BlueNRG-MS Stack v7.2c

Binary images and ifr configuration files

- **bluenrg_7_2_c_Mode_2-16MHz-XO32K_4M.img**: 16 MHz high-speed crystal and external 32 kHz low-speed crystal binary image (SMPS switching frequency 4MHz).
- **bluenrg_7_2_c_Mode_2-32MHz-XO32K_4M.img**: 32 MHz high-speed crystal and external 32 kHz low-speed crystal binary image (SMPS switching frequency 4MHz).
- **ifr_3v1_003_mode02-16MHz-RO32K_4M.dat**: 16 MHz high-speed crystal and internal low-speed crystal ifr configuration (SMPS switching frequency 4MHz).
- **ifr_3v1_003_mode02-16MHz-XO32K_4M.dat**: 16 MHz high-speed crystal and external 32 kHz low-speed crystal ifr configuration(SMPS switching frequency 4MHz).
- **ifr_3v1_003_mode02-32MHz-RO32K_4M.dat**: 32 MHz high-speed crystal and internal low-speed crystal ifr configuration (SMPS switching frequency 4MHz).
- **ifr_3v1_003_mode02-32MHz-XO32K_4M.dat**: 32 MHz high-speed crystal and external 32 kHz low-speed crystal ifr configuration(SMPS switching frequency 4MHz).

Notes

- BlueNRG-MS stack v7.2c binary image also supports the HCI APIs.
- Please check BlueNRG_MS platform crystal configuration (16 or 32 MHz, external 32KHz or internal low-speed crystal, SMPS switching frequency) and configure the BlueNRG-MS device IFR accordingly.
- The switching frequency for the internal SMPS block can be 4MHz or 8MHz (IFR has to be configured accordingly). On BlueNRG-MS HW platform the following inductors have to be used respectively: 10uH for 4MHz, 4.7uH for 8MHz.

New features/Changes

This section lists the new features or changes compared to BlueNRG-MS Stack v7.2b

- NA

Solved Issues

This section lists the solved issues compared to BlueNRG-MS Stack v7.2b

- ID 2047: LL_VERSION_IND packet was sent with a payload length equal to 7 instead of 6.
- ID 2242: Private address was sent as identity address in pairing when privacy was enabled. If BlueNRG had privacy enabled and was put in undirected connectable mode using the resolvable private address, when the Master connected and performed a pairing procedure the resolvable address was sent in the identity information message by BlueNRG, instead of the public random address or the static random address. This caused the security manager of the Master to refuse the address or lose the bond when the resolvable address changed. Public address is now distributed if a valid one is set, otherwise the static random address is used.
- ID 2299: The link is now dropped if any unexpected Data channel PDU is received during the encryption start procedure. The new LinkLayer test TP_SEC_MAS_BV-14-C did not PASS before. The test requires a Master IUT, which has started the encryption procedure, not to respond to an LL_VERSION_IND but instead it must drop the link. The BlueNRG-MS did not drop the link but enqueued the packet and answered to it after the encryption procedure was terminated.

- ID 2307: Default output power was set to -2 dBm. Now is 8 dBm.
- ID 2303: The Supported_Commands returned by HCI_READ_LOCAL_SUPPORTED_COMMANDS were not correct. The flags for the following commands (which are supported) are now set:
    - LE Set Scan Parameters
    - LE Set Scan Enable
    - LE Create Connection
    - LE Create Connection Cancel
    - LE Connection Update
    - LE Set Host Channel Classification
    - LE Read Remote Used Features
    - LE Start Encryption
    - LE Long Term Key Request Reply
    - LE Long Term Key Request Negative Reply
- ID 2340: If the slave sent a LL_REJECT_IND PDU and the next packet from the master was a non-empty packet, the connection was dropped by the slave.
- ID 2341: A wrong offset was used to evaluate if the current Random Address was Static or Private when distributing the address in the Identity Address Information packet.

Known Limitations/Bugs

This section lists the issues known at firmware image release time. Issues found after this release are listed as solved or limitations on newer releases.

