TCC803x Automotive Common BSP

User Guide for Boot Sequence

Rev. 0.01 [A]
2018-09-20
Preliminary version

TABLE OF CONTENTS

Contents

Figures

Tables

1 INTRODUCTION

This document describes a boot sequence of TCC803x from the power-on to the start of the kernel. The boot sequence consists of four Boot Levels (BL).

Figure 1.1 shows the overview of boot sequence.

- The first boot level is the on-chip boot ROM code (Chipboot ROM Code). TCC803x has three processors which are Cortex-A53 (A53), Cortex-R5 (MICOM), and Cortex-A7 (A7S). After power-on, the first processor that wakes up is MICOM. For this reason, MICOM executes Chipboot ROM Code in order to load the MICOM BL1 for the second boot level.
- A53 cannot execute Chipboot ROM Code like MICOM. ARM Trusted Firmware (ARM-TF) is used as the first level bootloader for A53. During the second boot level, MICOM loads ARM-TF and resets A53. After A53 runs ARM-TF, MICOM executes MICOM Firmware, if the boot mode is SNOR mode.
- At the third boot level, A53 loads various images such as U-boot, secure firmware, and DRAM initialization parameters. A53 initializes DRAM by using parameters and registers EL3 runtime services (Refer to Table 2.3) for security.
- Lastly, the fourth boot level is U-boot. At U-boot, A53 loads kernel and device tree for A53. If needed, A53 resets A7S and loads images for A7S.

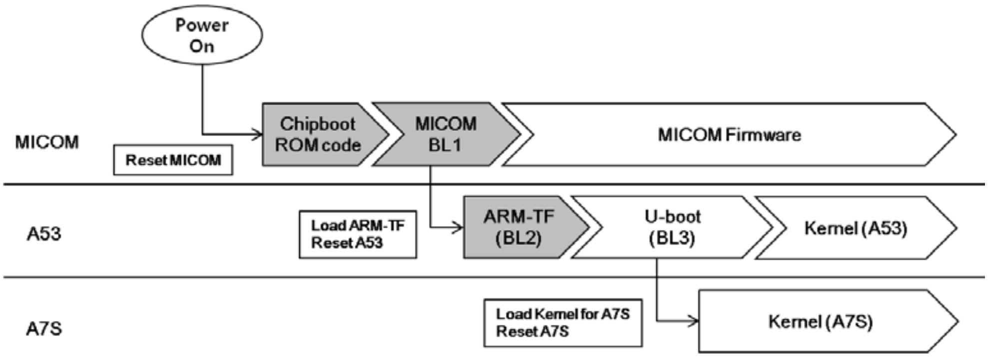

Figure 1.1 Overview of Boot Sequence

Note: Because of the security issues, the source code of each boot level is not provided except U-boot. Only binary images are provided for MICOM BL1 and ARM-TF.

2 Boot Sequence

2.1 Boot Level 0: Chipboot ROM Code

Figure 2.1 shows the workflow of Chipboot ROM Code. Chipboot ROM Code is masked at Boot-ROM region (from 0xC400_0000 to 0xC401_FFFF).
After the power-up sequence is completed, MICOM wakes up first and executes Chipboot ROM Code. First of all, MICOM checks whether the CPU#0 runs the code and initializes MPU, clock, and runtime environment. For more information about the power-up sequence, refer to [1].

