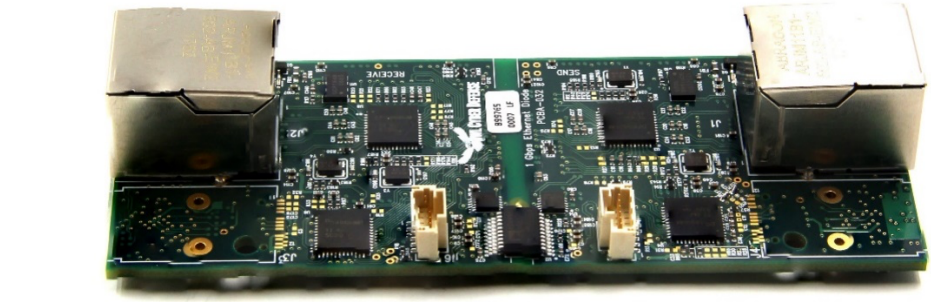
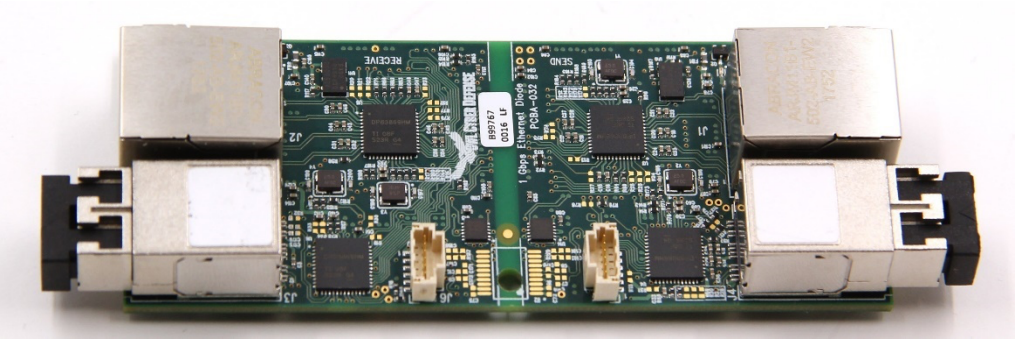
Owl XDE Radium V1.3 One-Way Transfer (OWT) Data Diode Module

Security Target

Common Criteria - EAL4+ Certification





Document: Owl XDE Radium V1.3-SecurityTarget-EAL4.doc
Version: 1.3
Date: 11 February 2022

Prepared By: Mike Parry
Prepared For: Owl Cyber Defense Solutions, LLC
42 Old Ridgebury Road
Danbury, CT 06810
USA

Web: http://www.owlcyberdefense.com
Tel: +01 203-894-9342
Fax: +01 203-894-1297
Toll-free Customer Service (USA Only): 866-695-3387

TABLES OF CONTENTS

LIST OF TABLES

1 Security Target Introduction (ASE_INT.1)

1.1 Security Target Reference

ST Title	Owl XDE Radium V1.3-SecurityTarget
ST Version	01m
ST Publication Date	07/05/22
Vendor and ST Author	Owl Cyber Defense Solutions, LLC
CC Identification	Common Criteria for Information Technology Security Evaluation, Version 3.1 Rev 5, April 2017
TOE Identification	The TOE consists of two security hardware product models – Optical model and Digital model.

Table 1 ST Identification

1.2 TOE Reference

TOE Hardware Products		**Maximum Speed**	**Channels**	**Part Number / PCB Version PCB Number (Card Identity)**
Owl XDE Radium V1.3 Optical Isolator module		1 Gbps	1	XDE-RAD-OWT-OI-XX (Optical Isolator Version)
Owl XDE Radium V1.3 Digital module		1 Gbps	1	XDE-RAD-OWT-DI-XX (Digital Isolator Version)

