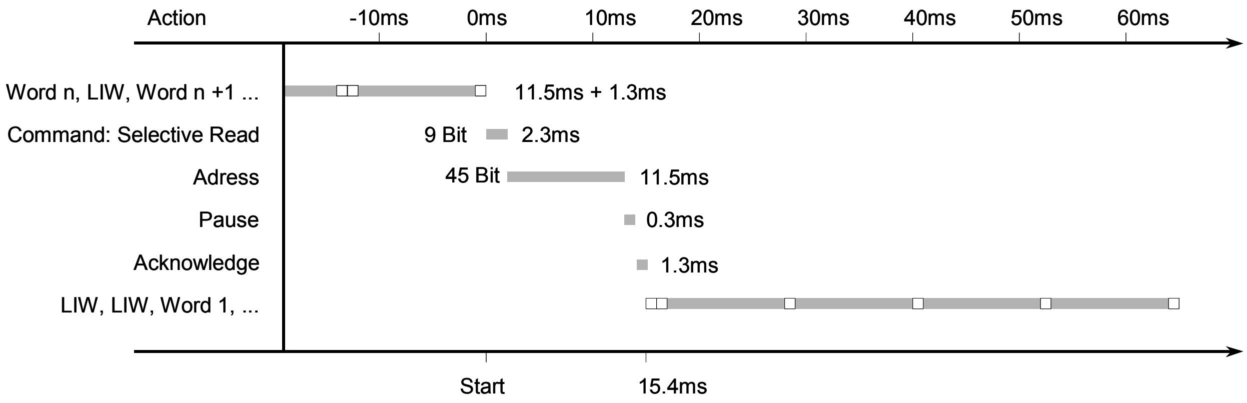


Figure 6: ***Selective Read timing***

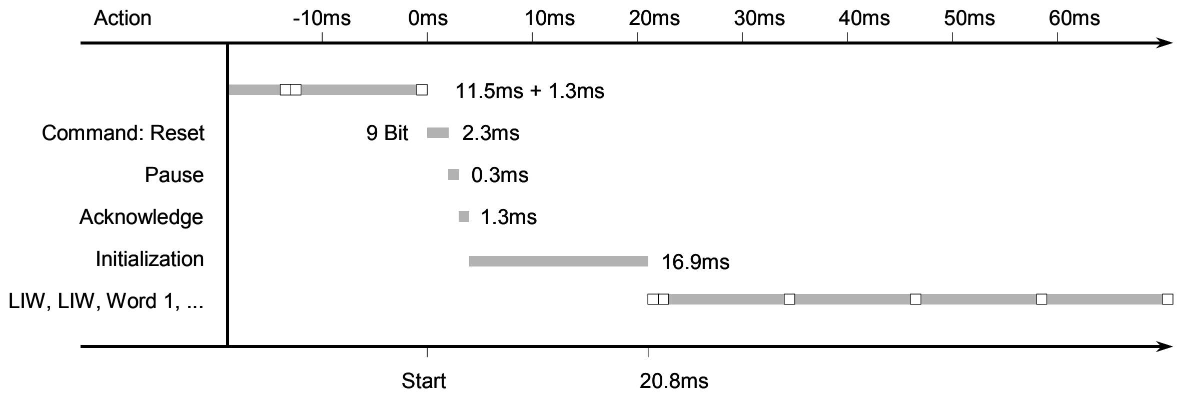


Figure 7: ***Reset timing***

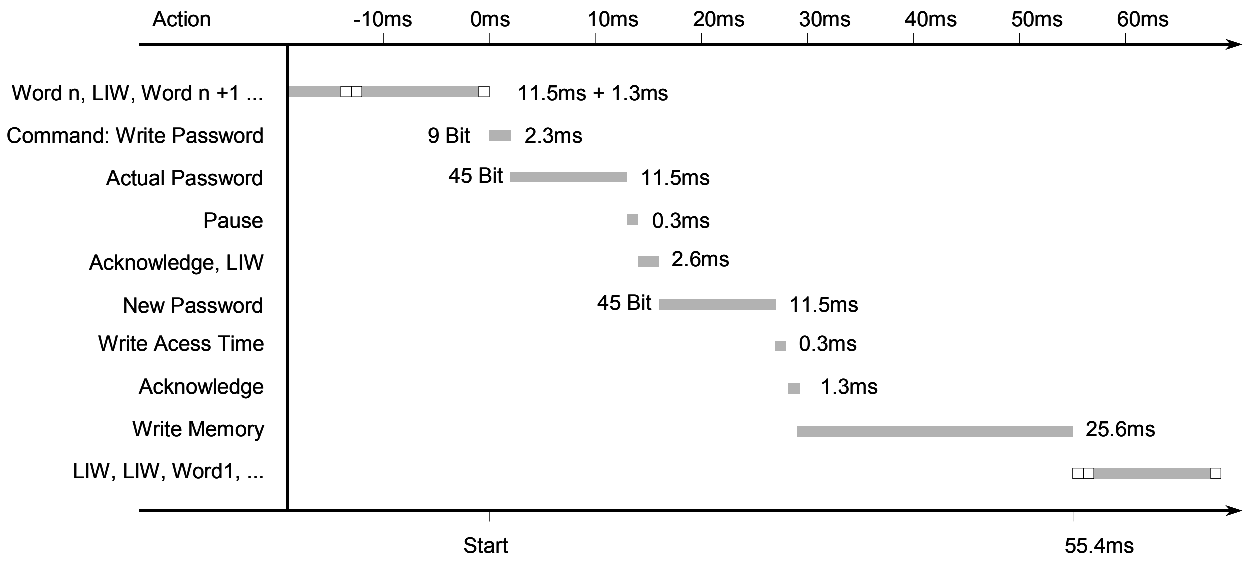


Figure 8: ***Write Password timing***

It should be noted that for the Login, Selective read and Write password command there is a very short time between the last possible modulation of the carrier signal (data sent to the transponder) and the ACK or NAK answer from the transponder. This requires a base station reader which is able to demodulate the carrier signal already 500µs after a modulation (carrier signal switched off).

If this is not feasible the software has to check the success of an operation by reading back the modified memory content. For