DATA SHEET

HT RM801 Family

HITAG™ Long Range Reader Module Hardware

Product Specification
Revision 1.0

October 2003

Frosch Electronics

Table of Contents

Definitions

Data sheet status	
Objective specification	This data sheet contains target or goal specifications for product development.
Preliminary specification	This data sheet contains preliminary data; supplementary data may be published later.
Product specification	This data sheet contains final product specifications.
Limiting values	
Limiting values given are in accordance with the Absolute Maximum Rating System (IEC 134). Stress above one or more of the limiting values may cause permanent damage to the device. These are stress ratings only and operation of the device at these or at any other conditions above those given in the Characteristics section of the specification is not implied. Exposure to limiting values for extended periods may affect device reliability.	
Application information	
Where application information is given, it is advisory and does not form part of the specification.	

Life support applications

These products are not designed for use in life support appliances, devices, or systems where malfunction of these products can reasonably be expected to result in personal injury. Customers of Frosch Electronics OEG using or selling these products for use in such applications do so on their own risk and agree to fully indemnify Frosch Electronics OEG for any damages resulting from such improper use or sale.

1 Introduction

hitag™ - is the name of one of the universal and powerful product lines of our 125 kHz family. The contactless read/write system that works with passive transponders is suitable for various applications. Inductive coupling helps you to achieve operating ranges up to 1000 mm and the use of cryptography guarantees highest data security.

Anticollision Mode, which is used only in long range operation, allows you to handle several transponders that are within the communication field of the antenna at the same time, thus achieving highest operating security and permitting to handle several data transfers quickly and simultaneously. In this context anticollision becomes an essential element of applications such as ski-ticketing and long range access control. With applications of that type it will always happen that several transponders arrive in the communication field of the antenna at the same time.

Nevertheless, the proximity application also prevents any type of malfunction even if several transponders arrive in the communication field of the antenna at the same time.

The HITAG product family is used both in the proximity area (operating range up to about 200 mm) and in the long range area (operating range up to about 1000 mm). In both cases the HITAG Core Module forms the central part.

The most outstanding features of the HITAG Long Range Reader Module are:

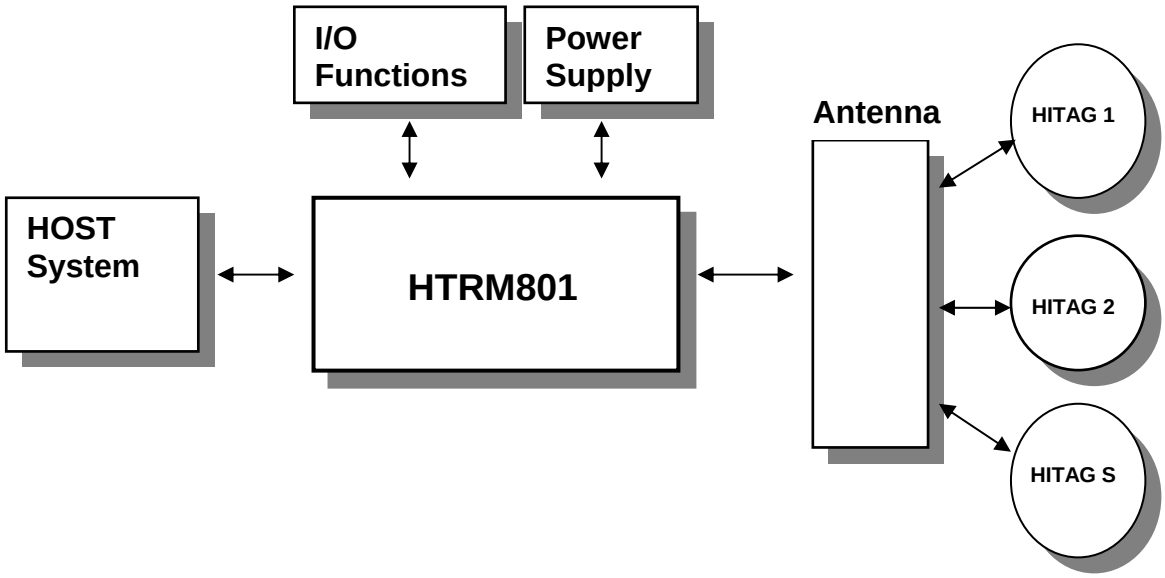
- easy integration
- high noise immunity
- small size
- uncomplicated interfaces
- very powerful RF-part

The following paper describes the reader hardware, interfaces and connection of the antenna.

.

2 System Overview

The following drawing shows the HITAG Long Range Reader Module as part of a complete Radio Frequency Identification (RFID) system.



2.1 Transponders

The HITAG Reader Module can communicate with transponders based on Philips HITAG 1, HITAG 2 and HITAG S .

