MU Restore FW

1. Root cause

In most cases, HSE FW erased caused by incorrect clock configuration. The proper operation of the HSE subsystem depends on the correct configuration of the clocks CORE_CLK, HSE_CLK, AIPS_SLOW_CLK, AIPS_PLAT_CLK, etc. Therefore, users need to follow the 23.7.2 clock option in the S32Kxx-RM, otherwise the HSE may not operate properly, or even HSE FW will be erased.

But I also found some other case, like clear FES-POR without DCF record config (K312), K312 enable “PLL_ENABLE” in IVT.

More detail can refer to S32K3-RM and HSE-RM, I also write mention this in HSE QSG.

Full mem firmware recovery is similar to AB swap, you can refer to
[S32K3 HSE installation using MU Interface - NXP Community]

2. Prepare

Need to prepare a HSE FW install project to download the firmware to FLASH, and then add a loop, avoid running the program to another location, click “**run**” in debug window each time after writing to the MU RR/TR register

3. HSE handshake mechanism

After POR, the MU -FSR reg all “0”, the HSE is not working

Check the HSE GPR

14.2.6.2 HSE GPR Register 3

Secure BAF updates status bits on HSE GPR Register 3 (0x4039C028) as explained in below table.

Table 136: Status Bits on HSE GPR Register 3 (0x4039C028)

Bit #	Description
31…	Reserved
5	Application cores booted in Recovery mode by SBAF.
4	No HSE Firmware is present in Device due to Erase performed by SBAF Handshake logic. This bit resets on presence of valid HSE Firmware.
3	HSE Firmware from Data flash area is erased by SBAF Handshake logic in current reset cycle.
2	HSE Firmware from code flash area is erased by SBAF Handshake logic in current reset cycle.
1	MU interface is enabled for installation of HSE Firmware.
0	HSE FW is present and SBAF Booted HSE Firmware

HSE_B Firmware Reference Manual, Rev 1.2, 01/2022

NXP Semiconductors 209

And the HSE GPR 3 register bit 0 is also 0 (normal should be 0x00000001), so it is obvious that the firmware is automatically erased by SBAF through the handshake mechanism.

Handshake mechanism in HSE-RM,

14.2.5 HSE Firmware Handshake

相互依赖的 防止变砖

Secure BAF and HSE Firmware have interdependent handshake mechanism which prevents bricking of device by erasing the erroneous or corrupted HSE Firmware and re-install new HSE Firmware . The Handshake mechanism is only functional over functional resets.

重新安装新的FW

擦除损坏的FW 要退出 shutdown mode 需主机 reset the device

HSE Firmware sets the status as successful after the device is successfully booted. In case, there is some major corruptions in the device, during its initialization flow, the device goes into shutdown mode only after the setting the handshake status as failure. 设置 握手状态 为 失败 FW 禁用所有中断进入 非操作 状态, 并最终进入 sleep mode

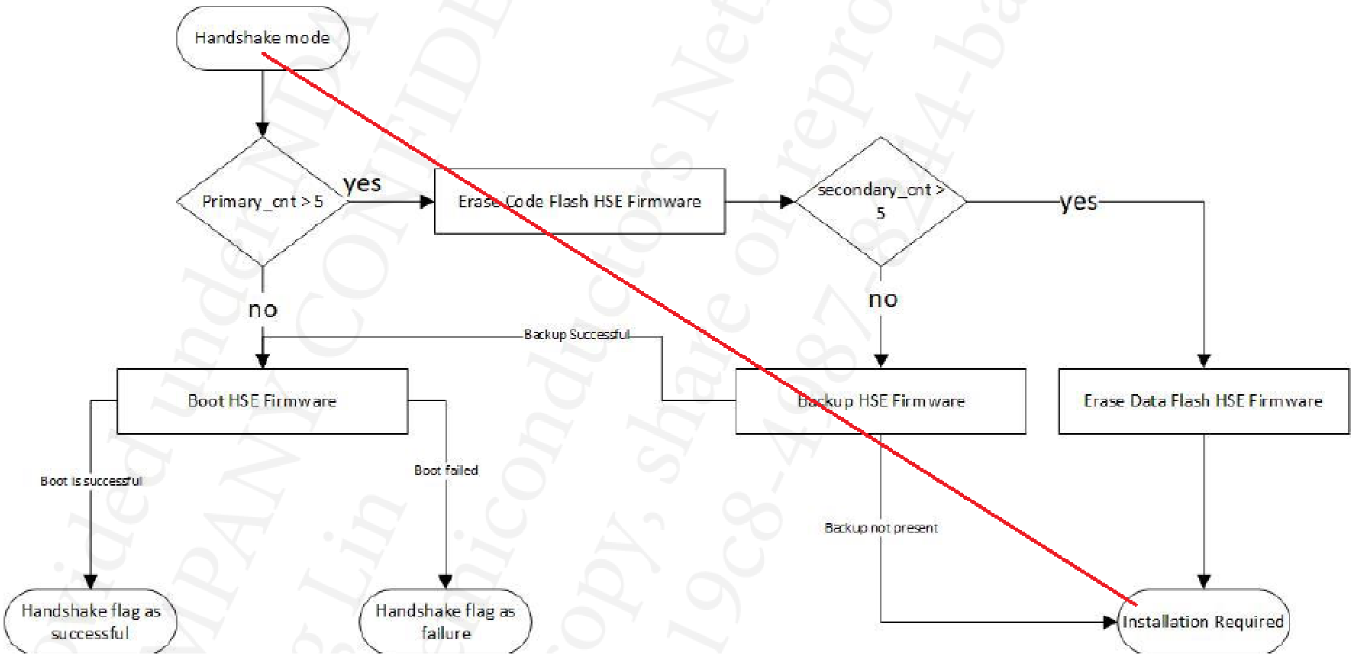
万一有重大损坏 由于中断禁用, 主机无法向 HSE FW 请求任何服务

In case, the user does not see the HSE_STATUS_INIT_OK set, the user is requested to assert a functional reset. The handshake mechanism is designed to repeat this process for 5 times. In case, the device is not booted even after the 5 resets, Secure BAF erases the HSE Firmware in the code flash location.