the Selective read command this verification is more difficult as it is not clear if the transponder is sending the original or the requested data.

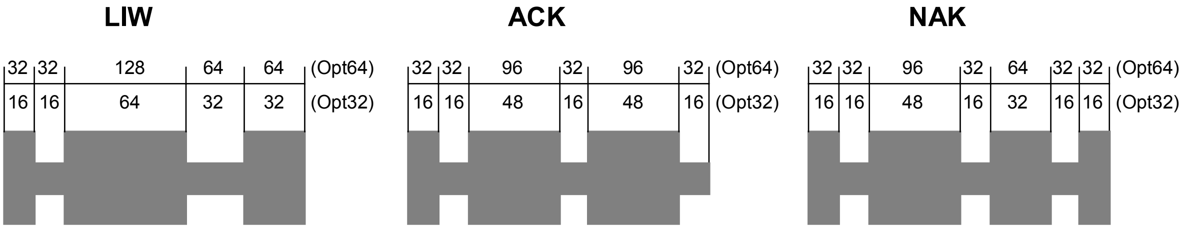
5 Communication details

The transponder can process several commands to access the internal memory and all functions. The communication structure for every available transponder command is identical. It starts with a status feedback sent by the transponder.

5.1 Status information

The status information consist of patterns which are sent by the transponder to show its internal status or the result of an operation. These patterns are designed to be different from any data bit sequence and can therefore not be confused with data sent by the transponder.