2.2 Host

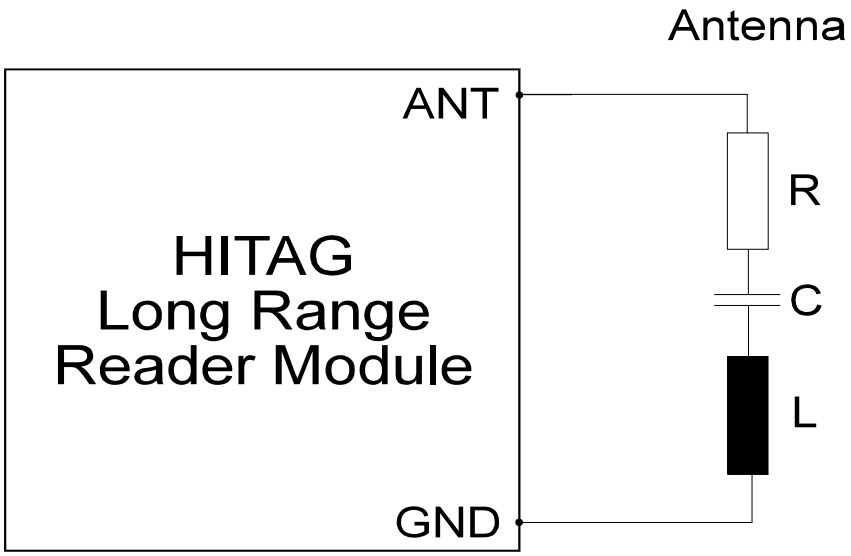
The connection to the host (e.g.: μC or PC) is a serial interface on RS232 level (version HT RM801/AED) for data transmission. Optionally wired interface drivers for CMOS (version HT RM801/EED) and RS485 (version HT RM801/CED) are integrated on the Reader Module.

2.3 I/O - Functions

One line of the HITAG Reader Module is wired as input from e.g. switches, one as output to drive a LED.

2.4 Connecting the Antenna

The antenna has to be mounted in the following way:



C is used for tuning the antenna. For more detailed information please see Chapter 6.1 (Building HITAG Long Range Antennas).

2.5 Behaviour with Several Transponders

If several HITAG 1 or HITAG S transponders arrive *simultaneously* within the communication field of the antenna of a HITAG Long Range Reader Module, all the HITAG transponders (theoretically up to 2^{32}) within the communication field of the antenna can be read and written simultaneously. Because of the mutual influence of the transponder coils - they detune each other if there are too many too close to each other - the number of the transponders that can be operated simultaneously is limited.

If several HITAG 2 transponders arrive *simultaneously* within the communication field of the antenna of a HITAG Long Range Reader Module, the „stronger“ transponder (the nearer one) takes over or - under special circumstances - no communication takes place. If the transponders arrive in the field one after the other, communication is established with the first one, all the other transponders are ignored. This ensures that no two (or several) HITAG 2 transponders will ever be processed (above all written to!) accidentally at the same time. By muting a selected HITAG 2 transponder (HALT Mode) another HITAG 2 transponder that is to be found in the communication field of the antenna can be recognized.

3 Specifications

3.1 Electrical Specifications

3.1.1 Power Supply

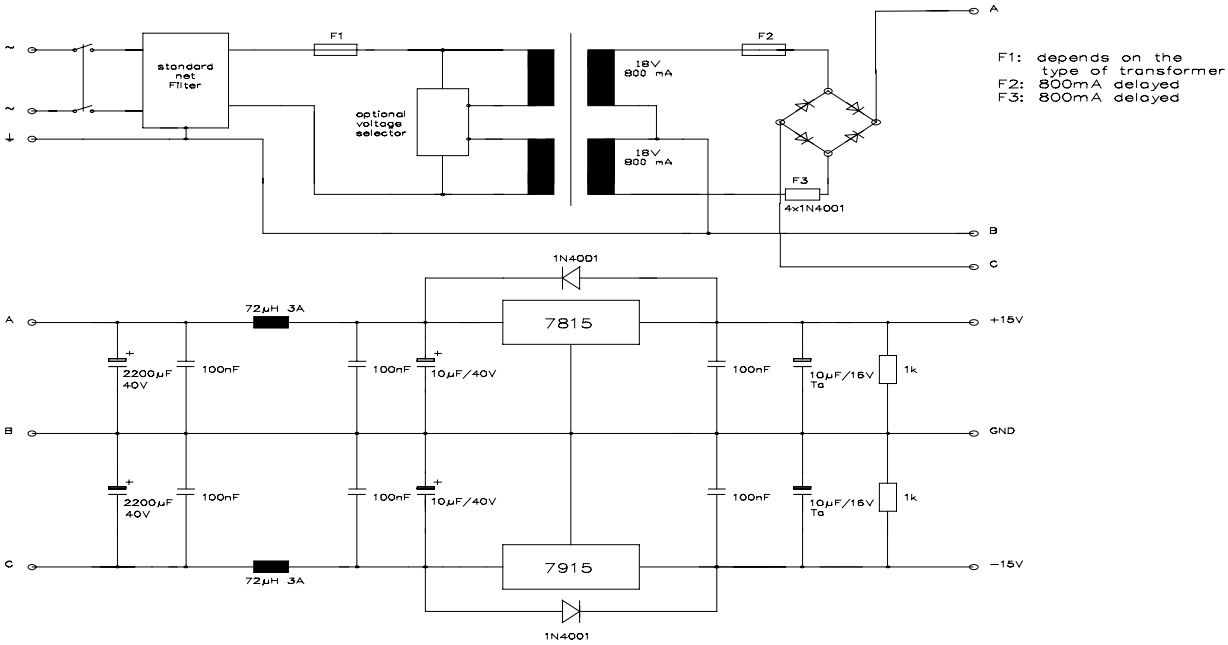
The Reader Module contains some filtering circuits for the power supply. Nevertheless some requirements are to be fulfilled by the power supply. This means the maximum ripple of the supply voltages (± 15V) must not exceed the values listed in the following table.

