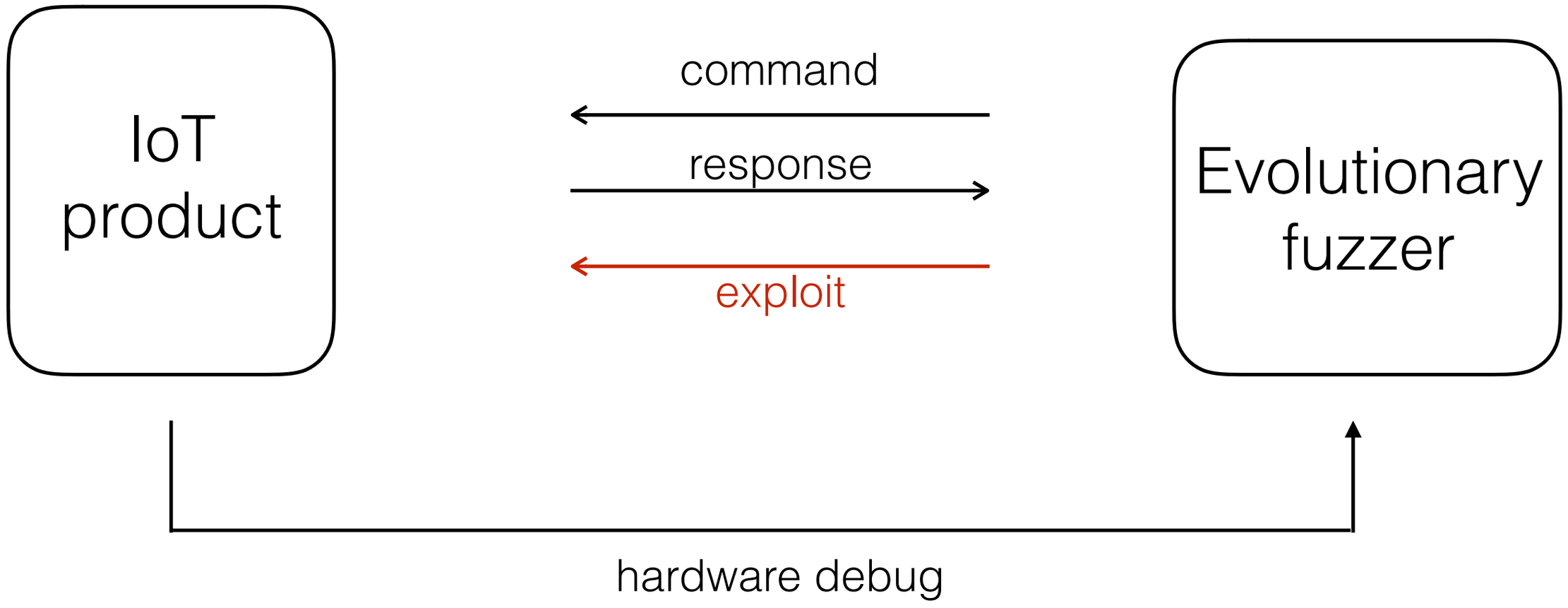
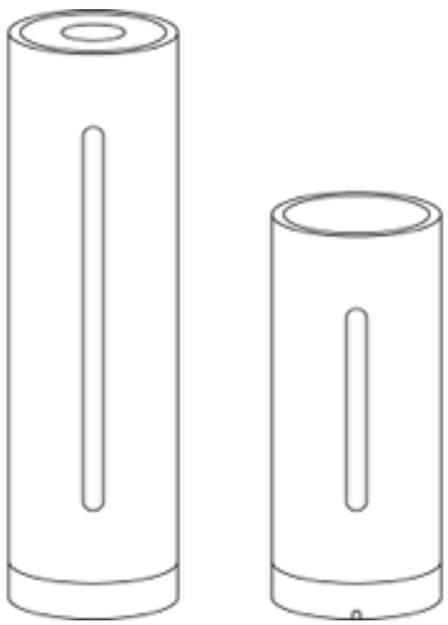
Goal


