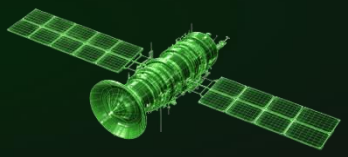
GENERAL DYNAMICS Mission Systems | IDAHO SCIENTIFIC

Helios Memory Guard (HMG)

Data-at-Rest and Inline Memory Protection



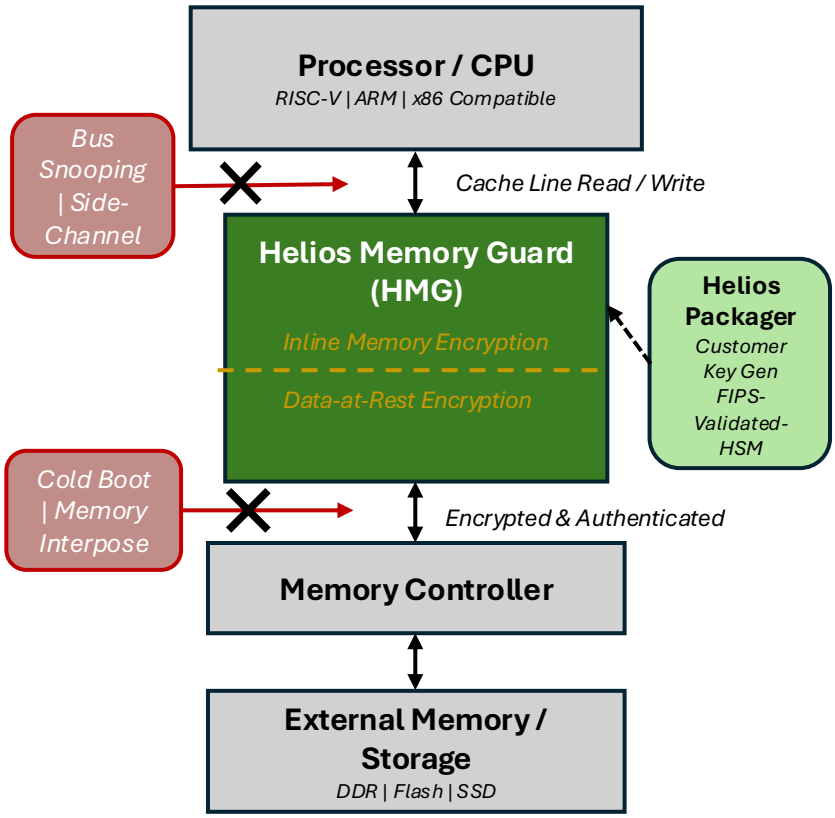
What problem does HMG solve?

Physical attacks on memory bus snooping, memory interposing, cold boot, and side-channel analysis- have proliferated to the point that hobbyists can perform them with consumer-grade equipment. HMG provides hardware-enforced, just-in-time encryption and authentication between the processor and memory controller, ensuring instructions are authentic and data remains confidential throughout its entire lifecycle- transparently, with no software changes required.

How It Works

HMG is FPGA IP that sits between the processor and its memory controller.

- **Runtime:** Encrypts and authenticates every memory read and write using ephemeral keys that roll on every write, eliminating replay and interpose attacks
- **Load-time:** Decrypts and authenticates boot images pre-encrypted by the Helios Packager
- **Key Ownership:** The customer generates and manages all cryptographic keys via the Helios Packager utility



Performance

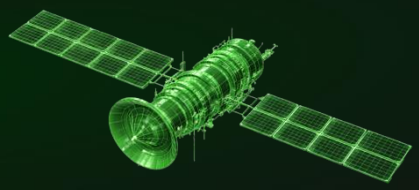
Metric	Value
Runtime throughout impact	**No impact below bus saturation**
Near-saturation impact	**~34% throughput reduction**
FPGA fabric utilization	**~60K LUTs/ ~71K Flip-Flops**
Max Frequency	**~250 MHz**

Compatibility

	Support
FPGAs	**Xilinx 7-Series, UltraScale, UltraScale+, Versal**
ASIC	**In design for 12nm**
CPU Architectures	**RISC-V, ARM, and others**
Porting	**Available for other FPGA vendors**

GENERAL DYNAMICS
Mission Systems

IDAHO SCIENTIFIC



Benefits

Benefit	Description
Low Risk	Proven in FPGAs on defense programs; NIST-approved, SCA-resistant algorithms
Simple Integration	Drag-and drop with reference designs and test benches
Set & Forget	No annual maintenance contracts; future updates optional
Customer Key Ownership	OEM and end customer control all cryptographic keys
Trusted Supplier	US DoD supplier- US engineers available to support via phone, email or in-person

Features

Feature	Detail
Inline Memory Encryption	AES-256-GSM encryption and authentication per cache line- ephemeral rolling keys
Data-at-Rest Encryption	Encrypts/signs at provisioning; decrypts/authenticates at load
Technology Protection	Maintains confidentiality and integrity of IP and CPI across memory and storage
Tamper Resistance	DPA-resistant; resistant to bus snooping, cold boot, and memory interpose attacks
CNSA 2.0 Cryptography	AES-256-GCM
Boot Image Security	Decrypts and authenticates Helios Packager-encrypted images at load time
FPGA & ASIC Ready	Verified on Xilinx ecosystem

Deliverables

RTL/ IP	IP-XACT Package- HMG RTL, Cacheline Normalizer RTL
Software	HMG Driver, Helios Packager (FIPS-validated HSM support)
Documentation	Product Guide, Hardware Integration Guide, Software Developer's Manual
Integration	Reference Designs, Simulation Testbench, Example Designs
Support	Technical support- phone, email, on-site; optional future updates