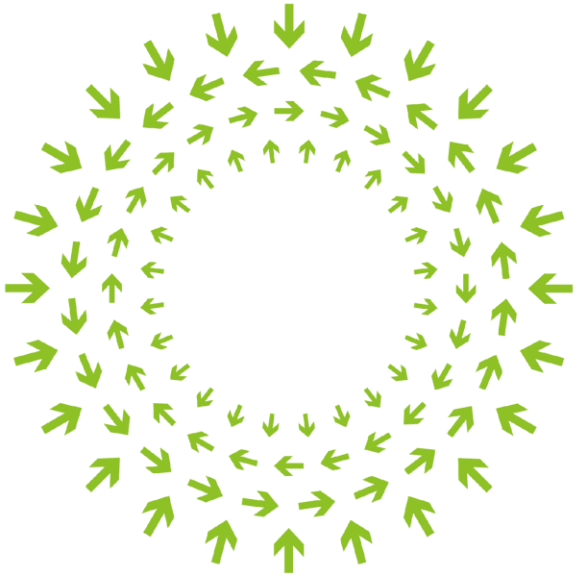


OPEN Compute Project

<Project Ersa AMC>
Design Specification

Revision 1
Version 1
Effective December 17, 2024

Authors
Intel: Kam Nasim, Evan Pang, Julien Carreno, Sreenadh Kareti, Karthick C
Microchip: Richard Wahler, Eileen Marando, Raghavendra Rao, Ravindra Kumar, Robert Schoepflin

Table of Contents

1. License 7
1.1. OPTION A: OCP CLA 7
1.2 Acknowledgements 8
2. Compliance with OCP Tenets 9
3. Change Log 10
4. Scope 11
5. Overview 12
6. Environmental / Regulatory Requirements 14
6.1 AMC Required Compliance 14
6.1.1 Required Environmental Compliance 14
6.1.2 Required EMC Compliance 15
6.1.3 Required Product Safety Compliance 16
6.1.4 Required Immunity (ESD) Compliance 16
7. Physical Specifications 17
7.1 TS1800 MCU 18
8 Mechanical 19
8.1 Accelerator + AMC PCB Overview 22
8.1.1 Board Stack-up 22
8.1.2 Board Placement Top Side 23
8.1.3 Board Placement bottom Side 23
8.1.4 Board Mechanical (unit: mm; Tolerance: ±0.1mm) 24
8.1.5 Board weight 24
9. Electrical Requirements 25
10. Thermal Design Requirements 26
10.1 Sensor Locations on Board 26
10.2 Fan Control 27
11. Interfaces 28
11.1 Interface Diagram 29
12. Onboard Power System 30

13. Prescribed Materials 32
14. System Firmware 32
15. Hardware Management 33
15.1 OOB Telemetry 33
15.1.1 Accelerator WAKE from D3Cold 35
15.1.2 Accelerator WAKE from D3Hot or Idle Mode 35
15.2 OOB Firmware Updates 37
15.2.1. Firmware Update Security Considerations 38
15.2.2 Firmware Update Image Layout 38
15.2.3 Firmware Update PLDM Flow 39
15.3 OOB Management and Debuggability 42
15.4 OOB Inventory Management 44
15.5 INB Hardware Management 45
16. Security 48
16.1 AMC PFR Compliance (NIST 800-193) 48
16.2 AMC RoT and System Secure Boot 48
16.2.1 AMC’s internal Secure Boot 51
16.2.2 Accelerator Secure Boot and RTM 53
16.3 AMC Survivability (RTRec) 55
16.4 Threat Model 56
16.4.1 Security Objectives 56
16.4.2 Assets 56
16.4.3 Minimum adversary model 58
16.4.4 Attack Surfaces 58
16.4.5 Vulnerability Analysis 58
16.5 Cryptographic Algorithms 58
16.6 Cryptographic Keys used in AMC 59
16.6.1 X.509 Certificate Chain 64
16.7 Random Number generation and sources of Entropy 64
16.8 Device Identity and Attestation 64
16.9 FIPS Certification 65
16.10 AMC Additional Security Requirements 65

16.11 Security Assurance 66
16.11.1 SBOM and provenance 66
16.11.2 Secure Development lifecycle 67
16.11.3 PSIRT process 67
17. Software Support (recommended) 68
18. References (recommended) 68
Appendix A - Checklist for IC approval of this Specification (to be completed by contributor(s) of this Spec) 69

Table of Figures

Figure 1: AMC + Accelerator System Diagram....17
Figure 2: Microchip TS1800 System Diagram....18
Figure 3: Microchip TS1800 Top and Bottom Plane Views....18
Figure 5: AMC (Microchip TS1800) WFBGA Pin Package – Top & Bottom Views....19
Figure 6: AMC (Microchip TS1800) WFBGA Pin Package – Planer Views....20
Figure 7: AMC (Microchip TS1800) WFBGA Pin Package – Routing Views....21
Figure 8: Board Stackup....22
Figure 9: Board Layout - Top View....23
Figure 10: Board Layout - Bottom View....23
Figure 11: Board Dimensions....24
Figure 12: Inlet/Outlet Thermal Sensor Placement....26
Figure 13: PWM and Tachometer based Fan Control....27
Figure 14: AMC to Accelerator Physical interconnects....28
Figure 15: AMC to Accelerator Interconnect Diagram....29
Figure 16: AMC Power Delivery....30
Figure 17: Accelerator Power On Sequence....31
Figure 18: OOB Telemetry System Diagram....33
Figure 19: OOB Firmware Update System Diagram....37
Figure 20: Unified Firmware Update Image....39
Figure 21: AMC's PLDM FW Update State Machine....41
Figure 22: In-Band and Out-of-Band SysDebug System Diagram....42
Figure 23: HPM to AMC In-Band over Accelerator I2C....46
Figure 24: AMC and Accelerator Secure Boot Flow:....49
Figure 25: AMC Internal Boot Flow....51
Figure 26: Accelerator Boot Flow....54
Figure 27: AMC Cert Chain - Single Stage Boot Loader....64
Figure 28: AMC Cert Chain - Two Stage Boot Loader....64

Table of Tables

Table 1: Compliance Summary 14
Table 2: Environmental Compliance....14
Table 3: EMC Compliance by Geo 15
Table 4: Product Safety Compliance standards....16
Table 5: Immunity (ESD) Compliance requirements....16
Table 6: Board Chassis Net Weight Target 24
Table 7:AMC's Electrical Requirements 25
Table 8: AMC Power Supply Operating Conditions 25
Table 9: Operating Temperature Range....26
Table 10: System Firmware Components 32
Table 11: Telemetry Domains and Data Types: 34
Table 12: PLDM command list for FW Updates....39
Table 13: SVID Error Reporting cmd group....43
Table 14: AMC Inventory (General FRU Table)....44
Table 15: AMC Inventory (OEM FRU Table) 45
Table 16: AMC RTRec features 55
Table 17: Primary Security Assets 56
Table 18: Secondary Security Assets....57
Table 19: Cryptographic Keys 59
Table 20: AMC Additional Security requirements 65

1. License

1.1. OPTION A: OCP CLA

Contributions to this Specification are made under the terms and conditions set forth in Open Compute Project Contribution License Agreement ("OCP CLA") ("Contribution License") by:

Intel Corporation, Microchip Technology Incorporated

You can review the Contributor License(s) for this Specification on the OCP website at https://www.opencompute.org/legal-documents. For actual executed copies of either agreement, please contact OCP directly.

Usage of this Specification is governed by the terms and conditions set forth in **Modified OWFa1.0 Final Specification Agreement (FSA) (As of August 16, 2021)** also known as a "Specification License".

Notes:

1. The above license does not apply to the Appendix or Appendices. The information in the Appendix or Appendices is for reference only and non-normative in nature.

NOTWITHSTANDING THE FOREGOING LICENSES, THIS SPECIFICATION IS PROVIDED BY OCP "AS IS" AND OCP EXPRESSLY DISCLAIMS ANY WARRANTIES (EXPRESS, IMPLIED, OR OTHERWISE), INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, FITNESS FOR A PARTICULAR PURPOSE, OR TITLE, RELATED TO THE SPECIFICATION. NOTICE IS HEREBY GIVEN, THAT OTHER RIGHTS NOT GRANTED AS SET FORTH ABOVE, INCLUDING WITHOUT LIMITATION, RIGHTS OF THIRD PARTIES WHO DID NOT EXECUTE THE ABOVE LICENSES, MAY BE IMPLICATED BY THE IMPLEMENTATION OF OR COMPLIANCE WITH THIS SPECIFICATION. OCP IS NOT RESPONSIBLE FOR IDENTIFYING RIGHTS FOR WHICH A LICENSE MAY BE REQUIRED IN ORDER TO IMPLEMENT THIS SPECIFICATION. THE ENTIRE RISK AS TO IMPLEMENTING OR OTHERWISE USING THE SPECIFICATION IS ASSUMED BY YOU. IN NO EVENT WILL OCP BE LIABLE TO YOU FOR ANY MONETARY DAMAGES WITH RESPECT TO ANY CLAIMS RELATED TO, OR ARISING OUT OF YOUR USE OF THIS SPECIFICATION, INCLUDING BUT NOT LIMITED TO ANY LIABILITY FOR LOST PROFITS OR ANY CONSEQUENTIAL, INCIDENTAL, INDIRECT, SPECIAL OR PUNITIVE DAMAGES OF ANY CHARACTER FROM ANY CAUSES OF ACTION OF ANY KIND WITH RESPECT TO THIS SPECIFICATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE, AND EVEN IF OCP HAS BEEN ADVISED OF

THE POSSIBILITY OF SUCH DAMAGE.

1.2 Acknowledgements

The Contributors of this Specification would like to acknowledge the following for their feedback:

Intel and Microchip engineering and project management teams involved in productizing the AMC and its various feature interactions with Accelerator devices

2. Compliance with OCP Tenets

- **Efficiency:** The On-Device Manageability solution, stipulated in this specification, allows for fine-grained Platform Security, Power sequencing, Psys flows, Thermal modulation, and Telemetry workflows allowing for more optimal monitoring and operation of the Accelerator device

- **Impact:** Leveraging Microchip's cutting edge TS1800 Manageability controller to meet Edge and Data Center Accelerator Manageability and Telemetry use-cases. Provides an implementation specification for the conceptualizations covered in the OCP Satellite Management Controller (SMC) smc-specification-1-0-final-pdf-1 (opencompute.org)

- **Scalability:** Allowing a single BMC/DC-SCM manageability scale out to multi-GPU via the Accelerator's on-device AMC supporting essential OOB Firmware Update, Telemetry/Monitoring/Attestation flows. This approach facilitates Accelerator ODMs to standardize the DC-SCM – AMC interactions via native DMTF protocols such as PLDM and Redfish, while relying on ODM's fine grained flows between AMC – Accelerator SOC. The converse of which (in the absence of the AMC) would have required aligning capabilities such as MCTP Bridging between the DC-SCM and the Accelerator SOC – limiting broad adoption against a wide range of Platforms.

- **Sustainability:** The AMC device referenced in this specification, as well as the target Accelerator device both follow strict Environmental, Regulatory, EMC, ESD and Product Safety Compliance requirements outlined later in this specification.

3. Change Log

Date	Version #	Author	Description
2024-12-17	1.0	Intel, Microchip	Initial Release

4. Scope

This document defines the Design Specification for Project Ersa which is an OCP **Auxiliary** **M**anagement **C**ontroller (formerly known as *Satellite Management Controller*), compliant module based on [smc-specification-1-0-final-pdf-1 (opencompute.org)] Base Specification. This specification shall here-on-after refer to this Module by its shortform “AMC”

The requirements and objectives for this specification include:

- Outline a reference implementation of the AMC module using the PCIe CEM card as the proposed form factor (but not limited to it)
    - AMC form-factor details include MCU, interconnects, mount-points, and electricals
- Definition of north-bound interfaces from AMC to DC-SCM
- Definition of south-bound interfaces from AMC to the Accelerator Device
- AMC’s Security posture, both as stand-alone security module, and relative to DC-SCM and Accelerator Device’s Silicon’s RoT
- INB and OOB Manageability use-cases in alignment with the SMC 1.0 specification
- Additional details and documentation to improve AMC’s adoption and interoperability across device designs including but not limited to schematic reference designs, PCB layouts, BOM list, component block diagrams, and firmware reference flows including Secure boot flow

Without limiting the scope, the following items are specifically out of scope for this specification:

- AMC as a Caliptra RoT
- Proprietary details pertaining to Intel’s Discrete GPU and Add-In Cards’ SOC and Process Node information
- Proprietary details pertaining to Microchip’s Management + Security Controller and Process Node information
- NIST ML-DSA usage for RoT enforcement and crypto functions
- At-Scale Debug (ASD) use-cases

5. Overview

This specification outlines the AMC module as a Manageability + Platform Firmware Resilient (PFR) compliant Device manageability solution specifically designed for Add-In Cards. We outline a reference design and firmware architecture for the AMC, based on the module's placement on our reference PCIe CEM v4 PCB for PCIe Gen5 compliant Add-In Cards. The AMC's Target of Evaluation (TOE) in this reference design includes a GPU Add-In Card for Data Center GPU Manageability solution and would fall under the **Accelerator** subsystem definition as outlined in Section 6 of the SMC v1.0 specification

The AMC module in alignment with the Accelerator sub-system definition shall have all of the following Roles & Responsibilities: -

- Telemetry Aggregation and INB/OOB Reporting to facilitate functions such as Thermal or Power Management
- Enable module management functions like Inventory(FRU) programming, VR configuration updates, Fan Control
- Software Management: INB/OOB Firmware Updates both of the AMC module as well as its TOE
- AMC as Device RoT for PFR functions such as RTD, RTU/RTRec, RTM

In our Project Ersa specification, the AMC conforms to API surfaces for the "Accelerator" device class as outlined in Section 6 of the SMC v1.0 base specification: -

Subsystem	Thermal	Inventory	Software Mgmt	Fan Control	Security	Power Mgmt
Accelerator	Supported	Supported	Supported	Supported	Supported	Supported

The Auxiliary Management Controller (AMC) design is meant to be complimentary to the DC-SCM. Where OCP DC-SCM TOE boundary includes the HPM (Host Platform Module) and the Satellite Controller on the Device, and correspondingly the AMC's TOE includes the Device Platform and Accelerator SOC.

The advantage of this dichotomy is that it allows for the Add-In Card vendor to control all infrastructure on the Device including its Remote Manageability and Device RoT posture allowing for great velocity and feature adoption along the device boundary.

A second advantage is scale-out as the AMC approach is a localized on-device management domain which acts an abstraction/funnel point for a DC-SCM that may have a number of Add-In devices connected on the platform and serialized switching across DC-SCM (BMC) – Accelerators is a larger management loop than switching across DC-SCM (BMC) -- AMC – Accelerators.

6. Environmental / Regulatory Requirements

Table 1: Compliance Summary

	(Microchip TS1800)
Operating Temp range	-40 C to +105 C
Storage Temperature Range	-55 C to +150 C
Transportation Temp	-55 C to +150 C
Lead Temp Range	Refer to JEDEC Spec J-STD-020B
Operating Voltage	3.3V +/- 5% 1.8V +/- 5%
RoHS, REACH, China ROHS	Comply

6.1 AMC Required Compliance

A card containing the AMC Module, and its downstream Accelerator device shall meet the following Environmental, EMC and Safety requirements.

6.1.1 Required Environmental Compliance

Table 2: Environmental Compliance

Standard	**Details**
China RoHS Directive	Chinese government regulation to control certain materials, including lead. The Ministry of Industry and Information Technology
EU RoHS 2 Directive (2011/65/EU)	Aims to reduce the environmental impact of electronic and electrical equipment (EEE) by restricting the use of certain hazardous materials. The substances banned under RoHS are lead, mercury, cadmium, hexavalent chromium, polybrominated biphenyls, polybrominated diphenyl ether, and four phthalates
EU REACH Regulation (EC) No 1907/2006	Addresses the production and use of chemical substances and their potential impact on human health and the environment.
	Mandates the treatment, recovery and recycling of EEE

EU Waste Electrical and Electronic Equipment (“WEEE”) Directive (2012/19/EU)	
The Persistent Organic Pollutants Regulation (EC) No. 850/2004	Bans production, placing on the market and use of certain persistent organic pollutants
The California Safe Drinking Water and Toxic Enforcement Act of 1986 (“Proposition 65”)	Sets forth a list of regulated chemicals that require warnings in the State of California
The Packaging and Packaging Waste Directive 94/62/EC	Limits certain hazardous substances in the packaging materials
Batteries Directive 2006/66/EC	Regulates the manufacture and disposal of all batteries and accumulators, including those included in appliances
Taiwan BSMI RoHS CNS 15663	Guidance to Reduce the Use of Restricted Chemical Substances in Electrical and Electronic Equipment (EEE)" acts as a roadmap for companies seeking to comply with Taiwan RoHS and reduce the presence of restricted chemicals in their products.

6.1.2 Required EMC Compliance

Radiated and Conducted Emissions requirements are based on deployed geographical locations. Refer to Table 3 for details.

Table 3: EMC Compliance by Geo

Targeted Geography	Applicable Specifications
USA	FCC, 47 CFR Part 15, Class A digital device (USA)
Canada	ICES-003, class A (CAN)
EU	EN 55032:2015/A11:2020 Class A Radiated and Conducted Emissions requirements for European Union
	EN 55035:2017/A11:2020 Immunity requirements for the European Union (EU)
Australia/ New Zealand	AS/NZS CISPR 32:2015 Class A
	CISPR 32:2015 for Radiated and Conducted Emissions requirements

Japan	VCCI 32-1 Class A Radiated and Conducted Emissions requirements
Korea	KS C 9832 – Radiated and Conducted Emissions
	KS C 9835- Immunity
Taiwan	BSMI CNS 15936:2016 (complete) Class A Radiated and Conducted Emissions requirements

- *CE – Equipment must pass the CE specification*
- *All technical requirements covered under EMC Directive (2014/30/EU)*

6.1.3 Required Product Safety Compliance

Table 4: Product Safety Compliance standards

Targeted Category	Applicable Specifications
Safety	IEC 62368-1:2018 or IEC 62368-1:2023, and UL 62368-1 and CAN/CSA C22.2 No. 62368-1-19, 3rd Edition. Audio/video, information, and communication technology equipment Part 1: Safety requirements.

