Ampere® Altra® Family 64-Bit Multi-Core Processor

System Control Processor User's Manual

May 18, 2021

Document Issue 0.58

Contents

Tables

1. Overview

This chapter provides a general introduction to the Ampere® Altra® System Control Processor (SCP).

1.1 Purpose

Ampere evaluation boards provide reference platforms for evaluating Altra processors. A typical evaluation board is a single-board solution built around one or two Altra processors. Such boards are parts of reference designs to test and evaluate the Altra processor with different system configuration options.

This document describes the software details provided by the evaluation kit for the SCP.

1.2 Intended Audience

This document is intended for hardware and software engineers who plan to build a system using the Altra devices.

1.3 Conventions

All numbers are decimal unless preceded by a ‘0x’, or appended by ‘h’, to indicate hexadecimal. *Table 1* outlines font conventions used to distinguish different types of text in this document.

Table 1: Text Conventions

FONT	USAGE
`Courier Bold`	Typed-in commands, or verbatim user-entered text.
`Courier`	Text response from the computer.
<text>	Mandatory field.
[text]	Text that may be optionally entered or omitted.
italic	Variable placeholder.

From this point forward, Altra evaluation boards are referred to as “boards.” Altra processors are referred to as “processors.”

2. SCP Firmware

This chapter describes the Altra SCP firmware used with all boards based on Altra processors. The SCP comprises SMpro and PMpro. SMpro is used for system management, and PMpro is used for power management.

2.1 Supported Features

For supported features and summary of changes, refer to the Release Note provided with each release.

2.2 SCP Firmware Content

The SCP firmware is delivered as a binary containing all files in a single tar archive:

```
altra_scp_V.VV.BB.tar.xz
```

where `V.VV` is the release version and `BB` is the build version.

The archive contains these files:

- `altra_scp_V.VV.BB.slim`: SCP firmware binary in Ampere SLIM format
- `altra_scp_V.VV.BB.cap`: SCP firmware binary in UEFI capsule format
- `altra_scp_um.pdf`: Altra SCP User's Manual (this document)
- `altra_scp_release_note.txt`: SCP Release Notes
- `altra_scp_capsule_V.VV.BB.hpm`: SCP firmware binary for the Baseboard Management Controller (BMC), used to perform a system recovery.

2.3 SCP Programming

An external I2C EEPROM programmer or BMC is required to program the SCP firmware. Consult your I2C EEPROM programmer's manual and the board manual for instructions. For BMC instructions, refer to the BMC documentation.

3. System Reset and Reboot

The SCP handles system reset and reboot. This enables the system to quiesce before triggering a system-wide reboot/reset. This is handled by writing to SMpro secure mailbox 5 interrupt register.

4. SCP TPC

The Thermal Protection Circuit (TPC) comprises a control loop running on the SCP that monitors on-die temperatures and takes appropriate actions. Two threshold levels are checked: high-temperature and over-temperature.

4.1 High-Temperature Threshold

When this threshold is crossed, SCP throttles the Arm® Armv8.x processor speed until the temperature falls below this threshold. The SCP asserts the HIGHTEMP pin to indicate that thermal throttling is active and sends a message to the Armv8.x core which must register to receives the message.

Each product SKU has a different high-temperature threshold value.

4.2 Over-Temperature Threshold (120°C)

When this threshold is crossed, the SCP asserts the OVERTEMP pin to indicate an over-temperature condition. After this, the SCP powers down the processor power domain.

4.3 TPC GPIO Pins

The TPC uses the HIGHTEMP pin as an output when the temperature exceeds the over-temperature threshold. By default, the HIGHTEMP pin is bidirectional. This pin is used as an output when the SCP detects a high-temperature condition. When an external agent asserts this pin, the SCP throttles the Armv8 processor frequency while the pin remains asserted.

4.4 TPC Linux Kernel Interface

The TPC status is available through sysfs on the Linux kernel. Refer to the Linux HWmon driver for SoC temperature and power information.

5. SMpro and PMpro Doorbell Message Assignments

This section lists the SMpro and PMpro doorbell message assignments.

