TCM 515 EnOcean Transceiver Gateway Module

05.02.2019

Observe precautions! Electrostatic sensitive devices!

Patent protected:
WO98/36395, DE 100 25 561, DE 101 50 128,
WO 2004/051591, DE 103 01 678 A1, DE 10309334,
WO 04/109236, WO 05/096482, WO 02/095707,
US 6,747,573, US 7,019,241

DOLPHIN
Self-powered IoT by EnOcean

TCM 515 – ENOCEAN TRANSCEIVER GATEWAY MODULE

REVISION HISTORY

The following major modifications and improvements have been made to this document:

Version	Author	Reviewer	Date	Major Changes
1.0	MKA	MK, CB	12.05.2017	First public release
1.1	MKA	MKA	22.05.2017	Added detailed antenna information
1.2	MKA	MH, MK	22.06.2017	Added receiver class due to RED requirement
1.3	OS	MKA	08.08.2017	Added FCC grant and regulatory information for FCC and ISED; Added maximum input power
1.4	MKA	MKA	31.08.2017	Added Tape & Reel specification
1.5	MKA	MKA	19.09.2017	Added detailed description of filtering functionality
1.6	MKA	MKA	25.10.2017	Added maximum number of filters
1.7	MKA	MKA	10.01.2018	Extensive update for production version. Added detailed description of telegram processing, security operations and noise filtering.
1.8	MKA	MKA	30.01.2018	Added product revision history Added maximum input power and RSSI accuracy. Added current during start-up.
1.9	MKA	MKA	30.04.2018	Added DA-7 to product history
1.10	MKA	MKA	31.07.2018	Added DB-8 to product history, extended description of ESP3 interface, telegram filtering and BaseID functionality
1.11	MKA	MKA	08.01.2019	Added application info for SAW circuit
1.12	MKA	MKA	05.02.2019	Added note regarding test points and regarding RLC storage.

TCM 515 – ENOCEAN TRANSCEIVER GATEWAY MODULE

Disclaimer

This user manual describes the type of component and shall not be considered as assured characteristics. No responsibility is assumed for possible omissions or inaccuracies. Circuitry and specifications are subject to change without notice. For the latest product specifications, refer to the EnOcean website: http://www.enocean.com.

As far as patents or other rights of third parties are concerned, liability is only assumed for modules, not for the described applications, processes and circuits.

EnOcean does not assume responsibility for use of modules described and limits its liability to the replacement of modules determined to be defective due to workmanship. Devices or systems containing RF components must meet the essential requirements of the local legal authorities.

The modules must not be used in any relation with equipment that supports, directly or indirectly, human health or life or with applications that can result in danger for people, animals or real value.

Components of the modules are considered and should be disposed of as hazardous waste. Local government regulations are to be observed.

Packing: Please use the recycling operators known to you.

TABLE OF CONTENT

TCM 515 – ENOCEAN TRANSCEIVER GATEWAY MODULE

1   General description

1.1   Basic functionality

TCM515 is an addition to the existing TCM 300 / 310 / 320 transceiver module family consisting of the following products:

- TCM 515
  868.3 MHz ASK, EnOcean Radio Protocol version 1, lead market Europe

- TCM 515U
  902.875 MHz FSK, EnOcean Radio Protocol version 2, lead market US

The term "TCM 515" in this document refers to all members of the TCM 515 family unless noted differently.

TCM 515 products are limited to OEM installation ONLY.

TCM 515 is optimized for application requiring smallest possible size and integrated security handling such as line-powered actuators or controllers.

For applications requiring highest radio performance - such as gateways or access points covering larger areas – consider using TCM 310 which provides the highest possible sensitivity and noise immunity.

TCM 515 provides a transparent radio link between EnOcean radio devices and an external host connected via UART interface using the standardized EnOcean Serial Protocol V3 (ESP3) communication protocol.

TCM 515 receives and transmits radio telegrams based on a 50 Ohm or whip antenna connected to the host PCB. It forwards received radio telegrams to an external host processor or host PC via the ESP3 interface. Messages received from an external host via the ESP3 interface will be transmitted by TCM 515 as EnOcean radio telegrams according to the chosen frequency.

TCM 515 is implemented as 31 pin reflow-solderable module with optimized form factor for size constrained applications. It is not pin compatible with existing TCM 310 products. Figure 1 below shows TCM 515.

Figure 1 – TCM 515 outline

TCM 515 – ENOCEAN TRANSCEIVER GATEWAY MODULE

1.2   Technical data

Antenna		50 Ohm whip antenna (connected at host board)
Supported Radio Frequencies	TCM 515: TCM 515U:	868.3 MHz ASK 902.875 MHz FSK
Data Rate		125 kbps
Receiver Sensitivity [1]	TCM 515: TCM 515U:	868.3 MHz ASK: -92 dBm 902.875 MHz FSK: -98 dBm
Maximum Input Power [1]		-23 dBm
Receiver Blocking Performance		Class 2 according to EN 300 220-1
Radiated RF Immunity		3 V / m according to EN 301 489-3
Transmit Power	TCM 515: TCM 515U:	868.3 MHz ASK: +10 dBm 902.875 MHz FSK: +1 dBm
Supply Voltage (typ)		2.0 V … 3.6 V
Supply Current (at 2.0V)		25 mA
Supply Current Sleep Mode (at 2.0V / 25°C)		0.05 mA
Power-up to Ready State Timing [2]		50 ms
Ready State to RX State Delay [2]		200 ms (adjustable via ESP3)
Supply Current between Power-up and RX		12 mA
TX to RX switching time [3]		< 1 ms
Serial Host Interface		UART according to ESP3 Standard (TURBO option)

Note 1: Sensitivity and Maximum Input Power figures are based on 0.1% telegram error rate for the combination of 3 received sub-telegrams measured at 25°C

Note 2: TCM 515 requires approximately 50 ms for start-up after power up. After completion of its internal start-up, it waits for the selected delay period before starting RX mode to allow for power supply stabilization. The delay period is adjustable via ESP3 command.

Note 3: TX to RX switch over time is measured from the transmission of the last bit (end of frame) of a radio frame until the receiver is ready to receive the first bit (preamble) of a radio frame

1.3   Physical dimensions

Module Dimensions	19.0 mm x 14.7 mm x 3.0 mm (all +- 0.3 mm)
Module Weight	1 g

1.4 Environmental conditions

Operating Temperature	-40°C … 85°C
Storage Temperature	-40°C … 85°C
Humidity	0% to 95% r.h. (non-condensing)

1.5 Packaging information

Packaging Unit / Method	250 units / Tape an

1.6 Ordering information

Type	Ordering Code
TCM 515	S3003-K515
TCM 515U	S3053-K515

2   Functional information

2.1   High level functionality

TCM 515 is a fully integrated radio transceiver family which enables communication with other devices implementing the EnOcean Radio Protocol (ERP).

TCM 515 is used to exchange (send and / or receive) radio telegrams with external sensors, switches or actuators.

TCM 515 is connected to an external host which for instance could be a microprocessor, a controller or a gateway.

Figure 2 below shows the integration of TCM 515 into a typical system environment.
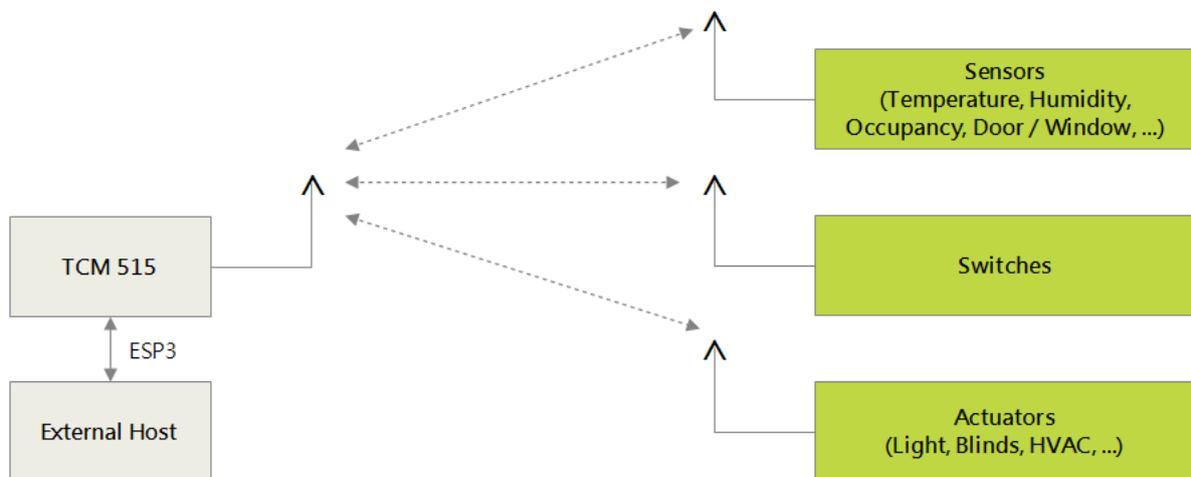
Figure 2 – TCM 515 system environment

TCM 515 – ENOCEAN TRANSCEIVER GATEWAY MODULE

2.2   Functional modes

TCM 515 implements the following functional modes:

- Telegram Reception

- Telegram Transmission

- Low Power Sleep

The transition between these functional modes is shown in Figure 3 below
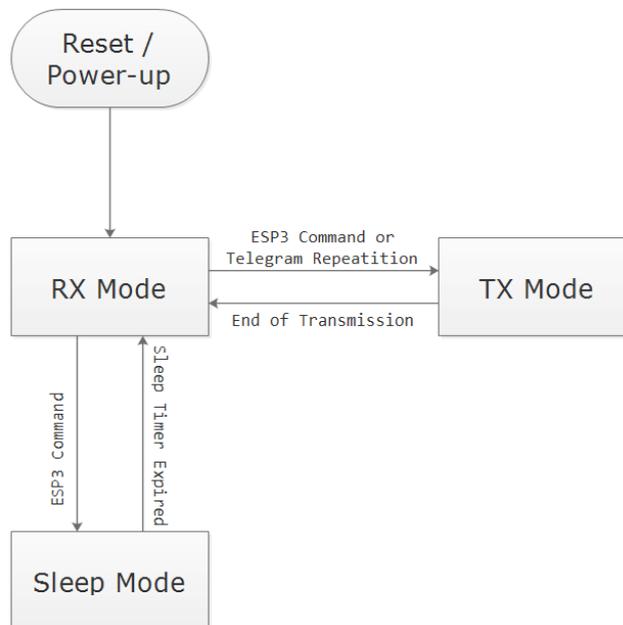
Figure 3 – TCM 515 functional modes

The following chapters describe these functional modes in more detail.

TCM 515 – ENOCEAN TRANSCEIVER GATEWAY MODULE

2.2.1 Telegram reception

In receive mode, TCM 515 processes received radio telegrams and verifies correct frame structure and check sum.

Received telegrams can be filtered according to a filter list that can be setup via dedicated ESP3 commands (see chapter 3.3 for the list of supported ESP3 commands).

For each received telegram, TCM 515 will check if the source address (sender of the telegram) is setup in its inbound secure link table. If that is the case then TCM 515 will automatically apply the specified security processing (authentication, decryption) specified by corresponding inbound secure link table entry.

Processed radio telegrams will then be forwarded to the external host via the ESP3 interface. See chapter 4 for a detailed description of the receiver functionality.

2.2.2 Telegram transmission

In transmit mode, TCM 515 receives radio telegrams for transmission from the external host via its ESP3 interface.

TCM 515 will check if the destination address (intended receiver of the telegram) is setup in the outbound secure link table. If that is the case then TCM 515 will automatically apply the security processing specified by the corresponding outbound secure link table entry.

TCM 515 will then properly format the radio telegram frame and transmit the telegram as a series of redundant telegrams. See chapter 4 for a detailed description of the transmission functionality.

2.2.3 Telegram repeating

TCM 515 can act as repeater for all or selected radio telegrams. The repeating functionality is configured via ESP3 interface.

If TCM 515 is configured to act as repeater and it receives a radio telegram that it has to repeat then TCM 515 will automatically transition from receive to transmit state to retransmit (repeat) this telegram. After successful transmission, it will automatically transition back to receive mode.

See chapter 4.5 for a description of the repeater functionality.

2.2.4 Low power sleep mode

TCM 515 can be set into a low power sleep mode for a defined period of time by means of an ESP3 command. After expiry of the requested sleep period, TCM 515 will automatically wake-up and transition back to receive mode.

TCM 515 – ENOCEAN TRANSCEIVER GATEWAY MODULE

2.3 Device Interface

TCM 515 implements a 31 pin reflow-solderable interface. Solder mask data is available on request from EnOcean.

2.3.1 Pin-out

The pin assignment (as seen from the top of the device) is shown in Figure 4 below. Solder mask and mechanical data is available from EnOcean.
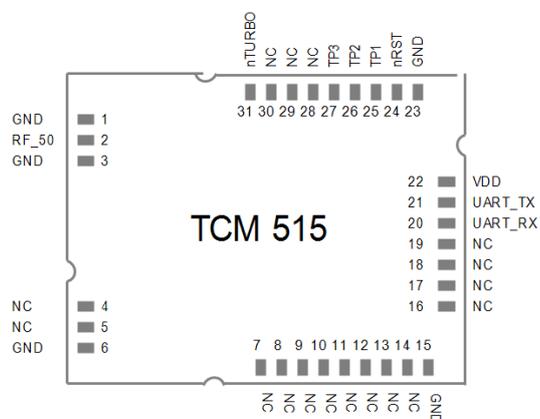
Figure 4 – TCM 515 device interface

Table 1 below summarizes the signal assignment.

PIN	NAME	PIN	NAME	PIN	NAME
1	GND	12	NC	23	GND
2	RF_50 (50Ω antenna)	13	NC	24	nRST (Reset, active low)
3	GND	14	NC	25	TP1 (Test Interface)
4	NC	15	GND	26	TP2 (Test Interface)
5	NC	16	NC	27	TP3 (Test Interface)
6	GND	17	NC	28	NC
7	NC	18	NC	29	NC
8	NC	19	NC	30	NC
9	NC	20	UART_RX (Input)	31	nTURBO (UART speed, active low)
10	NC	21	UART_TX (Output)		
11	NC	22	VDD		

Table 1 - TCM 515 pin assignment

Signals marked with "NC" are reserved for production test and future device variants and must not be connected in the design.

2.3.2 Power supply

TCM 515 is supplied by the VDD and GND Pins and supports a supply voltage range from 2.0V to 3.6V. For best radio performance it is very important to minimize noise on the supply voltage lines. Please see chapter 8.4.

2.3.3 Antenna

TCM 515 receives and transmits data based on a 50Ω whip antenna connected to its RF_50 input (Pin 2). Please see chapter 9.

2.3.4 UART interface

TCM 515 communicates with the external host using the standard ESP3 serial (UART) interface based on the signals UART_TX (Pin 21, direction from TCM 515 to external host) and UART_RX (Pin 20, direction from external host to TCM 515).

The default interface speed of the ESP3 interface is 57600 bit per second and data is transmitted using 8 data bits, 1 STOP bit and no parity (8N1).

It is possible to select faster communication speeds during operation using the ESP3 CO_SET_BAUDRATE command (see chapter 0). The following interface speeds are supported by TCM 515:

- 57600 bit per second

- 460800 bit per second

Additionally, it is possible to change the default ESP3 interface speed at power up from 57.600 Bit per second to 460.800 Bit per second by connecting the nTURBO input (Pin 31, active low) to Ground.

Subsequent modification of the interface speed during operation using the CO_SET_BAUDRATE command is always possible irrespective of the state of the TURBO input pin. Care should be taken not to select a UART interface speed which cannot be supported by the connected host processor as this would prevent subsequent communication.

