vi. Actual values of PIN, MITM, IOTYPE are displayed as per the current settings of device.
vii. Response to the settings command varies as per the device, e.g. for LM068/LM074 modules it includes MODEM command

4.3 UART Settings commands:

4.3.1 “AT*BAUD”\r\n

i. Query and set command
ii. Baud rate query: “AT*BAUD=?”\r\n
iii. Baud rate query report: “REP”:BAUD=19200(2)”. Number in curly brackets shows the serial number as per below table.
iv. Baud rate set command: “AT*BAUD=3” (Set Module baud rate as 38400 bps)
v. Module need to not to perform power-on-off after change of baud rate setting
vi. Refer below table for baud rate settings:

Sr No	Actual baud rate	LM951 / LM961 baud rate code	Report from LM961
1	9600	1	“REP”:BAUD=9600(1) ”
2	19200	2 – Default baud rate	“REP”:BAUD=19200(2)”
3	38400	3	“REP”:BAUD=38400(3) ”
4	57600	4	“REP”:BAUD=57600(4)”
5	115200	5	“REP”:BAUD=115200(5)”
6	230400	6	“REP”:BAUD=230400(6)”
7	460800	7	“REP”:BAUD=460800(7)”
8	921600	8	“REP”:BAUD=921600(8)”
9	1382400	9	“REP”:BAUD=1382400(9)”

4.3.2 "AT*PAR"\r\n

i. Query and set command
ii. Parity query command: "AT*PAR=?"\r\n
iii. Parity query report: "REP*:PARITY=None(0)" (Module uses default parity , parity = none). Number in curly brackets shows the serial number as per below table.
iv. Parity set command: "AT*PAR=1" (Set Module parity as odd)
v. Module need to not to perform power-on-off after change of parity setting.
vi. Refer below table for parity settings:

Sr No	Actual parity	LM951 / LM961 parity code	Report from LM961
1	Parity None	0 – default parity	"REP*:PARITY=None(0)"
2	Parity odd	1	"REP*:PARITY=Odd(1)"
3	Parity even	2	"REP*:PARITY=Even(2)"

4.3.3 "AT*STOP"\r\n

i. Query and set command
ii. Stop bit query command: "AT*STOP=?"\r\n
iii. Stop bit query report: "REP*:STOP=Stop_One(0)" (module uses default stop bit as = one). Number in curly brackets shows the serial number as per below table.
iv. Stop bit set command: "AT*STOP=1" (Set module stop bit as two)
v. Module need not to perform power-on-off after change of parity setting.
vi. Refer below table for stop bit settings:

Sr No	Actual Stop bit	LM951 / LM961 Stop bit code	Report from LM961
1	Stop bit One	0 – default stop bit	"REP*:STOP=Stop_One(0)"
2	Stop bit two	1	"REP*:STOP=Stop_Two(1)"

4.3.4 "AT*FLOW"\r\n

i. Query and set command
ii. Flow control query command: "AT*FLOW=?"\r\n
iii. Flow control query report: "REP*:FLOW=OFF" (module uses default flow control OFF)
iv. Flow control set command: "AT*FLOW=ON" (Set module flow control ON)
v. If the user is changing the flow control of device, after accepting command with OK response, module shows report as "REP*:FLOW_CHANGE=IN_Progress"
vi. Module will perform reboot in changed flow control mode

vii. If module is in flow control OFF mode and user gives command to make the flow control OFF, then module will respond as OK but shall not perform reboot. Similar applies to flow control OFF setting.

4.3.5 "AT*CTS"\r\n:

i. Query command
ii. CTS query command: "AT*CTS=?"\r\n
iii. CTS query report: module will report the actual status of CTS line e.g "REP*:CTS=OFF" or "REP*:CTS=OFF".
iv. CTS line cannot be set/reset.
v. This command is applicable to LM074 module and LM068 adapter

4.3.6 "AT*DSR"\r\n:

i. Query command
ii. DSR query command: "AT*DSR=?"\r\n
iii. DSR query report: module will report the actual status of DSR line e.g "REP*:DSR=OFF" or "REP*:DSR=OFF".
iv. DSR line cannot be set/reset
v. This command is applicable to LM074 module and LM068 adapter

4.3.7 "AT*RTS"\r\n:

i. Set only command
ii. RTS line set/reset command: "AT*RTS=ON"\r\n or "AT*RTS=OFF"\r\n.
iii. RTS line cannot be queried.
iv. This command is applicable for LM074 module and LM068 adapter.

4.3.8 "AT*DTR"\r\n:

i. Set only command
ii. DTR line set/reset command: "AT*DTR=ON"\r\n or "AT*DTR=OFF"\r\n.
iii. DTR line cannot be queried.
iv. This command is applicable to LM074 module and LM068 adapter

4.3.9 "AT*MODEM"\r\n:

i. Query and set command
ii. MODEM query command: "AT*MODEM=?"\r\n
iii. MODEM query report: "REP*:MODEM=NONE" (module uses default MODEM settings as "none")
iv. MODEM set command: "AT*MODEM=LOCAL" or "AT*MODEM=Remote"
v. Refer below table for MODEM settings:

Sr No	Modem setting	Comment
1	None	Default setting

2	Local	LM068/LM074 uses RTS/CTS and DTR/DSR in loopback mode
3	Remote	When LM068/LM074 is connected to remote device, LM068/LM074 sends RTS /DTR line status to remote device and receives CTS/DSR line status from remote device

vi. Modem settings LOCAL and REMOTE are followed when Flow-control is off
vii. MODEM command is applicable for LM074 module and LM068 adapter.

4.4 Bluetooth Security Settings commands:

4.4.1 "AT+PIN"\r\n

i. Query and set command
ii. PIN query command: "AT+PIN=?"\r\n
iii. PIN query report: "REP:PIN=1234" (module uses default PIN as 1234)
iv. PIN set command: "AT+PIN=00112233" or "AT+PIN=Abcd"
v. Maximum PIN length supported is as per BT2.1 standard i.e. 16 bytes. PIN string can be numeric only, alpha only, or alpha numeric.
vi. Examples for valid PIN set commands: "AT+PIN=0011223344556677 8" or "AT+PIN=001122aaBBccDDeef"

4.4.2 "AT+DPIN"\r\n

i. Query and set command
ii. Dynamic PIN query command: "AT+DPIN=?"\r\n
iii. Dynamic PIN query report: "REP:DPIN=OFF" (module uses default DPIN as off)
iv. Dynamic PIN set enable or disable command: "AT+DPIN=ON" or "AT+DPIN=off".
v. When module has DPIN setting as OFF, Module uses a fixed PIN provided default as 1234.
vi. When module has DPIN setting as ON, module expects the dynamic PIN from customer as per the MITM and IO-Type settings.
vii. For further on BT2.1 pairing and MITM, DPIN, PASSKEY messages refer "LM951/LM961 Pairing document".

4.4.3 "AT+MITM"\r\n

i. Query and set command
ii. (Man IN The Middle) MITM query command: "AT+MITM=?"\r\n
iii. MITM query report: "REP:MITM=OFF" (module uses default MITM as off)

iv. MITM set enable or disable command: "AT+MITM=ON" or "AT+MITM=off"

4.4.4 "AT+IOTYPE"\r\n

i. Query and set command
ii. (Input Output type for Dynamic PIN) IOTYPE query command: "AT+IOTYPE=?"\r\n
iii. IOTYPE query report: "REP:IOTYPE=NO_InOut" (module uses default IOTYPE as "no input output")
iv. IOTYPE modify command: "AT+IOTYPE=KB_ONLY" or "AT+IOTYPE=KB_OnLy".
v. Following IO-types are supported:

Sr No	IO type	LM951 / LM961 String for IOTYPE	LM951/LM961 IOTYPE set command	LM951/LM961 IOTYPE query response
1	No Input output	NO_InOut	at+iotype=no_inout	REP:IOTYPE=NO_InOut
2	Key Board only	KB_Only	at+iotype=Kb_OnLy	REP:IOTYPE=KB_Only
3	Display only	Disp_Only	at+iotype=DISP_only	REP:IOTYPE=Disp_Only
4	Display and confirmation for Yes / No	Disp_YN	at+iotype=DISP_YN	REP:IOTYPE=Disp_YN

4.4.5 "AT+DEL"\r\n

i. Execution only command.
ii. User issues this command to delete the device from its paired list.
iii. DEL command: "AT+del=00126f357215"\r\n
iv. "OK" response will be provided if the string entered has valid BT address. Module deletes the device from its pairing list.
v. "Err" response will be provided if invalid BT address, invalid length of address is provided.
vi. If device is deleted form the pairing list. Module will follow pairing procedure before getting connected with the device.