- ID 583: No ACI commands for internal ADC.
- ID 727: When BlueNRG is running as a master with one (or more) connections active, then any additional connection/scan slot request will be activated only after the next scheduled wake-up slot.
- ID 838: Some command complete events could only return the status (not equal to 0) without other parameters if the command does not completed successfully.
- ID 841: A flash erase can cause a disconnection. A flash erase will happen when the security database is full.
- ID 894: With a probability of (2**-24), the window length of the slave will be wrong, resulting in a lost communication opportunity (i.e. packet sent by the master could not be received).
- ID 919: Sometimes ACI_HAL_LE_TX_TEST_PACKET_NUMBER can return a value equal to the number of transmitted packets minus one.
- ID 1111: Sometimes, when using RO, BlueNRG master starts the connection event with a timing error larger than expected.
- ID 1126: No ACI function to access battery level detector.
- ID 1208: Client characteristic configuration descriptor not reset when only the master has lost its bond.
- ID 1222: ACI_GAP_SET_UNDIRECTED_CONNECTABLE uses fixed advertising interval.
- ID 1265: When BlueNRG has sent the first ADV_NONCONN_IND packet (just after advertising is enabled), it enters in an unexpected RX state. During following ADV_NONCONN_IND events, BlueNRG does not go in RX state, as expected.
- ID 1353: When a BlueNRG in mode 4 has all of its connections with a given connection interval (e.g. 1 second), it is not possible to do advertise with an advertising interval less than the connection interval of the existing connections (e.g. 100 ms). The ACI_GAP_SET_DISCOVERABLE is rejected with 0x85 error code ("too large interval").
- ID 1469: If BlueNRG performs a bonding procedure but it is reset before a clean disconnection can be made, the GATT database is not stored in Flash. Hence, BlueNRG cannot send an indication for the

service changed characteristic to the previously bonded device if the GATT database has been changed.

- ID 1567: Privacy-enabled slave allowed to use non-resolvable private address in connectable mode, while it has to be forbidden. Application must take care of using only resolvable private addresses while in connectable mode with privacy enabled.
- ID 1646: BlueNRG does not stop advertising immediately, but only after next scheduled packet or event. Hence, the timebase can potentially be updated only after this scheduled event.
- ID 1917: Non-compliance of default BD_ADDR: standard dictates that if this Controller does not have a Public Device Address, the value 0x000000000000 muts be returned. Instead all 0xFF's are now used if no public address is specified.
- ID 1920: From code inspection it could happen that when a Write response and a notification are processed in the same iteration of the GATT process function, the notification may be lost and an error response may be sent from the client to the server. However this has never been observed on BluenRG-MS.
- ID 1972: The size of the Offset field in ACI_GATT_READ_HANDLE_VALUE_OFFSET command is 1 byte instead of 2 bytes.
- ID 2054: If the device is connected as master with CE_Length <=2 and with hs_startup_time set to the maximum value (or close to it) and then it tries to start advertising, the advertising slot is never scheduled.
- ID 2076: Security requirements not checked before sending Indications or Notifications. Standard dictates that When a server reconnects to a client to send an indication or notification for which security is required, the server shall initiate or request encryption with the client prior to sending an indication or notification. Currently the stack does not check if security requirements are satisfied and this check must be done at application level in order to avoid security issues.
- ID 2188: Disconnections with timeout reason can be observed in a scenario where a BlueNRG is connected to a slave and a master and when connection parameter updates are done on both links. The disconnections have been observed only on the link between the master&slave and the slave device and when the master is a smartphone.

BlueNRG-MS stack update methods

- Use BlueNRG IFR updater & stack image updater utilities (files **bluenrg_utils.[ch]**. Refer to related demonstration application example (BlueNRG_Stack_IFR_Updater).
- Use BlueNRG GUI Updater Tool:
    1. Open the BlueNRG GUI
    2. Connect the BlueNRG platform to the PC USB port
    3. Put the platform in DFU mode and download the prebuilt BlueNRG_VCOM_x_x.hex binary image available on Firmware\STM32L1_prebuilt_images folder, using Tools, Flash Motherboard FW... utility
    4. Open the correct COM port related to the connected BlueNRG platform
    5. Go to Tools -> BlueNGR Updater
    6. Using the Browse.. tab, select latest Firmware\BlueNRG-MS_stack\bluenrg_7_2_c_Mode_2-16MHz-XO32K_4M.img and launch update procedure. This image has default parameters for the recommended 16 MHz crystal and use Mode 2 (see below).

