EMBS LoRa 433 benefits

Specification

- 433 MHz – 434.750 MHz frequency range
- LoRa modulation is used
- Multicast/broadcast
- Configurable confirmation modes: with or without ACK
- Configurable bandwidth: 125kHz (lower data rate, longer range) – 500 kHz (higher data rate, shorter range)
- Configurable spreading factor: SF7 (higher data rate, shorter range) – SF12 (lower data rate, longer range)
- Configurable TX power: 2 dBm – 17dBm
- Configurable channels: 15 frequencies, 8 non-overlapping when 125kHz bandwidth is used
- Protocol is optimized for using LoRa without batteries
- Fully European technology – the standard, ICs, final solution

Specification

- Filtering possibility for LoRa telegrams

- Listen before talk mechanism for collision avoidance

- Optional statistics data for each received telegram: physical address, RSSI and TX power

Address	Name	Datatype	Tags	Value	Properties
0/0/1	UIO8 (8 Universal IO ports + LoRa) - Statistics	4.5. 4 byte LoRa status		0.1 / -15 dB / 17 dBm	E R P

- Simultaneous wired and wireless connections (wired – for security sensitive operations to avoid sniffing, brute-force etc.). Transparent bridge mode

- No single point of failure compared to other widely used client-server technologies e.g. LoRaWAN

Date rates

Best case: SF7 / 500 kHz = 16ms per message (22 kbps)

Default: SF7 / 125 kHz = 62ms per message (5.5kbps)

Worst case: SF12 / 125 kHz = 1300ms per message (0.3 kbps)

2x increase in bandwidth provides 2x less air time

SF+1 takes approximately 2x more air time compared to previous SF

Why 433 MHz?

- 4x longer distance than 868 MHz
- 433 MHz is less crowded than 868 MHz used by other technologies like Zwave, EnOcean etc.
- Much lower mobile network interference
- Much better wall penetration
- Lower signal dissipation in atmosphere – less energy is needed for transmission of the same amount of data compared to 868 MHz (increasing the frequency by 2x increases losses by 4x)

Universal technology

- Most other technologies are not universal and are designed for either long-range LPWAN networks or short range e.g. BLE

- Type of priority – range, bit rate, energy (battery drain) can be freely adjusted depending on project needs

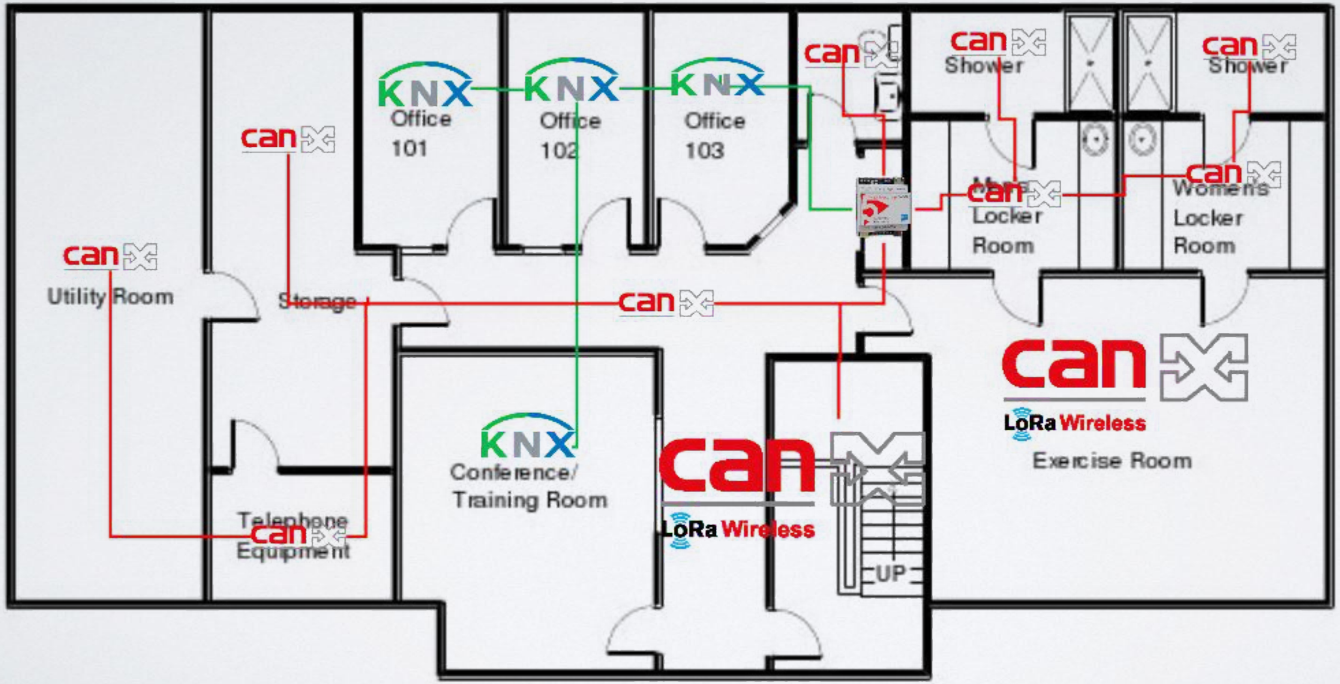
- Statistics data can be used to check signal levels. Channel Energy reserve is always known and can be increased by lowering bandwidth, increasing spreading factor or increasing TX power

Visual indicators

- Each device has LED indicators for RX/TX activity. This is very important for installers to be able to perform diagnostics without additional tools

- Statistics application provides a visual representation of signal levels for all received radio telegrams

CANx, KNX, LoRa architecture



Security – most important part of any installation

- Considering how major security flaws appear in many products today, soon enough people working with security will be the main decision makers whether a device can be installed or not
- Both passive and active security measures must be implemented in order to create a robust system

Passive security in CANx/LoRa

- Devices can only be configured over wired connection. This excludes any remote configuration changes without direct access to the network. Radio transport is used only for data messages
- There is no public key exchange or any other security-related configuration possible over wireless
- Firmware upgrades are possible only by physically accessing each device. There are plenty of precedents when over-the-air upgrades were used in attacks, for example Xiaomi Scooter: https://www.wired.com/story/xiaomi-scooter-hack/

Active security in CANx/LoRa

- Configuration messages can be blocked when using wired connection. Enabling and disabling this block requires a unique network key which is programmed once during commissioning and cannot be read back from devices

- Radio messages are time-stamped to prevent replay attacks. Each devic compares time-stamp from received messages with internal clock. If time difference is larger than accepted range the message is ignored. Central gateway device provides synchronization timing beacons

Security based on ChaCha20

- More advanced than AES128 encryption

- The implementation reference for ChaCha20 has been published in RFC 7539; proposed standardization of its use in TLS is published as RFC 7905; use of ChaCha20 in IKE and IPsec have been proposed for standardization in RFC 7634

- Widely used in operating systems, VPN protocols and Internet security (e.g. Google's implementation secures https (TLS/SSL) traffic between the Chrome browser on Android phones and Google's websites)*

* https://en.wikipedia.org/wiki/Salsa20

Regulatory compliance

Nonspecific short range device allowance in Europe*

Frequency Band	ERP	Duty Cycle	Channel Bandwidth
433.05 – 434.79 MHz	+10 dBm	<10%	No limits
433.05 – 434.79 MHz	0 dBm	No limits	No limits
433.05 – 434.79 MHz	+10 dBm	No limits	<25 kHz

* http://www.ti.com/lit/an/swra048/swra048.pdf

embedded
systems