Over-the-air (OTA) firmware upgrade for Bluetooth Mesh

Introduction

This document describes over-the-air (OTA) firmware upgrade process related to Bluetooth low energy (BLE) stack provided with the BlueNRG-1 and BlueNRG-2 systems-on-chip supporting Bluetooth Mesh.

Table 1. BLE OTA firmware upgrade for Mesh - list of supported devices

BLE device	Available Flash memory	Available RAM memory	Flash memory amount needed for OTA Service Manager	OTA FW upgrade and upload support
BlueNRG-2	256 KB	24 KB	~70 KB	Yes
BlueNRG-1	160 KB	24 KB	~70 KB	No

RELATED LINKS

For further information on OTA Firmware Upgrade, refer to AN4869

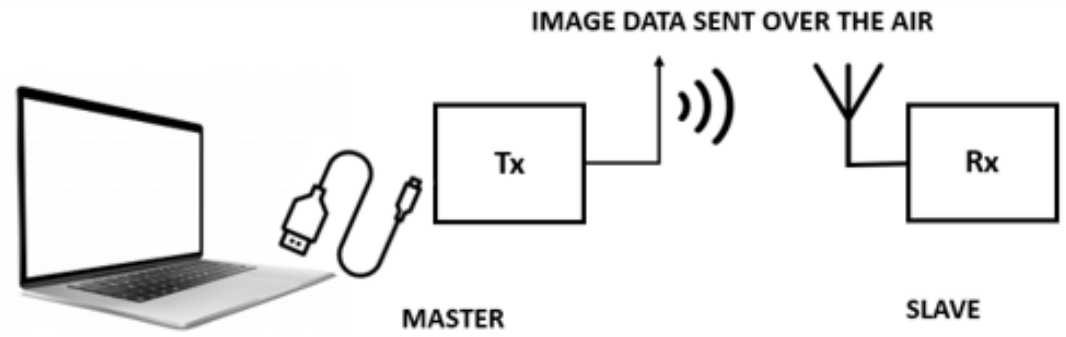
1 Over-the-air firmware upgrade overview

Over-the-air (OTA) firmware upgrade is a protocol that allows Bluetooth low energy slave devices to receive a firmware image from a Bluetooth low energy master device in a reliable fashion. The received image is then validated and stored into the Flash memory.

The OTA firmware upgrade framework defines a service compatible with services used by any application running on the BLE stack.

Figure 1. OTA firmware upgrade for BlueNRG-2 - Mesh messages sent over BLE using a smartphone

Figure 2. OTA firmware upgrade for BlueNRG-2 - master and slave devices



2 BLE application with BLE OTA service

Among the different architectures described in AN4869, OTA service manager has been used for Bluetooth Mesh as described hereafter.

2.1 OTA service manager application

The BLE OTA service manager architecture consists of the following components:

- **OTA service manager**
  - This application takes control at the device reset. In normal operation mode, it gives control to the main application. If, however, it detects a firmware upgrade flag, it exposes BLE OTA service. Service manager includes logic to assemble and validate the firmware image from the image chunks received from the OTA client. After the received image is checked and validated, it is programmed into the Flash memory and the control jumps to the newly upgraded application.
- **Main application**
  - This application usually runs on the device and is part of the firmware which can be downloaded through the OTA service manager. It is placed at fixed Flash address and does not require to include the OTA firmware upgrade service. To use this functionality, the application has to activate the OTA service manager only (a specific `OTA_Switch_To_OTA_Service_Manager_Application()` API is provided within OTA_btl.c file).

The OTA service manager acts as a standalone OTA firmware upgrade application providing the BLE OTA firmware upgrade capability to any application using this feature. It also includes the OTA reset manager capability to pass control to the latest updated and valid BLE application.