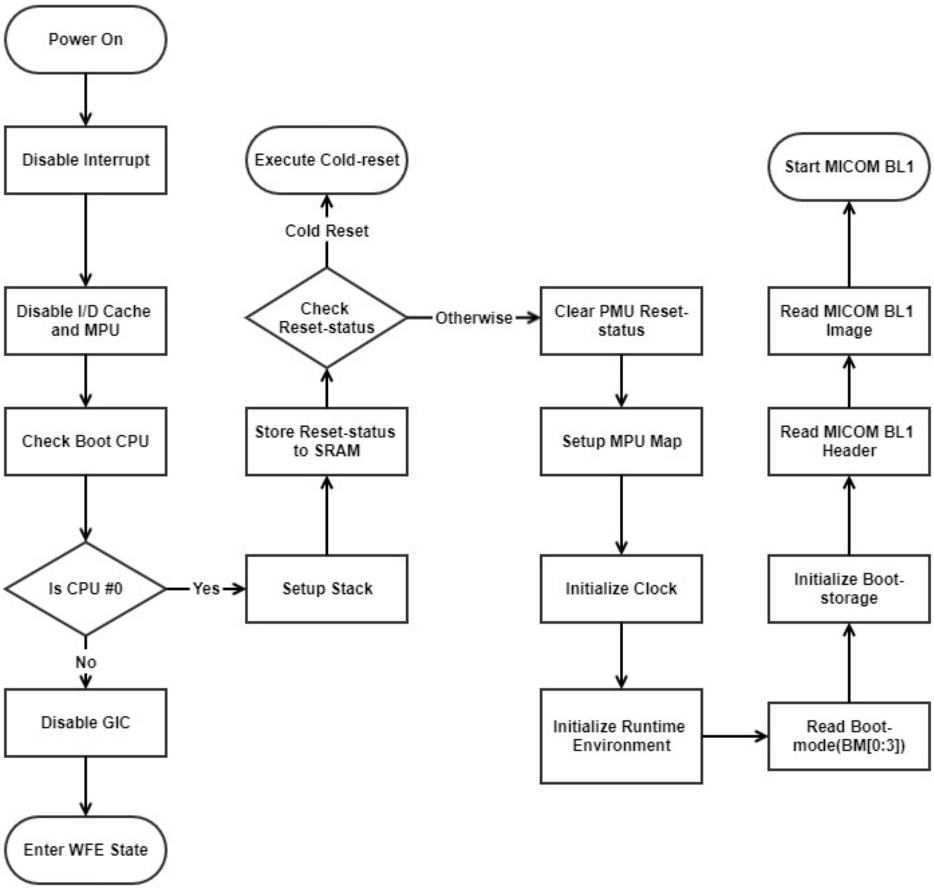

Figure 2.1 Chipboot ROM Code Workflow

After clearing the reset status, MICOM configures PMU, clock, and runtime environment. Refer to Table 2.1 below for clock settings.

Table 2.1 Clock Configuration at BL0

Clock	Frequency [MHz]
PLL0	400
PLL1	1200
PLL0 DIV	200
PLL1 DIV	600
CPU BUS	24
MEM BUS	600
HSIO BUS	200
SMU BUS	24
DDI BUS	24
IO BUS	200
MICOM PLL0	800
MICOM PLL1	200
MICOM PLL0 DIV	400
MICOM PLL1 DIV	100
MICOM CPU BUS	400
MICOM BUS	200

MICOM initializes the storage interface by checking BM[0:3]. Boot-mode is decided by BM[0:3] as in Table 2.2. After initializing the storage successfully, it loads MICOM BL1 header and image as well as runs MICOM BL1.

Table 2.2 Boot Mode

BM[0:3]	Boot Mode
0b0000	USB
0b0010	Serial NOR (3Byte Address Mode)
0b0011	Serial NOR (4Byte Address Mode)
0b0100	NAND
0b0101	eMMC (Channel #0)
0b0111	eMMC (Channel #1)

2.2 Boot Level 1: MICOM BL1

During MICOM BL1, MICOM resets A53 and loads ARM-TF BL2-1 to the specific memory. There are two methods in order to load ARM-TF BL2-1. One is loading MICOM BL1 image at BL0, and the other one is loading at BL1 by initializing the storage. The later one is slower than the former due to the interface initialization. For this reason, the former one is the default.

Figure 2.2 shows the workflow of MICOM BL1. First, MICOM checks the processor ID in order to prevent the other sub-cores to execute MICOM BL1. MICOM reconfigures stack, interrupt, cache, MPU, and so on. If MICOM BL1 image at BL0 includes ARM-TF BL2-1, it relocates ARM-TF BL2-1 image to the specific address. In order to change the vector base address to low (0x0000_0000), MICOM copies the exception vector to 0x0000_0000. After that, it configures peripherals such as clock and UART.