- **LIW**: Listen Window - Standard Read Mode / Ready to receive a new command
- **ACK**: Acknowledge - Operation completed successfully
- **NAK**: Not Acknowledge - Any error occurred


LIW
32 32 128 64 64 (Opt64)
16 16 64 32 32 (Opt32)
ACK
32 32 96 32 96 32 (Opt64)
16 16 48 16 48 16 (Opt32)
NAK
32 32 96 32 64 32 32 (Opt64)
16 16 48 16 32 16 16 (Opt32)

All numbers represent number of periods of RF field

(Opt64 is the chip option with a bit period corresponding to 64 periods of the RF field)
(Opt32 is the chip option with a bit period corresponding to 32 periods of the RF field)

Figure 9: Status information patterns

5.2 *Standard Read Mode*

In Standard Read Mode the EM4150 continuously sends Listen Windows alternating with the words of a user defined memory area set in the Control Word. Each First Word Read of this area is preceded by two Listen Windows, the other words are preceded by one Listen Window. All Listen Windows allow the transponder to receive commands from the base station.

The transponder switches to Standard Read Mode when it enters a carrier field (forced by the Power On Reset) or when any command operation is finished.

5.3 *Receive Mode*

In Receive Mode the base station sends at least a 9 bit command to the transponder.

To switch from Standard Read Mode to Receive Mode the base station sends two bit “0” (RM pattern) to the transponder.

The beginning of the first bit “0” must be placed within the 32 (Opt64: 64) clocks of the modulated phase in a Listen Window. The transponder stops sending Listen Windows. The second bit ”0” turns to Receive Mode.

The base station continues by sending the 9 bit command and data bits (depending on the command).

5.4 *Command Set*

Command	Pattern
Login	0 0 0 0 0 0 0 1 1
Write Password	0 0 0 1 0 0 0 1 0
Write Word	0 0 0 1 0 0 1 0 0
Selective Read Mode	0 0 0 0 1 0 1 0 0
Reset	1 0 0 0 0 0 0 0 1

The leftmost bit is the first received bit and the rightmost one is the parity bit.

Reading a valid command (plus data bits respectively), the transponder sends back data or starts an internal write process depending on the command.

An invalid command changes back to Standard Read Mode.

6 Software implementation

Corresponding to the different modes explained above the following structures for the software implementation can be used.

For reading transponder signals the used µController should be able to measure pulse widths and pulse periods and to switch to the inverted measuring edge (falling / falling ↔ rising / rising) while reading.

It is recommended to use an Input Capture Timer with a minimum resolution of 5 µs (better 0,5 - 2 µs) to determine the pulse lengths. The timer shall be able to measure up to 848µs (96 + 10 periods) (Opt64: 1616µs (192 + 10 periods)) corresponding to 3 bit periods for a 125kHz fixed frequency system as described below.

Please note that the reading software algorithms (LIW, Data) must be able to handle non-inverted and inverted signals from the reader demodulator output.

For sending bits to the transponder the µController should generate a fixed time cycle synchronized to the EM4150 uplink data rate. A timer in Compare / Timer Mode is recommended.