IoT product
command
response
exploit
Evolutionary fuzzer
hardware debug

Goal



command

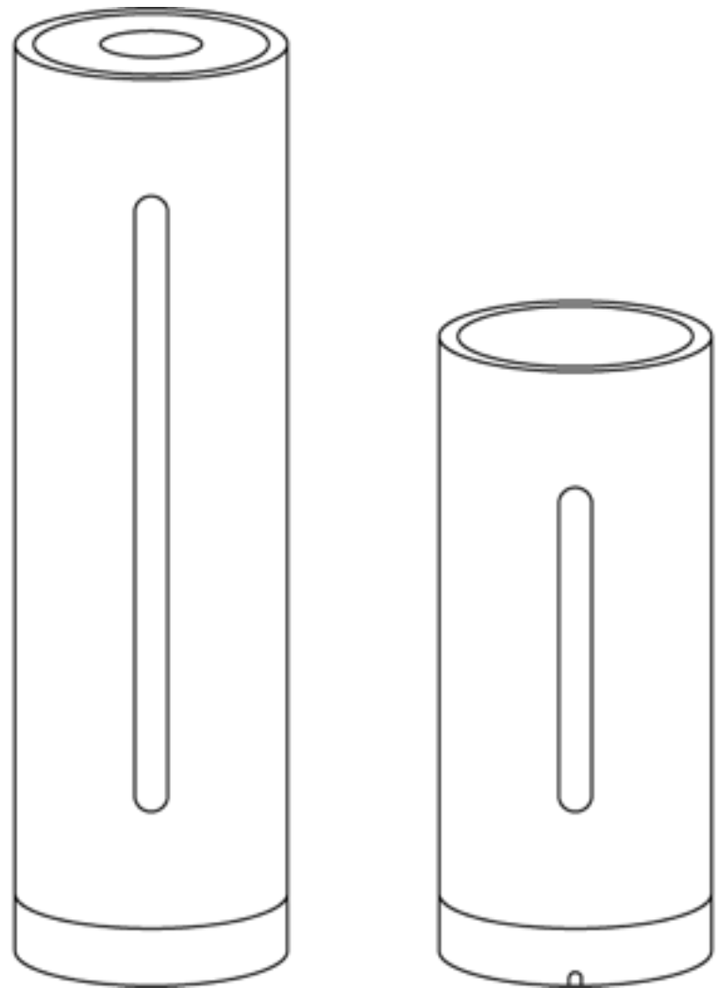
response

exploit

Evolutionary fuzzer

hardware debug

Netatmo weather station



Functionalities

Indoor
temperature

Indoor
humidity

Indoor
air quality

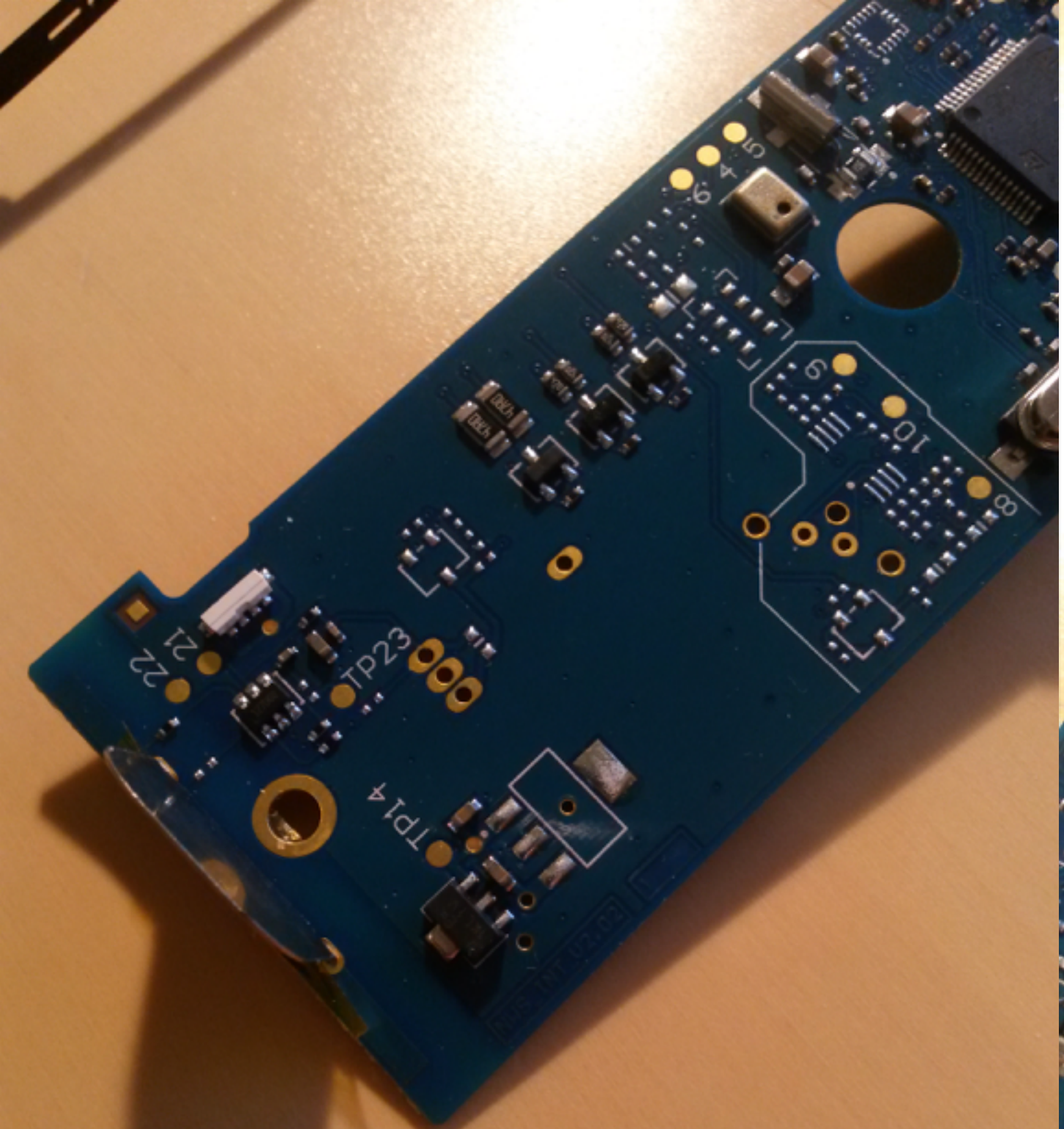
CO2

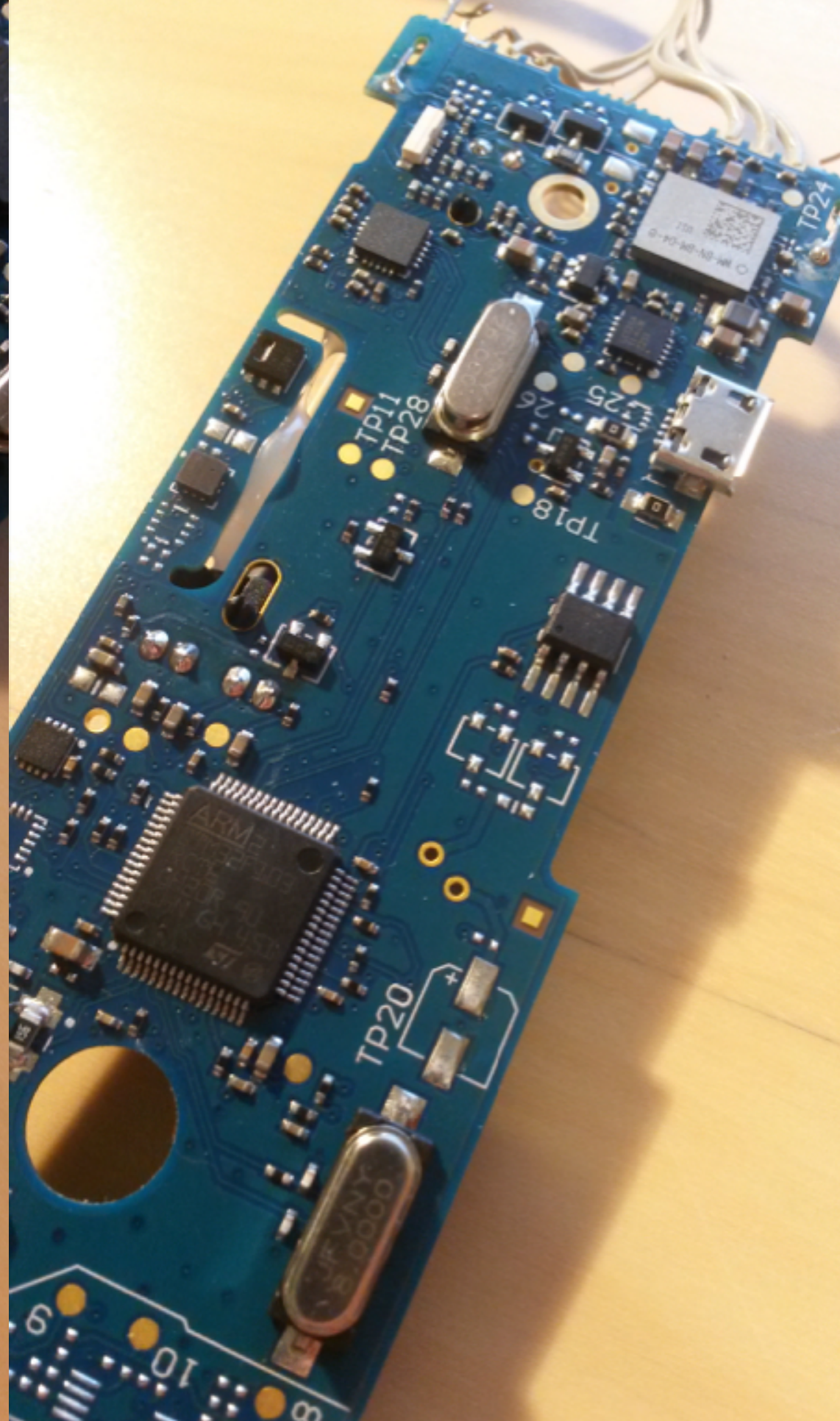
