USER MANUAL

PTM 210 / PTM 215 / PTM 215U / PTM 215J
DC Step code and later

PTM 210 / PTM 215
PTM 215U
PTM 215J

Pushbutton transmitter modules
DC Step code and later

The product is protected by the following granted Patents:

US7710227, DE10315765B4
US9614553, EP1312171B1, CN100508406C
EP1389358B1, JP4225792B2
US7019241, EP1550202B1, DE50303733D1, CN1689218B
US7391135, EP1611663B1, DE10315764B4,
US8502470, JP5617103B2
EP2524572B1

And also by pending or not yet published Patents and Designs.

REVISION HISTORY

The following major modifications and improvements have been made to the first version of this document:

No	Major Changes
2.0	Update to DC modules.

Published by EnOcean GmbH, Kolpingring 18a, 82041 Oberhaching, Germany

www.enocean.com, info@enocean.com, phone ++49 (89) 6734 6890

Important!

This information 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 devices, not for the described applications, processes and circuits.

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

The devices 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 devices are considered and should be disposed of as hazardous waste. Local government regulations are to be observed.

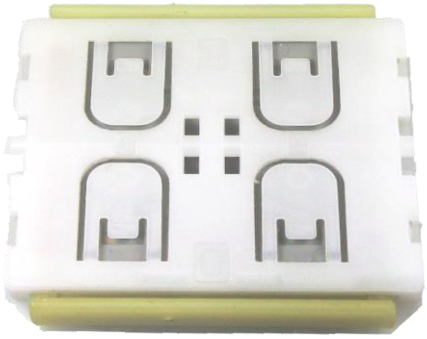
Packing: Please use the recycling operators known to you. By agreement we will take packing material back if it is sorted. You must bear the costs of transport. For packing material that is returned to us unsorted or that we are not obliged to accept, we shall have to invoice you for any costs incurred.

TABLE OF CONTENT

1 GENERAL DESCRIPTION

The pushbutton transmitter family PTM 21x from EnOcean enables the implementation of wireless remote controls without batteries. The PTM 21x pushbutton transmitters are self-powered (no batteries) and therefore maintenance-free. Power is provided by a built-in electro-dynamic power generator. They can be used in hermetically sealed systems or in remote (not easily accessible) locations.

PTM 21x devices support the 868 MHz, 902 MHz and 928MHz radio interface protocols of EnOcean Alliance Radio Standard ERP 1 & ERP 2.



Electro-dynamic powered radio transmitter device PTM 21x

With the major product update to step code DC an additional NFC interface was added and security mode possibility was extended to all PTM21x family members and frequencies.

1.1 Product variant and ordering codes

The PTM 21x product family contains (DC Step code) the following product variants:

Type	Frequency	Ordering Code	Product specifics
PTM 210	**868.300 MHz**	**S3001-A210**	Encryption capability
PTM 215	**868.300 MHz**	**S3001-A215**	Encryption capability & NFC Interface
PTM 215U	**902.875 MHz**	**S3051-A215**	Encryption capability & NFC Interface
PTM 215J	**928.350 MHz**	**S3061-A215**	Encryption capability & NFC Interface

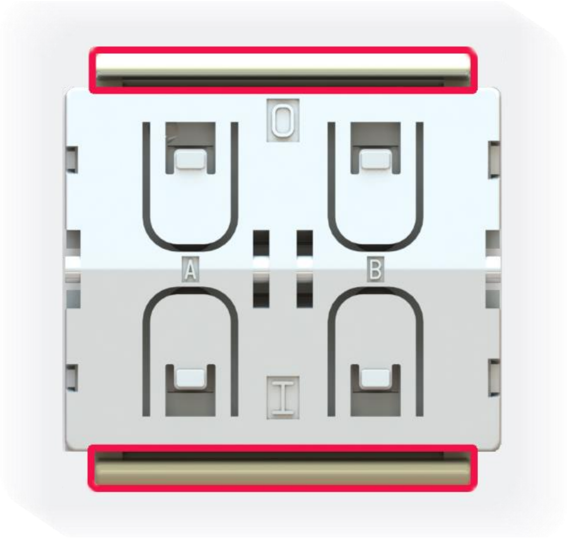
For PTM 21x Products with earlier step codes (DA, DB) please do not use this document as reference and refer to EnOcean support (support@enocean.com) for more details.

This document describes PTM modules with the EnOcean Radio Standard. To refer to other radio standards PTM Modules (e.g. Bluetooth, Zigbee) please visit the correct EnOcean Website Product page[1].

[1] https://www.enocean.com/en/products/

1.2 Basic Functionality

PTM 21x devices contain an electro-dynamic energy transducer which is actuated by the bow.



Drawing with highlighted energy bow

This bow is pushed by an appropriate push button, switch rocker or a similar construction mounted onto the device. An internal spring will release the energy bow as soon as it is not pushed down anymore.

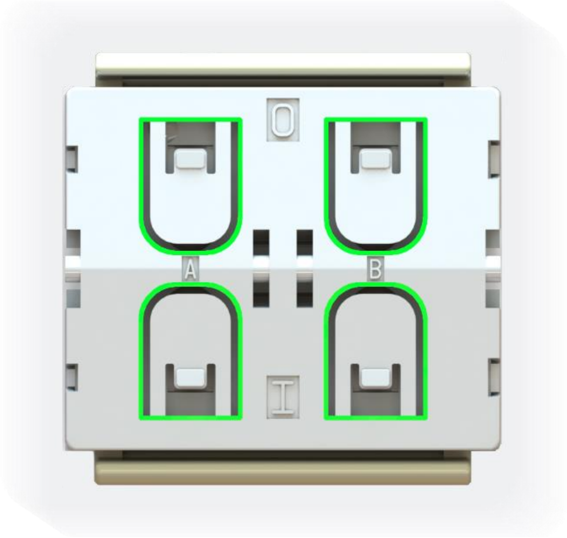
When the energy bow is pushed down, electrical energy is created and a radio telegram is transmitted. Releasing the energy bow similarly generates energy which is used to transmit an another radio telegram.

Energy bow released

Energy bow pressed

It is therefore possible to distinguish between radio telegrams sent when the energy bow was pushed and radio telegrams sent when the energy bar was released. By identifying these different telegrams types and measuring the time between pushing and releasing at the receiver, it is possible to distinguish between "Long" and "Short" push button presses. This enables simple implementation of applications such as dimming control or blinds control including slat action.