In case, the code flash firmware is attempted to boot 5 times, the primary counter value is set > 5. If the primary counter is set > 5 then, HSE Firmware is erased from the code flash. The status of firmware erase is set in HSE GPR (Register 3 (0x4039C028), refer chapter Hardware Security Engine (HSE_B) from [**REF02**]). In the same reset-cycle, Secure BAF checks if the valid backup firmware is present.

If valid backup firmware is present, it restores the firmware to code flash and retries booting the firmware. In case, the data flash firmware also has major defect/corruptions, which leads to HSE Firmware going into shutdown, the user is requested to assert functional resets which is the similar process as of code flash. This needs to be repeated for data flash firmware. In case, the data flash firmware is attempted to boot 5 times, the secondary counter value is set > 5. If the secondary counter is set > 5 then, HSE Firmware is erased from the code flash as well as data flash. The status of firmware erase is set in HSE GPR (Register 3 (0x4039C028), refer chapter Hardware Security Engine (HSE_B) from [**REF02**]). If no HSE Firmware is present in the device, the user needs to install the firmware as mentioned in "HSE Firmware Installation" chapter.

Figure 63: High level flow of HSE Firmware Handshake



11.2.1 HSE shutdown mode

Due to any error or tamper event in HSE subsystem, the firmware enters non-operational state by disabling all the interrupts and finally enters sleep mode. As the interrupts are disabled, the host cannot request any service to HSE Firmware. To exit the shutdown mode, the host needs to reset the device.

4. Using install HSE FW via mu interface to recover FW

In HSE RM:

4.2.3 Installation via MU interface

This method provides flexibility to install HSE firmware by placing encrypted FW-IMG at system RAM. HSE firmware can be installed via programming encrypted FW-IMG in code flash or in System RAM memory and the start address of encrypted FW-IMG must be provided via MU channel 0 interface by application.

To enable installation via MU interface, Host application must write bits 24th -31th of DCM Register (DCMRWP1 0x402AC400) with value 0xA5. On next functional reset, Secure BAF enables HSE Firmware installation via MU interface and sets HSE GPR (0x4039C028) bit 1th to indicate installation state machine is executing. Secure BAF transmits response over MU channel 0 to confirm installation of HSE Firmware then Host application transmits expected response within the timeout period. This sequence is mentioned in next flow chart.

APP 写 0xA5 后请求 functional reset, SBAF 就会启动 FW(MU) 安装, 此时 APP 需提供相应 response 至 SBAF 选择安装类型

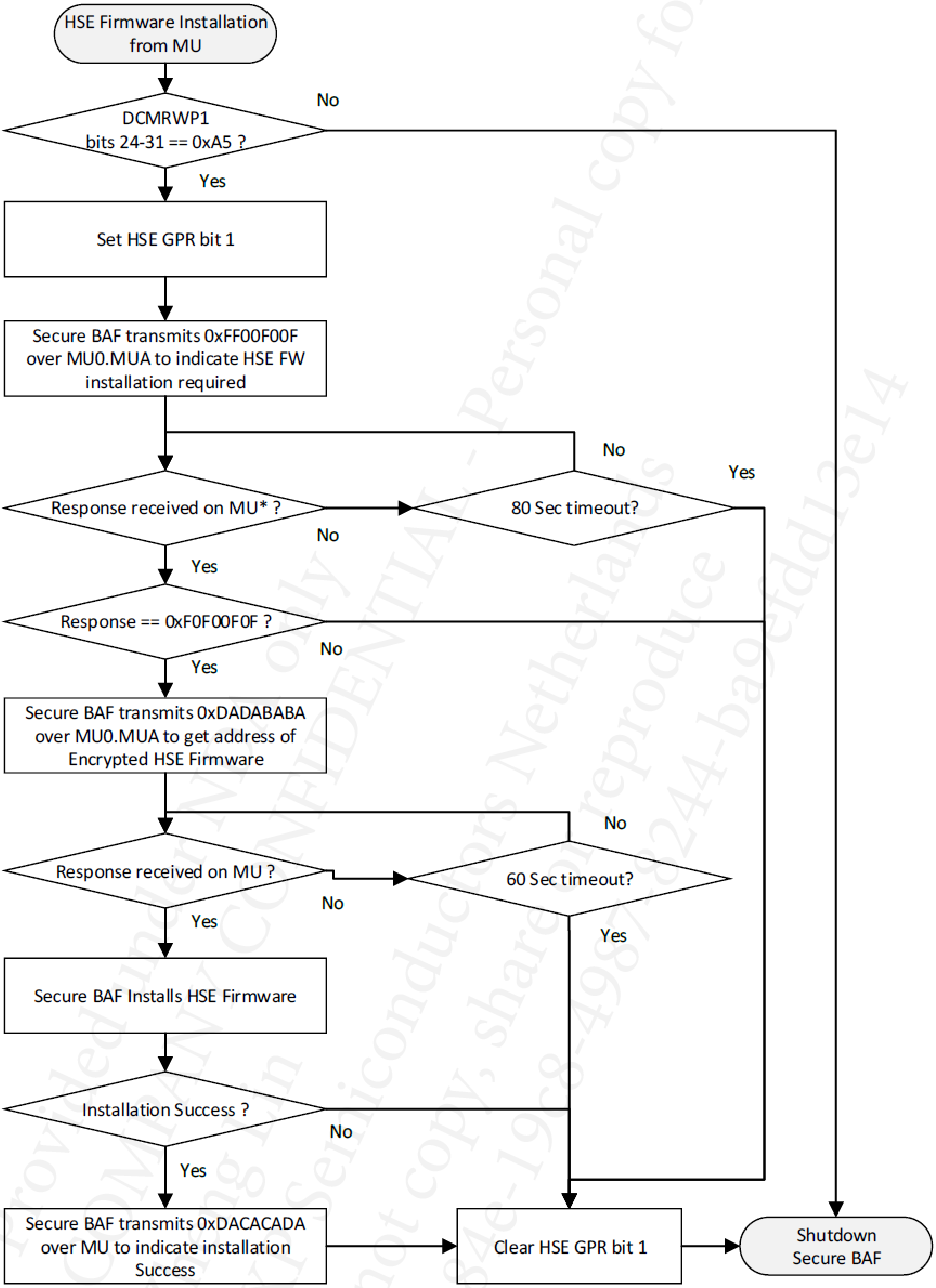
Below figures explains installation of HSE Firmware via programming encrypted FW-IMG and using MU interface.

