



TEST REPORT

Applicant Name..... : Mid Ocean Brands B.V.
Address..... : Unit 711-716, 7/F., Tower A, 83 King Lam Street, Cheung Sha Wan,
Kowloon, Hong Kong.
Manufacturer Name..... :
Address..... :
Product..... : smart band
Model(s)..... : MO2270
Additional Model(s)..... : /
Trademark..... : /
Model Difference..... : /
Prepared by..... : Guangdong Zhonghan Testing Technology Co., Ltd.
Address..... : Room 104/201, Building 1, Yibaolai Industrial Park, Qiaotou, Fuhai
Subdistrict, Bao'an District, Shenzhen, Guangdong, China
Date of Receipt..... : Aug. 14, 2026
Date of Test(s)..... : Aug. 14, 2026 to Aug. 27, 2026
Date of Issue..... : Sept. 15, 2026
Test Requested..... : Select test(s) as requested by the client.
Test Standard(s)..... : ETSI EN 300 328 V2.2.2 (2019-07)

In the configuration tested, the EUT complied with the standards specified above.

Prepared by:

Kimi Lu

Kimi Lu/ Engineer

Reviewed by:

Baret Wu

Baret Wu/ Director



Note: The results shown in this test report refer only to the sample(s) tested unless otherwise stated. This test report shall not be reproduced except in full, without prior written approval of ZHT. This document may be altered or revised by ZHT, personnel only, and shall be noted in the revision of the document.

**Table of Contents**

1. Revision History	4
2. Test Summary	5
3. Product Information And Test Setup	6
3.1. Product Information	6
3.2. Test Setup Configuration	6
3.3. Support Equipment	6
3.4. Channel List	7
3.5. Test Mode	7
3.6. Test Environment	7
4. Test Facility And Test Instrument Used	8
4.1. Test Facility	8
4.2. Test Instrument Used	8
4.3. Testing software	9
4.4. Measurement Uncertainty	9
5. RF Output Power	10
5.1. Block Diagram Of Test Setup	10
5.2. Limit	10
5.3. Test procedure	10
5.4. Test Result	12
6. Power Spectral Density	13
6.1. Block Diagram Of Test Setup	13
6.2. Limit	13
6.3. Test procedure	13
6.4. Test Result	15
7. Adaptivity	19
7.1. Block Diagram Of Test Setup	19
7.2. Limit	19
7.3. Test procedure	20
7.4. Test Result	21
8. Occupied Channel Bandwidth	22
8.1. Block Diagram Of Test Setup	22
8.2. Limit	22
8.3. Test procedure	22
8.4. Test Result	23
9. Transmitter Unwanted Emissions In The Out-of-band Domain	27
9.1. Block Diagram Of Test Setup	27
9.2. Limit	27
9.3. Test procedure	27
9.4. Test Result	30
10. Transmitter Unwanted Emissions In The Spurious Domain	32
10.1. Block Diagram Of Test Setup	32
10.2. Limits	32
10.3. Test Procedure	33



10.4. Test Results	34
11. Receiver Spurious Emissions	35
11.1. Block Diagram Of Test Setup	35
11.2. Limits	35
11.3. Test Procedure	35
11.4. Test Results	37
12. Receiver Blocking	38
12.1. Block Diagram Of Test Setup	38
12.2. Limit	38
12.3. Test procedure	39
12.4. Test Result	40
13. Photos Of Test Setup	41
14. EUT Photographs	42



1. Revision History

Report No.	Issue Date	Description	Approved
ZHT-260814107W01-2	Aug. 27, 2026	Original	Invalid
ZHT-260814107W01-2M1	Sept. 10, 2026	This report modifies the parameter description based on the original report number ZHT-260814107W01-2. The only difference between the new parameters and the original parameters is the way they are described, which does not affect the test results. Therefore, there is no need to add new tests to this report. All test data are referenced from the original report with reference number ZHT-260814107W01-2	Valid
ZHT-260910112W01-2	Sept. 15, 2026	This report has added the name and address of the applicant based on the original report number ZHT-260814107W01-2M1. The only difference between this report and the original report is their applicant name and address, which will not affect the test results. Therefore, there is no need to add new tests to this report. All test data are based on the original report, reference number ZHT-260814107W01-2M1	Valid



2. Test Summary

The Product has been tested according to the following specifications:

Standard	ETSI EN 300 328 V2.2.2		
Test Item	Test Requirement	Test Method	Results
Transmitter Parameters			
RF Output Power	Clause 4.3.1.2	Clause 5.4.2	PASS
Power Spectral Density	Clause 4.3.2.3	Clause 5.4.3	PASS
Duty cycle, Tx-Sequence, Tx-gap	Clause 4.3.1.3	Clause 5.4.2	N/A ²
Accumulated Transmit time, Frequency Occupation & Hopping Sequence	Clause 4.3.1.4	Clause 5.4.4	N/A ¹
Hopping Frequency Separation	Clause 4.3.1.5	Clause 5.4.5	N/A ¹
Medium Utilization	Clause 4.3.1.6	Clause 5.4.2	N/A ²
Adaptivity	Clause 4.3.1.7	Clause 5.4.6	N/A ³
Occupied Channel Bandwidth	Clause 4.3.1.8	Clause 5.4.7	PASS
Transmitter unwanted emissions in the OOB domain	Clause 4.3.1.9	Clause 5.4.8	PASS
Transmitter unwanted emissions in the spurious domain	Clause 4.3.1.10	Clause 5.4.9	PASS
Receiver Parameters			
Receiver spurious emissions	Clause 4.3.1.11	Clause 5.4.10	PASS
Receiver Blocking	Clause 4.3.1.12	Clause 5.4.11	PASS
Geo-location capability	Clause 4.3.1.13	Clause 5.4.12	N/A ⁴
Remark: N/A ¹ : Only for equipment using wide band modulations other than FHSS N/A ² : Only for non-Adaptive equipment. N/A ³ :The maximum output power of EUT less than 10dBm, so not applicable N/A ⁴ : Only for equipment with geo-location capability Tx: In this whole report Tx (or tx) means Transmitter. Rx: In this whole report Rx (or rx) means Receiver. RF: In this whole report RF means Radiated Frequency. CH:In this whole report CH means channel.			



3. Product Information And Test Setup

3.1. Product Information

Product Name: smart band

Test Model(s): MO2270

Hardware Version: V1.0

Software Version: V1.0

Operation Frequency: BLE: 2402MHz-2480MHz, 40 Channels

Type of Modulation: BLE: GFSK

Antenna installation: PCB Antenna

Antenna Gain: 0dBi

Ratings: Input: 5V --- 0.5A
Internal 3.7V Rechargeable Li-ion battery

Sample Number: 260814107YP001

Remark: The antenna gain is provided by the customer, if the data provided by the customer is not accurate, Guangdong Zhonghan Testing Technology Co., Ltd. does not assume any responsibility.

3.2. Test Setup Configuration

EUT

3.3. Support Equipment

Item	Equipment	Mfr/Brand	Model/Type No.	Note

Notes:

- 1) All the equipment/cables were placed in the worst-case configuration to maximize the emission during the test.
- 2) Grounding was established in accordance with the manufacturer's requirements and conditions for the intended use.



3.4. Channel List

CH No.	Frequency (MHz)	CH No.	Frequency (MHz)	CH No.	Frequency (MHz)	CH No.	Frequency (MHz)
0	2402	1	2404	2	2406	3	2408
4	2410	5	2412	6	2414	7	2416
8	2418	9	2420	10	2422	11	2424
12	2426	13	2428	14	2430	15	2432
16	2434	17	2436	18	2438	19	2440
20	2442	21	2444	22	2446	23	2448
24	2450	25	2452	26	2454	27	2456
28	2458	29	2460	30	2462	31	2464
32	2466	33	2468	34	2470	35	2472
36	2474	37	2476	38	2478	39	2480

3.5. Test Mode

All test mode(s) and condition(s) mentioned were considered and evaluated respectively by performing full tests, the worst data were recorded and reported.

Test mode	Low channel	Middle channel	High channel
Transmitting(GFSK)	2402MHz	2440MHz	2480MHz
Receiving(GFSK)	2402MHz	2440MHz	2480MHz

3.6. Test Environment

Humidity(%):	54.2
Atmospheric Pressure(kPa):	101.4
Normal Temperature(°C)	24.5
Low Temperature(°C)	-10
High Temperature(°C)	45



4. Test Facility And Test Instrument Used

4.1. Test Facility

Guangdong Zhonghan Testing Technology Co., Ltd.

Room 104/201, Building 1, Yibaolai Industrial Park, Qiaotou, Fuhai Subdistrict, Bao'an District,
Shenzhen, Guangdong, China

4.2. Test Instrument Used

Item	Equipment	Manufacturer	Model	Serial No.	Last Cal.	Next Cal.
1	Receiver	R&S	ESCI	100874	Apr. 24, 2026	Apr. 23, 2027
2	Loop Antenna	TESEQ	HLA6121	58357	Sept. 8, 2025	Sept. 7, 2026
3	Amplifier	Schwarzbeck	BBV 9743 B	00378	Apr. 24, 2026	Apr. 23, 2027
4	Amplifier	Schwarzbeck	BBV 9718 B	00040	May 8, 2026	May 7, 2027
5	Bilog Antenna	Schwarzbeck	VULB9162	00498	Apr. 25, 2026	Apr. 24, 2027
6	Horn Antenna	Schwarzbeck	BBHA9120D	02623	Apr. 25, 2026	Apr. 24, 2027
7	Horn Antenna	A.H.SYSTEM S	SAS574	588	Oct. 20, 2025	Oct. 19, 2026
8	Amplifier	AEROFLEX	100KHz- 40GHz	097	Oct. 20, 2025	Oct. 19, 2026
9	Spectrum Analyzer	R&S	FSV40	101413	Apr. 24, 2026	Apr. 23, 2027
10	Spectrum Analyzer	KEYSIGHT	N9020A	MY5342020 8	Apr. 24, 2026	Apr. 23, 2027
11	WIDBAND RADIO COMMUNICATION TESTER	R&S	CMW500	109863	Apr. 24, 2026	Apr. 23, 2027
12	Single Generator	Agilent	N5182A	MY4818057 5	Apr. 24, 2026	Apr. 23, 2027
13	Power Sensor	MWRFTest	MW100-RFCB	/	Apr. 24, 2026	Apr. 23, 2027
14	Power Amplifier Shielding Room	EMToni	2m3m3m	/	Apr. 11, 2026	Apr. 10, 2031
15	CABLE	EMToni	DA800-NM- NM-11000MM	/	Apr. 24, 2026	Apr. 23, 2027

4.3. Testing software

Project	Software name	Edition
RF Conducted	MTS 8310	4.0.0.0
Radiated electromagnetic disturbances	EZ-EMC	EMC-CON 3A1.1+

4.4. Measurement Uncertainty

Where relevant, the following measurement uncertainty levels have been estimated for tests performed on the Product as specified in CISPR 16-4-2. This uncertainty represents an expanded uncertainty expressed at approximately the 95% confidence level using a coverage factor of $k=2$.

No.	Item	Uncertainty
1	AC Conducted Emission Test	U=0.92dB
2	3m chamber Radiated spurious emission(9KHz-30MHz)	U=1.6dB
3	3m chamber Radiated spurious emission(30MHz-1GHz)	U=5.1dB
4	3m chamber Radiated spurious emission(1GHz-18GHz)	U=3.9dB
5	3m chamber Radiated spurious emission(18GHz-40GHz)	U=5.0dB
6	Conducted Adjacent channel power	U=1.38dB
7	Conducted output power uncertainty Above 1G	U=1.576dB
8	Conducted output power uncertainty below 1G	U=1.28dB
9	humidity uncertainty	U=5.3%

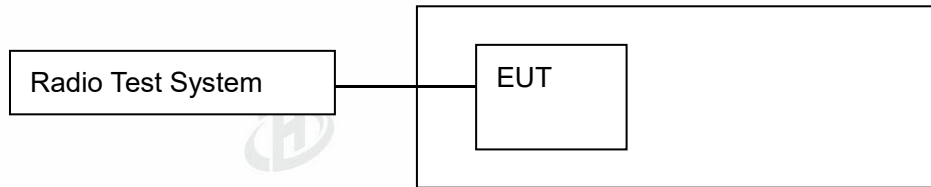
Decision Rule

- ☒ Uncertainty is not included
☐ Uncertainty is included



5. RF Output Power

5.1. Block Diagram Of Test Setup



5.2. Limit

For adaptive equipment using wide band modulations other than FHSS, the maximum RF output power shall be 20 dBm.

The maximum RF output power for non-adaptive equipment shall be declared by the supplier and shall not exceed 20 dBm. See clause 5.3.1 m). For non-adaptive equipment using wide band modulations other than FHSS, the maximum RF output power shall be equal to or less than the value declared by the supplier.

This limit shall apply for any combination of power level and intended antenna assembly.

Limit
20dBm

5.3. Test procedure

Step 1:

- Use a fast power sensor suitable for 2.4 GHz and capable of minimum 1 MS/s.
- Use the following settings:
 - Sample speed 1 MS/s or faster.
 - The samples shall represent the RMS power of the signal.
- Measurement duration: For non-adaptive equipment: equal to the observation period defined in clause 4.3.1.3.2 or clause 4.3.2.4.2. For adaptive equipment, the measurement duration shall be long enough to ensure a minimum number of bursts (at least 10) are captured.

NOTE 1: For adaptive equipment, to increase the measurement accuracy, a higher number of bursts may be used.

Step 2:

- For conducted measurements on devices with one transmit chain:
 - Connect the power sensor to the transmit port, sample the transmit signal and store the raw data. Use these stored samples in all following steps.
- For conducted measurements on devices with multiple transmit chains:
 - Connect one power sensor to each transmit port for a synchronous measurement on all transmit ports.
 - Trigger the power sensors so that they start sampling at the same time. Make sure the time



difference between the samples of all sensors is less than 500 ns.

- For each individual sampling point (time domain), sum the coincident power samples of all ports and store them. Use these summed samples in all following steps.

Step 3:

- Find the start and stop times of each burst in the stored measurement samples.

The start and stop times are defined as the points where the power is at least 30 dB below the highest value of the stored samples in step 2.

NOTE 2: In case of insufficient dynamic range, the value of 30 dB may need to be reduced appropriately.

Step 4:

- Between the start and stop times of each individual burst calculate the RMS power over the burst using the formula below. Save these P_{burst} values, as well as the start and stop times for each burst.

$$P_{burst} = \frac{1}{k} \sum_{n=1}^k P_{sample}(n)$$

with 'k' being the total number of samples and 'n' the actual sample number

Step 5:

- The highest of all P_{burst} values (value "A" in dBm) will be used for maximum e.i.r.p. calculations.

Step 6:

- Add the (stated) antenna assembly gain "G" in dBi of the individual antenna.
- If applicable, add the additional beamforming gain "Y" in dB.
- If more than one antenna assembly is intended for this power setting, the maximum overall antenna gain (G or G + Y) shall be used.
- The RF Output Power (P) shall be calculated using the formula below:

$$P = A + G + Y$$

- This value, which shall comply with the limit given in clause 4.3.1.2.3 or clause 4.3.2.2.3, shall be recorded in the test report.

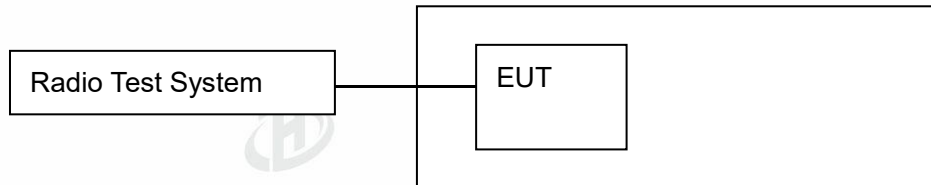
**5.4. Test Result**

Modulation	Test conditions (Temperature)	EIRP (dBm)		
		Low Channel	Middle Channel	High Channel
GFSK-1M	Normal	-4.18	-2.9	-4.02
	Low	-4.34	-3.14	-4.17
	High	-4.55	-3.27	-4.23
GFSK-2M	Normal	-4.33	-2.95	-4.06
	Low	-4.57	-3.15	-4.13
	High	-4.49	-3.21	-4.09
Limit		≤100mW (20dBm)		
Remark: P = A + G + Y, G=0dBi, Y=0				



6. Power Spectral Density

6.1. Block Diagram Of Test Setup



6.2. Limit

For equipment using wide band modulations other than FHSS, the maximum Power Spectral Density is limited to 10 dBm per MHz.

Limit
10dBm/MHz

6.3. Test procedure

Step 1:

Connect the UUT to the spectrum analyser and use the following settings:

- Start Frequency: 2 400 MHz
- Stop Frequency: 2 483,5 MHz
- Resolution BW: 10 kHz
- Video BW: 30 kHz
- Sweep Points: > 8 350

NOTE: For spectrum analysers not supporting this number of sweep points, the frequency band may be segmented.

- Detector: RMS
- Trace Mode: Max Hold
- Sweep time: 10 s; the sweep time may be increased further until a value where the sweep time has no impact on the RMS value of the signal

For non-continuous signals, wait for the trace to stabilize.

Save the data (trace data) set to a file.

**Step 2:**

For conducted measurements on smart antenna systems using either operating mode 2 or operating mode 3 (see clause 5.1.3.2), repeat the measurement for each of the transmit ports. For each sampling point (frequency domain), add up the coincident power values (in mW) for the different transmit chains and use this as the new data set.

Step 3:

Add up the values for power for all the samples in the file using the formula below.

$$P_{Sum} = \sum_{n=1}^k P_{sample}(n)$$

with 'k' being the total number of samples and 'n' the actual sample number

Step 4:

Normalize the individual values for power (in dBm) so that the sum is equal to the RF Output Power (e.i.r.p.) measured in clause 5.3.2 and save the corrected data. The following formulas can be used:

$$C_{Corr} = P_{Sum} - P_{e.i.r.p.}$$

$$P_{Samplecorr}(n) = P_{Sample}(n) - C_{Corr}$$

with 'n' being the actual sample number

Step 5:

Starting from the first sample $P_{Samplecorr}(n)$ (lowest frequency), add up the power (in mW) of the following samples representing a 1 MHz segment and record the results for power and position (i.e. sample #1 to sample #100). This is the Power Spectral Density (e.i.r.p.) for the first 1 MHz segment which shall be recorded.

Step 6:

Shift the start point of the samples added up in step 5 by one sample and repeat the procedure in step 5 (i.e. sample #2 to sample #101).

Step 7:

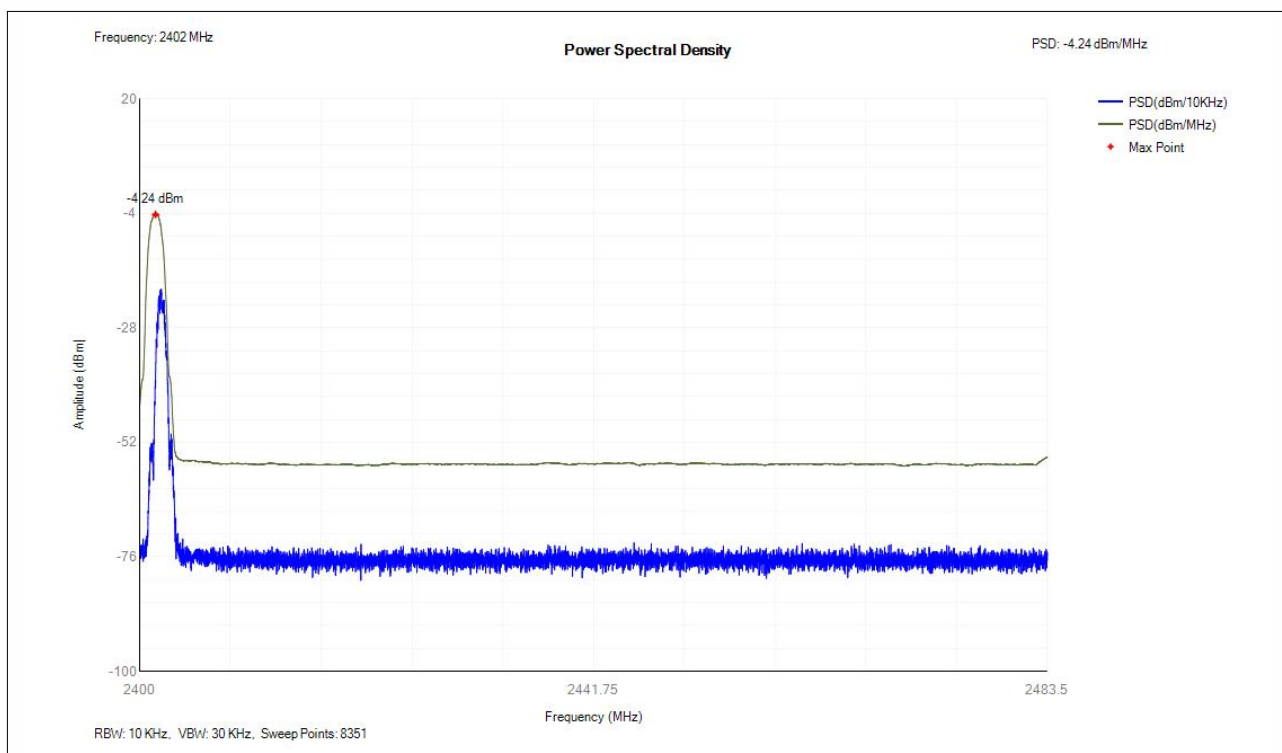
Repeat step 6 until the end of the data set and record the Power Spectral Density values for each of the 1 MHz segments.

From all the recorded results, the highest value is the maximum Power Spectral Density for the UUT. This value, which shall comply with the limit given in clause 4.3.2.3.3, shall be recorded in the test report.