4.4.6 "AT+PASSKEY"\r\n

i. Execution only command.
ii. When the module has DPIN=ON, MITM=ON and IOTYPE as Keyboard Only, in pairing procedure module gives indication "IND:PASSKEY=?".
iii. User shall provide the pass key in following format: "AT+PASSKEY=1234"\r\n .

iv. Any integer within the range uint32 is considered as valid Passkey

4.4.7 "AT*PASSCFM"\r\n

i. Execution only command.
ii. When the module has DPIN=ON, MITM=ON and IOTYPE as DISPLAY confirmation Yes/No, in pairing procedure module gives indication "IND*:PASSK=xxxxxx".
iii. User shall provide the confirmation for pass key in following format: "at*passcfm=00126f357215,Yes"\r\n or "at*passcfm=00126f357215,no"\r\n

4.4.8 "AT*STOPPAIR"\r\n

i. Execution only command.
ii. Used to stop the pairing procedure for a device
iii. Once the module starts pairing procedure, the stack completes the procedure within maximum 90 seconds. User can stop the pairing procedure within this time.
iv. Issue command to stop the pairing procedure with the BT address of the peer device e.g. "AT*stoppair=00126f357215"

4.4.9 "AT*PAIRLIST"\r\n

i. Query only command
ii. Pairlist query command: "AT*PAIRLIST=?"\r\n
iii. Pairlist report may be multiple line if module is paired with more than one device. Paired devices report is shown in following format

```
"REP*:PAIRLIST=00126f357201,
REP*:PAIRLIST=00126f357215,
REP*:PAIRLIST=END"
```

iv. Pairlist report can be multiple line, to indicate end of the report "REP*:PAIRLIST=END" is displayed at end.

4.5 SPP Related commands:

4.5.1 "AT*FIND"\r\n

i. Execution only command.
ii. Used to start the discovery of Bluetooth devices nearby.
iii. Start discovery command format is "AT*FIND=ON"\r\n
iv. Stop discovery of Bluetooth devices by command "AT*FIND=OFF"\r\n.
v. Module shows discovered devices with their name and addresses. Each device is reported as soon as it is discovered
vi. Report for each device is sent with new line. To indicate the end of the discovery report, "REP*:FIND=END" message is shown.
vii. If module did not get reply to name query of remote device it will display NULL in name string (e.g. row 3 in below report).
viii. Example report for discovery:

```
"at*find=onat*find=on
```

```
OK
REP*:FIND=Start
 =1 0002-5b-00a5a5  Serial Adapter
 =2 0026-4a-a19172  LML11
 =3 442a-60-da6c58 NULL
 =4 4c49-e3-68b246  Red minote
REP*:FIND_END= 4 devices found."
```

4.5.2 "AT*ROLE"\r\n

i. Query and Set command.
ii. Query command – "AT*ROLE=?"\r\n
iii. Report for SPP role query is "REP*:SPPRole=SLAVE"\r\n . Default role is Slave mode supporting SPP incoming connections.

Sr No	SPP Role	LM951/LM961 Role set command	LM951/LM961 Role query response
1	Dual role (SPP Slave and SPP master role)	At*role=dual	REP*:SPPRole=DUAL
2	SPP Slave Only	At*role=slave	REP*:SPPRole=SLAVE
3	SPP Master only	At*role=master	REP*:SPPRole=MASTER

iv. When the module is in Dual mode, it can accept incoming SPP connection as well as initiate outgoing SPP connection whereas module cannot accept or initiate new connection when it is already connected to any remote device. E.g if module has established an outgoing connection, then after terminating the outgoing connection it can accept incoming connection.
v. In slave-only role
   1. BOND=Valid-BD-address. (e.g. BOND=0012-6f-357215)
      - Module will accept connection request only from bonded device. Connection requests from other devices will be rejected by module.
   2. BOND=0000-00-000000.
      - Module will accept connection request from any device
vi. In master-only role, Refer ACON and BOND command for more details.
vii. In any role (dual, Slave only or Master only role) module can support only one connection at an instance.

4.5.3 "AT*ACON"\r\n

i. Query and set command.
ii. This setting is applicable for Master only role.
iii. Auto connect query command: "AT*ACON=?"\r\n
iv. Auto connect query report: "REP*:ACON=OFF"
v. Command to set ACON as ON is "AT*ACON=ON"\r\n
vi. When the module is in Master-only role and ACON setting is ON,
   1. BOND=Valid-BD-address. (e.g. BOND=0012-6f-357215)

- If device has valid address for BOND, it keeps issuing connection request to that device till the connection is established

2 BOND=0000-00-000000.

- If device has BOND address as Zero, it will start discovery of nearby Bluetooth devices and issues connection request to first found device.

vii. When module is in Master-only role and ACON setting is OFF, module will wait for AT command from user to initiate the connection request (module will not accept any incoming connection request).

4.5.4 "AT*BOND"\r\n

i. Query and set command

ii. Set command: "AT*BOND=00126f357215"\r\n. Device will establish connection only with remote device having BD address as 00126f357215.

iii. Set command: "AT*BOND=000000000000"\r\n. Device will establish connection with any device.

iv.

v. This setting is applicable for Master-only, slave-only role. When Bond Address setting holds a valid Bluetooth address then LM068/LM074/LM961 will establish connection only with that device.

vi. LM068/LM074/LM961 can be paired with maximum 8 devices and stores the device addresses in its permanent memory (this is called as TDL-Trusted_Devices_List or PDL-Paired_Devices_List) whereas it can be bonded to only one device at a time whose address is mentioned in BOND command setting.

vii. Bond device address query command: "AT*BOND=?"\r\n.

viii. Default settings is: "REP*:BOND=0000-00-000000".

ix. Setting for default bond device address is Zero i.e. device is not bonded to any remote device and can accept or issue connection request to any remote device

x. Command to set ACON as ON is "AT*ACON=ON"\r\n.

xi. When the module is in Master only role and ACON setting is ON, module performs the discovery of nearby devices and tries to connect with the first found device for SPP connection.

4.5.5 "AT*CONN"\r\n

i. Execution only command.

ii. Supported in SPP Master-only and Dual mode

iii. If module is MASTER role and ACON setting is ON, the module will always respond to this command as "ERR" as it only issues a connection request to BOND device, or it performs discovery on its own and attempts to connect to first device found.

iv. User can start to initiate outgoing SPP connection.

v. Outgoing connection command: "AT*conn=00126f357215"\r\n

vi. "OK" response will be provided if the string entered has valid BT address, module is not connected to any device.

vii. "Err" response will be provided if invalid BT address, invalid length of address is provided or if the module is already in connected state

viii. After module gives OK response to at+conn command, it starts the connection procedure. Result of connection procedure is indicated as indication message.