Magic number using in flow chart

1. ABSWAP MU code for HSE Firmware installation during handshake state machine

Magic Values	Transmitted by	Description	Expected Response
0xAA55A55A	SBAF	Secure BAF confirms these two operations can be performed: 1. Switching of active and passive flash partition OR 2. Installation of New HSE Firmware	1. Switching: 0x5A5AA5A5 2. Installation: 0xF0F00F0F
0xFF00F00F	SBAF	Secure BAF confirms only installation can be performed	0xF0F00F0F
0xDADABABA	SBAF	Secure BAF asks for HSE Firmware pointer which has to be installed.	Pink Image pointer Eg: 0x00420000
0xDABABADA	SBAF	Switching of Active to Passive Code flash partition is Successful. Reset is required.	NA
0x5A5AA5A5	APP Core	Application confirms for Switching	Switching Success Status 0xDABABADA
0xF0F00F0F	App core	Application confirms for Installation of new HSE FW.	HSE FW Pointer 0xDADABABA

Figure 19: Installation steps via MU interface in FULL_MEM configuration



*App core transmits response over MU Channel 0 (MU0.MUB)

然后是 AB_SWAP FW 的安装流程，可以看到更加复杂，但按照下面的步骤执行，经过验证，是可以恢复 AB_SWAP FW 的。

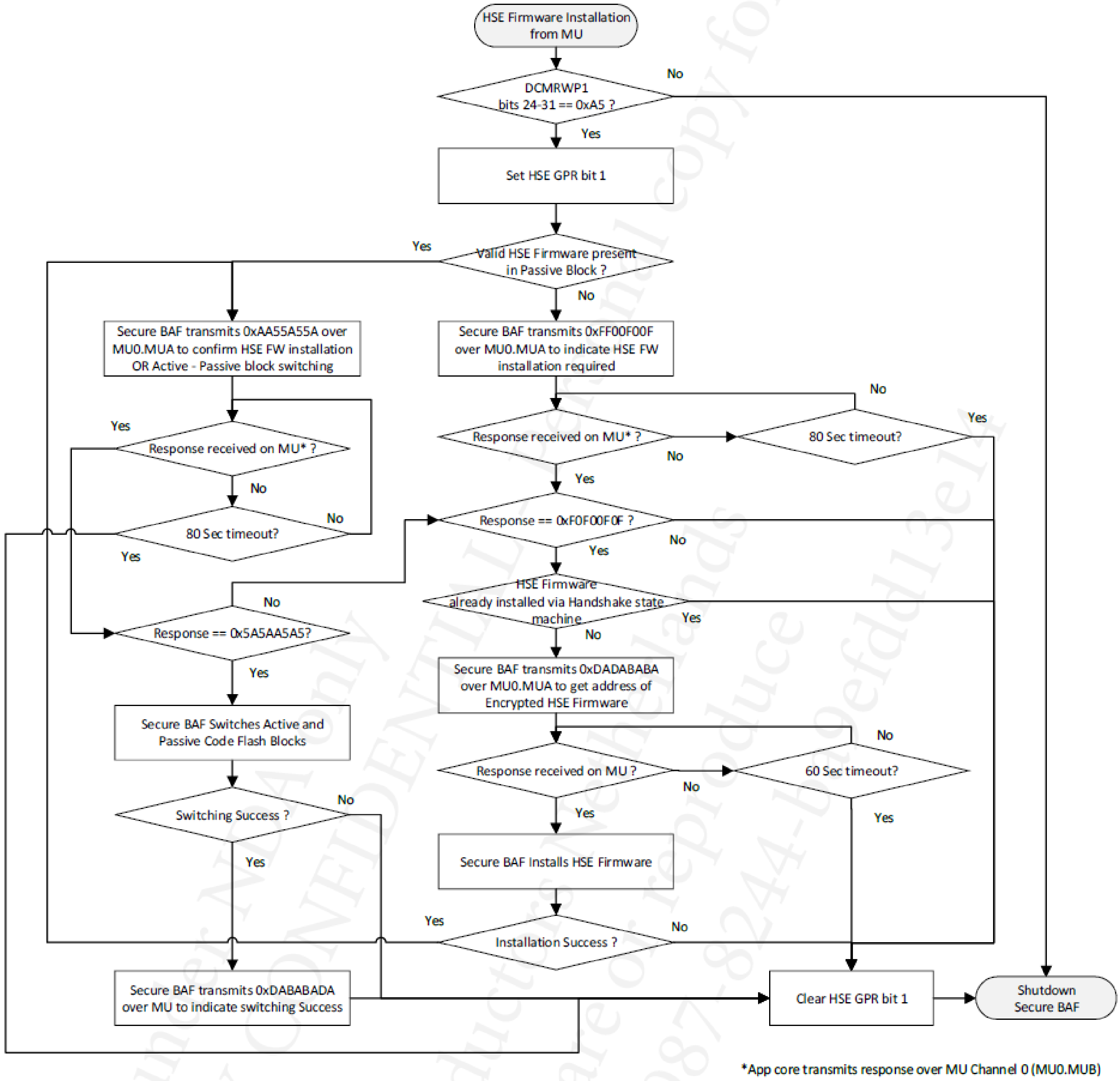
4.3 Installation process in AB_SWAP configuration

In this case, the need to install the firmware is required when firmware gets erased by SBAF because of some issue in firmware as explained in the section "HSE Firmware Handshake". There is only one option through which HSE Firmware can be installed which is "Installation via MU interface".

If HSE firmware is not present in passive block then, HSE Firmware can be installed as "Installation via MU interface" in passive block. And if HSE firmware is already present in passive block or if it is installed via MU interface then active – passive block switching is allowed via MU interface.

To enable installation via MU interface, Host application must write bits 24th -31th of DCM Register (DCMRWP1 0x402AC400) with value 0xA5. On next functional reset, Secure BAF enables HSE Firmware installation/active -passive block switching via MU interface and sets HSE GPR (0x4039C028) bit 1th to indicate installation state machine is executing. Secure BAF transmits response over MU channel 0 to confirm installation of HSE Firmware then Host application transmits expected response within the timeout period. This sequence is mentioned in below flow chart.

