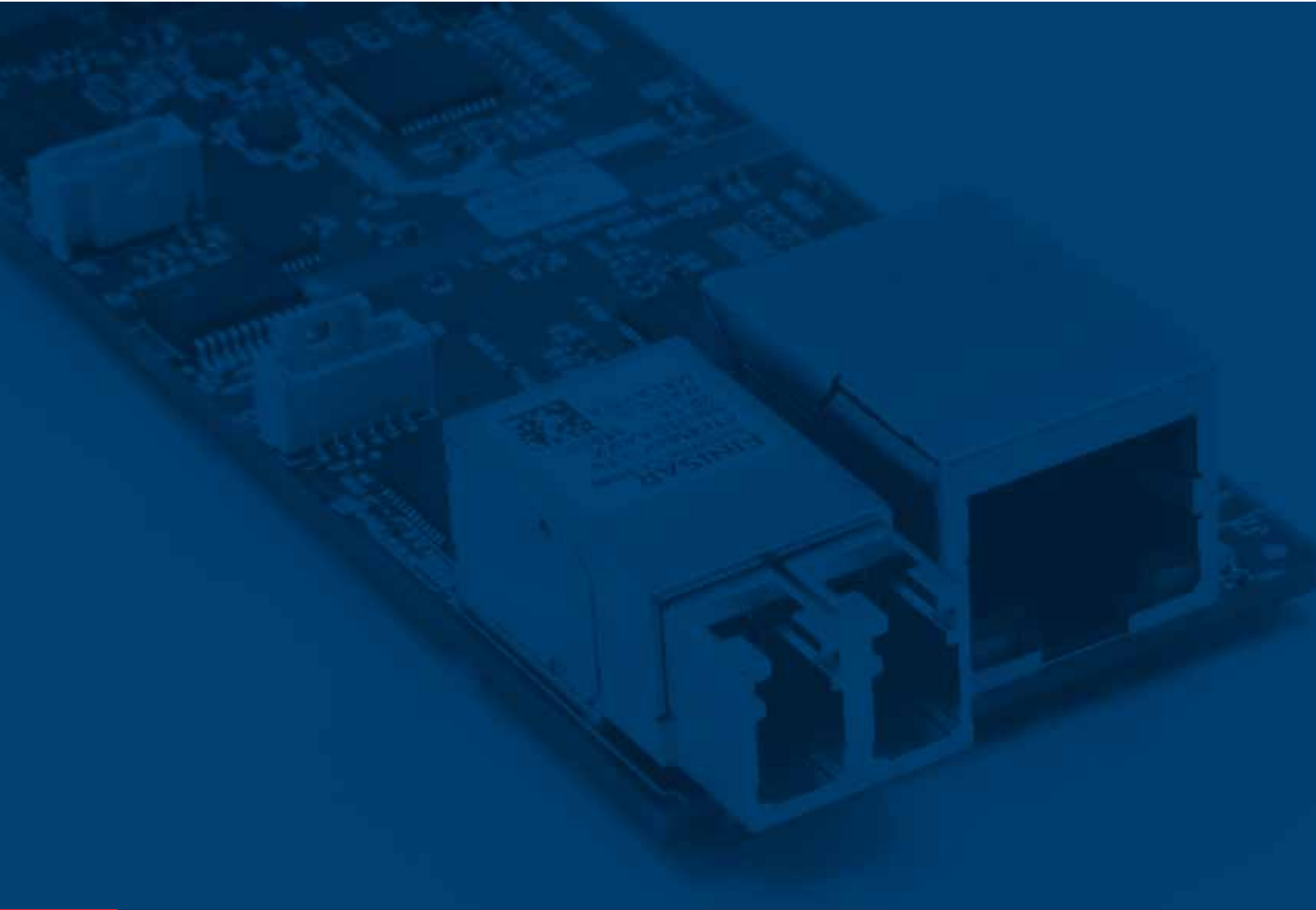OWL Cyber Defense

XDE

Embedded Cybersecurity Modules

Embedded Cybersecurity

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.

Planning on Developing Your Own Network Security Solution?