6.1.4 Required Immunity (ESD) Compliance

The AMC module and the card that contains it and the Accelerator Module shall meet or exceed the following ESD immunity requirements listed in *Table 5*

Table 5: Immunity (ESD) Compliance requirements

Targeted Category	Applicable Specifications
Immunity (ESD)	EN 55035:2017/A11:2020, and IEC 61000-4-2 2008 for ESD.
NEBS Level 3 (optional)	Optionally test devices to NEBS Level 3 – Required ±8 kV contact discharge and ±15 kV air discharge with interruptions not greater than 2 seconds. The device shall self-recover without operator intervention Note: NEBS compliance is part of the system level testing. The OCP DC-SCM 2.0 specification is providing a baseline minimum recommendation for ESD

7. Physical Specifications

The following block diagram outlines the AMC logical architecture in relation to its connections to the Accelerator, the HPM (Host) and the DC-SCM. The exact details of these interconnects are outlined in Section 11.

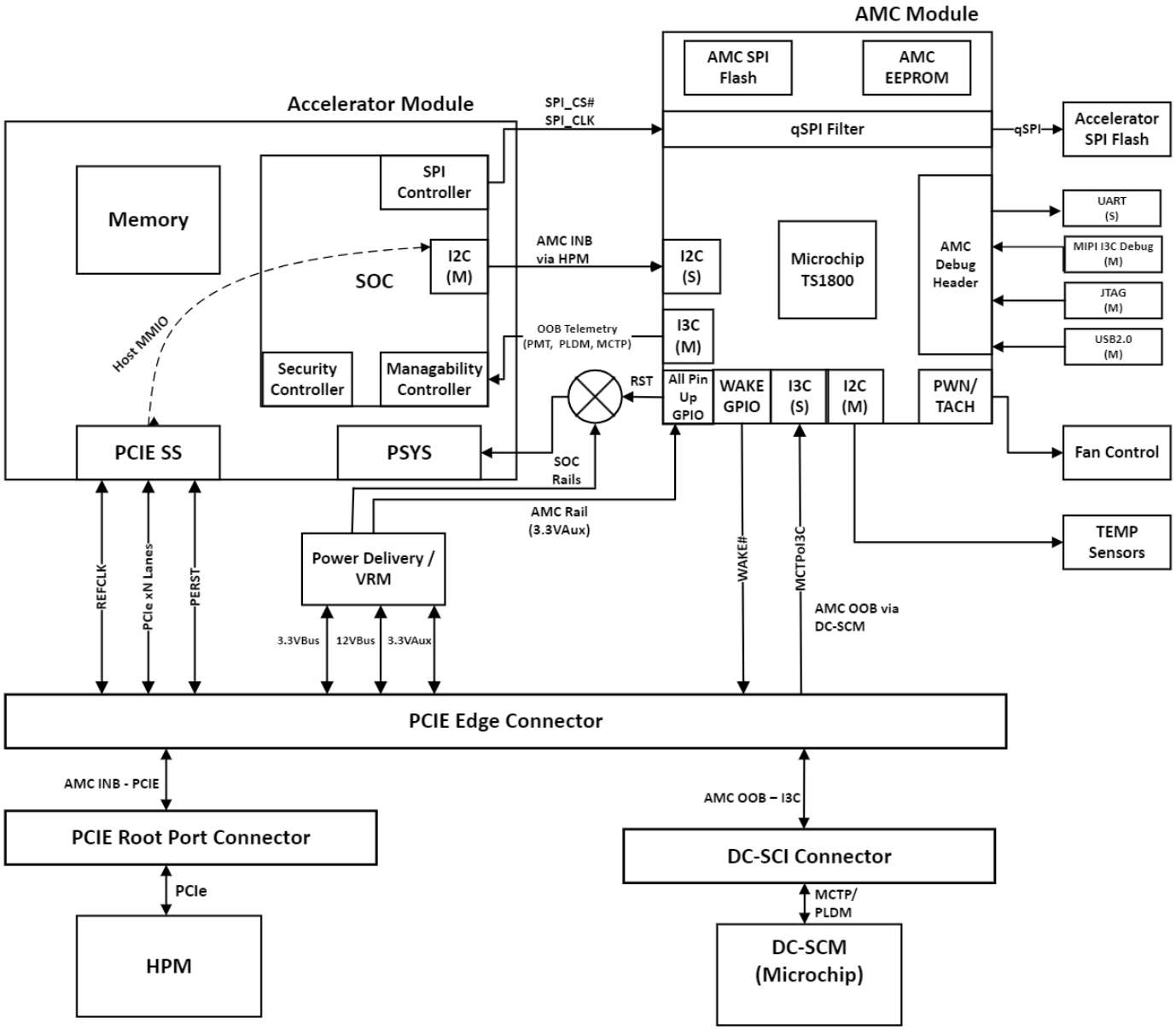


Figure 1: AMC + Accelerator System Diagram

7.1 TS1800 MCU

Project Ersa is built upon Microchip's TS1800 MCU part that functions as the AMC. The module's system diagram is as follows

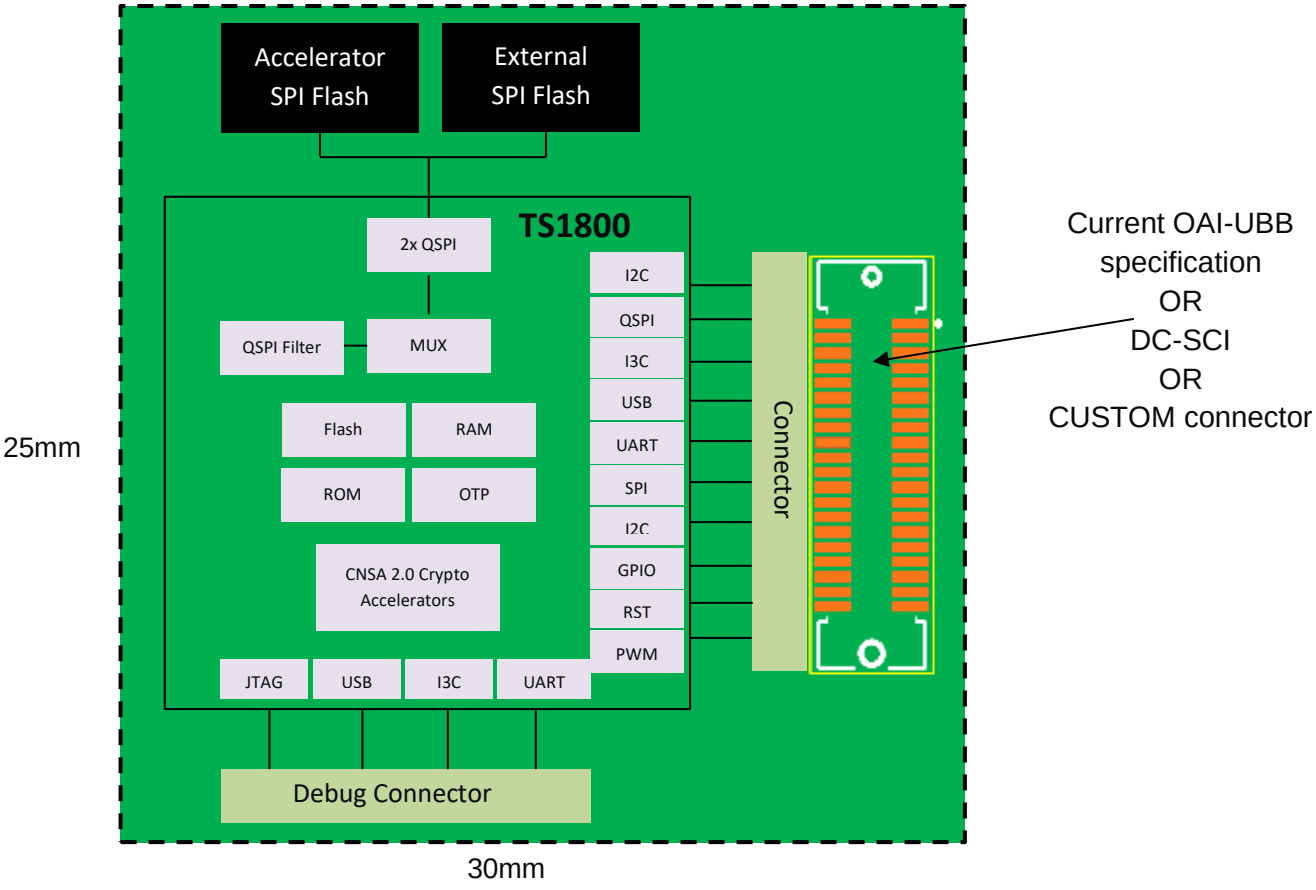


Figure 2: Microchip TS1800 System Diagram

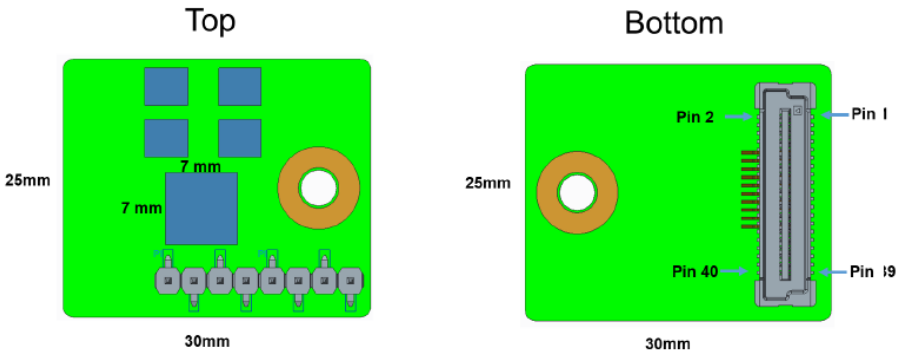


Figure 3: Microchip TS1800 Top and Bottom Plane Views

8 Mechanical

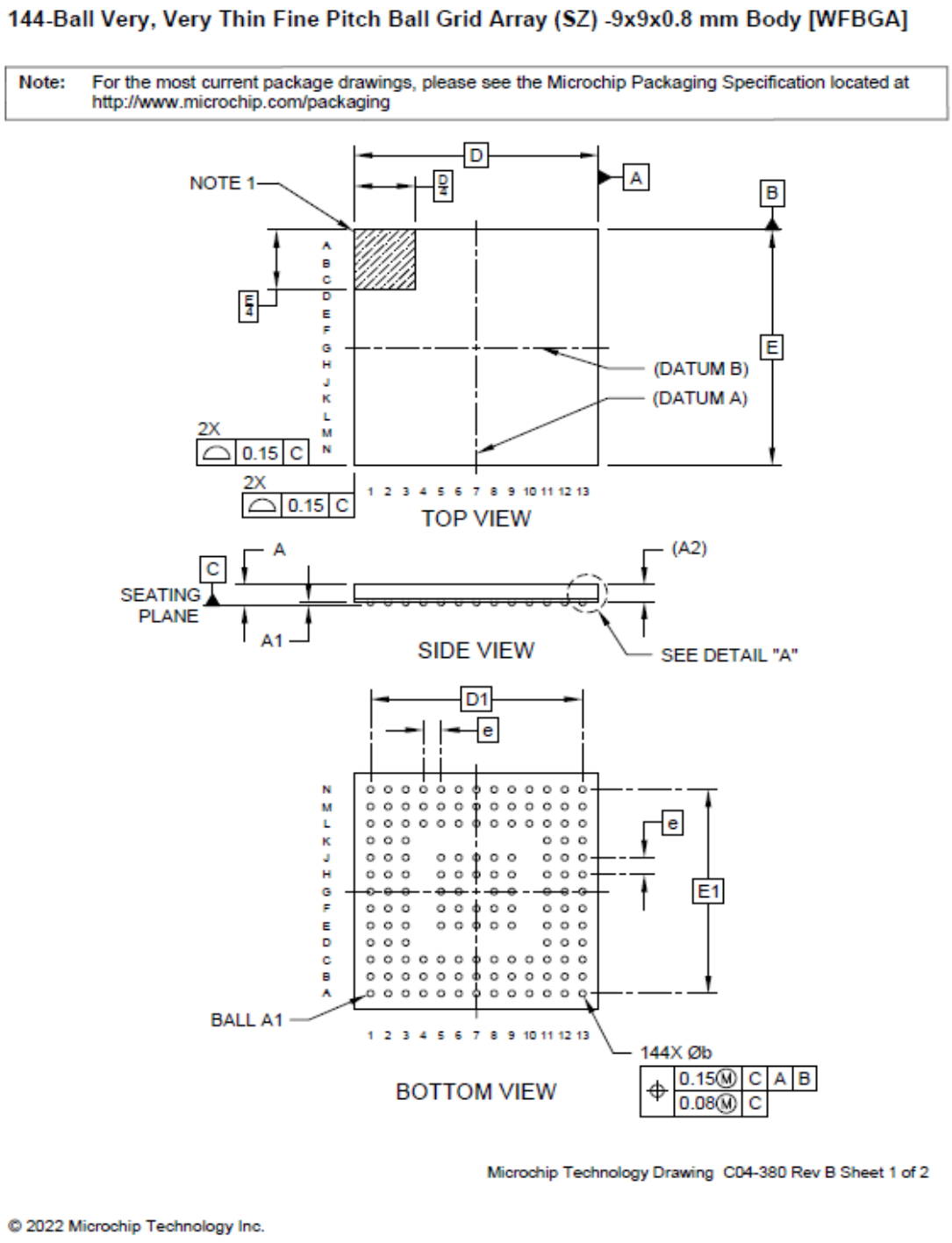
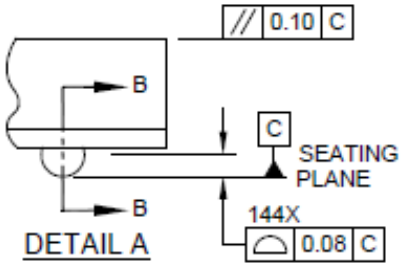
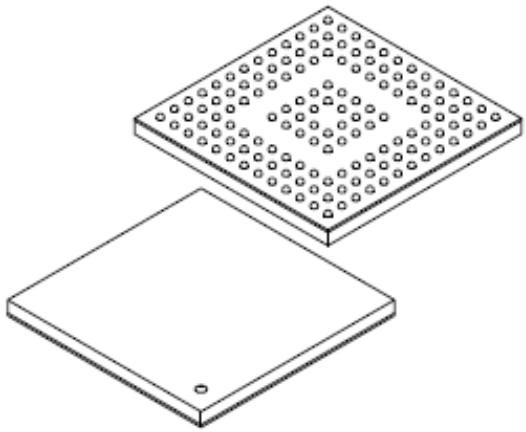


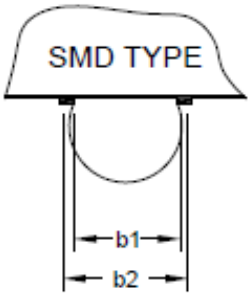
Figure 4: AMC (Microchip TS1800) WFBGA Pin Package – Top & Bottom Views

144-Ball Very, Very Thin Fine Pitch Ball Grid Array (SZ) -9x9x0.8 mm Body [WFBGA]

Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging







Units		MILLIMETERS		
Dimension Limits		MIN	NOM	MAX
Ball Pitch	e		0.65 BSC	
Overall Height (see Note 7)	A	-	0.70	0.80
Standoff	A1	0.12	0.17	0.22
Terminal Thickness	A2		0.53 REF	
Overall Length	D		9.00 BSC	
Overall Ball Pitch	D1		7.80 BSC	
Overall Width	E		9.00 BSC	
Overall Ball Pitch	E1		7.80 BSC	
Ball Diameter	b	0.20	0.25	0.30
Finished Solder Mask Opening	b1	0.22	0.25	0.28
Finished Bottom Ball Pad	b2	0.30	0.35	0.40

Notes:

1. Ball A1 visual index feature may vary, but must be located within the hatched area.
2. Package is saw singulated
3. Dimensioning and tolerancing per ASME Y14.5M
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.
   REF: Reference Dimension, usually without tolerance, for information purposes only.
4. Primary Datum "C" and Seating Plane are defined by the spherical crowns of the contact solder balls.
5. Dimension "A" does not include attached external featues, such as heat sink or chip capacitors.
6. The package ball solderable surface is solder-mask defined (SMD) type.
7. Maximum Overall Height for LAN7515 parts only is 0.90 mm.

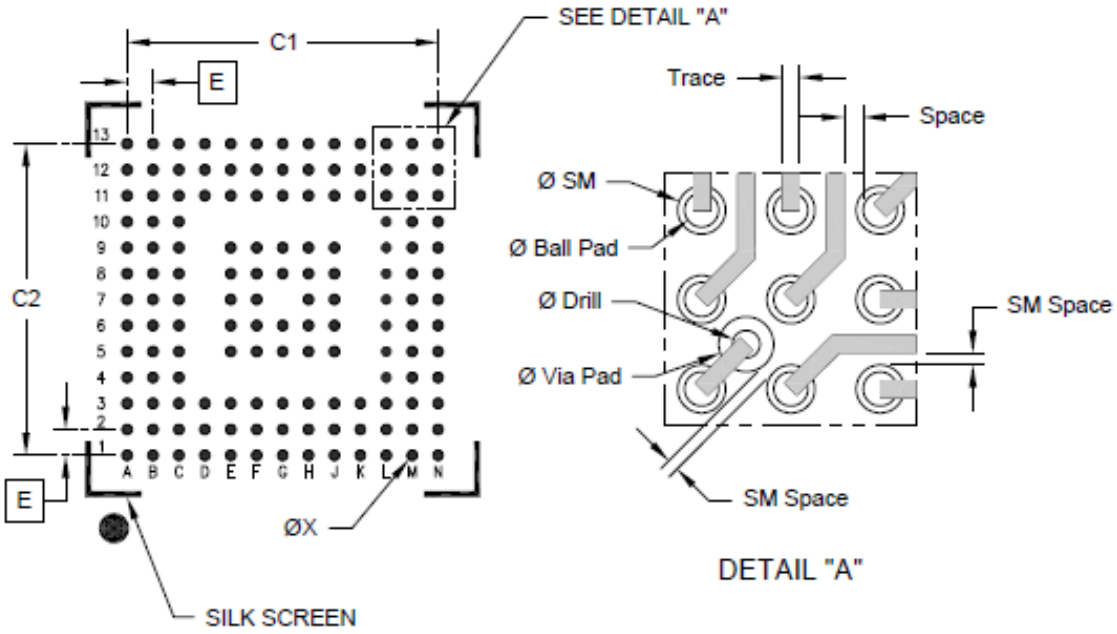
Microchip Technology Drawing C04-380 Rev B Sheet 2 of 2

© 2022 Microchip Technology Inc.