5.1 SMpro Doorbell Message Assignments

5.1.1 Secure World Message Assignments

- SMpro secure Mailbox 0 – Standard messages request for secure EL1
- SMpro secure Mailbox 1 – Standard messages request for secure EL3
- SMpro secure Mailbox 2 – ACPI Platform Error Interfaces (ACPI) ACPI Platform Error Interfaces (APEI) operation request for secure EL3
- SMpro secure Mailbox 3 – SMpro info for secure EL3 and EL1
- SMpro secure Mailbox 4 – Reserved
- SMpro secure Mailbox 5 – Power State Coordination Interface (PSCI) (Reboot and shutdown) operation request for secure EL3
- SMpro secure Mailbox 6 – True Random Number Generator (TRNG)
- SMpro secure Mailbox 7 – TPC operation for secure EL1
- SMpro secure Mailbox 8 – SMpro and PMpro communication

5.1.2 Non-Secure World Message Assignments

- SMpro Mailbox 0 – Standard and APEI messages for non-secure EL1
- SMpro Mailbox 1 – Reserved
- SMpro Mailbox 2 – Reserved
- SMpro Mailbox 3 – SMpro info for EL2
- SMpro Mailbox 4 – Hot plug service
- SMpro Mailbox 5 – Reserved
- SMpro Mailbox 6 – TRNG
- SMpro Mailbox 7 – TPC operation for non-secure EL1
- SMpro Mailbox 8 – Hardware monitor (energy)

5.2 PMpro Doorbell Message Assignments

5.2.1 Secure World Message Assignments

- PMpro secure Mailbox 0 – Reserved
- PMpro secure Mailbox 1 – Reserved
- PMpro secure Mailbox 2 – Collaborative Processor Performance Control (CPPC) for EL3
- PMpro secure Mailbox 3 – Reserved
- PMpro secure Mailbox 4 – Reserved
- PMpro secure Mailbox 5 – PSCI for EL3
- PMpro secure Mailbox 6 – Reserved
- PMpro secure Mailbox 7 – Reserved
- PMpro secure Mailbox 8 – SMpro and PMpro communication

5.2.2 Non-Secure World Message Assignments

- PMpro Mailbox 0 – Reserved
- PMpro Mailbox 1 – Maximum frequency information message for non-secure EL1
- PMpro Mailbox 2 – CPPC for non-secure EL1
- PMpro Mailbox 3 – Reserved
- PMpro Mailbox 4 – Reserved
- PMpro Mailbox 5 – Reserved

- PMpro Mailbox 6 – Reserved
- PMpro Mailbox 7 – Reserved
- PMpro Mailbox 8 – Reserved

6. BMC Support

The SCP provides support for the BMC. For more information, refer to the document titled *Altra SoC BMC Interface Specification*.

7. SCP Boot Process Codes

Table 2: SCP Boot Process Codes

MODULES	POST CODE BYTE 3	POST CODE BYTE 2	POST CODE BYTE 1	POST CODE BYTE 0	COMMENT
SMpro	0	0	0	0	SMpro not started
SMpro	0	1	0	0	SMpro boot started
SMpro	0	2	0	0	SMpro boot complete
SMpro	0	3	0	0	SMpro boot failure
SMpro	0	4	0	0	SMpro boot failure due to authentication
PMpro	1	0	0	0	PMpro not started (Not a possible value)
PMpro	1	1	0	0	PMpro boot started
PMpro	1	2	0	0	PMpro boot complete
PMpro	1	3	0	0	PMpro boot failure
PMpro	1	4	0	0	PMpro boot failure due to authentication

8. SCP Firmware Error Codes

The SCP provides error and progress logging. At the early stages of SCP booting, a fault LED indicates whether a boot failure occurs. This fault LED blinks a fixed number of times to indicate the trapped error code that can be used to debug various boot issues.

Table 3 summarizes the General Purpose IO (GPIO) fault error codes. The number of blinks with a long pause encodes the value. For example, a value of error code 10 causes the fault LED to blink 10 times, followed by a long pause; the cycle then repeats.

Table 3: GPIO Error Code Definitions

GPIO FAULT ERROR CODE	DESCRIPTION
0	No error
1	Invalid life cycle state
2	EEPROM file header invalid
3	EEPROM file integrity invalid
4	Key certificate authentication failure
5	Content certificate authentication failure
6	I2C hardware error
7	Crypto hardware error
8	ROTPK invalid
9	SEED invalid
10	Life cycle state invalid
11	Primary rollback invalid
12	Secondary rollback invalid
13	HUK invalid
14	Certificate data invalid
15	Internal hardware error

The MPA_SCRATCH1 and MPA_SCRATCH2 registers maintain error, warning, and progress information. The MPA_SCRATCH1 register is for error and progress while MPA_SCRATCH2 is for warnings (non-fatal errors). *Table 4* and *Table 5* describe these register definitions.

