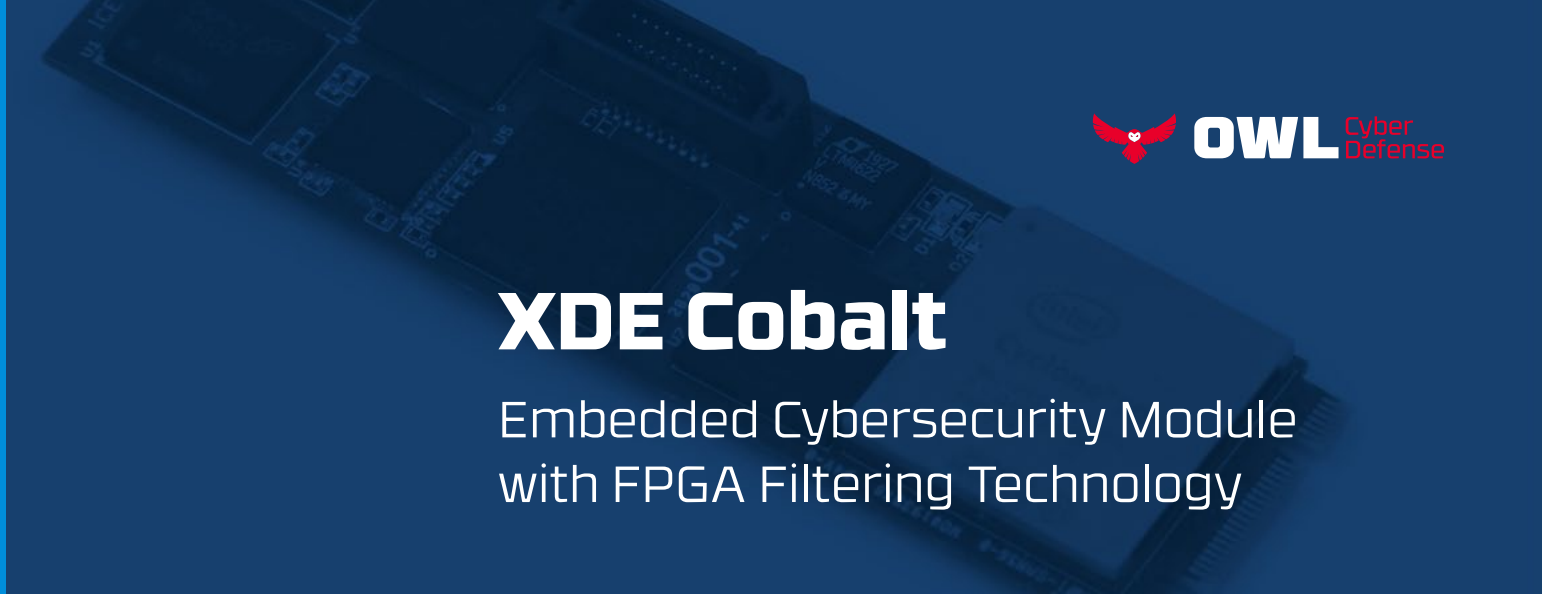
DATA SHEET



XDE Cobalt

Embedded Cybersecurity Module with FPGA Filtering Technology

AT-A-GLANCE

- Low SWaP-c (size, weight, power, and cost), 1 Gbps, cybersecurity module
- Developed with FPGA (Field Programmable Gate Array) filtering technology, with line-rate protocol inspection
- Available as an embedded module for new or existing product designs
- Enforces strict one-way traffic, or allow two-way traffic, with strict protocol validation and enforcement
- Satisfies NERC-CIP requirements for one-way data transfers in power generation applications
- Supports Department of Homeland Security (DHS) and National Institute of Standards and Technology (NIST) Special Publication 800-82 guidelines for protecting critical assets
- Security assurance does not depend on frequent software patches and updates

Defending Operational Technology

Industrial network owners are seeking alternatives to complex, maintenance-intensive industrial firewalls. Industrial device manufacturers that embed more secure, less expensive cybersecurity solutions into industrial network devices, position themselves to increase market value by meeting industrial network owners' expectations for enhanced security. Embedding cybersecurity into industrial devices helps industrial network owners confidently eliminate, or curtail, stand-alone industrial firewall devices, with a more secure and unified approach. This migration away from stand-alone to embedded cybersecurity, creates a compelling business case, by delivering a larger percentage of the overall network spend to industrial device manufacturers. Because of this, Owl is decomposing our technology and making it available as individual modules for industrial device manufacturers.

