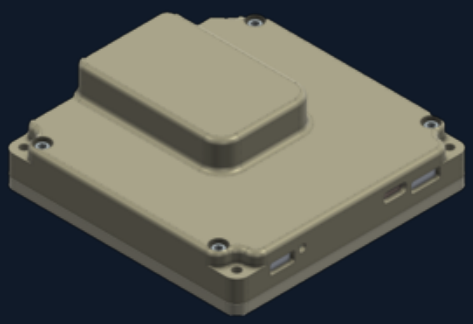
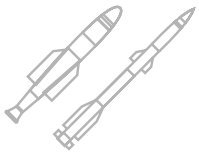
WebSensing



Edge Cyber Protection Suite

Encryption · Network Gateway · Anomaly Detection

Applications



Modernizing Legacy Platforms

Interface legacy systems to modern systems, enabling new capabilities while maintaining data integrity.

Space & Power-Constrained Environments

Our ultra compact form factor can embed anywhere without compromising on performance

DiD and Hardware Root of Trust For The Edge

Low latency anomaly detection for data in motion across all edge platforms

Specifications

Model	XCA-E2E	XCA-U2E (coming 2026)
Network Protocols Supported	ETHERNET to ETHERNET	USB 3.2 to ETHERNET
Protocols and Connectivity		
Maximum full throughput	20Gbps	20Gbps
Supported speeds	100M / 1G / 2.5G / 5G / 10G	100M / 1G / 2.5G / 5G / 10G
Protocol-Aware Validation	✓	✓
Security		
Red/Black Separation	✓	✓
Secure key fill interface	EKMS, DS101	EKMS, DS101
Tamper resistance	✓	✓
Environmental failure protection	✓	✓

Model	XCA-E2E	XCA-U2E (coming 2026)
Key zeroization	Button, Tamper, Command	Button, Tamper, Command
Encryption in transit at line rate	✓	✓
Authentication in transit at line rate	✓	✓
IP Address Filtering	✓	✓
Port Filtering	✓	✓
MAC Address Filtering	✓	✓
Protocol Filtering	✓	✓
Network Throttling	✓	✓

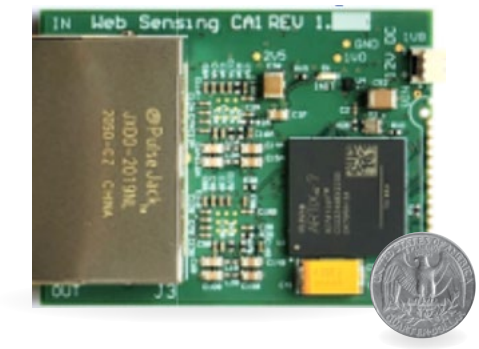
Model	XCA-E2E	XCA-U2E (coming 2026)
Encryption and Policy		
Quantum resilience	✓	✓
Encryption modes	AES-256 GCM w/PSK AES-256 GCM-SIV	AES-256 GCM w/PSK AES-256 GCM-SIV
Anomaly Detection	✓	✓
Certifications		
NSA Type 1	On Roadmap	On Roadmap
FIPS 140-3 Security Level 3	In Progress	In Progress
Performance		
Size, Weight Power	100mm x 100mm x 45mm 0.5 kg	

Model	XCA-E2E	XCA-U2E (coming 2026)
Power	9VDC - 35VDC 15W MAX	
Ultra low latency for high performance	✓	✓
Latency	<100µs	<100µs
Management		
SW Application	✓	✓
Console	✓	✓
Environment, Regulatory and Safety		
EMI/EMC/ENV	MIL-STD	MIL-STD

Security for data in motion

The Edge-CPS encrypts data in transit, and provides Defense-in-Depth security and hardware-based root of trust to secure communications at the edge in real-time.

- Symmetric cryptography using AES-GCM-256 with pre-shared keys (PSKs) ensures security against emerging quantum threats
- Supports AES-GCM-SIV mode for nonce misuse resistance and protection against replay attacks
- The anomaly detection can validate and mitigate malicious traffic by dropping invalid messages and closing connections.
- The all-hardware implementation is impervious to malicious software attacks and persistent implants; they are designed to combat reverse-engineering.
- Where needed, the devices can selectively operate on traffic within Virtual Private Network (VPN) tunnels.
- FIPS 140-3 approval and NSA Type 1 compatibility ensure interoperability with existing commercial and NSA standards



Network & Protocol Gateway

- The Edge CPS bridges the gap between bus architectures (MIL-STD-1553, CANbus/J1939, USB, PCI) and networking protocols (Ethernet, Link-16) with speeds up to 20Gbits/sec, allowing for real time encryption of various inputs and outputs simultaneously.
- FPGA-based NSA Type 1 compatible symmetric cryptography ensures security against emerging threats.

About WebSensing

We are experts in data encryption, protocol translation & system hardening

Decades of cutting-edge research in cryptography and cybersecurity in collaboration with the **US government, federal system integrators, and academia.**