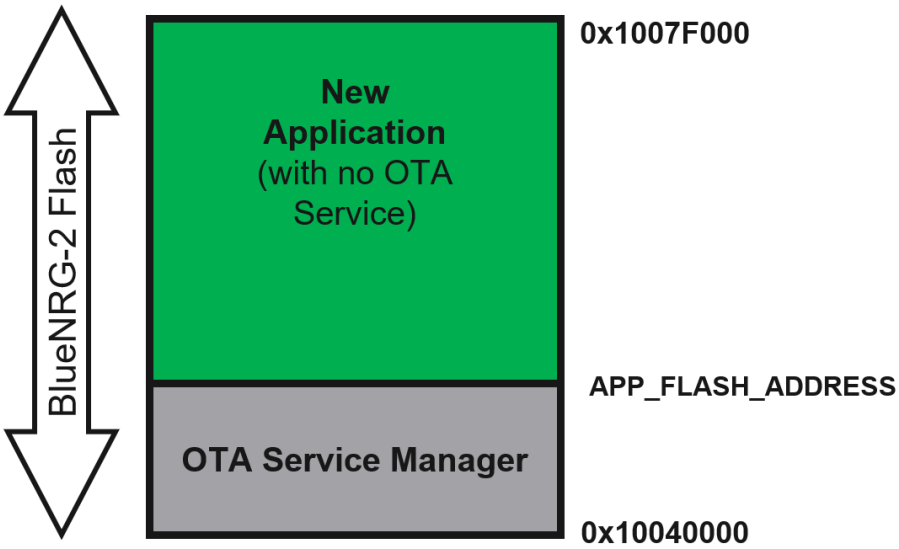
The OTA service manager application projects, header and source files are provided within the BlueNRG-1_2 DK SW packages (BLE_OTA_ServiceManager workspace).

To enable the data length extension support on OTA firmware upgrade process for the BlueNRG-2 device, BLE stack v2.1 or later, the `OTA_EXTENDED_PACKET_LEN=1` must be added as pre-processor option on OTA service manager application.

On the BlueNRG-2 device, BLE stack v2.1 or later, the OTA service manager application is built with a modular approach, OTA basic configuration (`BLE_STACK_CONFIGURATION=BLE_OTA_BASIC_CONFIGURATION`), that is:

- no controller privacy
- no LE secure connection
- no master/central role
- data length extension

Figure 3. **OTA service manager Flash memory layout**



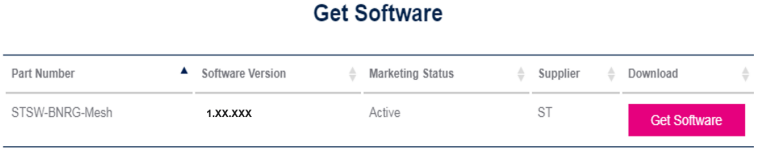
BlueNRG-2 BLE v2.x OTA service manager flash memory layout

3 OTA for BLE Mesh devices

3.1 How to install OTA service manager into BlueNRG-2 devices

Step 1. Download the ST BLE Mesh latest package, clicking on the pink button shown below.

Figure 4. STSW-BNRG-Mesh software package



Step 2. Flash the OTA_ServiceManager_32MHz binary into a STEVAL-IDB008VX evaluation board (starting Flash Address 0x10040000) using BlueNRG-X Flasher Utility available in Firmware\Projects\BlueNRG-2\Applications\Lighting_Demo\Binary as shown below.

Figure 5. Selecting the binary from the installed package

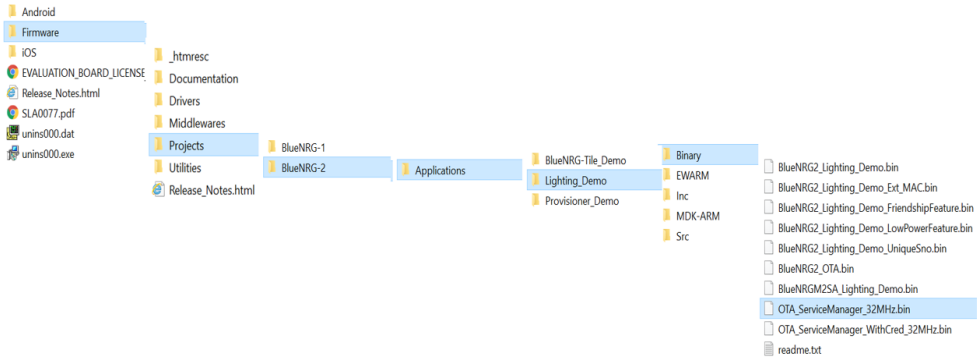
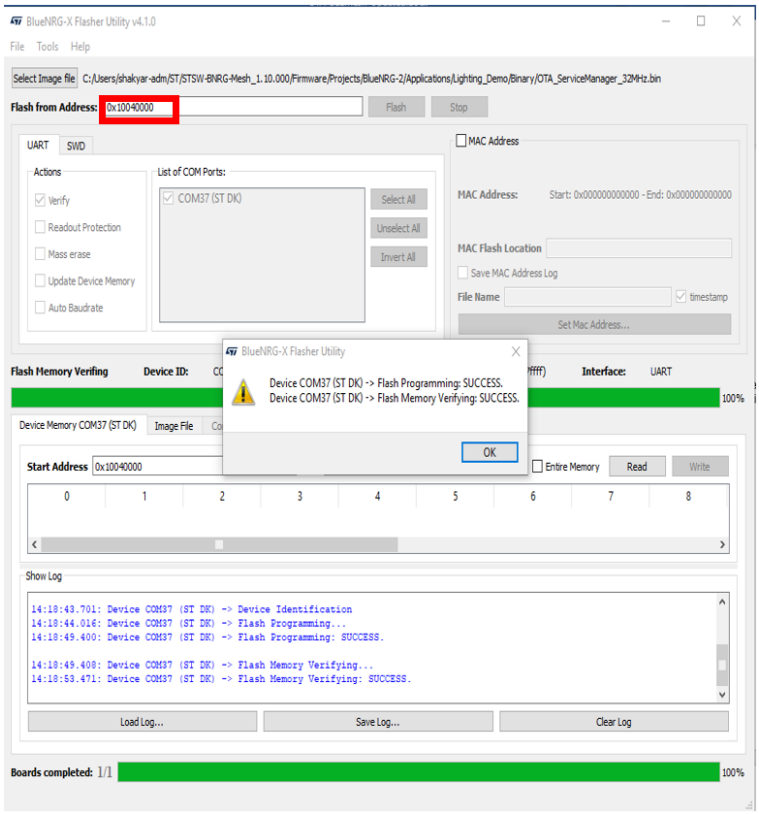