TCM 515 – ENOCEAN TRANSCEIVER GATEWAY MODULE

2.3.5   Reset

TCM 515 can be reset by pulling the nRST pin (Pin 24, active low) to Ground. Please see chapter 8.9 for reset circuit recommendations.

2.3.6   Test Interface (TP1, TP2, TP3)

TCM 515 provides a test interface (TP1, TP2 and TP3). The intended use of this interface is for analysis and debugging of customer products by EnOcean. It is strongly recommended that customer PCB design provides the ability to connect to this interface.

3 ESP3 interface

TCM 515 provides an external interface according to the EnOcean Serial Protocol, version 3 (ESP3).

This interface is used both to exchange telegrams and command / status messages with an external host system (e.g. microcontroller or PC) and EnOcean gateway transceiver modules.

The information in the subsequent chapters is provided as an introduction for information purposes. For detailed information, please refer to the ESP3 specification: https://www.enocean.com/esp

3.1 ESP3 physical interface

The physical interface used by ESP3 for communication between host system and an EnOcean Gateway Controller is a 3-wire full duplex UART / RS-232 connection (RX, TX, GND).

The standard UART baud rate is 57600 baud per second. TCM 515 supports a higher baud rate of 460800 baud per second which can be selected using the command CO_SET_BAUDRATE.

3.2   ESP3 Packet Structure

ESP3 is a point-to-point (one to one) protocol based on a packet data structure. Figure 5 below illustrates the ESP3 packet structure.

ESP3 Packet Structure
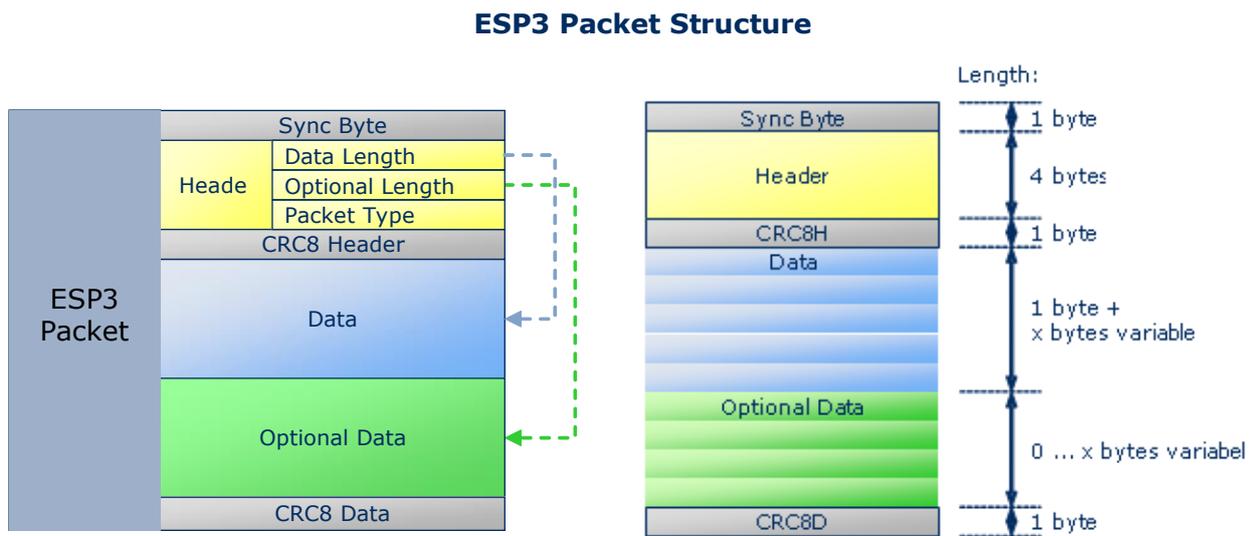
Figure 5 – ESP3 Packet Structure

Each ESP3 packet contains the following fields:
- Header
- Data
- Optional Data.

In addition to those fields, the Sync Byte (0x55) identifies the start of the packet while separate CRC8 for Header and Data (incl. Optional Data) are used to verify data integrity.

The Header consists of the following fields:
- Data Length (number of bytes of the group Data)
- Optional Length (number of bytes of the group Optional Data)
- Packet Type (RADIO, RESPONSE, EVENT, COMMAND ...)

The Data field encodes the ESP3 command together with the required parameter data. For some commands, the Optional Data field is used to provide additional parameter data.

DOLPHIN
Self-powered IoT by EnOcean

TCM 515 – ENOCEAN TRANSCEIVER GATEWAY MODULE

3.3 Supported ESP3 commands

The following ESP3 commands are supported by TCM 515:

- Type 1: ERP1 Radio Telegram

- Type 2: Responses
  - RET_OK
  - RET_ERROR
  - RET_NOT_SUPPORTED
  - RET_WRONG_PARAM
  - RET_OPERATION_DENIED
  - RET_LOCK_SET
  - RET_BUFFER_TO_SMALL
  - RET_NO_FREE_BUFFER

- Type 4: Events
  - SA_CONFIRM_LEARN to confirm/discard learn in/out
  - CO_READY to indicate wake up from deep sleep initiated by CO_WR_SLEEP
  - CO_EVENT_SECUREDEVICES to inform about security processing issues
  - CO_DUTYCYCLE_LIMIT to inform about a current limitation due to duty cycle

- Type 5: Common commands
  - CO_WR_RESET to reset the device
  - CO_RD_VERSION to read SW/HW versions, chip ID etc.
  - CO_GET_FREQUENCY_INFO to read the operating frequency of the device
  - CO_WR_STARTUP_DELAY
  - CO_WR_SLEEP to put the device into low power sleep mode
  - CO_WR_IDBASE to set the Base ID range
  - CO_RD_IDBASE to read the Base ID range
  - CO_WR_REPEATER to set repeater functionality
  - CO_RD_REPEATER to read repeater functionality
  - CO_WR_FILTER_ADD to add filter to filter list or to selective repeating
  - CO_WR_FILTER_DEL and CO_WR_FILTER_DEL_ALL to delete filters
  - CO_RD_FILTER to read the configured filters
  - CO_WR_FILTER_ENABLE to enable/disable the configured filters
  - CO_WR_LEARNMODE to set learn mode
  - CO_RD_LEARNMODE to read learn mode status
  - CO_WR_WAIT_MATURITY to wait until the end of the maturity time
  - CO_RD_DUTYCYCLE_LIMIT to read the duty cycle (for 868 MHz EU version)
  - CO_SET_NOISETHRESHOLD to set the input noise rejection threshold
  - CO_GET_NOISETHRESHOLD to read the input noise rejection threshold
  - CO_WR_REMAN_REPEATING to set the repeater level of Reman messages
  - CO_RD_REMAN_REPEATING to read the repeater level Reman messages
  - CO_SET_BAUDRATE to set the baud rate of the ESP3 interface
  - CO_WR_SECUREDEVICE_ADD
  - CO_WR_SECUREDEVICE_DEL
  - CO_RD_SECUREDEVICE_COUNT
  - CO_RD_SECUREDEVICE_BY_INDEX
  - CO_RD_SECUREDEVICE_BY_ID
  - CO_WR_SECUREDEVICE_SENDTEACHIN

- Type 6 Smart Acknowledge commands (postmaster / mailbox functions)
  - SA_WR_LEARNMODE to set/reset Smart Acknowledge learn mode
  - SA_RD_LEARNMODE to get learn mode
  - SA_WR_LEARNCONFIRM to add or delete a mailbox of a client
  - SA_WR_RESET to send a reset command to a client
  - SA_RD_LEARNEDCLIENTS to get learned mailboxes/clients
  - SA_WR_POSTMASTER to activate/deactivate post master functionality

- Type 7 Remote Management
  - Messages with up to 255 byte of payload

- Type 10: ERP2 Radio Telegram (TCM 515U only, selected using CO_WR_MODE)

3.4   Persistent versus not persistent configuration settings

TCM 515 will store certain configuration settings in persistent memory, i.e. those settings will be maintained even after a power cycle.

There are three classes of persistent settings:

1. Repeater and filter configuration
   Starting from product version DA-08 (see chapter 12), the repeater and filter con-figuration defined via the following commands will be maintained after power failure:
   - CO_WR_REPEATER
   - CO_WR_FILTER_ADD
   - CO_WR_FILTER_DEL
   - CO_WR_FILTER_DEL_ALL
   - CO_WR_FILTER_ENABLE

2. List of secure devices as defined by the following commands:
   - CO_WR_SECUREDEVICE_ADD
   - CO_WR_SECUREDEVICE_DEL

3. System parameters as defined by the following commands:
   - CO_WR_STARTUP_DELAY
   - CO_SET_NOISETHRESHOLD
   - CO_WR_IDBASE

All other settings need to be reinitialized at power up.

4 Telegram transmission

4.1 Transmission flow

TCM 515 performs the following functions to transmit radio telegrams:

■ Telegram input
TCM 515 receives the radio telegram data from the external host via the ESP3 interface as described in chapter 0

■ Security handling
Telegrams to receivers supporting high security mode can be automatically encrypted and authenticated according to the parameters specified by their outbound secure link table entry as described in chapter 6

■ Telegram transmission
Processed telegrams will be transmitted as a set of redundant subtelegrams as described in chapter 4.2

Figure 6 below shows the process for the transmission of EnOcean radio telegrams.

Figure 6 – Telegram Transmission Flow

TCM 515 – ENOCEAN TRANSCEIVER GATEWAY MODULE

4.2   Subtelegram Timing

EnOcean radio systems use the concept of redundant subtelegrams in order to increase the communication reliability. In addition to using redundant transmissions, first and second level repeaters can be used to increase communication distance and reliability as described in chapter 4.5.

Within this scheme, telegrams are transmitted redundantly with random (but small) delays between them. The total number of redundant subtelegrams can be either two or three. Certain telegram types (e.g. within remote commissioning functionality) do not support redundant transmission, i.e. they are transmitted only once.

If a telegram is transmitted redundantly as set of two or three subtelegrams then the first subtelegram is sent immediately upon receiving and processing the ESP3 command for telegram transmission.

The timing offset between this first subtelegram and the remaining (second or third) subtelegrams is random within pre-defined time intervals.

For the case of the sender, the time offset (interval) between the first subtelegram and the second subtelegram is a random value between 1 ms and 9 ms. Likewise, the time offset (interval) between the first subtelegram and the third subtelegram is a random value between 20 ms and 39 ms.

For the first-level repeater (which received the telegram from the sender), the time offset (interval) between the reception of the telegram and the transmission of the first subtelegram is a random value between 10 ms and 19 ms. Likewise, the time offset (interval) between the reception of the telegram and the second subtelegram is a random value between 20 ms and 29 ms.

For the second-level repeater (which received the telegram from the first-level repeater), the time offset (interval) between the reception of the telegram and the transmission of the first subtelegram is a random value between 0 ms and 9 ms. Likewise, the time offset (interval) between the reception of the telegram and the second subtelegram is a random value between 20 ms and 29 ms.

Both first and second level repeaters do not transmit a third subtelegram. The subtelegram timing is summarized in Table 2 below.

Repeater Level	Time Offset [ms] First Subtelegram	Time Offset [ms] Second Subtelegram	Time Offset [ms] Third Subtelegram
0 (Original Telegram)	0	1 … 9	20 … 39
1 (Repeated for the first time)	10 … 19	20 … 29	No 3rd Subtelegram
2 (Repeated for the second time)	0 … 9	20 … 29	No 3rd Subtelegram

Table 2 – Subtelegram timing

TCM 515 – ENOCEAN TRANSCEIVER GATEWAY MODULE

4.3   TX Maturity Time

The transmission (TX) maturity time defines the longest possible interval between the transmission of the first subtelegram and the transmission of the last subtelegram belonging to the same telegram.

As shown in Table 2, this TX maturity time is always < 40 ms (the transmission of the last subtelegram starts at 39 ms offset from the transmission first subtelegram).

4.4   Address types

EnOcean radio systems support three different types of addresses for radio transmission:

- ■ EnOcean Unique Radio ID (EURID)

- ■ Base ID

- ■ Broadcast ID

Each of these three address types corresponds to a specific address or address range as shown in Figure 7 below.
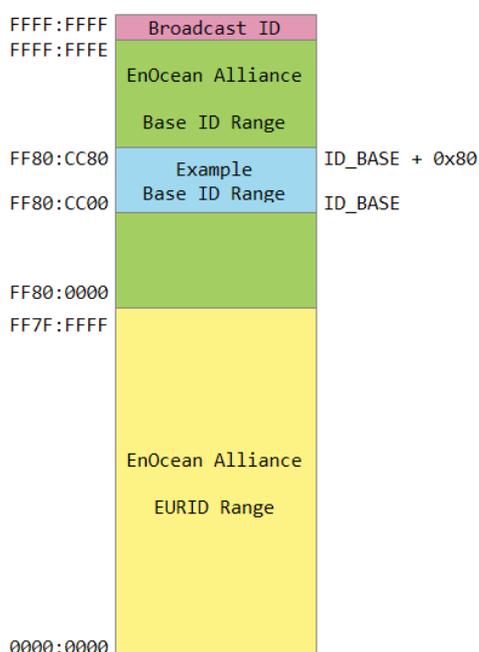

Figure 7 – EnOcean Address Map

The difference between these address types is described in the following chapters.

TCM 515 – ENOCEAN TRANSCEIVER GATEWAY MODULE

4.4.1 EURID

Each TCM 515 module contains its own EnOcean Unique Radio ID (EURID) which is assigned by EnOcean Alliance. The EURID uniquely identifies each EnOcean device; no two devices can have the same EURID.

The EURID is used during transmission to uniquely identify the originator (sender) of a message.

In addition, the intended receiver of a transmitted telegram can additionally (optionally) be specified using its EURID. Telegrams where the intended receiver is designated are called Addressed Data Telegram or ADT in short.

4.4.2 Base ID

Normally, EnOcean devices will use their own EURID in order to identify themselves as the originator of transmitted telegrams. For very specific use cases, they can instead choose to use an address (ID) from within a defined range of 128 addresses. These 128 addresses are called the Base ID Range of the device.

The Base ID Range (128 addresses) of a device can be allocated anywhere in between `0xFF80:0000` and `0xFFFF:FFFE` (which represents a total range of approximately 8 million addresses). The location of the Base ID Range is defined by the start (lowest) address of the range which will always be aligned on a 7 bit (128) boundary, i.e. the last byte of the address can be either `0x00` or `0x80`.

This start address is pre-configured randomly for each TCM 515 module during production but can be modified using the ESP3 command CO_WR_IDBASE. Alignment is automatically enforced within TCM 515, i.e. if a non-aligned address is provided in the ESP3 command then TCM 515 will use the next lower aligned address as start address of the Base ID range.

The use of Base ID allows TCM 515 modules to transmit messages using different sender ID. Additionally, the use Base ID allows replacement of one device by another without executing the teach-in procedure since the new device could be configured to use the same Base ID as the old device.

Base ID is a legacy feature that is not recommended for use anymore because Base ID are not globally unique. Many devices with the same Base ID exit within the EnOcean ecosystem.

Note that having two devices with the same Base ID within a system might lead to undefined system behaviour.

Note that the use of Base ID is not defined within the scope of secure communication. TCM 515 applications shall therefore not use the Base ID functionality for telegrams where TCM 515 is handling the security processing.

TCM 515 supports the use of Base ID for backwards compatibility.

TCM 515 – ENOCEAN TRANSCEIVER GATEWAY MODULE

4.4.3   Broadcast ID

The Broadcast ID can be used instead of the EURID of the receiver if a telegram is intended for several receivers or if the EURID of the intended receiver is unknown. Such telegrams are called "Broadcast Telegrams" and are commonly used by sensors and switches. The Broadcast ID is 0xFFFF:FFFF.

Receivers of broadcast telegrams can decide based on the EURID of the sender (originator) of the telegram if this telegram is relevant for them or not.