The PTM radio telegram identifies the status of the four contact nipples when the energy bow was pushed or released. This enables the implementation of up to two switch rockers or up to four pushbuttons.



Drawing with highlighted coding nibbles

All PTM 21x devices support two operating modes - a normal mode and a secure mode with rolling code encryption to enable secure applications.

Additionally, to the EnOcean Radio interface the PTM 215 modules have also an NFC interface. The interface is powered by the NFC Field of an NFC Reader or an NFC Capable smartphone, this makes the communication with the PTM 215 modules possible even when the PTM is not powered. With a Smartphone and an App e.g. EnOcean Tool or with an NFC Reader and a PC tool e.g. EnOcean NFC Configurator it is possible to read information about the PTM module

1.3 Typical Applications

Typical applications are found in the following areas:

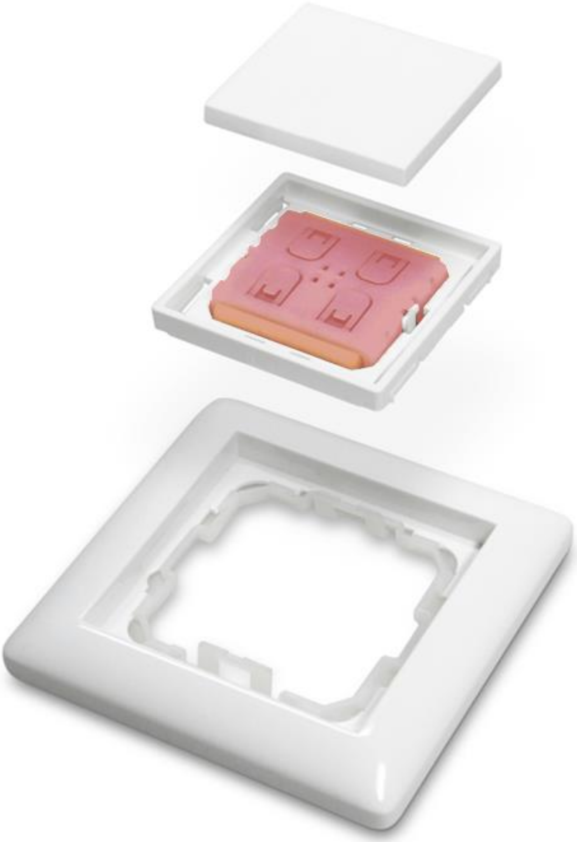
- Building installation
- Industrial automation
- Consumer electronics

Key products include wall-mounted switches and handheld remote controls supporting up to two rockers or up to four pushbuttons.

Please find below an example of an assembled PTM module into white housings. The left figure shows a two rocker application and the right a one rocker. This is commonly used in the European market. The various end application (frames and plastics) properties like shape, materials, colors etc. can differ as long they respect the PTM Module mounting instructions. This way you can create own and recognizable design offering well tested and promoted PTM modules.

Example of an assembled PTM Module into a wall switch housing with two and one rocker

To illustrate the stack up in complete switch please find below an explosion drawing showing one possible switch frame mounting with highlighted PTM Module inside.



Explosion drawing of complete wall switch with highlighted PTM Module

1.4 Technical Data

Power supply	electro-dynamic power generator
Antenna	PCB antenna
Frequency	PTM 210: 868.300 MHz (ASK)[2] PTM 215: 868.300 MHz (ASK)[1] PTM 215U: 902.875 MHz (FSK) PTM 215J: 928.350 MHz (FSK)
Data rate	125 kbps
Conducted output power	PTM 210 / PTM 215 / PTM 210U: +5 dBm PTM 210J: 0dBm
Channels	Two channels with two pushbuttons per channel Four action states per channel (upper/lower/pressed/not pressed)
EnOcean Radio Standard	ERP1 based on ISO/IEC 14543-3-10: PTM 210, PTM 215 ERP2 based on ISO/IEC 14543-3-11: PTM 215U, PTM 215J
EnOcean Equipment Profile supported	F6-02-xx, F6-04-xx (normal mode) D2-03-00 (secure mode)
Security mode	Rolling code with AES128
Transmission range	PTM 210 / PTM 215 / PTM 210U: typ. 300 m free field, typ. 30 m indoor PTM 210J: typ. 200m free field, typ. 30m indoor
Device identifier	Individual 32 or 48 bit ID (factory programmed)

1.5 Mechanical Interface

Device dimensions (inclusive rotation axis and energy bow)	40.0 x 40.0 x 11.2 mm
Device weight	20 g ± 1 g
Energy bow travel / operating force	1.8 mm / typ. 9 N At room temperature
Restoring force at energy bow	typ. 0.7 N to 4 N Minimum restoring force of 0.5 N is required for correct operation
Number of operations at 25°C	typ. 100.000 actuations tested according to EN 60669 / VDE 0632
Cover material	Hostaform (POM)
Energy bow material	PBT (50% GV)

1.6 Environmental Conditions

Operating temperature	-25 °C up to +65 °C
Storage temperature	-25 °C up to +65 °C
Humidity	0% to 95% r.h.

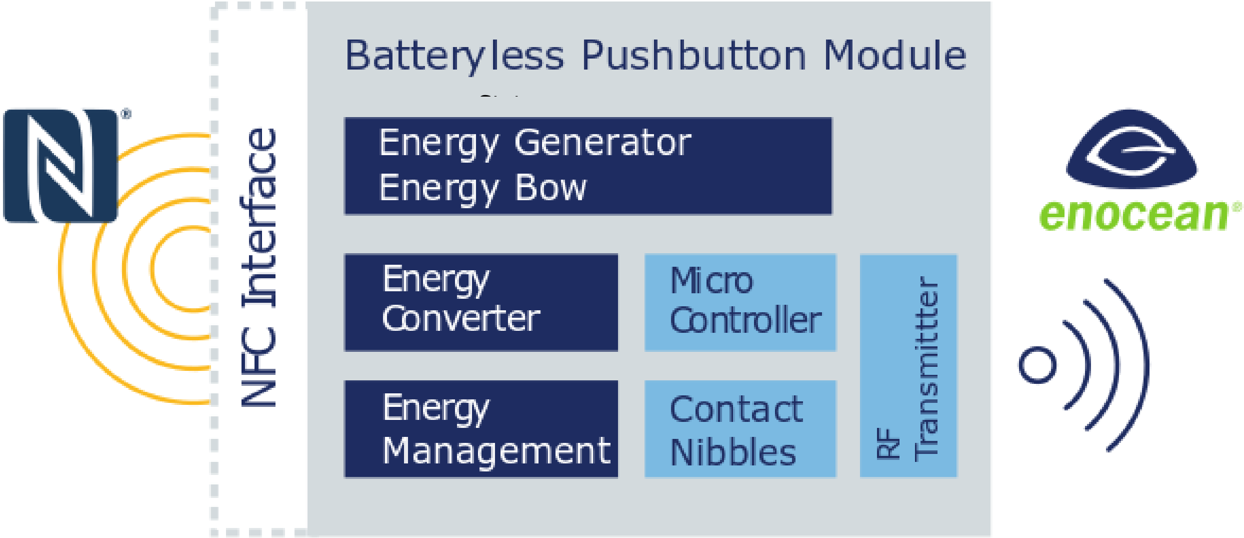
[2] According the international standard for energy harvesting wireless radio protocol for self-powered applications: ISO/IEC 14543-3-10

