makefile

A screenshot of a computer program

Description automatically generated

main.c

A screenshot of a computer code

Description automatically generated

Part1: startup.s

A screenshot of a computer program

Description automatically generated

linker\_script.ld

A screenshot of a computer code

Description automatically generated

map\_file.map

A screenshot of a computer program

Description automatically generated

=28B

A number of numbers on a white background

Description automatically generated with medium confidence

A number and numbers in a row

Description automatically generated with medium confidence

Disassembly of .elf file

A screenshot of a computer code

Description automatically generated

* 0x20001000 stored @0x08000000 in FLASH, Initialize SP @0x20001000.
* 0x080000098 stored @0x08000004 in FLASH, 0x080000098 is \_reset handler address.
* From 0x080000008 to 0x080000018 which is 28B is our vector table, 0x0800009f is stored in all of them, 0x0800009f is vector\_handler address, now we know that vector\_handler is alias for 5 handlers.
* Now expected that at runtime CPU go to entry point at 0x08000000 and initialize SP then go to 0x08000004 which branch execution to \_reset @0x08000098 and \_reset will branch execution to main @0x0800001c.
* Now expected that main instructions start @0x0800001c and ends @0x08000094 then\_reset starts @0x08000098 and ends @0x0800009c then vector\_handler starts.
* The question here is the address of vector\_handler is 0x0800009e and the vector section stores 0x0800009f which is after one byte of 0x0800009e, and the instruction itself e7fb takes 2 bytes which supposed be 0x0800009fe and 0x0800009f
* I tried to debug using QEMU, but the debugger cannot show what happens since it don’t stop at breakpoints unless complete the interrupt handler

A screenshot of a computer

Description automatically generated

A screenshot of a computer code

Description automatically generated

Part2: startup.c

Without alias:

A screenshot of a computer code

Description automatically generated

linker\_script.ld

A screenshot of a computer code

Description automatically generated

map\_file.map

A screen shot of a computer program

Description automatically generated

A number of numbers on a white background

Description automatically generated

A number and numbers on a white background

Description automatically generated

* Each fault handler has its own address.

Disassembly of .elf file

A computer code with colorful text

Description automatically generated with medium confidence

A screenshot of a computer code

Description automatically generated

A screenshot of a computer code

Description automatically generated

With alias:

A screenshot of a computer code

Description automatically generated

linker\_script.ld

A screenshot of a computer code

Description automatically generated

map\_file.map

A screenshot of a computer program

Description automatically generated

A number of numbers on a white background

Description automatically generated

A number and numbers on a white background

Description automatically generated

* All of fault handlers have the same address of Default\_handler, since all of them are alias for Default\_handler

Disassembly of .elf file

A screenshot of a computer code

Description automatically generated

A screenshot of a computer

Description automatically generated



A screenshot of a computer code

Description automatically generated

Part3: startup.c (alias & .data & .bss)

main.c

A screenshot of a computer code

Description automatically generated

startup.c

A computer screen shot of a program

Description automatically generated

A screen shot of a computer code

Description automatically generated

linker\_script.ld

A screenshot of a computer program

Description automatically generated

map\_file.map

A screenshot of a computer

Description automatically generated

A screenshot of a computer screen

Description automatically generated

* \*fill\* of 1B is for Alignment, the size of global initialized variable is 3B.

A screenshot of a computer code

Description automatically generated

* The size of initialized struct taken by the 8 because of auto alignment in C structures.

sections of .elf file

A computer screen shot of a black screen

Description automatically generated

Symbols of .elf file

A screenshot of a computer program

Description automatically generated