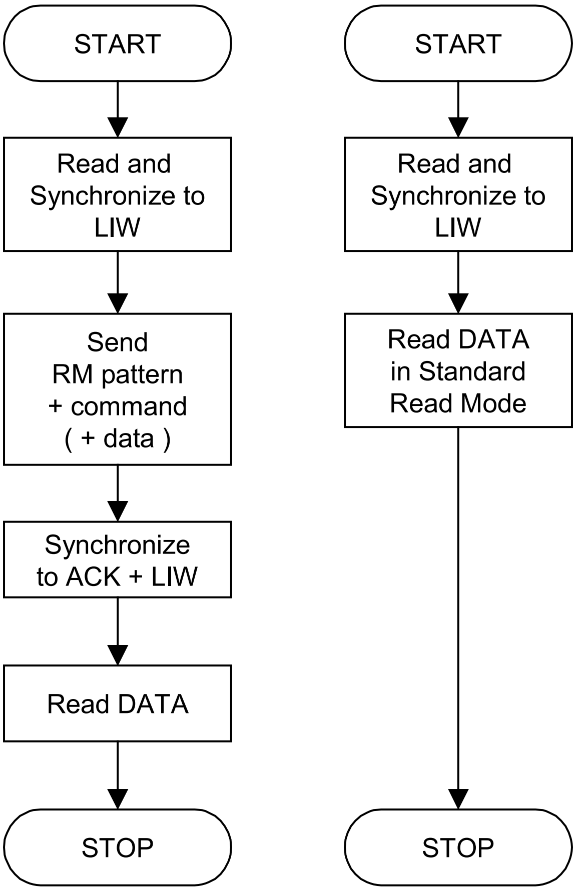

START
Read and Synchronize to LIW
Send RM pattern + command (+ data)
Synchronize to ACK + LIW
Read DATA
STOP
START
Read and Synchronize to LIW
Read DATA in Standard Read Mode
STOP

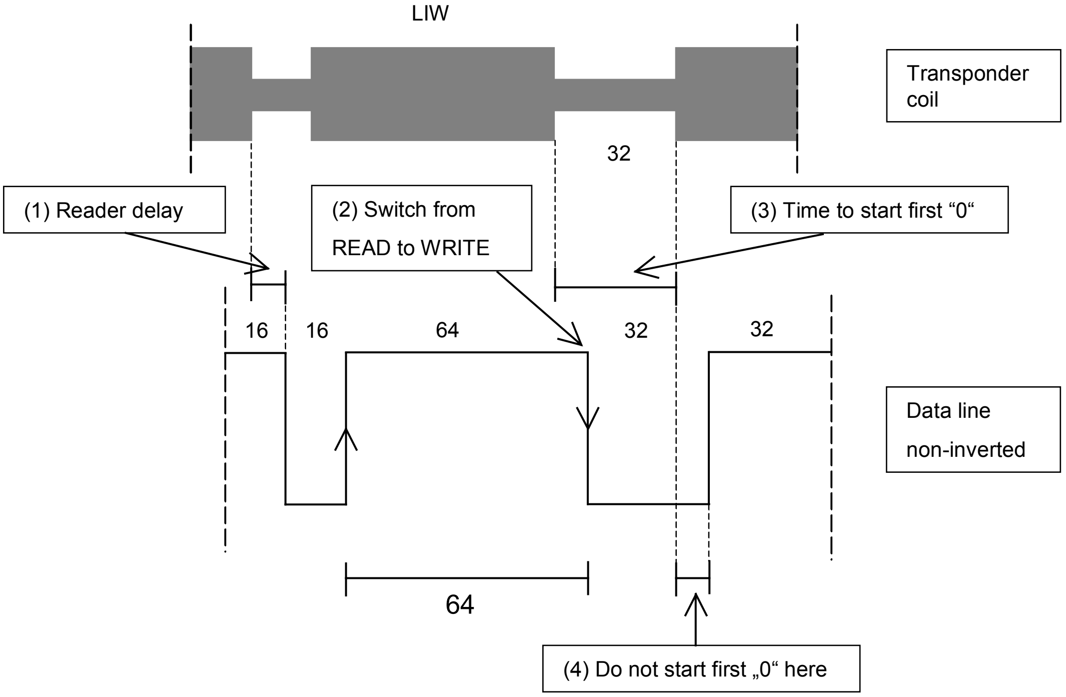
Figure 10: Software structure

6.1 *Reading Listen Windows*

The first step is to synchronize transponder and reader by reading the Listen Window pattern.

There are several methods to find a LIW on the data line of a receiver and to synchronize to it for sending the first “0”. One possible solution is to read the pulse of 64 ± 10 RF periods (Opt64: 128 ± 10). Due to the fact that only one listen window is sent the requirement for the base station reader is a data delay of maximum 100µs. If the demodulation chain is delaying the data signal longer than this value the modulation point can not be met.