Table 4: MPA_SCRATCH1: SMpro Error Code Bit Definitions

BIT	31	30	29	28	27	26 … 24	23 … 16	15 … 0
Field	Software Image				Enter/Exit	Reserved	Location	Error

Table 5: MPA_SCRATCH2: SMpro Warning Code Bit Definitions

BIT	31	30	29	28	27	26 ... 24	23 ... 16	15 ... 0
Field	Software Image				Enter/Exit	Reserved	Location	Error

These fields represent:

- Software image: Indicates the type of software that generates the error code
- Enter/Exit: Indicates entering or exiting of the function
- Location: Indicates the location of the code being executed
- Error: Indicates the error

Table 6, *Table 7*, *Table 8*, and *Table 9* describe the definitions.

Table 6: SCP Image Code Descriptions

IMAGE CODE	DESCRIPTION
0	Executing ROM image
1	Executing boot strap image
2	Executing ROM normal (non-secure) boot path
3	Executing ROM secure boot path
4	Executing ROM asymmetric secure boot path
5	Executing ROM symmetric secure boot path
6	Executing runtime image
7	Executing asymmetric secure runtime image
8	Executing symmetric secure runtime image
9	All others

Table 7: SCP Enter/Exit Code Descriptions

ENTER/EXIT CODE	DESCRIPTION
0	Beginning of the location
1	End of the location

Table 8: SCP Module Location Code Descriptions

LOCATION CODE	DESCRIPTION
1	Main routine
2	Interrupt controller (Nested Vectored Interrupt Controller (NVIC))
3	Advanced High-Performance Bus (AHB) to Advanced eXtensible Interface (AXI) mapping
4	eFuse initialization

LOCATION CODE	DESCRIPTION
5	eFuse loading
6	eFuse read fields
7	eFuse write fields
8	Crypto authentication
9	Cryptocell initialization
10	Certificate reading by Cryptocell library
11	Loading from I2C EEPROM to IRAM using IICDMA controller
12	ROM main
13	ROM dead
14	N/A
15	N/A
16	N/A
17	BL1 and PMpro Secure boot
18	Slim img file operations
19	ROM jump to runtime firmware
20	Adaptive Voltage Scaling (AVS) module
21	PMpro booting
22	On-Chip Memory (OCM) initialization
23	Media booting
24	SPI NOR read
25	Memory repair
26	Console
27	Board module
28	DDR ZQCS
29	Armv8 Initialization
30	Processor Complex (PCP) power down
31	Processing Element (PE) PLL initialization
32	PMDPLL initialization
33	PCP power up
34	PCP CPM initialization
35	Mesh clock reset initialization
36	PMD initialization
37	PSCI CPU power management
38	PSCI Processor Module (PMD) power management

LOCATION CODE	DESCRIPTION
39	PSCI PCP power management
40	L3C clock reset initialization
41	PCP initialization
42	TPC
43	Mainloop
44	Mainloop non-secure message processing
45	Mainloop secure message processing
46	Mainloop console proxy buffer processing
47	Mainloop PSCI request processing
48	Mainloop Command Line Interface (CLI) request processing
49	Mainloop thermal protection request processing
50	Mainloop board sensor processing
51	Mainloop Reliability, Availability, and Serviceability (RAS) request processing
52	SCP Yielding routine
53	Mainloop PMpro watchdog monitoring
54	Mainloop maximum frequency processing
55	Mainloop Alert module processing
56	Mainloop warm reset bottom half processing
57	I2C proxy
58	Mainloop Dynamic Voltage and Frequency Scaling (DVFS) request
59	Hard Fault handler
60	PCC AXI access
61	CPPC AXI access
62	I2C AXI access
63	Voltage Regulator Module (VRM) monitor
64	DDR scrubbing
65	SPI-NOR Write
66	SPI-NOR Erase
67	RAS Boot Error Record Table (BERT) storage
68	CCIX initialization
69	CCIX Extended Speed Mode (ESM) initialization
70	Generic Interrupt Controller (GIC) initialization
71	Mesh initialization
72	Power-On Self-Test (POST) module

LOCATION CODE	DESCRIPTION
73	DDR initialization
74	NVPARAM initialization
75	TPM initialization
76	TPM Extend
77	BMC module
78	VRM
79	2P module
80	Real-Time Clock (RTC) module