Why create, test, and validate a network security solution on your own? Owl has spent decades researching, strategizing, developing, testing, validating, updating, and maintaining cross domain solutions and data diodesto provide proven, high assurance, validated technology that critical infrastructure organizations can trust. Developing your own embeddable network security solution requires resources, high costs, and a tremendous amount of time and effort. Trust the experts and get to market faster by leveraging Owl's embedded modules and expertise.

Why Owl Cyber Defense?

EXPERTISE

- A leader in the network security industry for over 20 years
- U.S. owned and operated with a U.S. supply chain
- A leader in cross domain solutions
- Multi-market solutions – critical infrastructure, DoD, and intelligence agencies
- Trusted by the world's largest critical infrastructure and defense organizations
- 40+ patents | 20 patents pending
- 2,500+ deployments globally

SERVICES

- Build custom, hardware-based, application-specific filters that are tuned to enforce unique requirements for your protected asset
- Integration and testing of hardware security modules to provide validation in realistic networking environments
- Create customized versions of the modules or license the design for use in your own integrated layout

The Benefits of FPGA Technology

The goal of many network-based cyber attacks is to cause a remote CPU to execute new code and/or override data and application boundaries. Hackers strive to deliver malicious content into a CPU, trigger a fault or unexpected condition in the CPU, and then execute malicious behaviors. Typically, a firewall would be installed to mitigate network-based attacks, however firewalls are just another CPU running software with infinite programmable states. The bottom line is that CPU-based technologies can be reprogrammed to do anything (good or bad). Knowing this, Owl is introducing XDE, a new product line of FPGA-based, embedded cybersecurity modules that support high throughputs, enforce strict flow control, and implement simple-to-complex data filtering configurations.
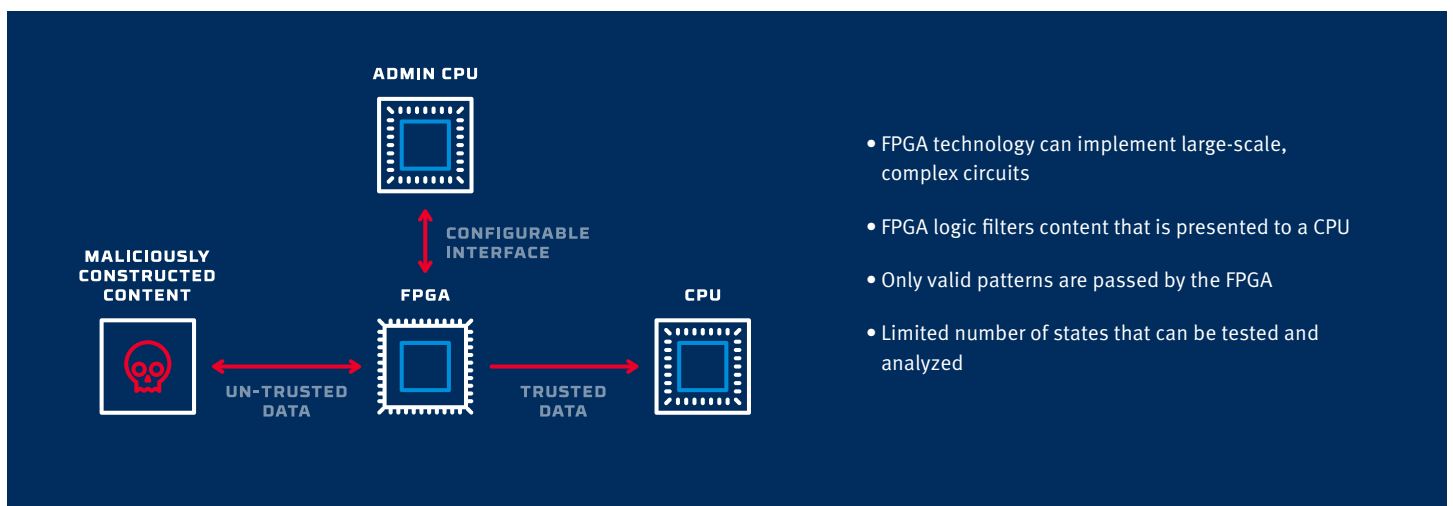
FPGA

