MANAMED™
5240 W. Charleston Blvd. Las Vegas Nevada 89146| P 888-508-0712 | F 949-298-3238

Cyber Security Controls for the ManaSport+ App

Specifications

Specifications of BLE Specification	***Value or value range***
Frequency band	2.4GHz ISM (2.40000 – 2.4835GHz)
On-air data rate	250 kbps, 1 Mbps or 2 Mbps
Modulation	GFSK
Output power	Programmable: +4 to -20dBm in 4dB steps
Sensitivity	-93dBm Bluetooth low energy -96dBm at 250kb -90dBm at 1Mbs -85dBm at 2Mbs
Radio current consumption LDO at 1.8V	16mA – TX at +4dBM output power 10.5mA – TX at 0dBm output power 13mA – RX at 1Mbs
Radio current consumption DC-DC at 3V	10.5mA – TX at +4dBm output power 8.06mA – TX at 0dBm output power 9.7mA – RX at 1Mbs
Bluetooth version	V4.2 LE
Bluetooth class	Class 2
Operating range	10 m
Number of Channels	40
FCC compliance	47 CFR, Part 15
FCC ID	2ANDXXXXX
Cybersecurity compliance	BLE connection can adopt pairing encryption connection and AES-128 algorithm for encryption. During the pairing process, the master and slave keep multiple keys: STK, LTK, IRK and CSRK; STK / LTK is mainly used for data encryption during transmission; Irk is mainly used for device authentication; CSRK is mainly used for message signature and verification; The use of multiple keys and CRC verification ensure the encryption and accuracy of BLE data transmission

Interference Robustness	Adaptive frequency hopping, Lazy Acknowledgement, 32-bit message integrity check using packet checksum
Antenna type	PCB antenna

Data Integrity

Design requirements for database integrity:

The database used by the product in the Android system adopts the GreenDao database, which is internally encrypted, and the database is processed by android-database-sqlcipher. When the database is introduced into the project, it only needs to configure the android-database-sqlcipher library and encrypt the database by setting the encrypted key;

IOS uses the WCDBS database, which is encrypted based on SQLCipher's database. The encryption method is enabled through setCipher, and the encryption stored in the database is encrypted by setting the encryption secret key.

Data integrity design requirements during data transmission:

In the process of BLE encrypted data transmission, STK or LTK is used as the key, AED128 algorithm is used to encrypt the transmitted data, and then 32bit message integrity verification and 24bit CRC verification are included. The receiver uses the same key for verification and decryption to ensure the integrity and accuracy of the data.

Non-invasive ultrasound device also complies with the BLE 4.2 protocol, and its data integrity is validated during transmission.

Data latency or throughput

We used BLEcommunication technology that can be used to communicate with smartphones. Through BLEcommunication, the APP can get the usage records data of Non-invasive ultrasound device and control Non-invasive ultrasound device. **BLEperformance (i.e., Quality of Service) including adequate bandwidth, controlled delay, throughput and reliability,** the loss of quality of service will creates an inconvenience only and does not affect operation and usage records of the product.

After the APPtransmitscommand to Non-invasive ultrasound device, the Non-invasive ultrasound device shall execute within 200ms.

The required data throughput is assessed as follows: the each data (such as ausage record) transmission does not exceed **20** bytes. The record of a complete data transmission normally does not exceed **20** bytes. For a BLE network with 1 Mb/s data throughput capacity, it can transmit more than 1000 measurement records per second, which is sufficient.

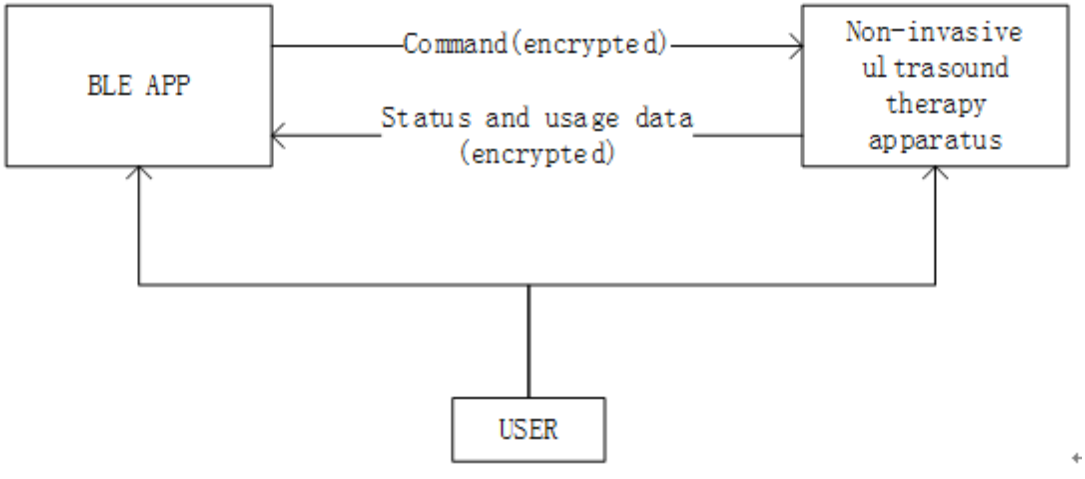
Moreover, even if some random wireless RF sources (e.g., electromagnetic security systems) in the vicinity of the device causes interruptions or failure in BLE transmission, in this case Non-invasive ultrasound device app will not function, but the working of Non-invasive ultrasound device will not be affected.

