A0 ROM Patch-sets Release Notes

Wednesday, September 12, 2018 7:13 AM

- A **patch-set** contains one or more patches to address one or more issues in ROM.
- A **cumulative patch-set** includes all patches released till date.
- A **delta patch-set** contains OTP patch words which should be applied on top of a previously released patch-set.
- A **sealed patch-set** with CRC32 check values will be created for production parts. That means the patch-set contains proper header and CRC value. On programmed with this patch-set the part cannot no longer be programmed with new delta patches. A sealed patch-set can use up to 208 words includ header.
- We have 208 patch words space available to ease distribution/management of patches, going forward all patches will be incremental and will not cons data patches. That is a part having version 0 patch-set can be upgradable to latest released patch-set.
- Programming instruction section for each release will contain OTP word index and value pair.
  - New patch additions to the patch-set are indicated through color coding (green existing and Red for new words).
  - Shell scripts to program a part on development board utilizing blhost.exe and ISP mode are also provided.

History

- ROM patch-set cumulative version 2:
  - Was based on ROM development team's (Fan's) quick testing.
  - Includes 9 cumulative patches.
  - Added debug patch (#8) from Matej.
  - Added I2C boot patch (#9) from Fan.
- ROM patch-set cumulative version 1:
  - Was based on ROM development team's (Fan's) quick testing.
  - But only includes non-secure boot ROM code fixes for critical issues.
  - Includes 7 cumulative patches.
- ROM patch-set cumulative version 0:
  - Was based FPGA testing done during FB demos.
  - Includes 3 patches.

2.0 A0_ROM Patch-set Cumulative Version 2

Released on **September 20th, 2018**.

2.1 Patch Programming instructions

```
@000000A1  0x55010003
@000000A2  0x1300A7A4
@000000A3  0x0010F2C5
@000000A4  0x130072d8
@000000A5  0x07C00400
@000000A6  0x1300838c
@000000A7  0x47704770

@000000A8  0x55010003
@000000A9  0x13004240
@000000AA  0x0400f2c0
@000000AB  0x13005c74
@000000AC  0x21010000
@000000AD  0x1301ee08
@000000AE  0x0200f240

@000000AF  0x55020103
@000000B0  0x13019c63
@000000B1  0x4400F240
@000000B2  0x0400F6C0
@000000B3  0x47709400

@000000B4  0x5502010290060002
@000000B5  0x130046d3
@000000B6  0x72fff64b
@000000B7  0x47709202

@000000B8  0x5502010d
@000000B9  0x130073b5
@000000BA  0x137cf240
@000000BB  0x0313f2c5
@000000BC  0xf242681a
@000000BD  0xf2c12000
@000000BE  0x2a000000
@000000BF  0x6a5bbf01
@000000C0  0xf64f2b00
@000000C1  0x600171ff
@000000C2  0x305af24c
@000000C3  0x20c3f6c5
@000000C4  0x98069000
```

```
@000000C5  0x0002f100
@000000C6  0x47709006

@000000C7  0x55020103
@000000C8  0x130133bb
@000000C9  0x1e416a38
@000000CA  0x0fc94189
@000000CB  0x47709100
```

2.2 Patch scripts

- To program the part using BLHost.exe and UART ISP mode. Use following script file.
- rompatc...

1.0 A0_ROM Patch-set Cumulative Version 1

Released on **August 29th, 2018**.

1.1 Patch Programming instructions

OTP Words starting word_161 onwards should be programmed with following values.

```
@000000A1  0x55010003
@000000A2  0x1300A7A4
@000000A3  0x0010F2C5
@000000A4  0x130072d8
@000000A5  0x07C00400
@000000A6  0x1300838c
@000000A7  0x47704770

@000000A8  0x55010003
@000000A9  0x13004240
@000000AA  0x0400f2c0
@000000AB  0x13005c74
@000000AC  0x21010000
@000000AD  0x1301ee08
@000000AE  0x0200f240

@000000AF  0x55020103
```

```
@000000B0  0x13019c63
@000000B1  0x4400F240
@000000B2  0x0400F6C0
@000000B3  0x47709400

@000000B4  0x55020102
@000000B5  0x130046d3
@000000B6  0x72fff64b
@000000B7  0x47709202
```