Figure 6. BlueNRG-X Fasher Utility to flash the binary



Note: Use BlueNRG-1 ST-Link Utility if USB Virtual COM Port is not supported on the required hardware.

3.2 Using ST BLE Mesh app

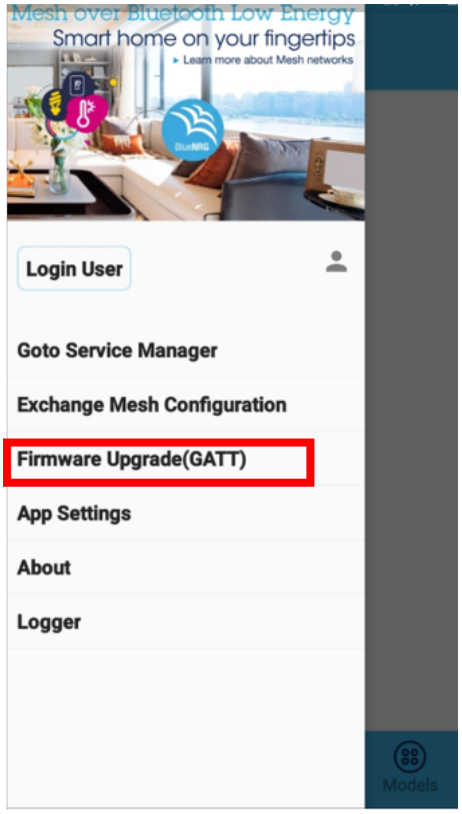
Step 1. Install the ST BLE Mesh app from Google Play/App store depending on the mobile device used.

Step 2. Copy the binary BlueNRG2_OTA.bin from Firmware\Projects\BlueNRG-2\Applications\Lighting_Demo\Binary into the smartphone by sending the required binary via e-mail or by plugging the phone into any open USB port on the computer and tapping the *File transfer* notification that appears after unlocking the phone.

Step 3. Open the app and accept the request to allow Bluetooth radio and GPS location to be turned on if a pop-up appears on the screen.

Step 4. Select *Firmware Upgrade (GATT)* option using the app drop-down menu.

Figure 7. Firmware Upgrade over GATT



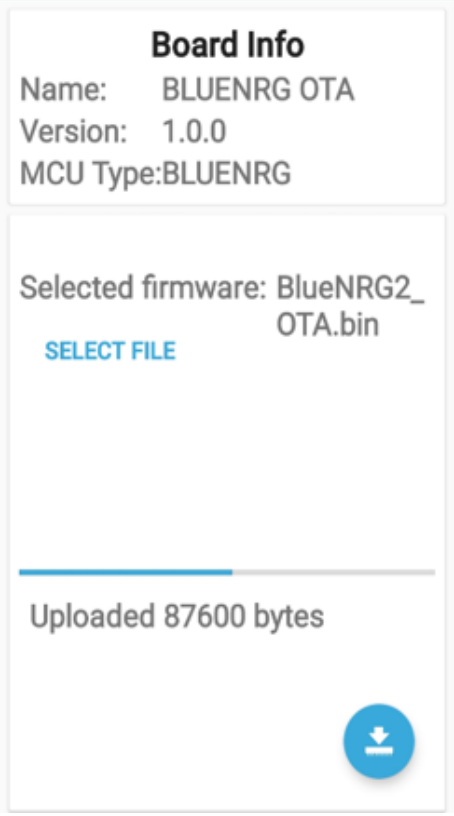
OTA Service Manager installed will be visible on the screen.