1.7 References

1) PTM_210_Mounting_Instructions_Jul2014_07.pdf(PDF 356,4 KB)
2) PTM_210_Mounting_Instructions_3D_April2013_07.zip(ZIP 2,5 MB)
3) PTM_210_Rocker_Model_2D_and_3D_Aug09_07.zip(ZIP 465,4 KB)
4) PTM Instructions -
5) Enocean radio standards
   a. ERP1
   b. ERP2
   c. Security
   d. EEP
   e. NFC
6) White papers
7) Support

2 FUNCTIONAL DESCRIPTION

2.1 Block Diagram



Block diagram of PTM 21x

Energy Generator / Energy Bow

Converts the motion of the energy bow into electrical energy. This is the main energy source for the PTM Modules.

Energy Converter

Converts the energy of the power generator into a stable DC supply voltage for the device electronics.

Energy Managemetn

Secures energy supply of the module for the required period. The generator provides an burst of energy which needs to be conserved for the much longer period than the burst lasts.

Microcontroller

Determines the status of the contact nipples and the energy bow, encodes this status into a EnOcean Data telegram, if required it encrypts this data and computes the CMAC, generates the proper radio telegram structure and sends it to the radio transmitter.

RF transmitter

Transmits the data in the form of a series of short EnOcean radio telegrams.

Contact Nipples

Via the 4 nibbles rockers or other custom plastics can code specific information into the radio telegram triggering different functions at the receiver.

NFC Interface

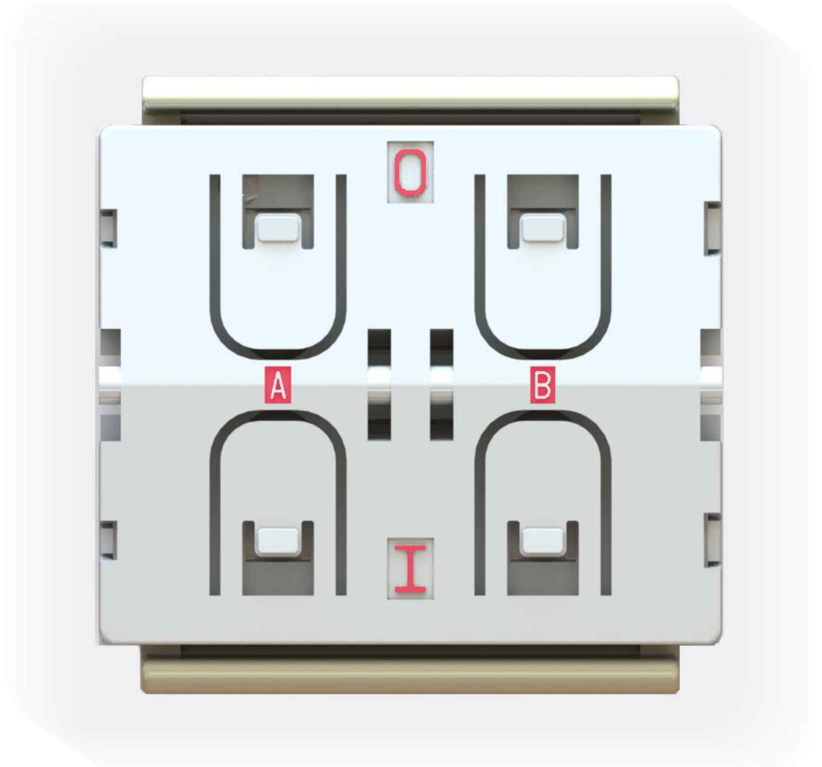
The NFC interface represents the second communication interface of the PTM and it is designed for commissioning of the PTM device. Via NFC module information, modes, runtime parameters can be read and in selected parameters also written.

2.2 Contact Nipples assignment

PTM 21x devices provide four contact nipples. They are grouped into two channels (Channel A and Channel B) each containing two contact nipples (State O and State I). Resulting the nibbles are referred to as: AO, AI, BO, BI.

The state of all four contact nipples is transmitted together with a unique device identification whenever the energy bow is pushed or released in an EnOcean Telegram. The exact coding is defined the EEP Profile. Which EEP is used is selected based on the Radio Standard (ERP1 or ERP2) and operating mode (normal or secure). See chapter 2.3 for details on used EEPs.

The picture below shows the arrangement of the four nipples and their designation:



Contact nipple designation

2.3 Available EnOcean Equipment Profiles

The (EnOcean Equipment Profile) EEP profile defines how the data inside the EnOcean telegram are coded. For the PTM it practically means how the nibbles and energy bow state are represented. Based on the specified EEP the receiver knows how to interpret the incoming telegrams from the PTM Module.

Usually a sensor has only one assigned profile. In case of PTM Modules (RPS Profiles) the receiver can decide in some cases which profile he chooses for interpretation of the data from the very same PTM module.

	Normal Mode	**Secure Mode**
ERP 1 **(PTM 210, PTM 215)**	F6-01-01 F6-02-01 F6-02-02 F6-02-03 F6-04-01	D2-03-00
ERP 2 **(PTM 215J, PTM 215U)**	F6-02-04 F6-04-02	D2-03-00

⚠ TCM 515U and TCM 310U does convert from ERP2 profiles to EPR1 profiles internally. On the ESP3 interface the commands they look like "ERP1".