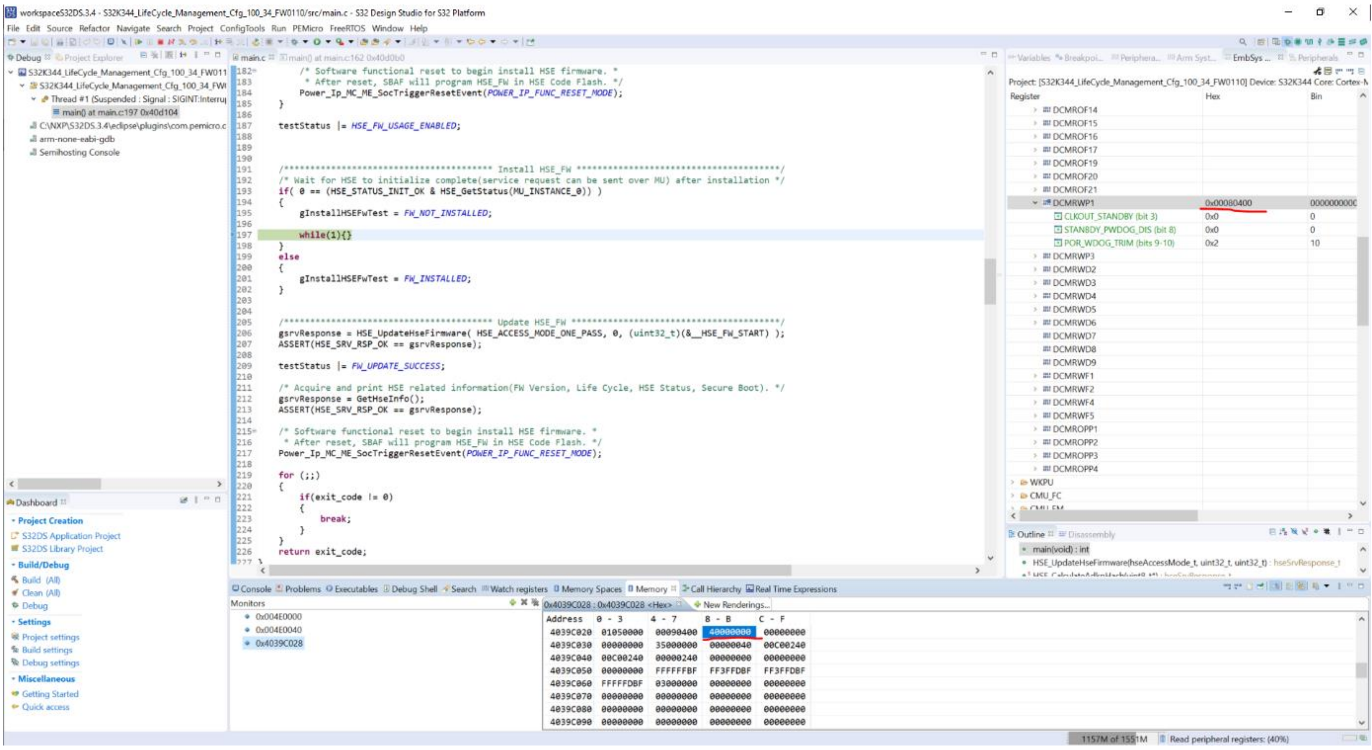
Figure 20: Installation steps via MU interface in AB_SWAP configuration



5. recovery steps (ab swap)