Figure 8. Node with OTA Service Manager

Step 5. Select the BlueNRG2_OTA.bin and press the down arrow button to start the firmware upgrade over the air.

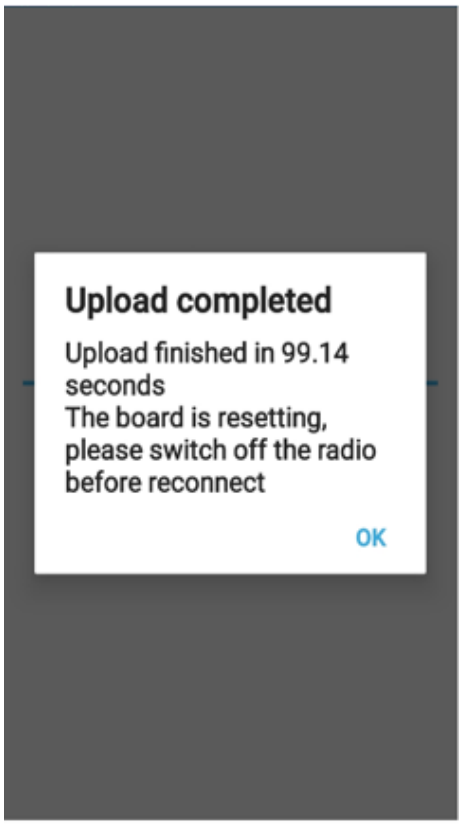
Note: The firmware version is different for the updated binary.

Figure 9. Firmware Upgrade over the air



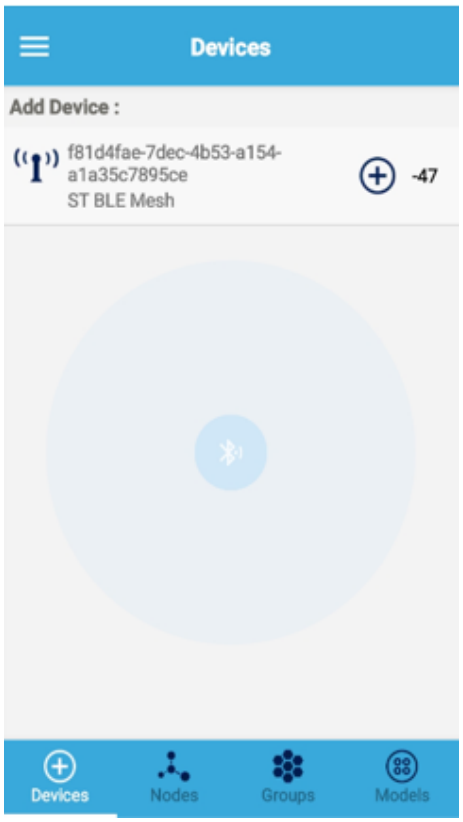
A pop-up appears once the OTA firmware upgrade is successfully completed.

Figure 10. Upload completed



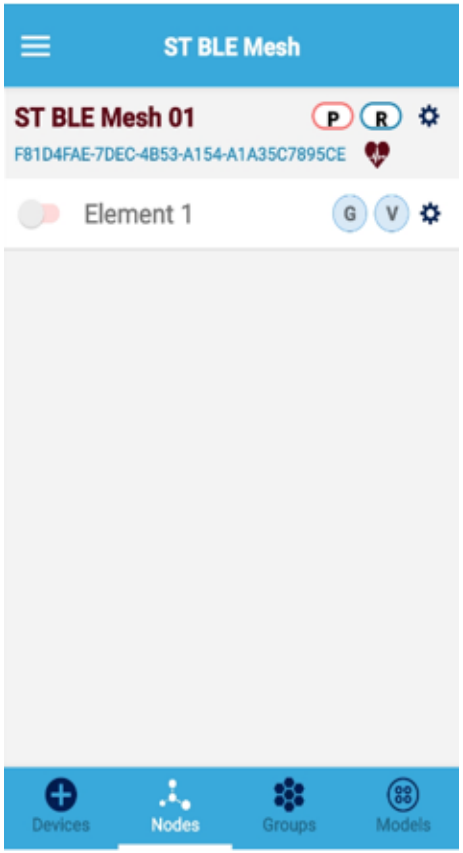
The node will be visible on ST BLE Mesh Scan Page after successful upgrade and ready to get provisioned.