If the used filter characteristics does not allow such short delays the software has to interrupt the carrier field before the falling edge of the 64 cycle pulse. This can be done when the 56th cycle has elapsed and therefore the current pulse could be identified as a 64 cycle pulse (values for Opt32).


LIW
Transponder coil
32
(1) Reader delay
(2) Switch from READ to WRITE
(3) Time to start first "0"
16
16
64
32
32
Data line non-inverted
64
(4) Do not start first „0" here

All numbers represent number of periods of RF field for Opt32

Figure 11: Read Listen Window

6.2 Synchronization to send the first "0"

Concerning (3) and (4) please note that the demodulator normally delays signals (1) on the data line compared to the transmission on the transponder coil. Delay times differ according to the reader IC and the surrounding circuit.

This delay must be taken into account since the modulation for the first "0" must start within the 32 (Opt64: 64) periods of modulated phase of the LIW related to the signal at the transponder coil (3) not to the data line (4).

The delay can be calculated by trying the minimum and maximum working values.

During the software development phase it can be helpful to start the first "0" in the middle (after 16 periods, Opt64: 32) of the required 32 (Opt64: 64) periods modulated phase in the LIW to startup with a tolerant timing.

For the final application the data line delay and starting of first "0" should be checked for all system conditions like temperature, tolerances and occurrence of interrupts etc. to make sure that the modulation for the first "0" starts always within the required range.

After reading the LIW pulse of 64 (Opt64: 128) RF clocks the software switches from Read to Write and can place the first "0" directly. Then a timer with an interval set to half of a bit period (16 RF clocks, Opt64: 32) might be started to send bits to the transponder.

The second step consists of sending RM pattern, command and data (if required) to the transponder.

6.3 Sending data to the transponder

The first bit "0" started in the LIW is the first bit of a data stream sent to the transponder depending on the operated command. The data bits are sent in the way shown in figure 12 below.

One bit period corresponds to 32 (Opt64: 64) RF periods.

During the first half of a bit period the transponder modulates the RF field and the base station sends the bit value "0" (Modulation ON = RF field OFF) or "1" (Modulation OFF = RF field ON).

When writing a bit "0" it is recommended not to modulate RF periods 1 – 4 (Opt64: 1 – 7) of this bit period and then turn ON modulation for RF periods 5 – 16 (Opt64: 8 – 32) with a minimum duration of 80µs (Opt64:160µs).

In general all transponder timings are related to the RF field considering that the transponder generates its internal clock from the RF field period. Turning modulation ON stops the RF field and the internal clock so the absolute value of 80µs (Opt64: 160µs) for the minimum modulation time is derived by an transponder internal monoflop.