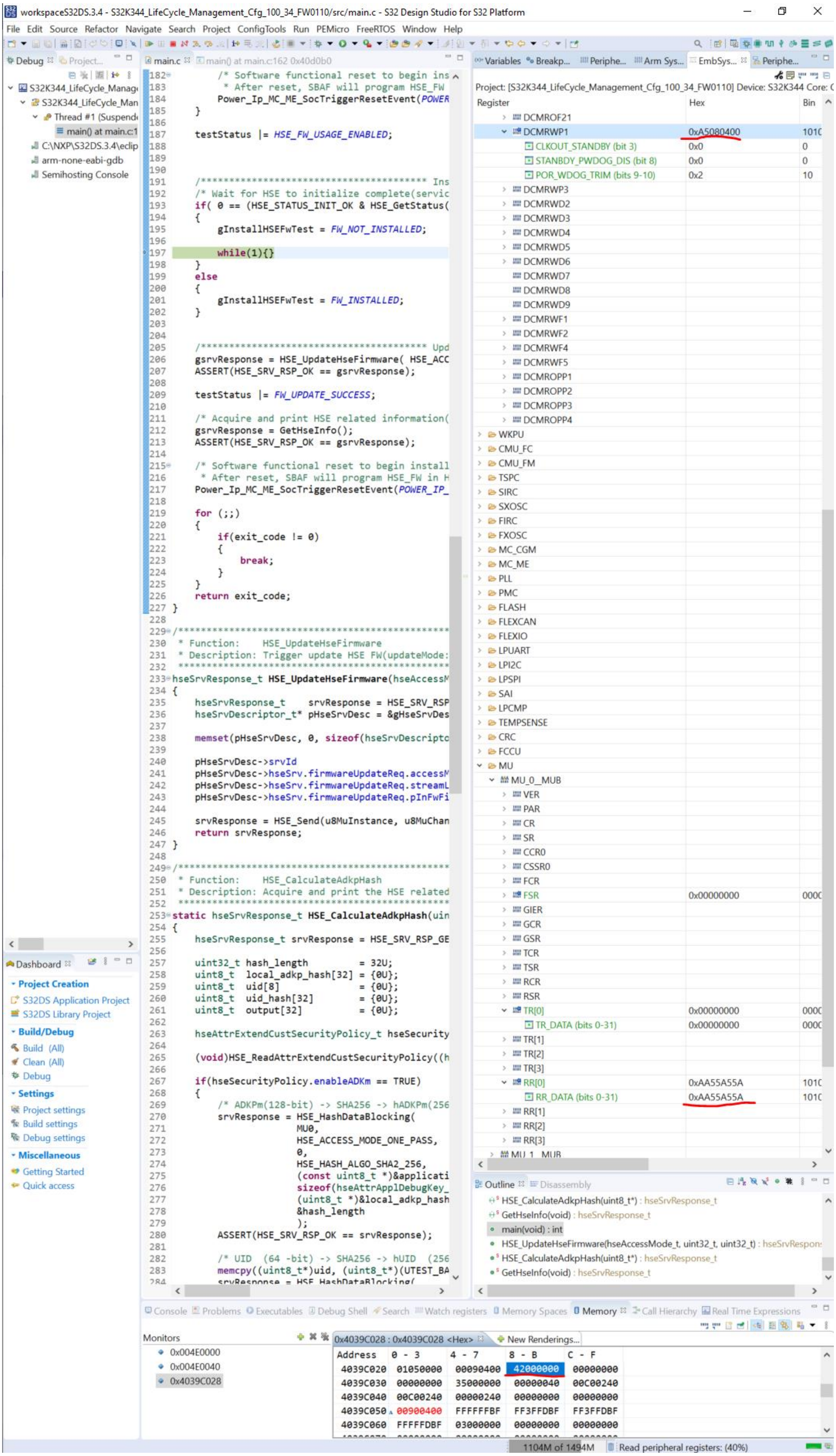
5.1 before start handshake

The bits 24-31 of DCMRWP1 register are all 0 by default, and bits 0-4 in 0x4039C028 are all 0 at this time, the FW Installation Process (MU) process is not started.



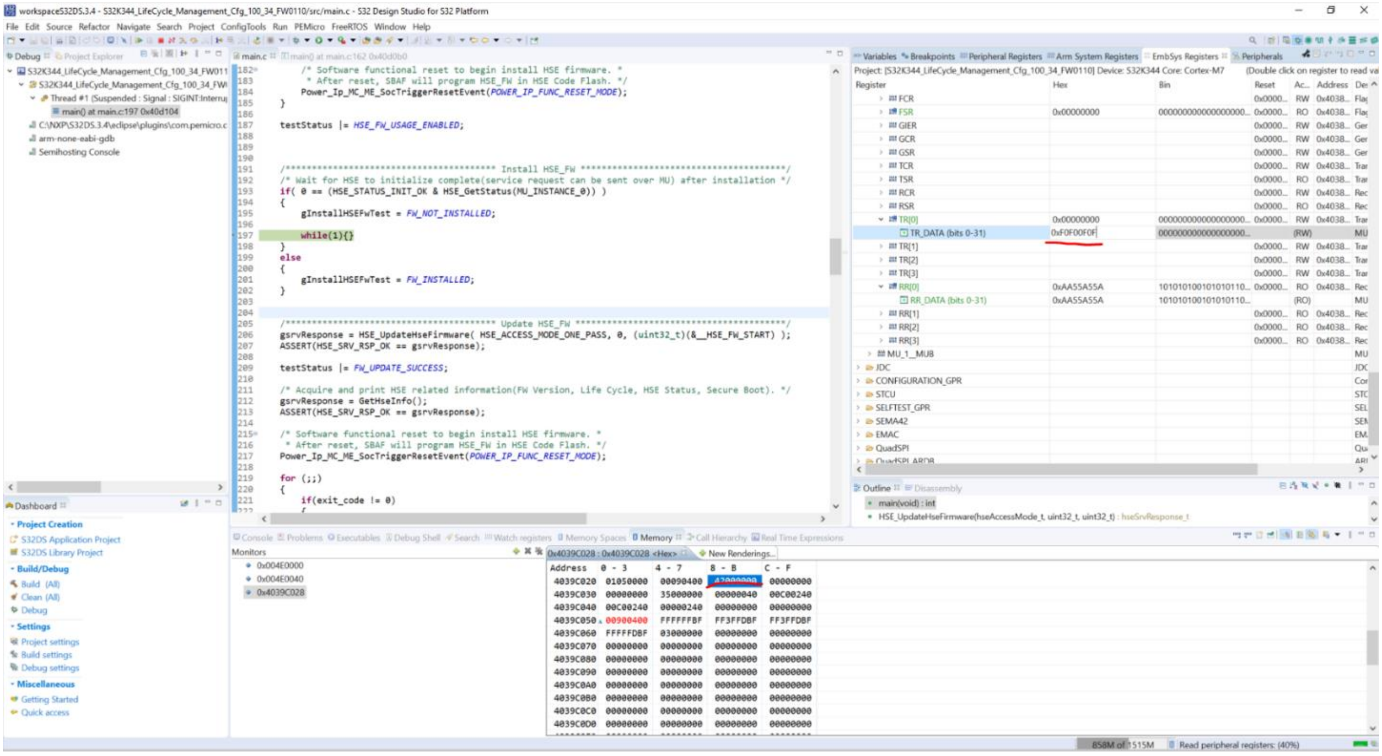
5.2 start handshake
Write A5 to bits 24-31 of DCMRWP1 register, click “run” and “stop”, the HSE GPR 3 bit 1 assertion (MU interface is enabled for installation of HSE Firmware.),

Meanwhile, **HSE** sends 0xAA55A55A to **M7 core** via MU0-**MUA** TR0, and the value can be viewed via MU0-**MUB** RR0, at the value can see from debug window