   1. "IND*:CONN_FAILURE=00126f357215" message is shown to indicate the failure in connection with BD address 0012-6f-357215.
   2. "IND*:CONNECTED=00126f357215" message is shown to indicate the SPP connection is successfully established and the devices are in connected state.
   3. Once the devices are connected, LM951/LM961 is in **SPP-connected-online-data** mode. Every string entered by host on UART is treated as data and is transmitted to connected device.
   4. User can come out of this mode by entering the Escape sequence

4.5.6 Escape sequence "+++"

i. Execution only command/sequence.

ii. Supported only in **SPP-connected-online-data** mode.

iii. User issues this command to enter in **SPP-connected-online-command** mode.

iv. If the user issues escape sequence in SPP-connected-online-data when LED D10 is Blinking, OK response is given by module and module enters in **SPP-connected-online-command** mode.

v. Once the module enters in SPP-connected-online-command mode, any strings entered on UART are considered as AT commands and are processed by module (still the module is in connected state).

vi. In SPP-connected-online-command mode, users can query/update module settings and start the disconnection by issuing at*drop command

4.5.7 "AT*AUTO"\r\n

i. Execution only command/sequence

ii. Supported only in **SPP-connected-online-command** mode.

iii. User issues this command to enter back in **SPP-connected-online-data** mode.

iv. After entering in SPP-connected-online-data mode, any data entered on UART is transmitted to the remote device over Bluetooth.

4.5.8 "AT*DROP"\r\n

i. Execution only command.
ii. Supported in all SPP roles (dual, master-only or slave-only).
iii. User issues this command in SPP-connected-online-command mode to terminate the existing SPP connection (applicable for existing incoming or outgoing SPP connection).
iv. connection termination command: e.g. "AT*DROP=00126f357215"\r\n
v. "OK" response will be provided if the string entered has valid BT address and module is connected to the device with entered BT address and module is in online-command mode.
vi. "Err" response will be provided if invalid BT address, invalid length of address is provided, module is not connected to any device.
vii. AT*drop command causes the indication message to indicate the devices are successfully disconnected.
viii. "IND*:DISCONNECTED=00126f357215" indication message is shown to indicate the module is disconnected from the device with BT address 0012-6f-357215.

4.6 Firmware Upgrade commands:

4.6.1 "AT*UPGRADE"\r\n

i. Execution only command.
ii. Supported in all SPP roles (dual, master-only or slave-only).
iii. The module should not be connected to BLE or any Bluetooth device before starting the procedure.
iv. User issues this command in **SPP-connected-online-command** mode to perform the OTA-firmware-upgrade.
v. User shall enter this command with password provided for firmware upgrade. If the password is correct, then module issues OK response and is ready for performing firmware upgrade.

5. LM961 Over The Air Firmware Upgrade Procedure

This section describes the procedure to perform an over the air firmware upgrade for the LM961 module.

Users can use serial terminals like Hercules, HyperTerminal, Tera term or Putty etc. for serial communication with LM961 module.

In this document, the term "new image" refers to the firmware image to which the LM961 will be upgraded to.

The LM961 receives the new image from a peer device which is connected to itself with Bluetooth.

The LM961 can receive new images over SPP profile only. The module does not support other Bluetooth profiles to receive a new image.

5.1 Pre-requisites for Firmware upgrade:

5.1.1 New Firmware image:

i. New Firmware image is provided as "xxxxxxx.bin" file to user.
ii. User shall store this image on PC/Laptop/device used to connect to the LM961 module for OTA upgrade.
iii. LM961 module can be upgraded with the image provided by LM Technologies only.

5.1.2 Peer Bluetooth device requirements:

i. Peer Bluetooth device should support sending file over SPP profile (some mobile applications may not support this).
ii. LM technologies has tested LM048/LM058 or LM961 module to send the new image with Hercules utility from windows PC.
iii. Peer device should support pairing requirements.
iv. LM961 will connect only with Paired device hence receives image only from paired device.

5.1.3 Pairing and Authentication of Peer device:

i. LM961 can pair with remote device with fixed PIN.
ii. LM961 can pair with remote device with dynamic PIN and MITM protection enabled.
iii. For detailed pairing procedure of LM961 with AT commands, please refer document "LM961 module Pairing procedure R1.0.pdf"

5.1.4 LM961 requirements:

- LM961 can be SPP master (initiate connection with remote device) or SPP Slave (Accept connection request from remote device)

5.2 Firmware upgrade procedure Flow chart:

The flow chart below illustrates the firmware upgrade procedure, highlighting messages when the upgrade operation is successful.

The comments show the failure points as FP1 to FP5.
The cause of failure points and actions to overcome them are discussed in the subsequent section.

Note: During the upgrade procedure, after the module displays the message "Ready to receive OTA file", if the user fails to send the image to the LM961 module, the module/user cannot terminate the OTA mode. The user has to provide power-on/off cycle to come out of OTA upgrade mode. Another way to come out of this mode; the remote connected device has to send at-least 200 bytes of data. The module will treat this data as an upgrade image but due to failure it will reboot itself with existing firmware