4.5   Built-in Repeater

TCM 515 provides the option to activate a one or two-level repeater for received EnOcean radio telegrams.

■ 1-level repeater: If a received telegram is a valid and original (not yet repeated), the telegram is repeated after a random delay. This delay will be chosen such that the maximum TX maturity time (as standardized in ISO 14543-3-10) of 40 ms will not be exceeded.

■ 2-level repeater: If a received telegram is valid and original or repeated once, the telegram is repeated after a random delay. This delay will be chosen such that the maximum TX maturity time (as standardized in ISO 14543-3-10) of 40 ms will not be exceeded.

Repeated telegrams are marked as "repeated" by an increased repeater counter. Configuration of the repeater functionality is done via serial interface commands.

⚠ When using repeaters, care must be taken to ensure that regulatory transmitter duty cycle limits (if applicable) are not exceeded.

⚠ 2-level repeating function should only be activated after careful study of the radio conditions! Otherwise the system function can be compromised by collisions of telegrams.

For detailed recommendations regarding the usage of repeaters please refer to our application note EnOcean Wireless Systems - Installation Notes (PDF), 09/2010.

TCM 515 also provides selective repeating, i.e. the option to only repeat certain telegrams with match pre-defined filter criteria. The filter criteria that can be applied for repeating are the same as the ones for telegram reception, please see chapter 0.

The repeater configuration (no repeating, 1-level repeating, 2-level repeating, selective repeating) is stored persistently in non-volatile memory and will therefore not be affected by a power cycle. This mechanism enables the option of configuring USB stick repeaters (similar to USB 300) on a PC via the ESP3 interface and then transferring them to a USB power supply for subsequent operation.

4.6   Duty Cycle Limit

European radio regulation mandates that the duty cycle limits of radio transmitters have to be enforced by technical means. The European (868.3 MHz) version of TCM 515 therefore implements a hardware duty cycle monitor which enforces the regulatory duty cycle limit of 1% per hour.

The functionality of this monitor is as follows:

- Each 1 hour (3600 seconds) period is sub-divided into 10 time slots of 360 seconds each. The total available transmission time (36 seconds per 3600 second period) is equally divided upon these 10 time slots, i.e. each time slot is allocated 3.6 seconds of transmission time.

- For each time slot, the total transmission time is accumulated

- The remaining available transmission time is calculated as difference between allocated and accumulated transmission time.

- If the available transmission time reaches zero (no more transmission time available) then TCM 515 will not transmit any additional messages during this time interval. TCM 515 will respond with RET_LOCK_SET to the host if this requests transmission of additional telegrams in this case.

The host can query the duty cycle status at any time using the ESP3 command CO_RD_DUTYCYCLE_LIMIT. The response from TCM 515 will specify both the already used percentage of available transmission time within the current time slot (0% … 100%) and the remaining time (in seconds) until the start of the next time slot.

5 Telegram reception flow

TCM 515 performs the following functions for each received radio telegram:

- Telegram filtering
  Received telegrams can be classified according to user-defined characteristics and only telegrams matching these characteristics will be processed

- Security handling
  Telegrams from senders using high security mode can be automatically decrypted and authenticated according to the parameters specified by their inbound secure link table entry

- Telegram output
  Processed telegrams will be forwarded to the external host via the ESP3 interface

Figure 8 below shows the handling for received telegrams.

Figure 8 – Telegram Reception Flow

Note that by default, TCM 515 will forward all telegrams received by it (including such that are addressed to a different receiver) to the host via its ESP3 interface.

If TCM 515 shall forward only telegrams that are addressed to it (either as addressed telegram or as broadcast) then you can configure a radio filter as described in the next chapter.

TCM 515 – ENOCEAN TRANSCEIVER GATEWAY MODULE

5.1   RX maturity time

The reception (RX) maturity time defines the longest possible interval between the reception of the first subtelegram and the reception of the last subtelegram belonging to the same telegram.

Considering the worst case of a telegram received after two levels of repeating, the RX maturity time is always < 100 ms (39 ms + 29 ms + 29 ms) as shown in Table 2.

TCM 515 can be configured to wait for the RX maturity time (100 ms) after reception of a subtelegram in order to determine the number of received subtelegrams. TCM 515 will in that case report the actual number of received subtelegrams to the external host.

Alternatively, TCM 515 can be configured to immediately forward a received subtelegram to the host and discard subsequent identical subtelegrams. This provides the lowest latency and is the default operation mode for TCM 515.

The selection between these two options is done using the CO_WR_WAIT_MATURITY command; see the ESP3 specification for details.

5.2 Telegram filtering

Telegram filtering is the process by which only radio telegrams that match specific user-defined parameters will be forwarded to the external host (selective forwarding) or repeated (selective repeating).

Telegram filtering is therefore to limit the amount of telegram processing required at the external host or to optimize the available radio bandwidth.

5.2.1 Filter types

Telegram filtering is the process by which only radio telegrams that match specific user-defined parameters will be forwarded to the external host (selective forwarding) or repeated (selective repeating).

The following parameters can be used as filter condition:

- Source ID
  Only radio telegrams originating from a specific sender (identified by its EnOcean Universal Radio ID = EURID) will be processed.
  This filter type can be used for instance in actuators which only accept input from devices (e.g. switches) that have been learned in.

- Destination ID
  Only radio telegrams addressed to a specific receiver (as identified by its EURID) will be processed.
  This filter type can be used by a receiver to accept only radio telegrams intended for itself.

- Telegram Type (RORG)
  Only radio telegrams of a specific type (RPS, 1BS, 4BS or VLD) will be processed.
  This filter type can be used for instance if an actuator should react only on switch (RPS) telegrams.

- Received signal strength (RSSI)
  Only radio telegrams above or below a specific signal strength will be processed.
  The first case – above - can for instance be used during learn-in if an actuator should only accept teach-in telegrams from devices close to the receiver.
  The second case – below - can be used in repeaters where only weak signals (with low RSSI) should be repeated in order to limit radio congestion.

TCM 515 – ENOCEAN TRANSCEIVER GATEWAY MODULE

5.2.2 Filter logic

Each filter criterion can be defined as positive filter (message is forwarded / repeated if the condition is true) or as negative filter (message is forwarded / repeated if the condition is false). If for instance the filter condition is a certain source ID then it can be selected if only telegrams originating from this source ID are repeated / forwarded (positive filter) or if all messages except the one originating from this source ID are repeated / forwarded (negative filter).

Moreover, for each filter criterion it can be defined if it shall apply for the forwarding functionality or for the repeating functionality of TCM 515. The maximum number of filter criteria is 30. Attempting to define more filter criteria will result in the response 01: RET_ERROR (memory space full).

Note that more than one filter can be defined, e.g. it is possible to setup filter rules such that telegrams originating from several source ID will be processed. If more than one filter condition per functionality is defined then it can be defined if all conditions must be true (logical AND) or one of the conditions must be true (logical OR).

TCM 515 – ENOCEAN TRANSCEIVER GATEWAY MODULE

5.2.3   Configuration of telegram filtering

Telegram filtering is configured using the following ESP3 commands:

- CO_WR_FILTER_ADD to add filter to filter list or to selective repeating
- CO_WR_FILTER_DEL to delete filter from filter list or from selective repeating
- CO_WR_FILTER_DEL_ALL to delete all filter
- CO_WR_FILTER_ENABLE to enable/disable supplied filters
- CO_RD_FILTER to read the currently active filters

The syntax of the CO_WR_FILTER_ADD command is shown in Table 3 below.

Group	Offset	Size	Field	Value hex	Description
-	0	1	Sync. Byte	0x55	
Header	1	2	Data Length	0x0007	7 bytes
	3	1	Optional Length	0x00	0 byte
	4	1	Packet Type	0x05	COMMON_COMMAND = 5
-	5	1	CRC8H	0xnn	
Data	6	1	COMMAND Code	0x0B	CO_WR_FILTER_ADD = 11
	7	1	Filter type	0x00...0x03	0x00 : Source ID 0x01 : Telegram Type (R-ORG) 0x02 : Received Signal Strength (RSSI) 0x03 : Destination ID
	8	4	Filter value	0xnnnnnnnn	Value of filter function 'compare': - device source or destination ID - R-ORG - dBm value RSSI of radio telegram (un-signed, but interpreted as negative dBm value)
	12	1	Filter kind	0x00 0x80 0x40 0xC0	0x00: Negative for telegram forwarding 0x80: Positive for telegram forwarding 0x40: Negative for telegram repeating 0xC0: Positive for telegram repeating
-	13	1	CRC8D	0xnn	

Table 3 – Syntax for CO_WR_FILTER_ADD command

Once all filters have been defined, the CO_WR_FILTER_ENABLE command shown in Table 4 below has to be used to select the logical relation between the defined filters (logical AND versus logical OR) and to enable the filtering mechanism for telegram forwarding via ESP3.

Group	Offset	Size	Field	Value hex	Description
-	0	1	Sync. Byte	0x55	
Header	1	2	Data Length	0x0003	3 bytes
	3	1	Optional Length	0x00	0 byte
	4	1	Packet Type	0x05	COMMON_COMMAND = 5
-	5	1	CRC8H	0xnn	
Data	6	1	COMMAND Code	0x0E	CO_WR_FILTER_ENABLE = 14
	7	1	Forward Filter ON/OFF	0x00 / 0x01	0x00: Forwarding filter disabled / 0x01: Forwarding filter enabled
	8	1	Filter Operator	0x00 / 0x01 / 0x08 / 0x09	OR composition of all filters = 0 / AND composition of all filters = 1 / OR for radio interface filters; AND for filtered repeating filters = 8 / AND for radio interface filters; OR for filtered repeating filters = 9
-	9	1	CRC8D	0xnn	

Table 4 – Syntax for CO_WR_FILTER_ENABLE command

The use of filters for the repeater is enabled by means of the CO_WR_REPEATER command shown in Table 5 below. There, REP_ENABLE has to be set to 0x02 to enable selective repeating based on the defined filters.

Group	Offset	Size	Field	Value hex	Description
-	0	1	Sync. Byte	0x55	
Header	1	2	Data Length	0x0003	3 bytes
	3	1	Optional Length	0x00	0 byte
	4	1	Packet Type	0x05	COMMON_COMMAND = 5
-	5	1	CRC8H	0xnn	
Data	6	1	COMMAND Code	0x09	CO_WR_REPEATER = 09
	7	1	REP_ENABLE	0x00…0x02	0x00: No repeating / 0x01: Repeating of all telegrams / 0x02: Selective repeating
	8	1	REP_LEVEL	0x00…0x02	0x00: No repeating / 0x01: One level repeating / 0x02: Two level repeating
-	9	1	CRC8D	0xnn	

Table 5 – Syntax for CO_WR_REPEATER command

TCM 515 – ENOCEAN TRANSCEIVER GATEWAY MODULE

Filters can be deleted individually using the CO_WR_FILTER_DEL command as shown in Table 6 below.

Group	Offset	Size	Field	Value hex	Description
-	0	1	Sync. Byte	0x55	
Header	1	2	Data Length	0x0007	7 bytes
	3	1	Optional Length	0x00	0 byte
	4	1	Packet Type	0x05	COMMON_COMMAND = 5
-	5	1	CRC8H	0xnn	
Data	6	1	COMMAND Code	0x0C	CO_WR_FILTER_DEL = 12
	7	1	Filter type	0x00…0x03	Device source ID = 0, R-ORG = 1, dBm = 2, destination ID = 3
	8	4	Filter value	0xnnnnnnnn	Value of filter function 'compare': - device source or destination ID - R-ORG - dBm value RSSI of radio telegram (unsigned, but interpreted as negative dBm value)
	12	1	Filter kind	0x00 0x80 0x40 0xC0	blocks radio interface = 0x00 apply radio interface = 0x80 blocks filtered repeating = 0x40 apply filtered repeating = 0xC0
-	13	1	CRC8D	0xnn	

Table 6 – Syntax for CO_WR_FILTER_DEL command

It is possible to delete all existing features using the CO_WR_FILTER_DEL_ALL command as shown in Table 7 below. It is strongly recommended to use this command to clear the filter table from existing entries before starting the filter table configuration.

Group	Offset	Size	Field	Value hex	Description
-	0	1	Sync. Byte	0x55	
Header	1	2	Data Length	0x0001	1 byte
	3	1	Optional Length	0x00	0 byte
	4	1	Packet Type	0x05	COMMON_COMMAND = 5
-	5	1	CRC8H	0xnn	
Data	6	1	COMMAND Code	0x0D	CO_WR_FILTER_DEL_ALL = 13
-	13	1	CRC8D	0xnn	

Table 7 – Syntax for CO_WR_FILTER_DEL_ALL command

TCM 515 – ENOCEAN TRANSCEIVER GATEWAY MODULE

5.2.4 Forwarding (Receiver) filter examples

The code snippets below give examples of common filter conditions for the telegram forwarding of received telegrams to the external host via the ESP3 interface.

```
// BLOCK telegram forwarding for telegrams sent from the specified ID
Filter_type = 0x0 (ID)
Filter_value = 0x12345678 (device source ID)
Filter_kind = 0x00 (negative filter - block)

// BLOCK telegram forwarding for all telegrams except those sent from the specified ID
Filter_type = 0x00 (ID)
Filter_value = 0x12345678 (device source ID)
Filter_kind = 0x80 (positive filter - apply)

// BLOCK telegram forwarding for telegrams with specified R-ORG
Filter_type = 0x01 (R-ORG)
Filter_value = 0xA5 (4BS)
Filter_kind = 0x00 (negative filter - block)

// BLOCK telegram forwarding for all telegrams except those with specified R-ORG
Filter_type = 0x01 (R-ORG)
Filter_value = 0xA5 (4BS)
Filter_kind = 0x80 (positive filter - apply)

//BLOCKS signals weaker than -70dBm
Filter_type = 0x02 (dBm)
Filter_value = 0x00000046 (dec 70)
Filter_kind = 0x00 (block)

//BLOCKS signals stronger than -70dBm
Filter_type = 0x02 (dBm)
Filter_value = 0x00000046 (dec 70)
Filter_kind = 0x80 (apply)
```

5.2.5 Repeater filter examples

The code snippets below give examples of possible filter conditions for the telegram repeating of received telegrams (selective repeating).

```
// Repeat only telegrams from the specified ID (requires REP_ENABLE = 0x02)
Filter_type = 0x00 (ID)
Filter_value = 0x12345678 (device source ID)
Filter_kind = 0xC0 (positive filter – apply - for filtered repeating)
```

```
//Do not repeat telegrams with specified R-ORG (requires REP_ENABLE = 0x02)
Filter_type = 0x01 (R-ORG)
Filter_value = 0xA5 (4BS)
Filter_kind = 0x40 (negative filter - block - for filtered repeating)
```

```
// Do not repeat signals stronger than -70dBm (requires REP_ENABLE = 0x02)
Filter_type = 0x02 (dBm)
Filter_value = 0x00000046 (decimal: 70)
Filter_kind = 0xC0 (positive filter – apply - for filtered repeating)
```

6 Security functionality

TCM 515 implements the security handling functions as specified in the EnOcean security specification: https://www.enocean.com/security-specification

TCM 515 can receive and decrypt messages from the following EnOcean modules:

- PTM 215

- PTM 335 / PTM 535

- STM 320 / STM 329 / STM 250 (or similar with same profile)

- STM 330 / STM 331 (or similar with same profile)

- STM 350

6.1 Basic concepts

Security for radio transmission addresses two main issues:

- Unauthorized interception (reception and correct interpretation) of transmitted data
  In doing so, a third (unauthorized) party is able to understand the content of a received content.

- Unauthorized transmission of radio telegrams
  In doing so, a third (unauthorized) party is able to transmit a radio telegram that is treated by a receiver as valid request.