Table 9: SCP Error Code Descriptions

SCP ERROR CODE	LED FAULT	DESCRIPTION
0	N/A	No error
1	RAS_GPIO_INVALID_LCS	IPP_FAULT_TMMCFG_FAIL
2	RAS_GPIO_FILE_HDR_INVALID	IPP_FAULT_FILE_NOT_FOUND
3	RAS_GPIO_FILE_HDR_INVALID	IPP_FAULT_FILE_SIZE_ZERO
4	N/A	IPP_FAULT_INVALID_FILE
5	N/A	IPP_FAULT_INVALID_KEYCERT
6	N/A	IPP_FAULT_INVALID_CNTCERT
7	RAS_GPIO_FILE_INTEGRITY_INVALID	IPP_FAULT_SLIM_HDRCRC_FAIL
8	RAS_GPIO_FILE_INTEGRITY_INVALID	IPP_FAULT_SLIM_BOOTHDR_FAIL
9	RAS_GPIO_FILE_INTEGRITY_INVALID	IPP_FAULT_SLIM_BOOTCRC_FAIL
10	RAS_GPIO_KEY_CERT_AUTH_ERR	IPP_FAULT_KEY_CERT_AUTH_ERR
11	RAS_GPIO_CNT_CERT_AUTH_ERR	IPP_FAULT_CNT_CERT_AUTH_ERR
12	N/A	IPP_FAULT_SOC_HW_FAIL
13	RAS_GPIO_I2C_HARDWARE_ERR	IPP_FAULT_IIDMA_TO
14	N/A	IPP_FAULT_SOC_BOOTDEV_INIT_FAIL
15	RAS_GPIO_CRYPTO_ENGINE_ERR	IPP_FAULT_CRYPTO_RST_FAIL
16	RAS_GPIO_CRYPTO_ENGINE_ERR	IPP_FAULT_CRYPTO_INIT_FAIL
17	RAS_GPIO_CRYPTO_ENGINE_ERR	IPP_FAULT_CRYPTO_LCS_INIT
18	RAS_GPIO_CRYPTO_ENGINE_ERR	IPP_FAULT_CRYPTO_CERT_CHAIN
19	N/A	IPP_FAULT_CRYPTO_AUTH_FAIL
20	RAS_GPIO_I2C_HARDWARE_ERR	IPP_FAULT_FILE_READ_FAIL
21	RAS_GPIO_ROTPK_EFUSE_INVALID	IPP_FAULT_INVALID_ROTPK_EFUSE