Figure 5: AMC (Microchip TS1800) WFBGA Pin Package – Planer Views

144-Ball Very, Very Thin Fine Pitch Ball Grid Array (SZ) -9x9x0.8 mm Body [WFBGA]

Note:	For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



RECOMMENDED LAND PATTERN

Units		MILLIMETERS		
Dimension Limits		MIN	NOM	MAX
Contact Pitch	E		0.65 BSC	
Overall Contact Pitch	C1		7.80	
Overall Contact Pitch	C2		7.80	
Contact Pad Diameter	X		0.25	

Routing Dimensions

Units	mm
Feature	
Ø PAD	0.250
Ø SM	0.350
Trace Width	0.125
Space (Min.)	0.135
SM Space (Min.)	0.085
Ø Via Pad	0.400
Ø Drill	0.200

Notes:

1. Dimensioning and tolerancing per ASME Y14.5M

BSC: Basic Dimension. Theoretically exact value shown without tolerances.

Microchip Technology Drawing C04-2380 Rev B

© 2022 Microchip Technology Inc.

Figure 6: AMC (Microchip TS1800) WFBGA Pin Package – Routing Views

8.1 Accelerator + AMC PCB Overview

8.1.1 Board Stack-up

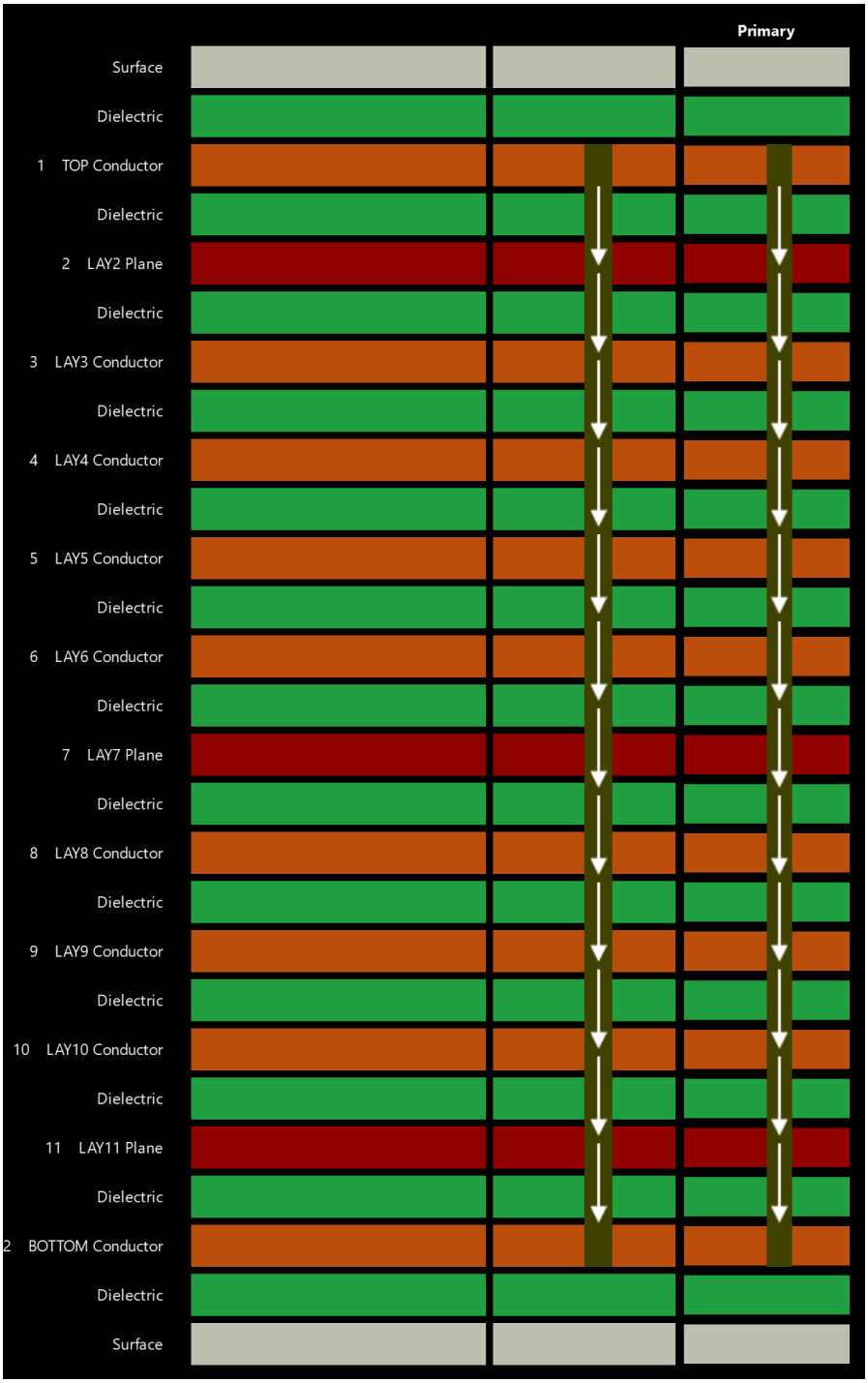


Figure 7: Board Stackup

8.1.2 Board Placement Top Side

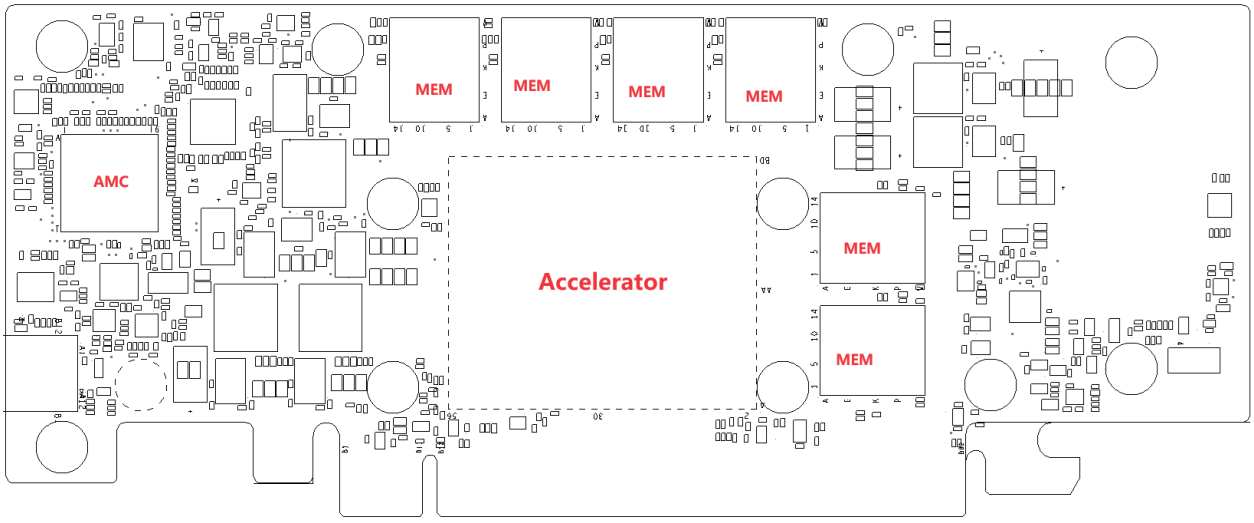


Figure 8: Board Layout - Top View

8.1.3 Board Placement bottom Side

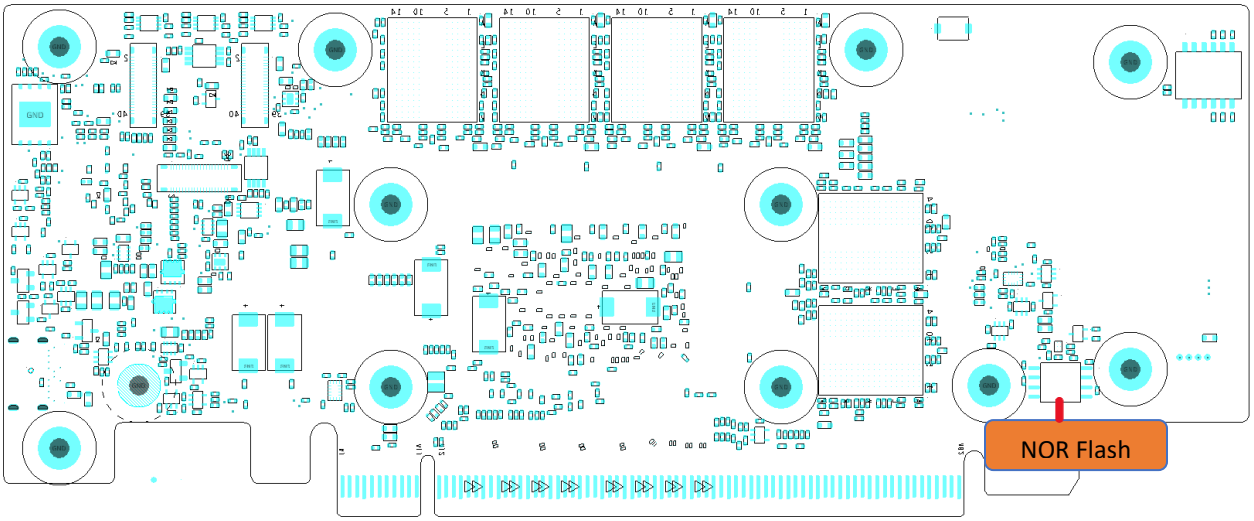


Figure 9: Board Layout - Bottom View

8.1.4 Board Mechanical (unit: mm; Tolerance: ±0.1mm)

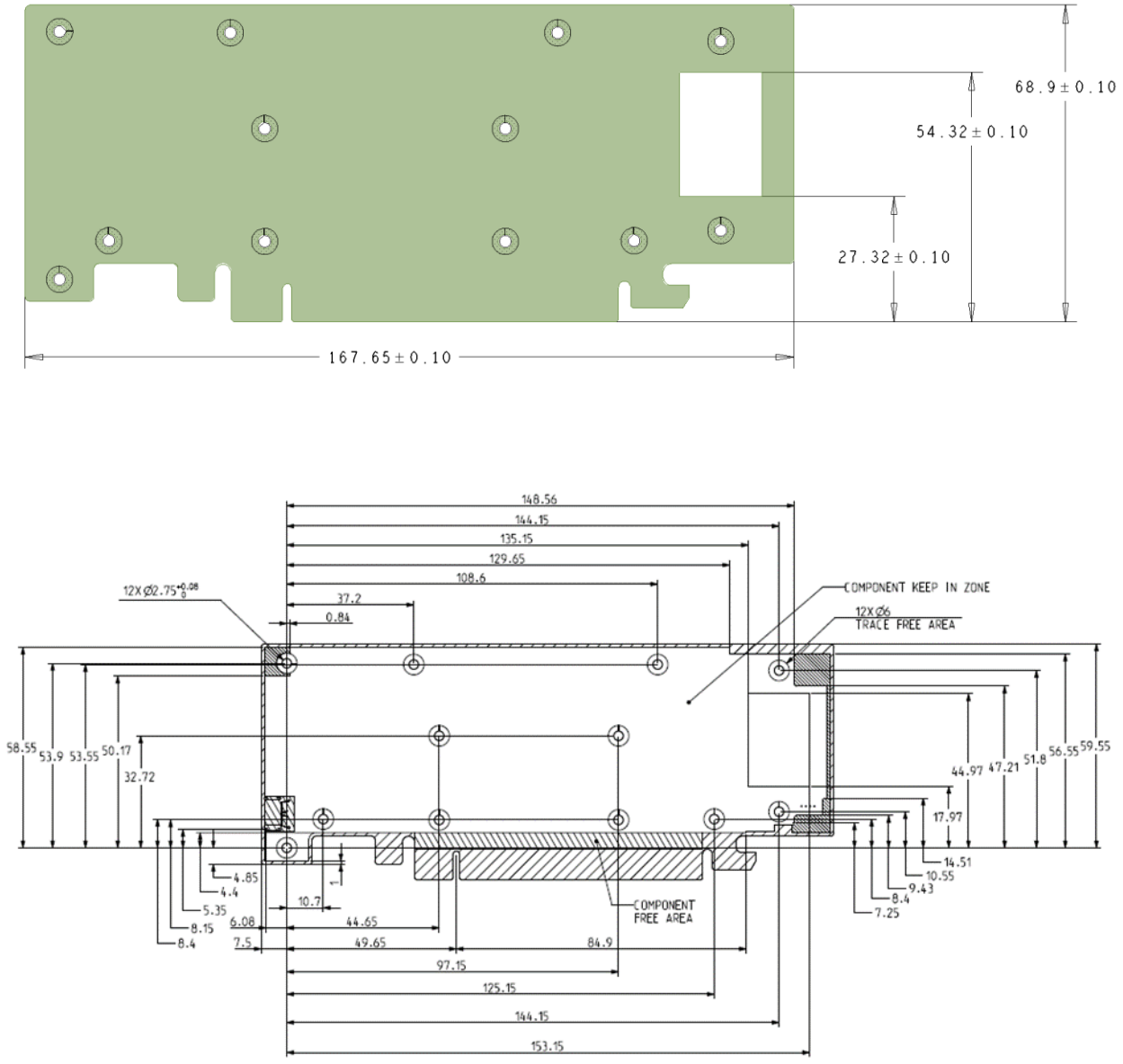


Figure 10: Board Dimensions

8.1.5 Board weight

Table 6: Board Chassis Net Weight Target

Net Weight	Less than 1.2 KG

9. Electrical Requirements

The AMC (Microchip TS1800) used within this specification has its base electrical requirements captured in *Table 7*. *Table 8* captures the PSU's operating conditions across min, max and typical

Table 7:AMC's Electrical Requirements

Power rail	+3.3V (Vcc3_3)	+V12	+3.3Vaux
Voltage tolerance	± 9% (max)	± 8% (max)	± 9% (max)
Supply Current	3.0 A (max)	5.5 A (max)	375 mA (max)
Capacitive Load	1000 µF (max)	2000 µF (max)	150 µF (max)

Table 8: AMC Power Supply Operating Conditions

Symbol	Parameter	MIN	TYP	MAX	Units
VTR_REG	*Main Regulator Power Supply (1.8V)*	*1.71*	*1.8*	*1.89*	*V*
	Main Regulator Power Supply (3.3V)	*3.135*	*3.3*	*3.465*	*V*
VTR_ANALOG	*Analog Power Supply*	*3.135*	*3.3*	*3.465*	*V*
VTRx	*3.3V Power Supply*	*3.135*	*3.3*	*3.465*	*V*
	1.8V Power Supply	*1.71*	*1.8*	*1.89*	*V*
VTR_PLL	*PLL Power Supply*	*3.135*	*3.3*	*3.465*	*V*
VTR_USB_PHY	*USB Phy Power Supply*	*3.135*	*3.3*	*3.465*	*V*
VTR_QSWITCH	*QSWITCH Power Supply*	*3.135*	*3.3*	*3.465*	*V*

10. Thermal Design Requirements

Table 9: Operating Temperature Range

Temperature Range (Ambient)	Min	Max
Operating (°C)	0	55
Storage (°C)	-40	70

Project Ersa and its components are expected to operate without any thermal issues and meet thermal reliability requirements in the above environmental conditions.

10.1 Sensor Locations on Board

There are two ambient temperature sensors on the module. When the card is installed at PCIe slot of the chassis, Temperature Sensor #2 measures the inlet temperature of the module and Temperature Sensor #1 measures the outlet temperature of the module. BMC firmware accesses these temperature sensors via I2C bus. See the figure below for the approximate sensor locations on the board.

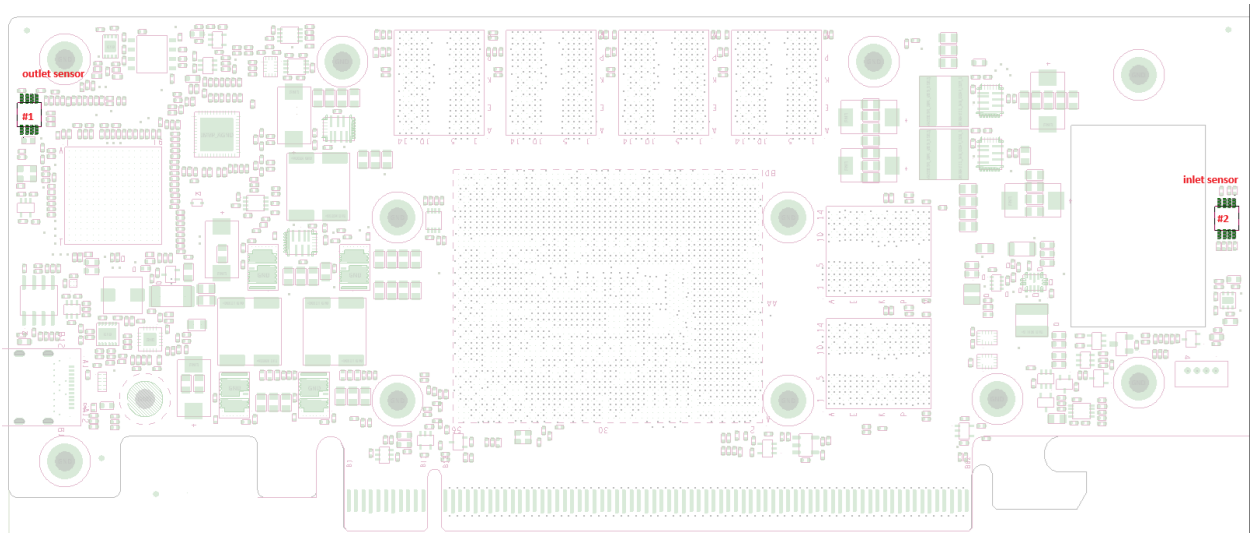


Figure 11: Inlet/Outlet Thermal Sensor Placement

10.2 Fan Control

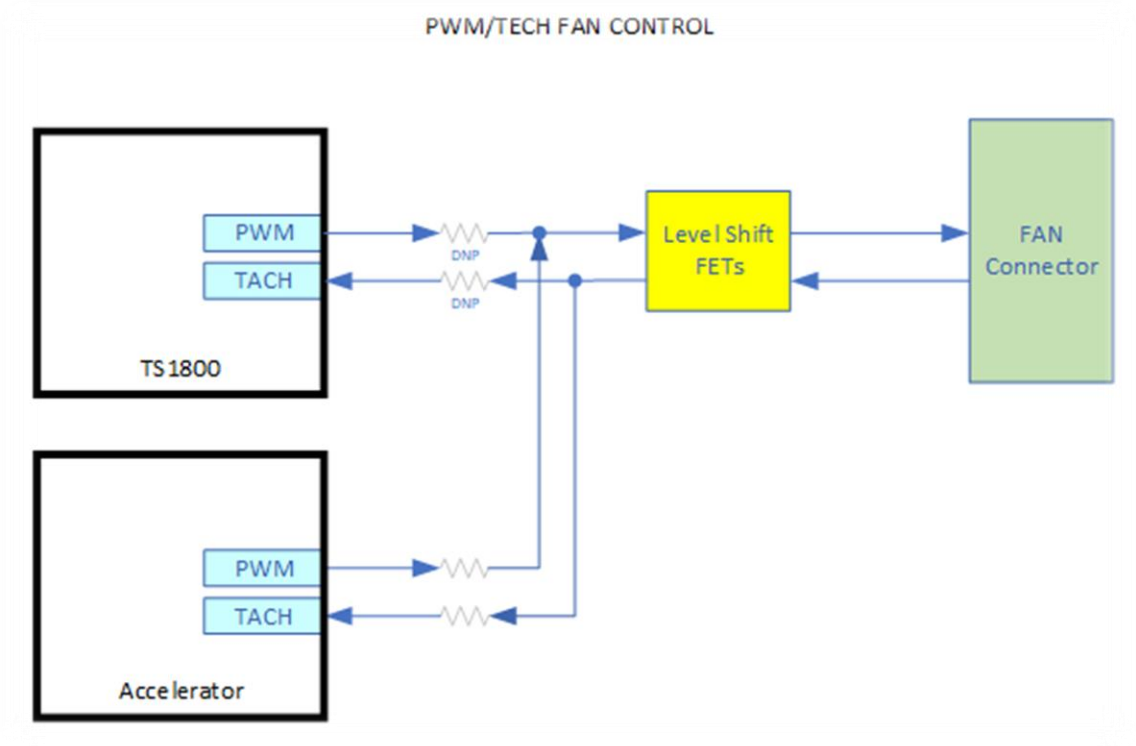


Figure 12: PWM and Tachometer based Fan Control

The Accelerator PCB may include a Fan Controller. With PWM and Tachometer control via the Accelerator SOC and the AMC (i.e. the Microchip TS1800 MCU). An isolation FET is provisioned on the Accelerator PCB to ensure that the INB Fan Control (via Accelerator SOC) and the OOB Fan Control (via AMC) do not conflict.

