Axiado SCM3080-MT

AI-Driven Secure Management Solution for Accelerated Computing

Axiado offers comprehensive integration of key platform security and infrastructure management functionalities with advanced AI capabilities into a standards-compliant Secure Control Module (SCM), based on the industry-leading AX3080 Trusted Control/Compute Unit (TCU). The Axiado SCM3080-MT Secure Management solution offers enormous architectural value by integrating intelligent management and security in one module to provide advanced platform security, AI-driven system security, system management capabilities, and improved thermal and power efficiency in an easily deployed standard form factor.

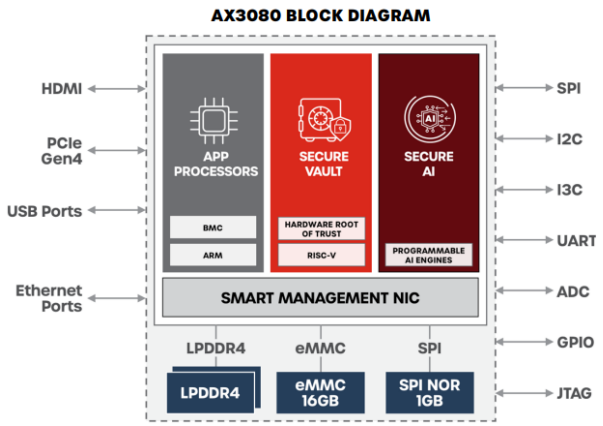
The Axiado AX3080 is a second-generation Trusted Control/Compute unit (**TCU**) System-in-Package that integrates the AX3000 SoC, which contains a Hardware Root of Trust (**HROT**), Baseboard Management Controller (**BMC**), Trusted Platform Module (**TPM**), Hardware Security Module (**HSM**), Network Firewall (**Smart NIC**), **AI/ML** Engines and more, in a single secure package with **LPDDR4 system memory, eMMC and SPI NOR Flash**. This package-scale integration further enhances platform security by eliminating potential attack surfaces, improves power efficiency, and reduces design complexity.

The Axiado SCM3080-MT offers comprehensive **intelligent and autonomous management, operational efficiency and security capabilities**. The SCM3080-MT board contains the industry's first 10GE management port as well as 1GE ports for high-speed communication with the network, along with an external USB for mouse/keyboard and micro-HDMI ports for display. The SCM3080-MT interfaces to the system via a DC-SCM slot and is powered via the DC-SCM connector.

Unlike SW-only security solutions, the Axiado SCM3080-MT based solution empowers IT/CISOs to detect, isolate, quarantine, and protect infrastructure in real time. Axiado SCM3080-MT is field upgradable by swapping out modules plugged in an existing OCP compliant DC-SCM connector.

The SCM3080-MT is designed to be used in **Nvidia Accelerated Computing Platforms – MGX, HGX, DGX** and others to enable comprehensive platform management and security capabilities.

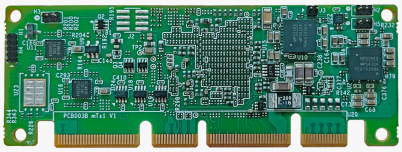
Axiado offers NVIDIA BMC and OpenBMC software stack as default management software with the option to qualify custom management software stacks.