If MICOM BL1 images do not include ARM-TF BL2-1, it initializes the storage interface and loads ARM-TF BL2-1 images. If the boot mode is eMMC or SNOR, it initializes eMMC. Otherwise, MICOM initializes USB firmware download mode and then wakes up A53. If the boot mode is SNOR, MICOM runs MICOM firmware. If not, MICOM is in WFE (Wait For Event) mode.

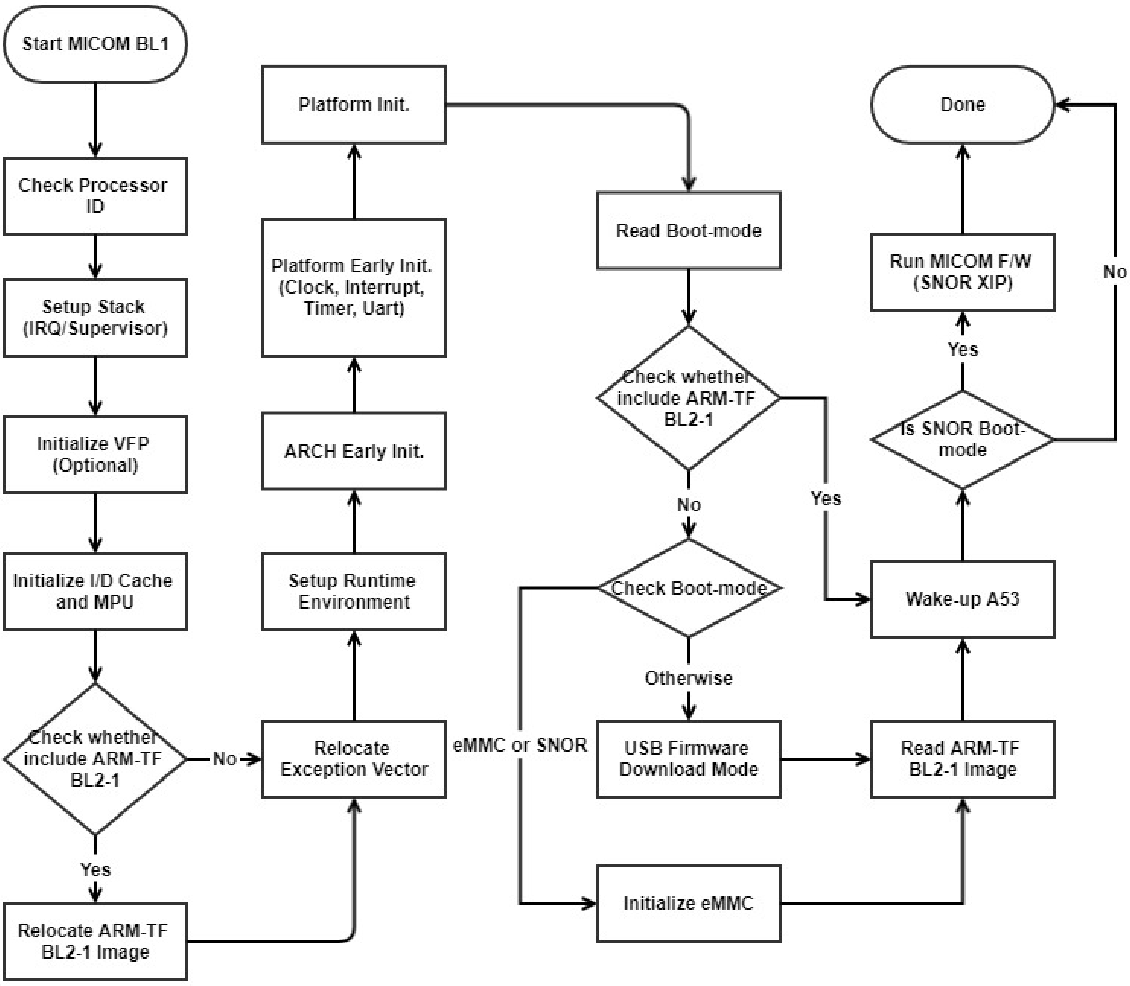

Figure 2.2 MICOM BL1 Workflow

2.3 Boot Level 2: ARM Trusted Firmware

Because ARM-TF is the open source project [2], only main function of ARM-TF is described in this Chapter. A53 does not execute the firmware like Chipboot ROM Code for MICOM. For this reason, MICOM loads the bootloader for A53 which is ARM-TF and wakes up A53. For TCC803x, ARM-TF BL2-1 and BL2-2 are used. The main functions for each step are summarized in Table 2.3.

Table 2.3 Main Function of ARM Trusted Firmware

Boot Level	ARM-TF	Exception Level	Functions
ARM-TF BL2-1	BL21	EL2	Load boot images for next level (ARM-TF BL2-2, U-boot) Load DRAM initialization parameters and initialize DRAM Load secure firmware images