Table 2 TOE Hardware Products

Developer Name	Owl Cyber Defense Solutions, LLC	**Firmware Revision**
TOE Identity	Owl XDE Radium V1.3 module	V1.3.0.0
TOE Version Number	Version 1.3	
Note: TOE Identity V1.3.0.0 is the top-level product version number. The V1.3 TOE consists of several different components – each of which has a unique version number. Specifically, V1.3.0.0 consists of the following major components: - Firmware Version: 1.4.0.15 - HW Version: Rev. B-01 RW-02 - XD Manager Version: 1.0.0.2 - User Guide Version: V1.3_r02a		

Table 3 TOE Identification

1.3 TOE Overview

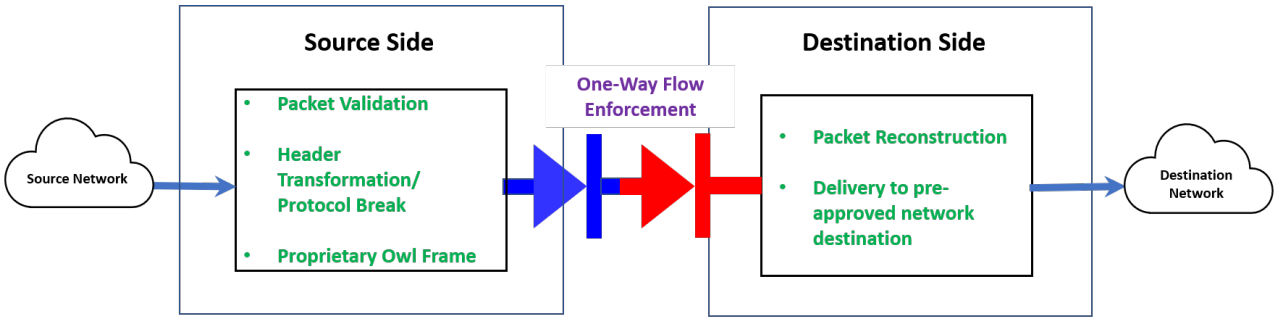
The Target of Evaluation (TOE) is the Owl XDE Radium V1.3 module, which is designed and manufactured by Owl Cyber Defense Solutions, LLC (Owl). The XDE Radium V1.3 module is a 101.6 mm x 38.1mm embeddable module for installation into a variety of industrial control and tactical devices, as well as being used in a variety of Owl branded products. Owl produces two XDE Radium models – one with an Optical Isolator and the other with a Digital Isolator; the two models are identical in every way except for the different hardware isolators. The XDE Radium (both models) performs two major cybersecurity functions: 1) packet header deconstruction and reconstruction to eliminate the possibility of malicious (header) code being passed from one domain to another, and 2) one-way data flow enforcement. XDE Radium's TOE is the circuit board and accompanying filtering firmware.

The XDE Radium is a relatively simple device. It has no Central Processor Unit (CPU), and thus no Operating System (OS). The major security components are two Field Programmable Gate Arrays (FPGAs) and either an optical or digital isolator. The FPGAs and Isolator (optical or digital) working together, and aided by the overall board architecture, perform packet-by-packet header filtering and enforce strict one-way transfer (OWT) between the Source and Destination networks.

XDE Radium will be a primary security component within host devices such as industrial servers, edge computers, gateways, sensors, programmable logic controllers (PLC), Perimeter Defense Systems (PDS), etc. XDE Radium is expected to be used in solutions that protect commercial critical infrastructure (primary) and in military and government-focused solutions.

It is assumed that XDE Radium will be implemented in host devices that connect two dissimilar networks, zones, or enclaves. There are two common (envisioned) functions for the TOE within the host device. The first is protecting the Source network and the host device from threats originating in the Destination network. The second function is protecting the Destination network from malicious content embedded in packet headers.

XDE Radium uses a software Configuration Utility application for setting Source and Destination network whitelisted connections. The Configuration Utility runs on Windows and Linux operating systems, and the configuration workstation/laptops connects to the circuit board's Source and Destination serial UART connectors to download network configuration policy prior to normal operations. Once configurations are downloaded to the FPGAs, the Configuration Utility's workstation/laptop will be disconnected from the circuit board and will not be used during normal operation.