SCP ERROR CODE	LED FAULT	DESCRIPTION
22	RAS_GPIO_SEED_EFUSE_INVALID	IPP_FAULT_INVALID_SEED_FROM_EFUSE
23	RAS_GPIO_LCS_FROM_EFUSE_INVALID	IPP_FAULT_INVALID_LCS_FROM_EFUSE
24	RAS_GPIO_PRIM_ROLLBACK_EFUSE_INVALID	IPP_FAULT_INVALID_PRIM_ROLLBACK_EFUSE
25	RAS_GPIO_SEC_ROLLBACK_EFUSE_INVALID	IPP_FAULT_INVALID_SEC_ROLLBACK_EFUSE
26	RAS_GPIO_HUK_EFUSE_INVALID	IPP_FAULT_INVALID_HUK_EFUSE
27	RAS_GPIO_CERT_DATA_INVALID	IPP_FAULT_INVALID_PRIM_ROLLBACK_CERT
28	RAS_GPIO_CERT_DATA_INVALID	IPP_FAULT_INVALID_HUK_FROM_CERT
29	RAS_GPIO_CERT_DATA_INVALID	IPP_FAULT_INVALID_SEED_FROM_CERT
30	RAS_GPIO_CERT_DATA_INVALID	IPP_FAULT_INVALID_SECOND_ROLLBACK_CERT
31	RAS_GPIO_CERT_DATA_INVALID	IPP_FAULT_INVALID_CERT_TYPE
32	RAS_GPIO_INTERNAL_HW_ERR	IPP_FAULT_ERR_PMPRO_FAIL
33	N/A	IPP_FAULT_SW_ERROR
34	RAS_GPIO_CERT_DATA_INVALID	IPP_FAULT_INVALID_DBG_DIS_CERT
35	RAS_GPIO_CERT_DATA_INVALID	IPP_FAULT_INVALID_ANTIROLLBACK_CERT
36	N/A	SLIM_OPEN_FILEHDL_MAXED_OUT
37	N/A	IPP_FAULT_CONSOLE_FIFO_TIMEOUT
38	RAS_GPIO_INTERNAL_HW_ERR	IPP_FAULT_EFUSE_OPS_TIMEOUT
39	RAS_GPIO_CERT_DATA_INVALID	IPP_FAULT_ANTIROLLBACK_VER_MISMATCH
40	RAS_GPIO_INTERNAL_HW_ERR	IPP_FAULT_NMI_EXCEP
41	RAS_GPIO_INTERNAL_HW_ERR	IPP_FAULT_HF_EXCEP
42	RAS_GPIO_INTERNAL_HW_ERR	IPP_FAULT_MEM_EXCEP
43	RAS_GPIO_INTERNAL_HW_ERR	IPP_FAULT_BUS_EXCEP
44	RAS_GPIO_INTERNAL_HW_ERR	IPP_FAULT_USE_EXCEP
45	RAS_GPIO_INTERNAL_HW_ERR	IPP_FAULT_EFUSE_COPY_FAIL
46	N/A	IPP_FAULT_SECJMP_FAIL
47	N/A	IPP_FAULT_PBAC_FAIL
48	N/A	IPP_FAULT_NO_LCS_EMU
49	N/A	IPP_FAULT_SEC_INTF_INIT_FAIL
50	N/A	IPP_FAULT_LOADER_INTF_INIT_FAIL
51	N/A	IPP_FAULT_SKIP_ERROR_CM_LCS
52	N/A	IPP_FAULT_CERT_SZ_OVERFLOW
53	RAS_GPIO_FILE_INTEGRITY_INVALID	IPP_FAULT_FILE_SZ_ZERO
54	RAS_GPIO_FILE_INTEGRITY_INVALID	IPP_FAULT_FILE_OFFSET_MISMATCH
55	RAS_GPIO_FILE_INTEGRITY_INVALID	IPP_INVALID_FILESZ_MORE_THAN_MAX

SCP ERROR CODE	LED FAULT	DESCRIPTION
56	N/A	IPP_FAULT_INVALID_VAL
57	RAS_GPIO_INTERNAL_HW_ERR	IPP_FAULT_ASEC_AUTH_AP_BL1
58	N/A	IPP_FAULT_APPLLLCK_FAIL
59	N/A	RAS_ERR_DDR_ZQCS_MC0
60	N/A	RAS_ERR_DDR_ZQCS_MC1
61	N/A	RAS_ERR_DDR_ZQCS_MC2
62	N/A	RAS_ERR_DDR_ZQCS_MC3
63	N/A	RAS_ERR_DDR_ZQCS_MC4
64	N/A	RAS_ERR_DDR_ZQCS_MC5
65	N/A	RAS_ERR_DDR_ZQCS_MC6
66	N/A	RAS_ERR_DDR_ZQCS_MC7
67	N/A	IPP_FAULT_PMDx_TIBDFT_FAIL
68	N/A	IPP_FAULT_PMDxPLLLCK_FAIL
69	N/A	AVS_ERR_VOLTAGE
70	N/A	AVS_ERR_VRM
71	N/A	AVS_ERR_PCP_PLL
72	N/A	AVS_ERR_PMD_PLL
73	N/A	PSCI_LPI_RUN_FAIL
74	N/A	PSCI_LPI_STANDBY_FAIL
75	N/A	PSCI_LPI_RETENTION_FAIL
76	N/A	PSCI_LPI_POWERDOWN_FAIL
77	N/A	IPP_BOARD_CFG
78	N/A	IPP_BOARD_CFG_VER
79	N/A	IPP_BOARD_CFG_SIZE
80	N/A	IPP_BOARD_CFG_DATA
81	N/A	IPP_FAULT_PCPPWR_FAIL
82	N/A	IPP_FAULT_CSW_TIBDFT_FAIL
83	N/A	IPP_FAULT_L3C_DFT_FAIL
84	N/A	IPP_FAULT_L3C_INIT_FAIL
85	N/A	IPP_FAULT_PCP_INIT_FAIL
86	N/A	IPP_FAULT_SPI_BUSERR
87	N/A	IPP_FAULT_SPI_NODEV
88	N/A	IPP_FAULT_SPI_READ_INCOMPLETE
89	N/A	RAS_ERR_CSR_MEM_NOT_RDY