frequency of the ripple f [kHz]	maximum amplitude of the ripple u [mV_{RMS}]
$0 \leq f < 0.5$	48
$0.5 \leq f < 20$	7
$20 \leq f < 120$	36
$120 \leq f < 130$	12
$130 \leq f$	48

3.1.1.1 Current Specification

	I_{typ}	I_{max}	I_{stby}
+ 15V	400 mA	550 mA	200 mA
- 15V	- 300 mA	- 400 mA	- 100 mA

I_{typ} ... typical current
I_{max} ... maximum current
I_{stby} ... typical standby current



Instead of a transformer type supply unit (see above), a switching frequency power supply unit can be used alternatively. The switching frequency must be in the range of:
165 kHz < f_{switch} < 210 kHz (over temperature, load and production)

3.1.2 Modulation

3.1.2.1 Reader Module ⇒ Transponder

Type of Modulation	Modulation Ratio
amplitude shift keying (ASK)	100 %

That means the carrier is blanked completely, the information is located in the intervals between the pauses.

3.1.2.2 Transponder ⇒ Reader Module

Type of Modulation	Modulation Ratio
amplitude shift keying (ASK)	depending on the distance between transponder and Reader Module

3.1.3 Interface

An interface driver for RS232 (version HT RM801/AED) is integrated on the HITAG Reader Module.

Optionally drivers are CMOS (version HT RM801/EED) and RS485 (version HT RM801/CED).

3.1.4 Metallic Environment, Interferences and other Readers

The communication range is impaired by metallic environment and electromagnetic interferences (e.g.: monitors, keyboards). Therefore, you should keep a distance of at least the antenna´s diameter to metallic surfaces or loops as well as to electromagnetic interferences. If this is not possible, you have to take preventive measures such as using ferrites or shielding for transponder and antenna. The HITAG Long Range Reader Module is able to suppress up to two harmonic electromagnetic disturbances. In order to be able to operate two systems side by side without negative influence on communication ranges, you must place the antennas at a minimum distance. To keep this distance low, magnetic shielding must be realized. This topic is handled in detail in the Design Instruction: Antenna Design for the HITAG™ Long Range System.

