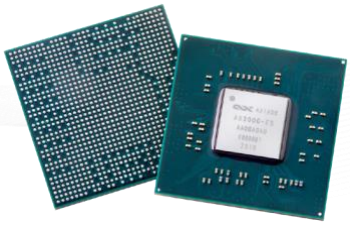


Axiado SCM3003
AI-Driven Secure Management Solution

AI-Driven Hardware-Anchored Secure Management Solution for Accelerated Computing

INTEGRATED SOLUTION FOR COMPREHENSIVE SECURITY AND MANAGEMENT

It is evident by the recent pervasiveness of cybercrime and ransomware that prevailing discrete Cybersecurity and Management Solutions, provided in a fragmented way by multiple vendors, lag behind the evolution in networking, compute & accelerators.

Axiado offers the requisite integration of key infrastructure security and management functionalities into a System-On-Chip (SoC). The Axiado SCM3003 Secure Management solution provides the essential AI-driven compute, networking & accelerators integration to offer enormous architectural value to end-applications by corelating sensor inputs more quickly to help prevent zero-day attacks in real time.

The Axiado SCM3003 Secure Control Module (SCM) offers an Integrated AI-driven Secure Management Solution with a Baseboard Management Controller (BMC), Root-of-Trust (RoT), Trusted Platform Module (TPM), Ethernet ports, and Spartan 7 FPGA for configuration and programmability. The SCM3003 SmartSCM board contains both industry's first 10GE and 1GE ports for high-speed communication with the network, along with an external USB for mouse/keyboard and micro-HDMI ports. The SCM3002 interfaces to the system via a DC-SCM slot and is powered via the DC-SCM connector.

Axiado Solutions empowers IT/CISOs to detect breaches, vulnerabilities, and attacks as they take place in the hardware. Unlike the SW-only security solutions, the Axiado SCM3002 can detect, isolate, quarantine, and protect infrastructure in real time. Axiado SCM3002 is field upgradable by swapping the existing OCP compliant DC-SCM.

COMPREHENSIVE AI-DRIVEN PLATFORM SECURITY & TRUST SERVICES

Axiado leads innovation in the AI era cybersecurity with an integrated, AI-driven security & management solution to offer unprecedented security against ransomware and supply chain/ side-channel/other cyberattacks in the growing deployments of cloud datacenters, 5G networks, and enterprise and carrier network switching. Axiado solutions are complementary & compatible with all existing Enterprise security XDR solutions.

The SCM3003 also contains built-in Artificial Intelligence (AI)/Machine Learning (ML) hardware that provides a new class of comprehensive platform security and trust services.

Axiado's solution uses AI/ML engines to detect/protect platform security during boot & Run time to offer unique cyber security trust services for end-to-end infrastructures like servers, switches and routers.

INCREASED RELIABILITY WITH OCP & INDUSTRY COMPLIANCE

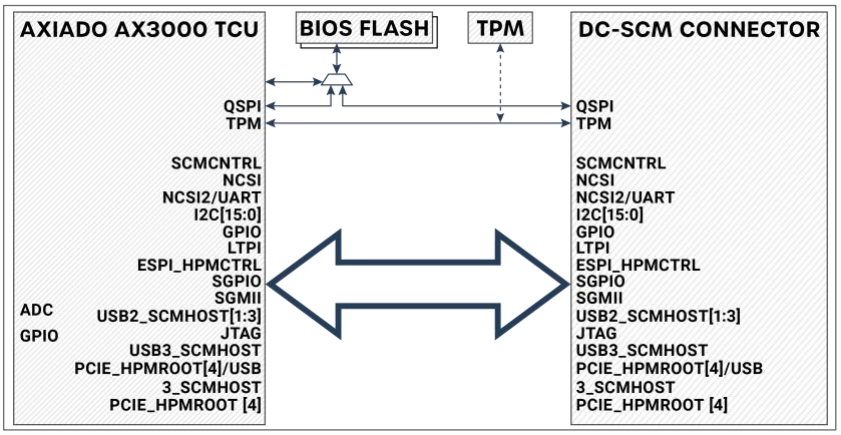
The Axiado SCM3003 Secure Control Module (SCM) is an Integrated AI-driven Secure Management Card for use in Open Compute Project's (OCP) compliant DC-SCM 2.0 platforms offering a comprehensive cybersecurity solution to secure your infrastructure in the AI era. Axiado SCM3003 also offers compliance with industry-standard SW-based cybersecurity solutions.

FEATURES

- 85.48mm (L) x 33.50mm (H) form factor
- Fully compliance with OCP DC-SCM Rev2.0
- Supports OpenBMC and third-party BMC software
- AX3000 Trusted Control/Compute Unit (TCU):
  - Integrated ASIC with trusted computing, BMC, TPM, HRoT, Ethernet port, FPGA, and AI/ML
  - Quad ARM A53 application cores running Linux with 32KB L1 cache and 1MB L2 cache
  - Four independent AI/ML islands running up to 4 TFLOPS
  - Supports up to 4GB LPDDR4
  - Encrypted memory for data and code protection
  - Single/Dual Node support
  - Hardware-based Firewall
  - Header and Crypto processing provide classification, security protocol processing, and cryptographic algorithm acceleration
  - Package: 23 x 23 BGA
- Power: 5W
- Ordering part number: SCM3003-02

SCM3003 Top View with AX3000 TCU

SCM3003 Back View with FPGA and Daughter Card



SCM3003 SECURE MANAGEMENT BOARD BLOCK DIAGRAM

SPECIFICATIONS

Security	• Secure Boot
	  • RSA 4K and ECC P521 based digital signature-based authentication mechanism as part of its hardware-anchored secure boot procedure
	  • On Chip OTP based root keys and flash-based code signing keys
	  • Three independent OTP memories, 4 Kbytes each
	  • On-Chip Physically Unclonable Function (PUF), TRNG
	  • Multiple message digest support: MD5, SHA-1, SHA-2 (224-bit, 256-bit), AES-CMAC, XCBC-MAC, CBC-MAC
	• Anti-rollback for firmware binaries based on image version and Security Version Number (SVN)
	• HRoT (Hardware Root of Trust)
	• Crypto offload with OpenSSL
	• Encrypted flash
	• Attestation and AC-ROT with SPDM
	• Secure firmware update
	• Secure Provisioning
	• Secure Manufacturing

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/SGPIO • SPI/QSPI (Controller and Target modes) and eSPI Rev 1.0 (Target mode) • DC-SCM 2.0 LTPI Rev 1.4.3
BSP, BMC	• SE Linux Kernel 5.15 based BSP with driver support for all the above peripherals • eMMC 5.1A with ext4-based file system • Host display over Display Port • System-wide TCU logging • Remote FPGA programmability • Supports OpenBMC v2.12 and other third-party BMC software • User, alert, policies, certificate management • Telemetry via Redfish interface
AI/ML	Reference Models for: • Agent-based behavioral ransomware detection • Network anomalies detection • Side-channel and supply chain attacks detection/prevention • Dynamic Thermal Management (DTM)