Somewhat loosely speaking, the goal of security has to be preventing an unauthorized person (often referred to as an *Attacker*) both from learning about the current state of a system and from actively changing it.

These goals can be achieved via techniques such as telegram encryption, telegram authorization and dynamic security key modification. All three techniques will be reviewed in the subsequent chapters for reference.

6.1.1 Telegram encryption

The goal of telegram encryption is to prevent unauthorized receivers from correctly interpreting the content of a telegram.

In order to do so, the original (plain text) data is *encrypted* with a *key* thus transforming it into encrypted, unreadable data. Only when the correct key is known it is possible to transform – *decrypt* - the encrypted data into readable data again. Figure 9 below shows the concept.
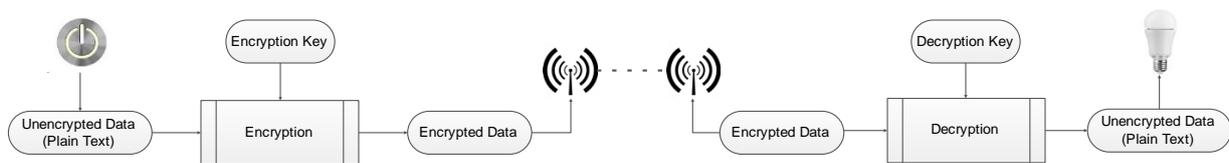

Figure 9 – Telegram encryption

6.1.2 Telegram authentication

The goal of telegram authentication is to prevent unauthorized senders to transmit apparently valid commands causing the receiver to perform unauthorized actions.

Telegram authentication works by creating a *message signature* (often referred to as *Message Authentication Code* or *MAC* in short) based on the content of the telegram and the secret key.

Essentially, the telegram data is transformed via a defined algorithm using the secret key into a unique, fixed size signature (where typical signature lengths include 24 Bit, 32 Bit, 512 Bit and 1024 Bit) which identifies this specific message.

For an optimal signature algorithm, the likelihood of two different messages creating the same message signature is inversely proportional to the signature size, so for instance for 24 Bit signatures the likelihood would be one in 16 million.

Conceptually the correspondence between message and signature is similar to the one between a person and a finger print:

- Each person has a unique fingerprint. Based on a given person one can determine her or his fingerprint

- Based on a given fingerprint one can check if it originated from a given person

- Based on the fingerprint one cannot determine any other properties of the person

TCM 515 – ENOCEAN TRANSCEIVER GATEWAY MODULE

For message authentication purposes, the message signature (MAC) is typically appended to the message itself and transmitted together with it.

When the receiver receives such a message, it will itself calculate the MAC based on the secret key and the content of the received message. The receiver then compares the MAC it calculated with the MAC it received as part of the message.

If both MAC are the same then the receiver can establish two important facts:

1. The message originates from an owner of the secret key

2. The content of the message has not been modified

Figure 10 below illustrates the content authorization via a MAC signature.
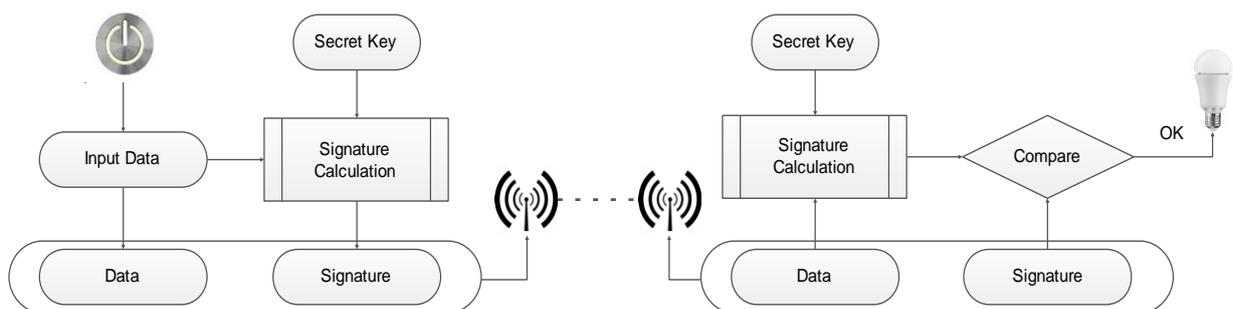
Figure 10 – Telegram authentication

6.1.3   Dynamic security key modification

One fundamental problem with both content protection and content authorization is that using the same input data (plain text) with the same key always yields the same encrypted data and the same signature.

This enables attacks based on monitoring previous system behaviour. If an attacker has observed that a certain data telegram results in a certain light being turned on then he could use this information to identify - or even actively send - similar telegrams in the future. This type of attack is often called *Replay Attack* since it works by reusing (replaying) previously used data telegrams.

In order to prevent this type of attack, either the telegram data or the security key must change to ensure that identical input data does not create identical encrypted radio telegrams. The mechanism used by the transmitter to change the telegram data or the security key has to be known to the receiver in order to correctly decrypt and authenticate received data telegrams.

The change of telegram data or security key is typically ensured by means of monotonously incrementing counters. The value of such counter is then used to either modify the telegram payload or the security key. EnOcean systems use the latter approach.

For this scheme it is important that the counter on the transmitter and on the receiver side remain synchronized, i.e. will always have the same values. Both counters will therefore have to start based on the same value and both have to be incremented whenever a data telegram is exchanged.

In order to guard against the case of telegrams being lost (not correctly received), the receiver needs to check if the received telegram has been decrypted correctly based on the counter value being used. This check can be done for via the message signature (MAC) or by other message integrity checks, e.g. based on *Cyclic Redundancy Codes*.

If a message is detected as non-valid based on the current counter value, the receiver can retry using the next counter value and so on. Typically, a maximum number of future counter values to be tried will be defined. This parameter is often referred to as the *Rolling Code Window Size*. If message decryption based on a future counter value is successful then the counter will be set to this value, thereby re-synchronizing the transmitter and receiver counters. Figure 11 below shows this mechanism.
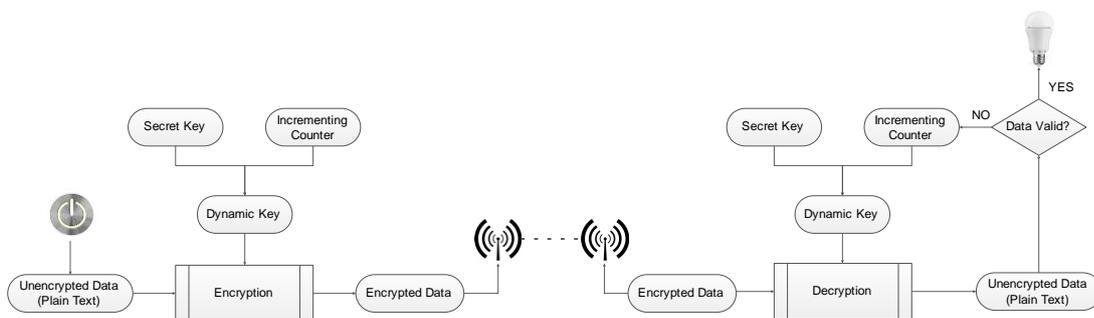
Figure 11 – Dynamic security key modification

6.2   TCM 515 implementation specifics

6.2.1   High level architecture

TCM 515 supports all three security mechanisms outlined above and can manage secure connection to up to 32 remote devices.

For each such connection, TCM 515 can maintain separate security key and rolling code information for the communication to the remote device (outbound, transmission) and for communication from the remote device (inbound, reception). All required information is stored in the so-called secure link table which has 32 entries.

Figure 12 below illustrates the two different directions of secure communication.
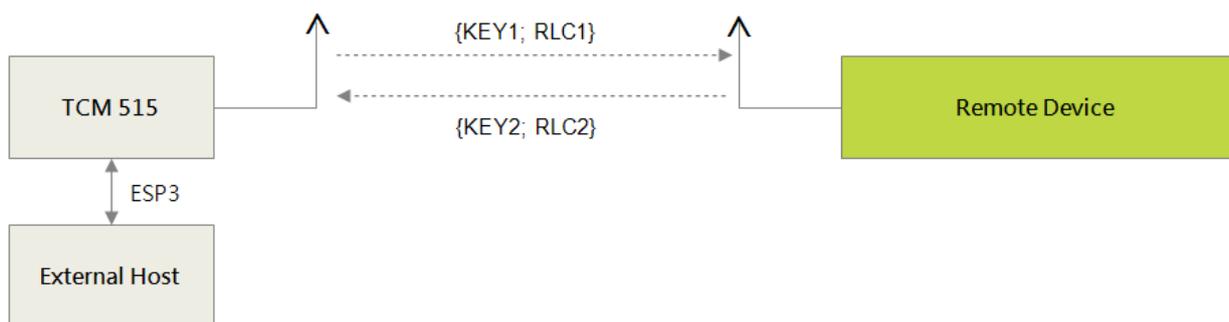
Figure 12 – Secure communication flow

TCM 515 – ENOCEAN TRANSCEIVER GATEWAY MODULE

6.2.2   High level execution flow

TCM 515 can automatically decrypt and authenticate messages originating from taught-in remote devices transmitting messages according to the EnOcean Network Security specification.

Security processing requires the receiver to know the security key and the latest rolling code counter. Therefore this is only possible for devices that have previously been taught-in.

If a high security radio telegram is received from a device that has not been taught in then TCM 515 will report a security event and forward the raw (unprocessed) telegram to the host for further analysis.

Figure 13 below illustrates the high level processing flow for received EnOcean high security radio telegrams.
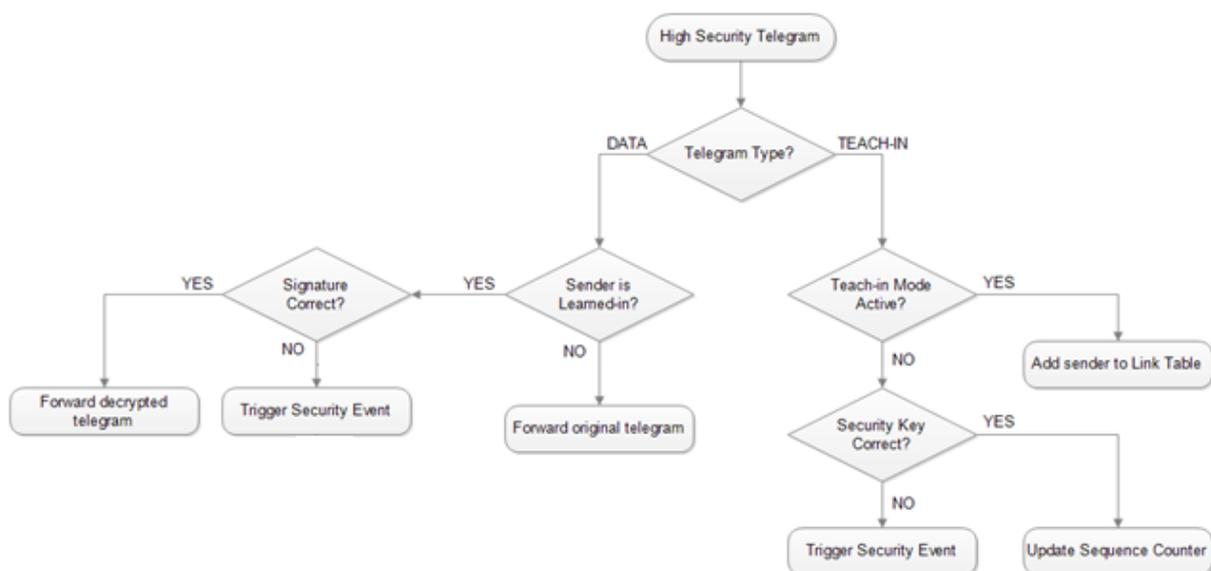
Figure 13 – TCM 515 high security telegram processing flow

TCM 515 – ENOCEAN TRANSCEIVER GATEWAY MODULE

6.2.3   Secure link table

TCM 515 stores all required information for secure communication with a remote device in the secure link table. This table can store up to 32 entries in order to manage secure connection to up to 32 remote devices.

Figure 14 below shows the structure of the secure link table.

Index	Remote Device ID	Direction	Security Key	Rolling Code	CMAC Error Counter	Teach-In Info	Security Format
0	ID0	Inbound (RX)	KEY0_I	RLC0_I	CMAC_ERR_CNT0	TI0	SLF0
		Outbound (TX)	KEY0_O	RLC0_O	Not Used		
1	ID1	Inbound (RX)	KEY1_I	RLC1_I	CMAC_ERR_CNT1	TI1	SLF1
		Outbound (TX)	KEY1_O	RLC1_O	Not Used		
2	ID2	Inbound (RX)	KEY2_I	RLC2_I	CMAC_ERR_CNT2	TI2	SLF2
		Outbound (TX)	KEY2_O	RLC2_O	Not Used		
				...			
31	ID31	Inbound (RX)	KEY31_I	RLC31_I	CMAC_ERR_CNT31	TI31	SLF31
		Outbound (TX)	KEY31_O	RLC31_O	Not Used		

Secure Link Table Structure

Figure 14 – Secure link table structure

6.2.3.1 Secure link table parameters

Each entry in the secure link table contains the following parameters:

- **Index**
  The index indicates the location of the entry in the secure link table. The table will be filled starting with Index = 0 and is full once Index = 31

- **Remote Device ID**
  Remote Device ID identifies the device with which TCM 515 can communicate securely based on the parameters for this entry

- **Direction**
  For each remote device, different parameters can be used for outbound (transmission) and inbound (reception) direction

- **Security Key**
  The security key is 16 byte long will can be used both for encryption and authentication

- **Rolling Code**
  The rolling code (RLC) is used to constantly modify the security key to avoid message replay. The rolling code is initialized to 0 at the time of production and increases for each transmission of a secure telegram.

- **Wrong CMAC Counter**
  The wrong CMAC counter monitors for each sender in the inbound link table the number of consecutive telegrams with incorrect CMAC. Typically a wrong CMAC is either due to the use of an incorrect key or due to the RLC being outside of the RLC window.

- **Teach-in Info**
  This field contains information about the device type (specifically if this is a rocker switch or not and if A or B side of the rocker switch were used for teach-in)

- **Security Level**
  The security level specifies the type of encryption and authentication used by for the communication with the remote device as described below. For bi-directional communication, the same Security Level has to be used for inbound and outbound connection.

TCM 515 – ENOCEAN TRANSCEIVER GATEWAY MODULE

6.2.3.2 Behaviour of outbound RLC after power loss

The constant part of the secure link table entries are stored in external EEPROM in order to preserve their content (device addresses, security keys, configuration flags) in case of a temporary power loss.

In contrast to that, the RLC value – which is incremented for each transmitted or received telegram – is buffered in internal SRAM to optimize encryption and decryption performance. The latest RLC value of a link table entry is written back to EEPROM once for every 64 telegrams that have been sent (outbound link table) or received (inbound link table) for that entry.

Should TCM 515 encounter a power loss then the RLC for each entry in the outbound link table will be incremented by 64 to account for the possibility that the last stored RLC might be too low by up to 63 (if power loss occurred directly before the next scheduled RLC storage).

If TCM 515 is continuously power-cycled such that it is only active during a brief period for the transmission of one or several telegrams then the transmitted RLC will "jump" by up to 64 every time the device is powered up and transmits a telegram. This can be avoided – if necessary - by storing the correct RLC in the external host and modifying the outbound link table entry to the correct RLC using the CO_WR_SECUREDEVICE_ADD command.

TCM 515 – ENOCEAN TRANSCEIVER GATEWAY MODULE

6.2.4 Secure EEP support

Radio telegrams using security mechanisms can be identified via their EEP (EnOcean Equipment Profile). Each such EEP is identified using three fields:

■ RORG
RORG identifies the high level telegram type, e.g. rocker switch telegram, four byte sensor telegram, variable length telegram etc.