SCP ERROR CODE	LED FAULT	DESCRIPTION
90	N/A	RAS_ERR_TPC
91	N/A	RAS_ERR_ALERT
92	N/A	RAS_ERR_WRST_FAIL
93	N/A	IPP_AXI_RESP_ERR
94	N/A	RAS_ERR_AXI_NON_FATAL
95	N/A	VRM_MONITOR_FAIL
96	N/A	RAS_ERR_DDR_SCRUB_MC0
97	N/A	RAS_ERR_DDR_SCRUB_MC1
98	N/A	RAS_ERR_DDR_SCRUB_MC2
99	N/A	RAS_ERR_DDR_SCRUB_MC3
100	N/A	RAS_ERR_DDR_SCRUB_MC4
101	N/A	RAS_ERR_DDR_SCRUB_MC5
102	N/A	RAS_ERR_DDR_SCRUB_MC6
103	N/A	RAS_ERR_DDR_SCRUB_MC7
104	N/A	RAS_BERT_STORE_FAIL
105	N/A	RAS_ERR_DDR_SERVICE_ZQCS
106	N/A	RAS_ERR_CCIX_RSB
107	N/A	RAS_ERR_CCIX_MEMRDY_FAIL
108	N/A	RAS_ERR_CCIX_TCVC_FAIL
109	N/A	RAS_ERR_CCIX_NOT_COMPLIANT
110	N/A	RAS_ERR_CCIX_GEN1_FAIL
111	N/A	RAS_ERR_CCIX_L1_PWR_FAIL
112	N/A	RAS_ERR_CCIX_L0_PWR_FAIL
113	N/A	RAS_ERR_CCIX_ESM_FAIL
114	N/A	RAS_ERR_CCIX_DR1_FAIL
115	N/A	RAS_ERR_CCIX_GEN4_FAIL
116	N/A	RAS_ERR_CCIX_RCA_LINKUP_FAIL
117	N/A	RAS_ERR_GIC_FAIL
118	N/A	RAS_ERR_MESH_CCIX_LINKUP_FAIL
119	N/A	IPP_ERR_IOB_SOC_WAKE
120	N/A	IPP_CONSOLE_OVERFLOW
121	N/A	IPP_FAULT_ASEC_AUTH_PMPRO
122	N/A	IPP_FAULT_NO_IIC_PROXY_DEV
123	N/A	IPP_POST_MSG

SCP ERROR CODE	LED FAULT	DESCRIPTION
124	N/A	RAS_ERR_DDR_SPD_READ_FAIL
125	N/A	RAS_ERR_PCP_MEM_REPAIR_FAIL
126	N/A	RAS_ERR_INVALID_OPERATION
127	N/A	RAS_ERR_NO_CPM_AVAIL
128	N/A	RAS_ERR_NO_MCU_AVAIL
129	N/A	IPP_FAULT_LOAD_AP_IMAGE
130	N/A	IPP_FAULT_LOAD_PMPRO
131	N/A	IPP_FAULT_PMD0DFT_FAIL
132	N/A	RAS_ERR_DDR_GET_DIMM_INFO
133	N/A	IPP_FAULT_OB2P_SLAVE_NOT_RDY
134	N/A	IPP_FAULT_PCP_PMPRO_INIT_FAIL
135	N/A	IPP_FAULT_TPM_INIT_FAIL
136	N/A	RAS_ERR_HOB_UPDATE_FAIL
137	N/A	RAS_SKU_NOT_VALID
138	N/A	IPP_FAULT_TPM_EXTEND_FAIL
139	N/A	RAS_ERR_BMC_OVERFLOW
140	N/A	RAS_ERR_MESH_FAIL
141	N/A	RAS_ERR_DDR_INVALID_MCU_MASK
142	N/A	IPP_FAULT_EFUSE_WR_TIMEOUT
143	N/A	IPP_FUSE_WR_DATA_MISTMATCH
144	N/A	IPP_FUSE_UNSUPPORTED_OPERATION
145	N/A	RAS_ERR_DDR_TRAINING_FAILED
146	N/A	RAS_ERR_PCIE_ROM_FAILED
147	N/A	RAS_ERR_CCIX_PHY_FAILED
148	N/A	RAS_ERR_DDR_NVDIMM_FAILED
149	N/A	IPP_FAULT_IIC_BUSERR
150	N/A	IPP_FAULT_ASEC_AUTH_AP_PLT
151	N/A	RAS_ERR_2P_RCA_PFA

The error code in the LED Fault column in *Table 9* causes the SCP to blink the fault LED accordingly.