Sound meter

indoor module

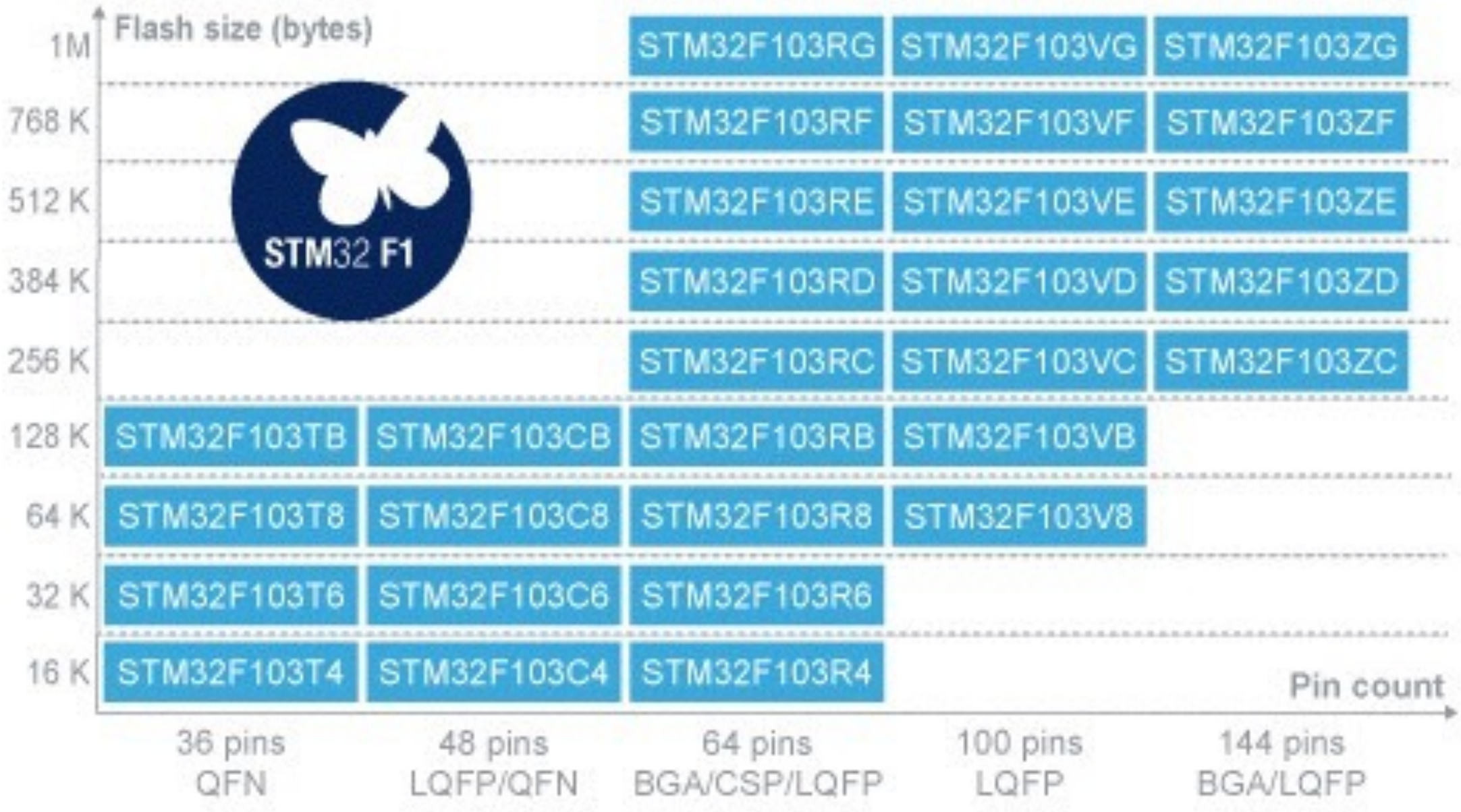
Netatmo components

- STM32F103 - 72MHz - 256KB - 32KB ram ARM CORTEX-M
- Flash Memory Spansion FL216KIF 2MB
- Sub 1GHz RF Transceiver CC110L
- 802.11 b/g/n, BT, FM radio WMBNBM04a
- Temperature and humidity sensor SHT20
- C02 sensor
- 2D 47 2429 E7S RT microphone

