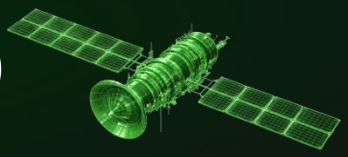
GENERAL DYNAMICS Mission Systems | IDAHO SCIENTIFIC

Helios Processing System (HPS)

A Fully Integrated Secure Processor



What problem does HPS solve?

The Helios Processing System combines Helios Memory Guard with a hardened RISC-V processor into a single, validated secure processor IP package- delivering full lifecycle protection from secure boot through runtime against the most critical attack classes targeting modern defense processors:

- Memory-Corruption Attacks- 56% of MITRE critical CVEs; 70% of Microsoft patches over 12 years
- ROP/ JOP/ COP Attacks- leveraging code fragments to bypass security controls
- Side-Channel & Cache Timing Attacks- enabling cryptographic key extraction
- IP Theft & Reverse Engineering- via debug exploitation, bus snooping, memory interposing
- Downgrade & Unauthorized Firmware Attacks- bypassing secure boot

THREAT VECTORS

- Memory Corruption- 56% of MITRE Critical CVEs
- ROP/ JOP/ COP Attacks Code fragment exploitation
- Side-Channel & Cache Timing Cryptographic key extraction
- IP Theft & Reverse Engineering Debug/ bus/ memory exploitation
- Firmware Downgrade Attacks Bypasses secure boot

HELIOS PROCESSING SYSTEM

Hardened RISC-V Processor + Helios Memory Guard

RISC-V PROCESSOR CORES
NOEL-V / RPX-105 | Up to 16x64-bit Cores | RV64GC, RV22, RV23 | MMU

CACHE LINE SEPARATION & AUTHENTICATION
Hardware-enforced cryptographic separation of instruction & data caches

INLINE MEMORY ENCRYPTION
Per cache line runtime encryption & authentication | Ephemeral rolling keys

HARDWARE SECURE BOOT
Hardware-enforced trusted boot from power-on | Data-at-Rest Encryption

SOFTWARE EXPLOIT PREVENTION + RISC-V SECURITY EXTENTIONS

PROJECT INTEGRATION

- OS Support Linux/ VxWorks/ FreeRTOS/ Bare Metal
- Toolchain Compatible GCC + Standard RV64G ISA
- Zero Trust Ready Cryptographically secure TCB
- DoD Trusted Supplier NIST-approved

WHY IT MATTERS

56% of Critical CVEs are Memory Corruption- HPS blocks all of them.

Minimal dev changes. Drag-and-drop integration.

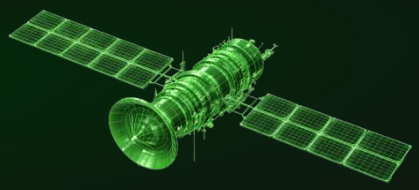
FULL LIFECYLE PROTECTION

Provisioning: Data-at-Rest Encryption & Signing → **Secure Boot:** Hardware-Enforced Trusted Boot → **Runtime:** Inline Encryption + Cache Auth → **Updates:** Set & Forget- No Mandatory Maintenance

Data Sheet Version: 2026.4
PRI-2605-0001

GENERAL DYNAMICS
Mission Systems

IDAHO SCIENTIFIC



Benefits

Benefit	Description
Zero Trust Enablement	Cryptographically secure platform or running a device's trusted computing base - integral to ZT architectures
Low Risk	Proven on defense programs; NIST approved algorithms with demonstrated SCA resistance
Full Lifecycle Protection	Maintains confidentiality and integrity of IP and CPI from provisioning through runtime
Transparent to Developers	Minimal changes to compilation process; compatible with existing development practices
Simple to Integrate	Drag-and-drop with reference designs, test benches, and common interface IP
Set & Forget	No annual maintenance contracts; future updates are optional
Efficient & Customizable	Power-efficient compute configurable from embedded to enterprise performance needs
Trusted Supplier	US DoD supplier with US engineering support via email, phone, or in-person

Features

Feature	Detail
Pre-Integrated RISC-V Cores	NOEL-V and RPX-105; up to 16x64-bit cores (RV64GC, RV22, RV23) with MMU
Cache Line Separation & Authentication	Hardware-enforced cryptographic separation and authentication of instruction and data caches
Inline Memory Encryption	Per cache line runtime encryption and authentication- ephemeral rolling keys
Data-at-Rest Encryption	Encrypts/signs at provisioning; decrypts/authenticates at load
Hardware Secure Boot	Hardware-enforced trusted boot from power-on
Software Exploit Prevention	Prevent memory corruption exploits from enabling arbitrary code execution
RISC-V Security Extensions	Zicfiss, Zicfilp, Crypto Vol I & II, PMP, Sv32/39/48
CNSA 2.0/ FIPS 140-3 Crypto	AES-256-GCM, DPA/ SCA resistant
Common OS Support	Linux, VxWorks, FreeRTOS, Bare Metal
Binary RISC-V Compatible	Standard RV64G ISA, works with GCC and standard toolchains