Cybersecurity

General description

The user can directly control the Non-invasive ultrasound device output ultrasonic, and check the ultrasonic output status and usage record from the Non-inv
asive ultrasound device; Non-invasive ultrasound devicecan be used without mobile controls, the smart phone APP is just an alternate way to increase the control and display of the Non-invasive ultrasound device. Therefore, the BLE function of Non-invasive ultrasound device is classified as a device with negligible Cybersecurity Risk (Category D). The delayed, disrupted, or lost data will result at most as an inconvenience to patients but with no risk to patients safety.
The objective of this section is to address the risks associated with vulnerabilities of the Non-invasive ultrasound device and demonstrate the cybersecurity controls considered in the design.
The ManaSport provides non-invasive therapy of low-intensity pulsed ultrasound for the treatment of selected sub-chronic and chronic medical conditions such as soft tissue injuries, shortened tendons due to past injuries and scar tissues, relief of pain, muscle spasms and joint contractures. The essential performance of Non-invasive ultrasound device is output 595mW ultrasound.

The network diagram and data flowchart are displayed on Figure 1.



Cybersecurity Risks and Controls

- Table Next Page -

Table 3 Cybersecurity risks **No.**	**Risk description**	**Harm scenarios**
H16-1	unauthorized access	The APP is operated by unauthorized user. Unauthorized access to the database / the user's usage data may be disclosed, unauthorized users may tamper with patient data / wrong judgement of historical data
H16-2	Unauthorized BLEconnection	The device is connected to unauthenticated APP / the user's historical data may be disclosed / wrong judgement of usage data
H16-3	Loss of data integrity	The loss of data integrity during data transmission/ get the wrong data on APP,fail to use the APP/ user unsatisfied
H16-4	Confidential leaks during BLE data transmission	Data leakage occurs during the transmission of command or data / the user's usage data may be disclosed or fail to use the APP/ user unsatisfied
H16-5	Wireless Coexistence	use the BLEfunction in the radio frequency (RF) field / BLE communication is interrupted / user unsatisfied
H16-6	Integrity of database data	The data stored in the database loss integrity/ the user refer to wrong historical data/ user unsatisfied
H16-7	Cybersecurity Vulnerabilities (Replay attack)	The third-party equipment may obtain the transmission information of the normal communication between the Non-invasive ultrasound device and the app./ Without understanding the detailed meaning, it may resend the same information for many times, which may make the

		Non-invasive ultrasound device run abnormally/ user unsatisfied

Table 4 Cybersecurity risk controls

No.	Item	Technical details of risk control measures
C16-1	unauthorized access	The login password and user ID are designed so that users can only use their own ID and password to log in. ID and password are commonly used security means for mobile App. Cracking ID and password requires very professional technology. Therefore, control is sufficient.
C16-2	Unauthorized BLEconnection	There is only a short pairing window after the device is turned on, and once connected, it cannot connect to other smart phone; if want to connect other smart phone, must be disconnected from the existing connection
C16-3	Loss of data integrity	When the APP issues an instruction, the Non-invasive ultrasound device must pass the verification completely after receiving the numerical instruction, and check its legality. Details are as follows： The integrity of BLE data depends on two aspects： 1.Verification of Bluetooth underlying transmission （1）The encrypted message format of Bluetooth transmission is： Preamble + access address + header + length + payload data + message integrity check (MIC) + CRC check （2）Data encryption and decryption process Bluetooth bottom layer encrypts "payload data" and "Message Integrity Check", and the header and length are not encrypted. The Bluetooth bottom layer takes the connected shared key as the key and uses AES-128 algorithm to encrypt a 128 bit plaintext block (the plaintext block contains packet counter, direction bit, initialization vector, etc.) to form a ciphertext block. Then the ciphertext block is XOR（⊕）with the payload data to be sent, and then the encrypted payload and MIC verification are generated.

		Because the receiver has the same shared key, packet counter, direction bit, initialization vector, etc. as the sender, the MIC verification value can be calculated in the same way. If the calculated MIC is inconsistent with the received MIC, the connection will be disconnected immediately; If the MIC is consistent, the payload data is decrypted in the same way. （3）CRC verification The CRC generation polynomial is： CRC_x=X24+X10+X9+X6+X4+X3+X1+X0 Multiply the "value to be verified" by X24 and divide it by the CRC_x value in the above equation. The remainder is the final CRC verification value. The receiver calculates the CRC verification value in the same way. If it is inconsistent with the received CRC verification value, the packet will be rejected and wait for re-transmission. 2,Verification of application protocols （1）The transmission data of the application program is the payload data in the Bluetooth data message. Its format is： CMD+length+data+checksum （2）The sum of CMD + length + data, and the last 8 digits of the sum value are taken as the checksum. The receiver will calculate the checksum. If it is inconsistent with the received checksum, it will reject the packet and wait for re-transmission. Cracking the dual verification of Bluetooth underlying transmission verification and application protocol verification requires very professional technology. Therefore, control is sufficient.
C16-4	Confidential leaks during BLE data transmission	The “Checkout of Bluetooth underlying transmission” is added during communication to consolidate data security. Details as follows： Verification of Bluetooth underlying transmission （1）The encrypted message format of Bluetooth transmission is： Preamble + access address + header + length + payload data + message integrity check (MIC) + CRC check （2）Data encryption and decryption process