■ FUNC
FUNC identifies the function group to which this telegram belongs, e.g. the function group of temperature sensors within the four byte sensor telegram type

■ VARIANT (or TYPE)
VARIANT (which is confusingly also called TYPE) identifies the exact sensor variant within the function group, e.g. a 0 °C – 40 °C temperature sensor that is defined within the function group of temperature sensors

Figure 15 below shows the structure of the EEP identifier.

RORG	FUNC	VARIANT
0x00 … 0xFF	0x00 … 0x3F	0x00 … 0x7F
8 bit	6 bit	7 bit
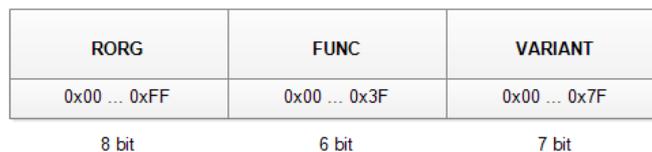
Figure 15 – EEP identifier structure

The EEP identifier is typically only transmitted during the initial teach-in (paring) between devices. For special cases (e.g. devices using more than one EEP), data telegrams might specify the EEP that is used.

The security processing in TCM 515 supports both secure messages that specify the original telegram type (RORG) and those who don't. Table 8 below summarizes the different RORG supported by TCM 515 security processing.

RORG	Description
0x30	Secure message that does not identify the type (RORG) of the encrypted telegram
0x31	Secure message that does identify the type (RORG) of the encrypted telegram
0x32	Message that results from the decryption of a secure message with RORG = 0x30 (secure message that does not identify the type (RORG) of the encrypted telegram)
0x35	Secure teach-in telegram

Table 8 – RORG supported by the security implementation in TCM 515

TCM 515 – ENOCEAN TRANSCEIVER GATEWAY MODULE

6.3 Supported security features

The SLF (Security Level Format) specifies the parameters of the encryption, authentication and rolling code algorithms used for communication with a specific device.

The SLF is communicated as part of a secure teach-in telegram and stored in the secure link table (see chapter 0). Figure 16 below shows the supported security parameters options encoded in the SLF field.

7	6	5	4	3	2	1	0
RLC_ALGO		**RLC_TX**	**MAC_ALGO**		**DATA_ENC**		
0 – No RLC algorithm		0 - No	0 – No MAC		0 – No data encryption		
1 – 16-bit x = (x+1)		1 - Yes	1 – AES128 3 byte		1 – N/A		
2 – 24-bit x= x+1			2 – AES128 4 byte		2 – N/A		
3 – N/A			3 – N/A		3 – VAES – AES128		
					4 – AES-CBC – AES128		

Figure 16 – SLF structure

6.3.1 Telegram encryption and decryption

TCM 515 can encrypt and decrypt radio telegrams using AES 128 based on a 16 byte security key that is dynamically modified using a rolling code as described in chapter 6.3.3.

TCM 515 supports both VAES and AES-CBC modes for encryption and decryption. The mode which is used can be selected using the DATA_ENC field in the SLF as described above.

Refer to the "Security of EnOcean Networks" specification for details about the VAES and AES-CBC modes.

TCM 515 – ENOCEAN TRANSCEIVER GATEWAY MODULE

6.3.2 Telegram authentication

TCM 515 can authenticate the content of received telegrams based on the telegram signature (CMAC), the security key and a rolling code as described in chapter 6.1.2. Additionally, TCM 515 can calculate the signature and add it to transmitted telegrams according to the same mechanism.

TCM 515 supports signature lengths of 3 byte and 4 byte. The signature length is identified by the MAC_ALGO field of the security level format that is transmitted during teach-in (see chapter 6.3).

MAC_ALGO encodes the following options:

- MAC_ALGO = 0: No CMAC is included in the secure telegram

- MAC_ALGO = 1: CMAC is a 3 byte long signature

- MAC_ALGO = 2: CMAC is a 4 byte long signature

Refer to the "Security of EnOcean Networks" specification for details about the CMAC modes.

6.3.3 Rolling code support

TCM 515 supports the dynamic modification of a given security key with a rolling code as described in chapter 6.1.3.

TCM 515 supports rolling code sizes of both 2 byte and 3 byte. Use of 2 byte rolling code size is not recommended anymore for new developments.

The rolling code size is identified by the RLC_ALGO field of the Security Level Format (SLF) field that is transmitted during teach-in (see chapter 6.4.1).

RLC_ALGO encodes the following options:

- If RLC_ALGO = 1 then a 2 byte long rolling code is used

- If RLC_ALGO = 2 then a 3 byte long rolling code is used

Refer to the "Security of EnOcean Networks" specification for details about the Rolling Code modes.

6.3.3.1 Explicit versus implicit rolling code

The rolling code used to transmit a specific telegram might be transmitted as part of the telegram. This case is called "explicit rolling code" and is the recommended setting.

For the purpose of conserving energy, the transmission of the rolling code used to transmit a specific telegram might be omitted after the initial teach-in (during which the current value of the rolling code is transmitted). This case is called "implicit rolling code".

The RLC_TX field defines if the rolling code is transmitted in the RLC field as part of the secure telegram. RLC_TX encodes the following options:

- If RLC_TX = 0 then secure telegrams do not include the rolling code

- If RLC_TX = 1 then secure telegrams do include the rolling code

If an implicit rolling code strategy is used then the receiver has to keep track of the expected rolling code based on the initial rolling code and the number of telegrams that have been received since then.

The receiver has to account for the option that it might miss one or several messages for instance because the distance between transmitter and receiver exceeds the transmission range or because the power supply to the receiver is temporarily lost. This will result in different values for the rolling code counter on the transmitter and the receiver side. More specifically, the rolling code counter of the transmitter will then be higher than that of the receiver with the difference being the amount of telegrams that have not been correctly received by the receiver.

In these cases, the receiver can test several consecutive rolling codes to check if the used rolling ode leads to a matching signature (CMAC). If the calculated CMAC matches the transmitted CMAC then the RLC is correct. Otherwise the next RLC can be tested.

The maximum number of RLC that will be tested under such schemes is called the RLC window. The size of the RLC window is 128. The size of the RLC window can be temporarily changed (increased) in order to attempt resynchronization using ESP3 Command Code 33: CO_WR_TEMPORARY_RLC_WINDOW. This increased RLC window is only applied to the first telegram received for each address in the inbound link table after the reception of this command. Refer to the ESP3 documentation for reference.

If the RLC window has been exhausted without successfully decrypting and authenticating the message then the message will be discarded. In order to re-synchronize the RLC between transmitter and receiver, the transmitter must send a teach-in telegram. The receiver – upon receiving a valid teach-in telegram from a previously taught-in transmitter – will adjust its own RLC to the one specified in the teach-in telegram.

TCM 515 – ENOCEAN TRANSCEIVER GATEWAY MODULE

6.4 Teach-in of secure devices

Teach-in is the process by which a remote device communicates to TCM 515 all parameters required to establish secure communication.

Until secure communication has been established, TCM 515 will transparently forward received telegram to the external host via UART and transmit telegrams it has received from the external host.

If secure communication between a remote device and TCM 515 has been established then TCM 515 will handle all security-related functionality such as encryption, decryption, authentication and rolling code management. This greatly facilitates the implementation of secure communication in resource-constrained applications such as simple actuators.

Teach-in can be performed in two different ways:

- Using a teach-in telegram
  TCM 515 can automatically extract all required parameters for receiving and authenticating data from a dedicated telegram, the so-called teach-in telegram.
  Conversely, TCM 515 can be instructed via its ESP3 interface to transmit such teach-in telegram to a remote device.

- Using an ESP3 command
  All required parameters for the correct transmission and reception of secure telegrams by TCM 515 can be configured via ESP3 command

Both possibilities are described in more detail now.

6.4.1   Teach-in of secure devices with teach-in telegram

Teach-in is the process by which a remote device communicates to TCM 515 all parameters required to establish secure communication.

The format of a secure teach-in message is shown in Figure 17 below.

Figure 17 – Secure teach-in telegram structure

The key parameters communicated in such secure teach-in telegram are the following:

- RORG
  Secure teach-in telegrams are identified by the RORG 0x35, see chapter 6.2.3.2

- Teach-in Info
  This field contains information about the device type (specifically if this is a rocker switch or not and if A or B side of the rocker switch were used for teach-in)

- Security Level
  The security level specifies the type of encryption and authentication used by for the communication with the remote device as described below.

- Rolling Code
  The rolling code is used to constantly modify the security key to avoid message re-play. The rolling code is initialized to 0 at the time of production and increases for each transmission of a secure telegram.

- Security key
  The 128 bit AES security key is used in high security mode to encode and / or au-thenticate radio telegrams

TCM 515 can be configured to automatically accept secure teach-in telegrams and store these parameters in the secure link table by enabling the so-called Learn Mode. Learn mode can be enabled for a specific period of time (default is 60 seconds) using the CO_WR_LEARNMODE command.

If a valid teach-in telegram is received while learn mode is active then the relevant parameters are added to the secure link table. The maximum number of remote devices that can be learned-in (having above parameters stored in the link table for security processing) is 32. Attempting to teach in additional devices will result in a CO_EVENT_SECUREDEVICES with error code 00 (Teach in failed, because no more space available).

TCM 515 can be configured to transmit a secure teach-in telegram to a remote device that has been setup in the outbound link table using the CO_WR_SECUREDEVICE_SENDTEACHIN command.

6.4.1.1 Handling of teach-in telegram when not in teach-in mode

If TCM 515 is not in teach-in mode then teach-in requests from unknown devices are ignored.

If TCM 515 receives a teach-in message from a known (previously taught-in) device with the correct security key then the sequence counter information in the TCM 515 secure link table is updated. This approach is used in case sequence counters of receiver and sender become desynchronized.

6.4.2 Teach-in of secure devices using ESP3

The security parameters required for secure communication with a remote device can also be setup by the external host via the ESP3 interface.

This approach is always used for the case of outbound communication (from TCM 515 to the remote device).

This approach might also be used (instead of relying on secure teach-in telegrams) for inbound communication (from the remote device to TCM 515) if the relevant parameters are known to the local host. This could for instance be the case if the security information of the remote device has been read by the host from a QR code on the remote device.

Secure device communication parameters can be added to the link table of TCM 515 using the CO_WR_SECUREDEVICE_ADD command.

TCM 515 – ENOCEAN TRANSCEIVER GATEWAY MODULE

6.5 Reporting of security-related events

TCM 515 can report to the host the following security-related events by means of a CO_EVENT_SECUREDEVICES event message. The structure of the CO_EVENT_SECUREDEVICES messages is shown below.

Group	Offset	Size	Field	Value hex	Description
-	0	1	Sync. Byte	0x55	
Header	1	2	Data Length	0x0006	6 bytes
	3	1	Optional Length	0x00	0 byte
	4	1	Packet Type	0x04	EVENT = 4
-	5	1	CRC8H	0xnn	
Data	6	1	Event Code	0x05	CO_EVENT_SECUREDEVICES = 5
	7	1	Event Cause	0xnn	**00** = Teach in failed because no more space is available in the secure link table **02** = Resynchronization attempt with wrong private key **03** = Configured count of telegrams with wrong CMAC received **04** = Teach-in failed due to incorrect teach-in telegram content or format **07** = CMAC or RLC not correct **08** = Standard telegram received from device in secure link table **Others** = reserved or not supported
	8	4	Device ID	0xnnnnnnnn	Device ID
-	12	1	CRC8D	0xnn	

Table 9 – Secure event reporting

The following reporting codes are supported by TCM 515:

■ 00 = Teach in failed
No more space is available in the secure link table

■ 02 = Resynchronization attempt with wrong private key
Secure teach in telegram received with non-matching security key from device already in the link table

■ 03 = Configured count of telegrams with wrong CMAC received
128 messages with wrong CMAC have been received from the same sender

■ 04 = Teach-In failed
The teach-in telegram did not have the expected structure and content

■ 07 = CMAC or RLC not correct
The received CMAC did not match the expected CMAC after exhausting all RLC within the RLC window

■ 08 = Standard Telegram from device in secure link table

TCM 515 – ENOCEAN TRANSCEIVER GATEWAY MODULE

7 Remote Management

TCM 515 provides a transparent radio channel also for remote management messages with a message length of up to 255 bytes. This enables an external micro controller connected to TCM 515 to handle remote management request from external devices or to control other devices via remote management.

For more information on remote management please refer to the EnOcean End Equipment Profiles (EEP) 2.6 specification.

TCM 515 – ENOCEAN TRANSCEIVER GATEWAY MODULE

8 Device Integration

TCM 515 is designed for integration onto a host PCB. Detailed Gerber data of the device footprint is available from EnOcean.

8.1 Recommended PCB Footprint

Figure 18 below shows the recommended PCB footprint for TCM 515.
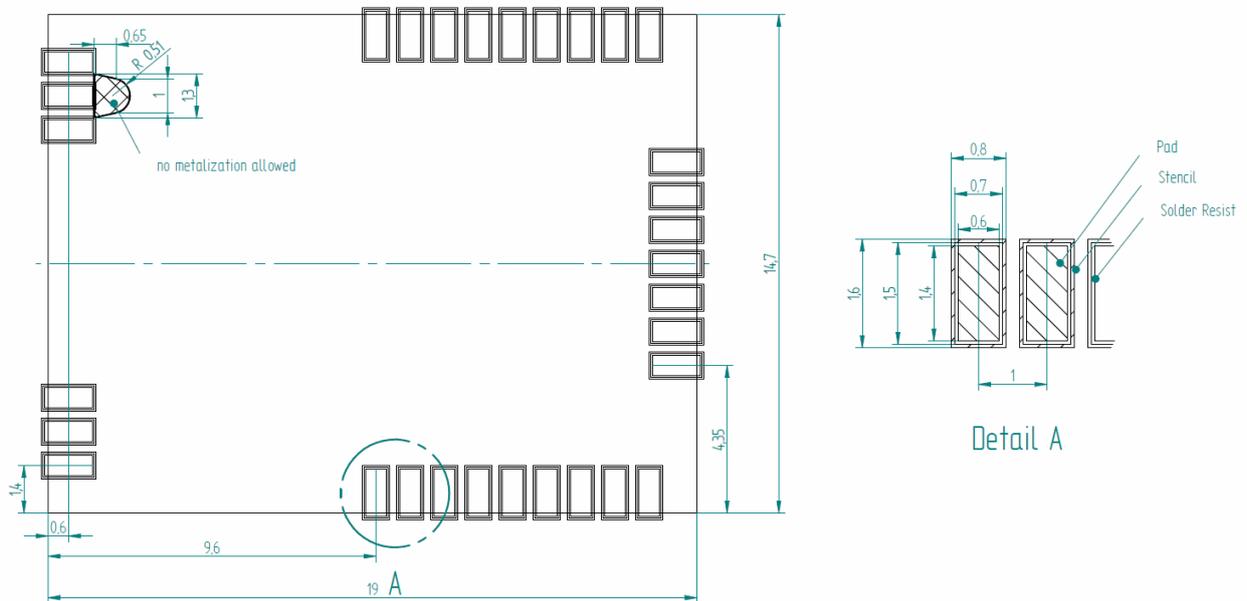
Figure 18 – Recommended PCB footprint