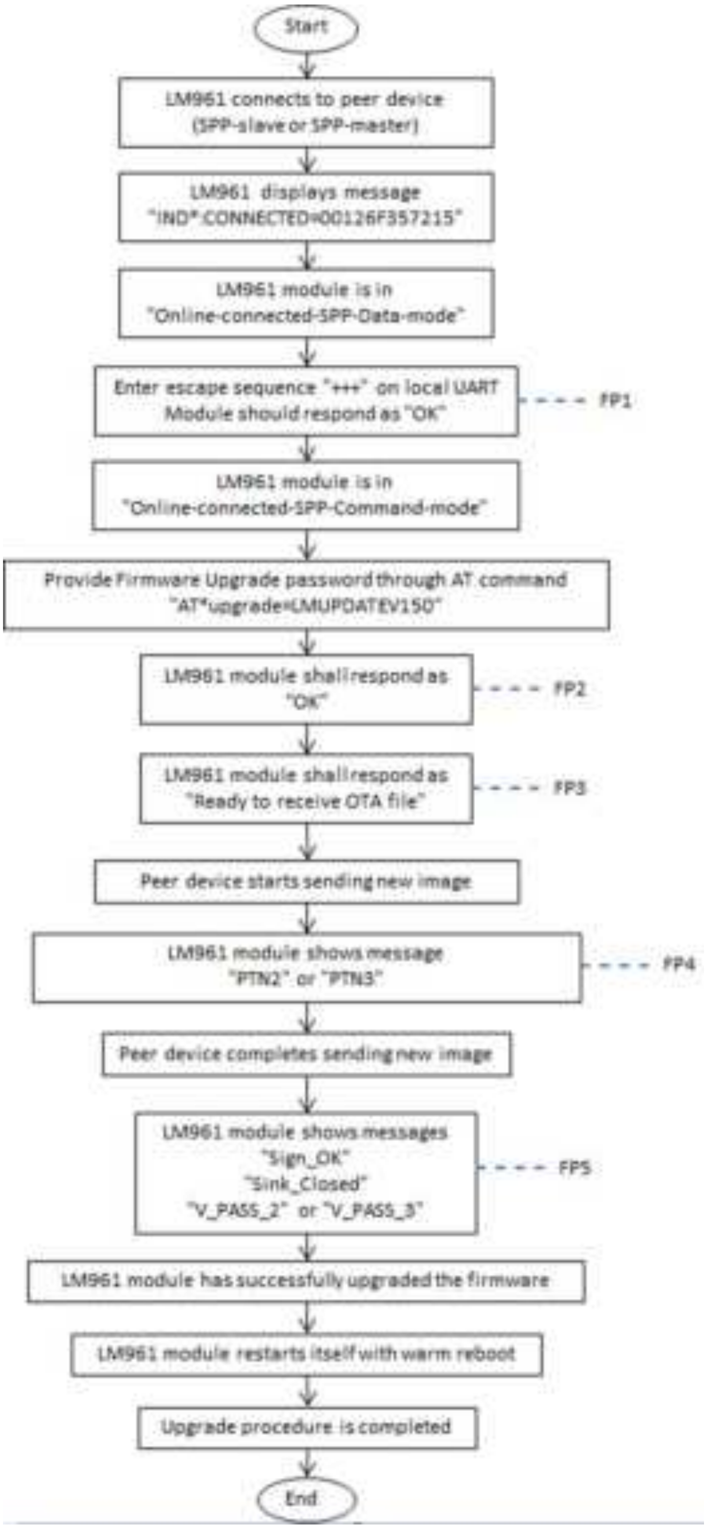

Start
LM961 connects to peer device
(SPP-slave or SPP-master)
LM961 displays message
"IND*:CONNECTED=00126F357215"
LM961 module is in
"Online-connected-SPP-Data-mode"
Enter escape sequence "+++" on local UART
Module should respond as "OK"
FP1
LM961 module is in
"Online-connected-SPP-Command-mode"
Provide Firmware Upgrade password through AT command
"AT*upgrade=LMUPDATEV150"
LM961 module shall respond as
"OK"
FP2
LM961 module shall respond as
"Ready to receive OTA file"
FP3
Peer device starts sending new image
LM961 module shows message
"PTN2" or "PTN3"
FP4
Peer device completes sending new image
LM961 module shows messages
"Sign_OK"
"Sink_Closed"
"V_PASS_2" or "V_PASS_3"
FP5
LM961 module has successfully upgraded the firmware
LM961 module restarts itself with warm reboot
Upgrade procedure is completed
End

Figure 1: Firmware Upgrade Flowchart

Note: The firmware upgrade password is dependent on the current firmware version

5.3 Possible Failure points and corrective actions

The following section describes the possible failure points while performing an Over the Air firmware upgrade. It also covers possible reasons for errors what a user can do to correct them.

5.3.1 Failure point 1:

i. After entering the escape sequence "+++", the module should respond as OK and enter in Online-connected-command-mode.
ii. If module does not respond as "OK" (it will not reply as "ERR" in this state), module is still in "online-connected-data-mode" and sends data to remote device.
iii. PIO-xx is toggled or LED D10 starts blinking to show the module is ready to accept the escape sequence.
iv. User should enter escape sequence immediately after the D10 led starts blinking
v. If module does not reply as "OK", user should wait till module is ready to receive next escape sequence.
vi. Module is ready to process firmware upgrade even if there are multiple attempts of failure to enter in Online-connected-command-mode.
vii. User cannot process further steps if module does not enter in online-connected-command-mode.

Note: If the Current firmware on the LM961 module is a Bridge application or GAP-Central-Only, then after SPP connection the LM961 enters into Command mode. Then there is no need to enter the Escape sequence. The user can directly issue the "AT+upgrade" command.

5.3.2 Failure point 2:

i. Once the module enters into the Online-connected-command-mode, the user should provide the firmware upgrade password through AT commands.
ii. If the user provides the correct firmware upgrade password, the module responds to the command as "OK" and displays the message "Ready to receive OTA file"
iii. The module replies as "ERR"
    a. If the user enters a wrong password for upgrade command, module responds as ERR.
    b. Firmware upgrade password is dependent on current firmware version of the module.
    c. E.g. if the current firmware version on the module is "1.50", the firmware upgrade password will be "AT+upgrade=LMUPDATEV150"
    d. In the "AT+upgrade" command the string after "=" is case sensitive and should be entered in all uppercase (for letters)
    e. If the module replies as "ERR", the user should try entering the correct password and try to get the message "Ready to receive OTA file".

   f. The module can process successfully even though it already had more than one failure attempt while getting "Ready to receive OTA file" message.

5.3.3 Failure point 3:

i. Once the module enters in Online-connected-command-mode, the user should provide the firmware upgrade password through AT command

ii. If the user provides the correct firmware upgrade password, the module responds to the command with "OK"

iii. After displaying the OK response, the module displays the message "Ready to receive OTA file" if it is in the state to receive the upgrade image.

iv. Module replies as "State Err"

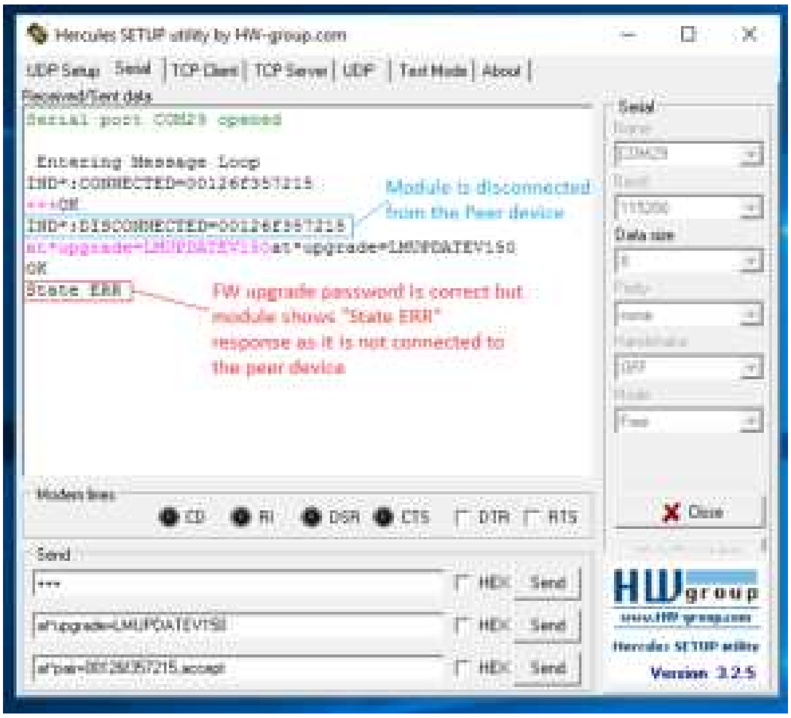
   a. If the firmware upgrade password is correct but module is not in state to perform the upgrade procedure, the module will respond as "State err" to the "AT'upgrade" command

   b. The module will display "State err" message if it is not connected to a remote device or it has lost the current connection.

   c. If module replies as "State err", the user cannot proceed to the firmware upgrade procedure and should check for the BT connection of LM961 with peer device

   d. In this case, the user shall start the upgrade procedure from the beginning.

   e. Refer to the image below:



```
Serial port COM29 opened

 Entering Message Loop
IND*:CONNECTED=00126f357215
+++OK
IND*:DISCONNECTED=00126f357215
at*upgrade=LMUPDATEV150at*upgrade=LMUPDATEV150
OK
State ERR
```

Module is disconnected from the Peer device

FW upgrade password is correct but module shows "State ERR" response as it is not connected to the peer device