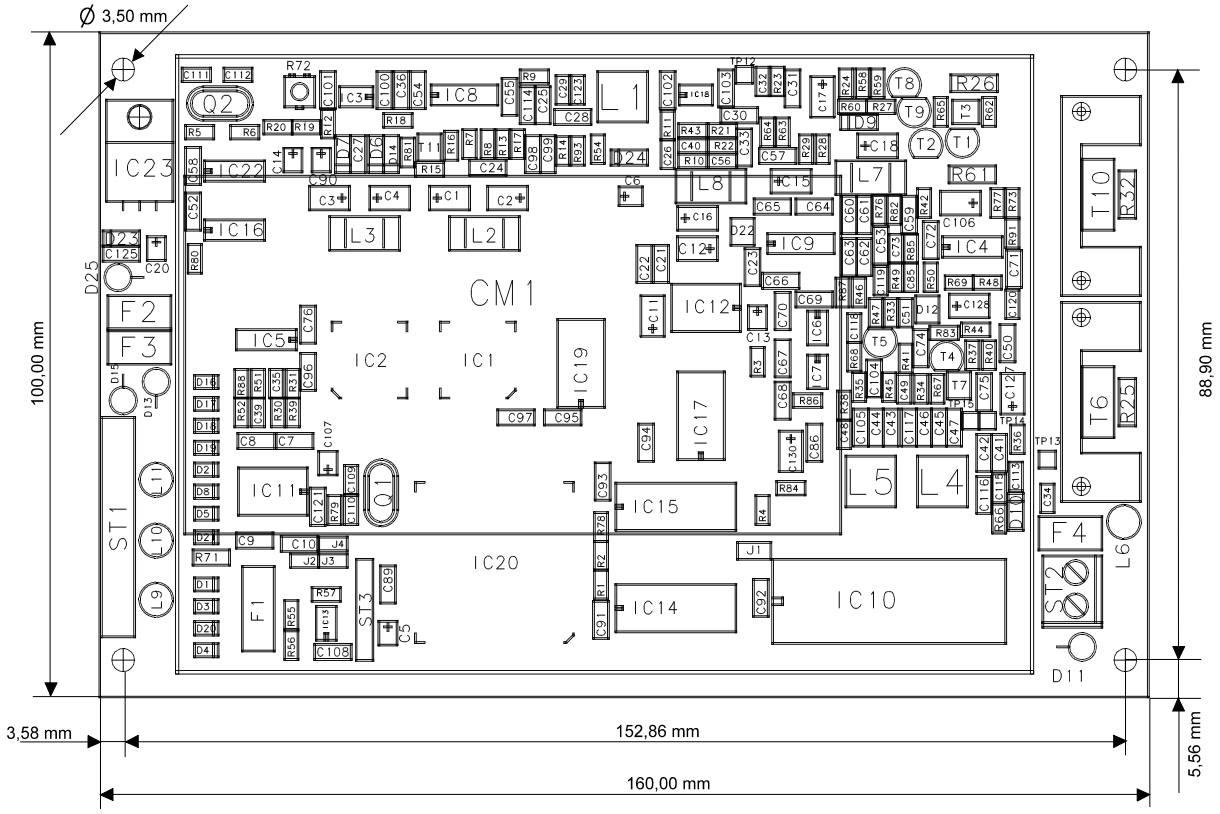
3.1.5 Temperature Range

- -25° C to +70° C (operating)
- -40° C to +85° C (storage)

3.2 Mechanical Specifications

3.2.1 Mechanical Dimensions

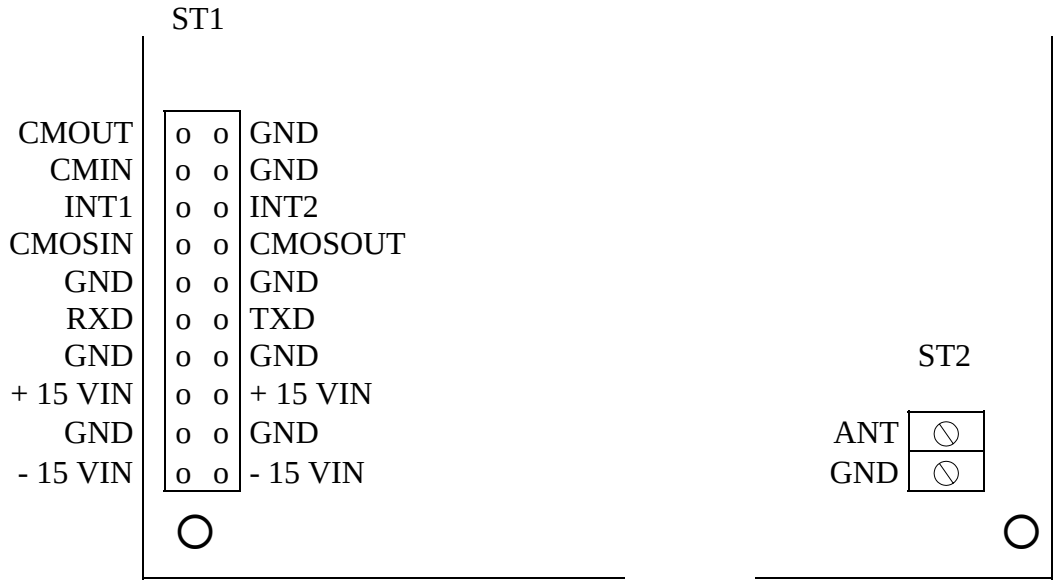
The following drawing (not to scale) shows the outer dimensions of the HITAG Reader Module with the four mounting holes, top view (component side).



The dimensions of the PCB are 160 x 100 mm. The height does not exceed 43 mm.

3.2.2 Pin Assignment

The following drawing (not to scale) shows the pin assignment of the HITAG Long Range Reader Module (top view).