BlueNRG-MS stack modes

Stack MODE1

- Master and Slave

- Only one connection
- The total number of attribute records for characteristics is 35 (9 records are reserved for GAP and GATT services)
- The max length for the characteristics records array is 302 bytes (36 bytes + length of the device name characteristic are reserved for GAP and GATT services)
- The service information are allocated in a specific pool of service records
- The total number of attributes records for services is 5 (2 are reserved for the default GAP and GATT services)
- Only 6 KB of RAM retention

Stack MODE2

- Master and Slave
- Only one connection
- The total number of attribute records for characteristics is 68 (9 records are reserved for GAP and GATT services)
- The max length for the characteristics records array is 700 bytes (36 bytes + length of the device name characteristic are reserved for GAP and GATT services)
- The service information are allocated in a specific pool of service records
- The total number of attributes records for services is 8 (2 are reserved for the default GAP and GATT services)
- 12 KB of RAM retention

Stack MODE3

- Master and Slave
- Up to 8 connections
- The total number of attribute records for characteristics is 22 (9 records are reserved for GAP and GATT services)
- The max length for the characteristics records array is 490 bytes (120 bytes + length of the device name characteristic * 8 are reserved for GAP and GATT services)
- The service information are allocated in a specific pool of service records
- The total number of attributes records for services is 5 (2 are reserved for the default GAP and GATT services)
- 12 KB of RAM retention

Stack MODE4

- Master and Slave
- Simultaneous advertising and scanning
- Up to 4 connections
- The total number of attribute records for characteristics is 42 (9 records are reserved for GAP and GATT services)
- The max length for the characteristics records array is 590 bytes (72 bytes + length of the device name characteristic * 4 are reserved for GAP and GATT services)
- The service information are allocated in a specific pool of service records
- The total number of attributes records for services is 8 (2 are reserved for the default GAP and GATT services)

- 12 KB of RAM retention

Note about characteristics records array size

- Each **characteristic** (declaration, value and descriptor) contributes to reach the max length for the characteristics records array bytes, as follow:
    1. **Declaration**: 5 bytes for UUID_16 or 19 bytes for UUID_128;
    2. **Value**: length of characteristic value (Char_Value_Length parameter in the ACI_GATT_ADD_CHAR command).
    3. **Client Configuration descriptor**: 2 bytes * max number of connections, i.e. 8 in Mode 3 and 4 in Mode 4.

Basic migration guidelines from BlueNRG v6.4 to BlueNRG-MS v7.x

- **aci_gap_init()**:
    1. Role parameter: modified bitmap of allowed roles (refer to file gap.h for new values).
    2. Added new parameter privacy_enabled for enabling (1) or disabling (0) privacy.
    3. Added new parameter device_name_char_len for setting the length of the device name characteristic.
- **aci_gap_set_direct_connectable()**: a new parameter, 'Advertising Type' has been added.
- **aci_gap_set_non_connectable()**: a new parameter, 'own address type' has been added.
- **aci_gap_set_undirected_connectable()**: the own address type parameter can take 0x02 and 0x03 also as its value.
- **aci_gap_start_general_conn_establishment()**: the own address type parameter can take 0x02 and 0x03 also as its value
- **aci_allow_rebond()**: a new parameter, 'connection handle' has been added.
- **aci_gap_get_bonded_devices()**: the command complete event parameters have changed to include the number of bonded devices.
- **aci_gap_resolve_private_address()**: the command complete event parameters have changed to include the public/static address of the bonded peer when the address is resolved.
- **aci_l2cap_conn_update_resp()**: two new parameters, 'Minimum CE length' and 'Maximum CE length' have been added.
- **aci_gap_set_broadcast_mode()**: new command added to the stack v7.1.
- **aci_gap_start_observation_Proc()**: new command added to stack v7.1.
- **aci_gap_is_device_bonded()**: new command added to the stack v7.1.
- **aci_gatt_Read_Handle_Value_Offset()**: newcommand added to the stack v7.1.
- **Evt_Blue_Gatt_Attribute_modified** event: an additional parameter 'offset' has been added to the event
- **Evt_Blue_Gap_Addr_Not_Resolved** event: an additional field 'connection handle' has been added to the event
- **Evt_Blue_Gap_Device_Found** event is not anymore returned from BlueNRG-MS stack v7.1 when a device is found during a discovery procedure
- **Evt_LE_Advertising_Report** event is returned from BlueNRG-MS stack v7.1c when a device is found durign a device discovery procedure.

Documentation

- Refer to BlueNRG-MS Bluetooth LE stack application command interface (ACI) user manual (UM1865) for detailed description of BlueNRG-MS ACI APIs and related events.

Generated by  1.8.10