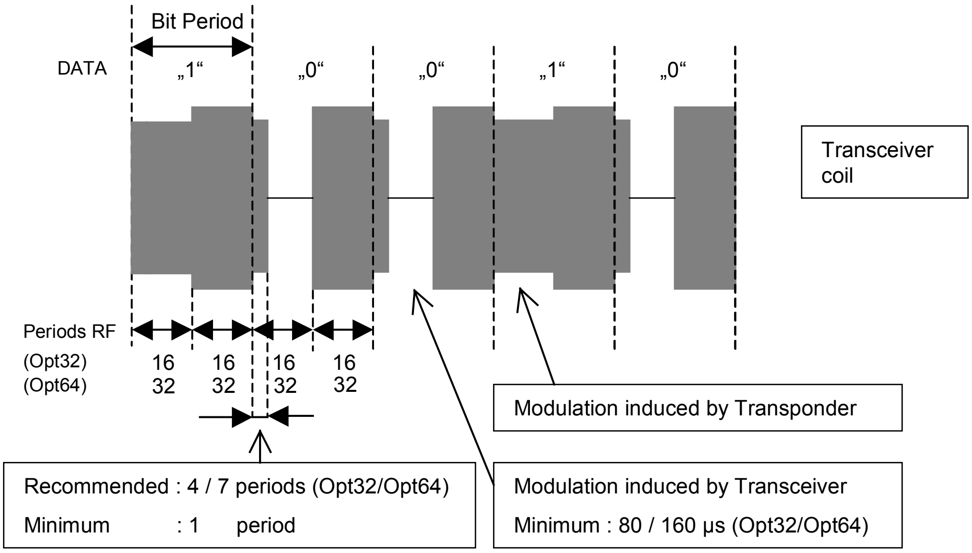

Bit Period
DATA
„1“
„0“
„0“
„1“
„0“
Transceiver coil
Periods RF
(Opt32)
(Opt64)
16
32
16
32
16
32
16
32
Modulation induced by Transponder
Recommended : 4 / 7 periods (Opt32/Opt64)
Minimum : 1 period
Modulation induced by Transceiver
Minimum : 80 / 160 µs (Opt32/Opt64)

Figure 12: Sending data

Turning OFF the modulation for the second half of the bit period the transponder starts counting clocks and therefore resynchronizes to the base station.

Bit streams without “0” can desynchronize transponder and base station because of different time bases in the µController and the transponder. The longest bit stream without forced “0”s is the Write Word command. The maximum possible desynchronization which occurs should be calculated to achieve reliable operation for all commands.

All data sent to the transponder are filled with parity bits every 8 bits. The worst case row of consecutive “1” in the data stream can therefore be maximum 8 Bit long. This is largely defusing the problem.

Anyway desynchronization errors are dependent from the transmitted numbers and they are causing an unstable behavior which is hard to debug. They should be eliminated upfront.

There are different possibilities to stay synchronized anyway:

- The reader carrier frequency is derived from the µController clock or vice versa. This may save a resonator or crystal but causes a high frequency signal to be routed over the printed circuit board. Some semiconductor manufactures do not allow to fetch signals from the oscillator circuit.
- The carrier frequency is captured by a timer and multiples of this value are used to determine the correct modulation moment. The resolution of this timer needs to be high enough because errors are accumulating. This mode is recommended for PLL systems.
- The timer is using the carrier frequency as clock and the timing is therefore derived from the carrier clock. The transponder is doing the same and therefore the synchronization is maintained. This mode can also be recommended for PLL systems. The requirements for the timer are relieved in comparison to the mode above.

The second half of the bit period is used by the transponder to recharge its internal supply therefore the carrier field has be switched on. One practicable software algorithm for sending bits to the transponder is to set a Timer to the regular interval of half a bit period:

1. Half : Next bit “0” = Modulation ON
   “1” = Modulation OFF
2. Half : Always Modulation OFF

When sending a “0” the recommended 4 (Opt64: 7) periods without modulation can be generated by program run time, for example the first instructions in an interrupt service routine.

6.4 Synchronizing to the ACK

After reception of a valid command bit sequence the transponder sends back an ACK and two Listen Windows followed by the requested data bits in Manchester code.