11. Interfaces

All Interfaces defined from AMC's point of view, i.e. either a Host or Device placement on the AMC and a corresponding placement either within the AMC itself, its Debug Module, the Accelerator Module, or as a Peripheral on the Board

- **Note:** The terms Host/Device, Output/Input, Primary/Secondary or other conventional variants are used interchangeably in this table and other sections of this document

Interface Type	TS1800 interface	Direction	Function	Pairing's Placement
I2C	I2C00	Host	FRU EEPROM (8KB)	AMC Module
fwSPI	QSPI2	Host	AMC SPI Flash (Accelerator staging)	AMC Module
UART	UART	Device	Serial Debug	AMC Debug Module
JTAG	JTAG	Device	Open Chassis Debug	AMC Debug Module
I3C	I3C00	Device	Closed Chassis Debug	AMC Debug Module
USB2.0	USB2.0	Device	At-Scale Debug	AMC Debug Module
PWM	PWM0	Host	Fan Controller	Board Module
TACH	ICT9	Host	Fan Controller	Boad Module
I2C	I2C10	Host	Ambient Temperature Sensors	Board Module
GPIO	GPIO017	Output	WAKE# Pinout to PCIe Edge Connector	Board Module
GPIO	GPIO114	Input	All-Pin-Up (Power Good)	Accelerator Module
I2C	I2C06	Device	AMC INB via HPM	Accelerator Module (legacy DC-SCM -> AMC connection)
QSPI1	QSPI0	Device	SPI Filter for incoming access to Accelerator SPI Flash	Accelerator Module
QSPI2	QSPI1	Host	Outgoing to Accelerator SPI Flash	Board Module
I3C	I3C01	Host	MCTP o I3C for OOB Telemetry, Firmware Updates	Accelerator Module
I2C	I2C15	Host	IMVP VR access and upgrade	Board Module

Figure 13: AMC to Accelerator Physical interconnects

11.1 Interface Diagram

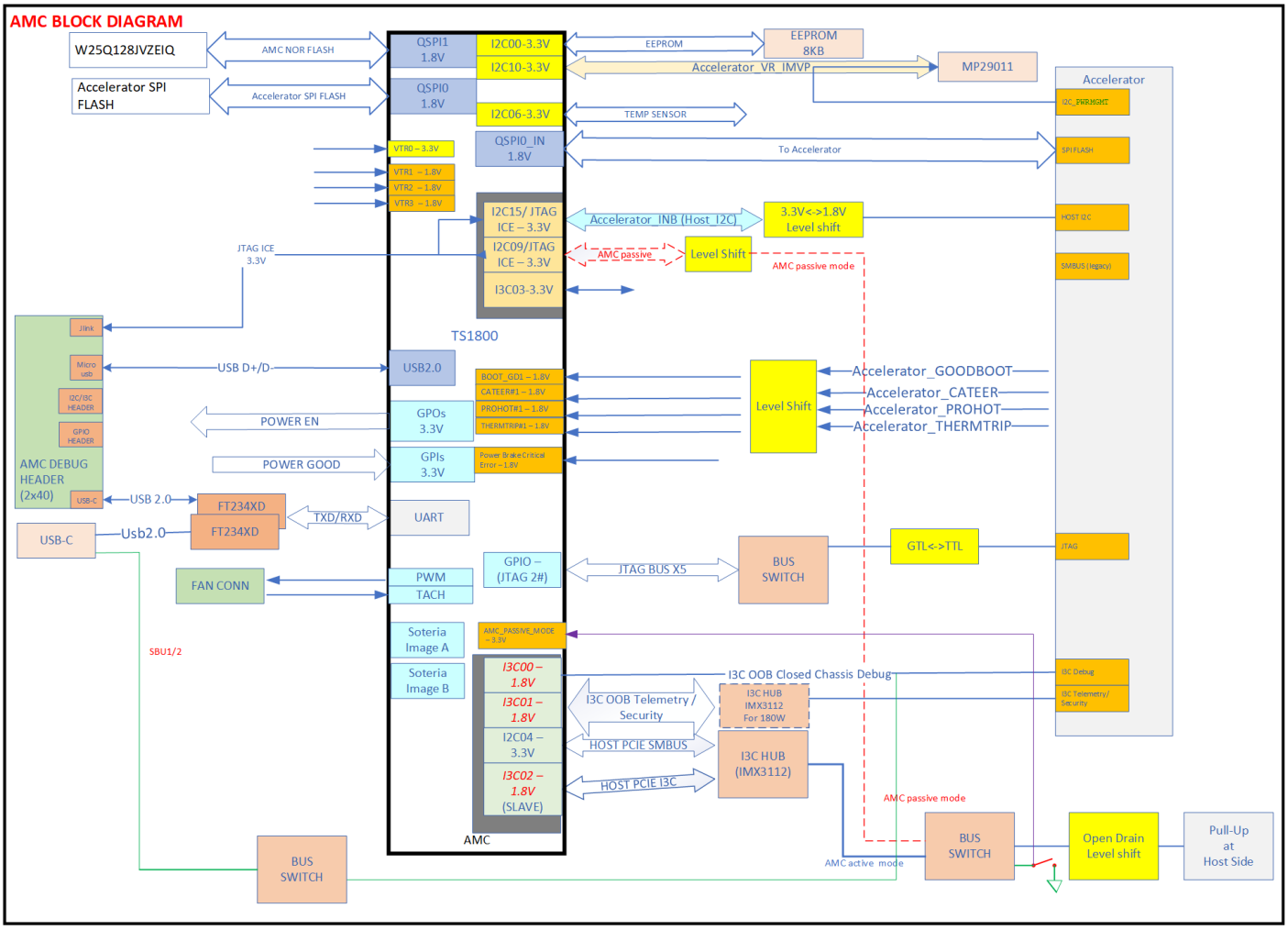


Figure 14: AMC to Accelerator Interconnect Diagram

12. Onboard Power System

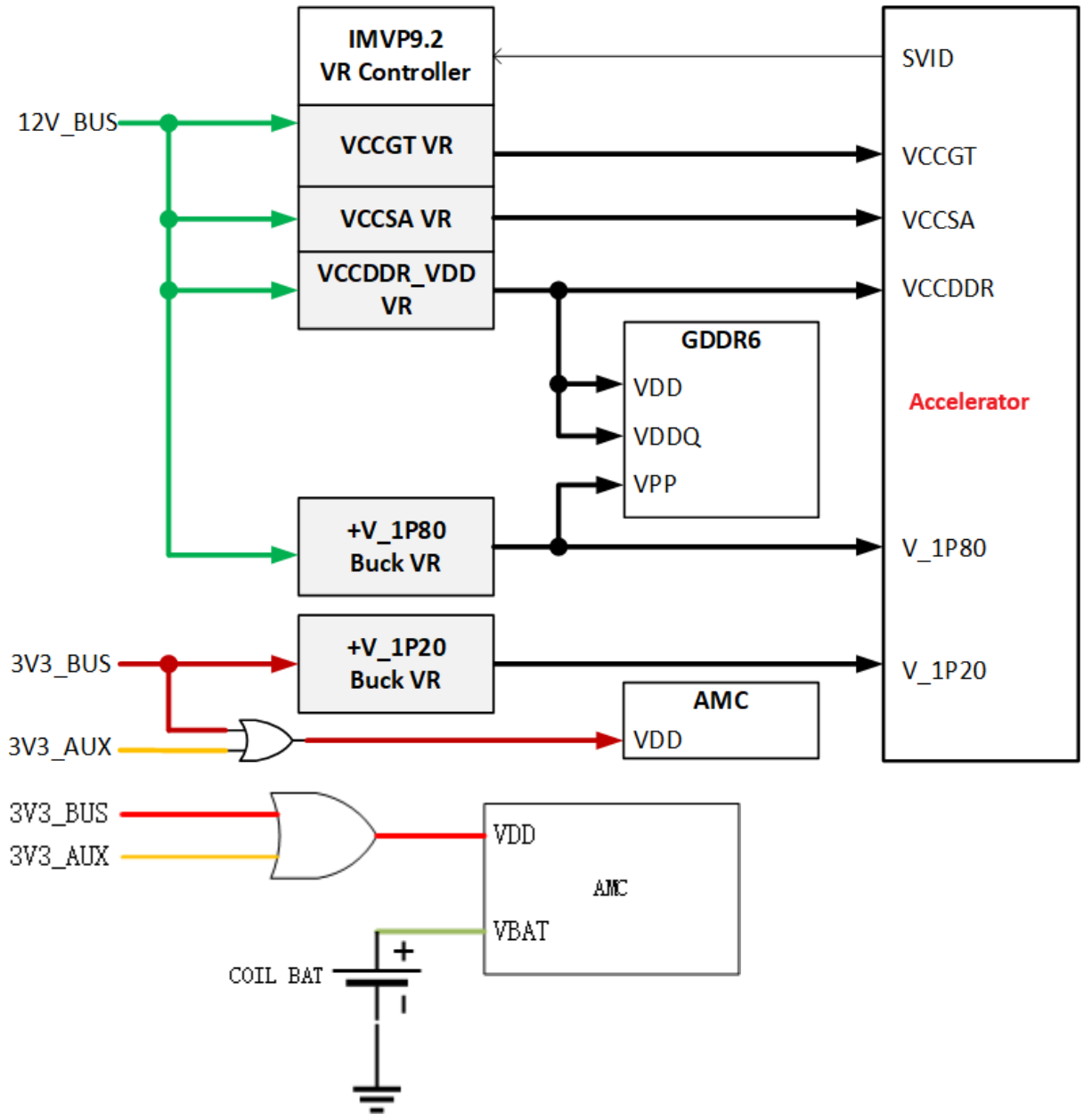


Figure 15: AMC Power Delivery

AMC typically runs on the 3.3Vaux rail. It is expected that the Platform supplies the Aux rail in conjunction to the 3.3VBus (Main) rail. The Accelerator runs off the 3.3VBus with AMC controlling the VR to Accelerator SOC rail de-assertion flow. The Power on Sequence for the AMC and the downstream Accelerator is defined as follows: -

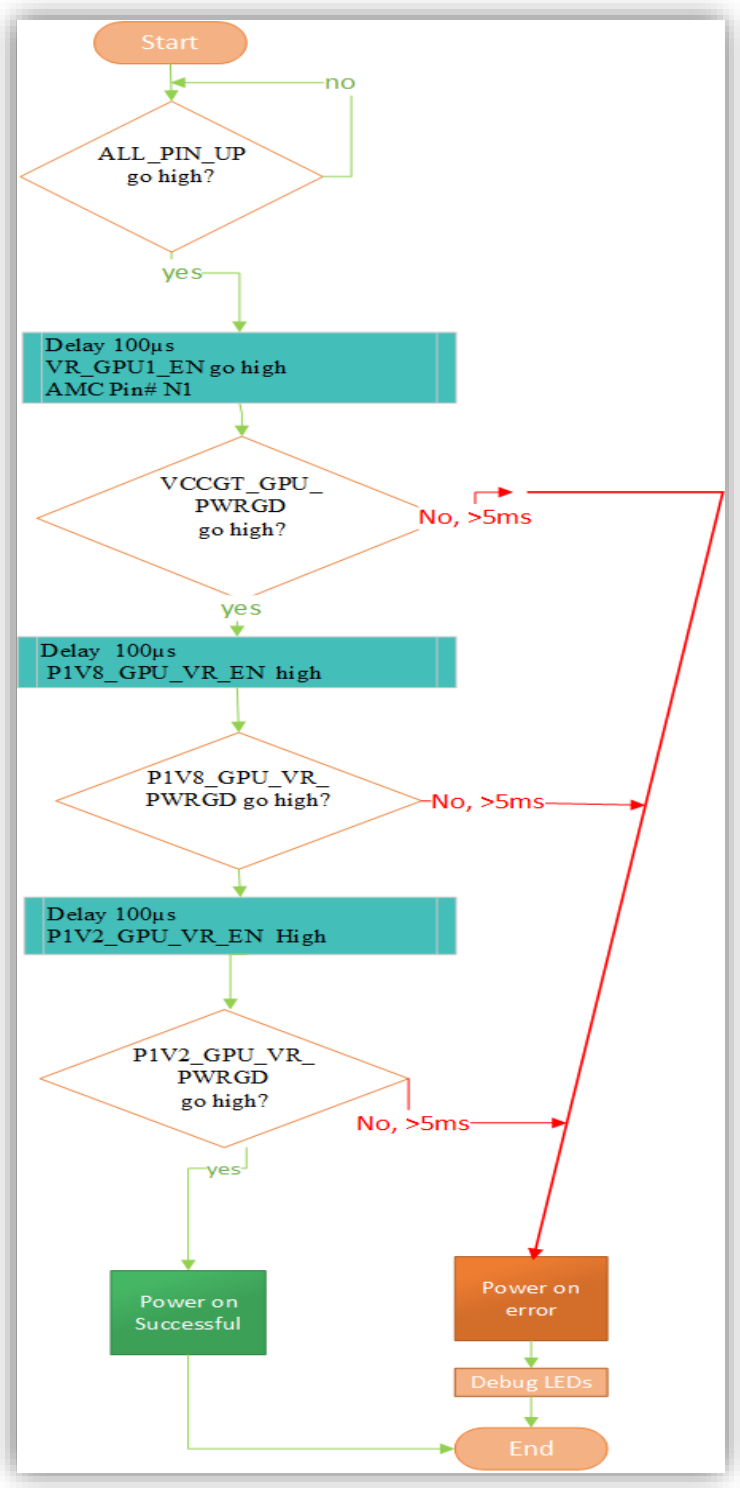


Figure 16: Accelerator Power On Sequence

13. Prescribed Materials

- Open-Source Zephyr RTOS (version 3.4 and above recommended) is the targeted base OS for the AMC Firmware stack. AMC's manageability, telemetry, security and workflows are provisioned as Kernel or User space applications within the context of the Zephyr RTOS

14. System Firmware

The System Firmware stack for customers planning to deploy Project Ersa, involves the following logical components:

Table 10: System Firmware Components

Component	Domain
AMC ROM and ROM Extensions	Microchip TS1800
AMC Boot Firmware	Microchip (Soteria FW) + Accelerator ODM (e.g. Intel)
AMC Runtime Firmware	Accelerator ODM
Accelerator Firmware Image (IFWI)	Accelerator ODM
Accelerator OOB Recovery Image	Accelerator ODM + OEM Signing Wrapper (if Ownership Transfer enabled)
Closed Manufacturing Tools - AMC	Closed Manufacturing Host SW applications for provisioning AMC FRU, OTP and Flash storage over HPM USB to UART connection to AMC
Closed Manufacturing Tools - Accelerator	Closed Manufacturing Host SW applications for provisioning Accelerator FRU, Fuses or Flash storage over HPM to Accelerator PCIe connection