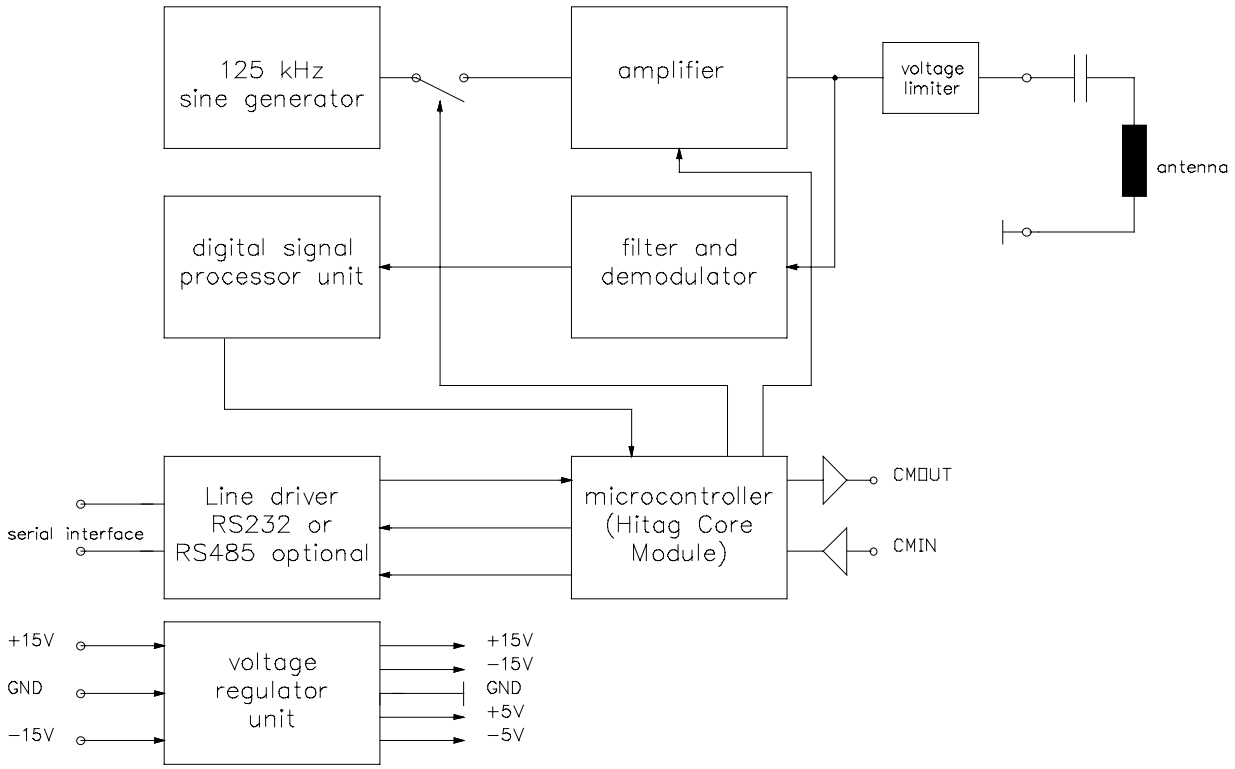
In the lower left corner of the PCB a connector is fixed (ST1) for connecting the power supply, the serial interface and the general purpose input pins.
ST2 in the lower right corner of the PCB is used to connect the antenna.

Pindescription:

Pin	Type	Description	Commend
+15VIN -15VIN GND	PWR PWR PWR	power supply	
RXD TXD	IN OUT	serial interface RS232 standard	mounting option as per agreement
INT1 INT2	IN/OUT IN/OUT	serial interface RS485 standard	
CMOSIN CMOSOUT	IN OUT	CMOS interface	
CMIN	IN	pins for general purpose	
CMOUT	OUT		
ANT	OUT	pins for connection of the antenna	
GND	OUT		

4 Description of the Reader Module Functions

4.1 Block Diagram



4.1.1 Sine Generator, Amplifier and Voltage Limiter

For transmitting power and data to the transponder a sine signal is switched by the microcontroller and amplified. The amplifier is designed as a current source. A voltage limiter is used to clamp the output voltage of the amplifier during the decay and transient phases of the sine signal.

4.1.2 Microcontroller

The microcontroller (placed in the Hitag Core Module) processes the protocol for the communication between the transponders and the read/write unit. The interface signals are converted so that the transponders are able to process them and the outgoing signals from the transponders are converted into interface-compatible signals.

The second essential microcontroller function is its control function. The microcontroller activates and deactivates the transmitter and switches the receiver between the modes for the different transponders reception.

Additional functions of the microcontroller are controlling the standby mode of the amplifier, detection of detuned or broken antennas (antenna malfunction) and controlling of the input and output for general purpose.

4.1.3 Interface: Microcontroller - HOST

The device communicates with the host (processor, PC, ...) via a serial interface using a baud rate of 9600 baud initially after a Power On, changes can be done by serial interface (up to 57600). Data transfer details are: 1 start bit, 8 data bits, 1 stop bit and no parity bit, the Least Significant Bit is sent first.

An RS232 interface device is connected to the reader module. Optionally a CMOS or an RS485 device is possible.

4.1.4 Receiver

After filtering and demodulation of the amplitude modulated signal received from the transponder the received data are converted and passed to the digital signal processing unit (DSP) for further processing.

4.1.5 Digital Signal Processing Unit (DSP)

The receiving part of the reader module includes bandpass filters which attenuate disturbances (3dB attenuation at 105 kHz and 145 kHz). For disturber frequencies near the 125 kHz (e.g. harmonics of the line frequency of PC monitors, long wave transmitters) a fourier transformation is used to recognize harmonic disturbers and to eliminate their influence. The DSP is also responsible for separating the responses of different transponders during anticollison cycles (multiple transponder operation).