⚠ Due to the mechanical hysteresis of the energy bow, in most rocker switch device implementations, pressing the rocker sends an N-message and releasing the rocker sends a U-message!

For the normal mode profiles (Starting with F6) there is no EEP Teach-in message send. For secure mode profile (starting D2) there is Secure Teach in. See secure teach in chapter 3.2.3 for details.

⚠ Note that PTM 21x in will not send a data telegram when pressing 2, 3 or 4 nibble SBC and actuating the energy bow. This button combination is reserved for mode change. Please see chapter 3.3 for details.

3 OPERATING MODES

This chapters describe the standard "out of the box" behaviour. The standard behaviour e.g. mode selection, secure teach-in telegram transmission can be altered by the NFC Interface. Please refer to the NFC Chapter (see).

There are two operating modes:

- Normal mode
- Secure mode, this mode has two additional sub options
    - Implicit RLC (legacy, not recommended)
    - Explicit RLC (recommended)

After production, PTM 21x is set to "normal mode operation

3.1 Normal mode operation

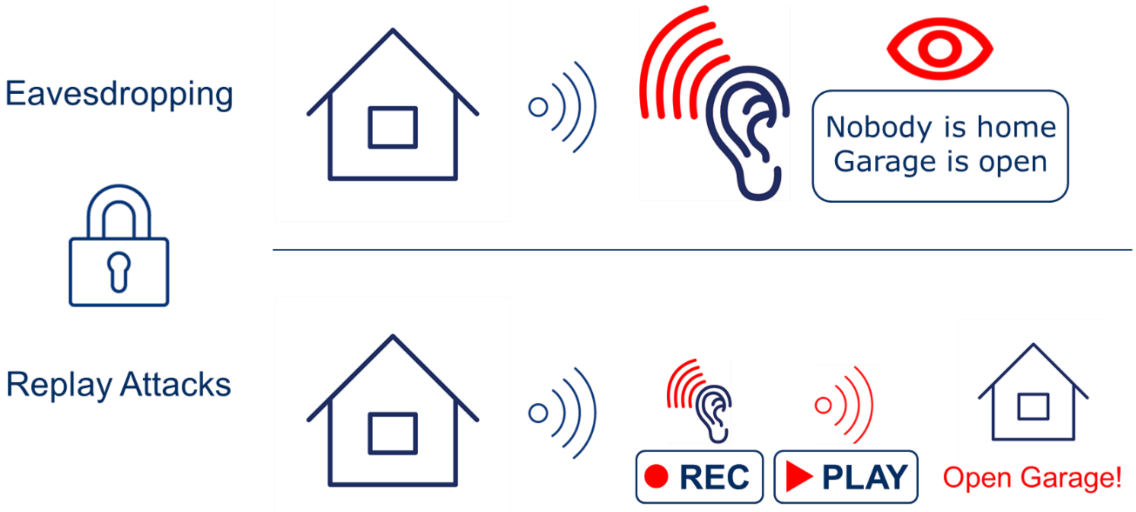
In normal mode, PTM 21x does transmit the telegrams in the EEP profile defined by the ERP1 or ERP2. Please refer to Chapter 2.3. for details.

In Normal mode the secure concept includes unique transmitter IDs. This means EnOcean products cannot be configured to transmit with identical transmitter ID, excluding Base ids.

3.2 Secure mode operation

While operating in secure mode, PTM 21x sends secure telegrams in accordance to EEP D2-03-00. Please refer to Chapter 2.3. for details.

In secure mode the PTM Module uses advanced security protection with data encryption and message authentication. These mechanisms offer effective protection against a series of different attacks. One of the most concerning are Eavesdropping and Reply attacks. Eavesdropping means somebody can receive and interpret the data correctly and replay attacks means an intruder receives and records the message and retransmits it later to trigger a defined action. Examples of intruding scenarios are in the figure below.



Example of harfull attacking scenarios PTM Modules are protected from

For details on the secure mechanisms please refer to the security specification of the EnOcean radio Protocol http://www.enocean.com/en/security-specification/. Or for practical explanation with examples please see APP note.

Secure telegrams include a rolling code based on an incrementing counter which guarantees that identical message content will be encrypted differently.

The counter can be:

- Included in each data message - explicit (recommended)

  Or

- Not included in data messages – implicit (legacy, not recommended)

The counter value is also part of the teach-in telegram. The selection if the counter is implicit or explicit is done via the NFC interface (see) or special button combinations at mode switching (for details visit chapter 3.3).

There is no advantage in term of being "more secure" or "more protected" by using the implicit mode over explicit or vice versa. The "protection level" and security mechanisms are same.

The RLC starts at production with value 0. By the size of the RLC counter (24 bit) it is practically ensured it will not run over and use the same value twice during the PTM lifetime.

The RLC counter is internally restarted to 0x0 once the AES key was changed via the NFC interface.

By doing factory reset (see chapter 3.4 for details) the PTM module returns to using the factory set AES key but does not reset the RLC counter associated with the key. The last used RLC value associated with the factory set AES key will be used.

3.2.1 Implicit RLC – legacy, not recommended

This mode is relevant only for the European market – 868 MHz because of legacy receivers. For the J and U market 928 MHz and 902 MHz, there are no legacy receivers and thus not reason to use this mode at all.

The initial counter value is transmitted from PTM 21x to the receiver only as part of the teach-in telegram. Subsequent secure telegrams do not include it. Therefore, receiver has to automatically increment his counter at every received telegram to keep it synchronized with the PTM Module.

When telegrams are not received by the receiver this may lead to a de-synchronization of PTM Module and receiver counters, i.e. the PTM Module counter will have a greater value than the receiver counter.

In order to prevent failure, the receiver will usually test the received rolling code against a defined window of future expected rolling codes and – if successful - resynchronize its counter automatically. The size of this rolling code window is defined on the receiver side.

It is important that the amount of consecutive, non-received telegrams does not exceed the size of this window.

For more details please refer to http://www.enocean.com/en/security-specification/.

3.2.2 Explicit RLC – recommended

This is the recommended secure mode for all frequencies and new applications.

In this mode the PTM does send the RLC inside every data telegram. With transmission of the RLC in every data telegram a desynchronization of RLC counters between receivers and transmitter like described above cannot happen.