- Can only do what it is programmed to do – finite number of states
- Circuit can be extensively tested and validated
- FPGA configuration can only be updated through an independent data path
- Attacks often require physical access
- Difficult to find open source hacker tools because FPGA circuits are so customized

VS.
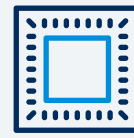
CPU

- Can be programmed to do anything – unlimited states
- Not practical to test every input/output combination
- Attack patterns are repeatable once successful
- Attacks can be done remotely
- Easy to find open source hacker tools with proven techniques – higher returns and quicker attack success

ADMIN CPU

CONFIGURABLE INTERFACE

MALICIOUSLY CONSTRUCTED CONTENT

FPGA

CPU

UN-TRUSTED DATA

TRUSTED DATA

- FPGA technology can implement large-scale, complex circuits
- FPGA logic filters content that is presented to a CPU
- Only valid patterns are passed by the FPGA
- Limited number of states that can be tested and analyzed

XDE Modules

Owl's Cross Domain Embedded (XDE) modules are disrupting the market due to their size, flexibility, power, and speed.

Supporting a high throughput range of 1 Gbps to 40 Gbps, these modules provide hardware-enforced data evaluation and control, without exposing the secure network to risk. Developed with FPGA (Field Programmable Gate Array) filtering technology, these miniaturized modules are disrupting the market due to their size, flexibility, power, and speed and can be designed directly into industrial control systems.
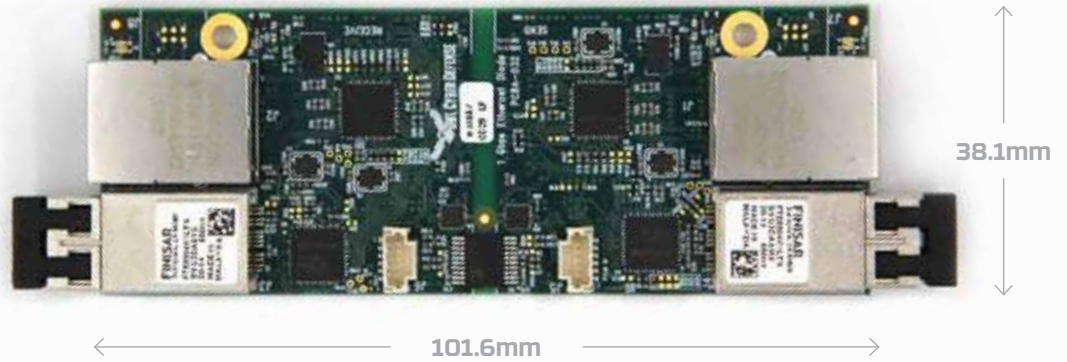
XDE Radium

Miniaturized, hardware-enforced, modular solution that provides high-assurance, one-way data transfers from trusted to untrusted networks, without requiring new software or computation resources. This FPGA-based module can be directly embedded into industrial devices where safety and assurance is critical.

XDE Cobalt

Miniaturized, hardware-enforced, modular solution that can be incorporated into industrial devices, including PLC modules, engineering workstation servers, and network gateways. This FPGA-based module can be configured to enforce strict one-way traffic, or allow two-way traffic, with strict protocol validation and enforcement. Supports a maximum throughput of 1 Gbps.

38.1mm

101.6mm
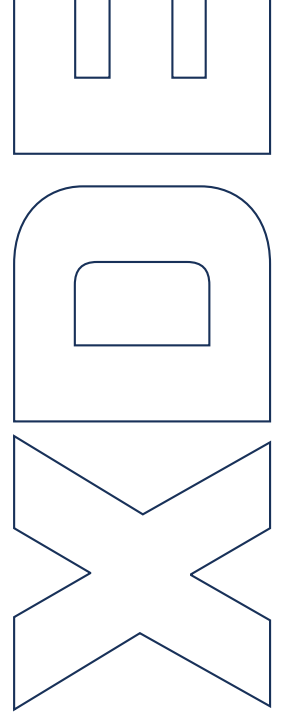
XDE Radium

A miniaturized, single-board, cross domain module that can be incorporated into the design of industrial devices where safety and assurance is critical. This compact hardware module provides high-assurance, one-way data transfers from trusted to untrusted networks, without requiring new software or computation resources. Unlike a network tap, XDE Radium implements a secure protocol break and no routable information is passed between source and destination networks. With a standard ethernet interface and a high-throughput maximum of 1 Gbps, this module performs one-way UDP (Unicast & Multicast) transfers, preventing external access to industrial devices.