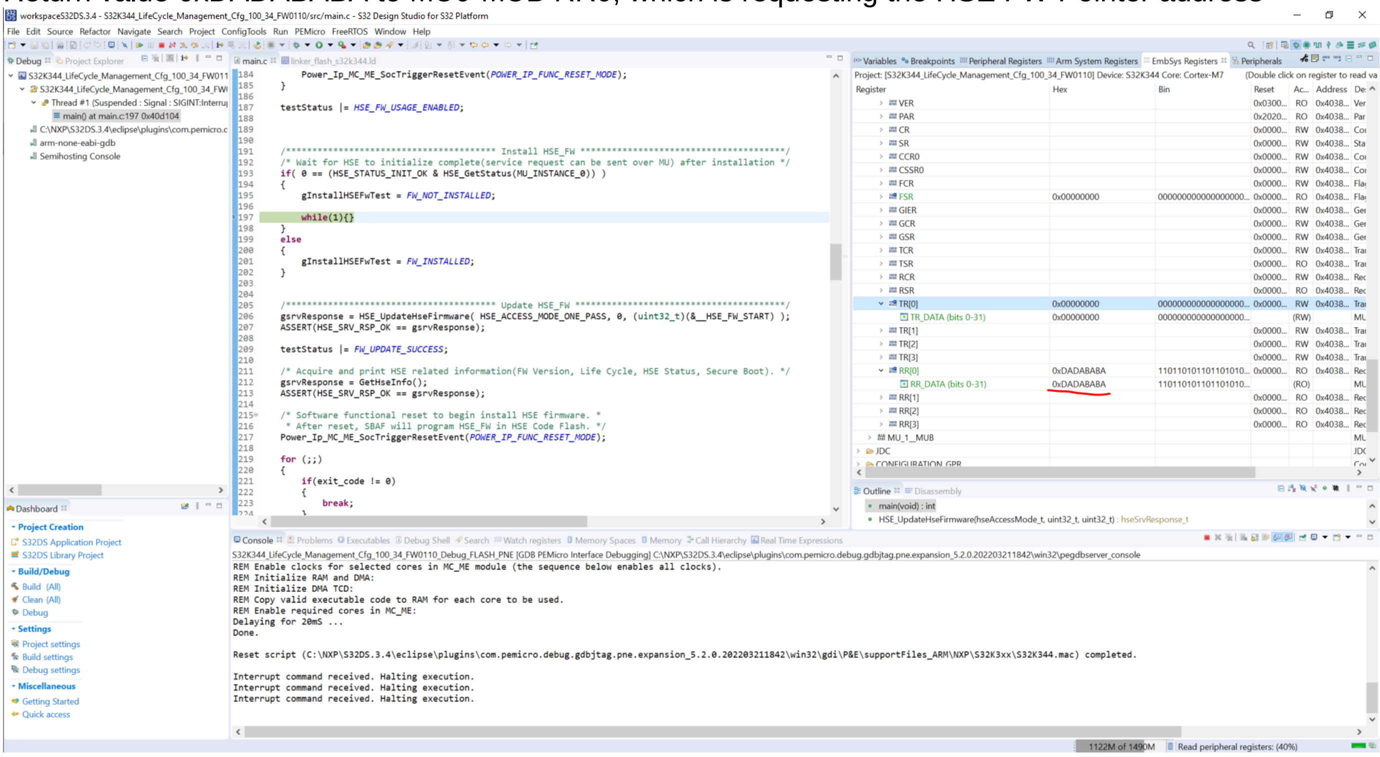

workspaceS32DS.3.4 - S32K344_LifeCycle_Management_Cfg_100_34_FW0110/src/main.c - S32 Design Studio for S32 Platform
File Edit Source Refactor Navigate Search Project ConfigTools Run PEMicro FreeRTOS Window Help
Debug
Thread #1 (Suspended)
main() at main.c:1
arm-none-eabi-gdb
Semihosting Console
main.c
main() at main.c:162 0x40d0b0
/* Software functional reset to begin ins
* After reset, SBAF will program HSE_FW
Power_Ip_MC_ME_SocTriggerResetEvent(POWER
testStatus |= HSE_FW_USAGE_ENABLED;
/* Wait for HSE to initialize complete(servic
if(0 == (HSE_STATUS_INIT_OK & HSE_GetStatus(
gInstallHSEFwTest = FW_NOT_INSTALLED;
while(1){}
else
gInstallHSEFwTest = FW_INSTALLED;
gsrvResponse = HSE_UpdateHseFirmware(HSE_ACC
ASSERT(HSE_SRV_RSP_OK == gsrvResponse);
testStatus |= FW_UPDATE_SUCCESS;
/* Acquire and print HSE related information(
gsrvResponse = GetHseInfo();
ASSERT(HSE_SRV_RSP_OK == gsrvResponse);
/* Software functional reset to begin install
* After reset, SBAF will program HSE_FW in H
for (;;)
if(exit_code != 0)
break;
return exit_code;
* Function: HSE_UpdateHseFirmware
* Description: Trigger update HSE FW(updateMode:
hseSrvResponse_t HSE_UpdateHseFirmware(hseAccessM
hseSrvResponse_t srvResponse = HSE_SRV_RSP
hseSrvDescriptor_t* pHseSrvDesc = &gHseSrvDes
memset(pHseSrvDesc, 0, sizeof(hseSrvDescripto
pHseSrvDesc->srvId
srvResponse = HSE_Send(u8MuInstance, u8MuChan
return srvResponse;
* Function: HSE_CalculateAdkpHash
* Description: Acquire and print the HSE related
static hseSrvResponse_t HSE_CalculateAdkpHash(uin
uint32_t hash_length = 32U;
uint8_t local_adkp_hash[32] = {0U};
uint8_t uid[8] = {0U};
uint8_t uid_hash[32] = {0U};
uint8_t output[32] = {0U};
if(hseSecurityPolicy.enableADKm == TRUE)
/* ADKPm(128-bit) -> SHA256 -> hADKPm(256
srvResponse = HSE_HashDataBlocking(
MU0,
HSE_ACCESS_MODE_ONE_PASS,
HSE_HASH_ALGO_SHA2_256,
ASSERT(HSE_SRV_RSP_OK == srvResponse);
/* UID (64 -bit) -> SHA256 -> hUID (256
Variables Breakp... Periphe... Arm Sys... EmbSys... Periphe...
Project: [S32K344_LifeCycle_Management_Cfg_100_34_FW0110] Device: S32K344
Register Hex Bin
DCMROF21
DCMRWP1 0xA5080400
CLKOUT_STANDBY (bit 3) 0x0 0
STANBDY_PWDOG_DIS (bit 8) 0x0 0
POR_WDOG_TRIM (bits 9-10) 0x2 10
DCMRWP3
DCMRWD2
DCMRWD3
DCMRWD4
DCMRWD5
DCMRWD6
DCMRWD7
DCMRWD8
DCMRWD9
DCMRWF1
DCMRWF2
DCMRWF4
DCMRWF5
DCMROPP1
DCMROPP2
DCMROPP3
DCMROPP4
WKPU
CMU_FC
CMU_FM
TSPC
SIRC
SXOSC
FIRC
FXOSC
MC_CGM
MC_ME
PLL
PMC
FLASH
FLEXCAN
FLEXIO
LPUART
LPI2C
LPSPI
SAI
LPCMP
TEMPSENSE
CRC
FCCU
MU
MU_0_MUB
VER
PAR
CR
SR
CCR0
CSSR0
FCR
FSR 0x00000000
GIER
GCR
GSR
TCR
TSR
RCR
RSR
TR[0] 0x00000000
TR_DATA (bits 0-31) 0x00000000
TR[1]
TR[2]
TR[3]
RR[0] 0xAA55A55A
RR_DATA (bits 0-31) 0xAA55A55A
RR[1]
RR[2]
RR[3]
Outline Disassembly
HSE_CalculateAdkpHash(uint8_t*) : hseSrvResponse_t
GetHseInfo(void) : hseSrvResponse_t
main(void) : int
HSE_UpdateHseFirmware(hseAccessMode_t, uint32_t, uint32_t) : hseSrvResponse_t
Dashboard
Project Creation
S32DS Application Project
S32DS Library Project
Build/Debug
Build (All)
Clean (All)
Debug
Settings
Project settings
Build settings
Debug settings
Miscellaneous
Getting Started
Quick access
Console Problems Executables Debug Shell Search Watch registers Memory Spaces Memory Call Hierarchy Real Time Expressions
Monitors
0x004E0000
0x004E0040
0x4039C028
0x4039C028 : 0x4039C028 <Hex>
New Renderings...
Address 0 - 3 4 - 7 8 - B C - F
4039C020 01050000 00090400 42000000 00000000
4039C030 00000000 35000000 00000040 00C00240
4039C040 00C00240 00000240 00000000 00000000
4039C050 00900400 FFFFFFBF FF3FFDBF FF3FFDBF
4039C060 FFFFFDBF 03000000 00000000 00000000
1104M of 1494M
Read peripheral registers: (40%)