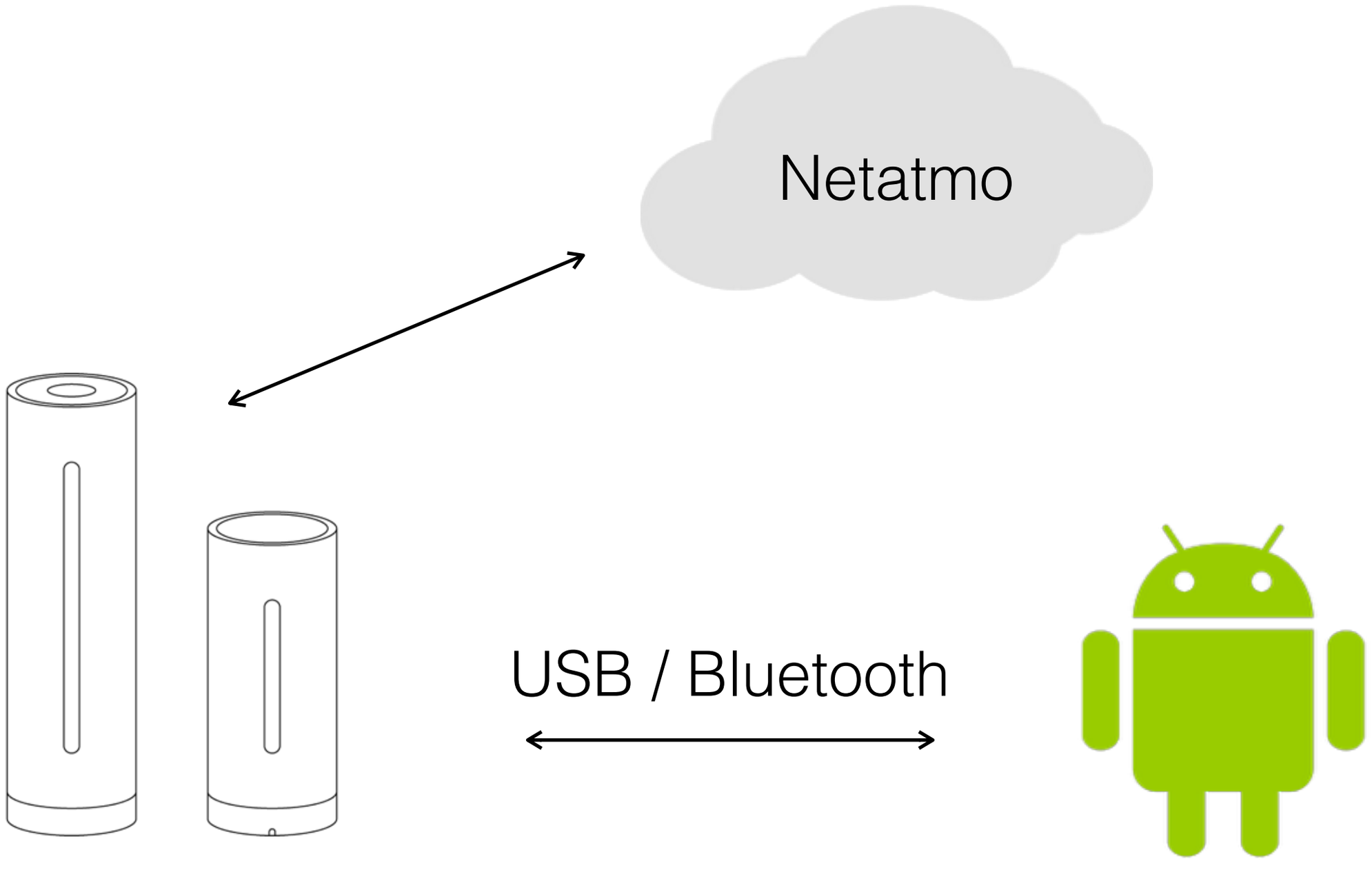

TP23
TP14


TP24
TP11
TP28
TP18
TP20

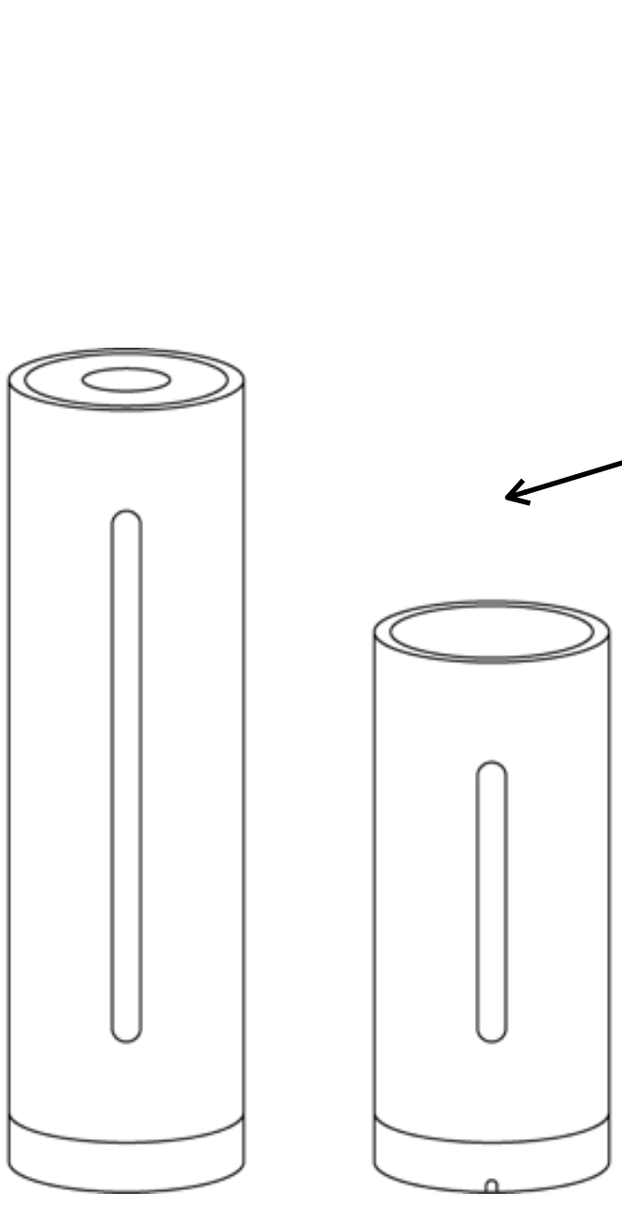
STM32F103

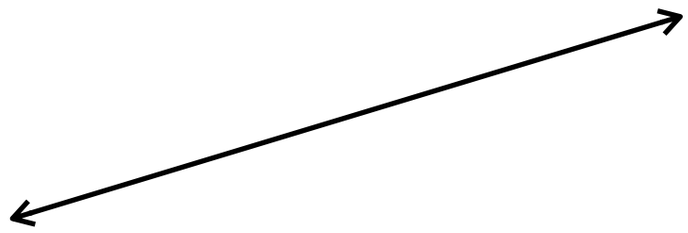

Flash size (bytes)
1M
768 K
512 K
384 K
256 K
128 K
64 K
32 K
16 K
STM32 F1
STM32F103RG
STM32F103VG
STM32F103ZG
STM32F103RF
STM32F103VF
STM32F103ZF
STM32F103RE
STM32F103VE
STM32F103ZE
STM32F103RD
STM32F103VD
STM32F103ZD