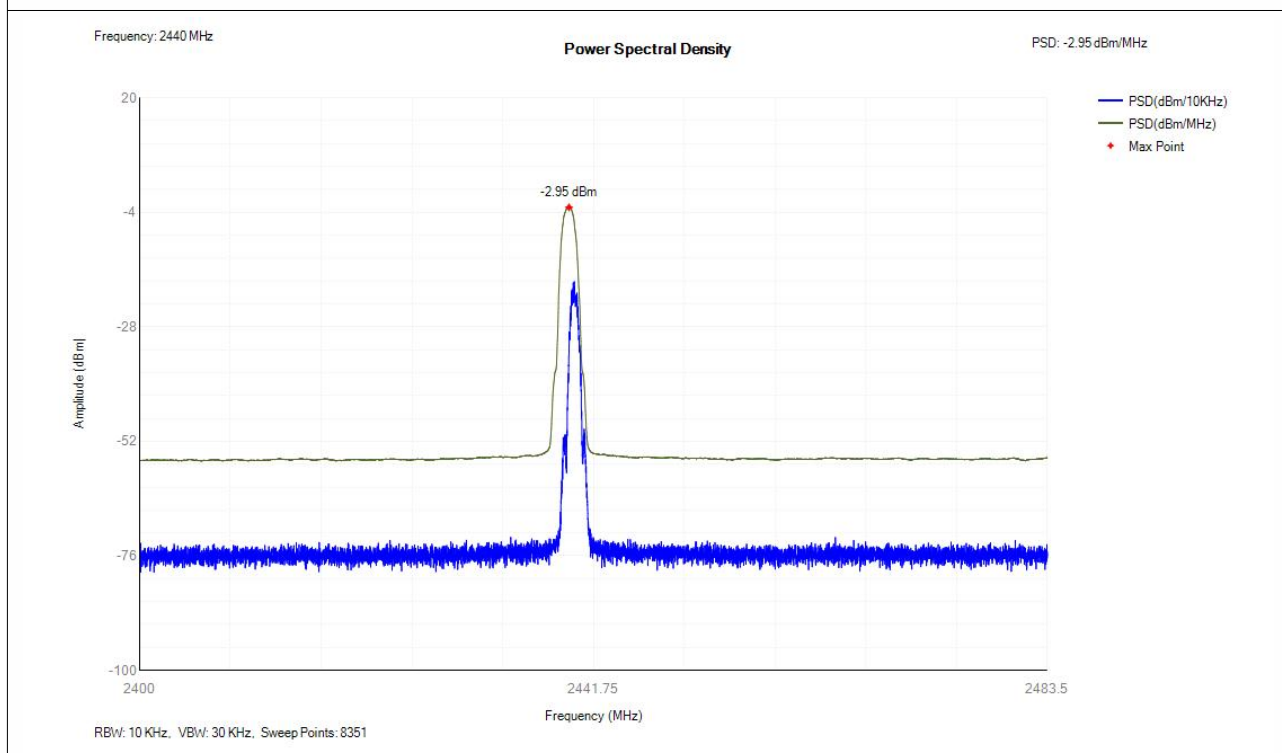


6.4. Test Result

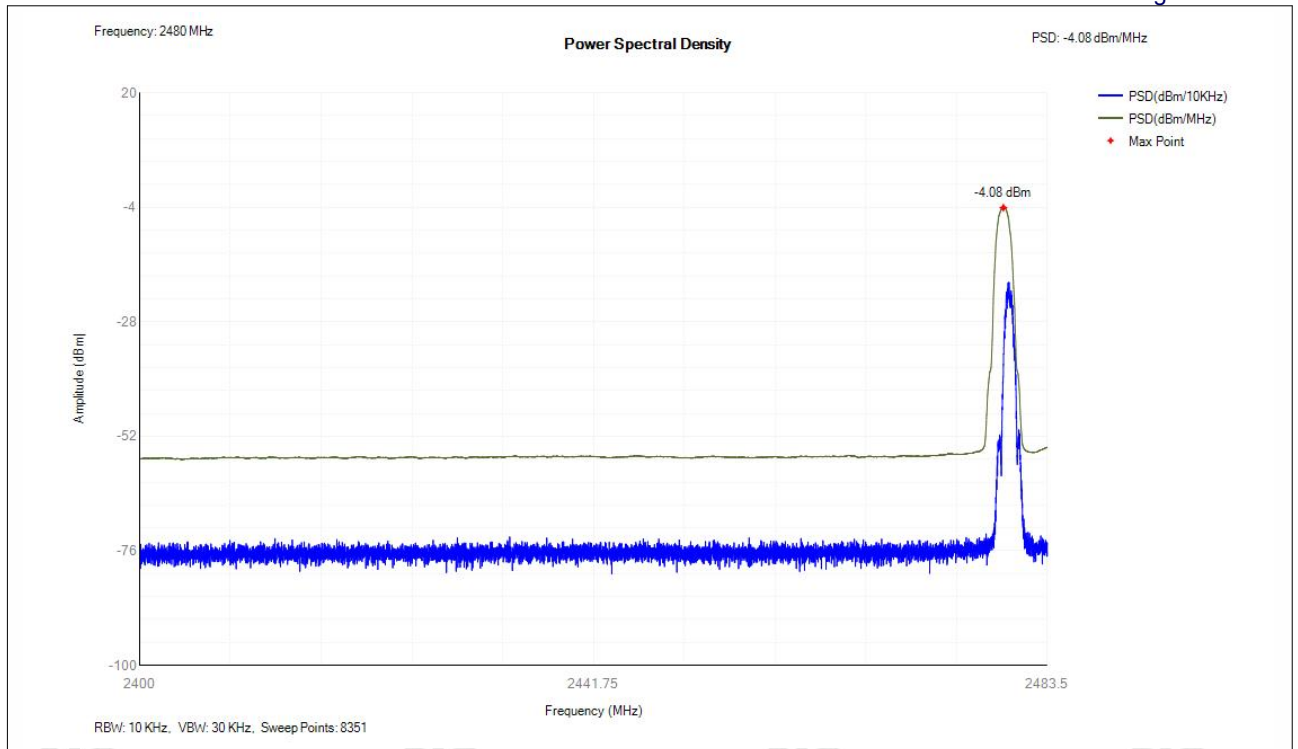
Modulation	Test conditions	Maximum e.i.r.p. Spectral Density (dBm/MHz)		
		Low Channel	Middle Channel	High Channel
GFSK-1M	Normal	-4.24	-2.95	-4.08
GFSK-2M	Normal	-5.35	-3.97	-5.08
Limit		≤10dBm/MHz		



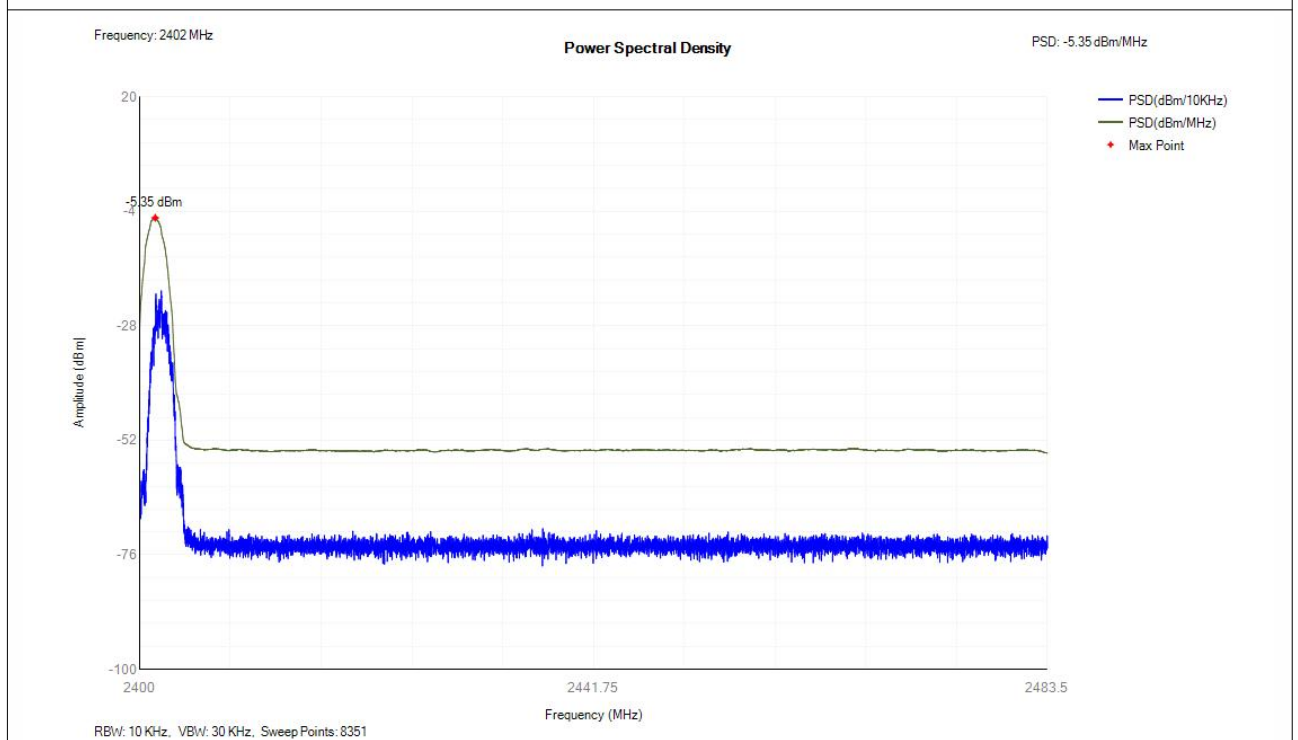
PSD NVNT BLE 1M 2402MHz Ant1



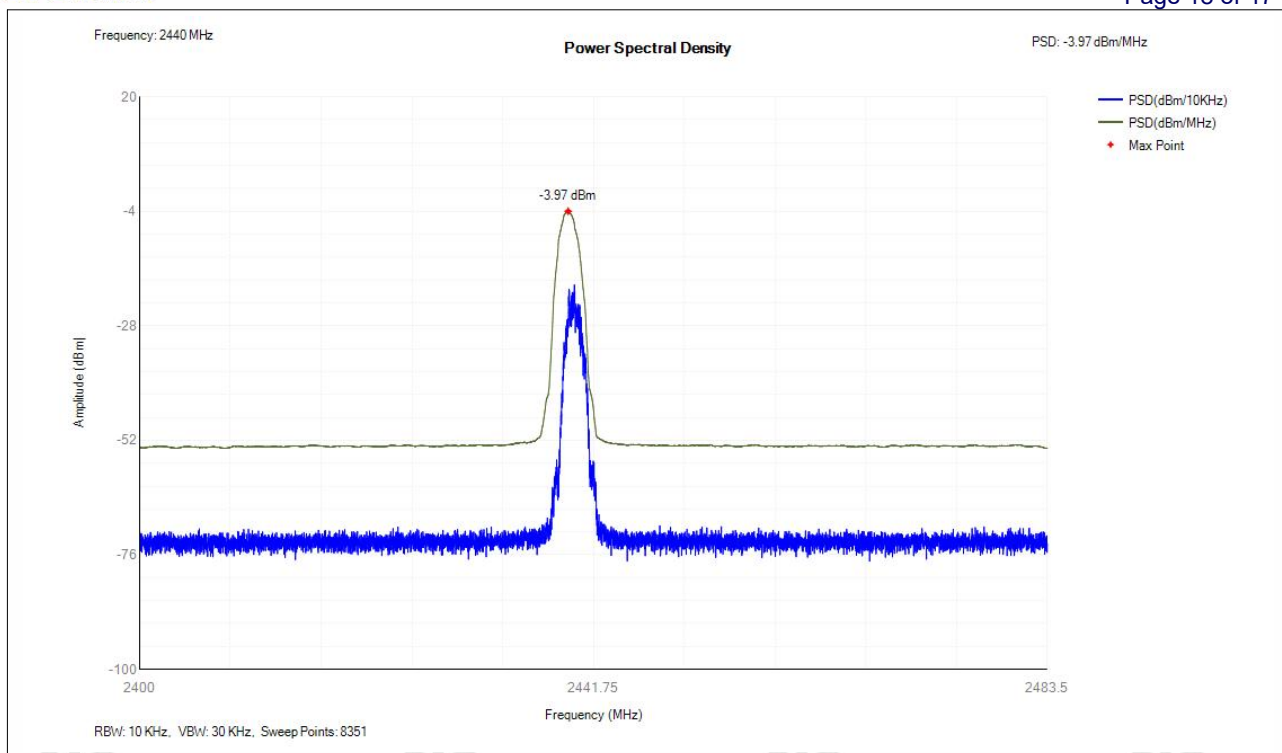
PSD NVNT BLE 1M 2440MHz Ant1



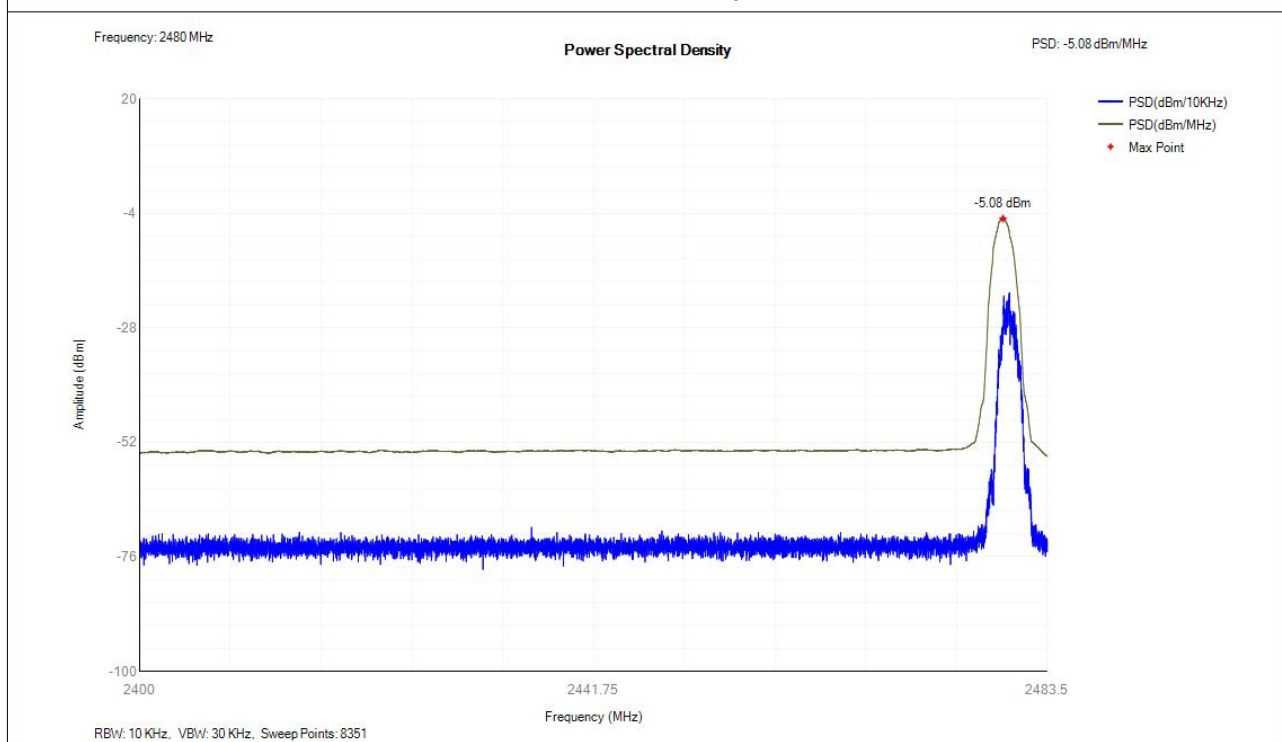
PSD NVNT BLE 1M 2480MHz Ant1



PSD NVNT BLE 2M 2402MHz Ant1



PSD NVNT BLE 2M 2440MHz Ant1

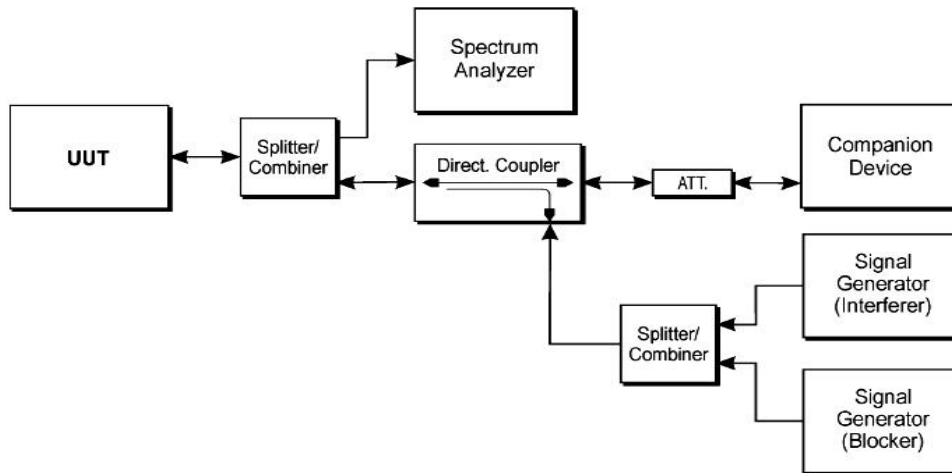


PSD NVNT BLE 2M 2480MHz Ant1



7. Adaptivity

7.1. Block Diagram Of Test Setup



7.2. Limit

The frequency range of the equipment is determined by the lowest and highest

Non-LBT based Detect and Avoid:

- 1 The frequency shall remain unavailable for a minimum time equal to 1 second after which the channel maybe considered again as an 'available' channel;
- 2 COT ≤ 40 ms;
- 3 Idle Period = 5% of COT;
- 4 Detection threshold level = $-70\text{dBm/MHz} + 20 - \text{Pout E.I.R.P}$ (Pout in dBm);

LBT based Detect and Avoid (Frame Based Equipment):

- 1 Minimum Clear Channel Assessment (CCA) time = 20 us;
- 2 CCA observation time declared by the supplier;
- 3 COT = 1~10 ms;
- 4 Idle Period = 5% of COT;
- 5 Detection threshold level = $-70\text{dBm/MHz} + 20 - \text{Pout E.I.R.P}$ (Pout in dBm);

LBT based Detect and Avoid (Load Based Equipment):

- 1 Minimum Clear Channel Assessment (CCA) time = 20 us;
- 2 CCA declared by the manufacturer;
- 3 COT $\leq (13 / 32) * q$ ms; $q = [4 \sim 32]$; 1.625ms~13ms;
- 4 Detection threshold level = $-73\text{dBm/MHz} + 20 - \text{Pout E.I.R.P}$ (dBm);

Short Control Signaling Transmissions:

Short Control Signaling Transmissions shall have a maximum duty cycle of 10% within an observation period of 50ms.

7.3. Test procedure

Step 1:

The UUT may connect to a companion device during the test. The interference signal generator, the blocking signal generator, the spectrum analyser, the UUT and the companion device are connected using a set-up equivalent to the example given by figure 5 although the interference and blocking signal generator do not generate any signals at this point in time. The spectrum analyser is used to monitor the transmissions of the UUT in response to the interfering and the blocking signals.

Adjust the received signal level (wanted signal from the companion device) at the UUT to the value defined in table 6

The analyzer shall be set as follows:

- RBW: $\geq$ Occupied Channel Bandwidth (if the analyser does not support this setting, the highest available setting shall be used)
- VBW: $3 \times$ RBW (if the analyser does not support this setting, the highest available setting shall be used)
- Detector Mode: RMS
- Centre Frequency: Equal to the centre frequency of the operating channel
- Span: 0 Hz
- Sweep time: $>$ Channel Occupancy Time of the UUT
- Trace Mode: Clear/Write
- Trigger Mode: Video

Step 2:

Configure the UUT for normal transmissions with a sufficiently high payload to allow demonstration of compliance of the adaptive mechanism on the channel being tested

Using the procedure defined in clause 5.3.7.2.1.4, it shall be verified that the UUT complies with the maximum Channel Occupancy Time and minimum Idle Period

Step 3: Adding the interference signal

A 100 % duty cycle interference signal is injected on the current operating channel of the UUT. This interference signal shall be a band limited noise signal which has a flat power spectral density, and shall have a bandwidth greater than the Occupied Channel Bandwidth of the UUT. The maximum ripple of this interfering signal shall be $\pm 1,5$ dB within the Occupied Channel Bandwidth and the power spectral density.

**Step 4: Verification of reaction to the interference signal**

The spectrum analyser shall be used to monitor the transmissions of the UUT on the selected operating channel with the interfering signal injected. This may require the spectrum analyser sweep to be triggered by the start of the interfering signal.

Using the procedure defined in clause 5.3.7.2.1.4, it shall be verified that:

The UUT shall stop transmissions on the current operating channel being tested.

Apart from Short Control Signaling Transmissions (see iii) below), there shall be no subsequent transmissions on this operating channel for a (silent) period defined in clause 4.3.2.5.1.2 step 2. After that, the UUT may have normal transmissions again for the duration of a single Channel Occupancy Time period. Because the interference signal is still present, another silent period as defined in clause 4.3.2.5.1.2 step 2 needs to be included. This sequence is repeated as long as the interfering signal is present.

The UUT may continue to have Short Control Signaling Transmissions on the operating channel while the interference signal is present. These transmissions shall comply with the limits

Alternatively, the equipment may switch to a non-adaptive mode

Step 5: Adding the blocking signal

With the interfering signal present, a 100 % duty cycle CW signal is inserted as the blocking signal

Repeat step 4 to verify that the UUT does not resume any normal transmissions

Step 6: Removing the interference and blocking signal

On removal of the interference and blocking signal the UUT is allowed to start transmissions again on this channel however, it shall be verified that this shall only be done after the period defined in clause 4.3.2.5.1.2 step 2.

Step 7:

The steps 2 to 6 shall be repeated for each of the frequencies to be tested.

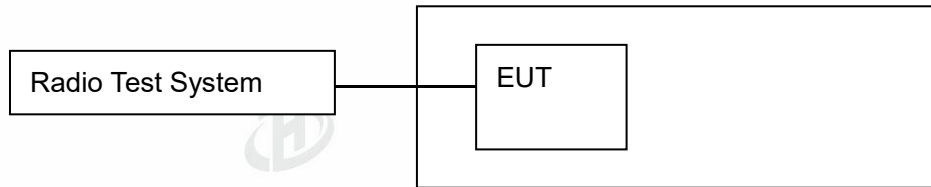
7.4. Test Result

Remark: this requirement does not apply for equipment when operating in a mode where the RF Output power is less than 10 dBm e.i.r.p.



8. Occupied Channel Bandwidth

8.1. Block Diagram Of Test Setup



8.2. Limit

The Occupied Channel Bandwidth shall fall completely within the band given in 2.4GHz to 2.4835GHz.

In addition, for non-adaptive systems using wide band modulations other than FHSS and with e.i.r.p greater than 10 dBm, the occupied channel bandwidth shall be less than 20 MHz.

8.3. Test procedure

Step 1:

Connect the UUT to the spectrum analyser and use the following settings:

- Centre Frequency: The centre frequency of the channel under test
- Resolution BW: ~ 1 % of the span without going below 1 %
- Video BW: $3 \times \text{RBW}$
- Frequency Span: $2 \times \text{Nominal Channel Bandwidth}$
- Detector Mode: RMS
- Trace Mode: Max Hold
- Sweep time: 1 s

Step 2:

Wait for the trace to stabilize.

Find the peak value of the trace and place the analyser marker on this peak.

Step 3:

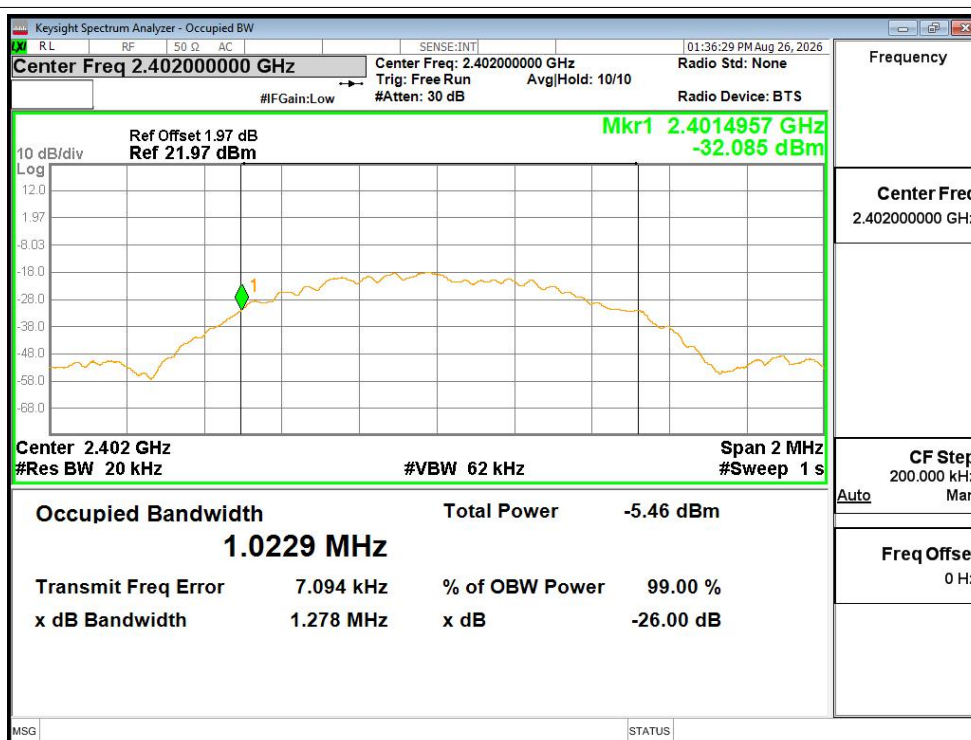
Use the 99 % bandwidth function of the spectrum analyser to measure the Occupied Channel Bandwidth of the UUT.

This value shall be recorded.

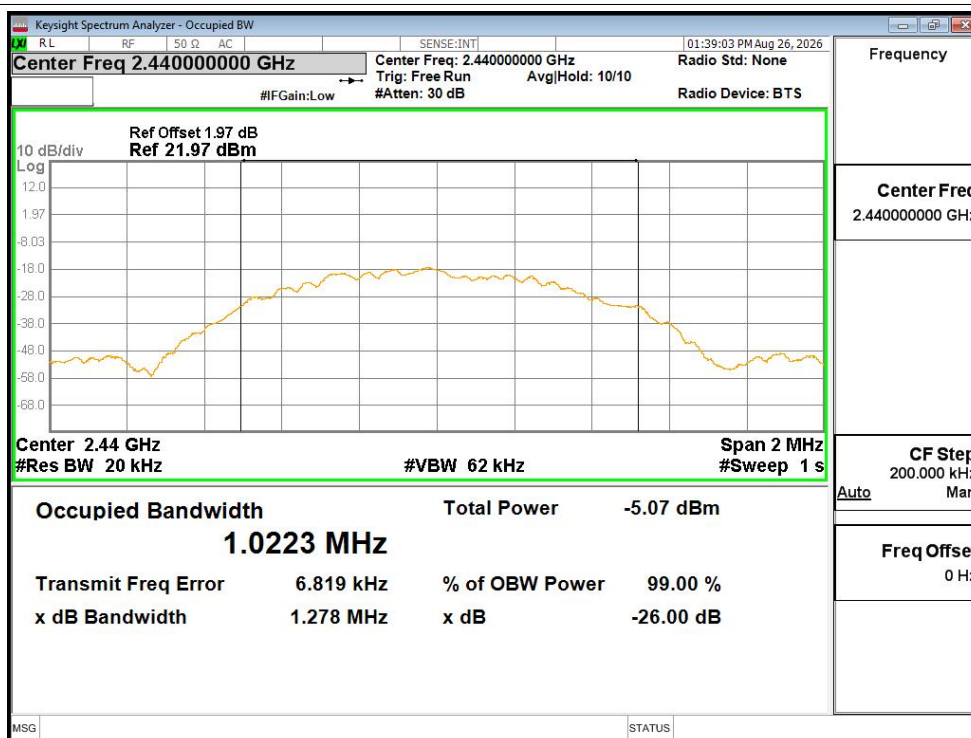
NOTE: Make sure that the power envelope is sufficiently above the noise floor of the analyser to avoid the noise signals left and right from the power envelope being taken into account by this measurement.