Figure 11. Un-provisioned node after OTA Firmware Upgrade



After Provisioning, the node becomes part of the network.

Figure 12. **Provisioned node**

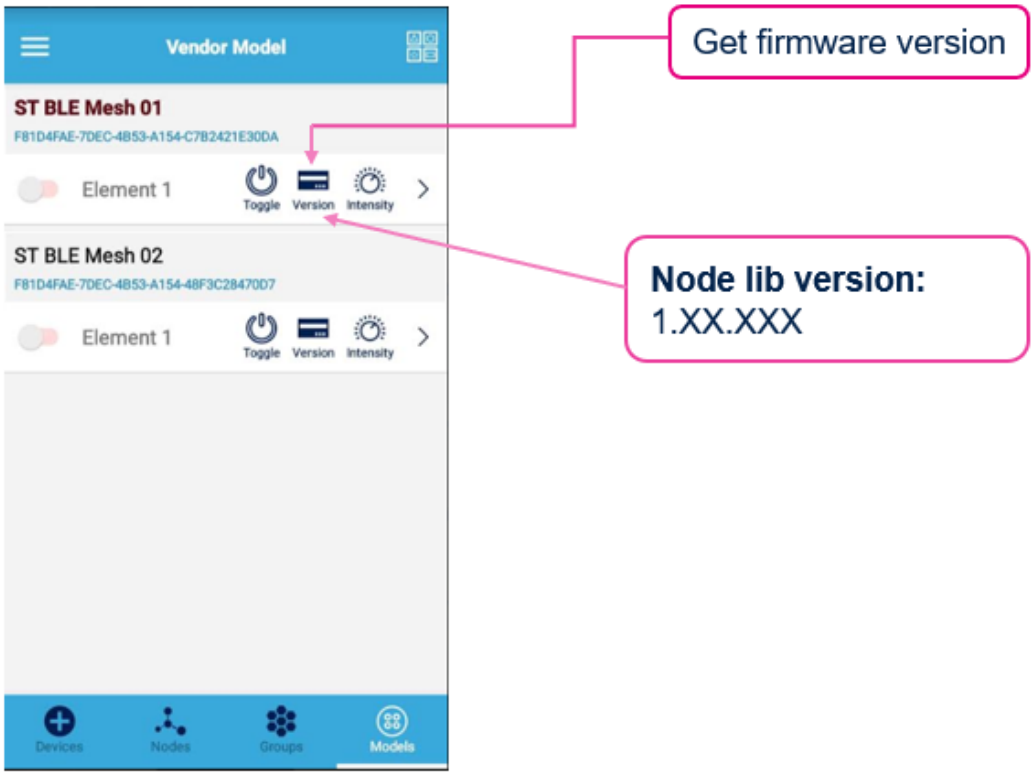


Step 6. To upgrade the firmware again, follow the steps mentioned above.

Step 7. Select [**Vendor Model**] under [**Models Tab**] of the provisioned node and then click [**Version**] to get the updated version of the firmware flashed on the board which is different for every upgrade.

After provisioning, the firmware version can be checked.

Figure 13. Checking the firmware version



3.2.1 Provisioned node firmware upgrade

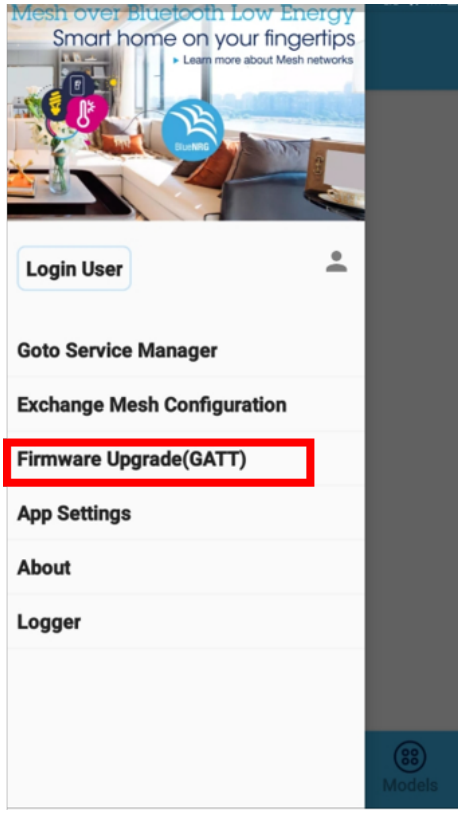
Step 1. To upgrade the firmware of the provisioned node, put it again in OTA mode using Vendor Mode.