TECHNICAL SPECIFICATIONS

POWER SUPPLY
Separate power sources on the source and destination sides of the module for security

NETWORK CONNECTIVITY
Single CAT 5/6 input and single CAT 5/6 output

BOARD DIMENSIONS
101.6mm × 38.1mm

SUPPORTED PROTOCOLS
UDP (Unicast, Multicast) & TCP/IP (in development)

OPERATING CONDITIONS*
-40°C to +70°C

DEVICE LIFESPAN
14 years

THROUGHPUT
Maximum of 1 Gbps

KEY FEATURES

- High throughput maximum of 1 Gbps

- One-way UDP (Unicast & Multicast) and TCP/IP (in development) support

- Optical isolation with a single fiber optic cable or digital isolation

- Protocol break – no routable information is passed between source and destination networks

- Extended operating temperature range (-40°C to +70 °C)

- Low power consumption – no new software or computation resources needed

- Standard CAT 5/6 ethernet interface (in/out)
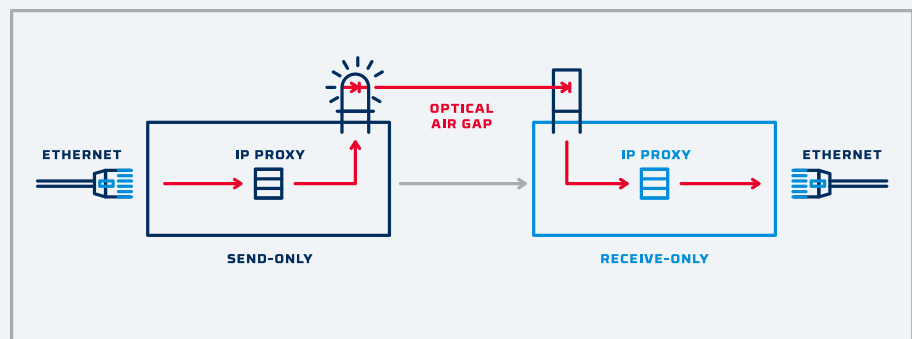
XDE Radium

Design Patterns

See how XDE Radium can be applied into your designs.

ONE-WAY DATA TRANSFER

- Guaranteed one-way transfer

- Protocol break – no routable information is passed between source and destination networks

- Secure UDP transfer

- Scalable module

ETHERNET   IP PROXY   OPTICAL AIR GAP   IP PROXY   ETHERNET

SEND-ONLY   RECEIVE-ONLY

XDE RADIUM USE CASE

- IP camera in a secure network needs to be secured to prevent threats from spreading and infecting the network

- XDE Radium is installed in front of, or embedded into, the IP camera to securely transfer data one-way out of the secure network to a monitoring center

- XDE Radium only sends data to whitelisted destinations

- IP camera becomes a secure, managed device on the network and can be monitored remotely