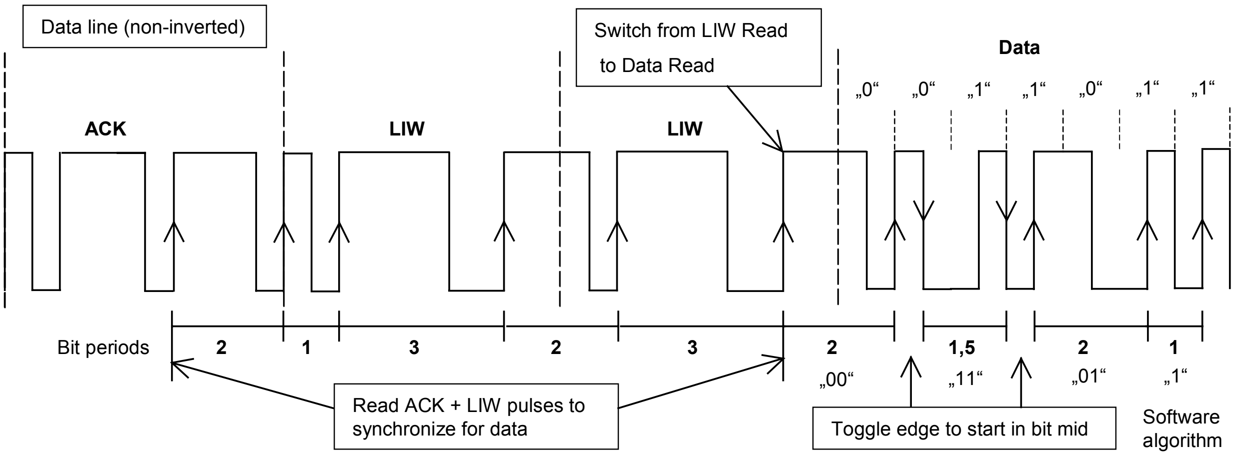


Figure 13: ACK / LIW synchronization and reading data

After sending the last bit to the transponder the software should switch the reader from Write to Read Mode if necessary. During Processing Pause Time (t_{pp}) when the reader is settling and the data line is unstable the software should not start the read timer. It is useful to run the Write Timer some further cycles with RF field ON until data are stable. Then the synchronization algorithm can be started.

Please note for the Write commands (Write 1 word, Write Password) additionally the specified Write Access Time (t_{wa}) and EEPROM Write Time (t_{wee}) including one further ACK.

For Reset command please note the Initialization Time (t_{init}) between ACK and the first LIW. The values for the times mentioned above can be found in the EM4150 data sheet.

The synchronization algorithm reads the pulses (in bit periods) in the following order from rising to rising edge for non-inverted data line: 2 → 1 → 3 → 2 → 3.

The recommended pulse tolerance for this algorithm is about ± 10 RF periods.

On any error concerning this order, for example the transponder sends a NAK, the software can abort the operation.

On completion of the synchronization algorithm the software starts reading data bits with the last rising edge of the second LIW (non-inverted data line). Before switching to the data read algorithm explained below, the first pulse which contains the first one or two data bits must be analysed. Three different pulse lengths can occur:

Measured pulse length	Length limits	Decoded bits with rising edge	Further Action
1.5	5/4 < 7/4	"1"	continue
2	7/4 < 9/4	"00"	toggle edge type
2.5	9/4 < 11/4	"01"	continue

After interpreting this pulse the actual data read algorithm is started.

6.5 Reading data from the transponder

Data can be decoded by reading pulse periods always beginning in the middle of a bit period. One practicable algorithm for the non-inverted data line is described here:

Measured pulse length	Length limits	Decoded bits with falling edge	Decoded bits with rising edge	Further Action
1	3/4 < 5/4	"0"	"1"	continue
1.5	5/4 < 7/4	"11"	"00"	toggle edge type
2	7/4 < 9/4	"10"	"01"	continue

Pulse tolerances can be set to a bit period divided by 4. Between the highest and lowest allowed pulse length no pulses should be excluded.

If the expected number of bits are read the algorithm is stopped.

For inverted data line the same algorithm can be used, only the reading edges must be inverted.

Algorithms reading pulse width will work as well but may have an increased interrupt load and a higher susceptibility for jittering signals.

7 Appendix

For further information see also:

Datasheet
EM4095 Read/Write analog front end for 125kHz RFID Basestation
EM Microelectronic-Marin SA, Marin, 2000

Datasheet
EM4150 1kBit Read/Write Contactless Identification Device
EM Microelectronic-Marin SA, Marin, 2000

EM Microelectronic-Marin SA cannot assume responsibility for use of any circuitry described other than circuitry entirely embodied in an EM Microelectronic-Marin SA product. EM Microelectronic-Marin SA reserves the right to change the circuitry and specifications without notice at any time. You are strongly urged to ensure that the information given has not been superseded by a more up-to-date version.