The receivers use the RLC value inside the radio telegram to resynchronize. The receiver has to check if the received RLC is higher than the last known value, but he does not have to apply any window mechanism.

3.2.3 Security Teach-in

A security teach-in telegram is sent by PTM 21x when:

- Executing the special button combination for secure mode 2x nibble SBC or 3x nibble SBC – see chapter 3.3 for details.
- Triggering the telegram by NFC interface.

The *Type* of the *Teach-in_info* in the secure teach-in telegram (`Teach_In_Info : Type`) is: `1-PTM`. The Security teach-in includes required information for the receiver to decrypt future data communication.

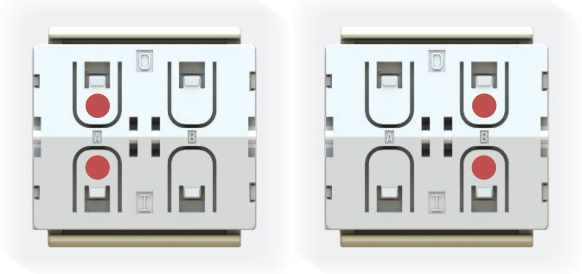
For more information on the structure of the teach-in telegram please refer to chapter 4.2 of http://www.enocean.com/en/security-specification/.

⚠ If the teach-in process is not successful, please repeat the procedure. Due to the enhanced telegram length of teach-in telegrams in secure mode only a single teach-in sub-telegram is sent at every actuation (no redundancy).

3.3 Switching between modes

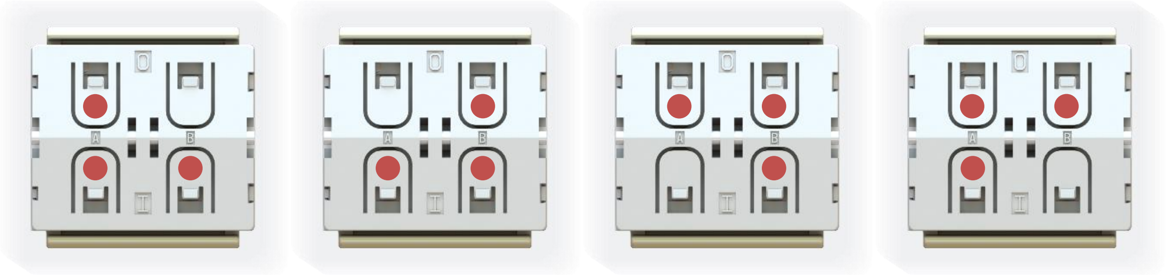
PTM 21x can be switched between normal mode and secure modes by a special button combination - SBC. There are three types of SBC:

- 2 nibbles SBC – pressing both nibbles of a channel i.e. AI & AO or BI & BO. This SBC is used to enter the secure mode with implicit RLC – legacy, not recommended. Picture below shows both variants



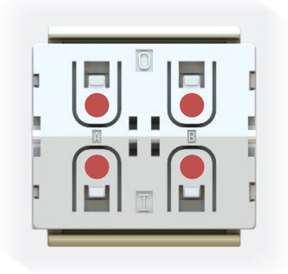
2 nibbles SBC - channel A left, channel B right

- 3 nibbles SBC – pressing any 3 nibbles, which results in 4 different combinations. This SBC is used to enter the secure mode with explicit RLC. Picture below shows all of them.



3 nibbles SBC - 4 different options

- 4 nibble SBC – pressing all 4 nibbles. This SBC is used to enter the normal mode and execute factory reset. RLC Picture below shows it.



4 nibbles SBC

To make a mode change with any of the SBC the energy bow must be activated in a defined sequence simultaneously. The SBC must be hold for the complete sequence. Following transitions applies:

	2 SBC	3 SBC	4 SBC
Energy bow press	N/A	N/A	Switch to Normal Mode
Energy bow press/release	Transmit secure teach in – if current mode is security with **implicit** RLC.	Transmit secure teach in – if current mode is security with **explicit** RLC.	N/A
Energy bow press/release/press	Switch to Security mode with **implicit** RLC & transmit secure teach-in.	Switch to Security mode with **explicit** RLC & transmit secure teach-in.	N/A

⚠ Before changing the operating mode please make sure to clear the device from all receivers which have been teached-in with this device before. Otherwise the receiver will ignore the telegrams and the application will not work.

3.4 Factory reset

The PTM can execute a factory reset to return to the defined factory defaults. With the factory default all changes done via SBC or NFC interface will be returned to factory defaults. The only changes NOT reverted is:

- Custom message – the value entered stays

The Factory reset is executed with the 4 nibble SBC and simultaneously the sequence of 7x times pressing & releasing the energy bow.

4 Radio Communication

U2S T2S – RPS, security ULP, security normal power

5 NFC INTERFACE CONFIGURATION – PTM 215 only

5.1 NFC interface overview

PTM 215 implements am NFC configuration interface that can be used to access (read and write) the PTM 215 configuration memory and thereby configure the device as described in the following chapters.

NFC communication distance is for security reasons set to require direct contact between the NFC reader and the PTM 215 device.

The NFC interface of PTM 215 uses NFC Forum Type 2 Tag functionality as specified in the ISO/IEC 14443 Part 2 and 3 standards. It is implemented using an NXP NT3H2111 Mifare Ultralight tag.

For specific implementation aspects related to the NXP implementation in NT3H2111, please refer to the NXP documentation which at the time of writing was available under this link:
https://www.nxp.com/docs/en/data-sheet/NT3H2111_2211.pdf

For a detailed description about the NFC functionality, please refer to the ISO/IEC 14443 standard.

5.2 NFC Interaction with the PTM Application

The PTM 215 application is not powered by the NFC interface when the NFC communication is executed. After parameters in the NFC memory were changed the energy bow has to be pressed and released so the PTM application can read the new parameters, check and apply them. For this purpose, also a special flag must be set to tell the PTM Application to look for changes.

In the first press / release cycle after NFC write operation was done no radio communication will be executed. In the afterwards following press / release cycle normal communication is executed.

By writing following parameters the standard behavior as explained in the chapter 3 is altered:
Security Mode
LRN Behaviour

Details are explained in chapter 5.4

5.3 NFC access protection

Protected data access is only possible after unlocking the configuration memory with the correct 32 bit PIN code. By default, the protected area is locked and the default pin code for unlocking access is `0x0000E15`.