15. Hardware Management

15.1 OOB Telemetry

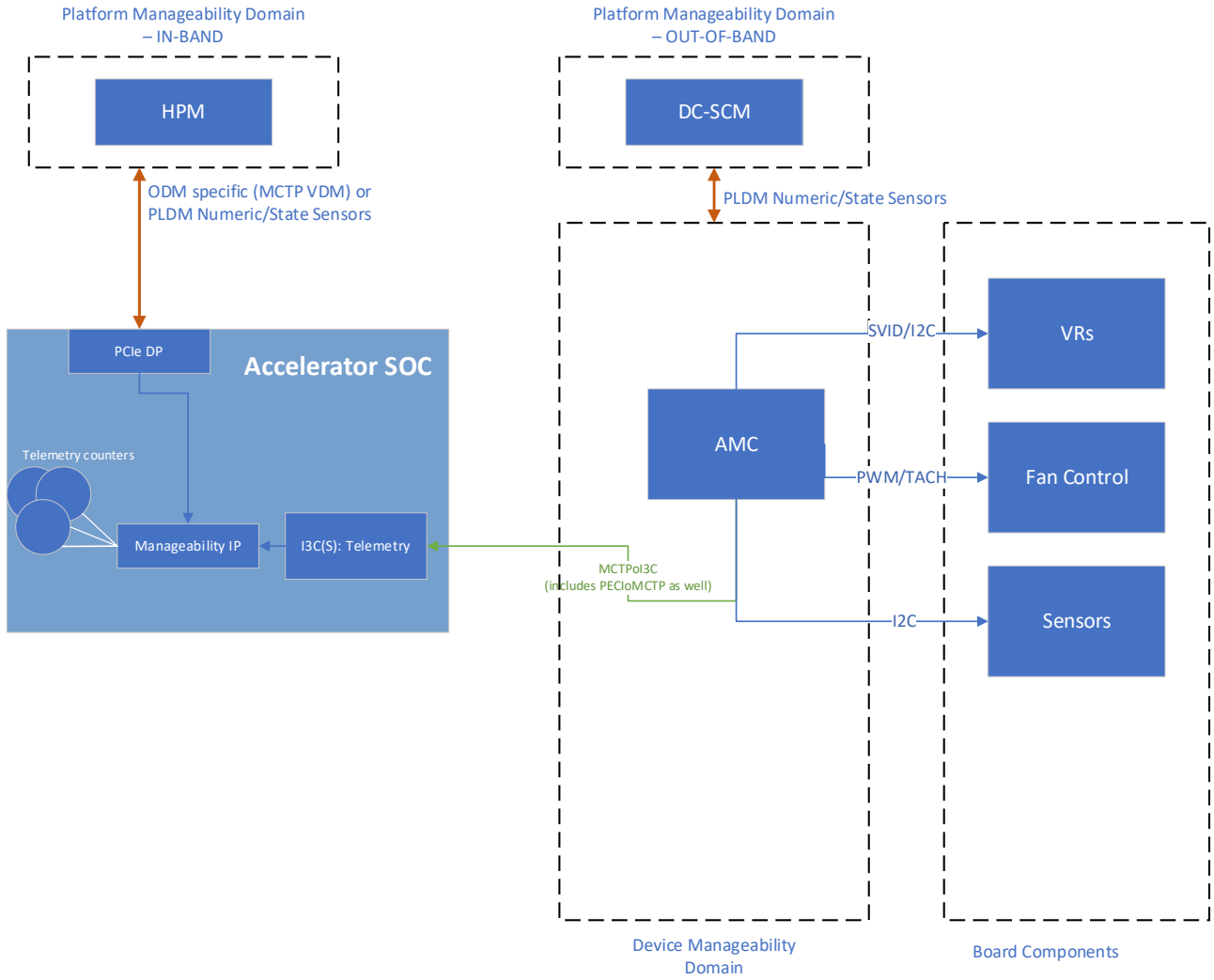


Figure 17: OOB Telemetry System Diagram

The AMC can retrieve Telemetry counters from the Accelerator either via:

1. A path to the Accelerator SOC's Manageability IP,
    a. AMC may use Accelerator SOC or industry defined Telemetry protocols tunneled as the MCTP Vendor Defined (opcode – 0x7E) message type

2. Or via a path to the Accelerator's onboard peripherals such as Sensors, VRs, Fan Controllers.
    a. Using standard SVID/PMBUS/Peripheral I2C commands

AMC establishes I3C connection to the Accelerator SOC's I3C subordinate. The subordinate supports I3C Direct Address Assignment (DAA) CCCs allowing for the AMC to dynamically allocate an I3C address to the Accelerator Subordinate during the initial boot. A target I3C Address may be specified in the FRU during Manufacturing and read by AMC Firmware off EEPROM as part of initializing the I3C Telemetry interconnect to the Accelerator.

AMC would map the Accelerator telemetry to PLDM State and Numeric Sensors. AMCs telemetry is polling based, and the Accelerator is generally not expected to be the I3C manager node for telemetry transmissions as shown in the Architecture block diagram in Section 7.

The polling duration may be an OEM defined policy configured as part of the AMC FRU data. The default polling loop is set to 100ms and can scale as much as 5 seconds

Table 11: Telemetry Domains and Data Types:

Domain	Data Types
PCIE	VID, DID, SSDID, SSVID, Link Speed, Width, Gen, BW TX/RX
PCIE AER	TLP/DLLP Packet Err Counts, DS/US Parity Err Counts, CPL Errors/Timeouts
Thermals	Inlet/Outlet Sensors, SOC/Die Temperature, Compute Core Temperature, Memory Temperature, VR Temperature
VR	VR Voltage/Current
Power	Total Board Power, SOC, Memory, VR Power, Idle Residencies
Frequencies	SOC, Compute, Memory Frequencies
DRAM Memory	Memory R/W BW, Err, Miss Counters
RAS & Card Health	Correctable, Uncorrectable, Fatal Error Counts. Poison Counts
Workloads	Compute (GT, Media, Training, Inference) workload statistics and duty cycles

The Telemetry is mapped to PLDM Sensors as outlined in the PLDM Platform Monitoring and Control Specification. The Telemetry is mapped under *Entity ID: 68 (Add-In Card)* or *Entity ID: 79 (Processor/Memory Module)* depending on the telemetry source. Ersa presently does not support Effecters as it is expected that future versions of Ersa will support PLDM Effecters wrapped under SPDM Payload as Secure Telemetry sessions.

Accordingly for the Sensors, Ersa supports the following PDRs:-

1. Numeric Sensor PDR

2. State Sensor PDR
3. Sensor Auxillary Names PDR
4. Entity Association PDRs
5. Entity Auxillary Names PDR
6. OEM Device PDR

15.1.1 Accelerator WAKE from D3Cold

If the HPM's Root Port has configured a Power saving policy for the Accelerator, then it may transition the Accelerator to D3Cold (Off) state once there are no active workloads from HPM to Accelerator. This would remove power to the 3.3VMain bus to the Accelerator, preventing the AMC from polling the Accelerator for Telemetry. To address, the AMC may use the WAKE# on the Accelerator's PCIe Edge connector via a connection over GPIO as outlined in the Architecture block diagram in Section 7.1.

AMC adopts the following flow prior to every telemetry loop cycle: -

1. Query the Accelerator *PowerGood* state to ensure that Accelerator is in D0 (Active)

2. If Accelerator is not in D0, assert WAKE# GPIO to trigger Root Port on HPM to transition Accelerator from D3 to D0 and enable the 3.3VBus

3. Accelerator SOC will go through a boot cycle

4. AMC to query a notification from Accelerator indicating it has booted to steady state

5. AMC to now initiate the OOB Telemetry polling request

6. While an OOB Telemetry session is active, the Accelerator will not transition to Idle state

15.1.2 Accelerator WAKE from D3Hot or Idle Mode

The Accelerator SOC's I3C Controller on receiving an incoming OOB I3C command from the AMC should allow for force wake notifications to the Accelerator's PSYS module that manages the Accelerator's Power Management flows.

If the Accelerator has been placed in D3Hot state by the HPM then the PSYS unit shall generate PCI PM_PM requests towards the HPM's Root Port triggering the HPM's PCI Bus Driver to transition the Accelerator to D0, at which point the Accelerator's Manageability and telemetry endpoints shall become functional after a given *Idle-Exit settling period*. For scenarios where the Accelerator has entered a device-initiated idle mode (but HPM still has device in D0),

the PSYS unit shall do a subset of this the D3Hot exit flow by making the Manageability and telemetry endpoints functional after a given *Idle-Exit settling period*.

AMC will query the maximum *Idle-Exit settling period*, provisioned as part of the FRU data in EEPROM during Manufacturing.

15.2 OOB Firmware Updates

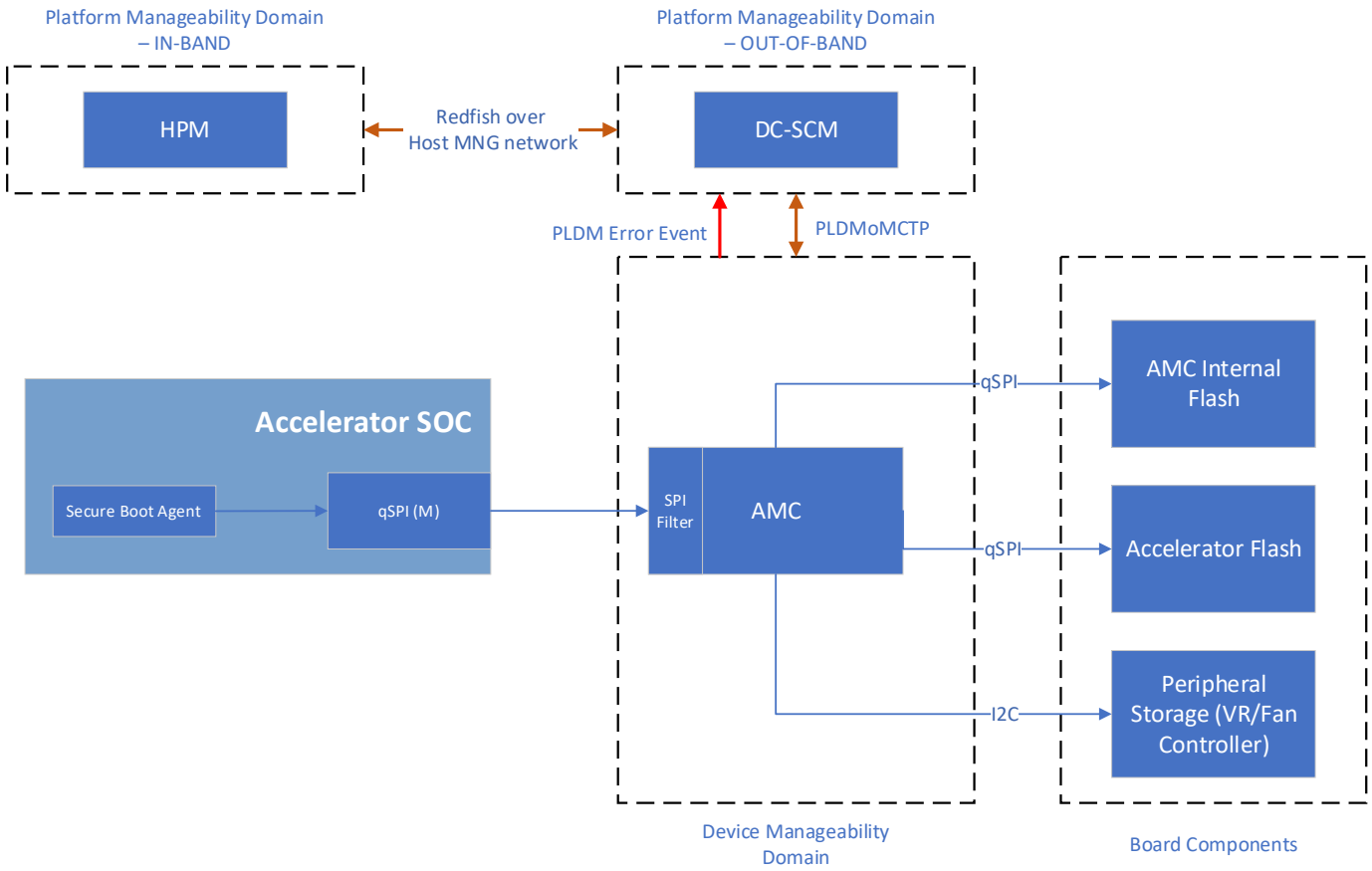


Figure 18: OOB Firmware Update System Diagram

AMC supports OOB Firmware update to:

- The AMC's internal SPI Flash
- The Accelerator's SPI Flash
- Peripherals on the Accelerator such as Voltage Regulator (VR) and Fan Controller NVRAMs or Config Space

AMC updates these components without interaction with any of the Accelerator or on-board peripheral firmware by directly managing accesses to these storage media via its qSPI Filter interface. This is an essential requirement for AMC to function as the Root of Trust of Recovery (RTRec) for the Accelerator and to be able to recover it in all cases regardless of the health state of the Accelerator's firmware.

AMC receives this update from the DC-SCM (i.e. BMC) via PLDM over I3C. The DC-SCM may in-turn have received this Firmware update from a Host based application via Redfish service deployed within the DC-SCM. The Redfish APIs are outside the scope of AMC, since AMC is not a Redfish endpoint.

- The OOB Firmware Update may be **user-initiated** either through the DC-SCM's manageability portal, or via Host manageability application through the Redfish manageability network.

- Alternatively, the OOB Firmware Update may be **device-requested.** If AMC detects that the Accelerator failed to boot due to bad FW image, then AMC will generate the “System Firmware Hang” (*SetID: 197*) PLDM State Sensor event as outlined in DMTF DSP0249. The DC-SCM on receiving this event may initiate the OOB Firmware Update using a Recovery image

15.2.1. Firmware Update Security Considerations

- Accelerator SPI Flash:- The AMC includes a qSPI Filter which is programmed prior to End of Manufacturing (EOM) being set in the FRU by the Manufacturer. The Accelerator SOC’s SPI controller connects its Data and Chip-Select outputs into the AMC’s SPI Filter. For all SPI write cycles generated from the Accelerator (either HPM initiated, or the Accelerator initiated), the write range is compared against the filter rules to resolve access control. Certain regions of the Accelerator SPI Flash are not updatable post EOM, and the SPI Filter would block those updates. Additionally, AMC supports throttling rules to minimize SPI Wearout attacks by throttling continuous write cycles to a given SPI sector.

- AMC SPI Flash:- Is only accessible either internally by the AMC native firmware, or externally via UART or SPI programming headers inserted during manufacturing, with the ability to disable UART post EOM.

15.2.2 Firmware Update Image Layout

The Unified OOB Firmware update image follows the PLDM Header and Component format

Package Header Information	
Firmware Device ID Record 1 (AMC)	Firmware Device Identification Area
Firmware Device ID Record 2 (Accelerator IFWI Signed Manifest)	
Firmware Device ID Record 3 (Accelerator IFWI)	

Firmware Device ID Record 4 (Accelerator Peripherals)	
Component Image 1 (AMC)	Component Image Area
Component Image 2 (Accelerator IFWI Signed Manifest)	
Component Image 3 (Accelerator IFWI)	
Component Image 4 (Accelerator Peripherals)	
Package Header Checksum	

Figure 19: Unified Firmware Update Image

- The Accelerator IFWI Signed Manifest is a catalog of hashes of the Accelerator's Flash based FW images. The Manifest is signed with the AMC's Key. Purpose of the Signed Manifest is to ensure that AMC authenticates the OOB FW Update images to the same "rigor" as the INB FW Update process where the RTU is the Accelerator's SOC RoT

- The OOB Firmware image is staged in AMC's external SPI Flash. Authenticated in this Flash, before being distributed to the downstream Accelerator. This is to minimize DoS attack surfaces to the Accelerator by ensuring that all updates to Accelerator follow a fully completed Authentication process

- The Unified OOB Firmware Image illustrated above may **optionally** be signed by an OEM signing Key. It is then the responsibility of the DC-SCM to authenticate and strip out the OEM signature header prior to transferring this unified image to the AMC via PLDM

15.2.3 Firmware Update PLDM Flow

We outline the PLDM commands used by AMC for FW updates as follows:

Table 12: PLDM command list for FW Updates

Command	Command Code	Requester	BMC Requirement
QueryDeviceIdentifiers	0x01 – Inventory	DC-SCM	AMC to provide device identification
GetFirmwareParameters	0x02 – Inventory	DC-SCM	AMC to provide FW parameter table data
RequestUpdate	0x10	DC-SCM	AMC enters Update Mode.

			MaximumTransferSize needs to be one of the supported values (32, 64, 128, 256, or 512)
PassComponentTable	0x13	DC-SCM	AMC receives component table (must support both upgrade and downgrade of FW versions)
UpdateComponent	0x14	DC-SCM	AMC receives specific ingredient component details
RequestFirmwareData	0x15	AMC	AMC asks for (offset, length bytes) of data
TransferComplete	0x16	AMC	AMC sends this after transfer success or failure
VerifyComplete	0x17	AMC	AMC sends verification result
ApplyComplete	0x18	AMC	Redundant command for AMC
ActivateFirmware	0x1A	DC-SCM	On reception of this command, AMC will reset either itself (for AMC FW component update) or the GPU (for GPU FW component update)
GetStatus	0x1B	DC-SCM	AMC responds with status
CancelUpdateComponent	0x1C	DC-SCM	Cancel Component Update
CancelUpdate	0x1D	DC-SCM	Cancel update

The PLDM based update follows below workflow outlining the DC-SCM (i.e. BMC) - AMC interactions. Note that per the PLDM specification, prior to *UPDATE_COMPONENT* (cmd code – 0x14), DC-SCM is Requestor, ACM is Responder. However following Component Update, the DC-SCM assumes Responder role

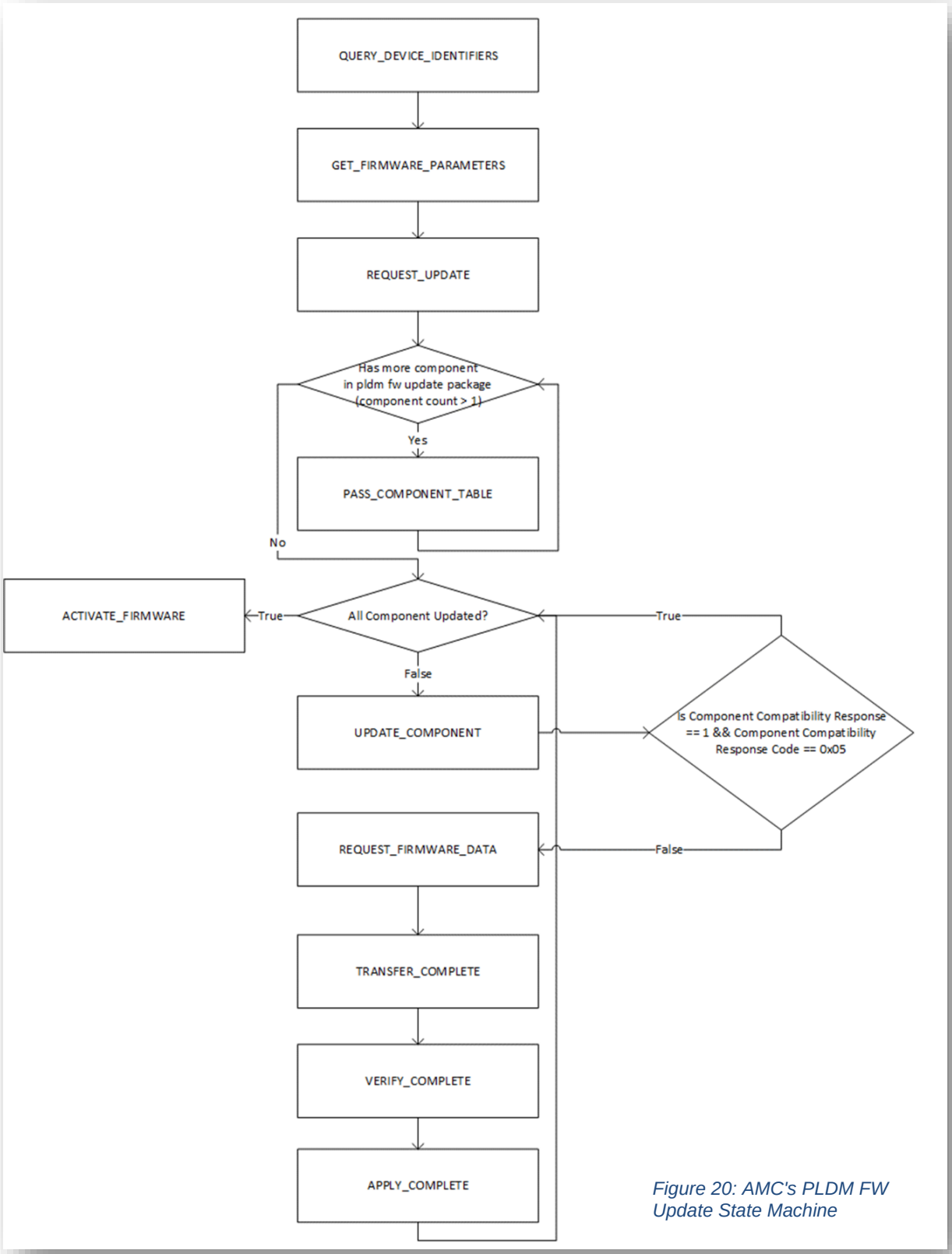


Figure 20: AMC's PLDM FW Update State Machine

15.3 OOB Management and Debuggability

AMC to support I3C based debugging to achieve two main usages.

a. Using I3C for bare-metal debugging: This is an alternative replacement to traditional JTAG interface.

b. Using I3C for communicating with board-components like VRs, Temperature Sensors, FRU etc.