Owl is breaking new ground by providing a low SWaP-c (size, weight, power, and cost) cybersecurity module that can be designed into industrial control systems to provide hardware-enforced data evaluation and control, without exposing industrial devices to new threat vectors. This module reduces operators' needs for additional cybersecurity solutions and the overhead associated with maintaining it, thereby reducing both their capex and opex costs.

XDE Cobalt

This technology is a miniaturized, hardware-based, cybersecurity module that be incorporated into industrial devices, including PLC modules, engineering workstation servers, and network gateways. This module incorporates advanced FPGA-based protocol validation and firewall rule enforcement, with the benefit of hardware-controlled flows. XDE Cobalt can be configured to enforce strict one-way traffic, or allow two-way traffic, with strict protocol validation and enforcement. Supporting a throughput maximum of 1 Gbps, XDE Cobalt is resilient against DDoS attacks with line-rate protocol inspection, while providing secure data transfers.

Embedded Modules

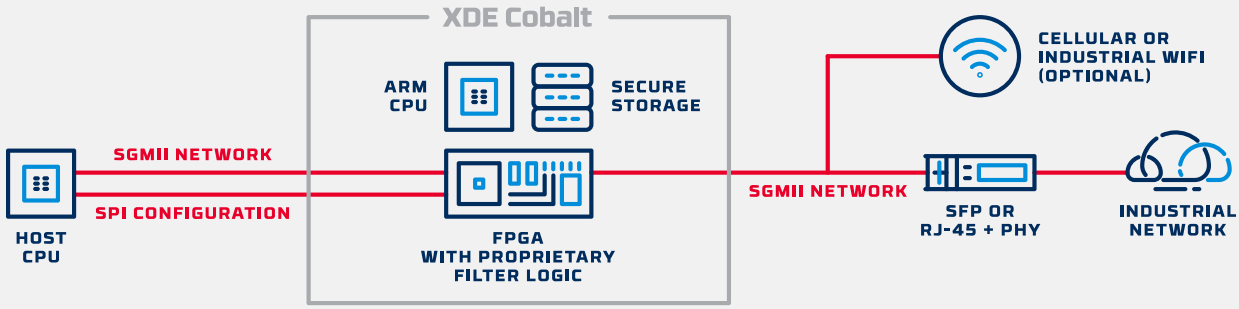
For operators, designers, and manufacturers of advanced, connected, industrial and critical infrastructure controllers and safety systems, this module can be built-into modular platforms, such as a controllers, SCADA devices, safety systems, and network switches. This module provides a deterministic, one-way data transfer that provides very secure data flow management between equipment and external networks.

XDE Cobalt

1 Gbps, Data Transfer Module with Filtering

PROTECTION INSPIRED BY GOVERNMENT REQUIREMENTS

For many years, the agencies and departments supporting the critical missions of the U.S. government, have recognized the need to not only keep threats out, but to also block infected data from getting in. Effective data filtering, at high speeds, allows this to be achieved. The FPGA technology within this module not only operates at line-rate, but also has low power consumption. XDE Cobalt protects application processors from external network threats in any industrial device and unlike software-based technologies, does not require extensive, on-going maintenance and updates. The run-time environment for this module is inaccessible, with no on-system configuration, user interface, or administration. A single, secured run-time executable with embedded security policies is downloaded and that is the only thing that can execute, therefore nothing else can be introduced into the environment.



Key Features

- High throughput maximum of 1 Gbps
- Hardware-based protocol validation and flow-control that is impervious to software-based threats
- Line-rate protocol inspection that is resilient against DDoS attacks
- Verification and authentication of common industrial protocols that operate over an IP network
- Internally performs a secure boot
- IPSec and TLS/DTLS VPN support
- The admin port is segmented from network traffic for configurations and software updates

Technical Specifications

POWER SUPPLY
Power, configuration, and data inputs/outputs are all through a single edge connector

NETWORK CONNECTIVITY
1x 1Gb 60 pin male edge connector

BOARD DIMENSIONS
22mm × 80mm
Standard M.2 module dimensions

SUPPORTED PROTOCOLS
UDP (Unicast, Multicast) and common industrial protocols

OPERATING CONDITIONS
-40°C to +70°C

DEVICE LIFESPAN
14 years

THROUGHPUT
Maximum of 1 Gbps