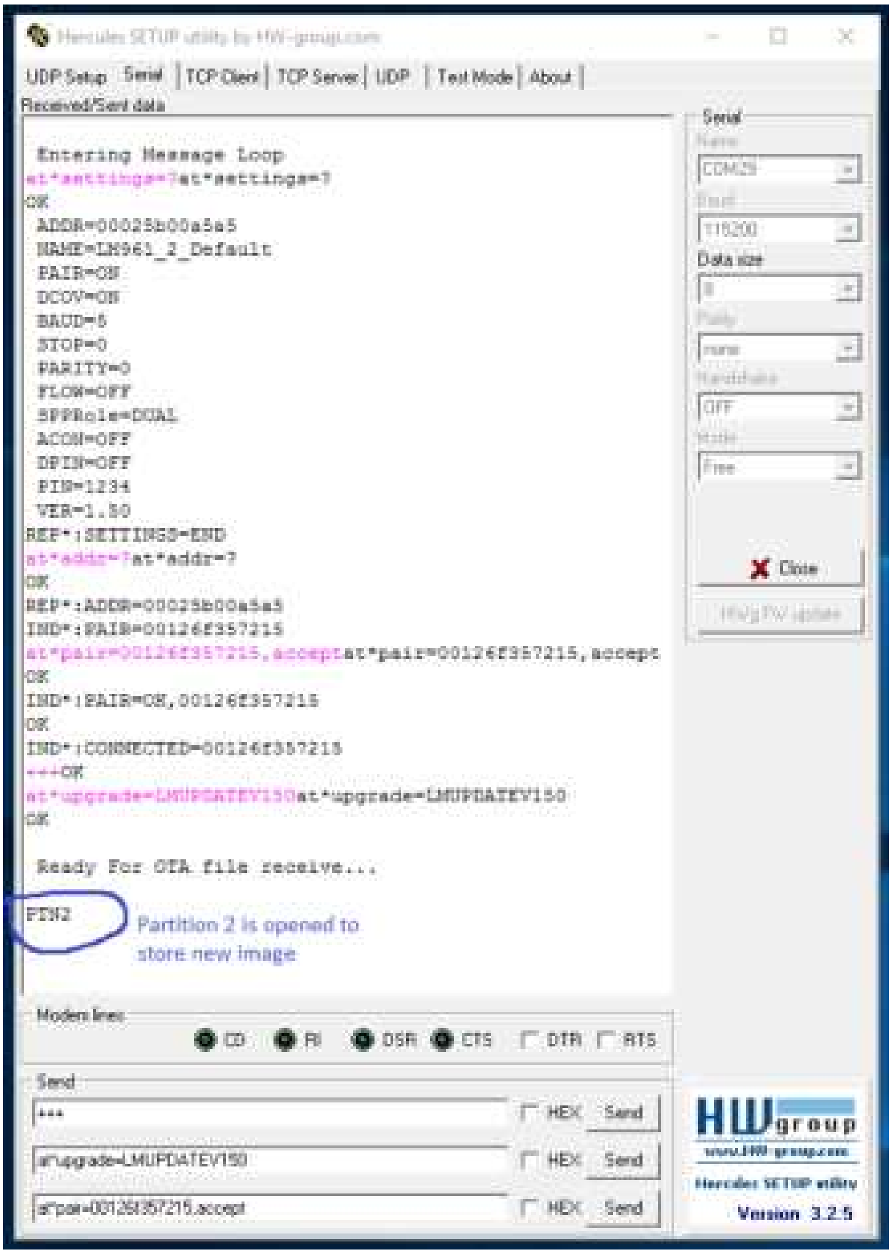
Send:

```
+++
at*upgrade=LMUPDATEV150
at*pair=00126f357215,accept
```

Figure 2: UART messages when the module is not connected to the peer device

5.3.4 Failure point 4:

i. After the module shows the message "Ready to receive OTA file", it is ready to receive the upgrade image.
ii. After the peer device begins sending the file, the module opens internal memory partition2 or partition3 to write this image
iii. The message "PTN2"/"PTN3" indicates that the module is writing the file to partition2/partition3.
iv. This message should appear one or two seconds after the peer starts sending the file.
v. If the module does not show this message, but the peer device indicates that the file has been sent, an error has occurred.
vi. In this case the user should power the module on and off or reset the module with the "AT*reset=1" command and try the procedure from start again.
vii. Refer to the image below



Hercules SETUP utility by HW-group.com
UDP Setup | Serial | TCP Client | TCP Server | UDP | Test Mode | About
Received/Sent data

```
 Entering Message Loop
at*settings=?at*settings=?
OK
 ADDR=00025b00a5a5
 NAME=LM961_2_Default
 PAIR=ON
 DCOV=ON
 BAUD=5
 STOP=0
 PARITY=0
 FLOW=OFF
 SPPRole=DUAL
 ACON=OFF
 DPIN=OFF
 PIN=1234
 VER=1.50
REP*:SETTINGS=END
at*addr=?at*addr=?
OK
REP*:ADDR=00025b00a5a5
IND*:PAIR=00126f357215
at*pair=00126f357215,acceptat*pair=00126f357215,accept
OK
IND*:PAIR=OK,00126f357215
OK
IND*:CONNECTED=00126f357215
+++OK
at*upgrade=LMUPDATEV150at*upgrade=LMUPDATEV150
OK

 Ready For OTA file receive...

PTN2
```

Partition 2 is opened to store new image

Serial

Name: COM29

Baud: 115200

Data size: 8

Parity: none

Handshake: OFF

Mode: Free

+++ □ HEX Send

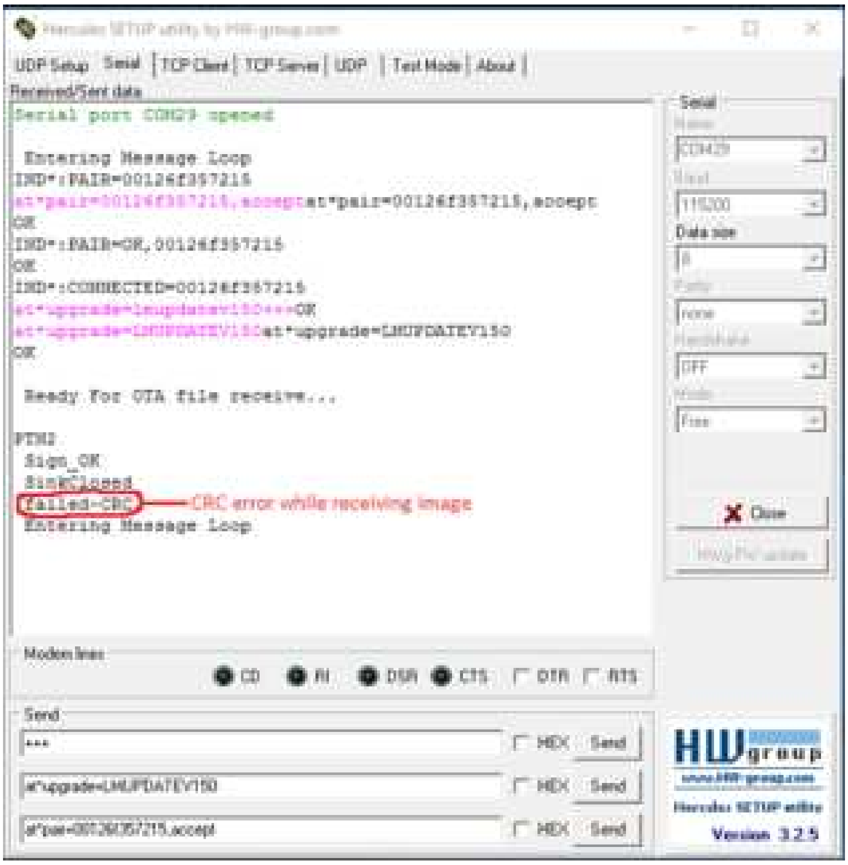
at*upgrade=LMUPDATEV150 □ HEX Send

at*pair=00126f357215,accept □ HEX Send

Figure 3: UART messages when the module opens a partition to write a new image

5.3.5. Failure point 5:

i. The message "PTN2"/"PTN3" indicates that the module is writing a file to partition2/partition3, module is receiving the file and writing it to the partition.
ii. After the peer device shows that it has successfully sent the file, LM961 will close the partition.
iii. After the partition is closed, the message "Sign_OK" indicates that the module has received Signature.
iv. The message "Sink_Closed" indicates that the module has closed the partition after receiving the random string.
v. After the partition is closed and if the upgrade procedure is completed successfully, the module shows the message "V_PASS_2" / "V_PASS_3"
vi. If module shows the "failed-CRC" message:
    a. If CRC of the received image is not matching to the CRC mentioned in the image, the module shows a "Failed-CRC" message.
    b. This may be because of disturbances/interferences in wireless transmission. If so the user should repeat the procedure from beginning.
    c. The module restarts itself with a warm reset and starts executing the existing image.
    d. Refer to the image below:



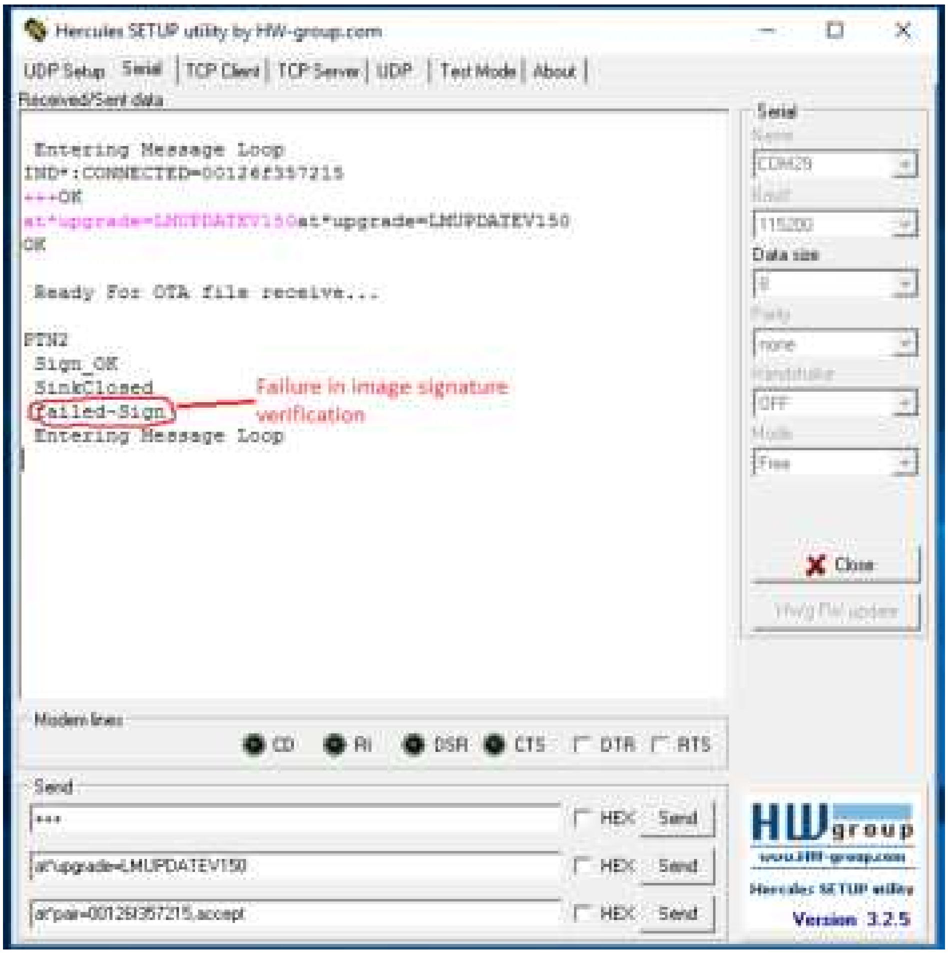
```
Serial port COM29 opened

 Entering Message Loop
IND*:PAIR=00126f357215
at*pair=00126f357215,acceptat*pair=00126f357215,accept
OK
IND*:PAIR=OK,00126f357215
OK
IND*:CONNECTED=00126f357215
at*upgrade=lmupdatev150+++OK
at*upgrade=LMUPDATEV150at*upgrade=LMUPDATEV150
OK

 Ready For OTA file receive...

PTN2
 Sign_OK
 SinkClosed
 failed-CRC
 Entering Message Loop
```

Serial
Name: COM29
Baud: 115200
Data size: 8
Parity: none
Handshake: OFF
Mode: Free

Send:
+++
at*upgrade=LMUPDATEV150
at*pair=00126f357215,accept

Figure 4: UART messages when the CRC of the received image does not match

vii. If the module shows "failed-Sign" message:
   a. If module shows the "failed-Sign" message, it indicates that the signature of module firmware is different than the signature of the new image.
   b. This indicates that the firmware upgrade procedure has been followed correctly but there is error in new image provided for the firmware upgrade.
   c. If the image is not suitable for performing a firmware upgrade the user should contact LM technologies.
   d. The module restarts itself with a warm reset and starts executing the existing image.
   e. Refer to the image below:


Hercules SETUP utility by HW-group.com
UDP Setup | Serial | TCP Client | TCP Server | UDP | Test Mode | About
Received/Sent data
Serial
Close
HWg FW update
Modem lines
● CD ● RI ● DSR ● CTS □ DTR □ RTS
Send
HW group
www.HW-group.com
Hercules SETUP utility
Version 3.2.5

```
 Entering Message Loop
IND*:CONNECTED=00126f357215
+++OK
at*upgrade=LMUPDATEV150at*upgrade=LMUPDATEV150
OK

 Ready For OTA file receive...

FTN2
 Sign_OK
 SinkClosed
 failed-Sign
 Entering Message Loop
```

Failure in image signature verification

Name: COM29
Baud: 115200
Data size: 8
Parity: none
Handshake: OFF
Mode: Free

+++ □ HEX Send
at*upgrade=LMUPDATEV150 □ HEX Send
at*pair=00126f357215,accept □ HEX Send

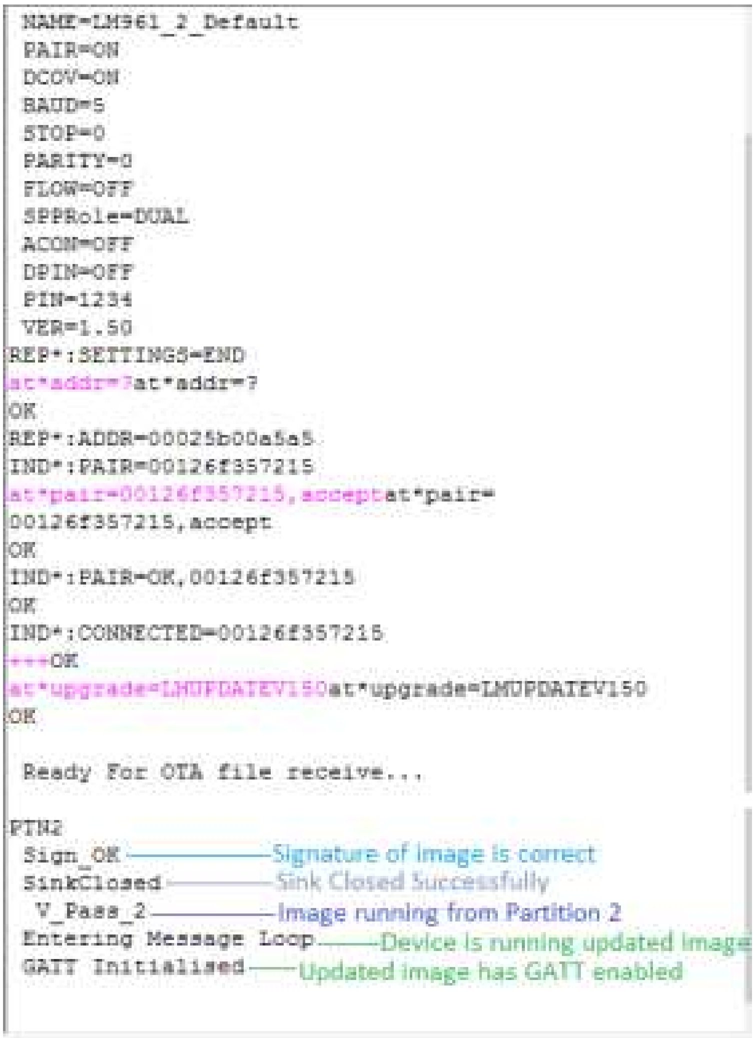
Figure 5: UART messages showing a failure in image verification