8.4. Test Result

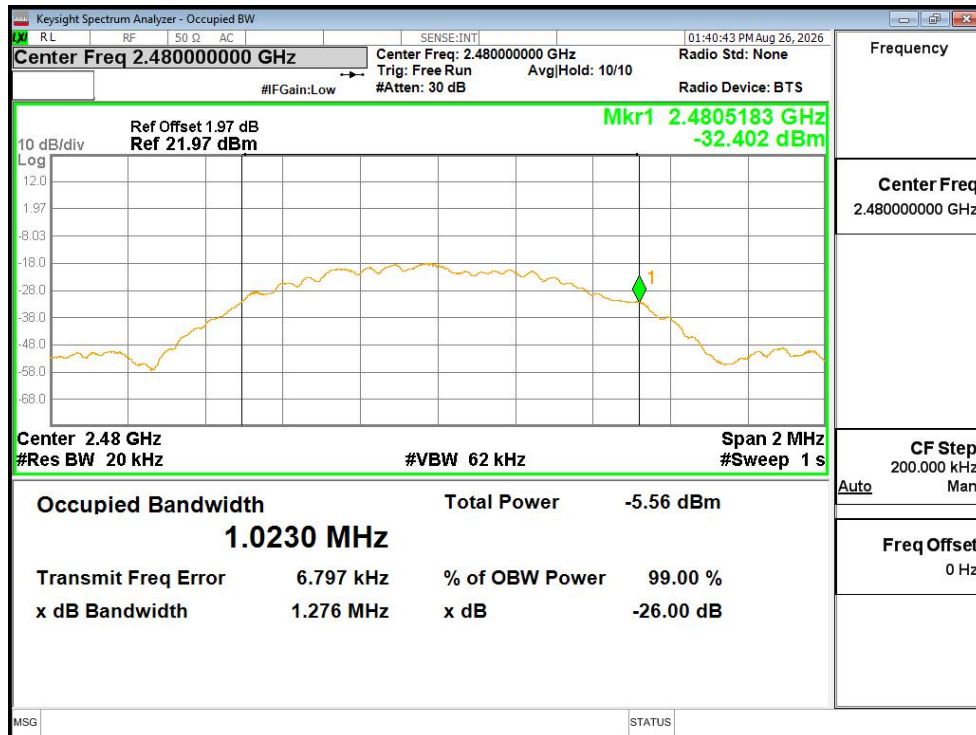
Modulation	Frequency (MHz)	Frequency Range (MHz)		Occupied Channel (MHz)
GFSK-1M	Low	2401.49565	2402.51855	1.0229
	Middle	2439.49565	2440.51795	1.0223
	High	2479.4953	2480.5183	1.023
GFSK-2M	Low	2401.0077	2403.0217	2.014
	Middle	2439.0078	2441.0224	2.0146
	High	2479.00915	2481.02445	2.0153



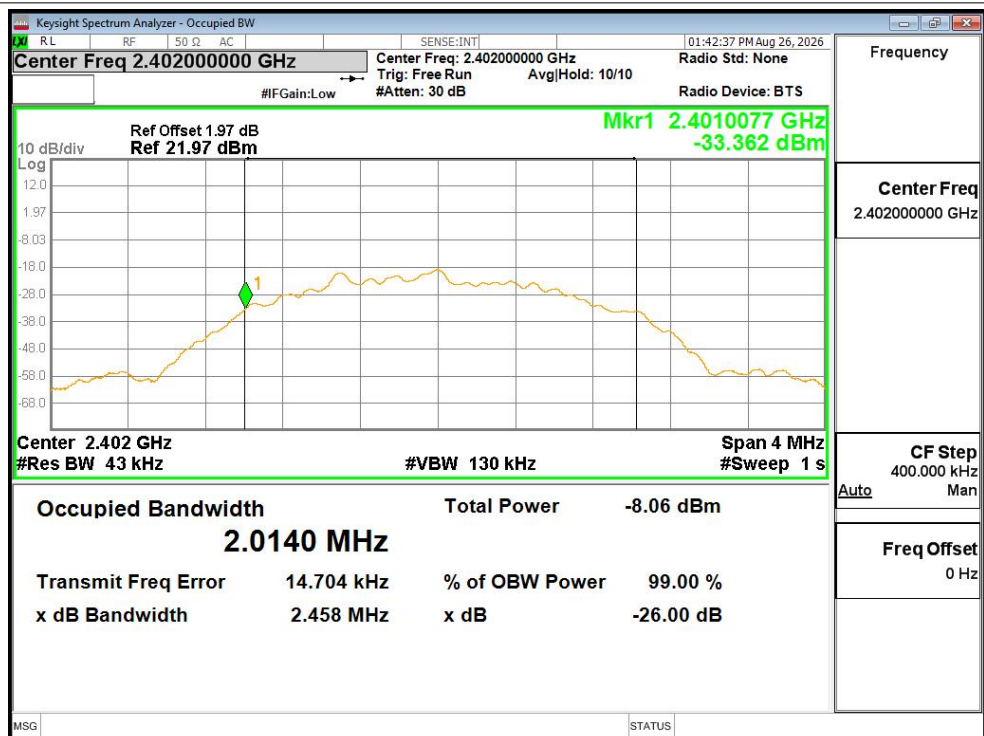
OBW NVNT BLE 1M 2402MHz Ant1



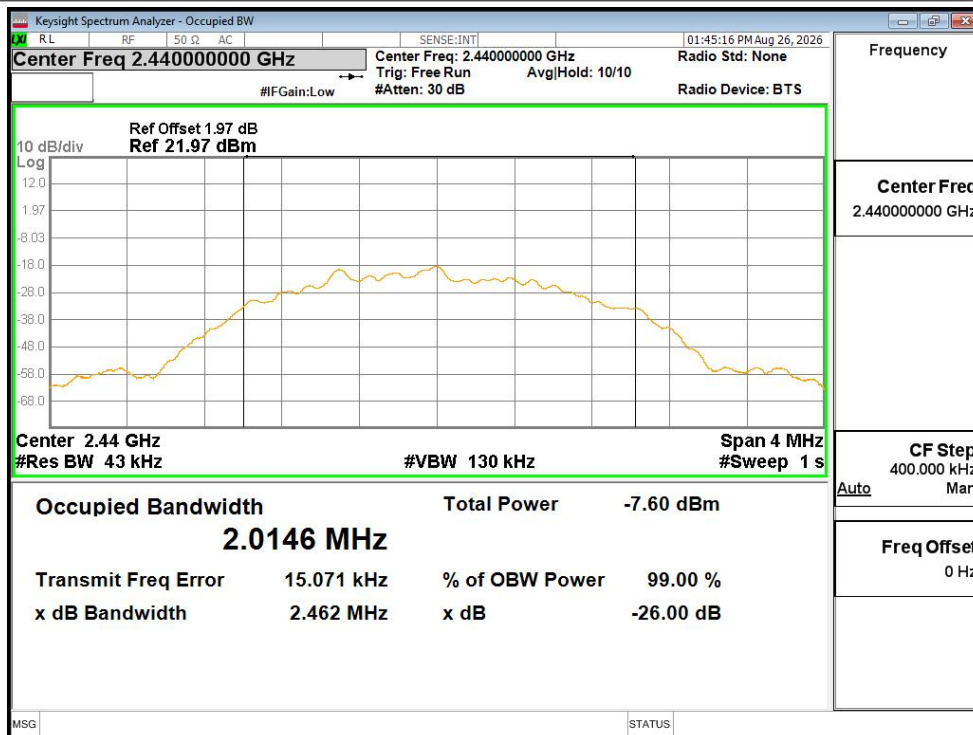
OBW NVNT BLE 1M 2440MHz Ant1



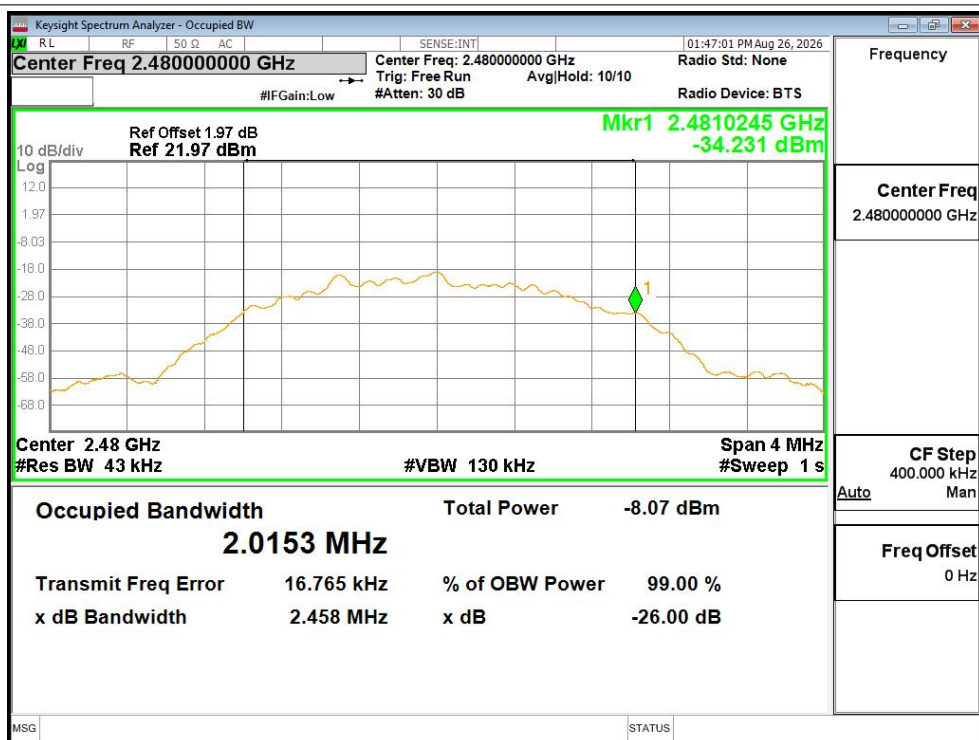
OBW NVNT BLE 1M 2480MHz Ant1



OBW NVNT BLE 2M 2402MHz Ant1



OBW NVNT BLE 2M 2440MHz Ant1

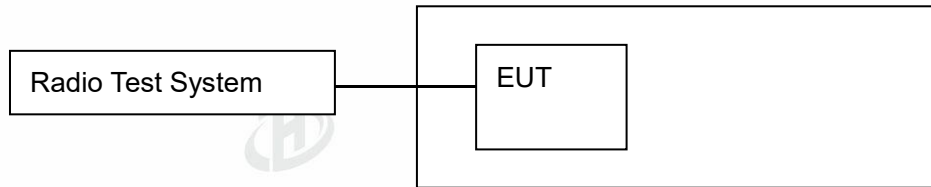


OBW NVNT BLE 2M 2480MHz Ant1



9. Transmitter Unwanted Emissions In The Out-of-band Domain

9.1. Block Diagram Of Test Setup



9.2. Limit

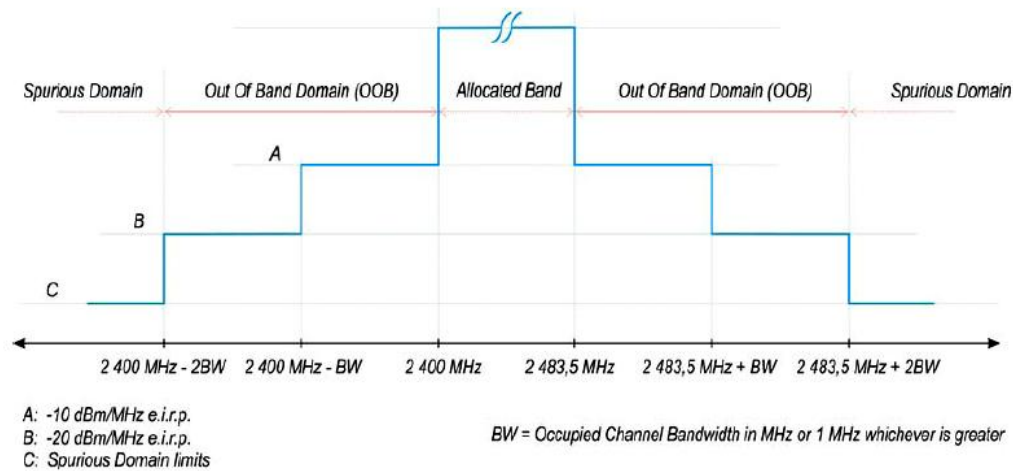


Figure 3: Transmit mask

9.3. Test procedure

The applicable mask is defined by the measurement results from the tests performed under clause 5.3.8 (Occupied Channel Bandwidth).

The test procedure is further as described under clause 5.3.9.2.1.

The Out-of-band emissions within the different horizontal segments of the mask provided in figures 1 and 3 shall be measured using the steps below. This method assumes the spectrum analyser is equipped with the Time Domain Power option.

Step 1:

- Connect the UUT to the spectrum analyser and use the following settings:
 - Centre Frequency: 2 484 MHz
 - Span: 0 Hz
 - Resolution BW: 1 MHz
 - Filter mode: Channel filter
 - Video BW: 3 MHz

- Detector Mode: RMS
- Trace Mode: Max Hold
- Sweep Mode: Continuous
- Sweep Points: Sweep Time [s] / (1 μ s) or 5 000 whichever is greater
- Trigger Mode: Video trigger

NOTE 1: In case video triggering is not possible, an external trigger source may be used.

- Sweep Time: > 120 % of the duration of the longest burst detected during the measurement of the RF Output Power

Step 2 (segment 2 483,5 MHz to 2 483,5 MHz + BW):

- Adjust the trigger level to select the transmissions with the highest power level.
- For frequency hopping equipment operating in a normal hopping mode, the different hops will result in signal bursts with different power levels. In this case the burst with the highest power level shall be selected.
- Set a window (start and stop lines) to match with the start and end of the burst and in which the RMS power shall be measured using the Time Domain Power function.
- Select RMS power to be measured within the selected window and note the result which is the RMS power within this 1 MHz segment (2 483,5 MHz to 2 484,5 MHz). Compare this value with the applicable limit provided by the mask.
- Increase the centre frequency in steps of 1 MHz and repeat this measurement for every 1 MHz segment within the range 2 483,5 MHz to 2 483,5 MHz + BW. The centre frequency of the last 1 MHz segment shall be set to 2 483,5 MHz + BW - 0,5 MHz (which means this may partly overlap with the previous 1 MHz segment).

Step 3 (segment 2 483,5 MHz + BW to 2 483,5 MHz + 2BW):

- Change the centre frequency of the analyser to 2 484 MHz + BW and perform the measurement for the first 1 MHz segment within range 2 483,5 MHz + BW to 2 483,5 MHz + 2BW. Increase the centre frequency in 1 MHz steps and repeat the measurements to cover this whole range. The centre frequency of the last 1 MHz segment shall be set to 2 483,5 MHz + 2 BW - 0,5 MHz (which means this may partly overlap with the previous 1 MHz segment).

Step 4 (segment 2 400 MHz - BW to 2 400 MHz):

- Change the centre frequency of the analyser to 2 399,5 MHz and perform the measurement for the first 1 MHz segment within range 2 400 MHz - BW to 2 400 MHz. Reduce the centre frequency in 1 MHz steps and repeat the measurements to cover this whole range. The centre frequency of the last 1 MHz segment shall be set to 2 400 MHz - BW + 0,5 MHz (which means this may partly overlap with the previous 1 MHz segment).

Step 5 (segment 2 400 MHz - 2BW to 2 400 MHz - BW):

- Change the centre frequency of the analyser to 2 399,5 MHz - BW and perform the measurement for the first 1 MHz segment within range 2 400 MHz - 2BW to 2 400 MHz - BW. Reduce the centre frequency in 1 MHz steps and repeat the measurements to cover this whole range. The centre frequency of the last 1 MHz segment shall be set to 2 400 MHz - 2BW + 0,5 MHz (which means this may partly overlap with the previous 1 MHz segment).

Step 6:

- In case of conducted measurements on equipment with a single transmit chain, the declared antenna assembly gain "G" in dBi shall be added to the results for each of the 1 MHz segments and compared with the limits

provided by the mask given in figure 1 or figure 3. If more than one antenna assembly is intended for this power setting, the antenna with the highest gain shall be considered.

- In case of conducted measurements on smart antenna systems (equipment with multiple transmit chains), the measurements need to be repeated for each of the active transmit chains. The declared antenna assembly gain "G" in dBi for a single antenna shall be added to these results. If more than one antenna assembly is intended for this power setting, the antenna with the highest gain shall be considered. Comparison with the applicable limits shall be done using any of the options given below:

- Option 1: the results for each of the transmit chains for the corresponding 1 MHz segments shall be added. The additional beamforming gain "Y" in dB shall be added as well and the resulting values compared with the limits provided by the mask given in figure 1 or figure 3.

- Option 2: the limits provided by the mask given in figure 1 or figure 3 shall be reduced by $10 \times \log_{10}(A_{ch})$ and the additional beamforming gain "Y" in dB. The results for each of the transmit chains shall be individually compared with these reduced limits.

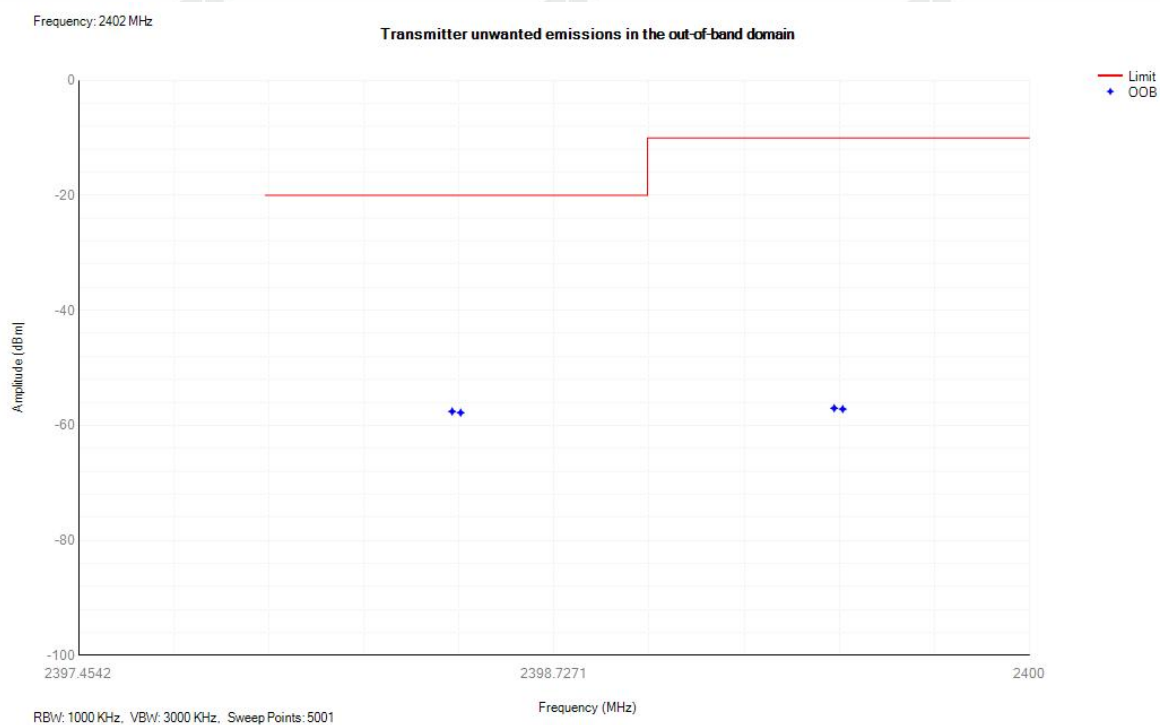
NOTE 2: A_{ch} refers to the number of active transmit chains.

It shall be recorded whether the equipment complies with the mask provided in figure 1 or figure 3.