The Android/iOS app sends the `Set Vendor Command: opcode > APPLI_TEST_CMD (0x01), sub opcode > APPLI_ENABLE_OTA (0x08)` command.

On the firmware side, `API Appli_Vendor_Test()` present in appli_vendor.c is called, together with the `APPLI_OTA_ENTER` sub-command to put the device again in OTA mode.

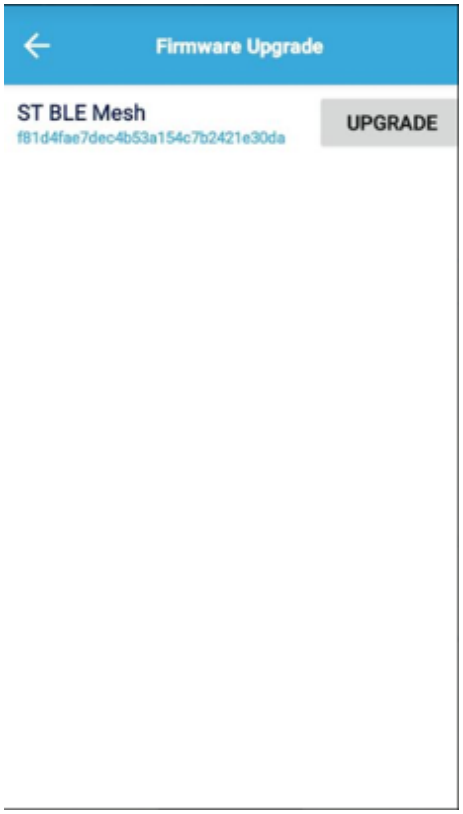
Step 2. Select *Firmware Upgrade (GATT)* option using the app drop-down menu.

Figure 14. Firmware Upgrade over GATT



Step 3. Press the upgrade button.

Figure 15. ST BLE Mesh upgrade button



Step 4. For STEVAL-IDB008VX boards, upgrade the firmware by directly using the BlueNRG-X Flasher Utility.

Step 4a. Flash the OTA Service Manager (if not already flashed) by selecting the [**Mass Erase**] option at address 0x10040000 and then the BlueNRG2_OTA binary or any other binary which needs to be upgraded at address 0x10051800 by un-selecting the [**Mass Erase**] option (OTA Service Manager will be deleted, if Mass Erase option is enabled).

Step 4b. To keep the credentials of the last provisioned node even after updating the firmware, use Service Manager - OTA_ServiceManager_WithCred_32MHz binary available at path BlueNRG2_OTA from Embedded\Projects\BlueNRG-2\Applications\Lighting_Demo\Binary.

Step 4c. When using BlueNRG-M2SP or BlueNRG-M2SA module, refer to the related datasheet.

Revision history

Table 2. **Document revision history**

Date	Version	Changes
01-Mar-2021	1	Initial release.

Contents

List of tables

List of figures

IMPORTANT NOTICE – PLEASE READ CAREFULLY

STMicroelectronics NV and its subsidiaries (“ST”) reserve the right to make changes, corrections, enhancements, modifications, and improvements to ST products and/or to this document at any time without notice. Purchasers should obtain the latest relevant information on ST products before placing orders. ST products are sold pursuant to ST’s terms and conditions of sale in place at the time of order acknowledgement.

Purchasers are solely responsible for the choice, selection, and use of ST products and ST assumes no liability for application assistance or the design of Purchasers’ products.

No license, express or implied, to any intellectual property right is granted by ST herein.

Resale of ST products with provisions different from the information set forth herein shall void any warranty granted by ST for such product.

ST and the ST logo are trademarks of ST. For additional information about ST trademarks, please refer to www.st.com/trademarks. All other product or service names are the property of their respective owners.

Information in this document supersedes and replaces information previously supplied in any prior versions of this document.

© 2021 STMicroelectronics – All rights reserved