5.3.5 Successful firmware Upgrade:

i. The image below depicts the messages shown by the module during a successful firmware upgrade procedure.

ii. After showing message "V_Pass_2" or "V_Pass_3", the module performs warm reset and starts executing the new image.

iii. In the image below, the message "Entering Message Loop" indicates that the device has performed warm reboot. The message "GATT Initialised" indicates that the new image has GATT is enabled for BLE connectivity.



```
 NAME=LM961_2_Default
 PAIR=ON
 DCOV=ON
 BAUD=5
 STOP=0
 PARITY=0
 FLOW=OFF
 SPPRole=DUAL
 ACON=OFF
 DPIN=OFF
 PIN=1234
 VER=1.50
REP*:SETTINGS=END
at*addr=?at*addr=?
OK
REP*:ADDR=00025b00a5a5
IND*:PAIR=00126f357215
at*pair=00126f357215,acceptat*pair=
00126f357215,accept
OK
IND*:PAIR=OK,00126f357215
OK
IND*:CONNECTED=00126f357215
+++OK
at*upgrade=LMUPDATEV150at*upgrade=LMUPDATEV150
OK

 Ready For OTA file receive...

PTN2
 Sign_OK
 SinkClosed
  V_Pass_2
 Entering Message Loop
 GATT Initialised
```

Sign_OK — Signature of image is correct

SinkClosed — Sink Closed Successfully

V_Pass_2 — Image running from Partition 2

Entering Message Loop — Device is running updated image

GATT Initialised — Updated image has GATT enabled

Figure 6: UART messages showing successful firmware upgrade

6. Simple Secure Pairing between LM961 and remote device

This section describes the indication messages given by the LM961 module during the pairing procedure. It also covers the AT commands that a user will need to provide as per the settings of DPIN, MITM and IOTYPE.

The LM961 uses BT2.1 security supporting the dynamic PIN, but is also compatible with BT2.0 devices which shares fixed PIN during the pairing procedure.

6.1 Pairing of LM961(BT2.1) with BT2.0 devices

Here the BT2.0 device is treated as LM Technologies' LM048 device, with firmware version 6.57. When the LM961 has DPIN as DPIN=OFF, it is compatible with BT2.0 devices. When DPIN=OFF, the module does not care about MITM, IOTYPE settings.
When DPIN is OFF, module uses PIN during the pairing procedure with remote devices. Default PIN is 1234, users can change this to numeric only, Alpha only or alphanumeric.
As per Bluetooth standards, maximum of 16 characters are allowed in PIN setting.

6.1.1 If LM961 has setting DPIN=OFF

i. When the pairing procedure is started on the LM961, it will show the indication message with the BD-Address of remote device e.g "IND:PAIR=00126f357215".
ii. The user shall provide accept/reject response to this indication as "AT+PAIR=00126f357215,accept" or "AT+PAIR=00126f357215,reject"
iii. LM961 uses its fixed PIN
iv. If the fixed PIN of LM961 is same as the other device pairing is successful.
v. After completing the pairing procedure, the LM961 indicates the status of pairing to user e.g. "IND:PAIR=OK,00126f357215" or "IND:PAIR=FAIL,00126f357215".
vi. If the fixed PIN of LM961 is not same as other device pairing fails

6.2 Pairing of LM961 (BT2.1) with BT2.1 devices

Here the BT2.0 device is treated as LM Technologies' LM048 device with firmware version 6.19. The passkey used during the pairing procedure is dependent on the IO-type setting on the LM961.

If IO-type is keyboard only, the LM961 will expect the passkey from the user and use it internally for the pairing procedure

When the IO-type is display only, the LM961 will display the passkey and the user should use the same passkey on the remote device to complete the pairing procedure

When IO-type is Display with yes/no confirmation, the LM961 displays passkey and expects confirmation from the user whether the passkey for remote device is the same.

When the IO-type is NO-INOUT i.e. no input no output then it depends on the peer device whether the pairing will be successful or not. If the IO-type is No-input-no-output, MITM should be off otherwise the LM961 will never be able to pair with a remote device.

If the LM961 and remote device has IO-type as No-input-no-output and MITM as off then devices may pair successfully by "just works" pairing type.

6.2.1 LM961 has settings DPIN=on, MITM=on, IO-type=Keyboard-only

i. After the LM961 indicates Pairing as "IND+:PAIR,00126f357215" and the user accepts the Pairing request with "AT+PAIR=00126f357215, accept", the LM961 starts the pairing procedure

ii. IO-type as Keyboard only indicates that user can provide Passkey for pairing using AT commands.

iii. The bluetooth stack will use this passkey for completing the pairing procedure with the remote device.

iv. During the pairing procedure, the LM961 displays the message "IND+:PASSK=?". This indicates that the LM961 requires a Passkey from the user.

v. The user should respond to this with "at+passkey=1234", i.e. the passkey for the remote device is 1234. It can be any integer in range of 32bit value

vi. After completing the pairing procedure, the LM961 indicates the status of pairing to the user e.g. "IND+:PAIR=OK,00126f357215" or "IND+:PAIR=FAIL,00126f357215".

6.2.2 LM961 has settings DPIN=on, MITM=on, IO-type=display only

i. After the LM961 shows indication of Pairing "IND+:PAIR,00126f357215" and user accepts the Pairing request with "AT+PAIR=00126f357215, accept", LM961 starts pairing procedure.

ii. When the LM961 starts the pairing procedure with a remote device and has IO-capability as Display only, LM961 shows the Passkey for remote device as message "IND+:PASSKEY=311303" here number 311303 is for reference only and should vary for every device.

iii. IO-type as Display only indicates that the Passkey generated by the Bluetooth stack for pairing is only displayed by the LM961.

iv. The user should ensure that the other device uses the passkey provided by the LM961 module in above indication.

v. If the remote device uses the passkey displayed by the LM961 then the pairing procedure should be completed successfully.

vi. After the pairing procedure is completed, the LM961 indicates this as "IND:PAIR=OK,00126f357215". 00126f357215 is the reference BD address and LM961 will show the remote devices BD-Address

6.2.3 LM961 has settings DPIN=on, MITM=on, IO-type=Display Y/N

i. After the LM961 indicates Pairing as "IND:PAIR,00126f357215" and the user accepts the pairing request with "AT+PAIR=00126f357215, accept", the LM961 starts the pairing procedure.

ii. When the LM961 starts the Pairing procedure with the remote device and has IO-capability as Display_YN i.e. Display passkey and Confirmation is required as Yes or No. LM961 shows the Passkey for remote device and expects the confirmation from user as yes or No

iii. The passkey is displayed by the LM961 module as "IND:PASSKEY=756830".

iv. User shall provide confirmation with the AT command as "at+passcfm=00126f357215,Yes" or "at+passcfm=00126f357215,No".

v. The remote device should be set as IO-type as display-only or display-YN otherwise pairing will not be possible.

6.2.4 LM961 has settings DPIN=on, MITM=on, IO-type=no-Input-no-output

i. Pairing with the remote device may or may not be successful and depends on MITM and IO-type settings of remote device.

ii. If the remote device also has the same settings, then pairing may be successful otherwise the pairing might fail.

6.2.5 LM961 has settings DPIN=on, MITM=off, IO-type=no-Input-no-output

i. Pairing with the remote device might be successful if the remote device also has DPIN=on, MITM=off and IO-type as no one.

ii. If the remote device has MITM=on or IO type other than no input no output, the LM961 cannot pair with that device.