Text Color	Protects
	The Destination Network from malicious code embedded in packet headers
	The Host Device and the Source Network from threats originating in the Destination Network

Figure 1 - XDE Radium Protection Features

Customer Usage: XDE Radium is envisioned for use in Industrial Networks, US Department of Defense, US Intelligence Community, CSE Canada, and allied networks to enforce one-way data transfer from one network domain to another. Example Use-Cases:

Industrial Data

- Inbound Protection: Approving connections and performing header validation and transformation of data arriving at the host device from low level industrial sensors. Blocking unauthorized connections and/or dropping packets with unauthorized header content. Performing a protocol break to eliminate routable information before a transformed Owl frame is passed across the hardware isolator.
- Outbound Protection: Ensuring authorized packet header content and establishing a one-way connection for delivery of industrial network performance data from a more critical operational technology (OT) network to a less critical information technology (IT) monitoring network.

Military Tactical Data

- Inbound Protection: Approving connections and performing header validation and transformation of data arriving at the host device from low level industrial sensors. Blocking unauthorized connections and/or dropping packets with unauthorized header content. Performing protocol break to eliminate routable information before transformed Owl frame is passed across the hardware isolator.
- Outbound Protection: Ensuring authorized packet header content and establishing a one-way connection for delivery of tactical sensor data from a more secure, classified network to a less secure, unclassified network.

Market Usage: XDE Radium responds to a growing trend in both industrial control and military-government networks to embed hardware-based cybersecurity capability inside network devices to support network defense-in-depth with FPGA-based technology that is virtually invulnerable to the tools and techniques developed for use against the x86/Windows/Linux ecosystem.

1.4 Document Overview

The Security Target has been developed in accordance with the requirements of the CC part 3, Class ASE: Security Target Evaluation. The ST contains the following additional sections:

Section 1	Security Target Introduction	Security Target (ST) introduction, provides the identification material for the ST and the TOE, it provides an overview and a physical and logical description of the TOE.
Section 2	Conformance Claims	Describes how the ST conforms to the CC.
Section 3	Security Problem Definition	Defines the security problem that is to be addressed by the TOE.
Section 4	Security Objectives	This section defines the security objectives for the TOE and its environment.
Section 5	Security Requirements	Describes the Security Functional Requirements (SFRs) and the Security Assurance Requirements (SARs).
Section 6	TOE Summary Specification	Provides a description of IT security functions and the assurance measures of the TOE to potential customers.

1.5 Conventions, Terminology, Acronyms

This section specifies the formatting information used in the Security Target.

1.5.1 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter in parenthesis placed at the end of the component. For example, FDP_ACC.1a and FDP_ACC.1b indicate that the ST includes two iterations of the FDP_ACC.1 requirement, a and b.
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.5.2 Terminology, Acronyms and Abbreviations

The following terms and acronyms are used in this Security Target:

Acronyms / Abbreviations	Terminology / Definition
CC	Common Criteria for Information Technology Security Evaluation
Destination Field Programmable Gate Array (FPGA)	The XDE Radium's Destination FPGA interfaces with the module's isolator on one side and the Destination Network on the other side. The Destination FPGA contains firmware logic which enables it to rebuild packet headers and deliver packets to pre-defined network destinations while simultaneously preventing data flow from Destination to Source networks.
Destination Domain or Destination	The destination host system or network to receive the information transmitted through the TOE.
EAL	Evaluation Assurance Level
FPGA	Field Programmable Gate Array is a COTS semiconductor device containing programmable logic components, interconnects, and memory. FPGAs include high level functionality fixed into the silicon but are also configurable by loading application programs to perform complex functions such as packet segmentation, framing or reassembly. FPGA are "deterministic," in that they only perform the functions for which they are programmed.
Isolator	XDE Radium V1.3uses either an optical or digital isolator to impose physical one-way flow control restrictions on data flowing through the device.