0.0 A0_ROM Patch-set Cumulative Version 0

0.1 Patch Programming instructions

OTP Words starting word_161 onwards should be programmed with following values.

```
@000000A1 55010003
@000000A2 1300a7a4
@000000A3 0010f2c5
@000000A4 130072d8
@000000A5 07c00400
@000000A6 1300838c
@000000A7 47704770
```

Patch List

Patch index	JIRA Ticket	Criticality	Patch details	Patch type	Patch data in ROM patcl
0	KBL-3324	**Must have**	The base address of debugmailbox is incorrect, it will cause hardfault when ROM is handling the commands in debugmailbox ROM patch for A0: Patch code at 0x1300a7a4 mailbox_get_base_address:	Data patch	0x1300A7A4 0x0010F2C5

			0x1300a7a0: 0xf24f 0x0000 MOVW R0, #61440 ; 0xf000 ***0x1300a7a4: 0xf2c4 0x0010 MOVT R0, #16400 ; 0x4010*** 0x1300a7a8: 0x4770 BX LR to ***MOVT R0, #0x5010***		
1	KBL-3319	**Must have**	VDDCORE_POR status bit position in code doesn't match with latest design specification ROM patch for A0. Patch code at 0x130072da // if (resetcause & RSTCTRL0_SYSRSTSTAT_VDDCORE_POR_MASK) 0x130072ca: 0xf642 0x75a4 MOVW R5, #12196 ; 0x2fa4 0x130072ce: 0xf242 0x2400 MOVW R4, #8704 ; 0x2200 0x130072d2: 0xf2c5 0x0500 MOVT R5, #20480 ; 0x5000 0x130072d6: 0xf2c1 0x0400 MOVT R4, #4096 ; 0x1000 ***0x130072da: 0x0740 LSLS R0, R0, #29*** To: ***LSLS R0, R0, #31***	Data Patch	0x130072d8 0x07C00400
2	KBL-3492	**Must have**	The secure counter cannot work in some branch. Bypass the secure counter	Data Patch	0x1300838c 0x47704770

			Patch code at line 1300838c: secure_counter_assert_fail: ***0x1300838c: 0xf017 0xfe1b BL go_fatal_mode ; 0x1301ffc6*** to BX LR (0x4770) BX LR (0x4770)		
3	KBL-3493	For SD card boot only	The Default SD boot via ISP pin selection is set to 1, however, both the validation board and the EVK board connects the SD to uSDHC0, need a ROM patch to change the ROM behavior Need to patch code at address 0x13004240 0x1300423a: 0xe0af B.N @1300439c // boot_device_info.instance = 1; @1300423c: 0x1300423c: 0xf240 0x4400 MOVW R4, #1024 ; 0x400 ***0x13004240: 0xf2c0 0x0410 MOVT R4, #16 ; 0x10*** To ***MOVT R4, #0***	Data Patch	0x13004240 0x0400f2c0
4	KBL-3494	For USB ISP/boot	OSC initialization is incorrect	Data Patch	0x13005c74 0x21010000

5	KBL-3495	For USB ISP/boot
		(program USB_IDs in OTP to bypass this patch)
			USB VID and PID is incorrect with the PID and VID fuse field are not blown
			Change below logic
			// if ((usbPid != (uint16_t)0xFFFF) || (usbVid != (uint16_t)0xFFFF))
			0x1301ee08: 0xf64f 0x72ff MOVW R2, #65535 ; 0xffff
			0x1301ee0c: 0x0c00 LSRS R0, R0, #16
			0x1301ee0e: 0xb289 UXTH R1, R1
			to
			// if ((usbPid != (uint16_t)0x0) || (usbVid != (uint16_t)0x0))
			MOVW, R2, 0,
				Data patch	0x1301ee08
					0x0200f240

6	KBL-3471	For QuadSPI flash boot	The Flash configuration block (FCB) offset in qspi_memory.c is incorrect, it should be 0x400 while it is 0x0 in the code. The issue happens at below code block // status = qspi_mem_write (s_qspi_mem_feature.qspiStartAddress, sizeof (*qspiNorConfig), // (const uint8_t *)qspiNorConfig); ***0x13019c62: 0x68a0 LDR R0, [R4, #0x8]*** 0x13019c64: 0x462a MOV R2, R5 0x13019c66: 0xf44f 0x7100 MOV.W R1, #512 ; 0x200 0x13019c6a: 0xf000 0xf895 BL qspi_mem_write ; 0x13019d98 A Code patch is required to fix this issue, we can patch the address 0x13019c56 and set the R0 value to 0x08000400 directly, below is the patch code. MOVW R4, #1024 ; 0x400 MOVT R4, #2048 STR R4, [SP] (the code patch is implemented by the SVC call, change the call stack to modify the R0 value directly). BX LR	Code patch	0x55020103 0x13019c63 0x4400F240 0x0400F6C0 0x47709400