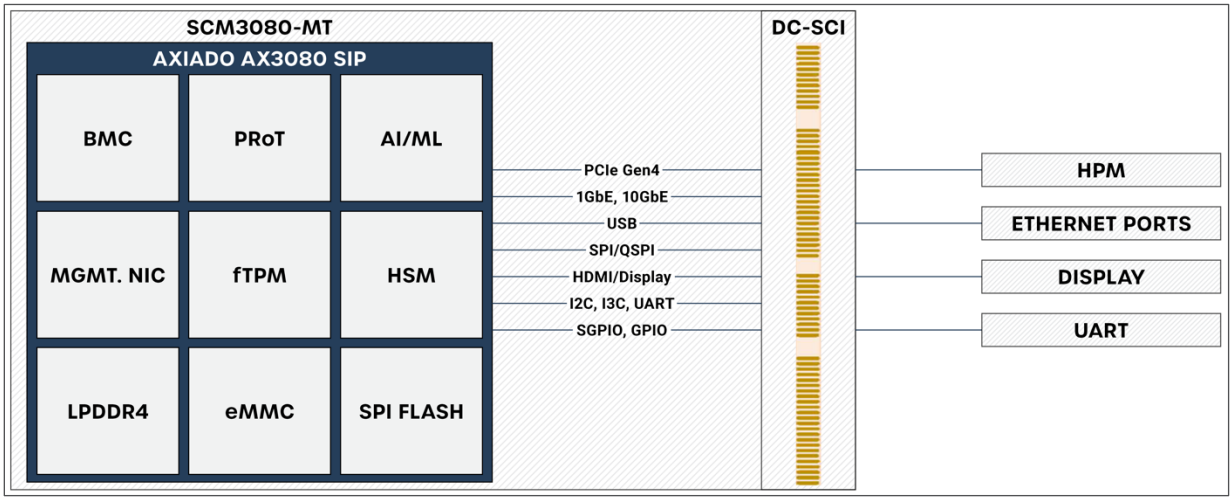
FEATURES

- 85.48mm (L) x 33.50mm (H) form factor
- Fully compliant with OCP DC-SCM Rev2.0
- AX3080 Trusted Control/Compute Unit (TCU)
- Supports OpenBMC, Nvidia OpenBMC, AMI MegaRAC OneTree and other third-party BMC software
- NIST800-193 and OCP Security compliant Platform Root of Trust
- Secure Host Connectivity with IDE enabled PCIe Gen4
- NC-SI, MCTP, Redfish, PLDM, SPDM support
- 10GbE and 1GbE network/management Port
- IPv4 and IPv6 support
- Advanced Management and Security features using built-in AI/ML engines
- Ordering part number: SCM3080-MT

SCM3080-MT Top View with AX3080 TCU



SCM3080-MT Bottom View



SCM3080-MT SECURE CONTROL MODULE BLOCK DIAGRAM

SPECIFICATIONS

Security	• Meets NIST800-193, Intel PFR and OCP Security Guidelines
	• Secure Enclave /Trusted Execution Environment
	• CNSA 1.0/2.0 Crypto Algorithms and Hardware Accelerators
	• PUF based unique secrets, TRNG, OTP
	• Secure boot, Secure Update, Secure Recovery, Rollback Protection, Key Revocation
	• Attestation (SPDM/DICE), Device Ownership Transfer, Life Cycle Management
	• Firmware -based TPM compliant with TCG TPM 2.0 Specification
	• Streaming boot (NetBoot) support
	• Confidential Computing support (Encrypted memories, protection for data at rest, in-use and in-transit)
	• Side-channel attack countermeasures
	• Secure Network-On-Chip for access, policy control and management
	• Network Firewall
	• Advanced AI-Driven Security features
	  • Real-time autonomous Threat Detection and Mitigation
	  • Real-time behavioral anomaly detection
	  • Real-time Vulnerability management

Networking	• IPv4 and IPv6 support • TCP/UDP, ICMP, ARP/RARP support • Encapsulating Security Payload (ESP) support • Exact match 5-tuple flow lookup table for up to 4K unidirectional flows • Receive-side packet steering of recognized flows for multiple tenants • 1Gbps encryption/decryption for IPsec, and Transport Layer Security (TLS) packets
Host Interface	• Fully compatible to OCP DC-SCI 2.0 interface • Secure host connectivity with IDE-enabled PCIe Gen4 • Two independent PCIe Gen4 interfaces configurable to either Root Port or End Point at run-time • MCTP 1.0 over PCIe/I2C • I2C/I3C MIPI Rev 1.1, SMBus Rev 3.2, SSIF, KVM, SOL, PWM, ADC, UART • USB 2.0/3.0 (Host and Device modes) • GPIO • SPI/QSPI (Controller and Target modes) and eSPI Rev 1.0 (Target mode) • DC-SCM 2.0 LTPI Rev 1.4.3
Software/ Firmware/ BSP	• OpenBMC (Upstream Version) • Nvidia OpenBMC • AMI MegaRAC OneTree • U-Boot, Linux Kernel(6.6.x) with all TCU drivers • Platform Root of Trust Firmware • Networking Firewall Firmware • AI/ML Foundational Models and Agents • Provisioning Tools
AI/ML Foundational Models and Agents	Reference models and agents for many applications, including: • Dynamic Thermal Management (DTM) • Vulnerability Management • Network Anomalies Detection • Side-channel and Supply Chain Attack Detection/Prevention

For more information, visit our website axiado.com. | 2610 Orchard Pkwy STE. 300, San Jose CA 95134