		Bluetooth bottom layer encrypts "payload data" and "Message Integrity Check", and the header and length are not encrypted. The Bluetooth bottom layer takes the connected shared key as the key and uses AES-128 algorithm to encrypt a 128 bit plaintext block (the plaintext block contains packet counter, direction bit, initialization vector, etc.) to form a ciphertext block. Then the ciphertext block is XOR（⊕）with the payload data to be sent, and then the encrypted payload and MIC verification are generated. Because the receiver has the same shared key, packet counter, direction bit, initialization vector, etc. as the sender, the MIC verification value can be calculated in the same way. If the calculated MIC is inconsistent with the received MIC, the connection will be disconnected immediately; If the MIC is consistent, the payload data is decrypted in the same way. （3）CRC verification The CRC generation polynomial is： CRC_x=X24+X10+X9+X6+X4+X3+X1+X0 Multiply the "value to be verified" by X24 and divide it by the CRC_x value in the above equation. The remainder is the final CRC verification value. The receiver calculates the CRC verification value in the same way. If it is inconsistent with the received CRC verification value, the packet will be rejected and wait for re-transmission. Cracking the dual verification of Bluetooth underlying transmission verification and application protocol verification requires very professional technology. Therefore, control is sufficient.
C16-5	Wireless Coexistence	adopts adaptive frequency hopping for Bluetoothconnection, it can effectively alleviates the wireless interference in the same frequency band： BLE low-power Bluetooth communicates in the 2.4G frequency band, in which the communication frequency band is divided into 40 channels, excluding the 3 channels used for broadcasting, and 37 channels are used for normal data transmission. In order to ensure that the communication is not interfered as much as possible, in the initial stage of connection, the master and slave sides save the frequency hopping interval value "hop". After each data

		transmission, the channel used in the next data transmission will skip "hop" channels and cycle in turn, so that different channels are used for different times of data transmission.
C16-6	Integrity of database data	In the App, the database is encrypted. The data stored in the data table is encrypted data. Details as follows： The APP program will judge the legitimacy of the instruction to prevent the operation of suspicious instructions. Meanwhile, the data stored in the database of app is encrypted data. Details as follows： 1、The APP program sets up rules and thresholds for the instructions. In case of suspicious instruction(s), the device will refuse to execute the instruction. Allcommandsreceived by Non-invasive ultrasound device during normal communication shall be judged to ensure that they are legal and not out of scope, so as to avoid unexpected and unreliable operation. Therefore, when receiving an illegal instruction ,APP will refuse to execute the relevant instruction . Android uses the GreenDao database and IOS uses the WCDB database, which is internally encrypted by SHA256 hash. Each time data is stored, a hash value will be generated and stored; When fetching data, the hash value of the data will be recalculated and verified to confirm that the database has not been maliciously modified App program judges the received instructions and encrypts the data when storing it. It is a very effective measure to protect database integrity. Therefore, control is sufficient.
C16-7	Cybersecurity Vulnerabilities (Replay attack)	Adopt the BLEunderlying protocol and AES-128 encryption Details are as follows： BLEunderlying protocol has taken this risk into account. The "packet counter" is included in the transmission data, and the packet counter value of the next packet will be accumulated, no identical instructions will appear. If the receiver verifies that the packet counter is incorrect, the packet data will be discarded. And because AES-128 encryption is used, the third-party device does not know the key, so it is

		difficult to crack the data information. Besides,the instructions with the same packet counter value will be discarded by BLE underlying protocol. Therefore, control is sufficient.

Software Integrity, Software updates

Method of Updating Bluetooth app of Non-invasive ultrasound device

Because the user's registered ID numbers are in email format, when the app has a new version, we will notify each user by email. After receiving the email, the user can download and install the app again in Apple App store or Google play.

For new versions of software, the manufacturer will put them into the APP stores, to ensure the integrity of the software.

The latest version of this app is V1.0.

Describe the process by which the security updates and patches will be identified and carried out over the lifetime of the device:

After the software is released, the feedback and abnormal problems will be continuously monitored according to the software maintenance plan. Briefly, when a problem is detected, it is determined whether software update is needed through the systematic review. When the software is updated, the software has to undergo relevant regression tests. When Non-invasive ultrasound device app software is to be updated, users should be notified by send out the E-mail.

Recommended cybersecurity controls.

Bluetooth App is installed only from a trusted source (i.e., Apple App Store and Google Play). The details cybersecurity controls measure see Table 4 Cybersecurity risk controls.