4.1.6 Voltage Regulator Unit

The voltage regulator unit supplies after filtering all parts of the reader module with the required voltages.

4.1.7 Antenna

To the design of HITAG Long Range Antennas see Chapter 6.1.

4.2 Standby Mode

The HITAG Long Range Reader Module offers a software controlled standby mode. This mode can be activated and deactivated by the host system via serial interface. During the standby mode the amplifier of the reader module is turned off and the power consumption decreases drastically.

5 Postal Approval and Disturbers

5.1 Postal Approval

The postal approval can only be granted for final products, not just for components like the HITAG Reader Module. But the reader module is designed in a way that it is possible to get the postal approval for a device including the HITAG Reader Module.

Electromagnetic emissions comply with the guidelines in FTZ 17 TR 2100, ETS 300 330 and ETS 300 683, electromagnetic immunity complies with the guidelines in ETS 300 683.

EMC, EMI Standards

The following configuration is in compliance with the European Telecommunication Standards:

- HITAG Long Range Reader Module
- Power supply according to the recommendations in chapter 3.1.1 (transformer)
- Antenna :50 x 70 cm, number of turns N=26, inductivity L=1.2 mH

The following measurements have been passed:

EMI: ETS 300330, September 1994 (FTZ 17 TR 2100)

RFI-Emissions: Limit class B according to EN 55022, 1987

Immunity: RF Electromagnetic Field according to ENV 50140
80 MHz - 1000 MHz: 3 V/m, AM 80 %, 1 kHz

Electrostatic Discharge according to IEC 801-2, 1991
Contact discharge: 4 kV, air discharge: 8 kV

Electrical Fast Transients (Burst) according to IEC 801-4, 1988
Signal ports: 0.5 kV, DC-power ports: 1 kV, AC-power ports 2 kV

RF Common Mode according to ENV 50141
Current clamp injection 150 kHz - 80 MHz: 3 V rms, AM 80 %, 1 kHz

Voltage Dips and Interruptions according to IEC 1000-4-11
Reduction of 30 % of UN for 10 ms, of 60 % of UN for 100 ms,
voltage interruption for 5000 ms

Surges, Common and Differential Mode according to IEC 1000-4-5
AC-power input ports: 1kV (lines-to-ground), 0.5 V (line-to-line)

Periodic Disturbers

There are a couple of possible sources for disturbances for a 125 kHz system like HITAG. The HITAG Long Range Reader Module is designed to handle this problem and achieve optimal performance under worst conditions.

Long Wave Transmitters, other 125 kHz systems and PC monitors are examples for periodic disturbers which can be relevant for 125 kHz systems. To eliminate these disturbers the digital signal processing unit is used.

After the Start FFT command is sent to the reader module a Fast Fourier Transformation (FFT) is started to locate periodic disturbers. After about 110 ms this calculation is finished and for the following communication between reader module and transponder the located disturbers are eliminated. The command FFT should be executed as often as the application allows.

Note:

- The DSP is able to suppress up to two harmonic electromagnetic disturbances.
- During FFT is running (about 110 ms) communication with a transponder is not possible.

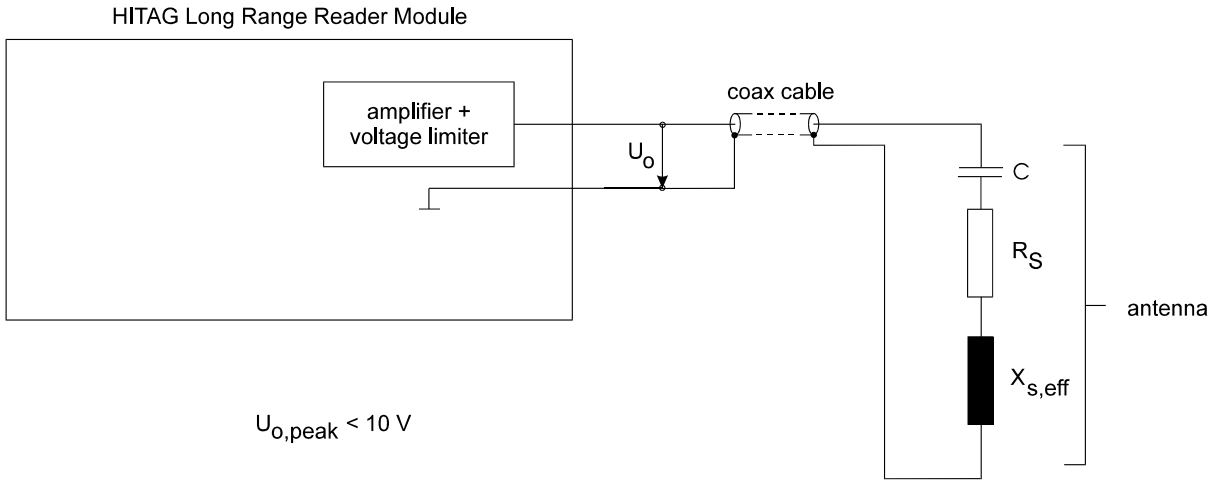
6 Connection of the HITAG Reader Module

In the lower right corner of the PCB of the reader module the connector for the antenna is fixed (ST2).