Usage of I3C for debugging promotes Closed Chassis Debug where the I3C connection is exposed on the both the PCB for a Debug Host to route OOB debug traffic to AMC and subsequently to the Accelerator. In addition, AMC supports a USB-C device (DC-SCM facing) and host (Accelerator facing) endpoint for At-Scale Debug (ATSD) for scenarios where the Accelerator SOC supports a native USB2 IP that can bridge into the SOC's internal TAP and DFT network. For scenarios where the Accelerator SOC does not a native USB IP, the Accelerator board may contain a USB2 to JTAG bridge. Further definition of ATSD use-cases is an exclusion from this specification and the capability has been left in place as a software development vehicle. Details will be covered in a future specification.

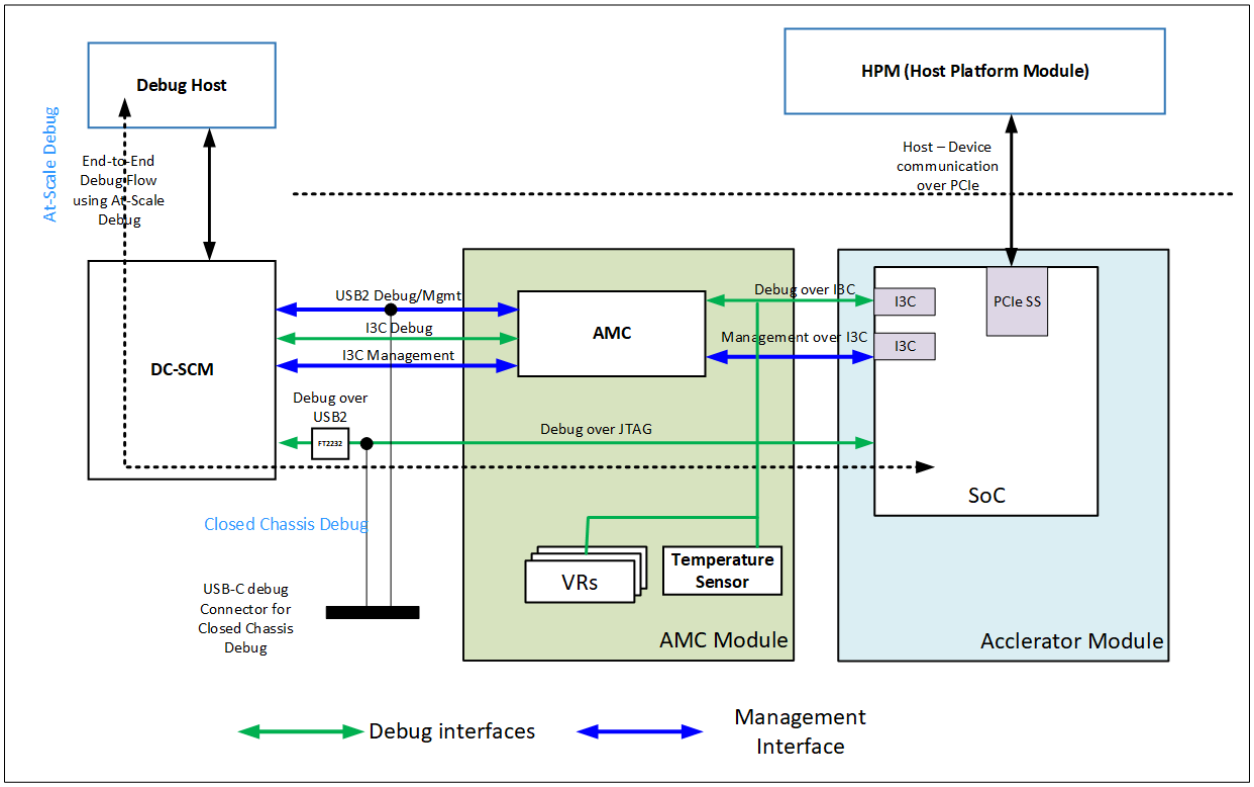


Figure 21: In-Band and Out-of-Band SysDebug System Diagram

AMC acts as a gateway to enable Module debug. As shown in the above illustration, AMC will enable debug interface to the following components by implementing a command checking and translation layer.

- *Accelerator SoC over I3C*
- *VRs*
- *Temperature Sensors*
- *FRU*
- *Other on-board components*

The accelerator comes with its own independent JTAG interface to enable debug in Open-Chassis environment. The I3C debug interface to accelerator will enable to perform debug in Closed Chassis environment.

The Voltage Regulator (VR)s deployed on the Accelerator module must support SVID debug commands to allow AMC to interface and debug issues at the module level. The VRs on Accelerator PCB should support the following debug commands within the ***Error Reporting*** SVID command group.

Table 13: SVID Error Reporting cmd group

Command	Description
Read Error Status	Reads the error status register to identify any issues associated with temperature, voltage, current etc.
Clear Error Status	Resets the error status register after the issues have been addressed.
Read Fault Log	Provides a history of errors for further analysis.
Set Alert Threshold	Configures the voltage, current, or temperature limits that will trigger an alert
Read Alert Status	Reads the alert status register to determine if any thresholds have been exceeded.

IMVP8 SVID compliant command samples:

1. **Read Error Status**: This command retrieves the current error status from the VRM.
   Command: 0x10
2. **Clear Error Status**: This command clears the error status register.
   Command: 0x11
3. **Read Fault Log**: This command retrieves a log of past faults and errors.
   Command: 0x12
4. **Set Alert Threshold**: This command sets the threshold for triggering alerts.
   Command: 0x13
5. **Read Alert Status**: This command checks the current alert status.

Command: 0x14

15.4 OOB Inventory Management

Customizations can be done to the AMC behaviour on a per-deployment basis during the Manufacturing flow where the AMC and the Accelerator are placed in a deployment platform with interconnects to the DC-SCM. These customizations take the form of Inventory data also colloquially referred to as FRU (Field Replacement Unit) data as it becomes critical for provenance, identification and triage workflows during field failure. For the entirety of this specification, we shall refer to this Inventory data as FRU data.

The FRU data is stored in the AMC's EEPROM during manufacturing, provisioned via UART. Certain FRU fields are customizable via in-field update. For provenance tracking, the AMC allows generating an HMAC tag against the FRU data via an owner hashing key. The DC-SCM may get the Accelerator capability (FRU information) from AMC through MCTPoI3C. Additionally the HPM may also be able to retrieve this data In-Band via the Accelerator's Host_I2C interconnect to AMC described later in section 15.5

The AMC FRU layout is complaint with DMTF's PLDM FRU specification and comprises of the General FRU Table, and the OEM FRU Table. Below is a proposed FRU layout for the *General FRU Table*

Table 14: AMC Inventory (General FRU Table)

FRU field	Data Type	Example Value
Chassis Type	String	PCIe, Blade, Mezz, OAM. Default: PCIe
Model	String	Intel Flex GPU
Part Number	String	Board MFG should provision Part #.
Serial Number	String	To be added by ODM by a manual command
Manufacturer	String	Intel Corporation
Manufacture Date	YYYYMMDDHHMM	To be added by ODM by manual command
Vendor	String	Intel Corporation
Name	String	Intel Data Center GPU Flex
SKU	String	XYZ
Version	String	<Firmware Stack Version> + <FRU Version #>
Asset Tag	String	<This is rework tag # for RMAs>
Description	String	<Product Description>
Engineering Change Level	String	<Capture AMC Anti-Rollback Version here>
Other Information	String	(NULL)
Vendor IANA	Unit32_t	343

In addition to the General FRU, AMC also populates the vendor defined OEM FRU Table that may contain the following additional information customizable on a per-deployment basis

Table 15: AMC Inventory (OEM FRU Table)

FRU field	Data Type	Example Value
ODM Code (e.g. 1 – Dell, 2-supermicro)	Integer	2
TDP (75 or or 150 or 180)	Integer	75
FRU CRC	Integer	0xFF
HPM to AMC I2C Address	Integer	0xCE
DC-SCM to AMC I3C Address	Integer	0x03
End of Manufacturing (EOM) bit	Integer	0xFF
Disable Write FRU	Integer	0xFF
Telemetry Refresh Duration (1 – 100ms, 2 – 500ms, 3 – 1 sec, 4 – 5 sec	Integer	0x01
Reserved	Integer	0xFF

15.5 INB Hardware Management

Certain deployments contain INB Manageability applications that execute on the HPM, alongside other Host Software applications and drivers targeting the Accelerator connected to the HPM via its Root Port. Given that the AMC doesn't have a PCIe Endpoint, these applications would proxy their INB requests to the AMC via the Accelerator which must provide steering capabilities (via its SOC, Firmware and associated Software drivers) between its Downstream Port, and an I2C manager port that then connects out to the AMC.

As outlined in the Architecture Block diagram earlier in this specification, there exists an Accelerator – AMC INB interconnect over I2C, that we now label as **Host I2C**. The Host I2C subsystem is depicted as follows: -

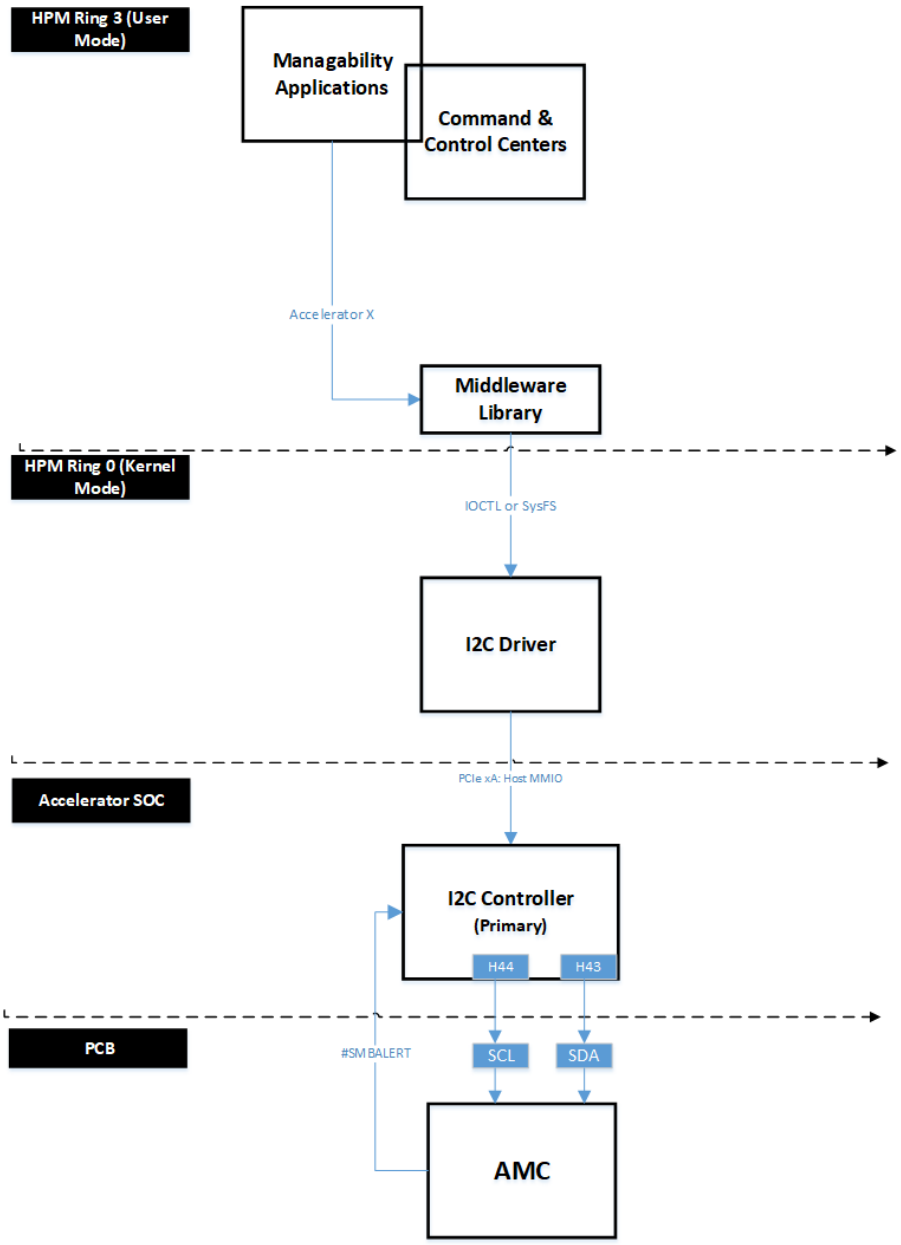


Figure 22: HPM to AMC In-Band over Accelerator I2C

The Host_I2C Subsystem supports the following capabilities: -

- SMBUS Alerts (for AMC to interrupt Host application on certain sensor/inventory configured thresholds, or internal RAS faults)
- SMBUS ARP for dynamic address assignment
- Multi-MCU capability for Board designers to pair AMC along with other MCU devices on the same Host_I2C interconnect

Via the Host_I2C interconnect, HPMs support manageability scenarios such as:

- AMC Firmware Update (In-Field) via PLDM over a SPDM trusted session
- INB Secure Telemetry over a SPDM trusted session
- Accelerator FRU Data extraction
- Debug/Vendor Logs from AMC
- In-Field HW Anti-rollback commit

16. Security

16.1 AMC PFR Compliance (NIST 800-193)

AMC implements Root of Trust of Detection (RTD), Root of Trust of Measurement (RTM), Root of Trust of Update (RTU) and Root of Trust of Recovery (RTRec) for its own domain as well as the downstream Accelerator device it manages and satisfies the Protected and Resilient properties of the NIST 800-193 standard

16.2 AMC RoT and System Secure Boot

The AMC module is a hardware Root-of-Trust (RoT) comprised of mutable and immutable code. The immutable code, referred to as the Boot ROM, is stored in an on-chip read-only memory (ROM). The first mutable code (FMC) is stored in the AMC module SPI Flash.

The Boot ROM is responsible for loading the FMC into SRAM, authenticating and decrypting the image, and then executing the FMC image. This secure bootloader is compliant with the *OCP Hardware Secure Boot V1.0* specification published by the OCP Security workgroup.

The FMC may be implemented as either a single-stage loader or a multi-staged loader. The last stage of the load contains the AMC firmware. The Microchip TS1800 MCU (AMC) currently supports a single-stage AMC firmware loader, also referred to as the Soteria G4 code.

The AMC firmware is responsible for bringing the system out of reset after it authenticates the Accelerator images stored in the external flash at boot time. In addition, the AMC firmware implements runtime SPI filtering & monitoring, referred to as time-of-use checks (TOCTOU), to detect if the firmware images have been altered unexpectedly. The AMC firmware may notify the host or take punitive action to protect the system if it detects the runtime images have been unintentionally altered.

The following diagram illustrates the Secure Boot Flow boot sequence with AMC Authenticating FW Image of Accelerator.

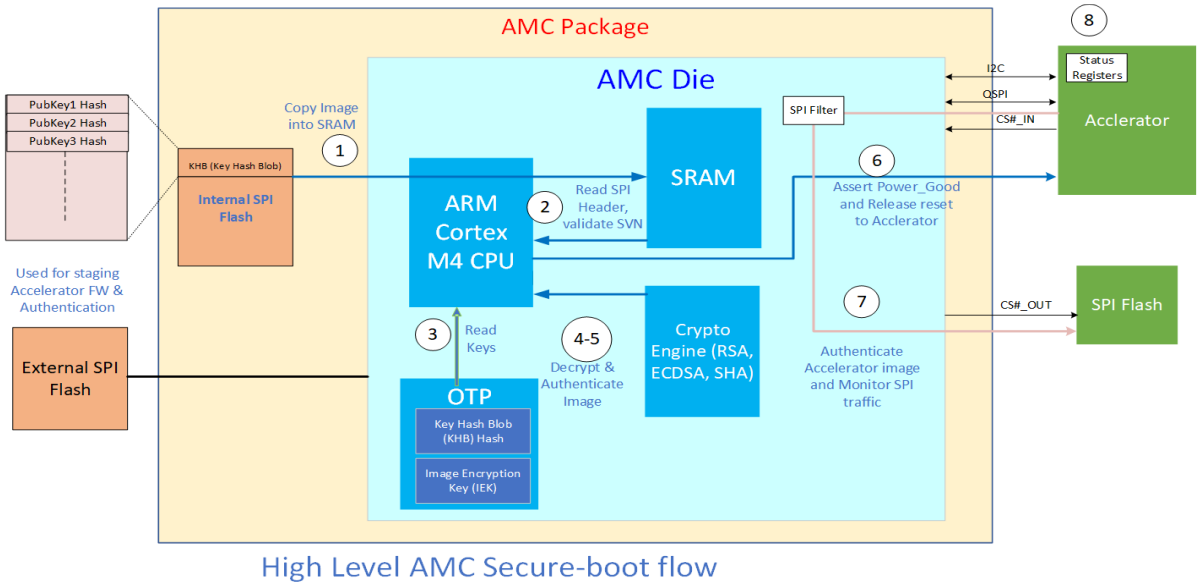


Figure 23: AMC and Accelerator Secure Boot Flow:

To meet stringent PCIe DP link training KPIs for the Accelerator device, AMC to release Power_Good signal to trigger Accelerator's secure boot, and this should happen within 100ms window after Host releases power.