9.4. Test Result

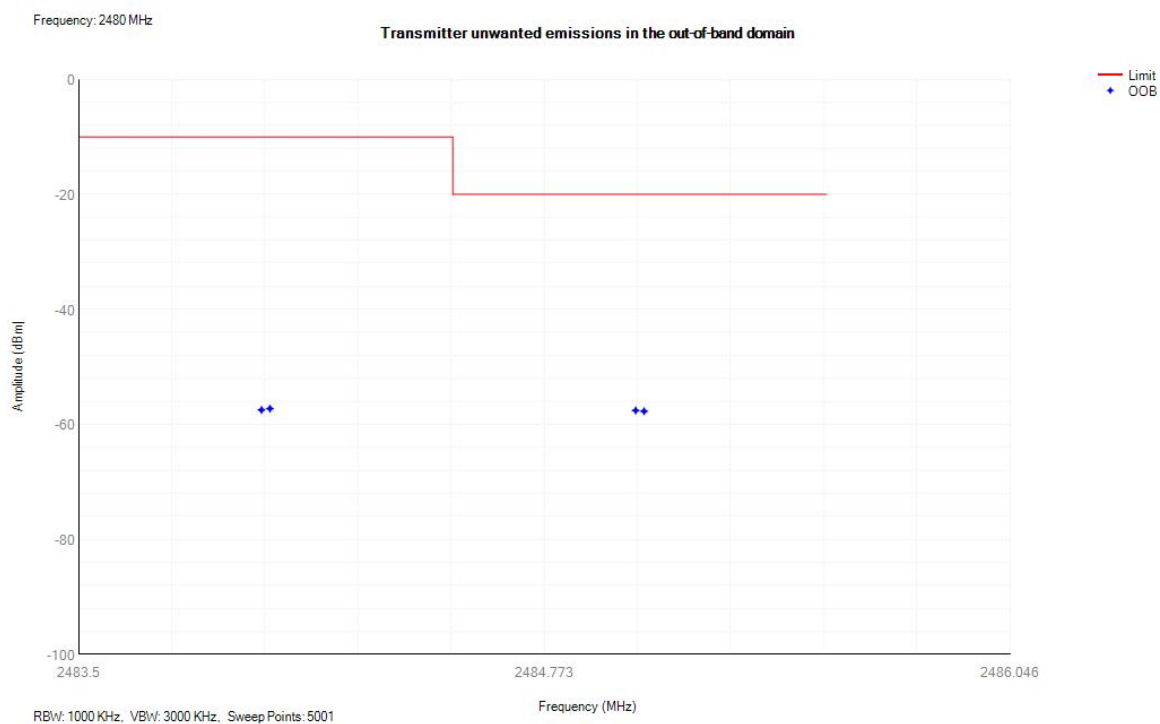
CH Low (Normal Temp)

BLE 1M				
Test Freq (MHz)	Antenna	Freq(MHz)	Level	Limit
2402	Antenna 1	2399.5	-57.16	-10
2402	Antenna 1	2399.4771	-57.01	-10



CH High (Normal Temp)

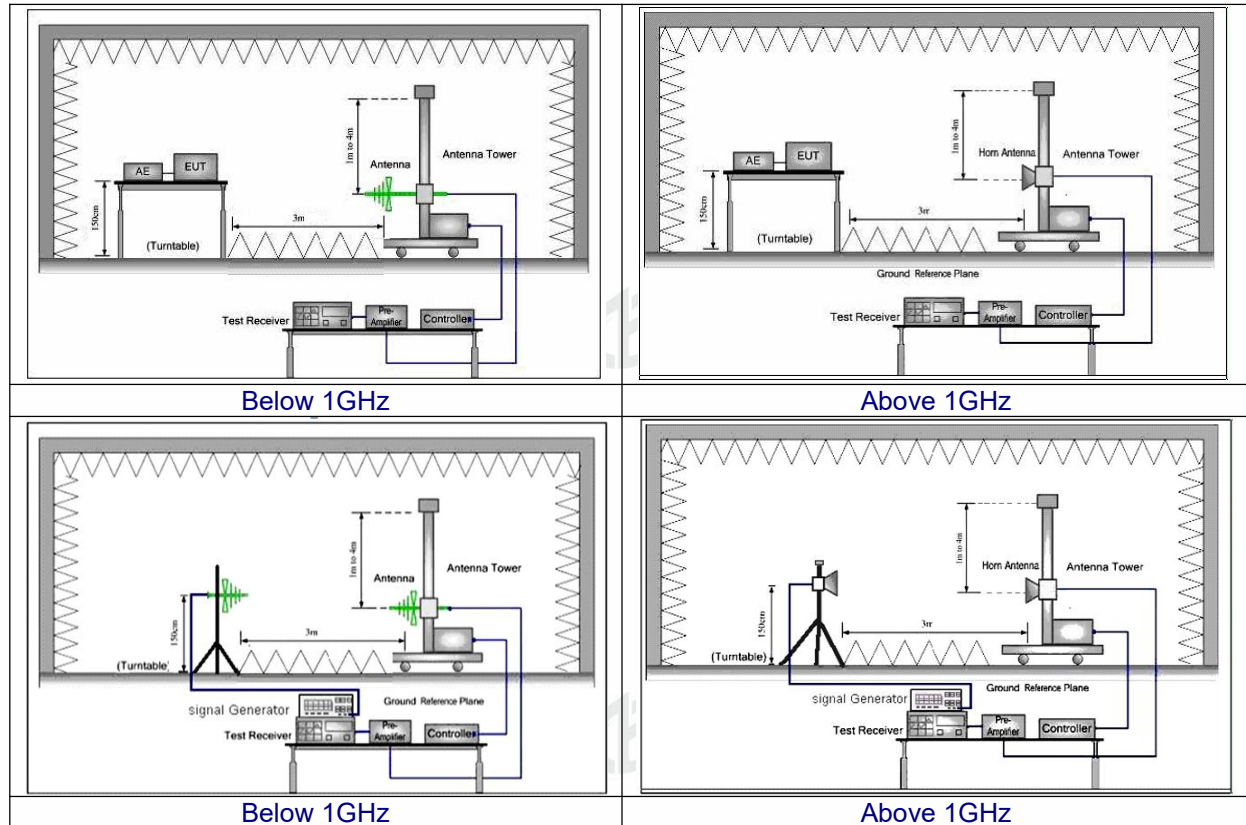
BLE 1M				
Test Freq (MHz)	Antenna	Freq(MHz)	Level	Limit
2480	Antenna 1	2484	-57.49	-10
2480	Antenna 1	2484.023	-57.26	-10





10. Transmitter Unwanted Emissions In The Spurious Domain

10.1. Block Diagram Of Test Setup



10.2. Limits

Frequency range	Maximum power, e.r.p. (≤ 1 GHz) e.i.r.p. (> 1 GHz)	RBW/VBW
30 MHz to 47 MHz	-36 dBm	100 kHz/300KHz
47 MHz to 74 MHz	-54 dBm	100 kHz/300KHz
74 MHz to 87,5 MHz	-36 dBm	100 kHz/300KHz
87,5 MHz to 118 MHz	-54 dBm	100 kHz/300KHz
118 MHz to 174 MHz	-36 dBm	100 kHz/300KHz
174 MHz to 230 MHz	-54 dBm	100 kHz/300KHz
230 MHz to 470 MHz	-36 dBm	100 kHz/300KHz
470 MHz to 694 MHz	-54 dBm	100 kHz/300KHz
694 MHz to 1 GHz	-36 dBm	100 kHz/300KHz
1 GHz to 12,75 GHz	-30 dBm	1 MHz/3MHz



10.3. Test Procedure

1. Scan from 30MHz to 12.75GHz, find the maximum radiation frequency to measure.
2. The technique used to find the Spurious Emissions of the transmitter was the antenna substitution method. Substitution method was performed to determine the actual ERP/EIRP emission levels of the EUT.

Test procedure as below:

- 1) The EUT was powered ON and placed on a 1.5m high table at a 3 meter fully Anechoic Chamber. The antenna of the transmitter was extended to its maximum length. modulation mode and the measuring receiver shall be tuned to the frequency of the transmitter under test.
 - 2) The EUT was set 3 meters (above 18GHz the distance is 1 meter) away from the interference-receiving antenna, which was mounted on the top of a variable-height antenna tower.
 - 3) The disturbance of the transmitter was maximized on the test receiver display by raising and lowering from 1m to 4m the receive antenna and by rotating through 360° the turntable. After the fundamental emission was maximized, a field strength measurement was made.
 - 4) Steps 1) to 3) were performed with the EUT and the receive antenna in both vertical and horizontal polarization.
 - 5) The transmitter was then removed and replaced with another antenna. The center of the antenna was approximately at the same location as the center of the transmitter.
 - 6) A signal at the disturbance was fed to the substitution antenna by means of a non-radiating cable. With both the substitution and the receive antennas horizontally polarized, the receive antenna was raised and lowered to obtain a maximum reading at the test receiver. The level of the signal generator was adjusted until the measured field strength level in step 3) is obtained for this set of conditions.
 - 7) The output power into the substitution antenna was then measured.
 - 8) Steps 6) and 7) were repeated with both antennas polarized.
 - 9) Calculate power in dBm by the following formula:
$$\text{ERP(dBm)} = P_{\text{SG}}(\text{dBm}) - \text{cable loss (dB)} + \text{antenna gain (dBi)}$$
$$\text{EIRP(dBm)} = P_{\text{SG}}(\text{dBm}) - \text{cable loss (dB)} + \text{antenna gain (dBi)}$$
$$\text{EIRP} = \text{ERP} + 2.15\text{dB}$$

where:
 P_{SG} is the generator output power into the substitution antenna.
 - 10) Test the EUT in the lowest channel, the Highest channel
- Repeat above procedures until all frequencies measured was complete.

**10.4. Test Results**

Frequency	Antenna Polar	Receiver Reading	Limit	Margin	Result
(MHz)	(H/V)	(dBm)	(dBm)	(dB)	
TX GFSK low channel					PASS
802.72	H	-53.42	-36	-17.42	
802.72	V	-49.72	-36	-13.72	
4824	H	-51.95	-30	-21.95	
4824	V	-49.23	-30	-19.23	
7236	H	-51.19	-30	-21.19	
7236	V	-51.1	-30	-21.1	
TX GFSK high channel					
846.75	H	-55.5	-36	-19.5	
846.75	V	-51.98	-36	-15.98	
4944	H	-49.63	-30	-19.63	
4944	V	-51.98	-30	-21.98	
7416	H	-50.41	-30	-20.41	
7416	V	-54.53	-30	-24.53	

Remark:

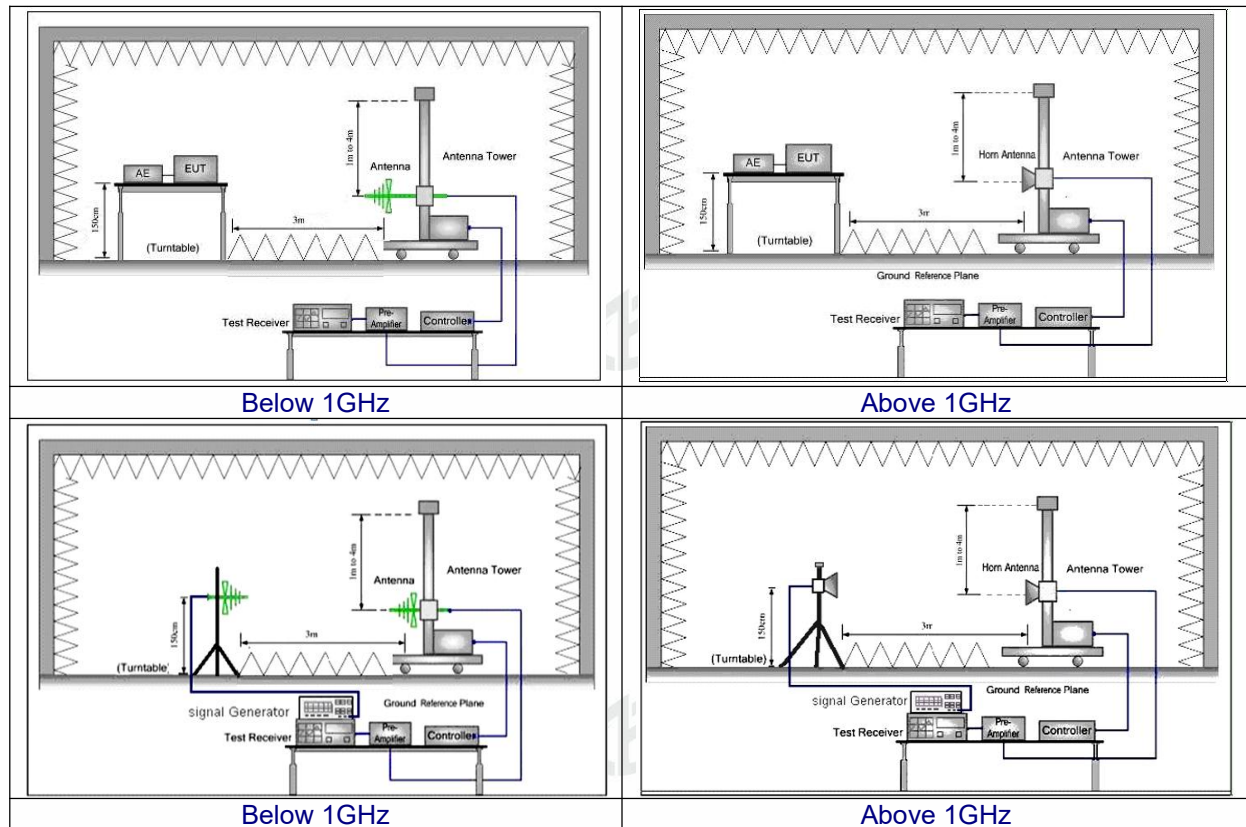
Absolute Level = Receiver Reading + Factor

Factor = Antenna Factor + Cable Loss – Pre-amplifier.



11. Receiver Spurious Emissions

11.1. Block Diagram Of Test Setup



11.2. Limits

Frequency(MHz)	Limit
30-1000	-57dBm
1000-12750	-47dBm

11.3. Test Procedure

1. Scan from 30MHz to 12.75GHz, find the maximum radiation frequency to measure.
2. The technique used to find the Spurious Emissions of the transmitter was the antenna substitution method. Substitution method was performed to determine the actual ERP/EIRP emission levels of the EUT. Test procedure as below:
 - 1) The EUT was powered ON and placed on a 1.5m high table at a 3 meter fully Anechoic Chamber. The antenna of the transmitter was extended to its maximum length. modulation mode and the measuring receiver shall be tuned to the frequency of the transmitter under test.
 - 2) The EUT was set 3 meters(above 18GHz the distance is 1 meter) away from the interference-receiving antenna, which was mounted on the top of a variable-height antenna tower.
 - 3) The disturbance of the transmitter was maximized on the test receiver display by raising and lowering from 1m to 4m the receive antenna and by rotating through 360° the turntable. After the fundamental emission was maximized, a field strength measurement was made.
 - 4) Steps 1) to 3) were performed with the EUT and the receive antenna in both vertical and horizontal polarization.



- 5) The transmitter was then removed and replaced with another antenna. The center of the antenna was approximately at the same location as the center of the transmitter.
- 6) A signal at the disturbance was fed to the substitution antenna by means of a non-radiating cable. With both the substitution and the receive antennas horizontally polarized, the receive antenna was raised and lowered to obtain a maximum reading at the test receiver. The level of the signal generator was adjusted until the measured field strength level in step 3) is obtained for this set of conditions.
- 7) The output power into the substitution antenna was then measured.
- 8) Steps 6) and 7) were repeated with both antennas polarized.
- 9) Calculate power in dBm by the following formula:
$$\text{ERP(dBm)} = P_{\text{SG}}(\text{dBm}) - \text{cable loss (dB)}$$
$$\text{EIRP(dBm)} = P_{\text{SG}}(\text{dBm}) - \text{cable loss (dB)} + \text{antenna gain (dBi)}$$
$$\text{EIRP} = \text{ERP} + \text{antenna gain}$$

where:
 P_{SG} is the generator output power into the substitution antenna.
- 11) Test the EUT in the lowest channel, the Highest channel
Repeat above procedures until all frequencies measured was complete.

**11.4. Test Results**

Frequency	Antenna Polar	Receiver Reading	Limit	Margin	Result
(MHz)	(H/V)	(dBm)	(dBm)	(dB)	
GFSK low channel					PASS
354.29	H	-60.73	-57	-3.73	
354.29	V	-63.68	-57	-6.68	
1763.18	H	-54.11	-47	-7.11	
1763.18	V	-61.69	-47	-14.69	
GFSK high channel					
345.29	H	-63.45	-57	-6.45	
345.29	V	-64.15	-57	-7.15	
2166.17	H	-56.77	-47	-9.77	
2166.17	V	-55.85	-47	-8.85	

Remk:

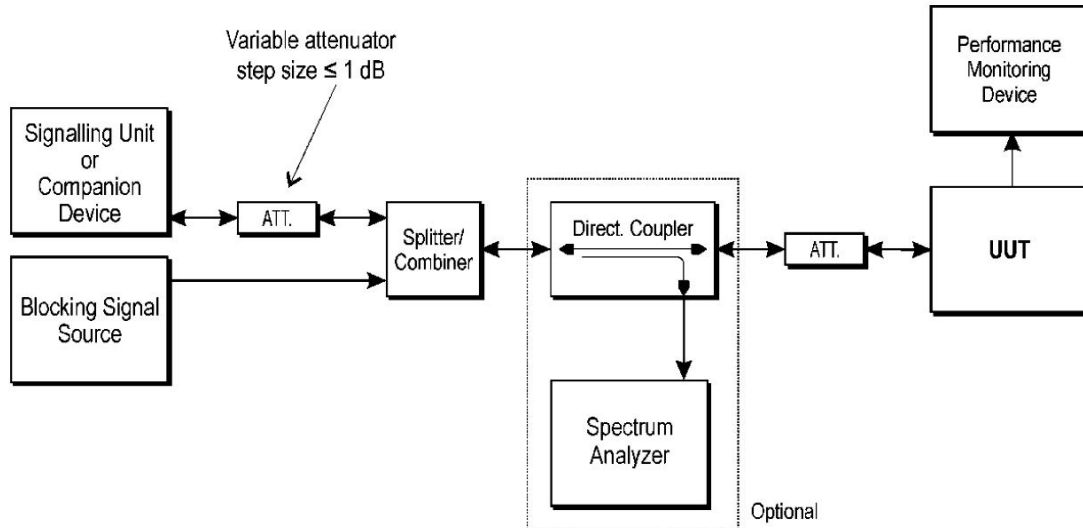
Absolute Level = Receiver Reading + Factor

Factor = Antenna Factor + Cable Loss – Pre-amplifier.



12. Receiver Blocking

12.1. Block Diagram Of Test Setup



12.2. Limit

Table 14: Receiver Blocking parameters for Receiver Category 1 equipment

Wanted signal mean power from companion device (dBm) (see notes 1 and 4)	Blocking signal frequency (MHz)	Blocking signal power (dBm) (see note 4)	Type of blocking signal
(-133 dBm + 10 × log ₁₀ (OCBW)) or -68 dBm whichever is less (see note 2)	2 380 2 504	-34	CW
(-139 dBm + 10 × log ₁₀ (OCBW)) or -74 dBm whichever is less (see note 3)	2 300 2 330 2 360 2 524 2 584 2 674		

NOTE 1: OCBW is in Hz.

NOTE 2: In case of radiated measurements using a companion device and the level of the wanted signal from the companion device cannot be determined, a relative test may be performed using a wanted signal up to $P_{\min} + 26$ dB where $P_{\min}$ is the minimum level of wanted signal required to meet the minimum performance criteria as defined in clause 4.3.1.12.3 in the absence of any blocking signal.

NOTE 3: In case of radiated measurements using a companion device and the level of the wanted signal from the companion device cannot be determined, a relative test may be performed using a wanted signal up to $P_{\min} + 20$ dB where $P_{\min}$ is the minimum level of wanted signal required to meet the minimum performance criteria as defined in clause 4.3.1.12.3 in the absence of any blocking signal.

NOTE 4: The level specified is the level at the UUT receiver input assuming a 0 dBi antenna assembly gain. In case of conducted measurements, this level has to be corrected for the (in-band) antenna assembly gain (G). In case of radiated measurements, this level is equivalent to a power flux density (PFD) in front of the UUT antenna with the UUT being configured/positioned as recorded in clause 5.4.3.2.2.

Table 15: Receiver Blocking parameters receiver Category 2 equipment

Wanted signal mean power from companion device (dBm) (see notes 1 and 3)	Blocking signal frequency (MHz)	Blocking signal power (dBm) (see note 3)	Type of blocking signal
$(-139 \text{ dBm} + 10 \times \log_{10}(\text{OCBW}) + 10 \text{ dB})$ or $(-74 \text{ dBm} + 10 \text{ dB})$ whichever is less (see note 2)	2 380 2 504 2 300 2 584	-34	CW
NOTE 1: OCBW is in Hz. NOTE 2: In case of radiated measurements using a companion device and the level of the wanted signal from the companion device cannot be determined, a relative test may be performed using a wanted signal up to $P_{\min} + 26 \text{ dB}$ where $P_{\min}$ is the minimum level of wanted signal required to meet the minimum performance criteria as defined in clause 4.3.1.12.3 in the absence of any blocking signal. NOTE 3: The level specified is the level at the UUT receiver input assuming a 0 dBi antenna assembly gain. In case of conducted measurements, this level has to be corrected for the (in-band) antenna assembly gain (G). In case of radiated measurements, this level is equivalent to a power flux density (PFD) in front of the UUT antenna with the UUT being configured/positioned as recorded in clause 5.4.3.2.2.			

Table 16: Receiver Blocking parameters receiver Category 3 equipment

Wanted signal mean power from companion device (dBm) (see notes 1 and 3)	Blocking signal frequency (MHz)	Blocking signal power (dBm) (see note 3)	Type of blocking signal
$(-139 \text{ dBm} + 10 \times \log_{10}(\text{OCBW}) + 20 \text{ dB})$ or $(-74 \text{ dBm} + 20 \text{ dB})$ whichever is less (see note 2)	2 380 2 504 2 300 2 584	-34	CW
NOTE 1: OCBW is in Hz. NOTE 2: In case of radiated measurements using a companion device and the level of the wanted signal from the companion device cannot be determined, a relative test may be performed using a wanted signal up to $P_{\min} + 30 \text{ dB}$ where $P_{\min}$ is the minimum level of wanted signal required to meet the minimum performance criteria as defined in clause 4.3.1.12.3 in the absence of any blocking signal. NOTE 3: The level specified is the level at the UUT receiver input assuming a 0 dBi antenna assembly gain. In case of conducted measurements, this level has to be corrected for the (in-band) antenna assembly gain (G). In case of radiated measurements, this level is equivalent to a power flux density (PFD) in front of the UUT antenna with the UUT being configured/positioned as recorded in clause 5.4.3.2.2.			

12.3. Test procedure

Refer to ETSI EN 300 328 V2.2.2 (2019-07) Clause 5.4.11.2.

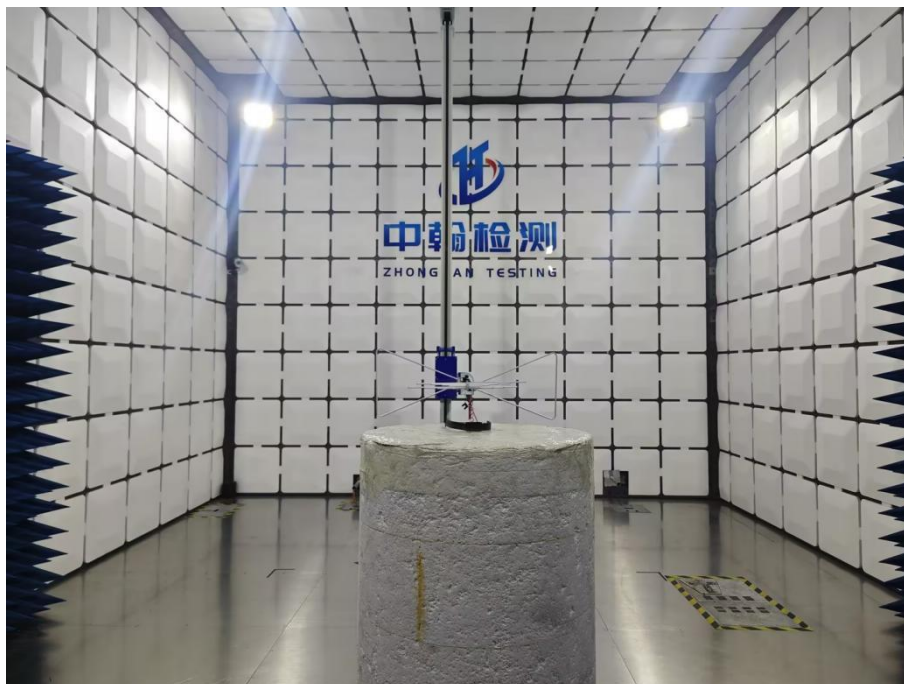
12.4. Test Result

Receiver Category 2					
Mode Hopping	Wanted Power(dBm)	Blocking Frequency(MHz)	Blocking Power(dB)	Type of Blocking Signal	Performance Criteria
GFSK-1M	-68.90	2380	-34	CW	Compliance
GFSK-1M	-68.90	2504	-34	CW	Compliance
GFSK-1M	-68.90	2300	-34	CW	Compliance
GFSK-1M	-68.90	2584	-34	CW	Compliance
GFSK-2M	-65.96	2380	-34	CW	Compliance
GFSK-2M	-65.96	2504	-34	CW	Compliance
GFSK-2M	-65.96	2300	-34	CW	Compliance
GFSK-2M	-65.96	2584	-34	CW	Compliance

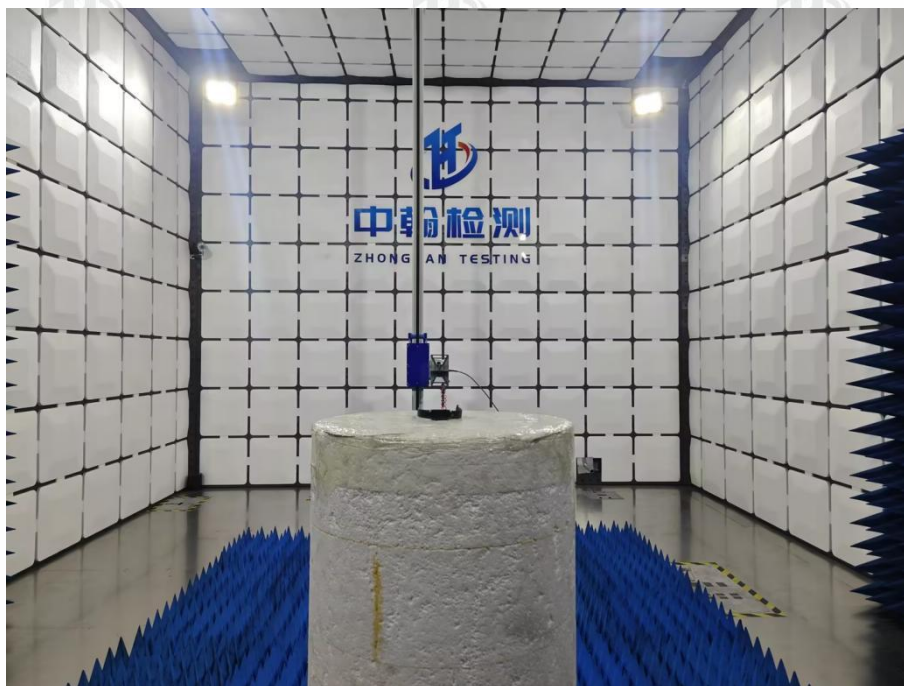


13. Photos Of Test Setup

Radiated measurements (Below 1GHz)