ARM-TF BL2-2	BL31	EL3	Register EL3 runtime services (such as PSCI, OPTEE, SiP (Silicon Provider), and so on)

Note: ARM-TF means the boot level defined at [2].

Figure 2.3 shows the workflow of ARM-TF BL2-1 main functions. A53 initializes the storage interface according to the boot mode. If the boot mode is SNOR or eMMC, A53 initializes eMMC. Otherwise, A53 sets up USB firmware download mode. After loading some images such as Key Table, ARM-TF BL2-2, and DRAM parameters, it initializes DRAM. Before running ARM-TF BL2-2, A53 loads secure firmware and U-boot. During ARM-TF BL2-2, A53 registers EL3 runtime services such as PSCI, OPTEE, and SiP, as well as runs U-boot.

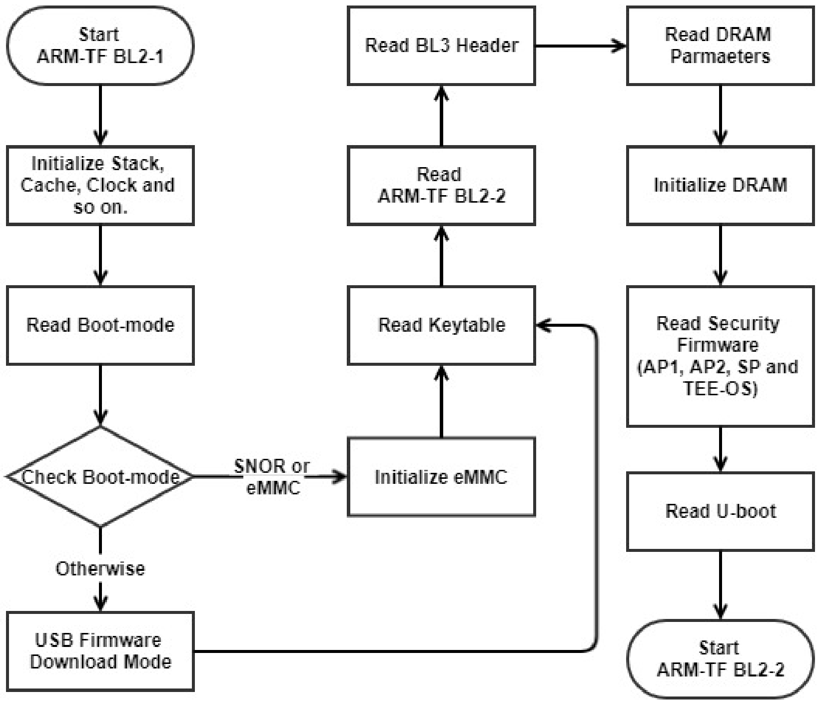

Figure 2.3 ARM-TF BL2-1 Workflow

2.4 Boot Level 3: U-boot

After U-boot initialization is completed, A53 loads kernel images and device tree according to the boot commands. Table 2.4 shows the commands for loading images and starting the kernel for each A53 and A7S.