5.3 response

Send 0xF0F00F0F via MU0-MUB TR0 , the response for the handshake , click “run” and “stop”

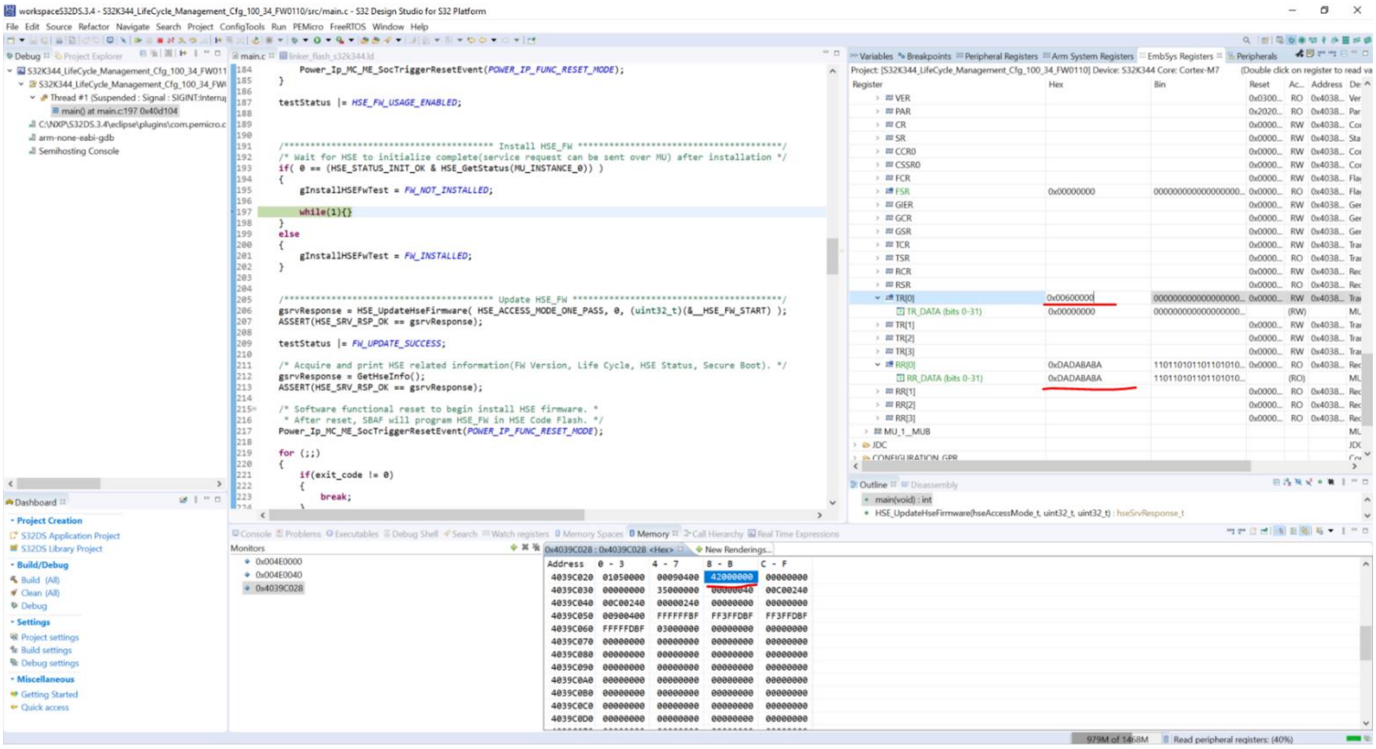


Return value 0xDADABABA to MU0-MUB RR0, which is requesting the HSE FW Pointer address