The default pin code shall be changed to a user-defined value as part of the installation process. This can be done by unlocking the NFC interface with the old PIN code and then writing the new PIN code. For details please refer to chapter 5.4.

5.4 NFC parameters – Memory map

The NFC memory is organized in pages (smallest addressable unit) where each page contains 4 byte of data. Several pages with similar functionality form an NFC memory area.

These NFC pages are allocated into the following areas:

- Device Identification NDEF string (Public read-only access; no PIN required)
  This area contains an NDEF string identifying key device parameters
- User Information NDEF string (Public read / write access; no PIN required)
  This area allows any user to read or write information about the device such as the intended installation location or additional instructions.
- NFC HEADER (Public read-only access; no PIN required)
  This area contains information about the NFC revision
- INTERNAL DATA (Non-accessible)
  This area contains calibration values and internal parameters and cannot be used
- CONFIGURATION (Read and Write access, PIN required)
  This area contains device configuration registers

The organization of the STM 550 NFC memory map is shown in Table 1 below.

NFC Address	Memory Area	Content
	PRODUCT NDEF	Device identification NDEF string (read-only)
	USER NDEF	User information NDEF string (read / write access)
	NFC HEADER	NFC memory revision (read-only)
0x40 … 0x54	CONFIGURATION	Configuration registers (Read / Write, PIN protected)
0x55 … 0xCF	INTERNAL DATA	Internal data (Do not use)

Table 1 – STM 550 NFC memory areas

Device identification NDEF

The NDEF area contains a device identification string using the NDEF (NFC Data Exchange Format) standard that is readable by most NFC-capable reader devices (including smartphones).

An example device identification string from the NDEF area of STM 550 could be:

```
6PENO+30S000012345678+1P000B0000004C+30PS6221-K516+2PDA04+2Z01234567891234
+3C31+01000000
```

This NDEF string encodes the parameters shown in Table 2 below.

Identifier	Length of data (excl. identifier)	Value
6P	3 characters	Standard: “ENO”
30S	12 characters	EURID (6 byte, variable)
1P	12 characters	EnOcean Alliance Product ID STM 550: „000B0000004C“ STM 550U: „000B0000004D“ STM 550J: „000B0000004E“
30P	10 characters	Ordering Code STM 550: “S6201-K516” STM 550U: “S6251-K516” STM 550J: “S6261-K516”
2P	4 characters	Step Code and Revision (“DA04”)
2Z	14 characters	NFC UID (14 byte, globally unique)
3C	2 characters	Header Start Address (“31” = 0x31)
16S	8 characters	SW Version Example: 01000000 = 01.00.00.00

Table 2 – NDEF Parameters

User information NDEF

The NDEF area allows the user to store a string of up to 64 characters starting at page 0x20 and ending at page 0x2F. The remaining pages in this area (0x1E, 0x1F, 0x30) provide the required NDEF formatting information and cannot be changed by the user.

NFC HEADER

The NFC HEADER area contains information about the NFC memory structure and can therefore be used to distinguish between different NFC memory layouts.

NFC HEADER area structure

The structure of the NFC HEADER area is shown in Figure 1 below.

NFC Address	Content			
	Byte 0	Byte 1	Byte 2	Byte 3
0x31	START (0xE0)	LENGTH (0x0A)	VERSION (0x01)	OEM MSB (0x00)
0x32	OEM LSB (0x0B)	DEVICE_IDENTIFIER (0x000003)		
0x33	REVISION (0x03)	END (0xFE)	UNUSED (0x0000)	

Figure 1 – NFC HEADER area structure

The NFC HEADER contains the following fields:

- START
  This field identifies the start of the NFC header and is always set to 0xE0

- LENGTH
  This field identifies the length of the NFC header.
  For STM 550, this field is set to 0x0A since the header structure is 10 bytes long

- VERSION
  This field identifies the major revision and is set to 0x01 currently

- OEM
  The 16 bit OEM field identifies the manufacturer of the device so that manufacturer-specific layout implementations can be determined.
  For EnOcean GmbH this field is set to 0x000B

- DEVICE_IDENTIFIER
  The 24 bit DEVICE_IDENTIFIER field identifies an individual device from the range of devices manufactured by the manufacturer specified in the OEM field.
  For STM 550, the DEVICE_IDENTIFIER is set to 0x000003

- REVISION
  The REVISION field identifies the exact revision of the NFC layout. This REVISION will be incremented whenever a change to the NFC layout is made.

- END
  The END field identifies the end of the NFC header and is always set to 0xFE. The number of bytes from START to END must equal LENGTH, otherwise the NFC header

is invalid.

CONFIGURATION

The CONFIGURATION area allows configuring the device parameters and is therefore the most important part of the NFC memory. Configuration registers larger than 8 bit use big endian format, i.e. the most significant byte comes first.

Read or write access to the CONFIGURATION area is only possible after issuing a PWD_AUTH command as described in chapter **Fehler! Verweisquelle konnte nicht gefunden werden.** using the correct 32 bit PIN code.

Using the NFC configuration functionality

Before making any changes to the default configuration, be sure to familiarize yourself with the functionality of the device and the effect of the intended changes. STM 550 will not accept the setting of non-valid values for its parameters. If any parameter is non-valid then all changes made will be rejected and the previous configuration will be restored.

CONFIGURATION area structure

The structure of the CONFIGURATION area is shown in Figure 2 below.

NFC Address	**Content**			
	Byte 0	**Byte 1**	**Byte 2**	**Byte 3**
0x40	PRODUCT_ID (as characters in ASCII format) Will be copied to NDEF Header			
0x41				
0x42				
0x43	RFU			
0x44 … 0x47	USER_KEY (128 Bit) (Write Only - Will be reset to zero after it has been copied to internal memory) Can be used as alternative security key instead of FACTORY_KEY			
0x48	SECURITY_KEY_MODE	SECURITY_CFG	RFU	
0x49	EEP	SIGNAL	LED_MODE	FUNCTIONAL_MODE
0x4A	STANDARD_TX_INTERVAL		RFU	
0x4B	NFC_PIN_CODE			
0x4C	THRESHOLD_CFG1	THRESHOLD_CFG2	LIGHT_SENSOR_CFG	ACC_SENSOR_CFG
0x4D	SOLAR_ THRESHOLD		SOLAR_ TX_INTERVAL	
0x4E	LIGHT_THRESHOLD		LIGHT_ TX_INTERVAL	
0x4F	ACCELERATION_THRESHOLD		ACCELERATION _TX_INTERVAL	
0x50	TEMPERATURE_THRESHOLD		TEMPERATURE _TX_INTERVAL	
0x51	HUMIDITY_THRESHOLD		HUMIDITY _TX_INTERVAL	
0x52	RFU		MAGNET_CONTACT_TX_INTERVAL	

0x53	RFU	RFU
0x54	LIGHT_TEST_RESULT	RFU

Figure 2 – CONFIGURATION area structure

NFC_PIN_CODE

The PIN code used to protect access to the NFC CONFIGURATION memory area should be changed from the default value to a user-specific value to avoid unauthorized access to the device configuration.