Table 10 describes the usage of MPA_SCRATCH, MPA_SCRATCH1, MPA_SCRATCH2, and other scratch registers.

Table 10: SMpro/PMpro Scratch Register Usage

MPA REGISTERS	USAGE	FIELDS	DESCRIPTION
MPA_SCRATCH	Firmware version	31:28	ID: Magic Identifier (0xA)
		27:26	Mode: 0b01: ROM boot mode 0b10: Runtime boot mode 0b11: External boot mode
		25	Reserved
		24:23	TPM Mode: 0b11: Asymmetric secure boot 0b01: Symmetric secured boot 0b00: Normal boot
		22	QSStarted: 0b1: Altra released from reset
		21:18	Boot Mode: maps to BOOTDEV
		17	WarmBoot: SLIMpro Warm Boot Indicator
		16:8	Reserved
		7:4	Major Version number
		3:0	Minor Version number
MPA_SCRATCH1	Boot progress error code	31:28	Image type 0x1: ROM 0x2: External 0x3: Normal ROM 0x4: Secured ROM 0x5: Asymmetric Secured ROM 0x6: Symmetric Secured ROM 0x7: Runtime 0x8: Asymmetric Secured Runtime 0x9: Symmetric Secured Runtime 0xA: Any
		27	0b0: Enter 0b0: Exit
		26:16	Boot progress location for debugging purpose
		15:0	Error code

MPA REGISTERS	USAGE	FIELDS	DESCRIPTION
MPA_SCRATCH2	Warning code	31:28	Image type 0x1: ROM 0x2: External 0x3: Normal ROM 0x4: Secured ROM 0x5: Asymmetric Secured ROM 0x6: Symmetric Secured ROM 0x7: Runtime 0x8: Asymmetric Secured Runtime 0x9: Symmetric Secured Runtime 0xA: Any
		27	0b0: Enter 0b0: Exit
		26:16	Boot progress location for debugging purpose
		15:0	Error code
MPA_SCRATCH14	SCP features	31	Reserved
		30	TPC enabled
		29	AVS feature supported
		28	Reset feature supported
		27	Power off feature supported
		26	Version info supported
		25	System warm reset
		24	DVFS feature supported
		23:0	Reserved
MPA_SCRATCH15	Build date	31:24	Firmware build date (DD)
		23:16	Firmware build month (MM)
		15:0	Firmware build year (YYYY)

9. PE (Armv8 Core) State

By default, Armv8 cores are configured in the reset state. The master core is taken out of reset and executes from OCM at address 0x1d00_0000. Slave cores are taken out of reset and execute from addresses configured by PSCI, which is at the BL31 address on DDR.

Note that the core reset address is configurable in each core RVBAR register.

10. AVS

The SCP supports AVS. The firmware programs the VRM to provide the correct voltage provided the part supports AVS.

11. CLI

The SCP has a built-in CLI. For more information, contact Ampere Computing Support.

12. PE (Armv8 Core) and SoC Power

The SCP provides power usage by the PE (Armv8) and the SoC. This interface is the same as the TPC alarm. Refer to the Linux HWmon driver for SoC temperature and power information.

13. RAS and APEI

The SCP provides RAS and APEI support. For more information, refer to the ACPI APEI specification and Unified Extensible Firmware Interface (UEFI)documentation.

14. DVFS

The SCP supports DVFS. When DVFS is enabled, firmware scales voltage and frequency based on system load.

15. Maximum Frequency Mode

The SCP supports application processor (Armv8) maximum frequency mode. When enabled by UEFI, the operating system (OS) can scale PE frequencies to a maximum frequency as specified in the CPU ACPI table in UEFI.

16. SLIM Image Format

SLIM is an Ampere-developed firmware image format for managing various files stored on EEPROM and SPI-NOR flash. The boot image in the device must follow this specific format to load correctly. This section describes the structure of this image format. Files with a ".slim"extension follow this format.

SLIM is a simple image format and does not contain directories. SLIM also has minimal metadata containing a few fields and a file table for files present in the image. A SLIM image can be of variable length.