5.4 Provide the HSE FW pink image address

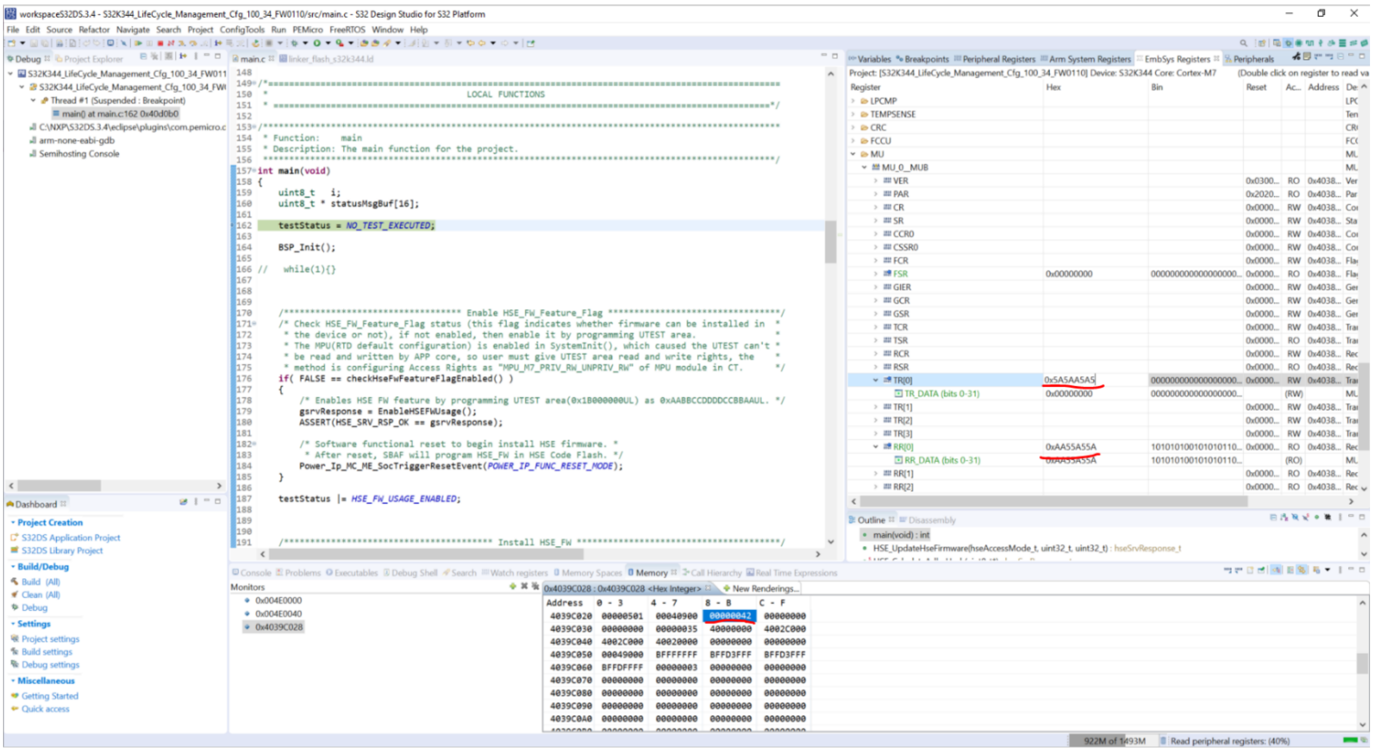
Provide the firmware address, in this pic is 0x00600000, users can fill in different values for the actual location of HSE FW without specific requirements, and then run the code.



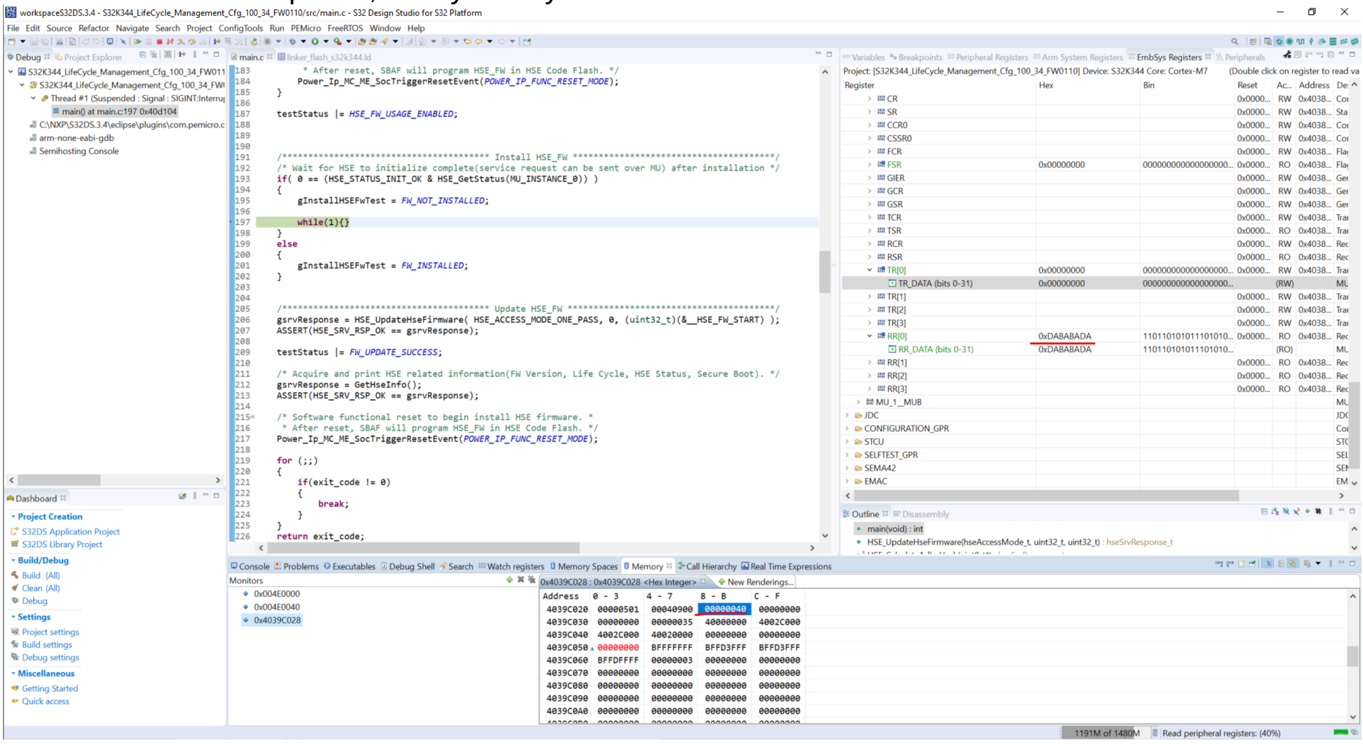
After successful installation, RR0 returns 0xAA55A55A, means Valid HSE FW present in Passive Block

5.5 Switch partition

Send 0x5A5AA5A5 via TR0, request the Switching active/passive Block.



Can see that the switch is successful, RR0 returns 0xDABABADA, and clears the HSE GPR bit 1 as the MU installation is completed, then you only need to reset.



After reset, the MU FSR value is 0x09600000, the HSE GPR bit 0 is set to “1”, HSE FW is present and SBAF Booted HSE Firmware.