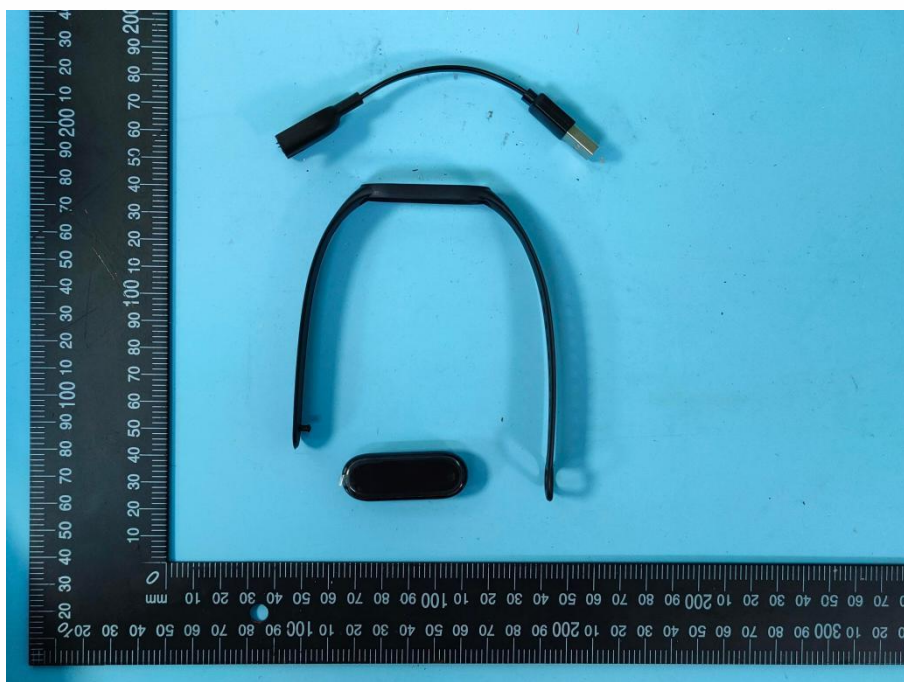
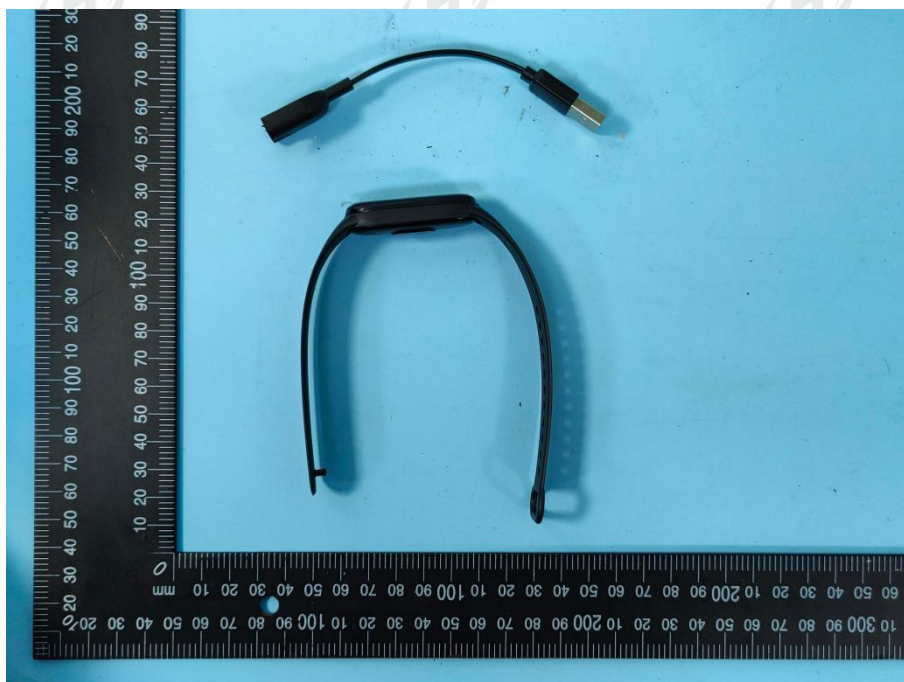


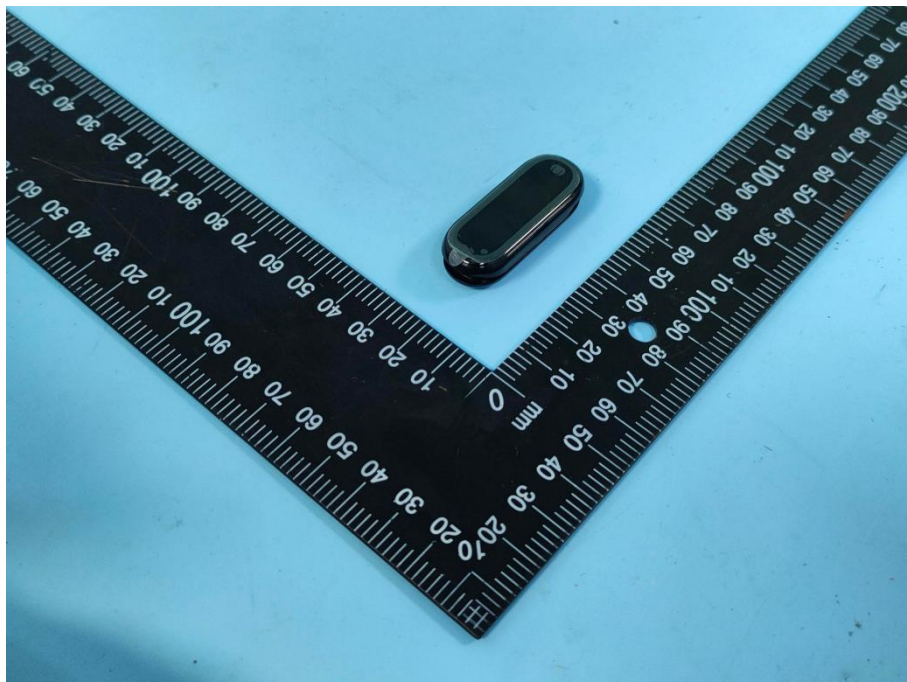
Radiated measurements (9KHz-30MHz)

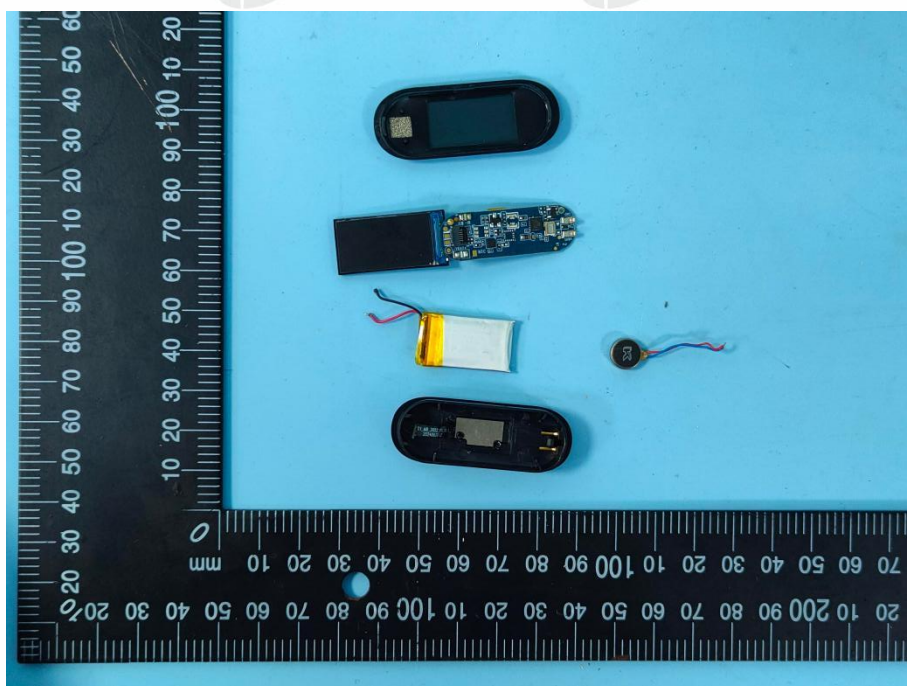
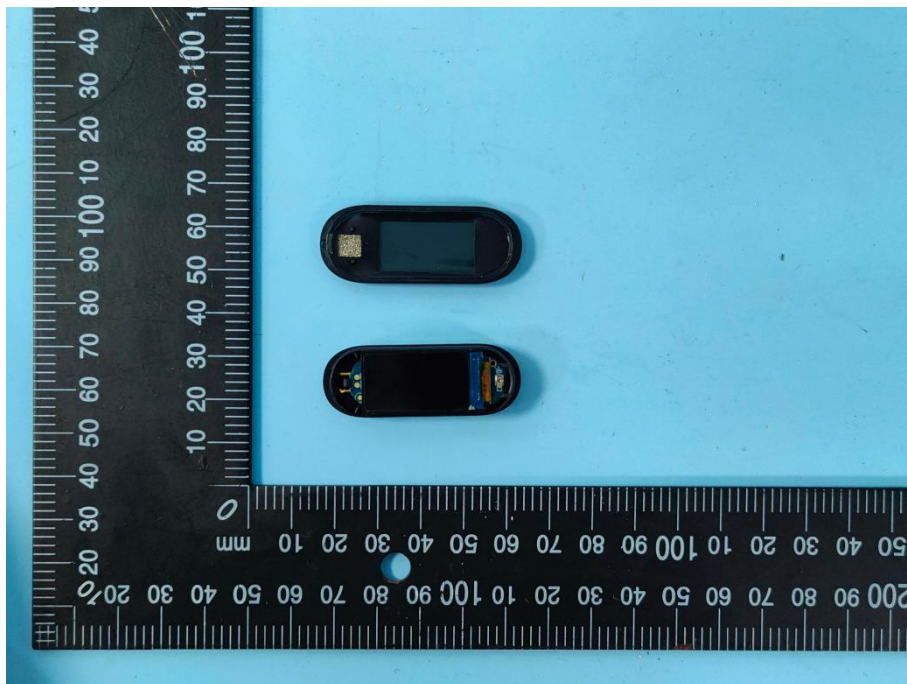


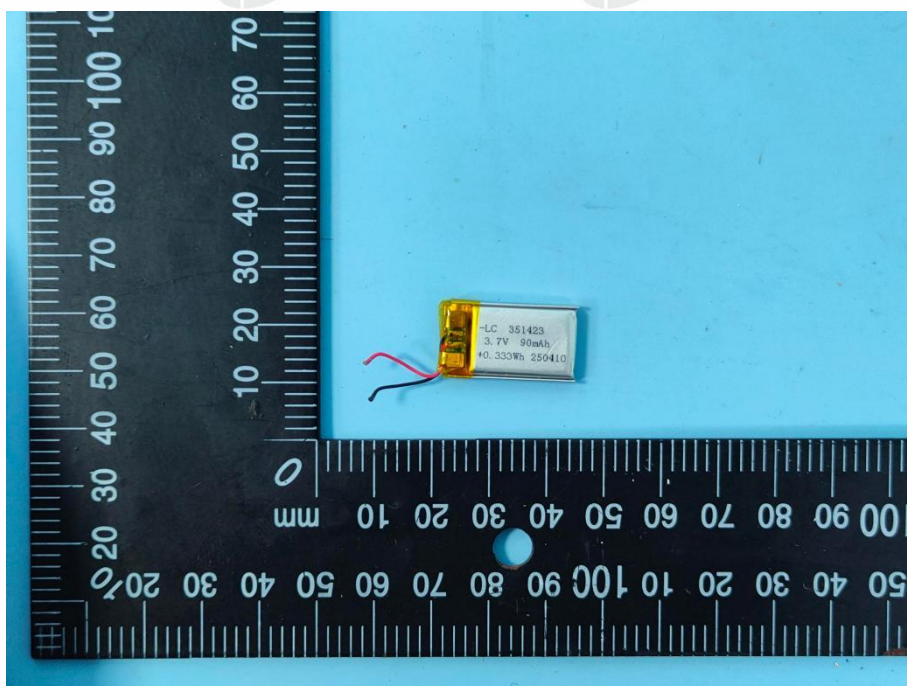
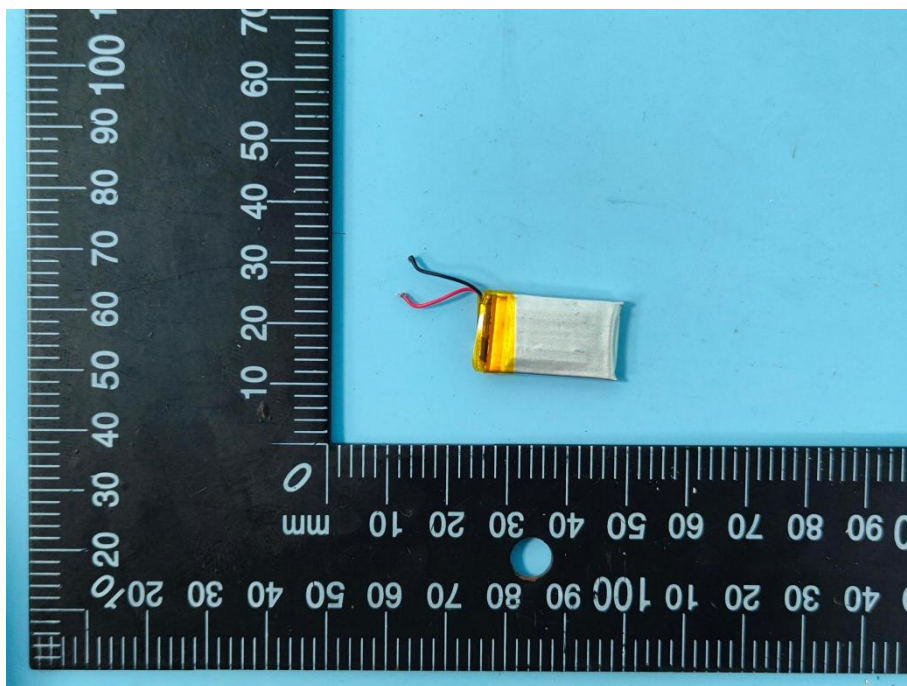


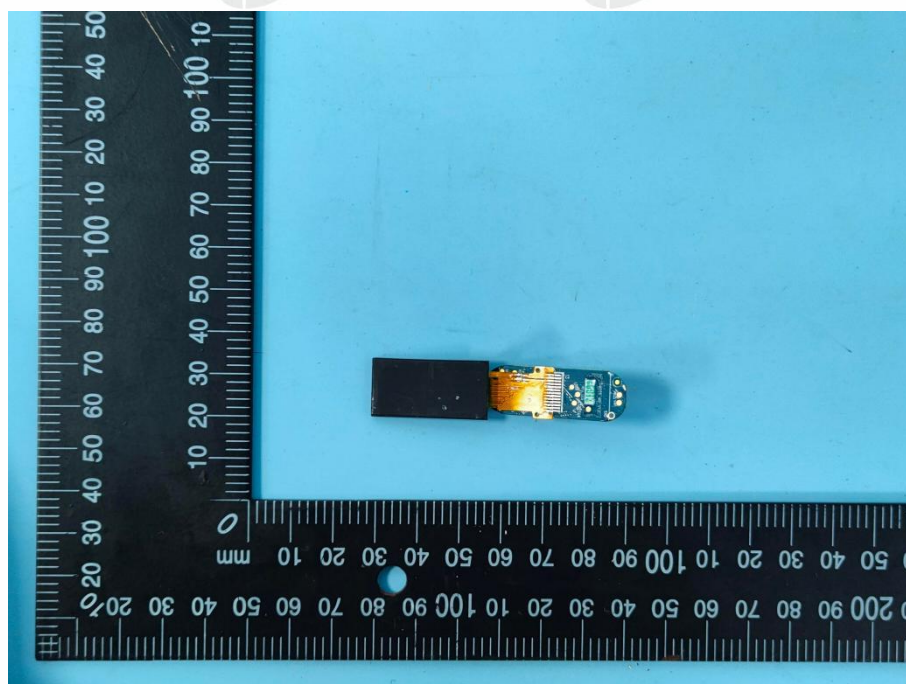
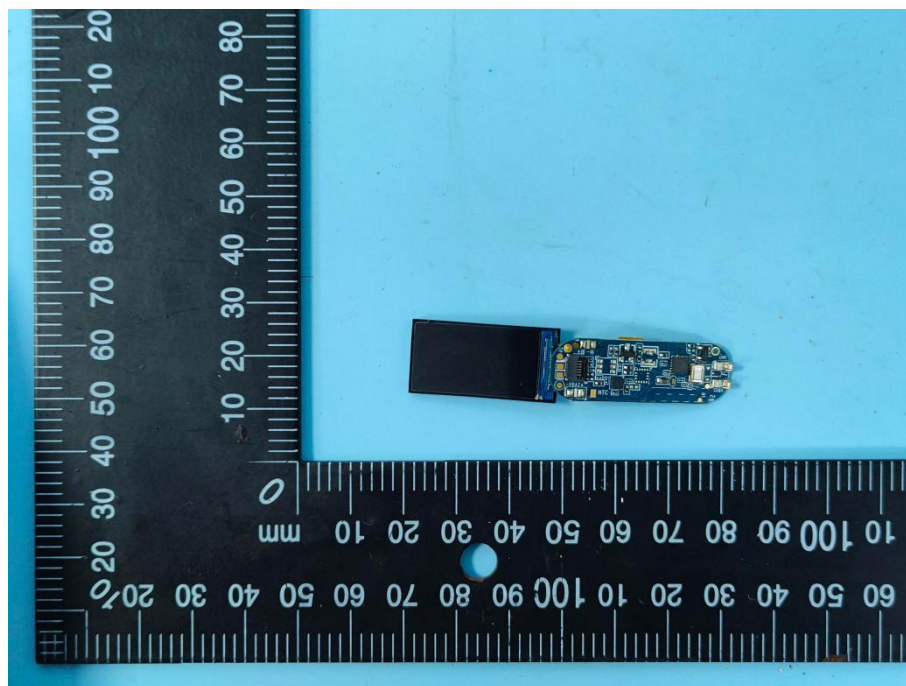
14. EUT Photographs

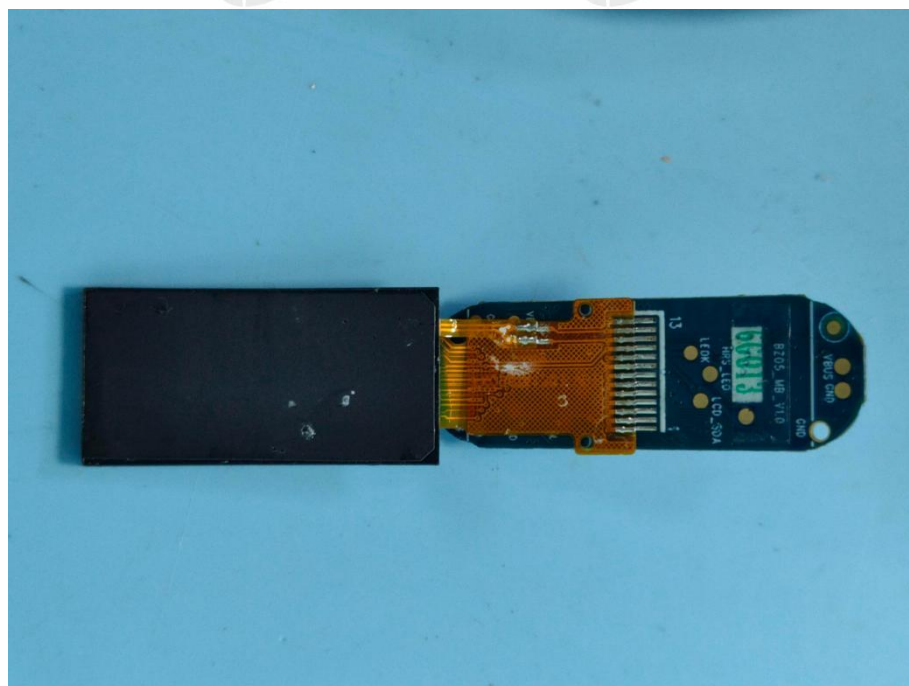
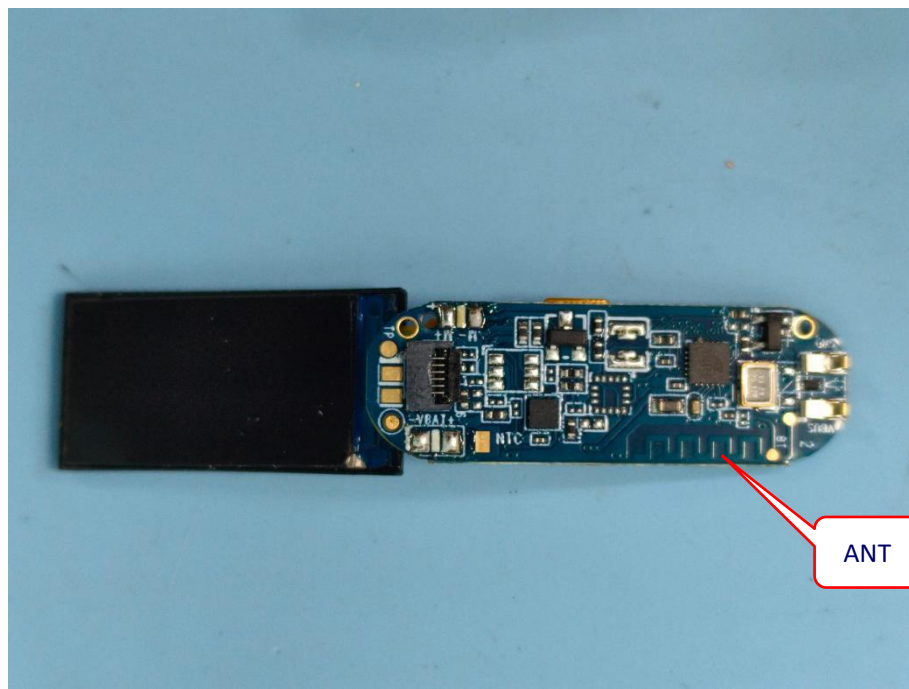












End of report



TEST REPORT

Applicant Name..... : Mid Ocean Brands B.V.
Address..... : Unit 711-716, 7/F., Tower A, 83 King Lam Street, Cheung Sha Wan, Kowloon, Hong Kong.
Manufacturer Name..... :
Address..... :
Product..... : smart band
Model(s)..... : MO2270
Additional Model(s)..... : /
Trademark..... : /
Model Difference..... : /
Prepared by..... : Guangdong Zhonghan Testing Technology Co., Ltd.
Address..... : Room 104/201, Building 1, Yibaolai Industrial Park, Qiaotou, Fuhai Subdistrict, Bao'an District, Shenzhen, Guangdong, China
Date of Receipt..... : Aug. 14, 2026
Date of Test(s)..... : Aug. 14, 2026 to Aug. 27, 2026
Date of Issue..... : Sept. 15, 2026
Test Requested..... : Select test(s) as requested by the client.
Test Standard(s)..... : EN 62479:2010
EN 50663:2017

In the configuration tested, the EUT complied with the standards specified above.

Tested by:

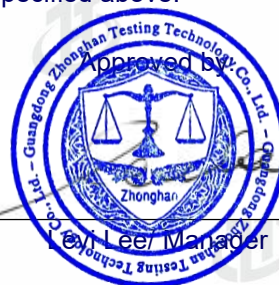
Reviewed by:

Leon Li

Leon Li/ Engineer

Baret Wu

Baret Wu/ Director



Note: The results shown in this test report refer only to the sample(s) tested unless otherwise stated. This test report shall not be reproduced except in full, without prior written approval of ZHT. This document may be altered or revised by ZHT, personnel only, and shall be noted in the revision of the document.



Table of Contents

1. Revision History	3
2. General Information	4
2.1. GENERAL DESCRIPTION OF E.U.T.	4
3. Requirement	5
3.1. GENERAL INFORMATION	5
3.2. LIMIT	5
3.3. GENERAL INFORMATION	5



1. Revision History

Report No.	Issue Date	Description	Approved
ZHT-260814107W01-3	Aug. 27, 2026	Original	Invalid
ZHT-260814107W01-3M1	Sept. 10, 2026	This report modifies the parameter description based on the original report number ZHT-260814107W01-3. The only difference between the new parameters and the original parameters is the way they are described, which does not affect the test results. Therefore, there is no need to add new tests to this report. All test data are referenced from the original report with reference number ZHT-260814107W01-3	Valid
ZHT-260910112W01-3	Sept. 15, 2026	This report has added the name and address of the applicant based on the original report number ZHT-260814107W01-3M1. The only difference between this report and the original report is their applicant name and address, which will not affect the test results. Therefore, there is no need to add new tests to this report. All test data are based on the original report, reference number ZHT-260814107W01-3M1	Valid

2. General Information

2.1. General Description of E.U.T.

Product Name:	smart band
Test Model(s):	MO2270
Hardware Version:	V1.0
Software Version:	V1.0
Operation Frequency:	BLE: 2402MHz-2480MHz, 40 Channels
Type of Modulation:	BLE: GFSK
Antenna installation:	PCB Antenna
Antenna Gain:	0dBi
Ratings	Input:5V---0.5A Internal 3.7V Rechargeable Li-ion battery
Sample Number:	260814107YP001

Remark: The antenna gain is provided by the customer, if the data provided by the customer is not accurate, Guangdong Zhonghan Testing Technology Co., Ltd. does not assume any responsibility.