AMC package secure boot steps are:

1) On Power-on, AMC's micro-controller (uC) starts execution using ROM Code.

2) AMC ROM authenticates the AMC FMC (i.e. the Microchip Soteria code), and then copies the boot image from AMC's internal SPI Flash into SRAM

3) Reads the Secure Boot header to determine the secure-boot configuration used by FW image. Reads KHB (Key Hash Block) Hash from the OTP and authenticates KHB in the internal SPI Flash, and this will ensure that KHB in the Flash is authentic.

4) Authenticate the image signature by using one of the Public Keys as part of the KHB based on the public key ID listed in image header.

5) Compare the image digest provided along with the image against generated image's signature.
    - If equal, enable firmware execution. Use the Vendor IEK (Image Encryption Key) to decrypt the image if the image is encrypted.
    - Else if there is no valid public key found in KHB, Secure Boot will fail, and AMC will attempt recovery.

6) After successful image verification, HW-ARB checks to be enforced. If SVN is smaller than specified in OTP, abort the secure boot and initiate the recovery flow. The AMC uC starts execution of firmware loaded in the SRAM.

7) AMC establishes a HW mailbox (DC-SCM – AMC I3C) checkpoint by which AMC reauthenticates the Accelerator's runtime image as the image is read from SPI Flash by Accelerator using AMC's SPI filter

8) The AMC's authentication status of the image is updated in I3C FW authentication status register for Accelerator's access.

16.2.1 AMC's internal Secure Boot

AMC has the following RoT anchor for secure boot. These flows are implemented by the Microchip TS1800 part that embodies the AMC in this design specification: -

1. Boot ROM acting as RoT for authenticating AMC's FW.
2. AMC's FW (aka Soteria-G4 FW) to act as RoT to authenticate Accelerator's FW.

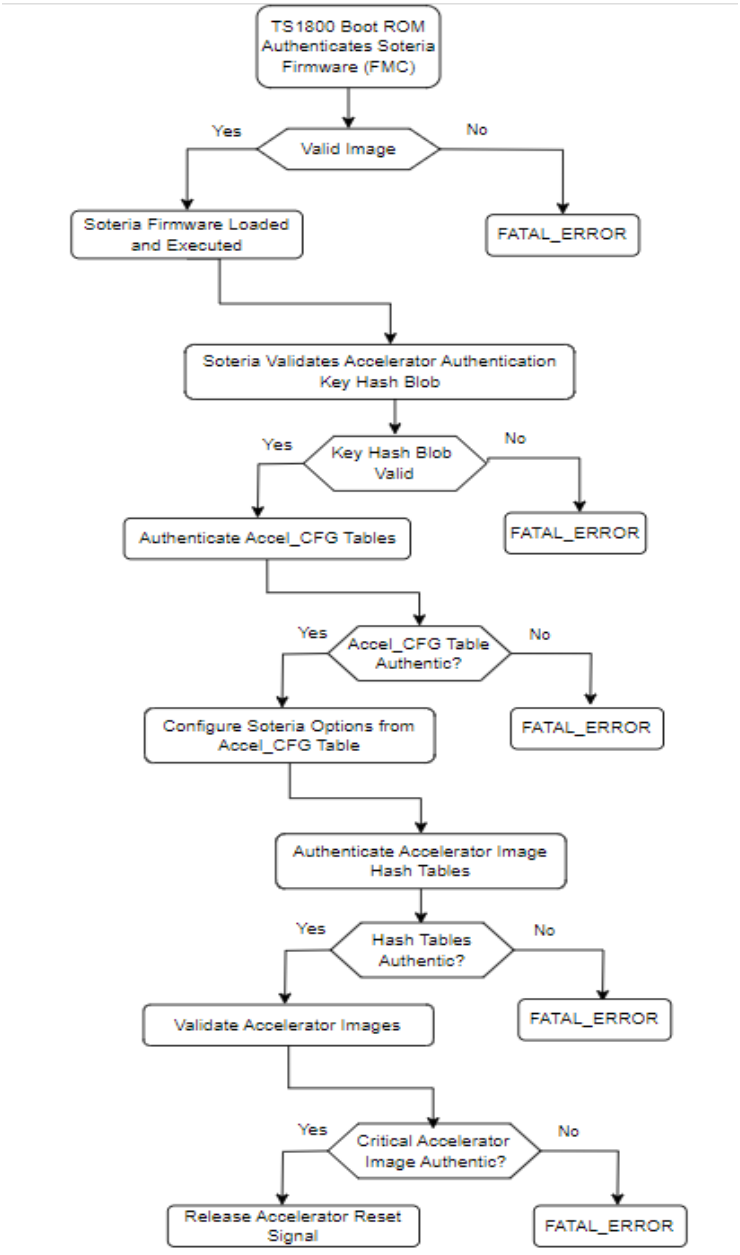


Figure 24: AMC Internal Boot Flow

Boot ROM acting as RoT for authenticating AMC's FW:

The Boot ROM is the Root of Trust for the TS1800 device, and it authenticates the Soteria-G4 code as part of the Secure Boot process of the device. Upon its successful completion, the Boot ROM hands control over to the Soteria code to authenticate the Accelerator firmware image.

The Soteria-G4 code uses information in the external SPI flash components to perform its Secure Boot process. This information, in the form of tables and key hash "blobs", is used by the Soteria code to authenticate the firmware images

Key Hash Blob = HASH (Key1) + HASH(Key2) + … HASH(Keyn)

AMC's FW to act as RoT to authenticate Accelerator's FW:

The Soteria code finds this information using base addresses contained in one-time programmable (OTP) memory in the TS1800 device. The base address values in OTP, give the location of the Public Key Hash Blobs 0 and 1 and Config Tables 0 and 1. Note that there are two of each of these items to provide redundancy in the flash components.

The Hash Blobs contain the hash value of up to 32 public keys. Each hash is used to authenticate the validity of the public key contained in tables in the SPI Flash.

The Config Tables provide configuration information about the system. The tables are signed with a private key and the Soteria code authenticates the active table. Soteria then uses information from the table to perform required hardware initialization and feature configuration as part of its Secure Boot process. The tables also contain configuration settings for the SPI monitor used for runtime monitoring.

The hash value from the Hash Table is used to authenticate the associated Accelerator firmware image before Accelerator reset is released. Upon successful completion of its Secure Boot, the Soteria-G4 releases Accelerator reset signal(s) and the runtime SPI monitoring uses the hash value to authenticate the Accelerator's firmware images as they are being read by the Accelerator.

The Soteria code supports up to 16 Accelerator firmware images. These may be a Primary Image, a Fallback Image or a Golden Recovery Image for a Primary Image. The image type is designated in the Hash Table associated with the image, and the Soteria code treats each image accordingly. For example, if a critical Primary Image fails authentication, but its Fallback Image passes, the Accelerator reset signal is released and allowed to boot. A Golden Recovery Image can be used to replace a failing Primary Image, either automatically during the Soteria Secure Boot process or through a Host_I2C command to restore the image.

16.2.2 Accelerator Secure Boot and RTM

The AMC is responsible for releasing Power Good to the Accelerator Module, causing the latter to go through its intrinsic Secure Boot Cycle. Note that there is a stringent timing constraint imposed on the AMC in terms of how quickly it can release power good to the Accelerator. The PCIe SS (downstream port) in response to a PCI PERST signal from the Root Port within the HPM, must initiate link training within a PCI-SIG allocated max time. If the Accelerator fails to complete link training within the allotted deadline, then the Root Port Driver within the HPM's System BIOS Firmware will fail to provision this Accelerator within the HPM's Device tree, effectively severing all INB communications from HPM to Accelerator.

There are a number of PCIe based critical KPIs in place between the HPM (RP) and the Accelerator (DP) which the AMC must be aware of: -

1. Minimum 100ms delay from when 3.3V power is delivered to (Accelerator + AMC) device to when HPM asserts PERST_N

2. Maximum 20ms delay for PCIe Link training if RP is Gen4 based. PCI-SIG relaxed link training deadline to 100ms in Gen5+

3. Maximum 1 second delay for DP to clear CRS Mode flag following Link Training. RP will start Device enumeration after this timeout

We outline a high-level sequence for the Accelerator Boot as follows

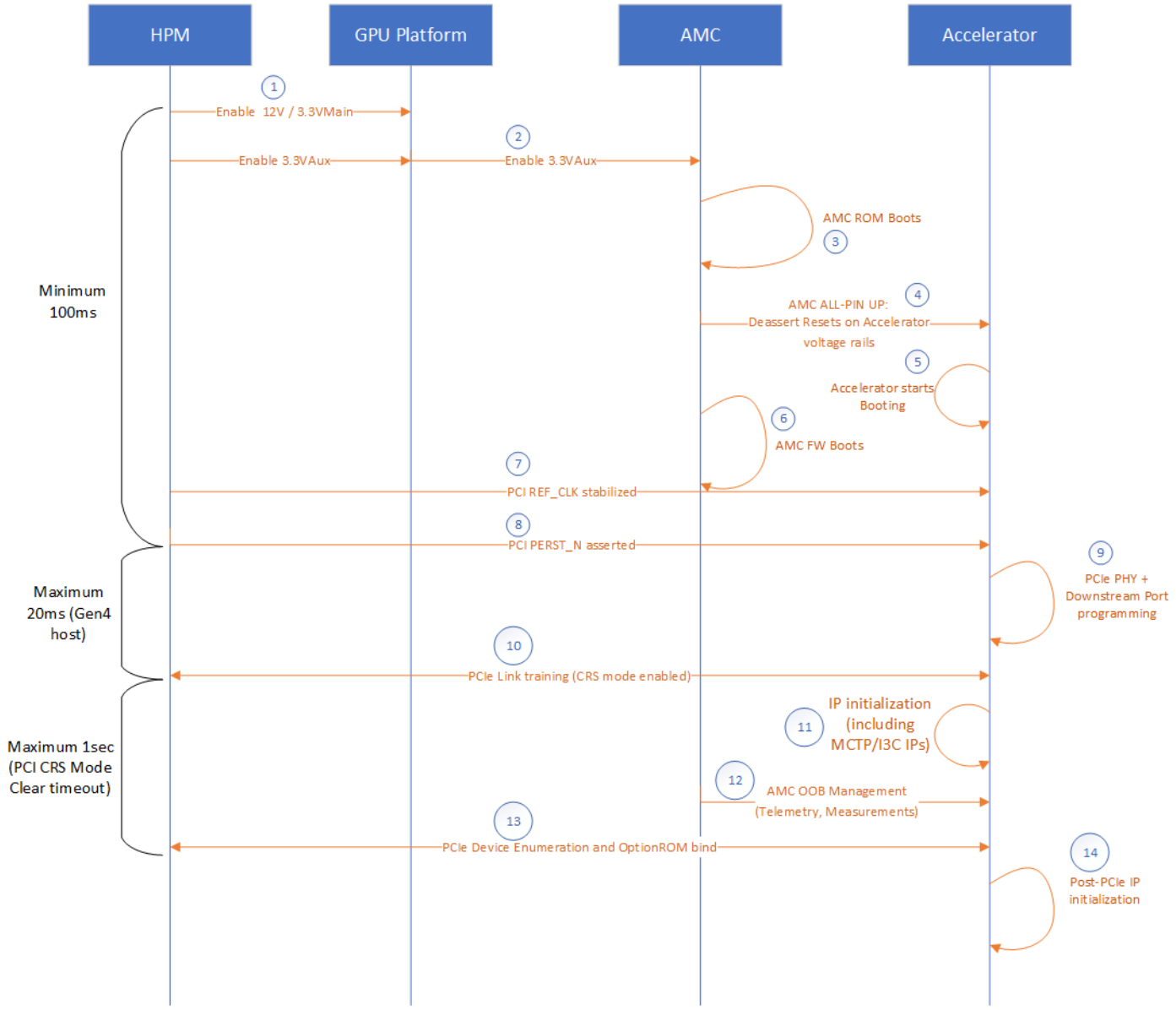


Figure 25: Accelerator Boot Flow

16.3 AMC Survivability (RTRec)

AMC provides services as the Root of Trust of Recovery (RTRec) to its own domain, as well as the Accelerator device it manages. The Microchip TS1800 based AMC supports the following survivability schemes to allow for recovery from bad firmware within its own Flash or SRAM domain, as well as the Accelerator's.

The AMC's RTRec features are classified as follows: -

Table 16: AMC RTRec features

Feature	Recovery Trigger	Recovery Target
Hardware Watchdog	On detecting Firmware hard hangs / uC processor exceptions	AMC
SECDED ECC on AMC Tightly Coupled SRAM	Single-Bit errors auto-corrected by uC. Double-Bit errors to trigger ROM based Firmware reload from Flash	AMC
Redundant firmware code images in Flash	Switch to secondary image when primary image fails authentication or execution	AMC
Hash & Verify support for runtime critical data, and critical data redundancies	Switch to secondary data copy when primary fails authentication or execution	AMC
AMC ROM based Flashless Recovery (via UART/I2C/I3C port reserved in ROM as Crisis Port)	Enable ROM based path for updating Flash when all copies of AMC runtime firmware fail authentication or execution. ROM Crisis Port access can be mapped to either DC-SCM, HPM or left floating on Accelerator PCB	AMC
OOB update to Accelerator SPI Flash on Accelerator Boot failure	Accelerator not setting GOOD BOOT GPIO within max KPI	Accelerator
OOB recovery image update to Accelerator VRM on Accelerator Power failure	Accelerator PowerOn sequence (Section 12) failure	Accelerator

16.4 Threat Model

Every deployment is expected to have its own variations in terms of adversaries and threats in scope for ensuring a secure platform. This specification aims to establish a baseline threat model that shall be the minimum set of requirements that the platform must deliver to.

16.4.1 Security Objectives

Any threat model begins with a set of security objectives. At a high level, they are as follows for this platform:

- The OCP AMC module shall maintain the general availability of the accelerator module for computation workloads submissions from the HPM against software adversaries targeting it.
- The OCP AMC Module shall guarantee the integrity and identity of the overall module against software adversaries.
- The OCP AMC module shall be resilient to permanent Denial of Service attacks on the availability of the platform against software adversaries targeting it.
- The OCP AMC module shall maintain the integrity and identity of the platform against software adversaries as well as adversaries with physical access but limited technology background (simple HW adversary).

It should be noted and acknowledged that the accelerator SoC itself has to contribute to these objectives also but it is out of scope of this document to detail those contributions.

16.4.2 Assets

Primary Assets

Table 17: Primary Security Assets

Asset	Property	Comments
Platform	Availability	This is primary asset that the AMC component is accountable for. It is at the center of the trust solution in terms of maintaining an available platform, as the RTRec illustrates.
Platform	Identity	This is specifically the identity of the platform as it relates to managing said platform. Other forms of identity can be present within the accelerator SoC which the HPM may leverage. Those are out of scope here.
Platform	Integrity	In the context of the AMC, it has limited participation to protecting the integrity of the workload execution on the platform. It does however participate in maintaining platform integrity as it applies to manageability, such as telemetry metrics.

As part of putting in place a security architecture that delivers to protecting the primary assets listed above, against the adversaries listed later on, a set of secondary assets emerge. These are listed below. It should be noted that, although specific to this AMC implementation, it is expected that any AMC would converge to a very similar set of secondary assets.

Secondary Assets

Table 18: Secondary Security Assets

Asset	Property	Comments
Immutable ROM	Integrity	Enforces Secure boot using HW RoT
AMC Public keys	Integrity	Per the cryptographic key section further down in this document.
AMC Symmetric keys	Confidentiality, Integrity, Availability	Per the cryptographic key section further down in this document.
FW Security Version Number	Integrity	Used to prevent FW versions with Security vulnerabilities.
AMC FMC Firmware	Integrity, Confidentiality	Initially located in internal flash, lives in internal SRAM once loaded and executing
Run-Time Firmware	Integrity, confidentiality (optional based on OEM choice)	Initially located in Flash, also lives in internal SRAM once loaded and executing
VR FW & Config	Integrity	Compromise to the VRs will directly result in availability issues.
AMC SoC Production state	Integrity	Protect AMC assets from debug interfaces by blocking interfaces like JTAG in production mode.
Recovery Firmware	Integrity, Availability	Availability is critical here to maintain overall availability of the platform
AMC Device identity	Availability, Integrity	Availability is a critical aspect for the overall availability of the platform via attestation.
AMC Encryption	Confidential	Symmetric key for FW confidentiality
DICE Attestation associated Secrets and Keys.	Confidentiality, Integrity, Availability	Protect Availability and Integrity of UDS, Immutable Device and Mutable Device Keys used for DICE Attestation.

16.4.3 Minimum adversary model

All software entities external to the AMC are not trusted in any circumstance.
Simple hardware adversaries are not trusted, except for availability property, as it is trivial for someone with physical access to a platform to perform a DoS.

16.4.4 Attack Surfaces

- All I2C & I3C management interfaces
- SPI bus
- Clock inputs
- Power supply rails
- Debug Interface (JTAG, USB, UART)

16.4.5 Vulnerability Analysis

Following from the above. A detailed vulnerability analysis is required to complete the threat model. This, for the sake of brevity as well not being prescriptive, shall be outside of the scope of this specification to include.

16.5 Cryptographic Algorithms

The solution is generally required to be compliant with the CNSA2.0 Guidance as well as the legacy CNSA1.0 guidance to ensure interoperability where needed.

