Segway G3 Max VCU Memory Dump and Modification Tutorial

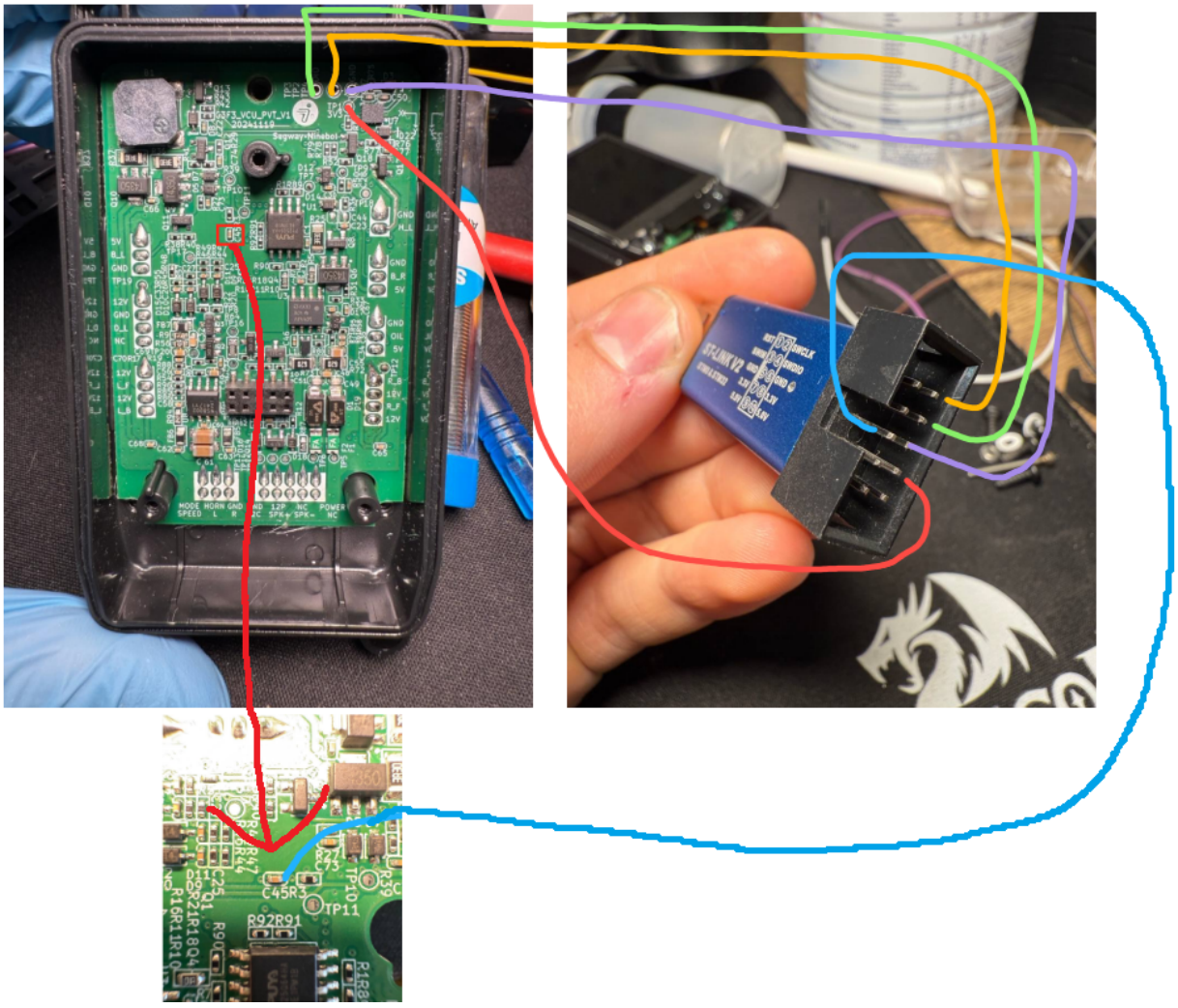
Prerequisites

- ST-Link programmer
- Target VCU board
- Computer with dump_memory.bat, fix_cpu.exe, and flash_memory_patched.bat files

Step-by-Step Guide

1. Initial Connection

1. Connect all pins from the ST-Link to the board **except pin 5**



2.

2. Prepare for Memory Dump

2. Short ST-Link pin 5 to the C45 capacitor on the board

3. Dump Memory

3. Execute dump_memory.bat script
4. When you see a specific line in the output (not specified which one), release the connection to the C45 capacitor

4. Verify Dump

5. After completion, you should see a MEMORY_G3.bin file appear in the same directory as your dump_memory.bat
6. Please verify that the MEMORY_G3.bin file is around 128kb

5. Modify Memory Contents

6. Execute fix_cpu.exe
7. When prompted:
    - Enter a speed value between 1 and 255 (example shows 255)
    - Enter Y or N to change the serial number region to US (Y for yes, N for no)

6. Patching Process

The program will:

- Delete any existing MEMORY_G3.bin_patched_bin file
- Create a new patched copy
- Write your speed value to multiple memory addresses
- If selected, write the US region code (0x43) to the serial number location

7. Flash Modified Memory

8. Again short ST-Link pin 5 to the C45 capacitor
9. Execute flash_memory_patched.bat
10. Release the capacitor connection when prompted (same as step 4)
11. dump is completed only when you see this. Try again if not

```
[stm32f1x.cpu] halted due to debug-request, current mode: Thread
xPSR: 0x01000000 pc: 0x0800020c msp: 0x20000890
stm32x mass erase complete
wrote 131072 bytes from file MEMORY_G3.bin.patched.bin to flash bank 0 at offset 0x00000000 in 3.472439s (36.862 KiB/s)
DEPRECATED! use 'read_memory' not 'mem2array'
Error executing event examine-end on target stm32f1x.cpu:
oocd/scripts/mem_helper.tcl:37: Error: wrong # args: should be "expr expression"
in procedure 'ocd_process_reset'
```

Important Notes

- The exact line when you should release the capacitor isn't specified in the document
- The mathematical formulas shown in the document appear to be decorative rather than functional
- The addresses shown (0xIF08D, etc.) appear to be example addresses with some obfuscation (note the "I" where you might expect "1")
- Always ensure proper connections and follow safety procedures when working with vehicle control units

Completion

Once the flash process completes successfully, the modification is complete and you can disconnect all programming equipment.