Table 2.4 U-boot Command

Command	Description
tcc_load	Load kernel image and device tree
avm_start	Reset A7S and start A7S kernel
bootm	Start A53 kernel

3 MEMORY LAYOUT

This chapter describes two kinds of memory layouts (eMMC and SNOR) for the boot.

3.1 SNOR Memory Layout

SNOR includes SNOR parameters, MICOM BL1, CM4 firmware, and MICOM firmware. It does not include secure firmware and U-boot image because the size is larger than the SNOR's. For this reason, SNOR should work with eMMC. SNOR parameters are used for initialization for SNOR during BL0.

Table 3.1 SNOR Memory Layout

Address	Image	Size
0x0000_0000 ~ 0x0000_00FF	SNOR Parameters (Primary)	256 byte
0x0000_0100 ~ 0x0000_0FFF	Reserved	3840 byte
0x0000_1000 ~ 0x0000_10FF	SNOR Parameters (Secondary)	256 byte
0x0000_1100 ~ 0x0000_1FFF	Reserved	3840 byte
0x0000_2000 ~ 0x0002_1FFF	MICOM BL1 Header (Primary)	128 Kbyte
	MICOM BL1 Image + ARM-TF BL2-1 (Primary)	
0x0002_2000 ~ 0x0004_1FFF	MICOM BL1 Header (Secondary)	128 Kbyte
	MICOM BL1 Image + ARM-TF BL2-1 (Secondary)	
0x0004_2000 ~ 0x0006_1FFF	CM4 Firmware Header/Image (Primary)	128 Kbyte
0x0006_2000 ~ 0x0008_1FFF	CM4 Firmware Header/Image (Secondary)	128 Kbyte
0x0008_2000 ~ 0x0008_2FFF	MICOM Firmware Header (Primary)	3840 byte
	BL1 Attribute(64B) + Signature(64B) for Security (Primary)	256 byte
0x0008_3000 ~ 0x0008_3FFF	MICOM Firmware Header (Secondary)	3840 byte
	BL1 Attribute(64B) + Signature(64B) for Security (Secondary)	256 byte
0x0008_4000 ~ End	MICOM Firmware Image (Primary)	
	MICOM Firmware Image (Secondary)	

3.2 eMMC Memory Layout

eMMC has three memory regions; boot area partition 1, 2, and user area partition.
Boot area partition 1 stores the primary boot images and headers, and the boot area partition 2 is for secondary of them. BL3 Sub Header includes the serial number for the Bluetooth device address and the MAC address.

Table 3.2 eMMC Boot Area Partition

Index of sector	Image
0	MICOM BL1 Header
1	MICOM BL1 + ARM-TF BL2-1 Images
MICOM_BL1_OFFSET	ARM-TF BL2-2 Header
MICOM_BL1_OFFSET + 1	ARM-TF BL2-2 Image
MICOM_BL1_OFFSET + 240	Key Table Image
MICOM_BL1_OFFSET + 248	BL3 Header
MICOM_BL1_OFFSET + 249	BL3 Sub Header
MICOM_BL1_OFFSET + 250	DRAM Parameters
MICOM_BL1_OFFSET + 250 + Size of DRAM Parameters	U-boot Image

Note:
- One sector is 512 byte.
- MICOM_BL1_OFFSET is sector 256.

The secure firmware is stored in user area partition because it is normally larger than the boot partition. Secure firmware is placed next to the MBR (Master Boot Record). In order to prevent overwriting of secure firmware, the first partition should be reserved for secure firmware and the size is 100MB.

Table 3.3 eMMC User Area Partition

Index of sector	Image
0	MBR
34	Secure Firmware (Primary)
34 + Size of Secure Firmware	Secure Firmware (Secondary)
-	-
204800~	Others

4 FWDN BOOTLOADER IMAGE

This chapter describes the structure of FWDN (Firmware Downloader) bootloader image. FWDN bootloader image is used for downloading the bootloader to boot storage such as eMMC and SNOR. Table 4.1 shows the overview of FWDN bootloader image and the bootloader image consists of various images and headers.