STM32F103RC
STM32F103VC
STM32F103ZC
STM32F103TB
STM32F103CB
STM32F103RB
STM32F103VB
STM32F103T8
STM32F103C8
STM32F103R8
STM32F103V8
STM32F103T6
STM32F103C6
STM32F103R6
STM32F103T4
STM32F103C4
STM32F103R4
Pin count
36 pins
QFN
48 pins
LQFP/QFN
64 pins
BGA/CSP/LQFP
100 pins
LQFP
144 pins
BGA/LQFP

Configuration (WiFi)



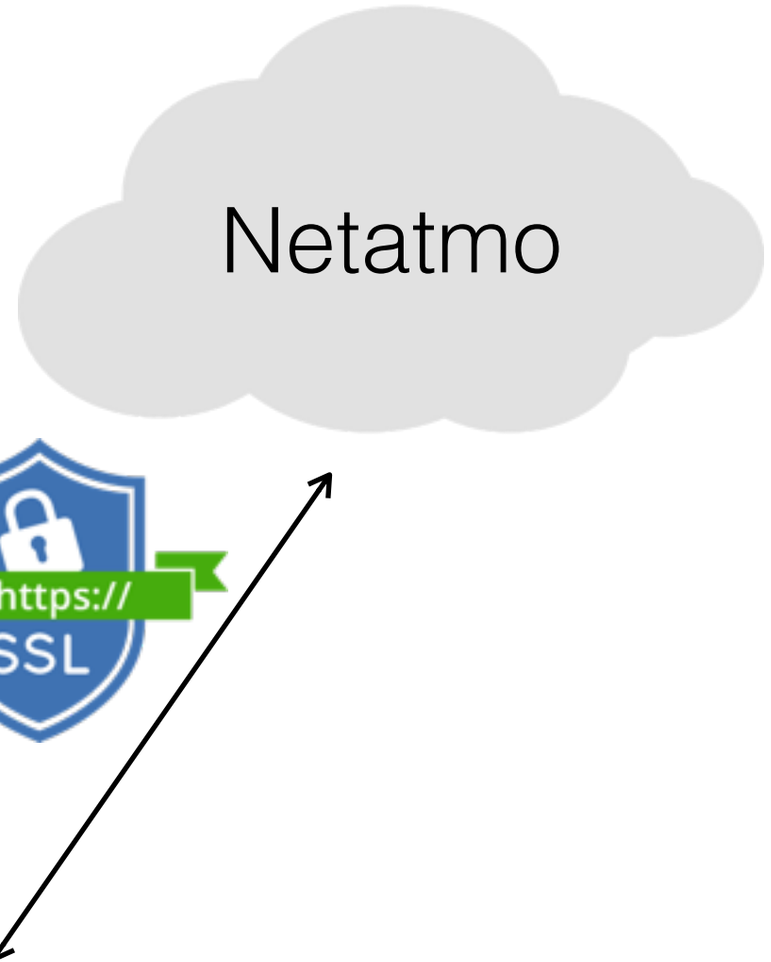
Working mode (WiFi)