SOURCE NETWORK

IP CAMERA   XDE RADIUM   MONITORING CENTER

22mm

80mm
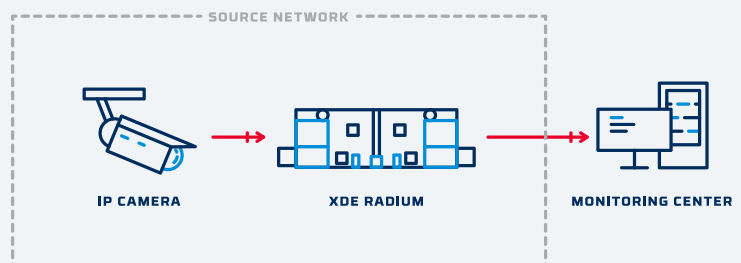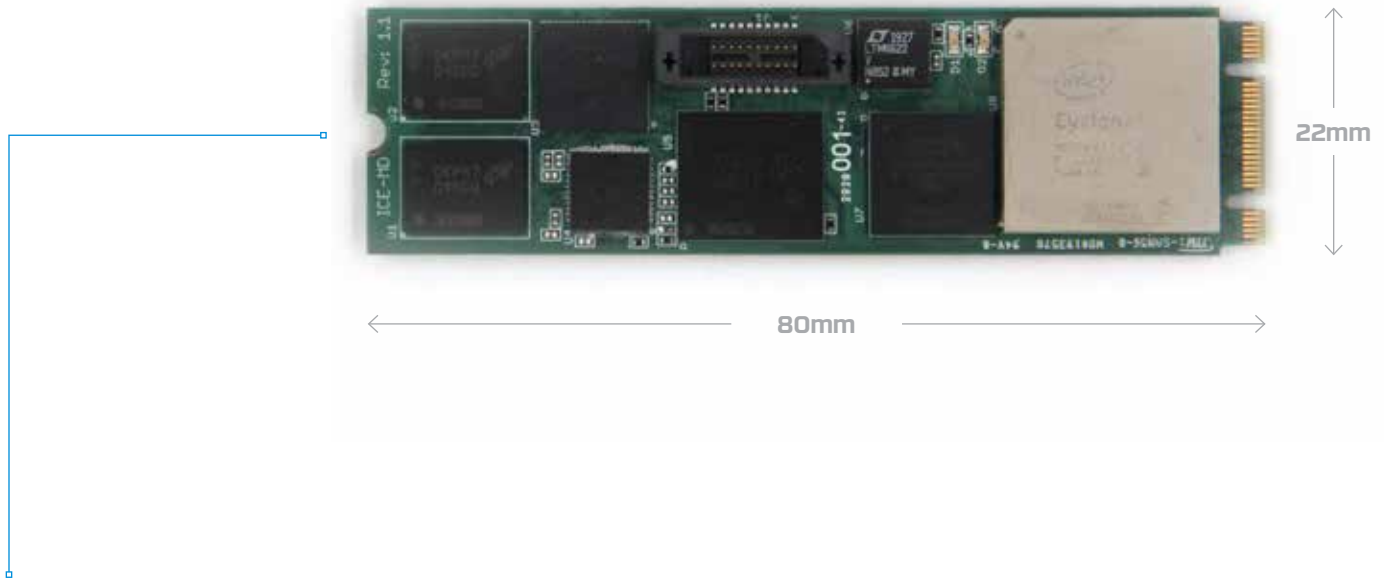
XDE Cobalt

A miniaturized, hardware-based, modular network security solution 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 (one-way only or two-way). 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.

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
SGMII network connection in/out

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

XDE Cobalt

Design Patterns

See how XDE Cobalt can be applied into your designs.

FPGA PROTOCOL FILTER

• Module with copper or SFP interconnects

• One network input and one network output

• Factory configured with mission-specific filters

• Field upgradable via a laptop with a USB to SPI
  interface and digitally signed config file

• Ethernet interface without ethernet cables

• Serial Gigabit Media Independent Interface (SGMII)
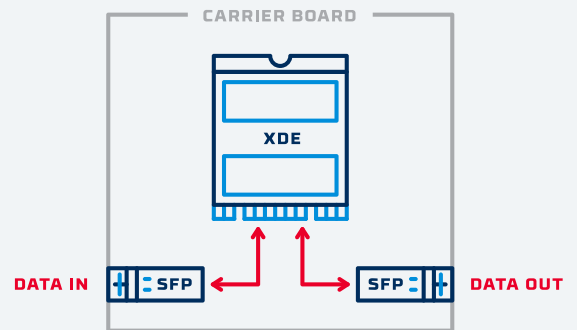
FPGA CROSS DOMAIN SOLUTION

• Two XDE Cobalt modules

• Dual-proxy cross domain solution with an
  FPGA filter – separate processing of data
  inputs and data outputs

