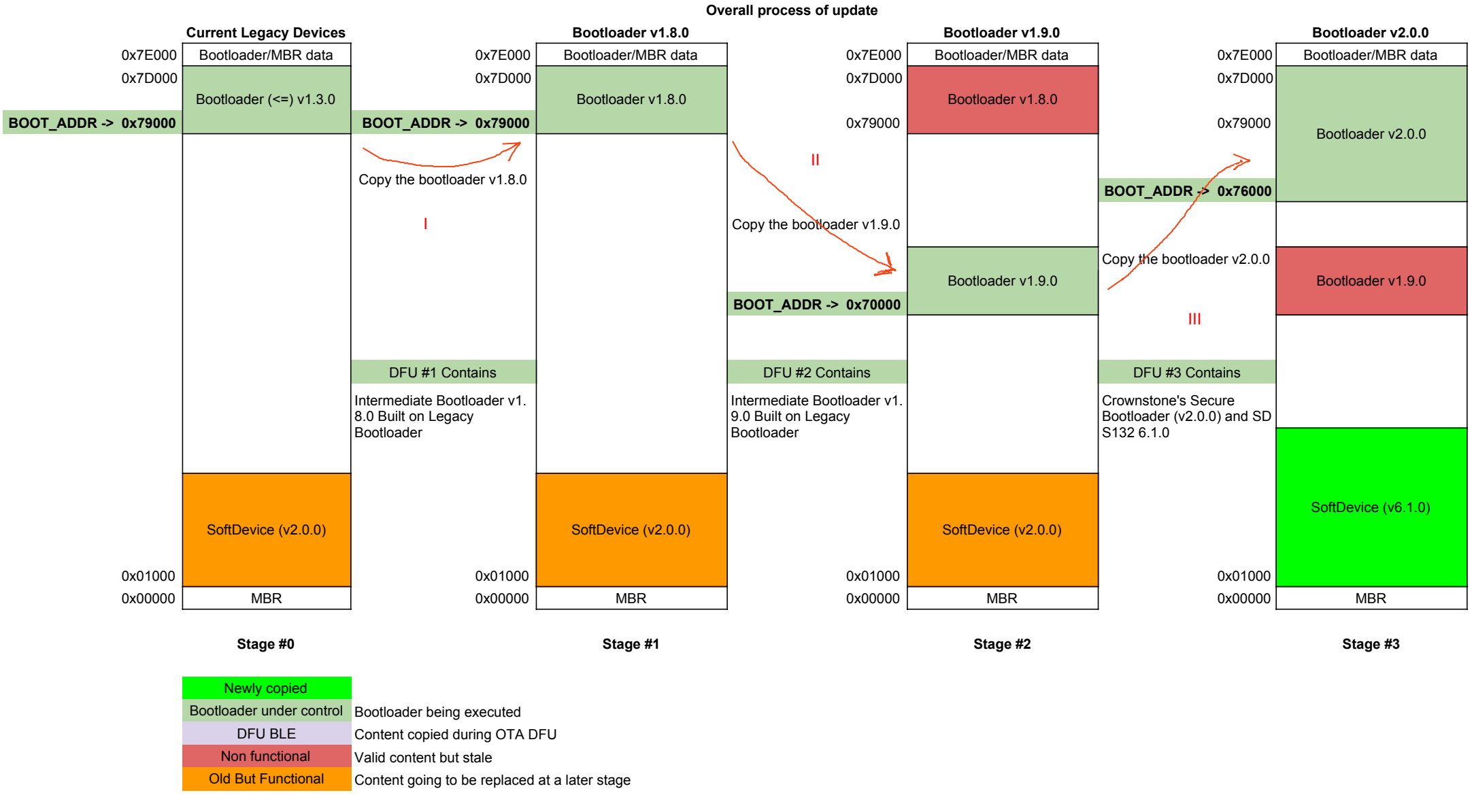
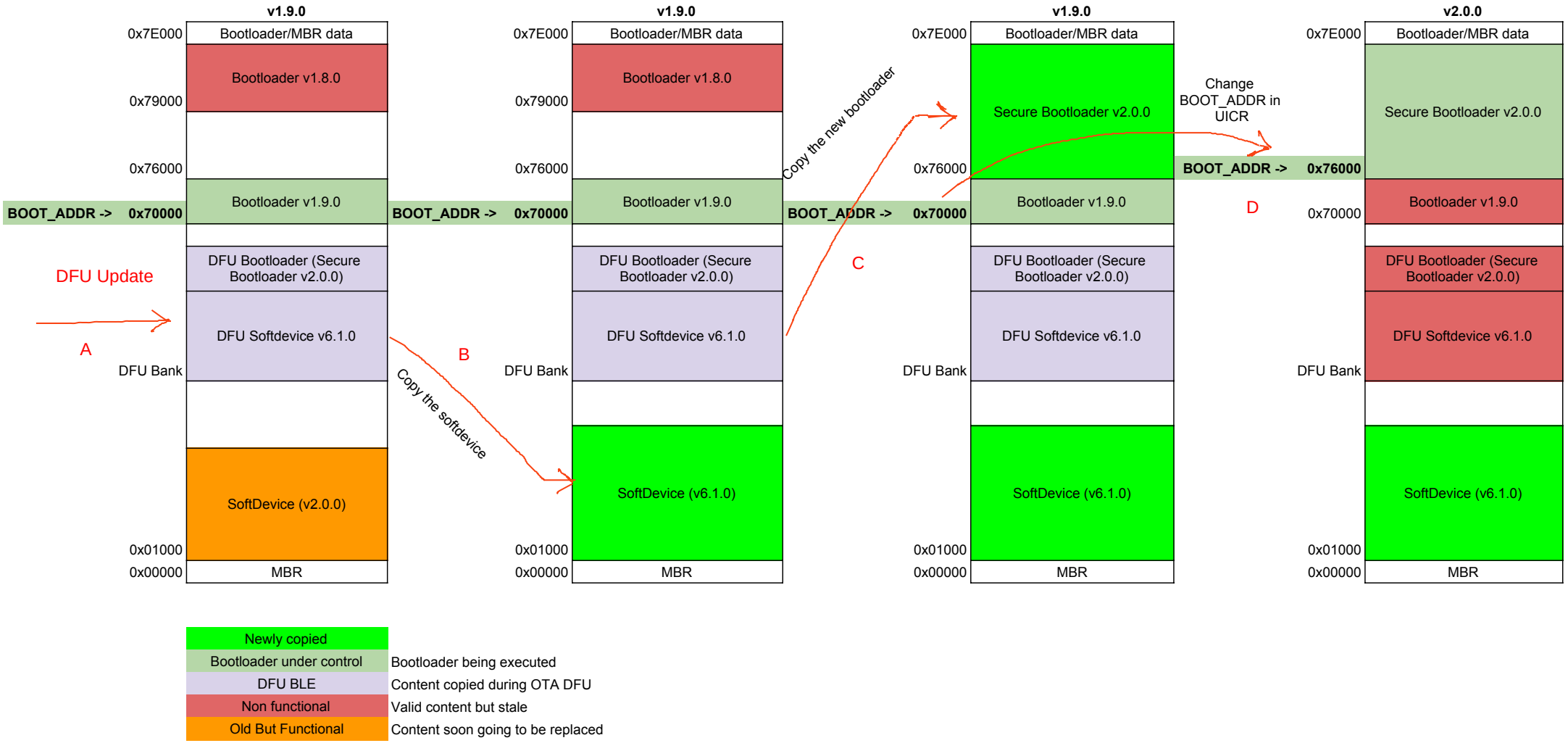