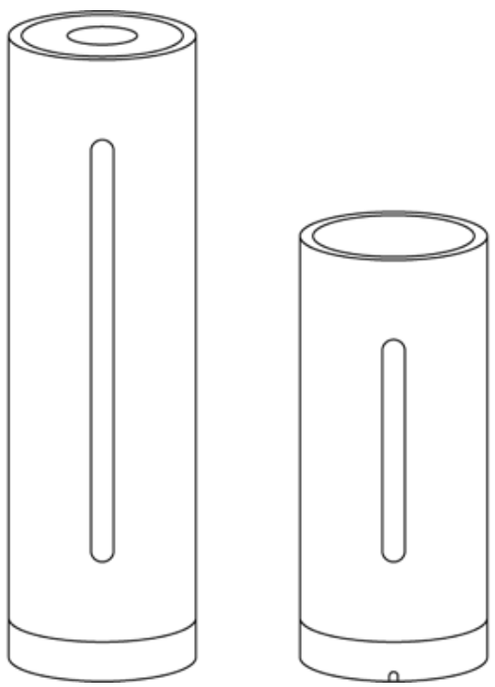




Communication is in plain
Data is probably obfuscated

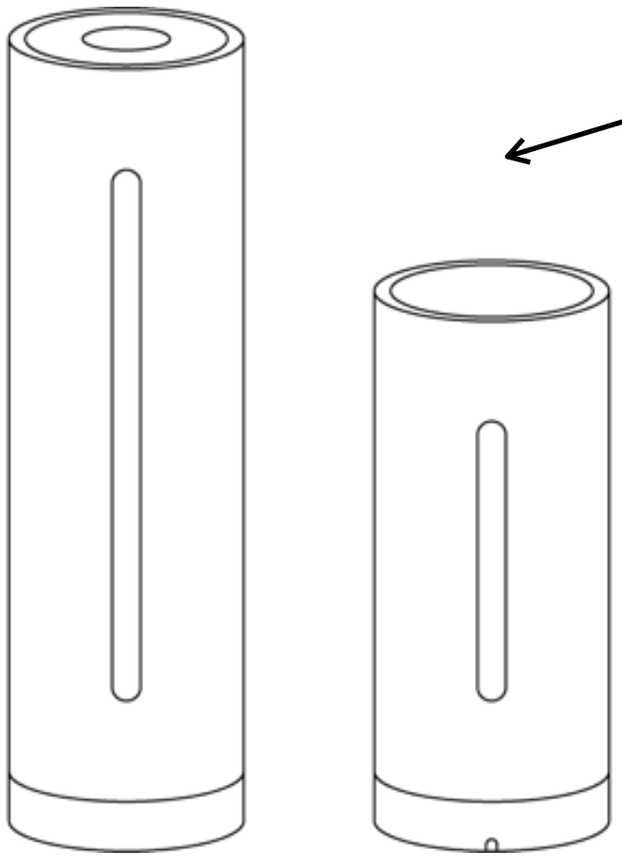
Firmware update

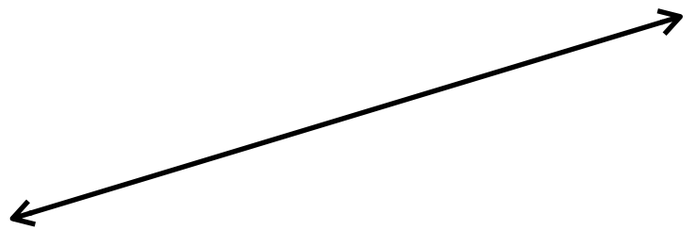




USB / Bluetooth

Firmware update 2





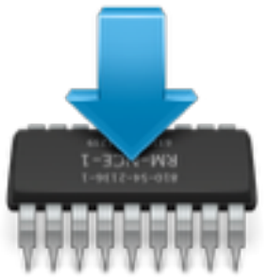
Still not tested

CVE
cve.mitre.org

- Send Clear Wifi password to Netatmo Server *(CVE-2015-1600)*

- Expose Wifi SSID e password through USB *(CVE requested)*

- Expose Wifi SSID e password through Bluetooth *(CVE requested)*



Firmware dump

- Download from Netatmo server
- Sniff network traffic during update
- Sniff Bluetooth/USB traffic during update
- Jtag / SWD, USART, DFU
- Read Flash memory

Firmware dump

- Download from Netatmo server
- Sniff network traffic during update
- Sniff Bluetooth/USB traffic during update
- Jtag / SWD, USART, DFU
- Read Flash memory