To do so, first authenticate with the current PIN code and then write the new PIN code (32 bit value) to the NFC_PIN_CODE register.

PRODUCT_ID

The EnOcean Alliance Product ID uniquely identifies each product within the EnOcean Alliance ecosystem. The Product ID consists of a 2 byte manufacturer identification code (assigned by EnOcean Alliance) and a 4 byte product identification code (assigned by the manufacturer.

EnOcean has been assigned the manufacturer identification code 0x000B. EnOcean has assigned the following product identification codes to STM 550:

STM 550:	0000004C
STM 550U:	0000004D
STM 550J:	0000004E

The PRODUCT_ID register contains the Product ID in ASCII format (12 characters) and allows changing both manufacturer and product identification. Changing the PRODUCT_ID will also cause the PRODUCT ID field in the NDEF string (described in chapter 0) to be updated.

Figure 3 below shows the structure of the PRODUCT_ID register. This register contains the sequence of 12 ASCII characters (1 byte each) starting with CH0 and ending with CH11.

PRODUCT_ID											
CH0	CH1	CH2	CH3	CH4	CH5	CH6	CH7	CH8	CH9	CH10	CH11
Manufacturer (“000B”)				Product ID (“0000004C”, “0000004D” or “0000004E”)							

Figure 3 – PRODUCT_ID

USER_KEY

Each STM 550 module is pre-programmed at the factory with a randomly generated 128 bit security key (FACTORY_KEY). This key will by default be used to encrypt and authenticate STM 550 radio telegrams when operating in high security mode.

In certain applications it might be desirable to assign a different (user-defined) security key (USER_KEY) during commissioning to STM 550. This can be done by writing the user-defined security key to the USER_KEY register and setting KEY SELECTION field of the SECURITY_KEY_MODE to 0b01 as described below.

Note that the USER_SECURITY_KEY register is a write-only register meaning that it is not possible to read back a user-defined security key.

SECURITY_KEY_MODE

The register SECURITY_KEY_MODE allows selecting if FACTORY_KEY or USER_KEY should be used to encrypt and authenticate STM 550 radio telegrams in high security mode. In addition, it allows disabling the transmission of Secure Teach-in telegrams in order to protecting the security key.

Note that if the transmission of a secure teach-in telegram has been disabled and is subsequently re-enabled then USER_KEY will be reset to FACTORY_KEY.

Figure 4 below shows the structure of the SECURITY_KEY_MODE register.

<table>
<tr><th colspan="8">SECURITY_KEY_MODE (Default: 0x00)</th></tr>
<tr><td>Bit 7</td><td>Bit 6</td><td>Bit 5</td><td>Bit 4</td><td>Bit 3</td><td>Bit 2</td><td>Bit 1</td><td>Bit 0</td></tr>
<tr><td colspan="4">RFU</td><td colspan="2">SECURE LRN TELEGRAM</td><td colspan="2">KEY SELECTION</td></tr>
</table>

Figure 4 – SECURITY_KEY_MODE register

The encoding for the KEY SELECTION bit field is shown in Table 3 below.

KEY SELECTION	Security key used
`0b00 (Default)`	FACTORY_KEY is used
`0b01`	USER_KEY is used
`0b10, 0b11`	Reserved, do not use

Table 3 – KEY SELECTION bit field encoding

The encoding for the SECURE LRN TELEGRAM bit field is shown in Table 4 below.

SECURE LRN TELEGRAM	Secure LRN telegram
`0b00 (Default)`	Secure LRN Telegram (containing security key) enabled
`0b01`	Secure LRN Telegram (containing security key) disabled
`0b10, 0b11`	Reserved, do not use

Table 4 – SECURE LRN TELEGRAM bit field encoding

SECURITY_MODE

The register SECURITY_MODE identifies the security settings used by STM 550. Figure 5 below shows the structure of the SECURITY_MODE register.

SECURITY_MODE (Default: 0x00)							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
RFU				SECURITY FORMAT		SECURITY MODE	

Figure 5 – SECURITY_MODE register

The encoding for the SECURITY MODE bit field is shown in Table 5 below.

SECURITY MODE	Security Mode
`0b00 (Default)`	Standard, can be changed by the user with the LRN button
`0b01`	High Security, can be changed by the user with the LRN button
`0b10`	Standard, cannot be changed by the user with the LRN button
`0b11`	High Security, cannot be changed by the user with the LRN button

Table 5 – SECURITY MODE bit field encoding

The encoding for the SECURITY FORMAT bit field is shown in Table 6 below.

SECURITY FORMAT	Advertising Interval
`0b00 (Default)`	32 bit RLC and 32 bit CMAC
`0b01`	24 bit RLC and 24 bit CMAC
`0b10, 0b11`	Reserved, do not use

Table 6 – SECURITY FORMAT bit field encoding

5.5 EnOcean Tool

Using the NFC interface

Using the NFC interface requires the following:

- NFC reader
  This can be either a USB NFC reader connected to a PC or a suitable smartphone with NFC functionality

- NFC SW with read, write, PIN lock, PIN unlock and PIN change functionality
  This can be either a PC application or an Android / iOS app

These options are described in more detail below.

PC with dedicated NFC reader

For PC-based applications, EnOcean recommends the TWN4 Multitech 2 HF NFC Reader (order code T4BT-FB2BEL2-SIMPL) from Elatec RFID Systems (sales-rfid@elatec.com).

This reader is shown in Figure 6 below.

Figure 6 – Elatec TWN4 MultiTech Desktop NFC Reader

Android or iOS smartphone with NFC

NFC functionality is available in certain Android (e.g. Samsung Galaxy S7 / S8 / S9 / S10) and iOS (iPhone7 or newer, firmware version 13 or newer) smartphones.