3. Requirement

3.1.General Information

According to its specifications, the EUT must comply with the requirements of the following standards:EN 62479: 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)]

3.2.Limit

- A. Typical usage, installation and the physical characteristics of equipment make it inherently compliant with the applicable EMF exposure levels such as those listed in the bibliography. This low-power equipment includes unintentional (or non-intentional) radiators, for example incandescent light bulbs and audio/visual (A/V) equipment, information technology equipment (ITE) and multimedia equipment (MME) that does not contain radio transmitters.NOTE Equipment is described as A/V equipment, ITE or MME if its main use is playback/recording of music, voice or images, or processing of digital information.
- B. The input power level to electrical or electronic components that are capable of radiating electromagnetic energy in the relevant frequency range is so low that the available antenna power and/or the average total radiated power cannot exceed the low-power exclusion level defined in 4.2.
- C. The available antenna power and/or the average total radiated power are limited by product standards for transmitters to levels below the low-power exclusion level defined in 4.2.
- D. Measurements or calculations show that the available antenna power and/or the average total radiated power are below the low-power exclusion level defined in 4.2.

3.3.General Information

The available antenna power of this EUT is **BLE:0.51mW(-2.9dBm)**, the power are below the low-power exclusion level defined in 4.2(Pmax: 20mW)."

End of report



中国认可
国际互认
检测
TESTING
CNAS L4062



Test Report

Reference No...... : WTF26X08245897W

Applicant : Mid Ocean Brands B.V.

Address..... : Unit 711-716, 7/F., Tower A, 83 King Lam Street, Cheung Sha Wan,
Kowloon, Hong Kong.

Manufacturer : 120754

Product Name : Smart wireless health watch

Model No...... : MO2270

Standards : EN 18031-2:2024

Date of Receipt sample : 19/08/2026

Date of Test..... : 19/08/2026-16/09/2026

Date of Issue : 23/09/2026

Test Result..... : **PASS**

Remarks:

The results shown in this test report refer only to the sample(s) tested, this test report cannot be reproduced, except in full, without prior written permission of the company. The report would be invalid without specific stamp of test institute and the signatures of approver.

Prepared By:

Waltek Testing Group (Shenzhen) Co., Ltd.

Address: 1/F., Room 101, Building 1, Hongwei Industrial Park, Liuxian 2nd Road,

Block 70 Bao'an District, Shenzhen, Guangdong, China

Tel.: +86-755-33663308 Fax.: +86-755-33663309 Email: sem@waltek.com.cn

Tested by:

Fred Hou

Approved by:

Rio Luo



Table of Contents

Revision History.....	3
1. Summary of Test Results	4
2. General Test Information	13
2.1. Description of EUT	13
2.2. Primary function of EUT	13
2.3. Physical Port of EUT	13
2.4. Document of EUT	13
2.5. Deviations of test standard	13
2.6. Test environment conditions	14
2.7. Test Equipment	14
2.8. Test structure.....	15
2.9. Test procedure	15
2.10. Test laboratory.....	15
3. TEST RESULT	16
3.1 [ACM] Access control mechanism	16
3.2 [AUM] Authentication mechanism.....	18
3.3 [SUM] Secure update mechanism.....	24
3.4 [SSM] Secure storage mechanism	27
3.5 [SCM] Secure communication mechanism.....	31
3.6 [LGM] Logging mechanism	35
3.7 [DLM] Deletion mechanism.....	38
3.8 [UNM] User notification mechanism	39
3.9 [CCK] Confidential cryptographic keys	41
3.10 [GEC] General equipment capabilities	44
3.11 [CRY] Cryptography	50
4. Assignment of verdict	52
Appendix I : Photos of the EUT	53



Revision History

Revision	Revisions	Issue Date	Revised By
V1.0	Initial released Issue	23/09/2026	Fred Hou

WALTEK



1. Summary of Test Results

By performing the Conceptual assessment, Functional completeness assessment, and Functional sufficiency assessment of ACM, AUM, SUM, SSM, SCM, RLM, NMM, TCM, CCK, GEC, and CRY, There are currently no remaining non-conformities..

Based on the above test results, the conclusion of this test is: **Pass**.

See below detailed test result:

Test items	Test content		Verdict
1	[ACM] Access Control Mechanism		
1.1	[ACM-1] Applicability of access control mechanisms	The equipment shall use access control mechanisms to manage entities' access to security assets and network assets	PASS
1.2	[ACM-2] Appropriate access control mechanisms	Access control mechanisms that are required per ACM-1 shall ensure that only authorized entities have access to the protected security assets and network assets	PASS
1.3	[ACM-3] Default Access Control for Children in Toys	When the device is a toy, for each child that has access to external content and the child's access to the privacy features managed by the access control mechanisms required by ACM-1, the access control mechanisms shall by default ensure that the child's access to external content through the privacy features is limited to content from authorised entities	N/A



1.4	[ACM-4] Default Access Controls to Children's Private Assets for Toys and Childcare Devices	When the device is a toy or childcare device, any ACM-1-required access control mechanisms for children's privacy features and personal information shall by default restrict access to children's privacy features and personal information processed by the device to any third party other than the child or the child's parent/guardian	N/A
1.5	[ACM-5] Parent/Guardian Access Control for Children in Toys	When the device is a toy, any ACM-1 required access control mechanisms to manage child access shall be configured by the authorised entity to restrict child access to protected security and privacy assets for each child-accessible security and privacy asset	N/A
1.6	[ACM-6] Parent/Guardian Access Controls for Access to Managed Children's Privacy Assets by Other Entities in Toys	When the device is a toy, for each child privacy asset that is accessible to entities other than the child and for which access is managed by an access control mechanism required by ACM-1, the access control mechanism shall be configured by the authorised entity to restrict access by other entities to the managed child privacy assets	N/A
2	[AUM] Authentication mechanism		
2.1	[AUM-1] Applicability of authentication mechanisms	[AUM-1-1] Shall use authentication mechanisms for managing entities' access via network interfaces	PASS
2.2		[AUM-1-2] Shall use authentication mechanisms for managing entities' access via user interfaces	N/A



2.3	[AUM-2] Appropriate authentication mechanisms	Authentication mechanisms that are required per AUM-1-1 (network interface) or AUM-1-2 (user interface) shall verify an entity's claim based on examining evidence from at least one element of the categories knowledge, possession and inherence (one factor authentication)	PASS
2.4	[AUM-3] Authenticator Validation	Authentication mechanisms that are required per AUM-1-1 (network interface) or AUM-1-2 (user interface) shall validate all relevant properties of the used authenticators, dependent on the available information in the operational environment of use	PASS
2.5	[AUM-4] Change Authenticator	Authentication mechanisms that are required per AUM-1-1 or AUM-1-2 shall allow for changing the authenticator except for authenticators where conflicting security goals do not allow for a change	PASS
2.6	[AUM-5] Password strength	[AUM-5-1] If factory default passwords are used by an authentication mechanism that is required per AUM-1-1 or AUM-1-2, they shall: — be unique per equipment; and — follow best practice concerning strength; or — be enforced to be changed by the user before or on first use	N/A



2.7		[AUM-5-2]If passwords other than factory default passwords are used by an authentication mechanism required per AUM-1-1 or AUM-1-2, they shall: — be enforced to be set by the user before or on first use and before the equipment is logically connected to a network; or — be defined by an authorized entity within a network where access is limited to authorised entities; or — be generated by the equipment using best practice concerning strength and only communicated to an authorized entity within a network where access is limited to authorised entities.	N/A
2.8	[AUM-6] Brute force breach protection	Authentication mechanisms required per AUM-1-1 or AUM-1-2 shall be resilient against brute force attacks	PASS
3	[SUM] Security Update Mechanism		
3.1	[SUM-1] Applicability of the updated mechanisms	The equipment shall provide at least one update mechanism for updating software, including firmware, affecting security assets and/or network assets	PASS
3.2	[SUM-2] Security updates	Each update mechanism as required per SUM-1 shall only install software whose integrity and authenticity are valid at the time of the installation.	PASS
3.3	[SUM-3] Automatic updates	update mechanism that is required per SUM-1 shall be capable of updating the software	PASS
4	[SSM] Secure Storage Mechanism		
4.1	[SSM-1] Applicability of safe storage mechanisms	The equipment shall always use secure storage mechanisms for protecting the security assets and network assets persistently stored on the equipment, except for persistently stored security assets or network assets	PASS



4.2	[SSM-2] Provide appropriate integrity protection for safe storage mechanisms	Secure storage mechanism that is required per SSM-1 shall protect the integrity of security assets and network assets it stores persistently	PASS
4.3	[SSM-3] Provide adequate confidentiality protection for secure storage mechanisms	Each secure storage mechanism that is required per SSM-1 shall protect the secrecy of confidential security parameter and confidential network function configuration it stores persistently	PASS
5	[SCM] Secure Communication Mechanism		
5.1	[SCM-1] Applicability of secure communication mechanisms	The equipment shall always use secure communication mechanisms for communicating security assets and network assets with other entities via network interfaces	PASS
5.2	[SCM-2] Provide adequate integrity and authenticity protection for secure communication mechanisms	Shall apply best practices to protect the integrity and authenticity of the security assets and network assets communicated	PASS



5.3	[SCM-3] Provide adequate confidentiality protection for secure communication mechanisms	shall apply best practices to protect the confidentiality of communicated network assets and security assets where confidentiality protection of those is needed	PASS
5.4	[SCM-4] Adequate replay protection for secure communication mechanisms	Shall apply best practices to protect the security assets and the network assets communicated against replay attacks	PASS
6	[LGM] Logging mechanism		
6.1	[LGM-1] Applicability of logging mechanisms	Devices should use logging mechanisms to record internal activities (called events) related to privacy assets and their protection	PASS
6.2	[LGM-2] Persistent storage of log data	The logging mechanism required by LGM-1 shall store log data of relevant events in the persistent storage of the device	PASS
6.3	[LGM-3] Minimum number of events in persistent storage	All log data stored in device persistent storage by the LGM-1-required logging mechanism shall include the minimum number of latest events, latest events	PASS



6.4	[LGM-4] Persistent storage of time-dependent information on log data	All log data stored in device persistent storage by the logging mechanism required by LGM-1 shall include timestamps or time-related information	PASS
7	[DLM] Deletion Mechanism		
7.1	[DLM-1] Applicability of the deletion mechanism	The device should provide a deletion mechanism that allows users to delete personal data and sensitive security parameters stored on the device	PASS
8	[UNM] User Notification Mechanism		
8.1	[UNM-1] Applicability of user notification mechanisms	The device should provide a user notification mechanism for notifying device users of changes that affect the protection or privacy of their personal information.	PASS
8.2	[UNM-2] Appropriate content of user notifications	The notification provided by the required UNM-1 user notification mechanism shall include, at a minimum, a description of the change and a description of how the change affects the protection and privacy of personal information.	PASS
9	[CCK] Confidential Cryptographic Key		
9.1	[CCK-1] Appropriate confidential encryption key	Confidential cryptographic keys that are preinstalled or generated by the equipment during its use, shall support a minimum security strength of 112-bits	PASS



9.2	[CCK-2] Confidential cryptographic key generation mechanism	The generation of confidential cryptographic keys shall adhere to best practice cryptography	PASS
9.3	[CCK-3] Preventing Static Defaults for Preloaded Secret Encryption Keys	Preinstalled confidential cryptographic keys shall be practically unique per equipment	N/A
10	[GEC] General equipment capacity		
10.1	[GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities	The equipment shall not include publicly known exploitable vulnerabilities	PASS
10.2	[GEC-2] Restriction of service exposure through relevant network interfaces	In factory default state the equipment shall only expose — network interfaces; and — services via network interfaces	PASS
10.3	[GEC-3] Configuration of optional services and associated public network interfaces	Optional network interfaces or optional services exposed via network interfaces affecting security assets or network assets, which are part of the factory default state shall have the option for an authorized user to enable and disable the network interface or service	PASS



10.4	[GEC-4] Documentation of network interface exposures and services exposed through network interfaces	The equipment's user documentation shall contain a description of — all exposed network interfaces; and — all services exposed via network interfaces	PASS
10.5	[GEC-5] No unnecessary external interfaces	The equipment shall only expose physical external interfaces if they are necessary for its intended Functionality	PASS
10.6	[GEC-6] Input validation	The equipment shall validate input received via external interfaces if the input has potential impact on security assets and/or network assets	PASS
10.7	[GEC-7] Documentation of external sensing capabilities	All external sensing capabilities of the device related to the privacy of the user or subscriber shall be logged to the user	N/A
11	[CRY] Cryptography		
11.1	[CRY-1] Best Practice Cryptography	The equipment shall use best practice for cryptography that is used for the protection of the security assets or network assets	PASS



2. General Test Information

2.1. Description of EUT

EUT Name	Smart wireless health watch
Model	MO2270
EUT Function Description	The EUT is a smartwatch that connects to a mobile app via Bluetooth.
Bluetooth	V5.2
Hardware Configuration	AB2026B3
Communication Modules	AB2026B3
Operating System	RISC-V
Hardware Version	V1.0
Software Version	V1.3
Firmware Version	V1.3
Communication Protocols	Bluetooth
Communication Module Certification Report	/

Note: The information above are provided by the manufacturer of the EUT.

2.2. Primary function of EUT

Function	Description
Smart wireless health watch	The EUT is a smartwatch that connects to a mobile app via Bluetooth.

2.3. Physical Port of EUT

Physical Port	Description
Touch button	Press to choose mode; Long press to confirm
Sensor light	Detect whether a watch is being worn
Contact for charging cable	Charging

2.4. Document of EUT

1. User manual;

2.5. Deviations of test standard



No deviation.

2.6. Test environment conditions

During the measurement the environmental conditions were within the listed ranges:

Temperature range:	25.1°C~29.5°C
Humidity range:	53.5%RH~66.8%RH

Note: The specific temperature and humidity information of each test item refers to the temperature and humidity record in the corresponding test data.

2.7. Test Equipment

1) Equipment:

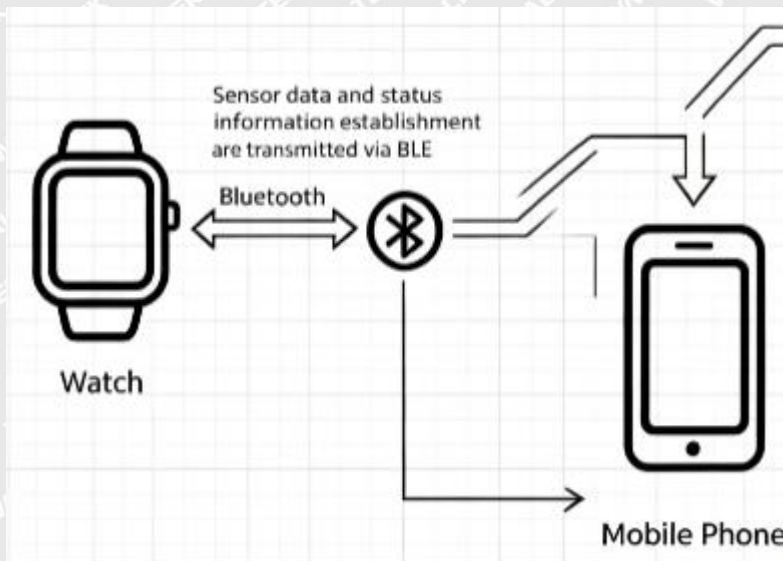
Fixed Asset Number	Hardware Environment		Software Environment
	Name/Model	Configuration (CPU/memory/hard drive)	
WTXW1105A1013	PC/ ThinkPad P52	CPU: intel i5 Memory: 16GB Hard disk: 1TSSD	1. Windows 11 Home Chinese Edition/Client Operating System.
Network environment: LAN.			

2) Tools:

Fixed Asset Number	Tool name	Version	Tool Usage	quantities
WTXW1105A1019	Wireshark	V4.6.2	WIFI protocol analysis	1
WTXW1105A1020	Proxypin	v1.2.3	Packet capture	1
WTXW2108B0001	BTP	v1.14.0	BLE protocol analysis	1



2.8. Test structure



2.9. Test procedure

- (1) The EUT placement requires reference to the test block diagram and is placed on a non-metallic table.
- (2) Setup the EUT and assistant equipment as shown above block diagram and equipment list.
- (3) Finish the Conceptual assessment and Functional completeness assessment based on the materials and evidences collected from customer.
- (4) Via WIFI network sniffer, replay and brute force password, with all kinds of manual test, the test engineer execute the Functional sufficiency assessment.

2.10. Test laboratory

Waltek Testing Group (Shenzhen) Co., Ltd.

1/F., Room 101, Building 1, Hongwei Industrial Park, Liuxian 2nd Road, Block 70 Bao'an District, Shenzhen, Guangdong, China

Tel.: +86-755-33663308 Fax.: +86-755-33663309 Email: sem@waltek.com.cn



3. TEST RESULT

3.1 [ACM] Access control mechanism

3.1.1 [ACM-1] Applicability of access control mechanisms

Conceptual assessment:

According to [E.Just.DT.ACM-1] in technical documentation, the verdict of this conceptual test is **PASS**.

Functional completeness assessment

All security assets and network assets accessible by entities have been recorded in [E.Info.ACM-1.NetworkAsset] and [E.Info.ACM-1.SecurityAsset]. Therefore the verdict of this Functional completeness assessment is **PASS**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
Access control mechanisms to manage the entity's use of assets existed and there was no evidence that they had not been implemented	EUT's Bluetooth is accessed and controlled via pairing packets using the SMP protocol.	PASS
Judgement (Verdict)	PASS	
Evidence	Bluetooth Access Control	

3.1.2 [ACM-2] Appropriate access control mechanisms

Conceptual assessment:



According to [E.Just.DT.ACM-2] in technical documentation, the verdict of this conceptional test is **PASS**.

Functional completeness assessment

This Functional completeness assessment is covered by the Functional sufficiency assessment of the applicability of the access control mechanism. Therefore, this Functional completeness assessment is not required.

Functional sufficiency assessment

Descriptions	Test results	Verdict
Roles assigned to each user have associated authorizations	Each EUT user has corresponding permissions.	PASS
Least privilege is associated with the role	Role permissions corresponding to each EUT user	PASS
Assets can only be accessed by authorized users given their role	Assets are only accessible to users who have been authenticated.	PASS
Only authorized users can change roles	EUT can only change the user role after verification	PASS
Judgement (Verdict)	PASS	
Evidence		

3.1.3 [ACM-3] Authenticator validation



The EUT is not a toy, therefore the verdict of this test is **NOT APPLICABLE**.

3.1.4 [ACM-4] Default access control to children's privacy assets for toys and childcare equipment

The EUT is not a toy, therefore the verdict of this test is **NOT APPLICABLE**.

3.1.5 [ACM-5] Parental/Guardian access controls for children in toys

The EUT is not a toy, therefore the verdict of this test is **NOT APPLICABLE**.

3.1.6 [ACM-6] Parental/Guardian access controls for other entities' access to managed children's privacy assets in toys

The EUT is not a toy, therefore the verdict of this test is **NOT APPLICABLE**.

3.2 [AUM] Authentication mechanism

3.2.1 [AUM-1] Applicability of authentication mechanisms

[AUM-1-1] Requirement network interface

Conceptual assessment:

There is no authentication mechanism through the network interface that needs to be evaluated, the verdict of this conceptual test is **NOT APPLICABLE**.

Functional completeness assessment

There are no authentication mechanism in user interface of the EUT. Therefore the verdict of this Functional completeness assessment is **NOT APPLICABLE**.

Functional sufficiency assessment

Descriptions		Test results	Verdict
The authentication mechanism is implemented as specified in [E.Info.AUM-1-1.ACM.AuthenticationMechanism].		Implementing identity authentication through Bluetooth binding	PASS
Judgement (Verdict)	PASS		

Bluetooth				
Time	Source	Destination	Protocol	Length Info
715.119.883880	controller	host	HC-L2CAP	7 Read Command Complete (L2CAP Set Scan Enable)
715.119.883873	controller	host	HC-L2CAP	7 Read Command Complete (L2CAP Set Scan Parameters)
715.119.883793	controller	host	HC-L2CAP	7 Read Command Complete (L2CAP Set Scan Enable)
715.119.879886	controller	host	HC-L2CAP	7 Read Command Complete (L2CAP Set Scan Enable)
715.119.879888	controller	host	HC-L2CAP	7 Read Command Complete (L2CAP Add Device To Filter Accept List)
715.119.879793	controller	host	HC-L2CAP	8 Read Command Complete (Vendor Command 000001 [Sequence 0x0001])
715.119.879888	controller	host	HC-L2CAP	8 Read Command Complete (Vendor Command 000001 [Sequence 0x0001])
442.119.489793	localhost (3)	41:42:55:06:5b:09 (3)	SNP	16 Read Pairing Request: Address: Binding, MTX Initiator Key[] 10K Responder
442.119.597908	localhost (3)	41:42:55:06:5b:09 (3)	SNP	16 Read Pairing Request: Address: Binding, MTX Initiator Key[] 10K Responder
442.119.644106	localhost (3)	41:42:55:06:5b:09 (3)	SNP	16 Read Pairing Confirm
442.119.717328	localhost (3)	41:42:55:06:5b:09 (3)	SNP	16 Read Pairing Confirm
442.119.727068	localhost (3)	41:42:55:06:5b:09 (3)	SNP	16 Read Pairing Random
442.119.907393	localhost (3)	41:42:55:06:5b:09 (3)	SNP	16 Read Pairing Random
442.119.908416	localhost (3)	41:42:55:06:5b:09 (3)	SNP	16 Read Encryption Information
442.119.937412	localhost (3)	41:42:55:06:5b:09 (3)	SNP	16 Read Central Identification
442.119.939793	localhost (3)	41:42:55:06:5b:09 (3)	SNP	16 Read Identity Information
443.119.739408	localhost (3)	41:42:55:06:5b:09 (3)	SNP	17 Send Identity Address Information
443.119.970816	localhost (3)	41:42:55:06:5b:09 (3)	SNP	16 Send Identity Information
445.119.739416	localhost (3)	41:42:55:06:5b:09 (3)	SNP	17 Send Identity Address Information

[AUM-1-2] Requirement user interface

Conceptual assessment:

According to [E.Just.DT.AUM-1-2] in technical documentation, the verdict of this conceptual test is **PASS**.

Functional completeness assessment

This Functional completeness assessment is covered by the Functional sufficiency assessment of the applicability of the certification scheme. Therefore, this Functional completeness assessment is not required. Therefore the verdict of this Functional completeness assessment is **NOT APPLICABLE**.

Functional sufficiency assessment

This Functional completeness assessment is covered by the Functional sufficiency assessment of the applicability of the certification scheme. Therefore, this Functional completeness assessment is not required. Therefore the verdict of this Functional completeness assessment is **NOT APPLICABLE**.

3.2.2 [AUM-2] Appropriate authentication mechanisms

Conceptual assessment:

According to [E.Just.DT.AUM-2] in technical documentation, the verdict of this conceptual test is **PASS**.