6.1 Building HITAG Long Range Antennas

The antenna is an important part of the HITAG Long Range System. The antenna must provide energy and data transmission between reader and transponder. Therefore, you should be particularly careful when implementing the antenna in order to achieve optimum results.

6.1.1 Basics



6.1.2 Specifications

30 < Q < 60 .....quality factor;
400 µH < L < 1200 µH.....inductance of the coil;

6.1.3 Recommended Antenna Cable and Length

The length of the antenna cable should be limited with five meters. In case of longer cables a type with low capacitance and resistance must be used. For standard applications a coaxial cable is recommended (50Ω-coaxial cable for standard applications and 75Ω or 95 Ω-coaxial cable for special applications).

6.1.4 Tuning of the Antenna Current

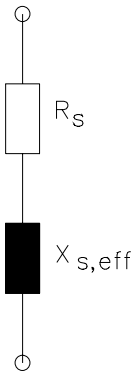
According to the layout diagram of Chapter 3.2 the potentiometer R72 is used to tune the current driven through the antenna. The default setting is 200 mA. It is not customary to change this value. However, if you want to change the current for a special application, please notice that the range for U_0 is

$U_{0peak} < 10$ V

6.1.5 Tuning of the Antenna Phase

The signal from a transponder is delayed by the decay time of the antenna of the reader module. To achieve optimal performance this signal and the digital signal processing unit of the reader module must be synchronous. Thus it is necessary to store a phase information called "Bit Clock Delay" (BCD), which is a function of the quality factor and the inductance (reactance) of the antenna connected to the reader module.

Equivalent circuit of the antenna:



$$Q = \frac{X_{s,eff}}{R_S}$$

R_S ... effective series resistance
$X_{s,eff}$ ... effective series reactance
Q ... quality factor

The default setting is 7 which is suitable in most of the cases. Apart from that, the user is able to change the BCD value. The reader module includes a non volatile memory (EEPROM) to store the bit clock delay. To load the BCD value to the reader module the command SetBCD is used.

HITAG ANTENNA TUNING DEVICE:
Especially for our HITAG product line the HITAG Antenna Tuning Device was designed. This Tuning Device can be used for tuning HITAG Proximity and HITAG Long Range Antennas.

6.1.6 Antenna Malfunction Indication

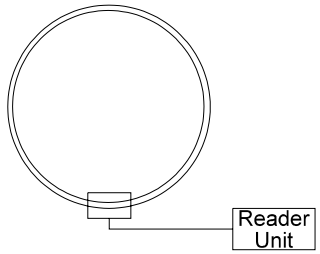
If the antenna is broken or badly detuned, the antenna overload bit is set. This bit can be read by the host system via the serial interface by using the *ReadLRStatus* command.

6.1.7 Additional Notes

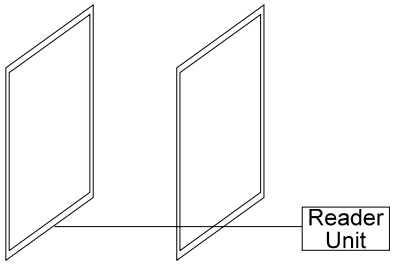
The following list is a summary about HITAG Long Range Antennas, the exact way how to design a HITAG Long Range Antenna is described in the document "**Antenna Design for the HITAG™ Long Range System**".

- Frosch Electronics OEG lays high emphasis on the research of antenna development.
- The choice of various antenna shapes (the electrical parameters) is characteristic to 125 kHz systems.
- The knowledge is transferred to Frosch Electronics OEG customers, in order to enable them to design and build antennas which fit best for the particular applications (antenna trainings).
- Solutions can be found for almost every environmental scene. (Metal, periodic disturbers, special antenna shapes ...).

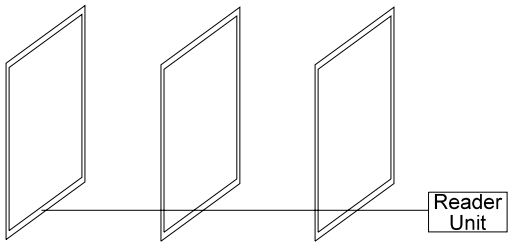
Possible arrangements of antennas:



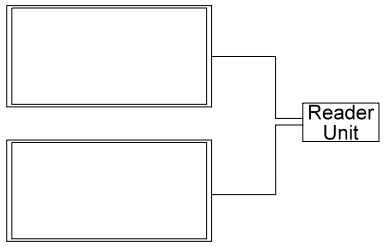
Single Loop Antenna



Gate Antenna



Double Gate Antenna



Antenna Multiplex

The different arrangements are suitable for different applications. So the single loop antenna is used for standard arrangements.