Overall process of update
Current Legacy Devices
Bootloader v1.8.0
Bootloader v1.9.0
Bootloader v2.0.0
0x7E000
0x7D000
0x79000
0x01000
0x00000
Bootloader/MBR data
Bootloader (<=) v1.3.0
BOOT_ADDR -> 0x79000
SoftDevice (v2.0.0)
MBR
Stage #0
Copy the bootloader v1.8.0
I
DFU #1 Contains
Intermediate Bootloader v1.8.0 Built on Legacy Bootloader
Bootloader v1.8.0
Stage #1
II
Copy the bootloader v1.9.0
BOOT_ADDR -> 0x70000
DFU #2 Contains
Intermediate Bootloader v1.9.0 Built on Legacy Bootloader
Bootloader v1.9.0
Stage #2
BOOT_ADDR -> 0x76000
Copy the bootloader v2.0.0
III
DFU #3 Contains
Crownstone's Secure Bootloader (v2.0.0) and SD S132 6.1.0
Bootloader v2.0.0
SoftDevice (v6.1.0)
Stage #3
Newly copied
Bootloader under control
Bootloader being executed
DFU BLE
Content copied during OTA DFU
Non functional
Valid content but stale
Old But Functional
Content going to be replaced at a later stage

#	Process	Vulnerable	Time Taken	Failure Consequence	DFU Content	Current Boot addr
I	The bootloader (v1.8.0) is copied to the same old address (0x79000)	No	~10 secs	Will fail to write the new bootloader	Bootloader v1.8.0	0x79000
II	The bootloader v1.9.0 is sent through the DFU to be copied at 0x70000.	No	~10 secs	Will fail to copy and set control to the new control, while the control is still at 0x79000.	Bootloader v1.9.0	0x70000
III	The secure bootloader v2.0.0 along with the softdevice v6. 1.0 is copied to 0x76000 and 0x1000 respectively.	No	~25 secs	* evaluated in a separate table	Bootloader v2.0.0 + Softdevice v6.1.0	0x76000

Intermediate steps when executing the bootloader v1.9.0 (regions in the images are not to scale)



Newly copied	
Bootloader under control	Bootloader being executed
DFU BLE	Content copied during OTA DFU
Non functional	Valid content but stale
Old But Functional	Content soon going to be replaced

#	Process	Vulnerable	Time Taken	Failure Consequence	Current Boot addr
A	The combined package of Softdevice v6.1.0 + Secure Bootloader v2.0.0	No	~25 secs	Will corrupt the data present in the DFU bank. A fresh copy would be placed during the later update as the bootloader v1.9.0 is still functional.	0x70000
B	The new Softdevice v6.1.0 is copied into its region 0x1000	No	~3-4 secs	Will fail to copy the new softdevice corrupting the current softdevice. However, the copy operation would be retried as the bootloader v1.9.0 is still operational (without the BLE Stack; disabling it to receive new updates)	0x70000
C	The new secure bootloader (v2.0.0) is copied into the address 0x76000	No	< 500 ms	Will fail to copy the new bootloader. However, the copy operation would be retried as the bootloader v1.9.0 at 0x70000 is still operational.	0x70000
D	The BOOTLOADER ADDR in the UICR region is set to 0x76000	No	< 100 ms	Will fail to transfer the control to the new bootloader. However, the address set operation would be retried as the bootloader v1.9.0 at 0x70000 is still operational	0x76000