The SLIM metadata comprises two parts: the SLIM header and SLIM file table. At 512 bytes, the SLIM header is of fixed size. The SLIM file table contains a SLIM file table entry for each file encapsulated in the SLIM image. Each SLIM file table entry is fixed at 64 bytes in size. The size of the SLIM file table entry section is variable because a SLIM image can encapsulate any number of files. The SLIM file table size is N*64 bytes, where N is the number of files contained in the SLIM image.

This example illustrates a SLIM Image layout.

```
============================================================================
SLIM Header (64 bytes)
============================================================================
SLIM File Table (64 bytes * Number of Files)
============================================================================
File 1 Image (Variable length)
============================================================================
.....
============================================================================
File N Image (Variable length)
============================================================================
Backup SLIM Header (64 bytes)
============================================================================


SLIM Header
---------------
Byte Offset  Name                Size          Description
============================================================================
0           SIGNATURE            4 bytes        0x43435041 ("AMPC")
4           BLOCK_SIZE           4 bytes        Block size of boot device
8           FILE_COUNT           4 bytes        Number of entries in file table
12          BOOTFILE_NUMBER      4 bytes        Index of file to load (default 0)
16          BOOTFILE_LOAD_OFFSET 4 bytes        Image offset for on chip memory (default 0)
20          BOOTFILE_LOAD_SIZE   4 bytes        Image size to load (default 0)
24          Reserved
60          HEADER_CRC32         4 bytes        CRC32 for header
```

```
SLIM File Table Entry
-------------------------
Byte Offset  Name                Size           Description
===========================================================================
0           FILENAME             16 bytes       File name
16          OFFSET               4 bytes        Offset of image from start of SLIM image
20          SIZE                 4 bytes        Size if file in bytes
24          TIMESTAMP            4 bytes        File creating time stamp
28          RESERVED
60          CRC32                4 bytes        CRC32 of file contents
```

17. Document Revision History

ISSUE	DATE	DESCRIPTION
0.58	May 18, 2021	• Updated *Section 4.1, High-Temperature Threshold* to change the high-temperature threshold based on the product SKU. • Changed the title to "Ampere® Altra® Family 64-Bit Multi-Core Processor" to indicate that the User's Manual applies to both Altra and Altra Max.
0.57	April 23, 2021	• Changed SCP Error Code 149 from IPP_FAULT_RTC_GPI_LOCK to IPP_FAULT_IIC_BUSERR in *Table 9.* • Changed SCP Error Code 150 from IPP_FAULT_IIC_BUSERR to IPP_FAULT_ASEC_AUTH_AP_PLT in *Table 9*. • Changed SCP Error Code 151 from IPP_FAULT_ASEC_AUTH_AP_PLT to RAS_ERR_2P_RCA_PFA in *Table 9*.
0.56	February 9, 2021	• Added Location Codes 78 through 80 in *Table 8*. • Added SCP Error Codes 146 through 15 in *Table 9*.
0.55	September 21, 2020	• Added *Section 7, SCP Boot Process Code.* • Updated *Section 5.1, SMpro Doorbell Message Assignments*.
0.50	July 17, 2020	Initial issue.

May 18, 2021

Ampere Computing reserves the right to change or discontinue this product without notice.

While the information contained herein is believed to be accurate, such information is preliminary, and should not be relied upon for accuracy or completeness, and no representations or warranties of accuracy or completeness are made.

The information contained in this document is subject to change or withdrawal at any time without notice and is being provided on an "AS IS" basis without warranty or indemnity of any kind, whether express or implied, including without limitation, the implied warranties of non-infringement, merchantability, or fitness for a particular purpose.

Any products, services, or programs discussed in this document are sold or licensed under Ampere Computing's standard terms and conditions, copies of which may be obtained from your local Ampere Computing representative. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Ampere Computing or third parties.

Without limiting the generality of the foregoing, any performance data contained in this document was determined in a specific or controlled environment and not submitted to any formal Ampere Computing test. Therefore, the results obtained in other operating environments may vary significantly. Under no circumstances will Ampere Computing be liable for any damages whatsoever arising out of or resulting from any use of the document or the information contained herein.

Ampere Computing
4655 Great America Parkway, Santa Clara, CA 95054
Phone: (669) 770-3700
https://www.amperecomputing.com

Ampere Computing reserves the right to make changes to its products, its datasheets, or related documentation, without notice and warrants its products solely pursuant to its terms and conditions of sale, only to substantially comply with the latest available datasheet.