Netatmo weather family

modulo interno

anemometro

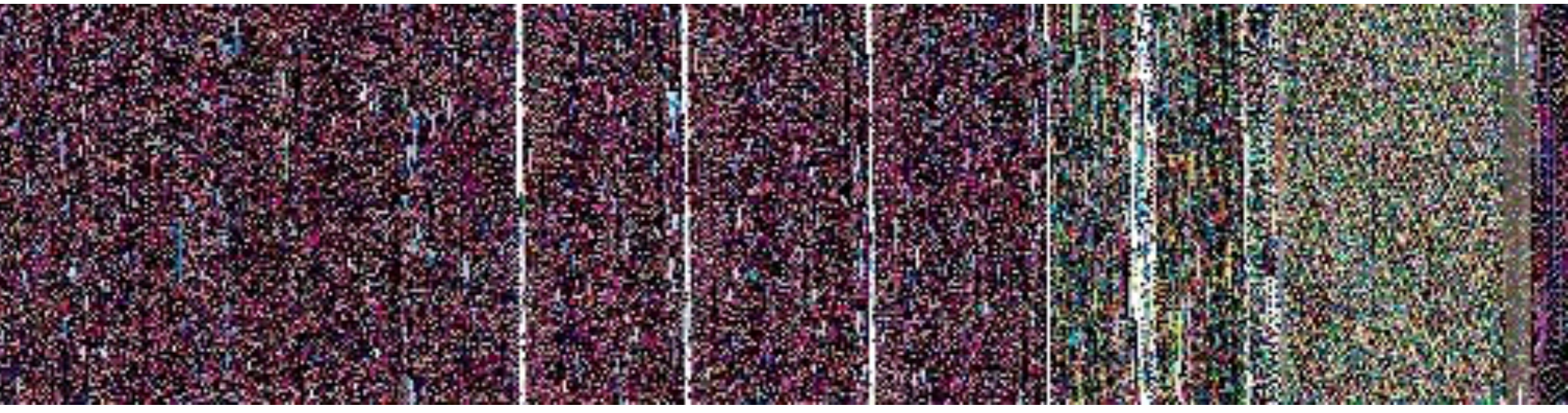
pluviometro

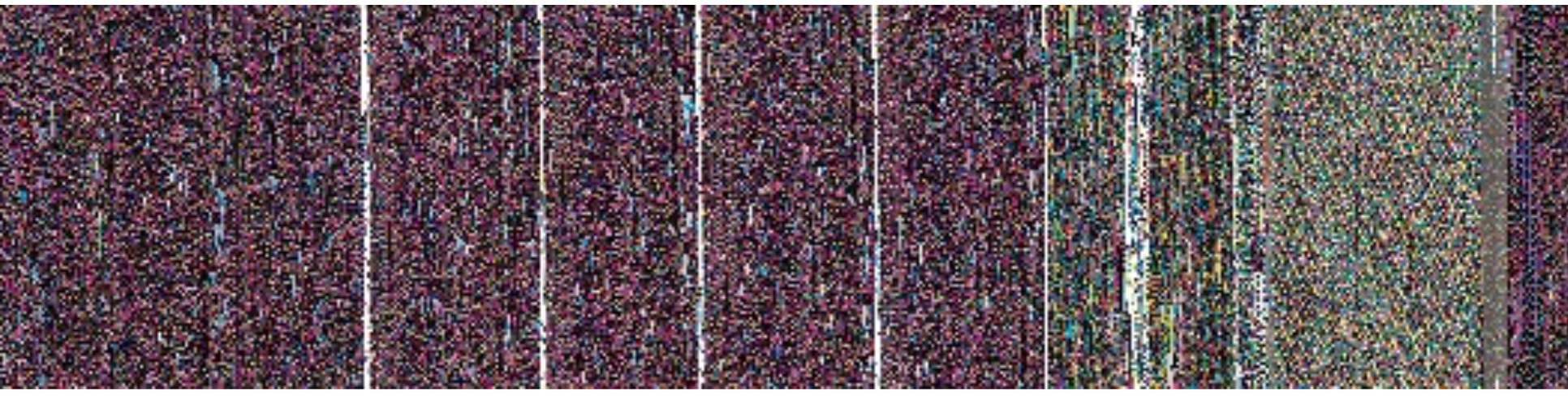
modulo esterno

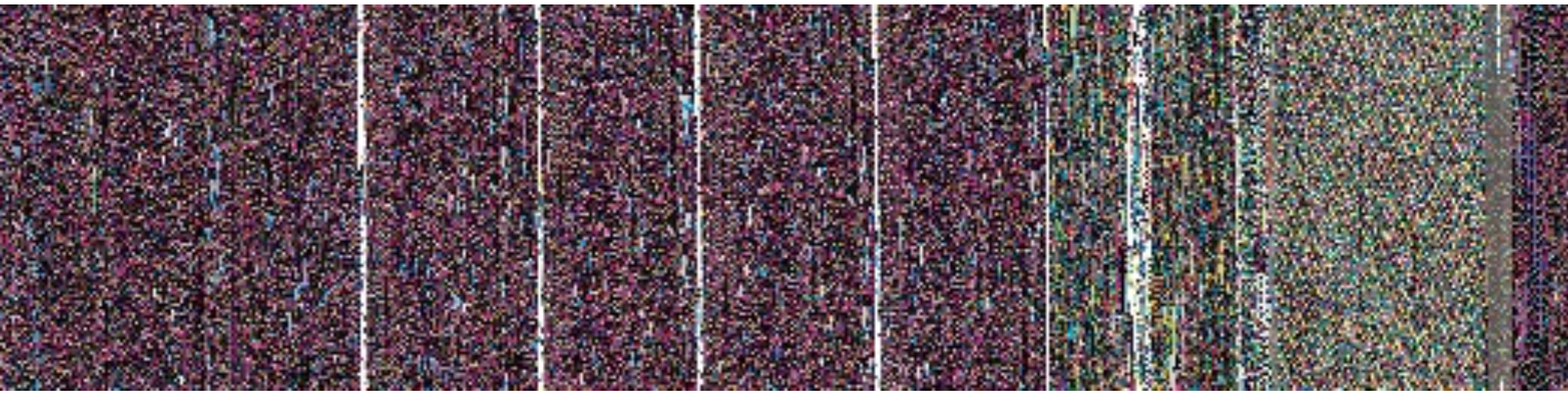
Firmware comparison

	nwsV2_101	nwsV2_115	nwsV2_119
Indoor	101	115	119
Outdoor	43	43	43
Rain Gauge	8	8	8
Wind Gauge	-	11	14
dimensione	540 KB	580 KB	580 KB