More specifically:

- Software and Firmware signing and verification shall be capable of being performed with LMS.
- For greater robustness of transition to PQC algorithms, the solution should support dual signing where software and firmware is signed with both LMS and a traditional public key algorithm such as RSA or ECC.
- Should the solution support legacy public key algorithms for SW and FW signing
    - where it is the sole algorithm used (no dual-signing), the solution must support a revocation mechanism to permanently switch to the supported PQC algorithm.
    - The minimum key strength shall be 3k for RSA & 384b for ECC.
- Symmetric key algorithm support shall strictly be per the CNSA2.0 guidance.
    - AES with 256b keys.
    - SHA-384 or SHA-512
- The AES implementation within the AMC should be implemented to be side-channel resistant (power & timing).

- The solution shall support both CNSA 1.0 Public Key algorithms (RSA, Diffie-Hellman, ECDH & ECDSA) as well as at least one CNSA 2.0 quantum resistant public key algorithm. This specification does not yet make any intercept recommendation with regards to NIST ML-DSA.

16.6 Cryptographic Keys used in AMC

The following table captures Cryptographic keys as part of AMC's ROM Code and Firmware.

Table 19: Cryptographic Keys

Crypto Key/ Security Parameter	Storage Mechanism	Purpose	Storage location	Relevant Standard	Comments
CAK_{pub}	FMC Header	Used to authenticate FMC image	Flash	OCP Secure Boot	The public code authentication key (CAK_{pub}) is used to authenticate the first mutable code (FMC) The CAK_{pub} key is validated against the digest stored in the KHB.
OCK_{pub}	Command Parameter	Used to authenticate command to establish first device owner	Not Stored	N/A	OCK is an asymmetric authentication public key validated against the digest stored in the KHB.
Vendor Key Hash Blob (KHB)	Direct	Used to provide storage for secure boot public key digests and assets	Flash	OCP Secure Boot	Example of key digests stored in KHB: - H(CAK_{pub} key) - H(OCK_{pub} key) - H(AKHB)
Vendor Key Hash Blob (KHB) Digest	H(KHB)	Used to authenticate vendor key assets	OTP	OCP Secure Boot	The digest of the vendor KHB provisioned in OTP during manufacturing

Crypto Key/ Security Parameter	Storage Mechanism	Purpose	Storage location	Relevant Standard	Comments
Owner Key Hash Blob (KHB)	Direct	Used to provide storage for secure boot public key digests and assets	Flash	OCP Secure Boot	Example of key digests stored in KHB: - H(CAK_{pub} key) - H(AKHB)
Owner Key Hash Blob (KHB) Digest	H(KHB)	Used to authenticate owner key assets	Flash	OCP Secure Boot & OCP DOT	The digest of the owner KHB or key manifest provisioned in flash during a device ownership transfer
Image Encryption Key (IEK)	Derived via ECDH key exchange	Support Image Encryption	Not Stored	N/A	Unique symmetric encryption key per image.
Vendor IEK ECDH private key	E($ECDH_{priv}$ key)	Used to derive vendor image encryption key (IEK)	OTP	N/A	ECDH private key is a vendor unique key provisioned during manufacturing
Owner IEK ECDH private key	E($ECDH_{priv}$ key)	Used to derive owner image encryption key (IEK)	Flash	N/A	ECDH private key is an owner unique key provisioned during ownership transfer
UDS (Unique Device Secret)	Generated	Used as part of DICE attestation	Not Stored	DICE	In production non-debug mode, the DICE UDS is generated as a function of a device unique secret (rooted in fuses and hardware) In production debug mode, DICE UDS is set to zero

Crypto Key/ Security Parameter	Storage Mechanism	Purpose	Storage location	Relevant Standard	Comments
$IDevID_{priv}$	Generated	Unique for each device Used to sign LDevID certificate	Not Stored	DICE	The $IDevID_{priv}$ key is an immutable key generated as a function of a device unique secret (rooted in fuses and hardware).
$IDevID_{pub}$	Generated	Used to Verify device identity.	Not Stored	DICE	Subject of IDevID certificate that is signed by $Signer_{priv}$.key.
$LDevID_{priv}$	Generated	Unique for each device per owner. Used to sign the $Alias_{FMC}$ certificate	Not Stored	DICE	Created during runtime as a function of the current owner. The $LDevID_{priv}$ key is a mutable device identity key generated as a function of a device unique secret and the current owner.
$LDevID_{pub}$	Generated	Used to verify current owner's device identity.	Not Stored	DICE	Subject of LDevID certificate that is signed by $IDevID_{priv}$ key.
$AliasFMC_{priv}$	Generated	Used when attesting device state.	Not Stored	DICE	Created during runtime as defined in the TCG DICE Profile for Devices.
$AliasFMC_{pub}$	Generated	Used to verify the device state.	Not Stored	DICE	Derived from $AliasFMC_{priv}$ key. Subject of AliasFMC end or CA certificate
$Signer_{priv}$	HSM	Used to sign IDevID certificate	HSM	N/A	Created during device provisioning to sign IDevID certificate for OEM vendor

Crypto Key/ Security Parameter	Storage Mechanism	Purpose	Storage location	Relevant Standard	Comments
$Signer_{pub}$	Subject of X.509 Certificate	Used to verify IDevID certificate	flash	N/A	Subject of Signer certificate that is signed by $RootCA_{priv}$ key
$RootCA_{priv}$	HSM	Used to sign Signer certificate	HSM	N/A	Used during device provisioning to sign Signer certificate
$RootCA_{pub}$	Subject of X.509 Certificate	Used to verify Signer certificate	flash	N/A	
Vendor PlatKpriv	HSM	Used to sign crisis recovery commands	HSM	N/A	
Vendor PlatKpub	Command Parameter	Used to authenticate crisis recovery commands	Not Stored	N/A	PlatKpub key is validated against the H(PlatK) digest stored OTP.
Vendor PlatKpub Digest	H(PlatKpub)	Used to authenticate Vendor PlatKpub	OTP	N/A	The digest of the vendor platform public key used to authenticate crisis recovery commands
Owner PlatKpriv	HSM	Used to sign crisis recovery commands	HSM	N/A	
Owner PlatKpub	Command Parameter	Used to authenticate crisis recovery commands	Not Stored	N/A	PlatKpub key is validated against the H(PlatK) digest stored OTP.
Owner PlatKpub Digest	H(PlatKpub)	Used to authenticate Owner PlatKpub	Flash	N/A	The digest of the owner platform public key used to authenticate crisis recovery commands

Crypto Key/ Security Parameter	Storage Mechanism	Purpose	Storage location	Relevant Standard	Comments
Accelerator Key Hash Blob (AKHB)	Direct	Used to provide storage for secure boot public key digests and assets	Flash	OCP Secure Boot	Example of key digests stored in KHB: - H($Accel_{pub}$ key)
$Accel_{Pub}$	SHA384 ($Accel_{pub}$)	Used to authenticate the Accelerator FW image before updating FW to Accelerator's Flash.	OTP	-	The same public key to be used by Accelerator during secure boot.
$PlatConfig_{Pub}$	SHA384(Plat $Config_{pub}$)	Used for verifying the platform components (like VRs) configuration update.	OTP	-	

Note: FMC = First Mutable Code
Note: AMC firmware, also referred to as Soteria-G4, is first mutable code (FMC) loaded into the AMC device by the first stage immutable secure boot ROM code.
Note: PQC = Post Quantum Computing
Note: PQC keys may be LMS or Dilithium-5
Note: OTP = One-time programmable memory (i.e., fuses)
Note: OCP DOT = OCP Device Ownership Transfer
Note: KHB is an extension of the OCP Secure Boot “Manifest with Hash Table Flow”
Note: E(value) is used to represent an AES256 encrypted value
Note: H(value) is used to represent a hash operation (e.g., SHA384)
Note: KEK = Key Encryption Key

16.6.1 X.509 Certificate Chain

The Boot ROM generates the IDevID CA certificate, the LDevID CA certificate and the Alias FMC CA certificate in X.509 ANSI.1 DER format.

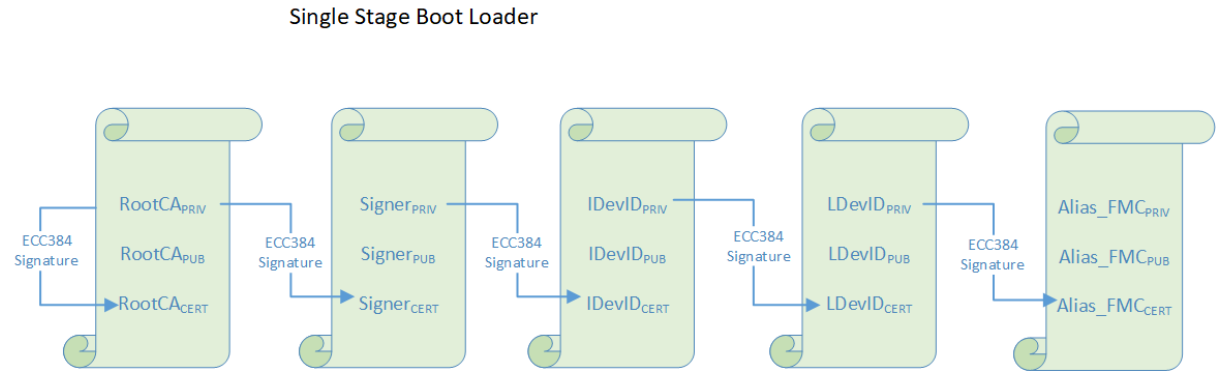


Figure 26: AMC Cert Chain - Single Stage Boot Loader

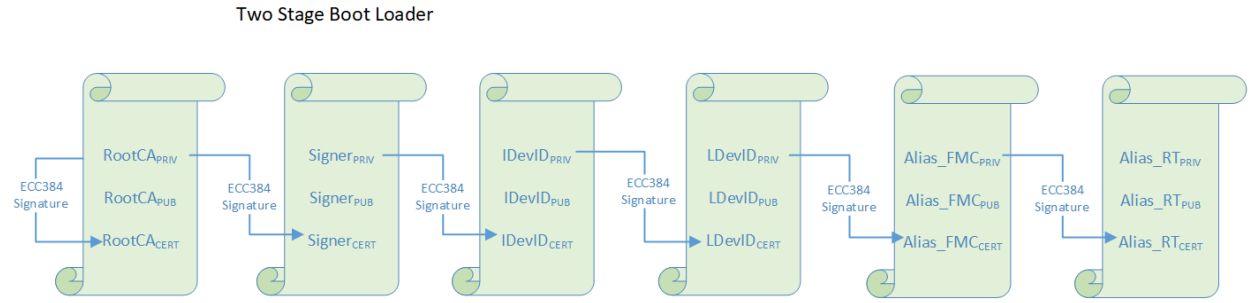


Figure 27: AMC Cert Chain - Two Stage Boot Loader

16.7 Random Number generation and sources of Entropy

Both manageability and PRoT functionality depend on random number generation of cryptographic quality.

The AMC shall support a source of entropy compliant with the NIST SP800-90B recommendation. This shall be combined with a DRBG mechanism compliant with NIST SP800-90A. The combined solution may be compliant with the NIST SP800-90C recommendation.

From a security architecture and design standpoint, the RNG on the AMC shall have its access restricted to only the trusted execution environment.

16.8 Device Identity and Attestation

The AMC is required to align with the Trusted Computing Group DICE specifications. Specifically, this means:

- The AMC device hardware and boot flow shall be compliant with the DICE layering architecture for the purpose of DICE identity establishment for attestation.
- The AMC device attestation shall be compliant with the DICE attestation architecture.

16.9 FIPS Certification

AMC shall support the following FIPS 140-3 Certification requirements from NIST:

- CMVP (Cryptographic Module Validation Program) Level 2 Certification for the AMC package level to ensure that AMC implementation is compliant FIPS 140-3 requirements.

- CAVP (Cryptographic Algorithm Validation Program) Certification for the Cryptographic algorithms ensures the cryptographic implementation is functionally correct.

16.10 AMC Additional Security Requirements

AMC to support the following additional Security requirements in addition to those listed in the afore-mentioned Section 16 subsections:-

Table 20: AMC Additional Security requirements

Security Requirement	Description
HW-ARB	HW ARB (Anti-Rollback) where the AMC's ROM code prevents booting FW images with SVN lower than the value programmed in OTP
SPI Monitor	SPI Monitor to ensure the integrity and validity of the SPI traffic from the Accelerator SoC. SPI Monitor can work in Passive and Active modes. ○ **Passive mode**: AMC simply observes the SPI traffic but doesn't intervene. ○ **Active mode**: AMC intervenes if a violation is detected such as a specific command sent over the SPI bus. AMC supports two kinds of interventions a) full intervention by blocking SPI access to accelerator b) reduced intervention by allowing only SPI reads.
Secure FW Update	The Secure FW update is supported by AMC for its own AMC's firmware and Accelerator's firmware images. AMC acts as the Firmware Device (FD) uses Platform Level Data Model (PLDM) specification for receiving the update details.
FW Recovery	Secure FW recovery in the case of exceptions during execution through Watchdog timer. This will allow AMC to be available all the time.

JTAG Access	Blocking JTAG access during production and allowing JTAG access only after authentication.
Secure Key Storage (OTP)	All AMC Signature verification, encryption, hashing and identity management keys to be in secure HW storage fused during Manufacturing flows. Where a soft extension (SRAM based) to the HW storage exists, it must be anchored in AMC's Secure trust chain
Key Revocation Scheme	The OTP or Secure HW Key storage must support a Key Revocation scheme. The revocation scheme must be anchored in ROM. In the case of the AMC ROM, it supports 3 types of revocations: - , 1. Auto Revocation when permitted (recommended) 2. Manual Revocation when permitted 3. Manual Revocation The key revocation permission bits are implemented in the Image Header. The ROM will revoke all images/keys that have their permission bit
Ownership Transfer	Allowing Platform Owner to securely provision the ownership key for FW authentication and enabling transfer of the ownership. Once the ownership transfer is performed, only the new owner signed FW images are allowed to execute.
Always Enforce Secure-boot	The manufacturing flow to ensure that no-backdoors on AMC that can bypass Secure-boot authentication. Even during crisis mode, the AMC allows only the signed images to update SPI Flash.
Redundancy & Repair	OTP and AMC SRAMs shall support SECDED ECC or Redundancy schemes to repair random bit errors created via non-malicious actions but leading to a Availability impact to AMC's security posture

16.11 Security Assurance

In order to achieve a secure platform solution, it is imperative that the AMC component be developed according to the latest BKMs with regards to secure development. This section aims to provide a set of general guidelines that articulate what is meant by good secure development practices.

16.11.1 SBOM and provenance

Pertaining to items such as the US government executive order (EO-14028), the AMC solution needs to deliver a SBOM. The objective of such is to deliver a complete view to the adopting customer of the entire software and firmware contents that make the AMC solution for the purpose of establishing supply chain trust via clear evidence of provenance, versioning and associated known vulnerabilities. This enables product traceability for the complete platform that incorporates an AMC component.

16.11.2 Secure Development lifecycle

The objective of the security development lifecycle (SDL) is to ensure a trustworthy product is delivered and supported through its lifecycle.

Security development lifecycle is a set of tasks and activities that can drive high-quality security outcomes in product and services development. Any AMC development should follow a secure development lifecycle as defined by the vendor. Basic recommendations for activities to include would be:

- Product Threat modeling
    - Security objectives
    - Adversary model
    - Asset identification
    - Threat mitigation definition.
- 3rd party IP security analysis
- Cryptography usage guidelines and reviews
- Product Artifact secure signing infrastructure where appropriate
- HW & SW Secure coding and & secure code reviews on identified risk target areas.
- Software & Firmware Security best practices
    - Static analysis
    - Binary analysis
- Structured Security Validation
    - Security validation planning & execution
    - Penetration testing & Hackathon planning & execution
    - Formal validation benefit analysis and targeted use

Note that the above is a non-exhaustive list. Each vendor should define their SDL to best fit their overall development practices. These are just the best security practices generally acknowledged across the industry which could be considered as the absolute minimum baseline to achieve.

16.11.3 PSIRT process

AMC deployments must be accompanied by an appropriate Product Security Incident Response Team (PSIRT) process.
An AMC vendor must put in place a structure that supports and governs AMC product engineering in the identification, mitigation, and disclosure of security vulnerabilities that may affect the complete AMC product solution. This includes defining policies that define the expectation for the handling of potential security vulnerabilities that may affect the AMC. These

policies should be consistent with the industry standard ISO/IEC 29147 for vulnerability disclosure and ISO/IEC 30111 for vulnerability handling.

Policies are expected to achieve the following:

- ***Identification***: unmitigated potential security vulnerabilities in a current or future AMC are immediately reported to the PSIRT team
- ***Mitigate:*** mitigation plans and solutions are put in place to address all reported security issues by AMC product engineering.
- ***Disclose:*** PSIRT team discloses vulnerability information in accordance to a vendor defined process aiming to achieve consistency with the common industry practice of Coordinated Vulnerability Disclosure (CVD).

17. Software Support (recommended)

For Software Toolchain and support for closed source software, contact Intel and Microchip. For open-source software used in this project such as Zephyr, refer to their respective project workgroups.

18. References (recommended)

TCG DICE: Hardware Requirements for a Device Identifier Composition Engine, Version 1.0 Revision 0.91 August 8, 2024
TCG DICE Layering Architecture, Version 1.0 Revision 0.19 July 23, 2020
TCG DICE Profile for Devices, Version 1.0, Revision 0.1, July 21, 2022 (Draft)
NIST 800-193 Platform Firmware Resiliency, Version 1.0, May, 2018
OCP SMC, Version 1.0, Revision 1.0, September 15, 2023
DMTF MCTP Base Specification, Version 1.3.1, September 4, 2019
DMTF PLDM Base Specification, Version 1.1.0, February 11th, 2021

Appendix A - Checklist for IC approval of this Specification (to be completed by contributor(s) of this Spec)

Complete all the checklist items in the table with links to the section where it is described in this spec or an external document .

Item	Status	Link to detailed explanation
Has this contribution been presented to an OCP Project group during a project call or engineering workshop?	Yes or No	If “No”, please state the reason.
Approval by Project Leads	Yes or No	If “No”, please state the reason.
Is this contribution entered into the OCP Contribution Portal?	Yes or No	If “No”, please state the reason.
Was it approved in the OCP Contribution Portal?	Yes or No	If “No”, please state the reason.