Table 4.1. Overview of FWDN Bootloader Image

Image
FWDN Header
MICOM BL1 Header
MICOM BL1 + ARM-TF BL2-1 Images
ARM-TF BL2-2 Header
ARM-TF BL2-2 Image
Key Table
BL3 Header
DRAM Parameters
U-boot Image
Secure Firmware

The target system requests FWDN header to the host system first when starting the download. Table 4.2 shows the entry of FWDN header. The FWDN header includes the start address and size of each header and image. By using FWDN header, the target system can request the header and images that you want to load.

Table 4.2. FWDN Header Structure

Parameter	Offset	Size [Byte]	Value
Magic Code	0x00	8	“ANDROID@”
Boot Mode	0x08	4	“TCSB”
ROM Type	0x0C	4	“LBS_”
Base Address	0x10	4	0x0
Flash memory Type	0x14	4	0x0
FWDN Type	0x18	4	“V7 “
Chipset Name	0x1C	4	“803x”
ARM-TF BL2-2 Header Start	0x20	8	-
ARM-TF BL2-2 Header Size	0x28	8	-
ARM-TF BL2-2 Image Start	0x30	8	-
ARM-TF BL2-2 Image Size	0x38	8	-
Secure Firmware Start	0x40	8	-
Secure Firmware Size	0x48	8	-
Key Table Start	0x50	8	-
Key Table Size	0x58	8	-
BL3 Header Start	0x60	8	-
BL3 Header Size	0x68	8	-
DRAM Parameter Start	0x70	8	-
DRAM Parameter Size	0x78	8	-
U-boot Image Start	0x80	8	-
U-boot Image Size	0x88	8	-
MICOM BL1 Header Start	0x90	8	-
MICOM BL1 Header Size	0x98	8	-
MICOM BL1 Image Start	0xA0	8	
MICOM BL1 Image Size	0xA8	8	
Reserved	0xB0	336	

5 REFERENCES

[1] TCC803x Full Specification.
[2] ARM Trusted Firmware Git-hub, https://github.com/ARM-software/arm-trusted-firmware

6 REVISION HISTORY

6.1 Rev. 0.01: 2018-09-20

- Preliminary Version Release.

DISCLAIMER

COPYRIGHT STATEMENT

Important Notice

This material may include technology owned by the 3rd party licensor and the technology may be subject to its associated licenses. It is solely customer's responsibility to identify and comply with such licenses. No other licenses are granted or implied by Telechips with making available this material.

For customers who use licensed Codec ICs and/or licensed codec firmware of mp3:
“Supply of this product does not convey a license nor imply any right to distribute content created with this product in revenue-generating broadcast systems (terrestrial. Satellite, cable and/or other distribution channels), streaming applications(via internet, intranets and/or other networks), other content distribution systems(pay-audio or audio-on-demand applications and the like) or on physical media(compact discs, digital versatile discs, semiconductor chips, hard drives, memory cards and the like). An independent license for such use is required. For details, please visit http://mp3licensing.com”.

For customers who use other firmware of mp3:
“Supply of this product does not convey a license under the relevant intellectual property of Thomson and/or Fraunhofer Gesellschaft nor imply any right to use this product in any finished end user or ready-to-use final product. An independent license for such use is required. For details, please visit http://mp3licensing.com”.

For customers who use Digital Wave DRA solution:
“Supply of this implementation of DRA technology does not convey a license nor imply any right to this implementation in any finished end-user or ready-to-use terminal product. An independent license for such use is required.”

For customers who use DTS technology:
"This product made under license to certain U.S. patents and/or foreign counterparts."

For customers who use Dolby technology:
"Supply of this Implementation of Dolby technology does not convey a license nor imply a right under any patent, or any other industrial or intellectual property right of Dolby Laboratories, to use this Implementation in any finished end-user or ready-to-use final product. It is hereby notified that a license for such use is required from Dolby Laboratories."

For customers who use Google technology:

For customers who use MS technology:
"This product is subject to certain intellectual property rights of Microsoft and cannot be used or distributed further without the appropriate license(s) from Microsoft."