• TLS encryption

• Optional optical OWT on carrier board

• Factory configured with mission-specific filters
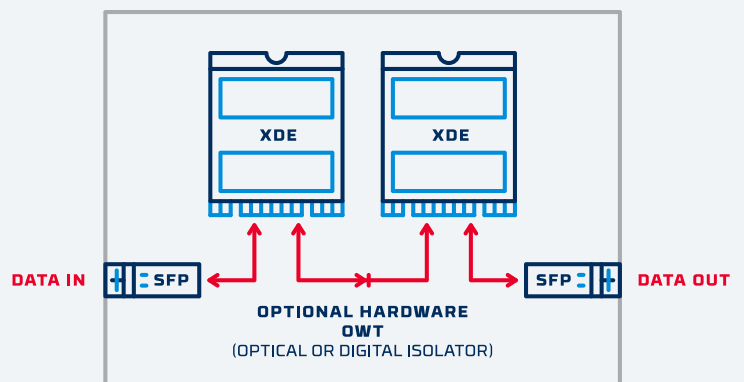
CROSS DOMAIN DISTRIBUTOR

- Supports a single input with multiple isolated outputs or a single output with multiple isolated inputs (not limited to only four)

- Optional optical OWT

- Supports secure data distribution (e.g., navigation data, position and timing data, and industrial protocol signal distribution)

- Supports isolated redundant paths for high resiliency
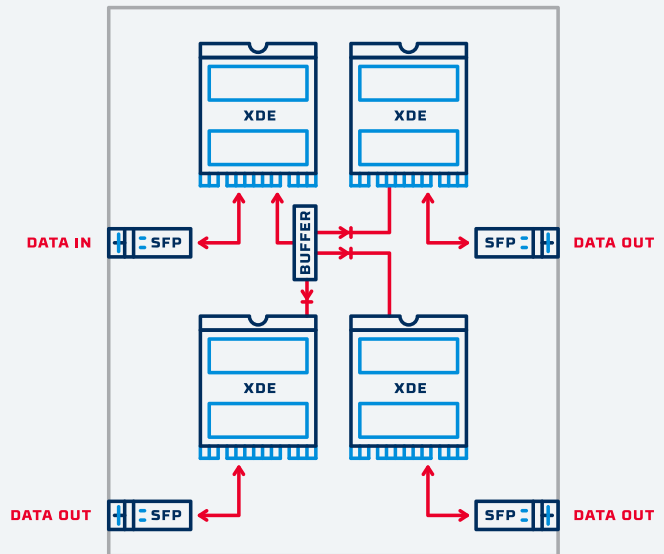
SECURE MEDIA CONVERTER

- Hardware-enforced protocol filtering

- Supports non-Ethernet adapters

- Supports serial data

- Can support low speed RX-232 data
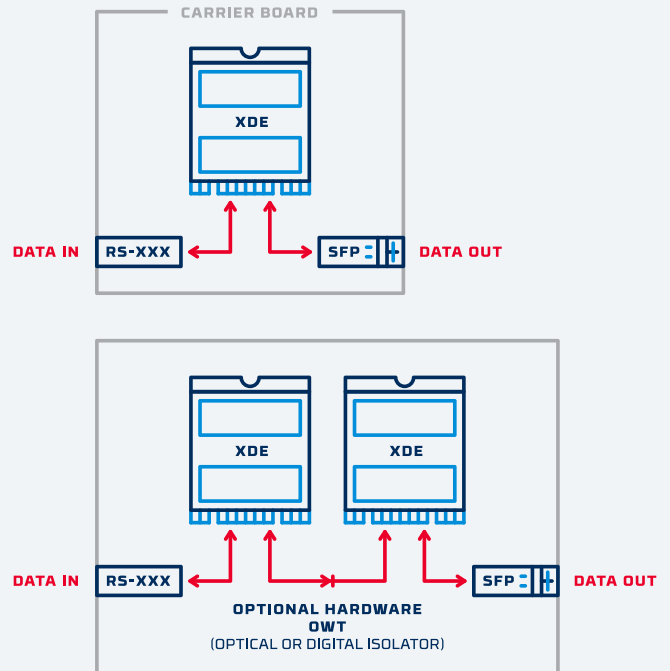
OWL Cyber Defense

Owl Cyber Defense Solutions, LLC leads the world in data diode and cross domain network cybersecurity. With a constant focus on customers in the military, government, critical infrastructure, and commercial communities, Owl develops market-first, one-way data transfer products to meet a variety of operational needs, from entry level to enterprise.

For more information on Owl, or to schedule a demo, visit www.owlcyberdefense.com

@OwlCyberDefense   203-894-9342 | Info@owlcyberdefense.com