The gate antenna is used for typical access control applications, for access control during passing through the gate.

The double gate antenna is similar to the gate using two rows.

An antenna multiplex system is a cost efficient application, because one reader drives many antennas. The number of multiplexed antennas is only limited by timing restrictions.

By changing the arrangement of the antenna, the total system performance and reliability can be significantly improved. As an example: building gate antennas with opposite magnetic orientation leads to a very reliable system.

6.2 Possible Sources of Errors by Connecting the HITAG Long Range Reader Module

The following error list should be checked if any error (e.g. read/write distances that do not reach the specified values) occurs:

- Power supply cable not mounted correctly.
- Power supply not in the specified range (see 3.1.1)
- Serial interface not connected correctly.
- Interference received by the antenna because of an external noise source (e.g. monitor, keyboards).
  Remedial measure: Removal of the antenna from the interfering area, use the *StartFFT command*.
- Connecting cables of the antenna changed by mistake.
- Antenna is mounted in metal environment.
  Remedial measure: Mount a non-metal space keeper between the antenna and the metal.
- Antenna is not designed following the antenna design instructions.
- Inductance of the antenna is not in the specified range.
- Quality factor of the antenna is not in the specified range.

Command names mentionned in the previous chapters are fully described in the document: „Protokoll HTRM801 V1.x: Interface Protocol Reader - Host“

7 Security Considerations

Developing the HITAG System special consideration was given to aspects of security. The following items represent the fundamental framework of the security concept:

- cryptography
- mutual authentication
- password verification and
- Cyclic Redundancy Check (CRC)

7.1 Operating Security

The following mechanisms ensure the operation security of the HITAG system.

7.1.1 Anticollision Mode

Anticollision Mode in long range applications permits you to process several HITAG 1 transponders simultaneously. Theoretically up to 2^{32} HITAG 1 transponders can be processed simultaneously. In practice this number is limited, because of the mutual influence of the transponders - they detune each other, if there are too many too close to each other.
In long range applications using HITAG 2 transponders, only one transponder is handled even if there are several transponders within the communication field of the antenna. In this case either no communication takes place or the "stronger" or closer transponder takes over. By muting a selected transponder (HALT Mode) another transponder that is to be found in the communication field of the antenna can be recognized.

7.1.2 Monitoring the Supply Voltage of the HITAG Long Range Reader Module

Supply voltage is controlled by a watch dog circuit which triggers a system reset if the supply voltage of the HITAG Core Module drops below 4.75 V or if the microcontroller fails.

7.1.3 Antenna Rupture, Antenna Short Circuit

The HITAG Long Range Reader Module does not get permanently damaged in case of an antenna rupture or a brief antenna short circuit. The detection of detuned or broken antennas (antenna malfunction) is possible.

7.2 Data Privacy

The use of cryptography (Stream Cypher), mutual authentication, and password verification prevents monitoring and copying the data channel. Therefore, the area of the transponder that only can be accessed enciphered is called “secret area“.

To make use of cryptography for HITAG 1 transponders you need keys and logdata.

> **Keys** are used to **initialise the crypto block**
> and **logdata** are used for **mutual authentication**.

To make use of cryptography for HITAG 2 and HITAG S transponders you need a key and passwords.

> The **Key** is used to **initialise the crypto block** using HITAG 2/S in Crypto Mode
> and **passwords** are used for **authentication** for HITAG 2/S in Password Mode.

The transponders and the HITAG Reader Module are provided with identical transport keys and transport logdata so that you can start operating them right away.

The KeyInit Password is set to 0x00000000, HITAG 1 Keys and Logdata are set to 0x00000000, HITAG 2 Key is set to 0x4D494B524F4E, HITAG 2 Password TAG to 0xAA4854 and HITAG 2 Password RWD to 0x4D494B52, HITAG S Key is set to 0x4D494B524F4E, HITAG S Password TAG to 0xCA4854 and HITAG S Password RWD to 0x4D494B52 (*transport* values predifined by Philips on transponder side and by Frosch Electronics OEG on reader side).

In order to offer our OEM clients high flexibility, the configuration of the transponder memory, password, keys and logdata can be changed.
We strictly recommend to rigorously restrict these possibilities for the end customers (by setting the configuration page to read only, setting password, keys and logdata to neither read nor write).

8 Ordering Information

HITAG Long Range Reader Modules:

Type Name	Description	Ordering Number
HT RM801/AED	RS232 Interface	R31002.1
HT RM801/CED	RS485-Interface	R31002.2
HT RM801/EED	CMOS-Interface	R31002.3

INTENIONALLY LEFT BLANK

Frosch Electronics OEG

Customized RFID Solutions

Am Andritzbach 26A/5
8045 Graz
Austria

Münzgrabengürtel 10
8010 Graz
Austria

Tel.: +43 697055/0
Fax: +43 697055/12
mail to: info@froschelectronics.com

www. froschelectronics.com