GENERAL DYNAMICS Mission Systems | IDAHO SCIENTIFIC

Keystone Security Architecture

Securing Defense Systems with COTS Hardware Confidence

The Problem

COTS hardware was not designed for defense weapon system threat models, leaving programs exposed to:

- **Battlefield Loss & Foreign Military Sales (FMS)-** Adversary access to sensitive technology
- **Anti-Tamper / Reverse Engineering-** Critical Program Information (CPI) exposed through physical access
- **Cyber Exploitation-** Software and firmware attack surfaces inherent in commercial designs
- **Performance Maintenance Gaps-** Lack of secure update and authentication mechanisms

Keystone Solution

Keystone™ is a defense-grade security infrastructure that addresses the inherent vulnerabilities of Commercial-Off-The-Shelf (COTS) hardware in weapon systems. Keystone operates as a **federated security hierarchy** with two primary roles:

- **System-Level Root of Security (RoS)- Broker** Central security authority managing cryptographic operations, key management, secure boot, and system state monitoring.
- **Local Root of Security (RoS)- Agent** Deployed at each x86 subsystem, enforcing policy locally and out-of-band, fully transparent to the host OS and applications

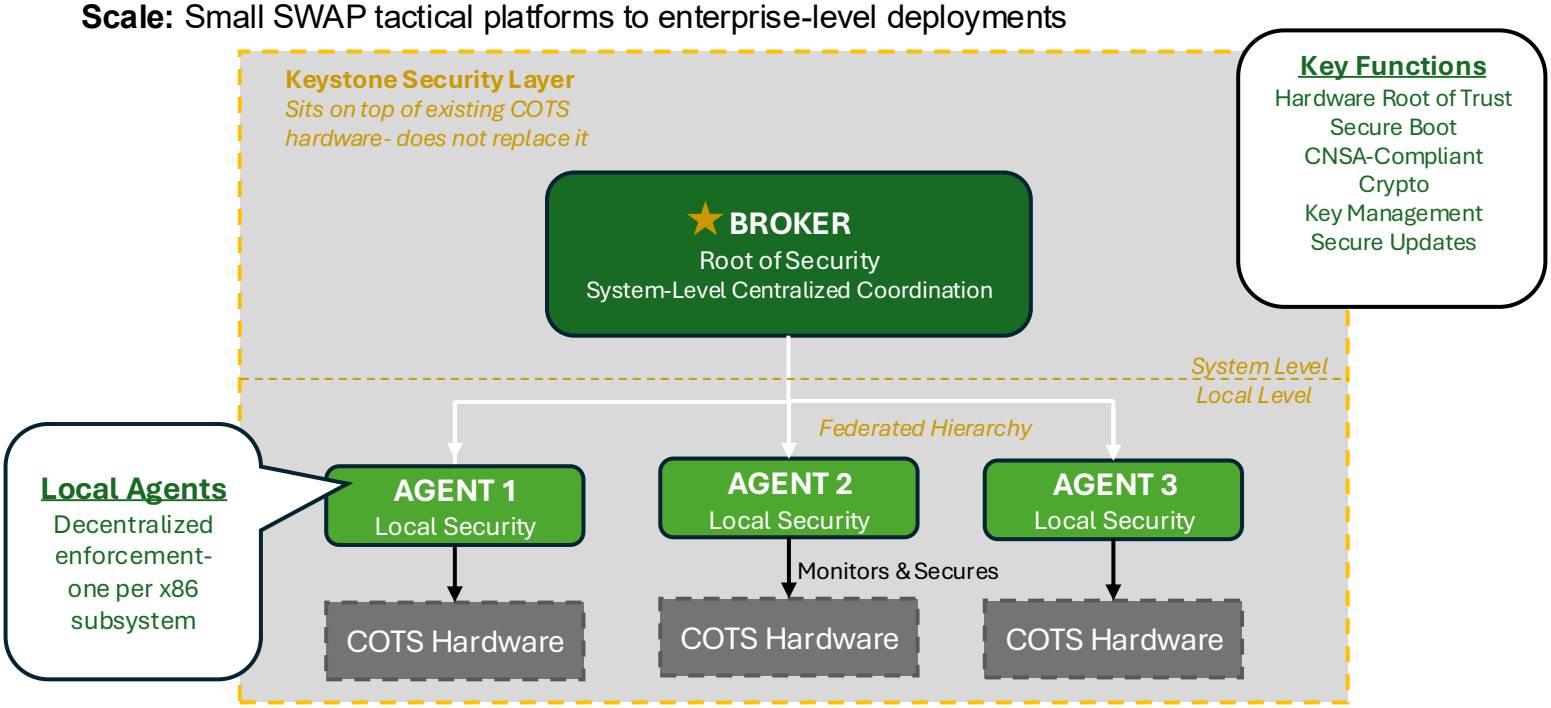
Supported Hardware

Pre-Integrated COTS SBCs: Abaco Systems, Curtiss-Wright

Custom Hardware: Supported via embedment specification & engineering assistance

Supported FPGAs: Xilinx UltraScale, UltraScale+, Zynq UltraScale+ MPSoC/RFSoC, Versal

Scale: Small SWAP tactical platforms to enterprise-level deployments



GENERAL DYNAMICS
Mission Systems

IDAHO SCIENTIFIC

Benefits

Benefit	Description
Low Risk	Proven on other defense programs; use existing hardware investment
Set and Forget	No annual maintenance contracts. Implementation of future updates is optional.
Compliance Ready	Addresses core AT and Cyber Survivability requirements common to defense programs
COTS Enhancement	Fully leverages native COTS/ S-SOTA security features while closing residual vulnerabilities

Features

Feature	Detail
Hardware Root of Trust (HwRoT)	Hardware-based RoS or system monitoring, sensing, and response
CNSA-Compliant Crypt	Side-channel resistant cryptographic cores meeting NSA suite requirements
Secure Boot w/ CFI Sensing	Detects and response to boot-process attacks on x86 processors
Key Management Engine	Full cryptographic key lifecycle management within the hardware boundary
Purpose-Built FPGA Logic	Out-of-band security enforcement independent of the host software stack
Tailored BIOS	Custom BIOS hardened for defense weapon system use cases
Secure Maintenance & Updates	Cryptographically authenticated update mechanism
Federated Hierarchy	System-level Broker+ local Agents for centralized coordination and decentralized enforcement

Deliverables

RTL / IP

Hardware

Documentation

Support

Software