Following are few bullet points about the WEAK Symbol Bug:

1>

Here is the BL Instruction in ARM Mode is supposed to work:

BL **24-Bit Signed OFFSET Destination Address [4-Byte Aligned]**

2>

In the current MAP file [dbcBootCAN_BUG.map], you will see that “Delay_Before_PLL_Setup” is at 0x60 address.

3>

Similarly, in the current MAP file [dbcBootCAN_BUG.map], you will see that “WEAK_Symbol_Call_Bug” is at 0x1DC address.

4> So, the BL instruction destination should be:

(0x60 – 0x1E4)/4 = 0xFFFFFF9F [Signed Subtraction]

0x1DC + 8 = 0x1E4 because of ARM7 Prefetch value of PC, which is 2 instruction ahead always.

Divide by 4 above because BL Instruction OFFSET is always WORD Aligned [32-Bit].

5>

Hence, the expected value at address 0x1DC within HEX file output should be:

0xEBFFFF9F, where

0xEB is opcode for “BL Always” instruction

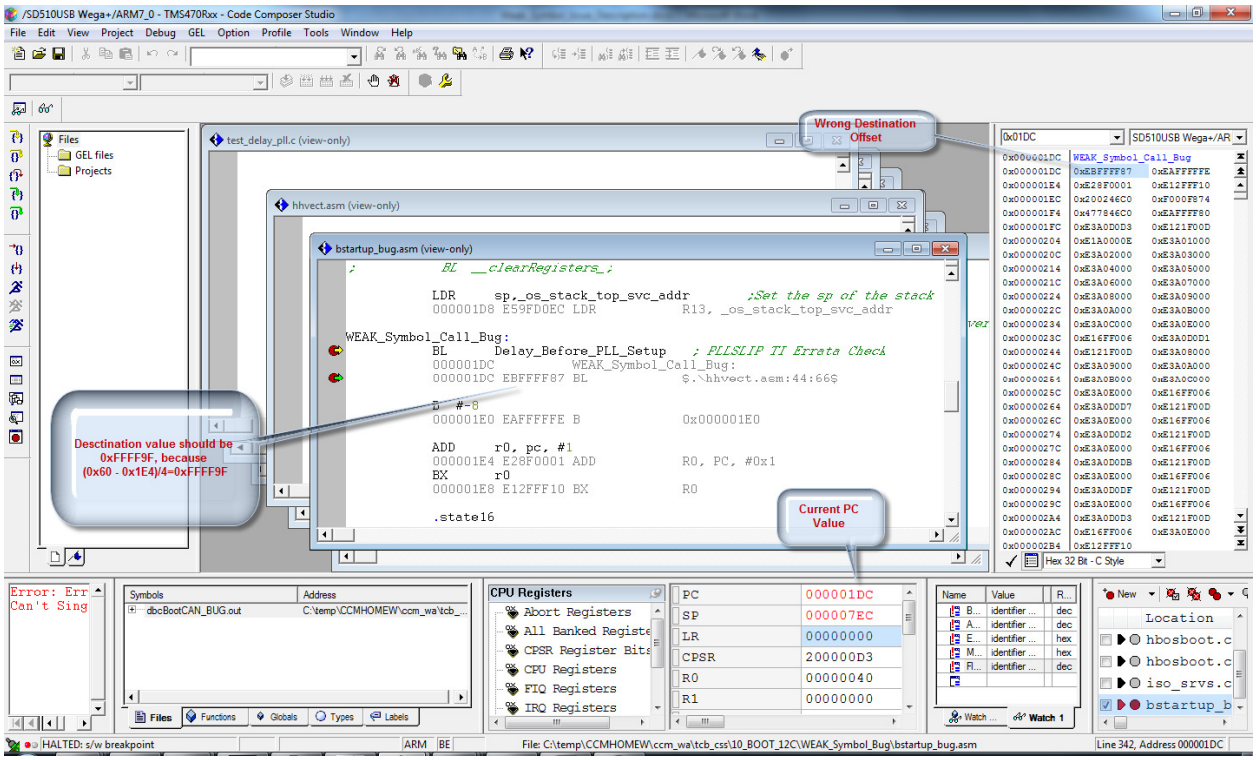
0xFFFF9F is destination offset [signed]

6> In the HEX file at that address you will see instead

0xEBFFFF87

6> The problem is in dbcBootCAN_BUG.out file and not within dbcBootCAN_BUG.hex file as I have loaded dbcBootCAN_BUG.out file in debugger and verified the result.

7> Shown below is the Code Composer Dump during “BL Delay_Before_PLL_Setup” instruction, when I loaded dbcBootCAN_BUG.out file into the ARM7TDMI CPU and ran it.



8> Below is a snapshot of dbcBootCAN_BUG.hex, showing the wrong OFFSET Address for "BL Delay_Before_PLL_Setup" instruction as present within bstartup_bug.asm file.