7. Appendix

7.1 Abbreviations

SSP	Simple Secure Pairing
BT	Bluetooth
BLE	Bluetooth low energy
BD-Address	Bluetooth address of device
BT2.0	Bluetooth 2.0 stack
BT2.1	Bluetooth 2.1 stack
MITM	Man In The Middle protection
IOTYPE	Input Output Type (IO capability of device)
DPIN	Dynamic PIN
PIN	Personal Identification Number

7.2 BLE Peripheral characteristics

Characteristic	Bit field for characteristic	Indication on LM961	Description
broadcast	0x01	"Bc"	Broadcasts of the Characteristic Value User cannot read or write on this characteristic
read	0x02	"Rd "	Reads of the Characteristic Value. User can read this characteristic with RDCHARVAL command
write_cmd	0x04	"Wr_cmd "	Writes of the Characteristic Value without response. User can write on this characteristic with AT+WRWORESP command
write	0x08	"Wr_req "	Writes of the Characteristic Value with response. User can write on this characteristic

			with AT+WRCHARVAL command
notify	0x10	'CCFG'	Client configuration flag for notification enable If user enables this flag, remote device shows notification
indicate	0x20	'Indi'	Indications of a Characteristic Value with acknowledgement. LM961 will show indication message if receives data form this characteristic
write_sig	0x40	'Wr_signed'	Signed writes to the Characteristic Value using Signed Write Command. User can write on this characteristic with AT+SWRWORESP command

7.3 GATT UUID type

1. All UUID values are in Hex.
2. 16-bit Attribute UUID is represented as "1801"
3. 32-bit UUID is represented as "32005b32"
4. All UUIDs are Big Endian, i.e. for example 128-bit UUID 00112233-4455-6677-8899-aabbccddeeff
5. uuid[0] = 0x00112233, uuid[1] = 0x44556677, uuid[2] = 0x8899aabb, and uuid[3] = 0xccddeeff.
6. If the service-UUID is 128-bit, it is completely mentioned in the report of FindServ e.g. "00005500-d102-11e1-9b23-00025b00a5a5"
7. If the characteristic has 128-bit UUID then only first 32 bits are shown e.g
8. "00005501" is shown whereas the actual 128-bit UUID is "00005501-D1021E1-93230002-5300a5a5" here the remaining bits are same as that of the 128-bit Service UUID shown above

7.4 GATT_Status_code

The BLE stack outputs an error if the required operation fails. The table below lists the possible error codes with a description

Sr No	Error code	Error description
1	0x0	gatt_status_success
2	0x1	gatt_status_invalid_handle
3	0x2	gatt_status_read_not_permitted
4	0x3	gatt_status_write_not_permitted
5	0x4	gatt_status_invalid_pdu
6	0x5	gatt_status_insufficient_authentication
7	0x6	gatt_status_request_not_supported
8	0x7	gatt_status_invalid_offset
9	0x8	gatt_status_insufficient_authorization
10	0x9	gatt_status_prepare_queue_full
11	0xa	gatt_status_attr_not_found
12	0xb	gatt_status_not_long
13	0xc	gatt_status_insufficient_encr_key_size
14	0xd	gatt_status_invalid_length
15	0xe	gatt_status_unlikely_error
16	0xf	gatt_status_insufficient_encryption
17	0x10	gatt_status_unsupported_group_type
18	0x11	gatt_status_insufficient_resources
19	0x12	gatt_status_application_error
20	0x13	gatt_status_initialising
21	0x14	gatt_status_failure
22	0x15	gatt_status_att_req_failure
23	0x16	gatt_status_att_db_failure
24	0x17	gatt_status_max_connections
25	0x18	gatt_status_abnormal_disconnection
26	0x19	gatt_status_link_loss
27	0x1a	gatt_status_mtu_already_exchanged
28	0x1b	gatt_status_value_mismatch
29	0x1c	gatt_status_rej_psm

Sr No	Error code	Error description
30	0x1d	gatt_status_ref_security
31	0x1e	gatt_status_key_missing
32	0x1f	gatt_status_connection_timeout
33	0x20	gatt_status_retrying
34	0x21	gatt_status_peer_aborted
35	0x73	gatt_status_device_not_found
36	0x74	gatt_status_sign_failed
37	0x75	gatt_status_busy
38	0x76	gatt_status_timeout
39	0x77	gatt_status_invalid_mtu
40	0x78	gatt_status_invalid_uuid
41	0x79	gatt_status_success_more
42	0x7a	gatt_status_success_sent
43	0x7b	gatt_status_invalid_cid
44	0x7c	gatt_status_invalid_db
45	0x7d	gatt_status_db_full
46	0x7e	gatt_status_invalid_phandle
47	0x7f	gatt_status_invalid_permissions

7.5 BLE Service UUIDs

BLE Service UUIDs for reference only.

Sr No	Service	UUID
1	Generic Access	0x1800
2	Alert Notification Service	0x1811
3	Automation IO	0x1815
4	Battery Service	0x180F
5	Blood Pressure	0x1810
6	Body Composition	0x181B
7	Bond Management Service	0x181E
8	Continuous Glucose Monitoring	0x181F
9	Current Time Service	0x1805
10	Cycling Power	0x1818
11	Cycling Speed and Cadence	0x1816
12	Device Information	0x180A
13	Environmental Sensing	0x181A
14	Fitness Machine	0x1826
15	Generic Attribute	0x1801

Sr No	Service	UUID
16	Glucose	0x1808
17	Health Thermometer	0x1809
18	Heart Rate	0x180D
19	HTTP Proxy	0x1823
20	Human Interface Device	0x1812
21	Immediate Alert	0x1802
22	Indoor Positioning	0x1821
23	Internet Protocol Support Service	0x1820
24	Link Loss	0x1803
25	Location and Navigation	0x1819
26	Mesh Provisioning Service	0x1827
27	Mesh Proxy Service	0x1828
28	Next DST Change Service	0x1807
29	Object Transfer Service	0x1825
30	Phone Alert Status Service	0x180E
31	Pulse Oximeter Service	0x1822
32	Reference Time Update Service	0x1806
33	Running Speed and Cadence	0x1814
34	Scan Parameters	0x1813
35	Transport Discovery	0x1824
36	Tx Power	0x1804
37	User Data	0x181C
38	Weight Scale	0x181D

2.2 List of applicable FCC rules

FCC Part 15.247

2.6 RF exposure considerations

This module certified that complies with RF exposure requirement under 5mm RF distance.

2.8 Label and compliance information

FCC ID label on the final system must be labeled with “Contains FCC ID: VVXLM961-1” or “Contains transmitter module FCC ID: VVXLM961-1”.

2.9 Information on test modes and additional testing requirements

Contact LM Technologies Ltd. will provide stand-alone modular transmitter test mode. Additional testing and certification may be necessary when multiple modules are used in a host.

2.10 Additional testing, Part 15 Subpart B disclaimer

To ensure compliance with all non-transmitter functions the host manufacturer is responsible for ensuring compliance with the module(s) installed and fully operational. For example, if a host was previously authorized as an unintentional radiator under the Supplier’s Declaration of Conformity procedure without a transmitter certified module and a module is added, the host manufacturer is responsible for ensuring that the after the module is installed and operational the host continues to be compliant with the Part 15B unintentional radiator requirements. Since this may depend on the details of how the module is integrated with the host, LM Technologies Ltd. shall provide guidance to the host manufacturer for compliance with the Part 15B requirements.

FCC Warning

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:
(1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

NOTE 1: Any changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance.

Note 1: This module certified that complies with RF exposure requirement under 5mm RF distance.

Note 2: Any modifications made to the module will void the Grant of Certification, this module is limited to OEM installation only and must not be sold to end-users, end-user has no manual instructions to remove or install the device, only software or operating procedure shall be placed in the end-user operating manual of final products.

Note 3: The module may be operated only with the antenna with which it is authorized. Any antenna that is of the same type and of equal or less directional gain as an antenna that is authorized with the intentional radiator may be marketed with, and used with, that intentional radiator.