TCM 515 – ENOCEAN TRANSCEIVER GATEWAY MODULE

8.2 Device outline

Figure 19 below shows the device outline of TCM 515.
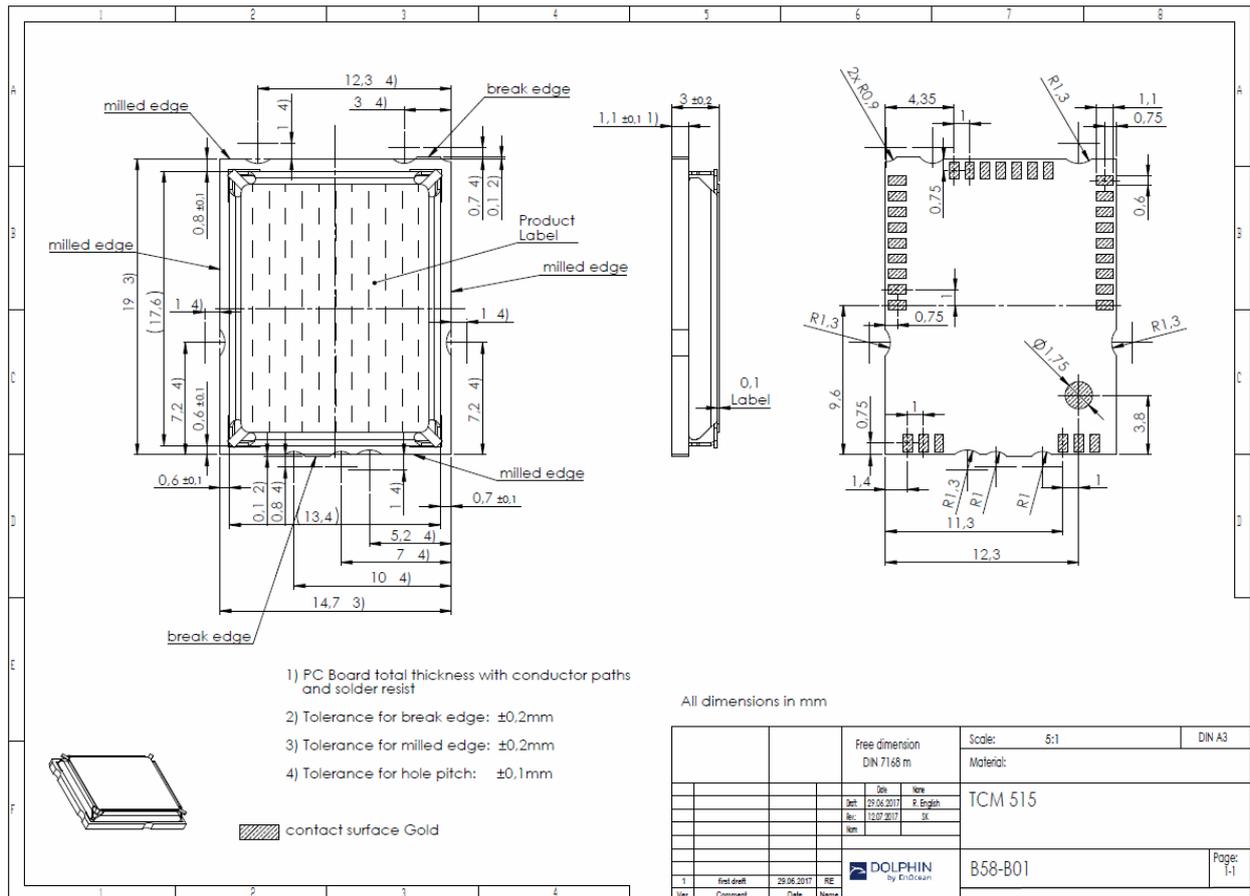
Figure 19 – Device outline

8.3   Soldering information

TCM 515 shall be soldered according to IPC/JEDEC J-STD-020C standard.

Profile Feature	Pb-Free Assembly
Average Ramp-Up Rate (Ts_{max} to Tp)	3° C/second max.
Preheat – Temperature Min (Ts_{min}) – Temperature Max (Ts_{max}) – Time (ts_{min} to ts_{max})	150 °C 200 °C 60-180 seconds
Time maintained above: – Temperature (T_L) – Time (t_L)	217 °C 60-150 seconds
Peak/Classification Temperature (Tp)	260 °C
Time within 5 °C of actual Peak Temperature (tp)	20-40 seconds
Ramp-Down Rate	6 °C/second max.
Time 25 °C to Peak Temperature	8 minutes max.

Note 1: All temperatures refer to topside of the package, measured on the package body surface.
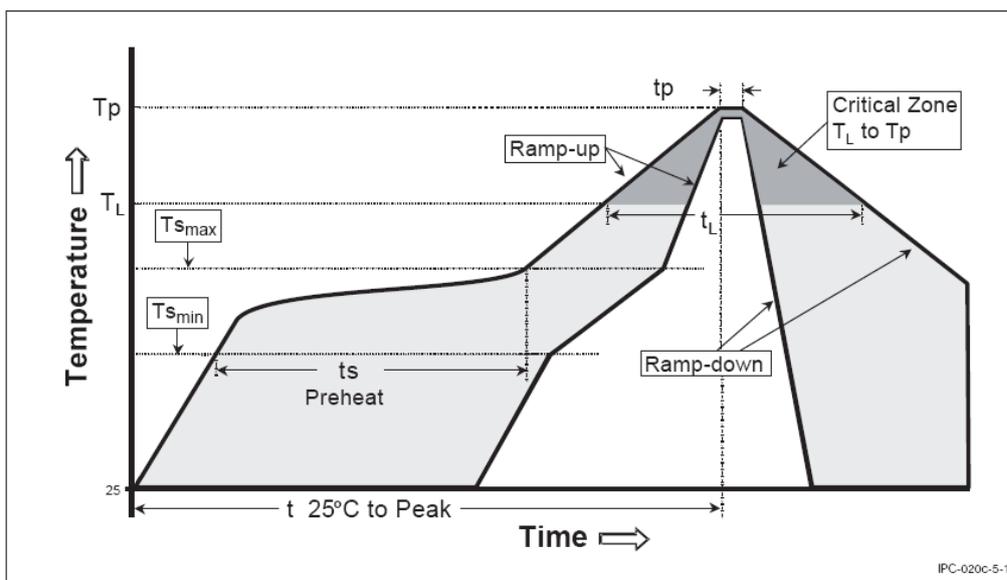

Figure 20 – Recommended soldering profile

TCM 515 shall be handled according to Moisture Sensitivity Level MSL4 which means a floor time of 72 h. TCM 515 may be soldered only once, since one time is already consumed at production of the module itself.

Once the dry pack bag is opened, the desired quantity of units should be removed and the bag resealed within two hours. If the bag is left open longer than 30 minutes the desiccant should be replaced with dry desiccant. If devices have exceeded the specified floor life time of 72 h, they may be baked according IPC/JEDEC J-STD-033B at max. 90°C for less than 60 h.

Devices packaged in moisture-proof packaging should be stored in ambient conditions not exceeding temperatures of 40 °C or humidity levels of 90% r.H.

TCM 515 modules shall be soldered within 6 months after delivery!

TCM 515 – ENOCEAN TRANSCEIVER GATEWAY MODULE

8.4   Packaging information

TCM 515 is delivered in Tape & Reel packaging with 250 units per reel. Figure 21 below illustrates the dimensions.

**Figure 21 – Tape & Reel dimensions of TCM 515**

Figure 22 below shows the positioning of TCM 515 in the Tape & Reel packaging.

Figure 22 – Position of TCM 515 in the reel

TCM 515 – ENOCEAN TRANSCEIVER GATEWAY MODULE

8.5 Layout recommendations

⚠️ The length of lines connected to I/O signals should not exceed 5 cm.

⚠️ It is recommended to have a complete GND layer in the application PCB, at least in the area below the module and directly connected components (e.g. mid-layer of your application PCB).

⚠️ Due to non-isolated test points there are live signals accessible on the bottom side of the module. We suggest avoiding any copper structure in the area directly underneath the module (top-layer layout of your application PCB). If this is not possible in your design, please provide coating on top of your PCB to prevent short circuits to the module. All bare metal surfaces including vias have to be covered (e.g. adequate layout of solder resist).

⚠️ Distortive signals (e.g. bus signals or power lines) should not be routed underneath the module. If such signals are present in your design, we suggest separating them by using a ground plane between module and these signal lines.

⚠️ For applications with strong external noise sources (e.g. gateways with LTE functionality) it is strongly recommended to use an external SAW filter. See chapter 8.8.

⚠️ If distortion / radiated noise cannot be minimized to acceptable levels then consider also using the adjustable internal noise filter. See chapter 8.8.

8.6 Power supply requirements

In order to provide a good radio performance, great attention must be paid to the power supply and a correct layout and shielding. It is recommended to place a 22 µF ceramic capacitor between VDD and GND close to the module (material: X5R, X7R, min 6.3 V to avoid derating effects).

In addition, an HF SMD EMI Suppression Ferrite Bead such as the Würth WE-CBF HF SMD EMI Suppression Ferrite Bead (Würth order number 742863160) shall be inserted in the power supply line.

For best performance it is recommended to keep the ripple on the power supply rail below 10 mVpp.

Radiated emissions from power supply inductors (especially DCDC inductors) towards the TCM 515 RF input must be minimized as they impact RF performance. Place such inductors as much as possible away from TCM 515 or – if this is not possible – consider using switched capacitor designs.

TCM 515 integrates approximately 10 uF of capacitance for filtering the internal supply voltage bus. The power supply architecture has to be capable of supplying sufficient current to charge this capacitance during power up.

8.7 Using an SAW Filter with TCM 515 (868 MHz version only)

Applications using the 868 MHz (EU) frequency band can be affected by strong external noise sources such as LTE modems or RFID scanners operating in the 860 MHz band.

For best performance, TCM 515 has to be separated as far as possible from such noise sources. Additionally, the use of an external SAW filter is strongly recommended if such noise sources might be present. The recommended SAW filter is B3744 from RF360JV (Qualcomm / TDK joint venture).

At the time of writing, documentation about B3744 was available under the following link: https://en.rf360jv.com/inf/40/ds/ae/B3744.pdf

The recommended application circuit for B3744 is shown in Figure 23 below.
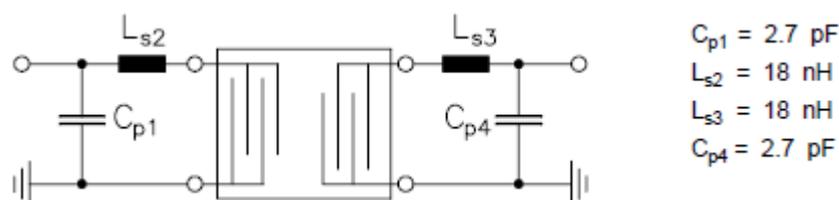
Figure 23 – SAW application circuit for 868 MHz

TCM 515 – ENOCEAN TRANSCEIVER GATEWAY MODULE

8.8 Low noise design considerations

For best performance, HW design of TCM 515 systems has to minimize radiated or conducted noise that interferes with the correct reception of RF signals. Strong emphasis should therefore be placed onto good RF and power supply design to eliminate or minimize the level of noise introduced into the RF path.

In addition, special consideration should be used to minimize periodic noise sources (such as radiated noise from DCDC inductors) in TCM 515 based systems. Those systems transmit and receive signals using amplitude shift keying (868.3 MHz ASK) where the amplitude of a carrier frequency (868.3 MHz) is changed according to the encoded bit value (0 = high amplitude or 1 = low amplitude).

Periodic noise signals where the time period between high and low signal states is close to the symbol duration of 8us can be erroneously interpreted as the preamble of an ASK telegram (10101010 sequence) and therefore prevent correct reception of other ASK telegrams that are received at the same time.

Using HW filtering (separate signal lines and sufficient ground plane in the layout, decoupling and filtering on the power supply, implementation of SAW filter in the antenna path) should always be the first priority to minimize the performance degradation due to noise.

In some applications it might not be possible to sufficiently minimize external noise due to space or design constraints. For those cases, TCM 515 provides an adjustable noise filter. This noise filter can be configured via ESP3 using the CO_SET_NOISETHRESHOLD command to reject input noise below the configured minimum signal strength. The structure of the ESP3 command CO_SET_NOISETHRESHOLD is shown below.

-	0	1	Sync. Byte	0x55	
Header	1	2	Data Length	0x0002	2 bytes
	3	1	Optional Length	0x00	0 byte
	4	1	Packet Type	0x05	COMMON_COMMAND = 5
-	5	1	CRC8H	0xnn	
Data	6	1	COMMAND Code	0x32	CO_SET_NOISETHRESHOLD = 50
	7	4	RSSI level	0xnn	RSSI Level to initiate telegram detection
-	11	1	CRC8D	0xnn	

Table 10 – CO_SET_NOISETHRESHOLD command structure

TCM 515 – ENOCEAN TRANSCEIVER GATEWAY MODULE

The noise threshold is encoded as positive offset from the theoretical noise minimum (-146 dBm) as shown in the table below. The default value is 0x32 (-96 dBm).

Value	Noise Threshold
0x2E	-100 dBm
0x2F	-99 dBm
0x30	-98 dBm (Default value TCM 515U)
0x31	-97 dBm
0x32	-96 dBm (Default value TCM 515)
0x33	-95 dBm
0x34	-94 dBm
0x35	-93 dBm
0x36	-92 dBm
0x37	-91 dBm
0x38	-90 dBm

Table 11 – Noise threshold encoding for CO_SET_NOISETHRESHOLD

For environments with strong noise which cannot be sufficiently reduced, consider using an external SAW filter as described in chapter 8.7 to minimize out of band noise. Alternatively, consider using a TCM 310 device which integrates an SAW filter.

8.9   Suggested Reset circuit

TCM 515 can be reset by pulling the nRST pin (active low) to Ground. TCM 515 integrated a weak (50kΩ) pull-up resistor that will maintain the internal nRST input active high (not active).

In order to avoid spurious reset events, it is recommended to filter the input signals by means of a small capacitor which is placed as close as possible to the TCM 515 nRST pin as shown in Figure 24 below.
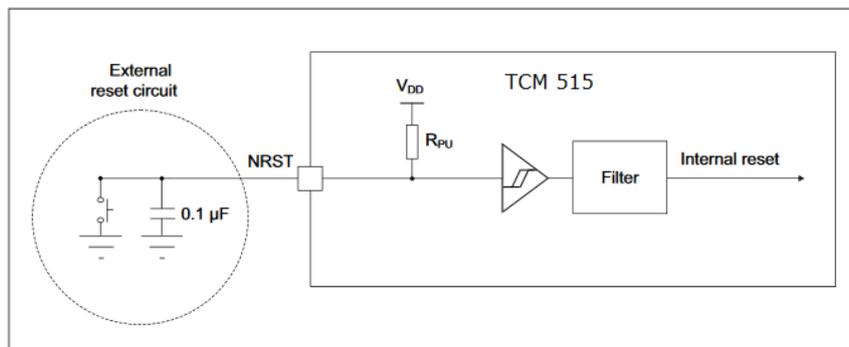

Figure 24 – Recommended reset circuit

The reset pulse should have a duration of at least 1 ms in order to guarantee reliable reset operation.

9 Antenna options

This chapter outlines options for antenna that can be used with TCM 515. Note that this chapter is for guidance purposes only, please consult with an authorized certification body for specific information.

9.1 Antenna options for 868 MHz (European Union)

In order to be compliant with the Radio Equipment Directive (RED) of the European Union, an antenna needs to fulfil at least following requirements to be usable with TCM 515:

Frequency band	868.300 MHz ISM	Antenna must be suited for this band
Antenna type	Passive	Mandatory for radio approval
Impedance	~50 Ohm	Mandatory for radio approval
Maximum gain	≤ 0 dBd	Mandatory for radio approval

In addition, it is important to fulfill the following requirements in order to achieve compatibility with other EnOcean products and to ensure EMI robustness:

VSWR	≤ 3:1	Important for compatibility with EnOcean protocol
Return Loss	> 6 dB	Important for compatibility with EnOcean protocol
Bandwidth	≤ 20 MHz	Important if 10 V/m EMI robustness required for device

See chapter 11.1 for additional important remarks regarding RED certification.