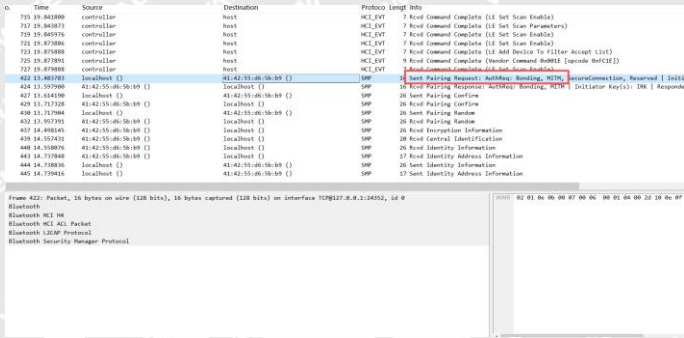
Functional completeness assessment

This Functional completeness assessment is covered by the Functional sufficiency assessment of the applicability of the certification scheme. Therefore, this Functional completeness assessment is not required. Therefore the verdict of this Functional completeness assessment is **NOT APPLICABLE**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
--------------	--------------	---------



Authentication is possible and the authentication mechanism is implemented as specified in [E.Info.AUM-2-1.AuthenticationMechanism].	1. After start-up, the EUT will sending pairing request. If the terminal app receive request and reply with response. The two device will begin pairing stage. The SMP is responsible for the pairing process between devices, ensuring that both parties can securely exchange keys and authentication information before establishing a connection. Through this pairing, devices can establish a secure connection to protect subsequent data transmission.	PASS
Judgement (Verdict)	PASS	
Evidence	Bluetooth 	

3.2.3 [AUM-3] Authenticator validation

Conceptual assessment:

According to [E.Just.DT.AUM-3] in technical documentation, the verdict of this conceptional test is **PASS**.

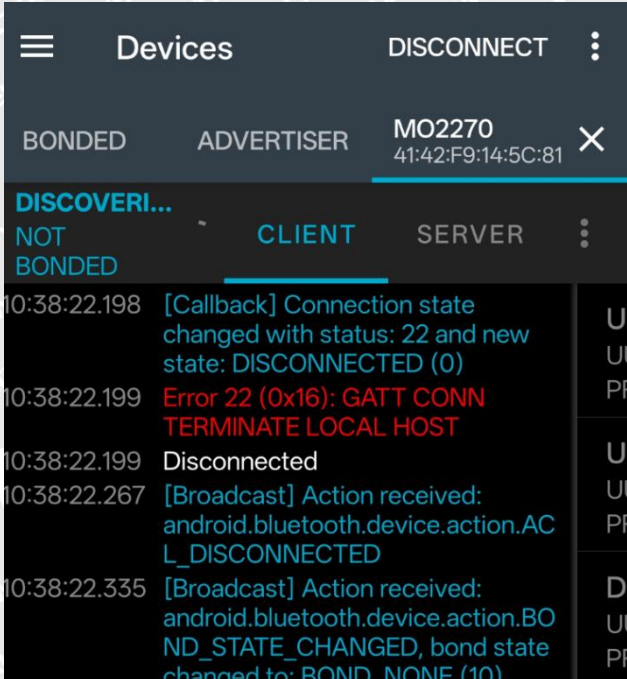
Functional completeness assessment

This Functional completeness assessment is covered by the Functional sufficiency assessment of the applicability of the certification scheme. Therefore, this Functional completeness assessment is not required. Therefore the verdict of this Functional completeness assessment is **NOT APPLICABLE**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
--------------	--------------	---------



Incorrect validators cannot to used for successful validation	The EUT only accepts Bluetooth connections from the mobile app; all other connections will be rejected or the EUT Bluetooth cannot be detected.	PASS
Judgement (Verdict)	PASS	
Evidence	The Bluetooth restriction of the EUT allows connection only through the app; all other connection methods will fail or the EUT Bluetooth cannot be detected. 	

3.2.4 [AUM-4] Changing authenticator

Conceptual assessment:

According to [E.Just.DT.AUM-1] in technical documentation, the verdict of this conceptional test is **PASS**.

Functional completeness assessment

This Functional completeness assessment is covered by the Functional sufficiency assessment of the applicability of the certification scheme. Therefore, this Functional completeness assessment is not required. Therefore the verdict of this Functional completeness assessment is **NOT APPLICABLE**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
--------------	--------------	---------



Authenticators can be changed according to the instructions in [E.Info.AUM-4.AUM.AuthChange].	The Bluetooth connecter of the EUT can be changed.	PASS
Newly Assigned Authenticators Allow access to Secure, Private Assets on Every Route	Newly assigned authenticators can view the device and Internet information of the EUT through BLE and the EUT	PASS
Previous authenticator no longer allows access to secure, private assets via any path	Previous authenticator no longer allows subscribe request of the BLE	PASS
Judgement (Verdict)	PASS	
Evidence		

3.2.5 [AUM-5] Password strength

Conceptual assessment:

According to [E.Just.DT.AUM-5] in technical documentation, the verdict of this conceptional test is **PASS**.

Functional completeness assessment

This Functional completeness assessment is covered by the Functional sufficiency assessment of the applicability of the certification scheme. Therefore, this Functional completeness assessment is not required. Therefore the verdict of this Functional completeness assessment is **NOT APPLICABLE**.



Functional sufficiency assessment

Descriptions		Test results	Verdict
factory default passwords must be set "before or on first use".		Bluetooth is not a password, and the network interface and user interface have no other authentication mechanisms.	NOT APPLICABLE
Judgement (Verdict)	NOT APPLICABLE		
Evidence	/		

3.2.6 [AUM-6] Applicability of access control mechanisms

Conceptual assessment:

According to [E.Just.DT.AUM-6] in technical documentation, the verdict of this conceptual test is **PASS**.

Functional completeness assessment

This Functional completeness assessment is covered by the Functional sufficiency assessment of the applicability of the certification scheme. Therefore, this Functional completeness assessment is not required. Therefore the verdict of this Functional completeness assessment is **NOT APPLICABLE**.

Functional sufficiency assessment

Descriptions		Test results	Verdict
The number of consecutive failed attempts before the device blocks further attempts matches the value recorded in [E.Info.AUM-6.AUM.BFProtection		1. Bluetooth has a pairing authentication for confirmation to prevent brute-force attacks	PASS
Judgement (Verdict)	PASS		



Evidence	 4
------------------------	---

3.3 [SUM] Secure update mechanism

3.3.1 [SUM-1] Applicability of update mechanisms

Conceptual assessment:

According to [E.Just.DT.SUM-1] in technical documentation, the verdict of this conceptual test is **PASS**.

Functional completeness assessment

This Functional completeness assessment is covered by the Functional sufficiency assessment of the applicability of the certification scheme. Therefore, this Functional completeness assessment is not required. Therefore the verdict of this Functional completeness assessment is **NOT APPLICABLE**.

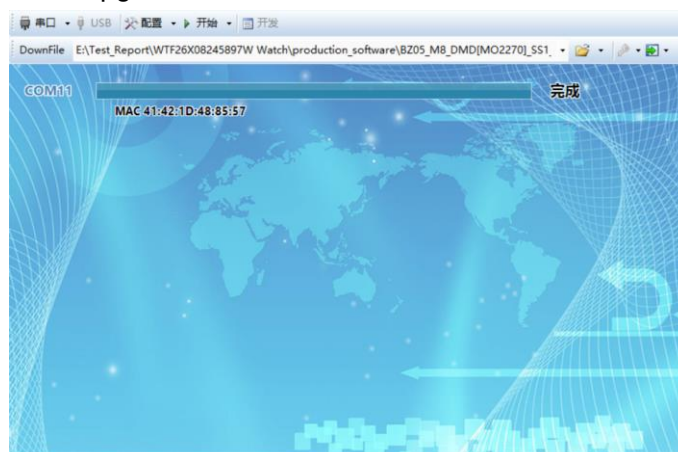
Functional sufficiency assessment

Descriptions	Test results	Verdict
Update (SW-a) Installation was successful and relevant software components were effectively updated	The software can be updated by local upgrade.	PASS
Judgement (Verdict)	PASS	



Evidence

Local upgrade



3.3.2 [SUM-2] Secure updates

Conceptual assessment:

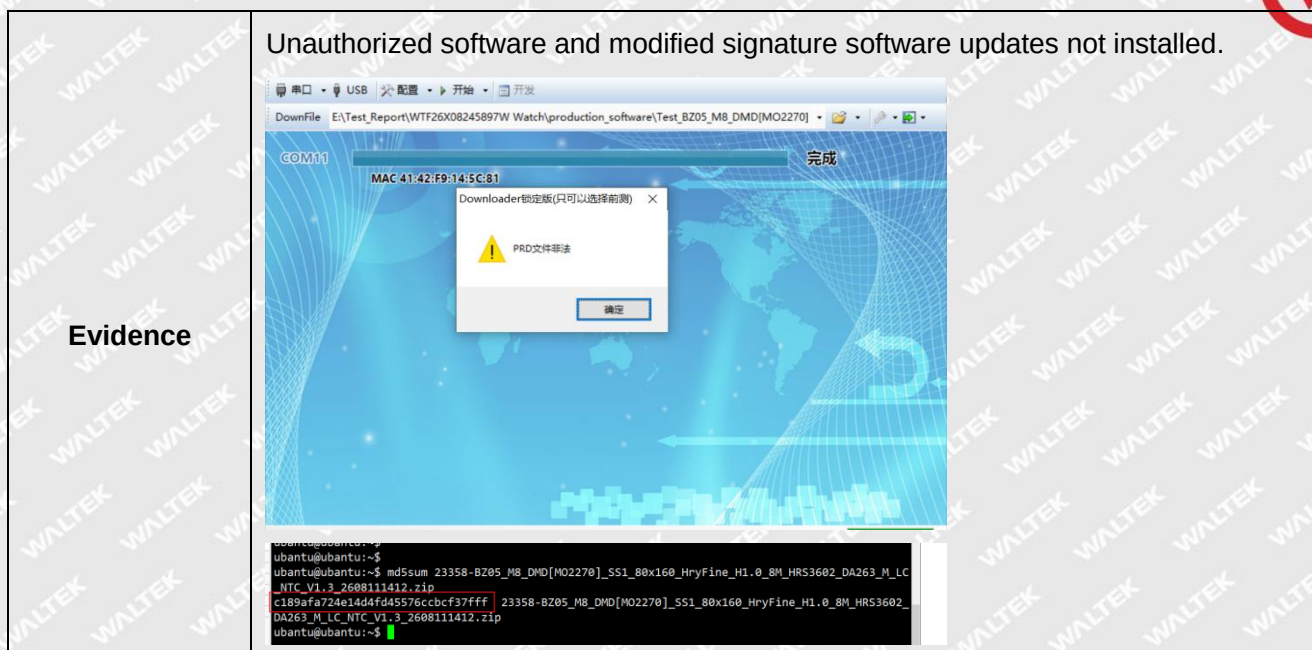
According to [E.Just.DT.SUM-2] in technical documentation, the verdict of this conceptional test is **PASS**.

Functional completeness assessment

This Functional completeness assessment is covered by the Functional sufficiency assessment of the applicability of the certification scheme. Therefore, this Functional completeness assessment is not required. Therefore the verdict of this Functional completeness assessment is **NOT APPLICABLE**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
It is implemented according to the SCM using [IC.SUM-2.AuthInt Val.Sign]	The EUT update package includes a hash to verify its integrity and authenticity	PASS
Test upgrading the software using an unsigned upgrade package	Unauthorized software updates not installed.	PASS
Test the EUT using the modified signature upgrade package for an upgrade	The modified signature cannot be upgraded	PASS
Judgement (Verdict)	PASS	



Evidence

Unauthorized software and modified signature software updates not installed.

3.3.3 [SUM-3] Automated updates

Conceptual assessment:

According to [E.Just.DT.SUM-3] in technical documentation, the verdict of this conceptual test is **PASS**.

Functional completeness assessment

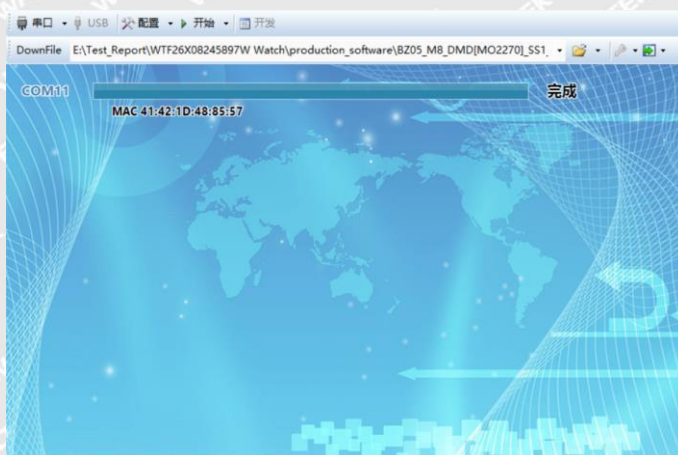
This Functional completeness assessment is covered by the Functional sufficiency assessment of the applicability of the certification scheme. Therefore, this Functional completeness assessment is not required. Therefore the verdict of this Functional completeness assessment is **NOT APPLICABLE**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
The device can install updates "without human intervention on the device" or "by scheduling the installation of updates with human approval" or "by triggering the installation of updates with human approval". Successful update of relevant software components	The device can install updates by triggering the installation of updates with human approval.	PASS
Judgement (Verdict)	PASS	

**Evidence**

The upgrade can be done with the user's approval to use the vendor's software.



3.4 [SSM] Secure storage mechanism

3.4.1 [SSM-1] Applicability of secure storage mechanisms

Conceptual assessment:

Wi-Fi credentials, which are protected by multiple security mechanisms. Physically, as a household product, the device enjoys basic environmental security; its storage chip is wrapped in a solid shell to resist direct contact under non-destructive disassembly. At the interface level, the device does not reserve any available physical debugging ports, thus cutting off the path to directly access internal storage through hardware. At the logical level, all high-risk remote network services (such as SSH) have been disabled, effectively preventing unauthorized network access. Therefore, the verdict of this conceptional test is **NOT APPLICABLE**.

Functional completeness assessment

There are no assets accessible by entities. Therefore the verdict of this Functional completeness assessment is **NOT APPLICABLE**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
Security, network assets are "persistently stored only through the secure storage mechanism documented in [E.Info.SSM-1.SecurityAsset.SSM]"	The data information of the running EUT is protected by hardware, the EUT is not expected to have a serial port set, and the user cannot access the backend to view the data.	PASS



Judgement (Verdict)	PASS
Evidence	Physical protection 

3.4.2 [SSM-2] Appropriate integrity protection for secure storage mechanisms

Conceptual assessment:

According to the SSM-1 Conceptual assessment, there are no assets are accessible by entities, therefore.the verdict of this conceptional test is **NOT APPLICABLE**.

Functional completeness assessment

According to SSM-1 functional completeness assessment.The verdict of this Functional completeness assessment is **NOT APPLICABLE**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
Secure storage mechanism "implemented in accordance with [E.Info.SSM-2.SSM.AccessControl]"	EUT's privacy assets and security assets both have hardware protection that provides a secure storage mechanism	PASS
Deny unauthorised modification of stored security, network assets	Deny unauthorised modification of stored security, privacy assets	PASS
Judgement (Verdict)	PASS	



Evidence

Hardware protection

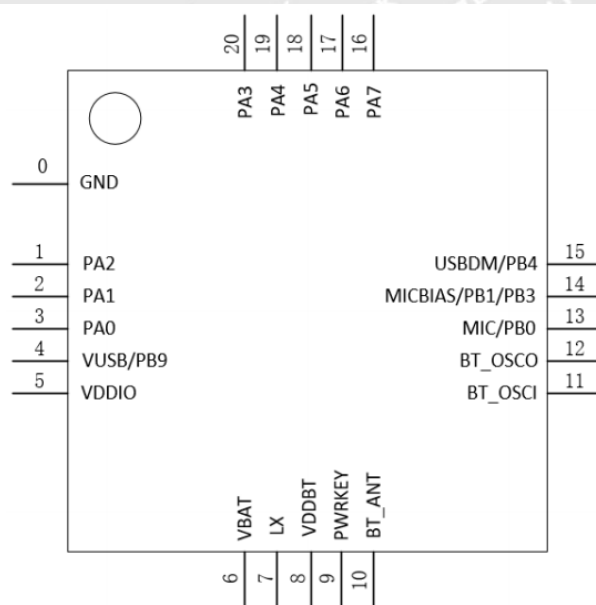


Figure 3-1 Pin assignment for QFN20

3.4.3 [SSM-3] Appropriate confidentiality protection for secure storage mechanisms

Conceptual assessment:

According to the SSM-1 Conceptual assessment, there are no assets are accessible by entities, therefore the verdict of this conceptual test is **PASS**.

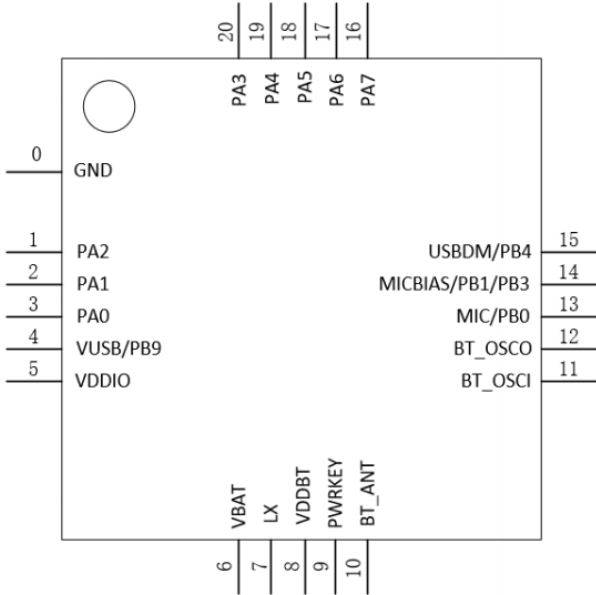
Functional completeness assessment

According to SSM-1 functional completeness assessment. The verdict of this Functional completeness assessment is **NOT APPLICABLE**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
Secure storage mechanism "implemented in accordance with [E.Info.SSM-3.SSM.AccessControl]"	Hardware protection mechanism are implemented to protect the assets.	PASS
Deny unauthorised access to stored confidential security, network assets	Bluetooth files is unavailable if authorized user deny the request	PASS



Judgement (Verdict)	PASS
Evidence	Hardware protection  Figure 3-1 Pin assignment for QFN20 Replay message will not be accepted 



3.5 [SCM] Secure communication mechanism

3.5.1 [SCM-1] Applicability of secure communication mechanisms

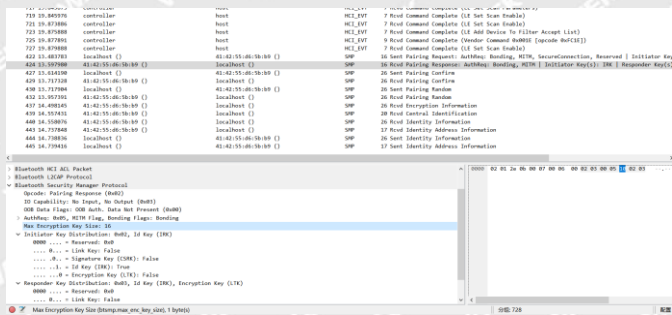
Conceptual assessment:

According to [E.Just.DT.SCM-1] in technical documentation, the verdict of this conceptional test is **PASS**.

Functional completeness assessment

All security assets and network assets accessible by entities have been recorded in [E.Info.SCM-1.NetworkAsset] and [E.Info.SCM-1.SecurityAsset]. Therefore the verdict of this Functional completeness assessment is **PASS**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
As described in [E.Info.SCM-1.SCM], a communication mechanism exists for communicating this security asset	1. After click the bluetooth connection button, the EUT will initiate a Bluetooth connection request ,which uses AES-CCM as encryption algorithm	PASS
Judgement (Verdict)	PASS	
Evidence	BLE link key is encrypted with AES-CCM 128bits 	

3.5.2 [SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms

Conceptual assessment:

According to [E.Just.DT.SCM-1] in technical documentation, the verdict of this conceptional test is **PASS**.



Functional completeness assessment

This Functional completeness assessment is covered by the Functional sufficiency assessment of the applicability of the certification scheme. Therefore, this Functional completeness assessment is not required. Therefore the verdict of this Functional completeness assessment is **NOT APPLICABLE**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
Secrets used to protect authenticity and integrity cannot be intercepted and misused	The EUT can initiate a Bluetooth connection request ,which uses AES-CCM as encryption algorithm.	PASS
Tampered with information is not considered complete information	The EUT will reject non-app data.	PASS
Unauthorised messages not accepted as authentic	Unauthorised messages not accepted as authentic	PASS
Successful man-in-the-middle attacks are not possible when using channel-based communication	Successful man-in-the-middle attacks are not possible when using channel-based communication	PASS
Judgement (Verdict)	PASS	

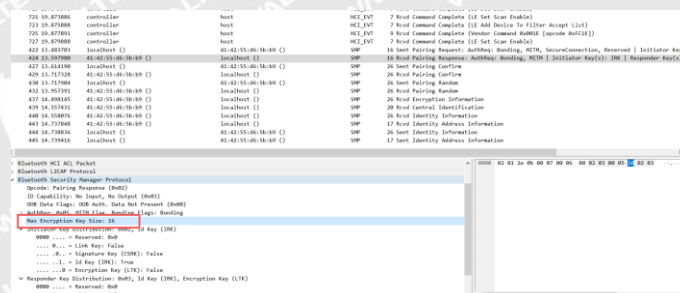


Evidence

Sending repeat BLE request, unauthorised messages not accepted as authentic.



EUT Bluetooth uses the ACM encryption algorithm with a key length of 16 bits, in accordance with best encryption practices.



3.5.3 [SCM-3] Appropriate confidentiality protection for secure communication mechanisms

Conceptual assessment:

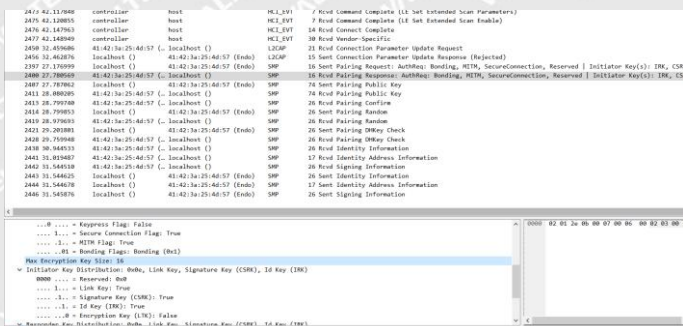
According to [E.Just.DT.SCM-3] in technical documentation, the verdict of this conceptual test is **PASS**.

Functional completeness assessment

This Functional completeness assessment is covered by the Functional sufficiency assessment of the applicability of the certification scheme. Therefore, this Functional completeness assessment is not required. Therefore the verdict of this Functional completeness assessment is **NOT APPLICABLE**.

Functional sufficiency assessment



Descriptions	Test results	Verdict
Communication security, privacy assets cannot be tapped	The security assets and network assets captured by Wireshark and are encrypted.	PASS
Judgement (Verdict)	PASS	
Evidence	BLE link key is encrypted with AES-CCM 128bits 	

3.5.4 [SCM-4] Appropriate replay protection for secure communication mechanisms

Conceptual assessment:

According to [E.Just.DT.SCM-4] in technical documentation, the verdict of this conceptual test is **PASS**.

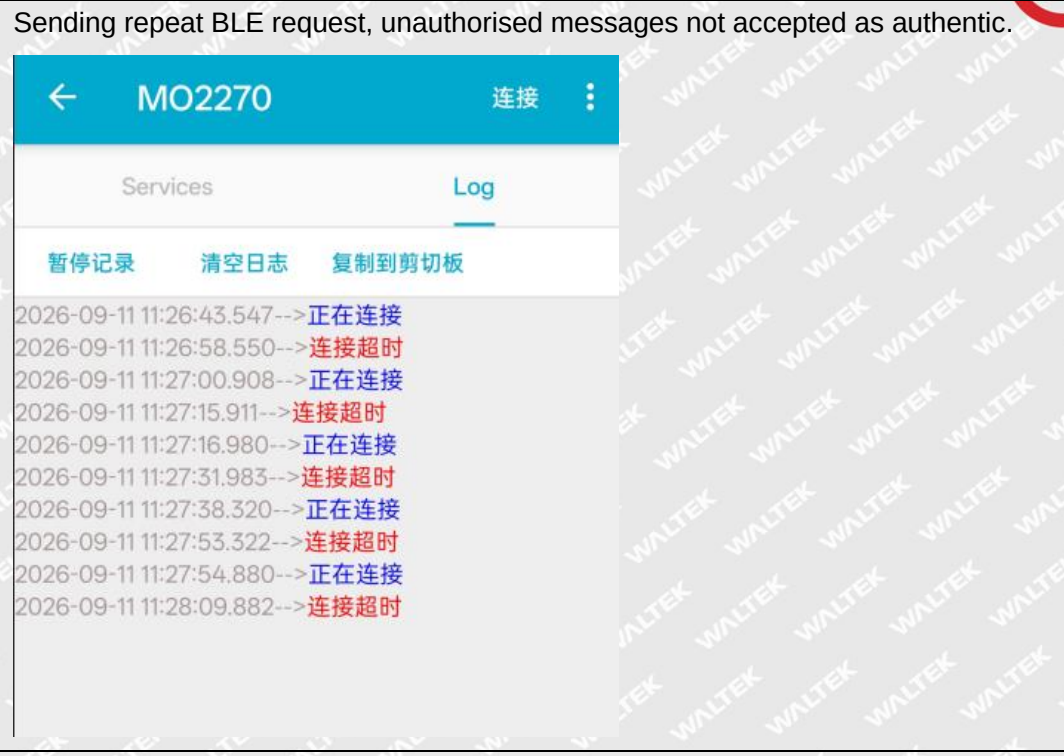
Functional completeness assessment

This Functional completeness assessment is covered by the Functional sufficiency assessment of the applicability of the certification scheme. Therefore, this Functional completeness assessment is not required. Therefore the verdict of this Functional completeness assessment is **NOT APPLICABLE**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
No longer accepts copies (binary copies) of accepted information (part of secure, private asset communications)	1. The Bluetooth encryption key cannot be intercepted.	PASS
Judgement (Verdict)	PASS	



Evidence	Sending repeat BLE request, unauthorised messages not accepted as authentic. 

