PCN #: 2017-11-22
Change title: Adding security features and chip update.
Date of publication: November 22, 2017

Products affected / EnOcean ordering codes

- STM 431J / S3061-D431
- STM 429J / S3061-D429
- STM 250J / S3061-C250
- STM 400J / S3061-D400
- TCM 410J / S3063-K410
- USB 400J / S3064-K400
- PTM 430J / S3101-A430

Description of change STM 431J, STM 429J, STM 250J:

- Added enhanced security mode in addition to present standard mode. Enhanced security includes: AES 128 payload encryption & decryption, Protection against re-play attacks & message forgery by RLC counter and authentication (CMAC)
- Pressing LRN button triggers immediately transmission of TEACH-IN telegram ac-cording actual mode.
- By press & hold (min 10 sec) of LRN Button the module can be switched from standard to secure mode and back at any moment. Factory mode is standard mode. Customers who do not require using enhanced security mode, can continue to use module as before in standard mode. Prevent unintentional pressing of LRN button longer than 10 Sec.
- Removed possibility to configure the behavior of WAKE 1 – LRN Button (Falling and Rising edge). Behavior set to falling edge – press of the button. (Only STM 431J).
- Added configuration of RLC & AES key and parameters to define what is the default mode – secure or standard and whether mode change is allowed or not. Thus mode selection is permanent and no later change enabled. (Only STM 431J).
- LED blinking behavior changed. The LED flashes once after transmission of teach-in telegram in standard mode and twice in secure mode.
- EEPROM to store RLC and AES Key in non-volatile memory added to the product.
- PSK teach-in mode is optional – can be activated by configuration
- Dolphin V4 Chip revision update

Description of change STM 400J:

- Added enhanced security mode in addition to present standard mode. Enhanced security includes: AES 128 payload encryption & decryption, Protection against re-play attacks & message forgery by RLC counter and authentication (CMAC)
- Pressing LRN button triggers immediately transmission of TEACH-IN telegram ac-cording actual mode.
- By long connection (10 sec) of WAKE 1 Pin to GND (LRN Button) the module can be switched from standard to secure mode and back at any moment. Factory mode is standard mode. Customers who do not require using enhanced security mode, can continue to use module as before in standard mode. Prevent unintentional connec-tion of WAKE 1 Pin to GND (LRN Button) longer than 10 Sec.
- Removed possibility to configure the behavior of WAKE 1 – LRN Button (Falling and Rising edge). Behavior set to falling edge – press of the button.

PCN #: 2017-11-22
Change title: Adding security features and chip update.
Date of publication: November 22, 2017

- Added configuration of RLC & AES key and parameters to define what is the default mode – secure or standard and whether mode change is allowed or not. Thus mode selection is permanent and no later change enabled.
- LED blinking behavior adjusted. The LED flashes once after transmission of teach-in telegram in normal mode. The LED flashes twice after transmission of teach-in telegram in secure mode.
- Defined interface for external EEPROM module, EEPROM module is needed to add to customer board to enable secure communication. If secure communication is not required, EEPROM is not needed to add. (STM 400J only)
- If secure communication is not required no change in design-in is needed. Secure mode will not be active, even on long connection of WAKE 1 Pin to GND.
- Hardware configuration pins updated
- Dolphin V4 Chip revision update

Description of change TCM 410J, USB 400J:

- Added enhanced security mode in addition to present standard mode. Enhanced security includes: AES 128 payload encryption & decryption, Protection against replay attacks & message forgery by RLC counter and authentication (CMAC)
- If possible module decrypts secured communication from known IDs and transmits decrypted information on ESP 3 interface. Secured communication from unknown IDs is forwarded on ESP 3 unchanged.
- Unencrypted radio communication is forwarded on ESP 3 interface as usual - function as current TCM 410J is ensured.
- Possibility to encrypt outgoing radio communication
- Added support for ESP 3 commands to configure RLC & AES Key for inbound and outbound communication
- EEPROM to store RLC & AES Key in non-volatile memory added (USB 400J only).
- Defined interface for external EEPROM module. EEPROM module is needed to add to customer board to enable secure communication. If secure communication is not required, EEPROM is not needed to add (TCM 410J only).
- If secure communication is not required no change in design-in is needed
- Dolphin V4 Chip revision update

Description of change PTM 430J:

- Dolphin V4 Chip revision update only

Dolphin V4 Chip revision update (all modules in PCN):

- More precise analog measurement – remove marginal offset to GND
- Mass production chip revision

PCN #: 2017-11-22
Change title: Adding security features and chip update.
Date of publication: November 22, 2017

Milestones

- Samples of new revision available Q4 2017 (Step code DB, Status code pilot series) distributed to all companies ordering affected modules.
- Ordering times of pre change products and post change products will be communicated

Reason for change

- Add security mode to enable security features to protect communication against eaves dropping and replay and forgery attacks. Raise the security confidence of EnOcean radio networks.
- Introduce updated chip revision to products

Step codes & status code after change and serial production started

- STM 431J DB - 10
- STM 429J DB - 10
- STM 250J DB - TBD
- STM 400J DB - 7
- TCM 410J DB - 8
- USB 400J DB - 7
- PTM 430J DB - 5

Customer impact of change and recommended action

- LRN Button behaviour changed.
- Add description of Security and LRN Button behaviour to user manual of final product.
- If secure operation is not required / used module can be used as-is today

Reference Documents / Attachments

- User manuals of affected products will be distributed with samples

PCN revision history

Date of revision	Author	Revision number	Reason
November 22, 2017	MH	00	Original PCN