TCM 515 – ENOCEAN TRANSCEIVER GATEWAY MODULE

9.1.1 Whip antenna

TCM 515 modules have been certified for use with a whip antenna under EU (RED) regulations. Figure 25 below shows key whip antenna parameters.
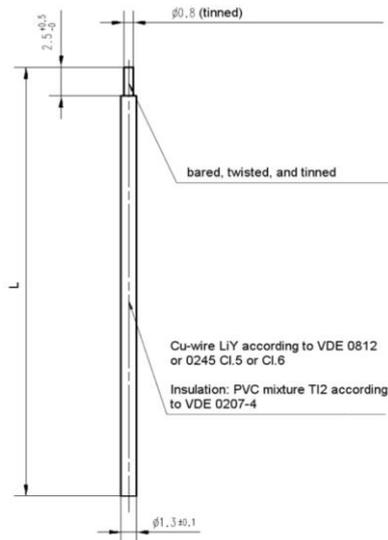

Figure 25 – Whip antenna parameters

The whip antenna has to meet the following parameters in order to be compliant to the regulations mentioned above:

- Antenna length (L): 86 mm wire, connect to RF_50
- Minimum GND plane: 38 mm x 18 mm
- Minimum distance space: 10 mm

9.2 Antenna options for 902 MHz (US / Canada)

TCM 515U has been tested and certified with a number of antennas as described below. A separate approval is required for all other operating configurations, including portable configurations with respect to Part 2.1093 and different antennas.

9.2.1 Whip antenna

TCM 515U has been certified for use with a whip antenna which meets the following parameters (see Figure 25):

- Antenna length (L): 64 mm wire, connect to RF_50
- Minimum GND plane: 50 mm x 50 mm
- Minimum distance space: 10 mm

9.2.2 Helical antenna

TCM 515U has been certified for use with the ANT 300 helix antenna from EnOcean which uses the following parameters (see Figure 26):

- Shape according to drawing below
- Minimum GND plane: 35 mm x 30 mm
- Minimum distance space: 10 mm
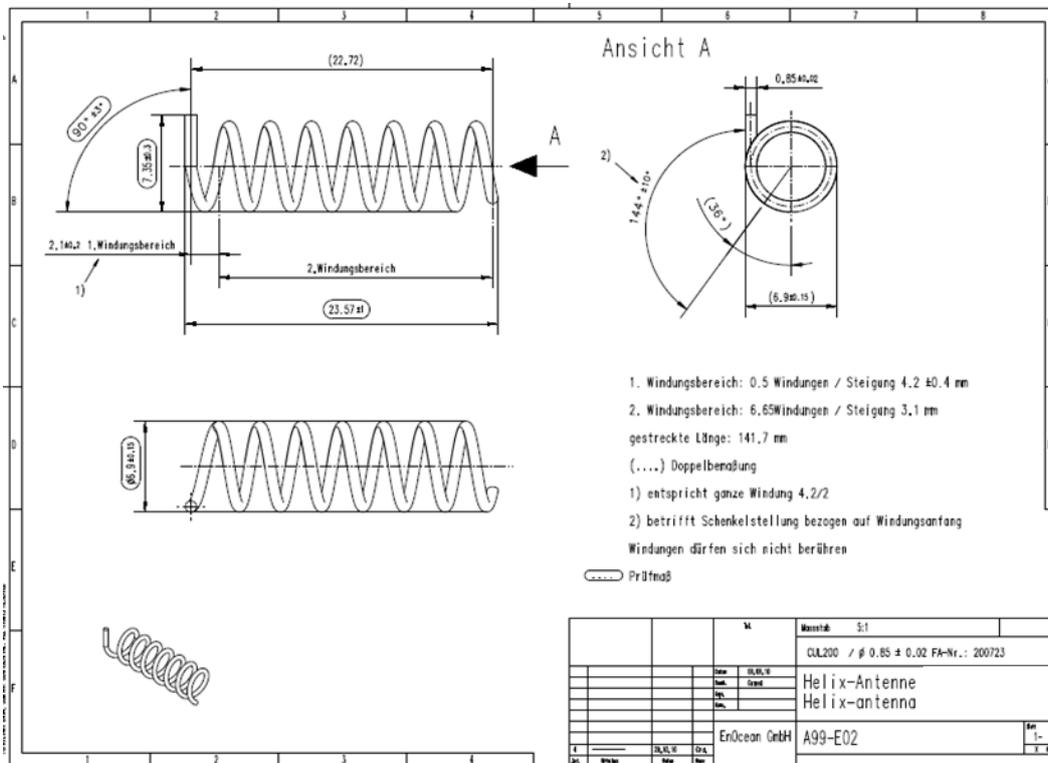
Figure 26 – Helix antenna parameters

TCM 515 – ENOCEAN TRANSCEIVER GATEWAY MODULE

9.2.3   Chip antenna (Supplier: Mitsubishi Material, Type AM11DP-ST01T)

TCM 515U has been certified for use with the chip antenna AM11DP-ST01T from Mitsubishi Material provided that the following layout guidelines are met:

- Dimensions may not be shortened

- Matching circuit is part of the single modular approval and may not be changed

- Matching circuits values: L2 = 33 nH; L3 = 3,9 nH, L4 = 12 nH

- Use High Q wire wound inductors, e.g. 0603 Murata LQW18A series

- Minimum top and bottom side ground plane required as shown below

- Connect ground planes using multiple via as shown in Figure 27

- Connect matching circuit to RF_50 pin

Figure 27 below shows the reference layout that has to be used.
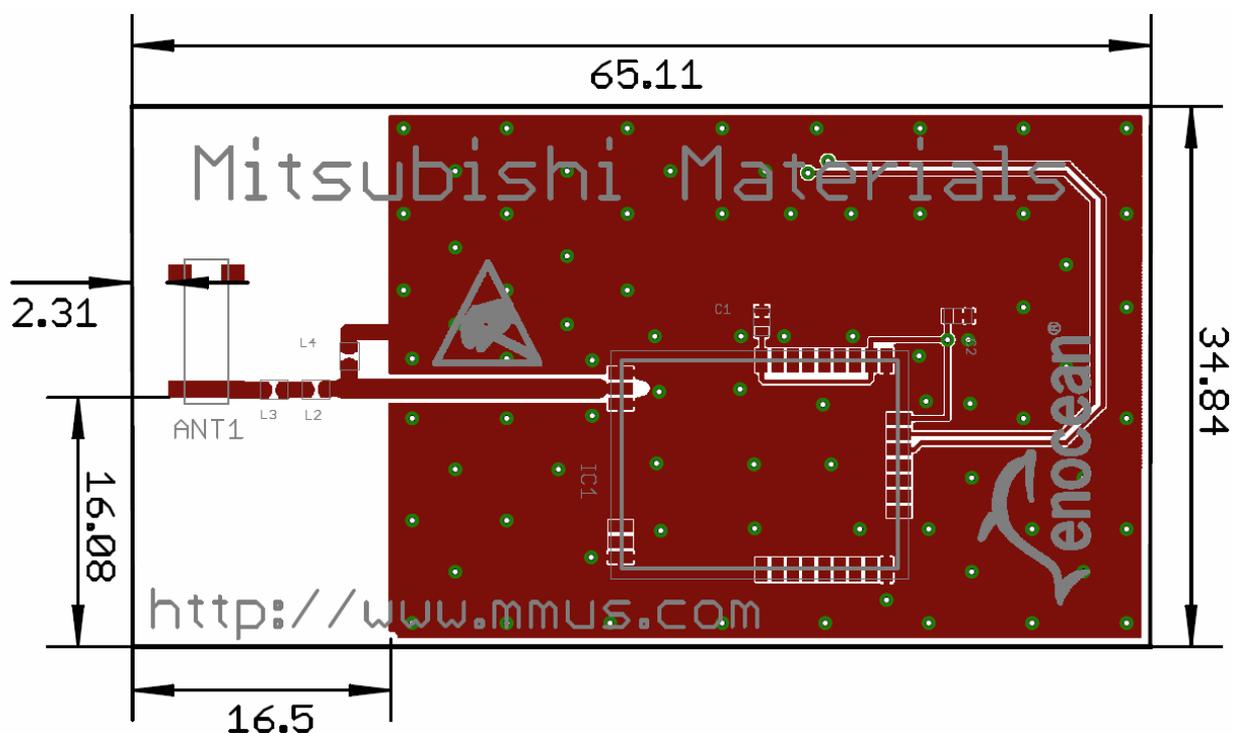
Figure 27 – Required layout for AM11DP-ST01T

For any further questions or chip antenna quotes, please refer to Mitsubishi Materials website at www.mmea.com or email to electroniccomponents@mmus.com.

TCM 515 – ENOCEAN TRANSCEIVER GATEWAY MODULE

9.2.4   Dipole antenna (ANT-916-CW-HWR-RPS)

TCM 515U has been certified for use with the dipole antenna ANT-916-CW-HWR-RPS from Linx provided that a non-standard connector such as RP-SMA-Female from Linx is used.

Figure 28 below shows ANT-916-CW-HWR-RPS from Linx.
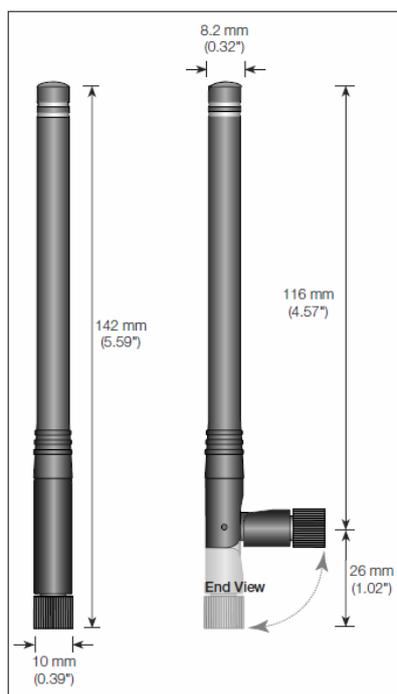
Figure 28 – ANT-916-CW-HWR-RPS

Figure 29 below shows RP-SMA- Female from Linx.
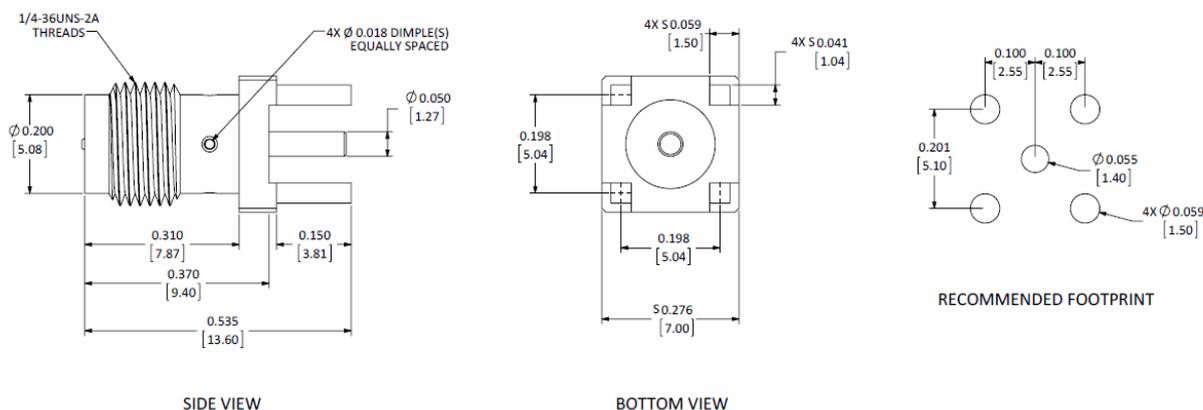
Figure 29 – RP-SMA-Female

10 Application information

10.1 Transmission range

The main factors that influence the system transmission range are:

- Type and location of the antennas of receiver and transmitter

- Type of terrain and degree of obstruction of the link path

- Sources of interference affecting the receiver

- "Dead spots" caused by signal reflections from nearby conductive objects.

Since the expected transmission range strongly depends on this system conditions, range tests should always be performed to determine the reliably achievable range under the given conditions. The following figures should be treated as a rough guide only:

- Line-of-sight connections
  Typically 30 m range in corridors, up to 100 m in halls

- Plasterboard walls / dry wood
  Typically 30 m range, through max. 5 walls

- Ferro concrete walls / ceilings
  Typically 10 m range, through max. 1 ceiling

- Fire-safety walls, elevator shafts, staircases and supply areas
  Such areas should be considered as screening.

The angle at which the transmitted signal hits the wall is very important. The effective wall thickness – and with it the signal attenuation – varies according to this angle. Signals should be transmitted as directly as possible through the wall. Wall niches should be avoided. Other factors restricting transmission range include:

- Switch mounting on metal surfaces (up to 30% loss of transmission range)

- Hollow lightweight walls filled with insulating wool on metal foil

- False ceilings with panels of metal or carbon fibre

- Lead glass or glass with metal coating, steel furniture

The distance between the receiver and other transmitting devices such as computers, WiFi routers, audio and video equipment that also emit high-frequency signals should be at least 0.5 m.

TCM 515 – ENOCEAN TRANSCEIVER GATEWAY MODULE

10.2 Maximum input power

The rated maximum input power for TCM 515 is -23 dBm in line with EnOcean Alliance air interface specification.

Under ideal conditions (free line of sight connection between two fully stretched whip antennas without any housing damping or obstruction) this input power level is equivalent to approximately 10 cm of distance between transmitter and receiver. If this input power level is exceeded then the telegram error rate might increase.

In actual products, the required minimum distance between transmitter and receiver is typically much less due to the damping introduced by the product housing of sender and receiver.

10.3 RSSI reporting

TCM 515 will report the signal strength (RSSI) for received telegrams as part of the ERP1 or ERP2 radio packet. This information can be treated as an indicator for the quality of the radio link keeping in mind that this is affected by a number of factors such as temporary fading or obstructions.

The RSSI reporting of TCM 515 works within a range from -90 dBm up to -40 dBm with an accuracy of approximately +- 2dBm.

If the input signal strength significantly exceeds a level of -40 dBm (corresponding to a distance of less than 1m between sender and receiver) then the reported signal strength might not be accurate anymore.

Specifically for TCM 515 (868.3 MHz ASK), the reported signal strength for input signals with very high power might be that of the low power state - and therefore significantly too low - as the signal strength of the low power state will be strong enough to trigger the RSSI detection mechanism.

TCM 515 – ENOCEAN TRANSCEIVER GATEWAY MODULE

11 Regulatory information

TCM 515 has been tested according to standards for RED (European Union) certification, FCC (US) and ISED (Canada) regulations.

11.1 RED (European Union)

The Radio Equipment Directive (2014/53/EU, typically referred to as RED) replaces the old R&TTE directive from 1999 as regulatory framework for radio products in the European Union. All products sold to final customers after 12th of June, 2017 have to be compliant to RED.

At the time of writing, the text of the RED legislation was available from this link:
http://eur-lex.europa.eu/eli/dir/2014/53/oj

Dolphin radio modules such as TCM 515 are components which are delivered to OEM manufacturers for their use in final or combined products.

It is the responsibility of the OEM manufacturer to demonstrate compliance to all applicable EU directives and standards. The attestation of conformity for TCM 515 serves as input to the declaration of conformity for the full product.

At the time of writing, guidance on the implementation of EU product rules – the so called "Blue Guide" – was available from this link:
http://ec.europa.eu/DocsRoom/documents/18027/

Specifically within the new RED framework, all OEM manufacturers have for instance to fulfill the following additional requirements:

- Provide product branding (on the product) clearly identifying company name or brand and product name as well as type, charge or serial number for market surveillance
- Include (with the product) documentation containing full postal address of the manufacturer as well as radio frequency band and max. transmitting power
- Include (with the product) user manual, safety information and a declaration of conformity for the final product in local language
- Provide product development and test documentation upon request

Please contact an accredited test house for detailed guidance.