EnOcean provides the configuration app “EnOcean Tool” for these devices which can be downloaded directly from the respective app store.

At the time of writing, the tool was available from the Google Play Store using this link:
https://play.google.com/store/apps/details?id=de.enocean.easytool&hl=en

6 APPLICATIONS INFORMATION

6.1 Product Label & QR Code

LABELS

6.2 Construction of application specific Switch Rockers

For CAD system development support, 3D construction data is available from EnOcean (IGS data). Using this data, the mechanical interface is fixed, and the shape and surface of the rocker(s) can be changed according to requirements.

Polycarbonate is recommended as rocker material since it is both buckling resistant and wear-proof. It is also recommended to apply Teflon varnish in the areas of actuation.

⚠ It is recommended using non-conductive material for the rockers to ensure best transmission range. Avoid if possible metallic materials or plastics with conducting ingredients such as graphite.

⚠ If the rocker is not mounted on the rotation axis of PTM 21x several tolerances have to be considered! The measure from support plane to top of the energy bow is 7.70 mm +/- 0.3 mm!

⚠ The movement of the energy bow must not be limited by mounted rockers!

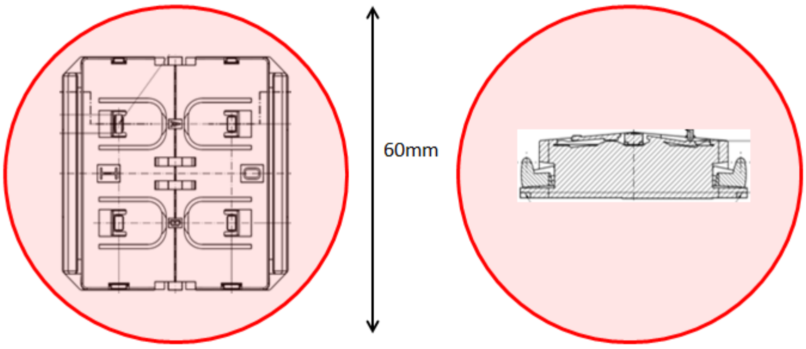
⚠ Catwalks of the switch rocker must not exert continuous forces on contact nipples!

6.3 Device Mounting

For mounting the PTM 21x device into an application specific case, the package outline drawings of the device are given in chapter 1.5. More detailed 3D construction data is available from EnOcean in IGS format.

⚠ It is recommended not to mount the device directly onto metal surfaces or into metal frames since this can lead to significant loss of transmission range.

PTM 215B is powered by the electromagnetic generator ECO 200. For proper function magnets or ferromagnetic materials are not permitted within a keep-out zone of 60mm around the center of PTM 215B.



6.4 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 for expected transmission range are considered by using a PTM, an STM or a TCM radio transmitter device together with a TCM radio receiver device with preinstalled whip antenna.
These 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 similar areas should be considered as shielded

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 EnOcean receivers and other transmitting devices such as computers, audio and video equipment that also emit high-frequency signals should be at least 0.5 m.

A summarized application note to determine the transmission range within buildings is available from www.enocean.com.

7 AGENCY APPROVALS

7.1 PTM 210 and PTM 215: Radio Approval for the European Market

The module is developed and tested according to the R&TTE EU-directive on radio equipment. The assembly conforms to the European and national requirements of electromagnetic compatibility. The conformity has been proven and the corresponding documentation has been deposited at EnOcean. The PTM devices can be operated without notification and free of charge in the area of the European Union, and in Switzerland.

From 12th of June 2016 the new European Radio Equipment Directive (RE-D) is in place. Unfortunately, necessary radio standards (e.g. EN 300 220) are still in definition and review phase, finalization is expected for Q1/2017. In order to overcome this issue a transition period till 12th of June 2017 has been defined by the European Union. During this period, products developed and tested according to R&TTE can be sold to the market.

The following provisos apply:

- EnOcean switch modules must not be modified or used outside specification limits.
- EnOcean switch modules may only be used to transfer digital sensor data
- The final product including EnOcean switch module must meet all necessary application specific requirement for CE conformity (e.g. product labelling, manual and conformity to all application specific directives and standards).

If transmitters are used according to the regulations of the 868.300 MHz SRD/ISM band, a so-called “Duty Cycle” of 1% per hour for each transmitter must not be exceeded. Permanent transmitters such as radio earphones are not allowed.

For conventional applications, it must be ensured that the PTM 215 or PTM 210 radio device is not operated more than 6000 times within one hour (one operation: energy bow is pressed and released). Within this calculation, the extraordinary short telegram length is considered including three sub-telegrams. Also a tolerance of 5% in the telegram length is included.

7.2 PTM 210U: FCC and Industry Canada Regulatory Statements

This device complies with part 15 of the FCC rules and Industry Canada ICES- 003. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. Any changes or modifications not expressly approved by manufacturer could void the user's authority to operate the equipment.

When the product is placed on the US / Canadian market, it must carry the Specified Radio Equipment marking as shown below:

FCC ID:	SZV-PTM210U
IC:	5713A-PTM210U

IMPORTANT! Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

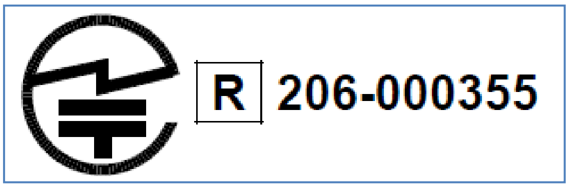
Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes: (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, meme si le brouillage est susceptible d'en compromettre le fonctionnement.

IMPORTANT! Tous les changements ou modifications pas expressément approuvés par la partie responsable de la conformité ont pu vider l'autorité de l'utilisateur pour actioner cet équipment.

7.3 PTM 210J: Japanese Type Approval

PTM 210J complies with the Japanese radio law and is certified according to ARIB STD-T108 V1.0 (2012-02). There is a certification marking on the back side of the module.

When the product is placed on the Japanese market, it must carry the Specified Radio Equipment marking as shown below:



If the certification label cannot be recognized from outside (e.g. installation in a host) appropriate information must be referenced in the user manual.

Using the key combination A0+A1+B1 (see contact nipples designation), PTM 210J transmits a telegram with 48-bit ID as required by Japanese radio law.