7	KBL-3496	Not critical for 32 entry patches Should be included in large patch (208 entries)	The reserved region range is incorrect Need to change code at address 0x130046d2 // const memory_map_entry_t *map = (memory_map_entry_t *)&g_bootloaderContext.memoryMap[0]; 0x130046c6: 0x6844 LDR R4, [R0, #0x4] 0x130046c8: 0x6909 LDR R1, [R1, #0x10] 0x130046ca: 0xf101 0x0290 ADD.W R2, R1, #144 ; 0x90 0x130046ce: 0x6853 LDR R3, [R2, #0x4] 0x130046d0: 0x6812 LDR R2, [R2] ***0x130046d2: 0x1a9a SUBS R2, R3, R2*** 0x130046d4: 0x2300 MOVS R3, #0 To MOVW R2, 0xBFFF STR R2, [SP, #8] BX LR	Code patch	0x55020102 0x130046d3 0x72fff64b 0x47709202
8	KBL-3469	**Must have**	Here is the patch code: MOVW R3, #380 ; 0x17c MOVT R3, #20499 ; 0x5013 LDR R2, [R3] MOVW R0, #8704 ; 0x2200 MOVT R0, #4096 ; 0x1000 CMP R2, #0 ITTTT EQ LDREQ R3, [R3, #0x24]	Code patch	0x5502010d 0x130073b5 0x137cf240 0x0313f2c5 0xf242681a 0xf2c12000 0x2a000000 0x6a5bbf01 0xf64f2b00 0x600171ff 0x305af24c

			CMPEQ R3, #0 MOVWEQ R1, #65535 ; 0xffff STREQ R1, [R0] MOVW R0, #50010 ; 0xc35a MOVT R0, #23235 ; 0x5ac3 STR R0, [SP] LDR R0, [SP, #0x18] ADD.W R0, R0, #2 STR R0, [SP, #0x18] BX LR		0x20c3f6c5 0x98069000 0x0002f100 0x47709006

9	KBL-3505	For I2C boot/ISP	ROM Code Bug
			// s_flexcommI2cInfo.irq_notifier_callback(true);
			0x130133b6: 0x2001 MOVS R0, #1
			0x130133b8: 0x4788 BLX R1
			// while (!s_flexcommI2cLateByteIsSend)
			@130133ba:
			0x130133ba: 0x7838 LDRB R0, [R7]
			0x130133bc: 0xb9d0 CBNZ R0, @130133f4
			// endTicks = microseconds_get_ticks();
			ROM Code Fix
			- while (!s_flexcommI2cLateByteIsSend)
			+ while (s_flexcommI2cInfo.bytesToTransfer)
			ROM Patch Assemble Code
			LDR R0, [R7,#0x20]
			SUBS R1, R0, #0x1
			SBCS R1, R1, R1
			LSRS R1, R1, #0x1F
			STR R1, [SP]
			BX LR
				Code patch	0x55020103
					0x130133bb
					0x1e416a38
					0x0fc94189
					0x47709100

10	KBL-3774		ROM code bug
			base->MASTER_SEC_REG = 0x10000000u;
			ROM code fix
			base->MASTER_SEC_REG = 0x80000000u;
				Data patch	0x55010001
					0x1300a19c
					0x60104000
					From
					<https://jira.sw.nxp.com/brov
					3774>

11	KBL-3738	For XIP signed image boot	Rom code bug
			In fsl_hashcrypt.c need to change:
			base->MEMADDR = HASHCRYPT_ALIAS_OFFSET | HASH_MEMADDR_BASE(input);
			
			To
			base->HASH_MEMADDR_BASE(input);
			
			ROM Patch Assemble Code
			LDR R0, [SP, #0x18]
			ADD.W R0, R0, #2
			STR R0, [SP, #0x18]
			BX LR
				Code patch	0x55020103
					0x1300b617
					0xf1009806
					0x90060002
					0x47704770