The maximum transmitting power of TCM 515 using a whip antenna is +10.8 dBm.

11.1.1 RED Attestation of Conformity for TCM 515

Attestation of Conformity

We,

PKM electronic GmbH

confirm hereby that the product
(description of the apparatus, system, installation to which it refers)

Transceiver Modul
TCM 515

complies with

Used Standard(s):

EN301489-3:V1.6.1	Electromagnetic compatibility and Radio spectrum Matters (ERM); EMC standard for radio equipment and services; Part 3: Specific conditions for Short-Range Devices (SRD) operating on frequencies between 9 kHz and 246 GHz
EN61000-3-2:2014	Electromagnetic compatibility (EMC) - Part 3-2: Limits - Limits for harmonic current emissions (equipment input current up to and including 16A per phase)
EN61000-3-3:2013	Electromagnetic compatibility (EMC) - Part 3-3: Limits - Limitation of voltage changes, voltage fluctuations and flicker in public low-voltage supply systems, for equipment with rated current up to 16A per phase and not subject to conditional connection
EN300220-2:V3.1.1	Short Range Devices (SRD) operating in the frequency range 25 MHz to 1 000 MHz; Part 2: Harmonised Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU for non specific radio equipment
EN60950-1:2006+A11:2009+A1:2010 +A12:2011+A2:2013	Information technology equipment - Safety Part 1: General requirements
EN62479:2010	Assessment of the compliance of low power electronic and electrical equipment with the basic restrictions related to human exposure to electromagnetic fields (10 MHz to 300 GHz)

The attestation based on a positive testing of a representative test sample. The test sample fulfills the requirements of the above listed standard(s).

TESTED
IN GERMANY

Date: 02.05.2017
Ref.-No.: 17/04-0028
Based on Test report, Ref.-No.: 17/04-0028
ACCREDITATION:
DAkkS D-PL-17379-01-00

PKM electronic GmbH
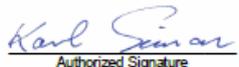
Karl Simon
Authorized Signature

11.2 FCC (United States)

TCM 515U has been tested against and is in compliance with FCC Part 15 Subpart B Class B.

11.2.1 FCC Grant Of Equipment Authorization

TCB

GRANT OF EQUIPMENT AUTHORIZATION

Certification
Issued Under the Authority of the
Federal Communications Commission
By:

Timco Engineering, Inc.
849 NW State Road 45
P.O. Box 370,
Newberry, FL 32669

Date of Grant: 08/07/2017

Application Dated: 08/07/2017

TCB

EnOcean GmbH
Kolpingring 18a
Oberhaching, 82041
Germany

Attention: Armin Anders , Director Product Marketing

NOT TRANSFERABLE

EQUIPMENT AUTHORIZATION is hereby issued to the named GRANTEE, and is VALID ONLY for the equipment identified hereon for use under the Commission's Rules and Regulations listed below.

FCC IDENTIFIER: SZV-TCM515U
Name of Grantee: EnOcean GmbH
Equipment Class: Part 15 Security/Remote Control Transmitter
Notes: Transceiver Module
Modular Type: Single Modular

Grant Notes	FCC Rule Parts	Frequency Range (MHZ)	Output Watts	Frequency Tolerance	Emission Designator
	15.231	902.875 - 902.875			

Single Modular Approval. Approval is limited to OEM installation only. Compliance of this device in all final host configurations is the responsibility of the Grantee. Only antennas investigated in the application for Equipment Authorization for this device are allowed. OEM integrators must be provided labeling requirements for finished products. This grant is valid only when the device is sold to OEM integrators and the OEM integrators are instructed to ensure that the end user has no manual instructions to remove or install the device. Separate approval is required for all other operating configurations, including portable configurations with respect to 2.1093 and different antenna configurations. This module can only be used with a host antenna circuit trace layout design in strict compliance with the OEM instructions provided.

DOLPHIN
Self-powered IoT by EnOcean
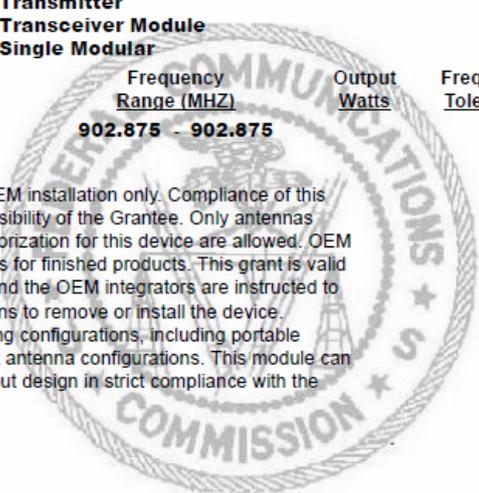
TCM 515 – ENOCEAN TRANSCEIVER GATEWAY MODULE

11.2.2 FCC Usage Conditions

TCM 515U is a RF module approved for Single Modular use. It is limited to OEM installation ONLY. A separate approval is required for all other operating configurations, including portable configurations with respect to Part 2.1093 and different antenna configurations not covered by chapter 10.2

The module is limited to installation in mobile or fixed application.

By incorporating this module into the final product, the final product may have to be tested to the FCC Part 15 Subpart B requirements. It is important to follow all notes regarding the installation and use of this module to ensure that the final product does comply with the FCC Part 15 Subpart B requirements.

To ensure compliance for all non-transmitter functions, a host product manufacturer is responsible for ensuring compliance with the module installed and fully operational. For example, if a host product was previously authorized as an unintentional radiator under the Declaration of Conformity procedure without containing a certified transmitter module, then a module is added, the host manufacturer is responsible for ensuring that the host continues to be compliant with the Part 15 subpart B unintentional radiator requirements after the module is installed and operational. Because this may depend on the details of how the module is integrated within the host, EnOcean will provide any guidance to the host manufacturer if needed for the final product for ensuring compliance with the Part 15 Subpart B requirements.

The module is optimized to operate using small amounts of energy, and may be powered by a battery. The module transmits short radio packets comprised of control signals, (in some cases the control signal may be accompanied with data) such as those used with alarm systems, door openers, remote switches, and the like.

The module does not support continuous streaming of voice, video, or any other forms of streaming data; it sends only short packets containing control signals and possibly data. The module is designed to comply with, has been tested according to 15.231(a-c), and has been found to comply with each requirement.

Thus, a finished device containing the TCM 515U radio module can be operated in the United States without additional Part 15 FCC approval (approval(s) for unintentional radiators may be required for the OEM's finished product), under EnOcean's FCC ID number if the OEM requirements are met and an OEM Modular Approval Agreement with EnOcean has been signed.

11.2.3 OEM Requirements

In order to use EnOcean's FCC ID number, the OEM must ensure that the following conditions are met:

- End users of products, which contain the module, must not have the ability to alter the firmware that governs the operation of the module. The agency grant is valid only when the module is incorporated into a final product by OEM integrators.

- The end-user must not be provided with instructions to remove, adjust or install the module.

- Changes or modifications not expressly approved by EnOcean could void the user's authority to operate the equipment.

- The module must be used with the approved antenna(s) as listed in chapter 9.2

- The OEM must ensure that timing requirements according to 47 CFR 15.231(a-c) are met.

- The Original Equipment Manufacturer (OEM) must ensure that FCC labeling requirements are met. This includes a clearly visible label on the outside of the final product. Attaching a label to a removable portion of the final product, such as a battery cover, is not permitted. The label must include the following text:
  Contains FCC ID: SZV-TCM515U
  The enclosed device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (i.) this device may not cause harmful interference and (ii.) this device must accept any interference received, including interference that may cause undesired operation.
  When the device is so small or for such use that it is not practicable to place the statement above on it, the information required by this paragraph shall be placed in a prominent location in the instruction manual or pamphlet supplied to the user or, alternatively, shall be placed on the container in which the device is marketed. However, the FCC identifier or the unique identifier, as appropriate, must be displayed on the device.

- The user manual for the end product must also contain the text given above.

DOLPHIN
Self-powered IoT by EnOcean

TCM 515 – ENOCEAN TRANSCEIVER GATEWAY MODULE

11.2.4   Module Activation

The module can be triggered manually or automatically as described below.

Manual Activation
The radio module can be configured to transmit a short packetized control signal if triggered manually. The module can be triggered, by pressing a switch, for example.

The packet contains one (or more) control signals that is(are) intended to control something at the receiving end. The packet may also contain data. Depending on how much energy is available from the energy source, subsequent manual triggers can initiate the transmission of additional control signals. This may be necessary if prior packet(s) was (were) lost to fading or interference.

Subsequent triggers can also be initiated as a precaution if any doubt exists that the first packet didn't arrive at the receiver. Each packet that is transmitted, regardless of whether it was the first one or a subsequent one, will only be transmitted if enough energy is available from the energy source.

Automatic Activation
The radio module also can be configured to transmit a short packetized control signal
if triggered automatically, by a relevant change of its inputs or in response to receiving a signal from another transmitter, for example.

Again, the packet contains a control signal that is intended to control something at the receiving end and may also contain data. As above, it is possible for the packet to get lost and never reach the receiver. However, if enough energy is available from the energy source, and the module has been configured to do so, then another packet or packets containing the control signal may be transmitted at a later time.

11.3   ISED (former Industry Canada) Certification

TCM 515U has been tested and meets the requirements of Industry Canada's license-exempt RSSs.

11.3.1   ISED Technical Acceptance Certificate

TIMCO ENGINEERING INC.

849 NW State Road 45
Newberry, Florida 32669
http://www.timcoengr.com
888.472.2424 F 352.472.2030 email: cb@timcoengr.com

No. ➢ 1352IC17

TECHNICAL ACCEPTANCE CERTIFICATE

Certification No.   ➢ IC: 5713A-TCM515U

Issued To	Tested By
➢ EnOcean GmbH Kolpingring 18A Oberhaching 82041, Germany	➢ VPI LABORATORIES, INC. Company No: 2041A 29145 Old Lincoln Hwy Wanship, UT 84017 801-260-4056 joej@vpitech.com

Type of Equipment   ➢ Low Power Device (902-928 MHz)
                                   ➢ Modular Approval (MA)

Type of Service   ➢ New Certification (Single)

Hardware Version Id Number (HVIN)   ➢ TCM 515U

Product Marketing Name: (PMN)   ➢ TCM 515U

Firmware Version Id Number (FVIN)   ➢ N/A

Host Marketing (HMN)   ➢ N/A

FREQUENCY RANGE	EMISSION DESIGNATIONS NECESSARY BANDWIDTH & EMISSION CLASSIFICATION	R.F. POWER	ANTENNA INFO	SPECIFICATION/ ISSUE & DATE	
902.875 MHz	276KF1D	81.8dBuV/@3m	See Note 2	RSS-210	Issue 9; Aug 16

Note 1: This equipment also complies with RSS-102, Issue 5 (March 2015) and RSS-Gen, Issue 4 (Nov 2014)
Note 2: Mitsubishi AM11DP-ST01T, Linx ANT-916-CW-HWR-RPS, EnOcean ANT300 helical, trace antenna, wire whip antenna

Certification of equipment means only that the equipment has met the requirements of the above noted specifications. License applications, where applicable to use certified equipment, are acted on accordingly by the issuing office and will depend on the existing radio environment, service and location of operation.

This certificate is issued on condition that the holder complies and will continue to comply with the requirements of the radio standards specifications and procedures issued by Industry Canada.

I hereby attest that the subject equipment was tested and found in compliance with the above-noted specifications.

La certification du matériel signifie seulement que le matériel a satisfait aux exigences de la norme indiquée ci-dessus. Les demandes de licences nécessaires pour l'utilisation du matériel certifié sont traitées en conséquence par le bureau de délivrance et dépendent des conditions radio ambiantes, du service et de l'emplacement d'exploitation.

Le présent certificat est délivré à la condition que le titulaire satisfasse et continue de satisfaire aux exigences et aux procédures d'Industrie Canada.

J'atteste par la présente que le matériel a fait l'objet d'essai et jugé conforme à la spécification ci-dessus.

ISSUED UNDER THE AUTHORITY OF MINISTER OF INDUSTRY
DÉLIVRÉ AVEC L'AUTORISATION DU MINISTRE DES INDUSTRIES

DATE: August 14, 2017

S. S. Sanders, President

TCM 515 – ENOCEAN TRANSCEIVER GATEWAY MODULE

11.3.2   ISED Usage Conditions

This device complies with Industry Canada's license-exempt RSSs. Operation is subject to the following two conditions:

(1) This device may not cause interference; and

(2) This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

(1) l'appareil ne doit pas produire de brouillage, et

(2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

In order to use EnOcean's IC number, the OEM must ensure that the following conditions are met:

- Labeling requirements for ISED are similar to those required by the FCC. The Original Equipment Manufacturer (OEM) must ensure that ISED labeling require-ments are met. A clearly visible label on the outside of a non-removable part of the final product must include the following text:
  Contains IC: 5713A-TCM515U
  Contient le module d'émission IC: 5713A-TCM515U

- The OEM must sign the OEM Modular Approval Agreement with EnOcean

Pour utiliser le numéro IC EnOcean, le OEM doit s'assurer que les conditions suivantes sont remplies:

- Les exigences d'étiquetage pour ISED sont similaires à ceux exigés par la FCC. Le fabricant d'équipement d'origine (OEM) doit s'assurer que les exigences en matière d'étiquetage ISED sont réunies. Une étiquette clairement visible à l'extérieur d'une partie non amovible du produit final doit contenir le texte suivant:
  Contains IC: 5713A-STM300U
  Contient le module d'émission IC: 5713A-TCM515U

- L'OEM doit signer l'accord OEM Approbation modulaire avec EnOcean

11.4   Repeater Function (FCC/IC)

The device is capable to operate as a repeater, which can receive signals from the following list of FCC/IC approved transmitters, and retransmit the signals:

- PTM 210U   FCC ID:SZV-PTM210U   IC:5713A-PTM210U
- PTM 330U   FCC ID:SZV-PTM330U   IC:5713A-PTM330U
- STM 300U   FCC ID:SZV-STM300U   IC:5713A-STM300U
- STM 320U   FCC ID:SZV-STM320U   IC:5713A-STM320U
- STM 332U   FCC ID:SZV-STM332U   IC:5713A-STM332U
- TCM 300U   FCC ID:SZV-STM300U   IC:5713A-STM300U
- TCM 310U   FCC ID:SZV-STM300U   IC:5713A-STM300U
- TCM 320U   FCC ID:SZV-TCM320U   IC:5713A-TCM320U
- TCM 330U   FCC ID:SZV-STM300U   IC:5713A-STM300U
- TCM 515U   FCC ID:SZV-TCM515U   IC:5713A-TCM515U

TCM 515 – ENOCEAN TRANSCEIVER GATEWAY MODULE

12   Product history

Table 12 below outlines the product history of TCM 515 and indicates key changes made between different revisions.

Revision	Introduction	Key features / changes
CC-3	March 2017	- First product prototypes for customer evaluation
DA-4	July 2017	- First release with full TCM 310 equivalent functionality - Introduction of option for repeated Reman telegrams - Introduction of CO_GET_STEPCODE feature
DA-5	November 2017	- Introduction of full end to end security support (encryption, decryption and authentication supported for all telegram types) - Bug fix for duty cycle supervisor
DA-6	January 2018	- Implementation of customer enhancement requests for security processing (identification of processed telegrams via ESP3, rejection of standard telegrams from devices in secure link table, support for secure telegram broadcast, option to determine number of remaining link table entries) - Introduction of adjustable noise filter functionality
DA-7	March 2018	- Bug fix: Incorrect radio ID handling might lead to use of wrong source ID when responding to SYS_EX messages
DB-8	August 2018	- Persistent repeater and filter settings - no reinitialization needed after power cycle

Table 12 – TCM 515 product history