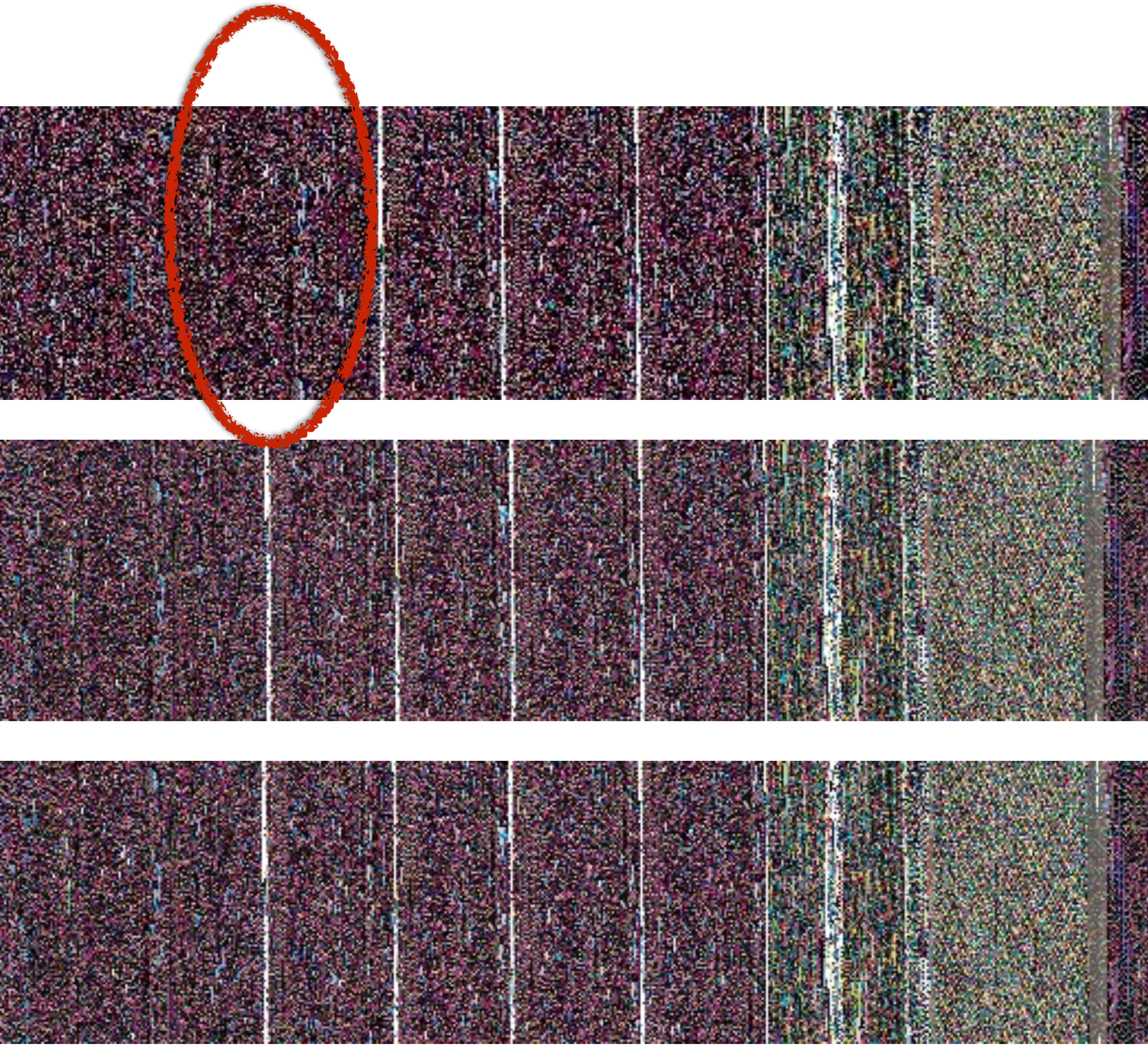
Firmware comparison



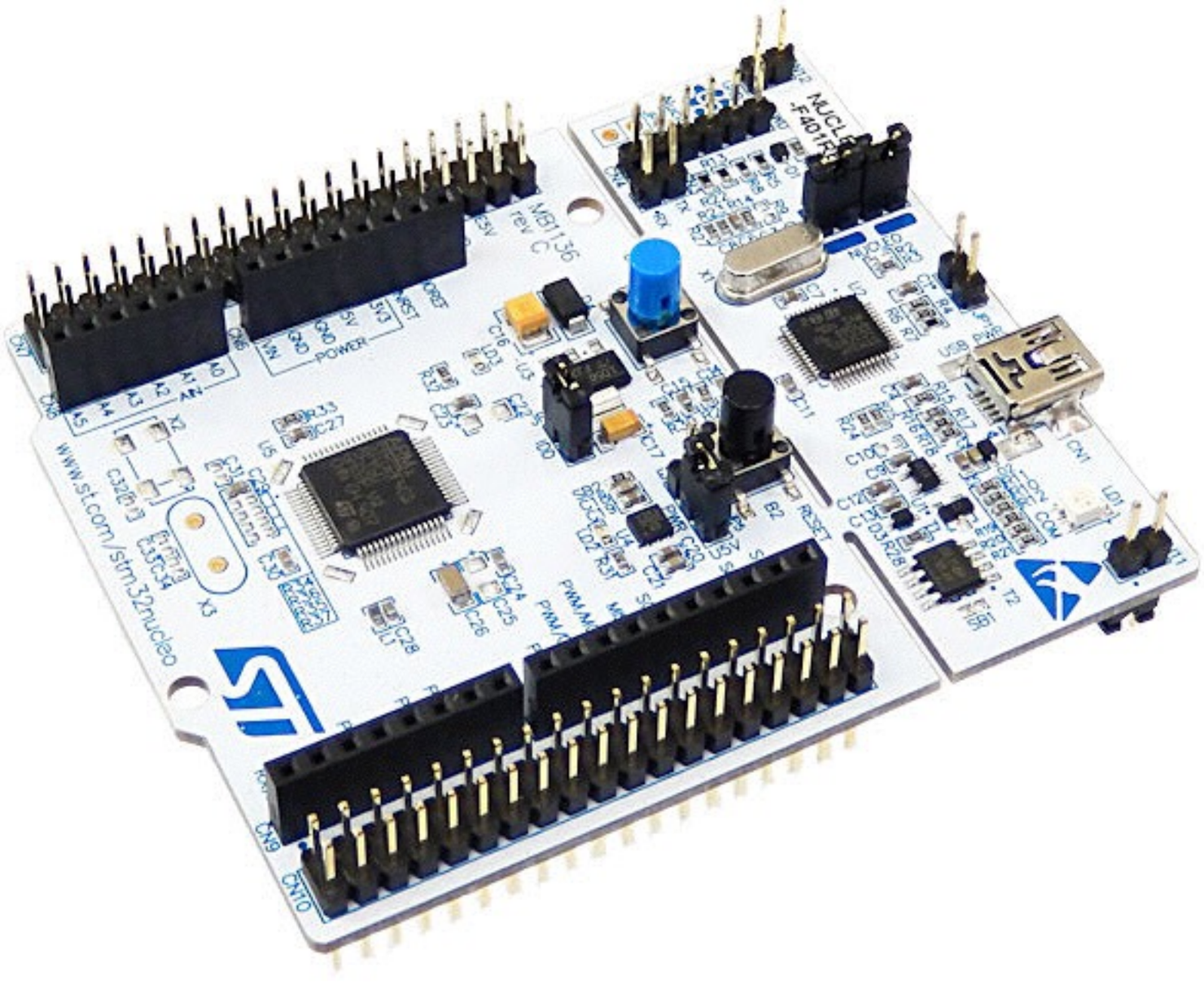




Firmware comparison



Debugging



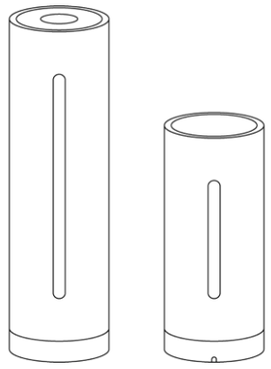
STM32 nucleo

JTAG/SWD

UART

Fuzzing

- Real Firmware
  - Simple to execute
  - Hard to detect bugs



- Emulated Firmware
  - Hard to setup
  - Simpler to detect bugs

Qemu