3.6 [LGM] Logging mechanism

3.6.1[LGM-1]Applicability and appropriateness of logging mechanisms

Conceptual assessment:

According to [E.Just.DT.LGM-1] in technical documentation, the verdict of this conceptional test is **PASS**.

Functional completeness assessment

The verdict of this Functional completeness assessment is **NOT APPLICABLE**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
This event can be generated as documented in [E.Info.LGM-1.PrivacyAssetEvent.	The EUT will record device logs, which can document the changes that occur.	PASS
Log data can be accessed as described in [E.Info.LGM-1.PrivacyAssetEvent.	Device log can be accessed in the app	PASS
Judgement (Verdict)	PASS	



Evidence

```

Hyfine2026-09-09.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
2026-09-09 17:01:31.444.app main status change == true
2026-09-09 17:01:31.457.onActivityResumed:base.activity.WebViewActivity
2026-09-09 17:01:31.755.Current URL: https://app.howruf.com/web/runset/index?lang=zh&sys_code=miui
2026-09-09 17:01:31.759.canGoBack: false
2026-09-09 17:01:31.761.canGoForward: false
2026-09-09 17:01:32.953.performUnbind: false
2026-09-09 17:01:39.747.onActivityResumed:function.home.activity.MainActivity
2026-09-09 17:01:41.302.app background
2026-09-09 17:01:41.304.app main status change == false
2026-09-09 17:01:42.810.performUnbind: false
2026-09-09 17:02:01.560.performUnbind: false
2026-09-09 17:02:02.735.通知栏服务正常, 可以获取到通知信息
2026-09-09 17:02:11.227.app main status change == true
2026-09-09 17:02:11.240.onActivityResumed:function.home.activity.MainActivity
2026-09-09 17:02:12.745.performUnbind: false
2026-09-09 17:02:14.239.app background
2026-09-09 17:02:14.250.app main status change == false
2026-09-09 17:02:41.880.performUnbind: false
2026-09-09 17:02:41.912.app main status change == true
2026-09-09 17:02:41.922.onActivityResumed:function.home.activity.MainActivity
2026-09-09 17:02:43.429.performUnbind: false
2026-09-09 17:02:49.243.Ble---disconnect
2026-09-09 17:02:49.272.getWeatherInfo isNewDay: true
2026-09-09 17:02:49.343.onActivityResumed:function.home.activity.MainActivity
第 1 行, 第 1 列 100% Windows (CRLF) UTF-8

```

3.6.2 [LGM-2] Persistent storage of log data

Conceptual assessment:

According to [E.Just.DT.LGM-2] in technical documentation, the verdict of this conceptual test is **PASS**.

Functional completeness assessment

This Functional completeness assessment is covered by the Functional sufficiency assessment of the applicability of the certification scheme. Therefore, this Functional completeness assessment is not required. Therefore the verdict of this Functional completeness assessment is **NOT APPLICABLE**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
Log data of relevant events (i.e. test items) exists in the device memory	EUT logs are stored internally on the device and can be exported via the app.	PASS
Judgement (Verdict)	PASS	
Evidence	<pre> Hyfine2026-09-09.txt - 记事本 文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H) 2026-09-09 17:01:31.444.app main status change == true 2026-09-09 17:01:31.457.onActivityResumed:base.activity.WebViewActivity 2026-09-09 17:01:31.755.Current URL: https://app.howruf.com/web/runset/index?lang=zh&sys_code=miui 2026-09-09 17:01:31.759.canGoBack: false 2026-09-09 17:01:31.761.canGoForward: false 2026-09-09 17:01:32.953.performUnbind: false 2026-09-09 17:01:39.747.onActivityResumed:function.home.activity.MainActivity 2026-09-09 17:01:41.302.app background 2026-09-09 17:01:41.304.app main status change == false 2026-09-09 17:01:42.810.performUnbind: false 2026-09-09 17:02:01.560.performUnbind: false 2026-09-09 17:02:02.735.通知栏服务正常, 可以获取到通知信息 2026-09-09 17:02:11.227.app main status change == true 2026-09-09 17:02:11.240.onActivityResumed:function.home.activity.MainActivity 2026-09-09 17:02:12.745.performUnbind: false 2026-09-09 17:02:14.239.app background 2026-09-09 17:02:14.250.app main status change == false 2026-09-09 17:02:41.880.performUnbind: false 2026-09-09 17:02:41.912.app main status change == true 2026-09-09 17:02:41.922.onActivityResumed:function.home.activity.MainActivity 2026-09-09 17:02:43.429.performUnbind: false 2026-09-09 17:02:49.243.Ble---disconnect 2026-09-09 17:02:49.272.getWeatherInfo isNewDay: true 2026-09-09 17:02:49.343.onActivityResumed:function.home.activity.MainActivity 第 1 行, 第 1 列 100% Windows (CRLF) UTF-8 </pre>	

3.6.3 [LGM-3] Minimum number of persistently stored events

Conceptual assessment:

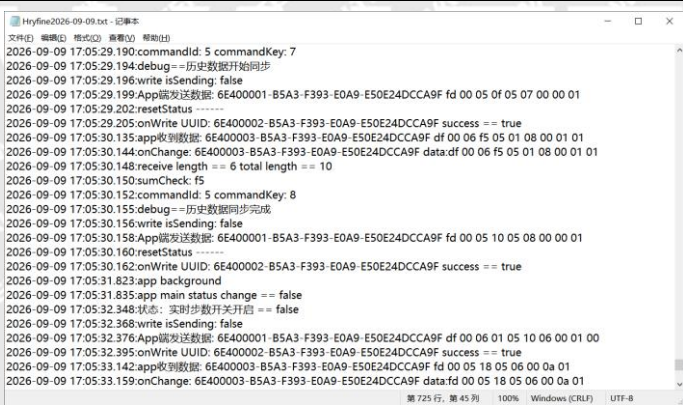
According to [E.Just.DT.LGM-3] in technical documentation, the verdict of this conceptual test is **PASS**.



Functional completeness assessment

This Functional completeness assessment is covered by the Functional sufficiency assessment of the applicability of the certification scheme. Therefore, this Functional completeness assessment is not required. Therefore the verdict of this Functional completeness assessment is **NOT APPLICABLE**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
Generates the number of logging events recorded in [E.Info.LGM-3.Quantity].	the number of logging events recorded in [E.Info.LGM-3].	PASS
The number of recorded events stored in the device persistent storage matches the number recorded in [E.Info.LGM-3.Quantity].	EUT logs are transmitted to the mobile app through log synchronization, and in theory, there is no limit on the log storage space.	PASS
Judgement (Verdict)	PASS	
Evidence		

3.6.4 [LGM-4] Time-related information of persistently stored log data

Conceptual assessment:

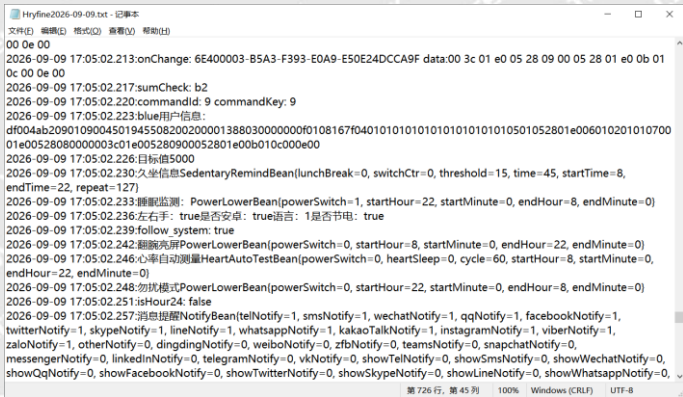
According to [E.Just.DT.LGM-4] in technical documentation, the verdict of this conceptual test is **PASS**.

Functional completeness assessment

This Functional completeness assessment is covered by the Functional sufficiency assessment of the applicability of the certification scheme. Therefore, this Functional completeness assessment is not required. Therefore the verdict of this Functional completeness assessment is **NOT APPLICABLE**.

Functional sufficiency assessment



Descriptions	Test results	Verdict
When real-time information is not available, "Log data stored continuously on the device includes time-related information recorded in [E.Info.LGM-4.LGM.Timerelated].	Log data stored continuously on the device includes time-related	PASS
Judgement (Verdict)	PASS	
Evidence		

3.7 [DLM] Deletion mechanism

3.7.1 [DLM-1] Applicability of deletion mechanisms

Conceptual assessment:

According to [E.Just.DT.DLM-1] in technical documentation, the verdict of this conceptional test is **PASS**.

Functional completeness assessment

All security assets and privacy assets accessible by entities have been recorded in [E.Info.DLM-1.PrivacyAsset] and [E.Info.DLM-1.SecurityAsset]. Therefore the verdict of this Functional completeness assessment is **PASS**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
--------------	--------------	---------



Personal information may be deleted through the deletion mechanism recorded in [E.Info.DLM-1.DLM].	The EUT app contains a factory reset function. Clicking confirm will clear all personal data.	PASS
Judgement (Verdict)	PASS	
Evidence		

3.8 [UNM] User notification mechanism

3.8.1 [UNM-1] Applicability of user notification mechanisms

Conceptual assessment:

According to [E.Just.DT.UNM-1] in technical documentation, the verdict of this conceptional test is **PASS**.

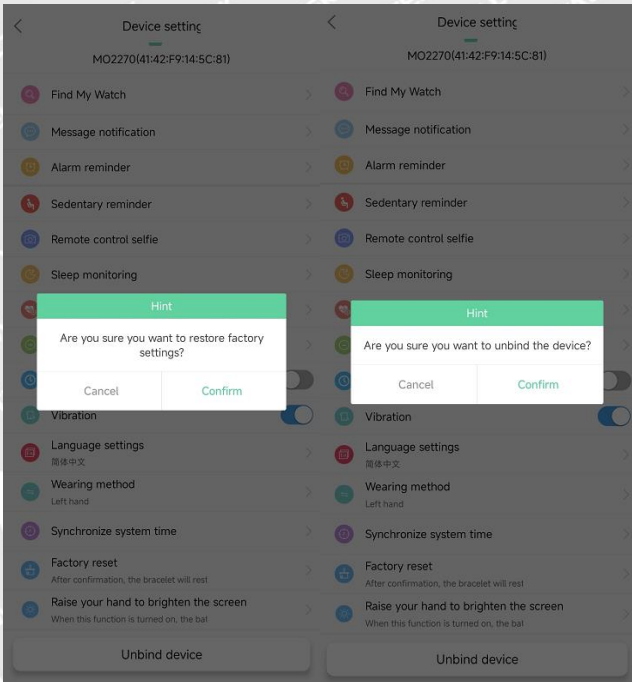
Functional completeness assessment

All security assets and privacy assets accessible by entities have been recorded in [E.Info.UNM-1]. Therefore the verdict of this Functional completeness assessment is **PASS**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
--------------	--------------	---------



This test item "Each use case documented in [E.Info.UNM-1.PersonalInformation.UseCase.Notification] has at least one user notification mechanism"	When clicking the 'Factory reset' and 'Unbind device' buttons in the app, a notification will prompt whether to confirm the operation.	PASS
Judgement (Verdict)	PASS	
Evidence		

3.8.2 [UNM-2] Appropriate user notification content

Conceptual assessment:

According to [E.Just.DT.UNM-2] in technical documentation, the verdict of this conceptional test is **PASS**.

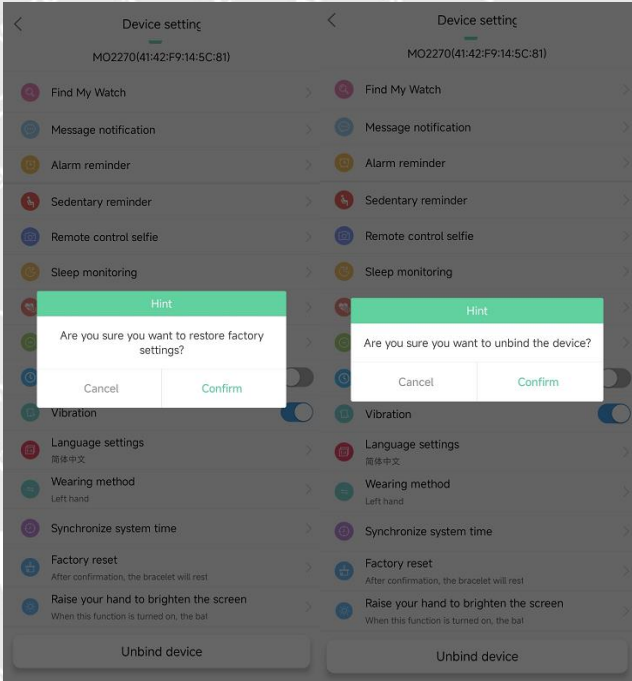
Functional completeness assessment

This Functional completeness assessment is covered by the Functional sufficiency assessment of the applicability of the certification scheme. Therefore, this Functional completeness assessment is not required. Therefore the verdict of this Functional completeness assessment is **NOT APPLICABLE**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
--------------	--------------	---------



The content of each notification for the test item is as described in [E.Info.UNM-2.Notifications.UseCase.Content]	The notification content includes a description of the changes and their impact on users.	PASS
Judgement (Verdict)	PASS	
Evidence		

3.9 [CCK] Confidential cryptographic keys

3.9.1 [CCK-1] Appropriate CCKs

Conceptual assessment:

The device does not have a pre-installed key when it leaves the factory, and the encryption key generation mechanism is not used yet. Therefore, the verdict of this conceptual test is **NOT APPLICABLE**.

Functional completeness assessment

The device does not have a pre-installed key when it leaves the factory, and the encryption key generation mechanism is not used yet. Therefore, the verdict of this conceptual test is **NOT APPLICABLE**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
--------------	--------------	---------



M/S T.



There is significant complexity surrounding the validation of cryptographic key generation mechanisms and typically they will be implemented by a third party with significant cryptographic expertise, who is unlikely to share details of such key generation processes. Given these considerations, no functional sufficiency assessment is provided for this requirement	1.The data being transferred by BLE using AES-CCM cryptography to encrypt the method by which the keys are exchange	PASS
Judgement (Verdict)	PASS	
Evidence	BLE Link key generation mechanism <pre> graph TD PIN --> E2 E2 --> LinkKey[Link Key] UnitKey[Unit key] --> LinkKey CombinationKey[Combination key] --> LinkKey MasterKey[Master key] --> LinkKey LinkKey --> E3 E3 --> EncKey[Encryption Key] LinkKey -- "For Authentication Procedure" --> AuthProc[] EncKey -- "For Encryption Procedure" --> EncProc[] </pre>	

3.9.3 [CCK-3] Preventing static default values for preinstalled CCKs

Conceptual assessment:

The device does not have a pre-installed key when it leaves the factory, and the encryption key generation mechanism is not used yet. Therefore, the verdict of this conceptual test is **NOT APPLICABLE**.

Functional completeness assessment

The device does not have a pre-installed key when it leaves the factory, and the encryption key generation mechanism is not used yet. Therefore, the verdict of this conceptual test is **NOT APPLICABLE**.

Functional sufficiency assessment



Descriptions	Test results	Verdict
comparing the CCKs and confirming that they are not the same and there is no obvious way to derive one from the other	There are no preinstalled CCKs in the EUT	NOT APPLICABLE
Judgement (Verdict)	NOT APPLICABLE	
Evidence	N/A	

3.10 [GEC] General equipment capabilities

3.10.1 [GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities

Conceptual assessment:

According to [E.Just.DT.GEC-1] in technical documentation, the verdict of this conceptional test is **PASS**.

Functional completeness assessment

All security assets and network assets accessible by entities have been recorded in [E.Info.GEC-1]. Therefore the verdict of this Functional completeness assessment is **PASS**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
--------------	--------------	---------



Measures have been taken as described in [E.Info.GEC-1.ListOfVulnerabilities] to ensure that assets cannot be affected if test items are utilized	The EUT only enables Bluetooth services. By capturing and analyzing the Bluetooth SMP pairing traffic, it is observed that the BLE device under test negotiates with the communication terminal to use the LE Secure Connections (SMP v2) security connection mechanism. Both parties complete key negotiation based on the ECDH elliptic curve algorithm. The negotiation process includes standard secure connection exchange messages such as public key exchange and DH key check. In the pairing negotiation messages, the AuthReq field simultaneously enables the Bonding flag, MITM protection flag, and Secure Connections mandatory flag. The communication link uses AES-128 encryption key length, and the protocol layer refuses to downgrade to the traditional SMP v1 pairing process. After the negotiation is complete, the device normally distributes key materials such as the IRK identity resolving key and CSRK signing key, and supports the bonding reconnection mechanism. It is determined that the EUT does not have any known publicly exploitable vulnerabilities.	PASS
Judgement (Verdict)	PASS	
Evidence		

3.10.2 [GEC-2] Limit exposure of services via related network interfaces

Conceptual assessment:



According to [E.Just.DT.GEC-2] in technical documentation, the verdict of this conceptional test is **PASS**.

Functional completeness assessment

All security assets and network assets accessible by entities have been recorded in [E.Info.GEC-2]. Therefore the verdict of this Functional completeness assessment is **PASS**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
Functionally assess whether there are further network interfaces or services (via network interfaces) exposed in factory default state, which are not listed in [E.Info.GEC-2.NetworkInterface.Exposure] or which are not required for setup according to [E.Info.GEC-2.Setup] or to operate the equipment in basic operation.	EUT only enables Bluetooth services, that is necessary.	PASS
Judgement (Verdict)	PASS	
Evidence	/	

3.10.3 [GEC-3] Configuration of optional services and the related exposed network interfaces

Conceptual assessment:

According to [E.Just.DT.GEC-3] in technical documentation, the verdict of this conceptional test is **PASS**.

Functional completeness assessment

All security assets and network assets accessible by entities have been recorded in [E.Info.GEC-3]. Therefore the verdict of this Functional completeness assessment is **PASS**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
Test items are configurable	Bluetooth is configurable.	PASS



Only authorized users can configure the [test project] settings (i.e., access control mechanisms and authentication mechanisms have been established)	The EUT can disable Bluetooth by long pressing the power off button.	PASS
Judgement (Verdict)	PASS	
Evidence		

3.10.4 [GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces

Conceptual assessment:

According to [E.Just.DT.GEC-4] in technical documentation, the verdict of this conceptional test is **PASS**.

Functional completeness assessment

All security assets and network assets accessible by entities have been recorded in [E.Info.GEC-4]. Therefore the verdict of this Functional completeness assessment is **PASS**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
--------------	--------------	---------



The EUT user documentation should describe the network interfaces and related services.	The EUT user documentation describes the Bluetooth network interface.	PASS
Judgement (Verdict)	PASS	
Evidence	interface. BPM: This interface allows you to measure the heart rate, blood pressure and blood oxygen. The results displayed on the watch and synchronized automatically in the APP. You can start the measurement from the APP. Sports: This device allows you to monitor sports activities such as running, skipping and sit-up. Message: When receiving a message, the device will vibrate and display with text, if you turn on the notification icon from APP- "Device Management" - "Reminder". Sleep Monitor: It records sleep hours with deep sleep, light sleep and awake times from wrist swing during sleep. Activate the start/end time in the APP. Weather: When connected to Bluetooth, the watch can display the weather for the day. Music: You can play or pause/go forward/backward any music track by pressing the touch button.	

3.10.5 [GEC-5] No unnecessary external interfaces

Conceptual assessment:

According to [E.Just.DT.GEC-5] in technical documentation, the verdict of this conceptional test is **PASS**.

Functional completeness assessment

All security assets and network assets accessible by entities have been recorded in [E.Info.GEC-5]. Therefore the verdict of this Functional completeness assessment is **PASS**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
Is the physical external interface necessary for the intended functionality	The physical external interfaces of the EUT are all necessary	PASS
Judgement (Verdict)	PASS	
Evidence	 1. Touch button: Press to choose mode; Long press to confirm 2. Sensor light 3. Contact for charging cable	



3.10.6 [GEC-6] Input validation

Conceptual assessment:

According to [E.Just.DT.GEC-6] in technical documentation, the verdict of this conceptional test is **PASS**.

Functional completeness assessment

All security assets and network assets accessible by entities have been recorded in [E.Info.GEC-6].Therefore the verdict of this Functional completeness assessment is **PASS**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
The test item validates the inputs as specified in [E.Info.GEC-6.ExternalInterface.Validation].	The Bluetooth interface rejects unexpected input	PASS
Judgement (Verdict)	PASS	
Evidence		

3.10.7 [GEC-7] Documentation of external sensing capabilities

**Conceptual assessment:**

According to [E.Just.DT.GEC-7] in technical documentation, the verdict of this conceptional test is **NOT APPLICABLE**.

Functional completeness assessment

There is no non-network external interfaces that may affect the privacy of users or subscribers. Therefore the verdict of this Functional completeness assessment is **NOT APPLICABLE**.

Functional sufficiency assessment

Descriptions		Test results	Verdict
None		None	NOT APPLICABLE
Judgement (Verdict)	NOT APPLICABLE		
Evidence	N/A		

3.11 [CRY] Cryptography**3.11.1 [CRY-1] Best practice cryptography****Conceptual assessment:**

According to [E.Just.DT.CRY-1] in technical documentation, the verdict of this conceptional test is **PASS**.

Functional completeness assessment

All security assets and network assets accessible by entities have been recorded in [E.Info.CRY-1]. Therefore the verdict of this Functional completeness assessment is **PASS**.

Functional sufficiency assessment

Descriptions		Test results	Verdict
Mechanisms using encryption are implemented as described, with no indication of any deviation from the documentation		1. Bluetooth connection request uses AES-CCM as the encryption algorithm	PASS
Judgement (Verdict)		PASS	

[illegible]



4. Assignment of verdict

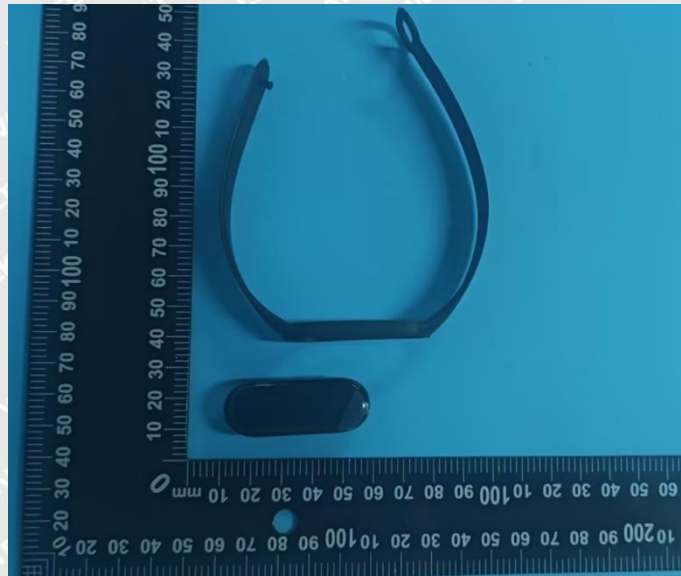
Tests may be judged as "PASS" or "FAIL" or "NOT APPLICABLE".

- If there is no evidence that the documented security mechanism has not been implemented, the judgement is "PASS";
- If there is evidence that the documented security mechanism has not been implemented, the judgement is "FAIL";
- The verdict "NOT APPLICABLE" for the assessment case is assigned otherwise.

WALTEK



Appendix I : Photos of the EUT



[END OF REPORT]