JTAG	Joint Test Action Group (JTAG) interface is the usual name used for the IEEE 1149.1 standard entitled Standard Test Access Port that used for testing printed circuit boards. The JTAG interface is used only once during manufacture of the XDE Radium V1.3module to load the FPGA firmware and is left unconnected thereafter. Use of the JTAG interface requires physical access to the XDE Radium V1.3module.
PP	Protection Profile (Does not exist for one-way packet transfer systems)
Source Field Programmable Gate Array (FPGA)	The XDE Radium's Source FPGA interfaces with the Source network on one side and the modules optical or digital isolator on the other side. The Source FPGA contains firmware logic which enables it to evaluate and deconstruct packet headers before delivering packets to the isolator for one-way transfer.
Source or Source Domain	The originating network and / or source host system whence information is transmitted through the TOE.
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation – XDE Radium V1.3module
TSF	TOE Security Function
TSP	TOE Security Policy
XDE	An Owl product brand acronym representing the term, "Cross-Domain Embedded"

Table 4 Acronyms & Abbreviations

1.6 TOE Description

Owl's Security Target focuses on the Owl XDE Radium V1.3 embeddable module. The TOE controls the flow of IPv4 UDP data packets that enter the Source side of the module before exiting the Destination side of the module. XDE Radium is designed to support data rates up to 1Gbps, and packet sizes up to 1518-byte MTU. XDE Radium does not support IPv4 packet fragmentation. As mentioned in Section 1.3, XDE Radium is a relatively simple device that implements its security functions in the pre-configured FPGAs and an optical isolator or digital isolator. Together, the module's components and overall architecture support NIST 800-53r5 Information Flow Enforcement controls AC-4 (7) and (8).

1) Ethernet frames entering XDE Radium via the Source side RJ45 connector undergo several validation and transformation steps before exiting the Destination side RJ45 connector. Figure 3 is a block diagram of XDE Radium's major security processes and is described in detail below.

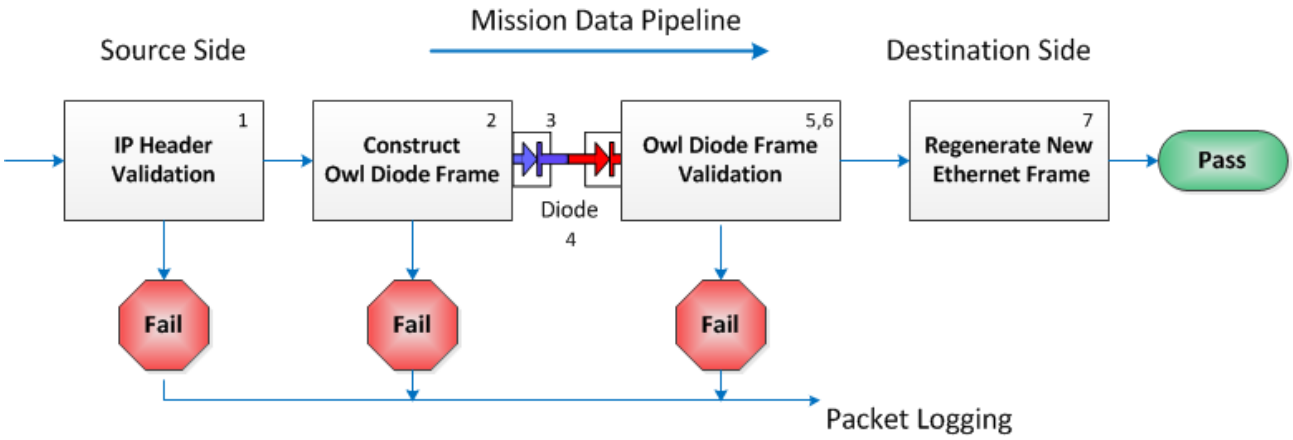


Figure 2 – XDE Radium Ethernet Frame Evaluation and One-Way Flow Enforcement Scheme

a. Step 1: The Source Side FPGA validates each Ethernet Frame based on Owl Policy. Packets must originate from a pre-approved Port, IP Address, and MAC address, and must have a valid checksum and length. Non-compliant packets will be dropped. Figure 3 shows a standard ethernet frame that will be delivered from the Source net[1]work to XDE Radium.

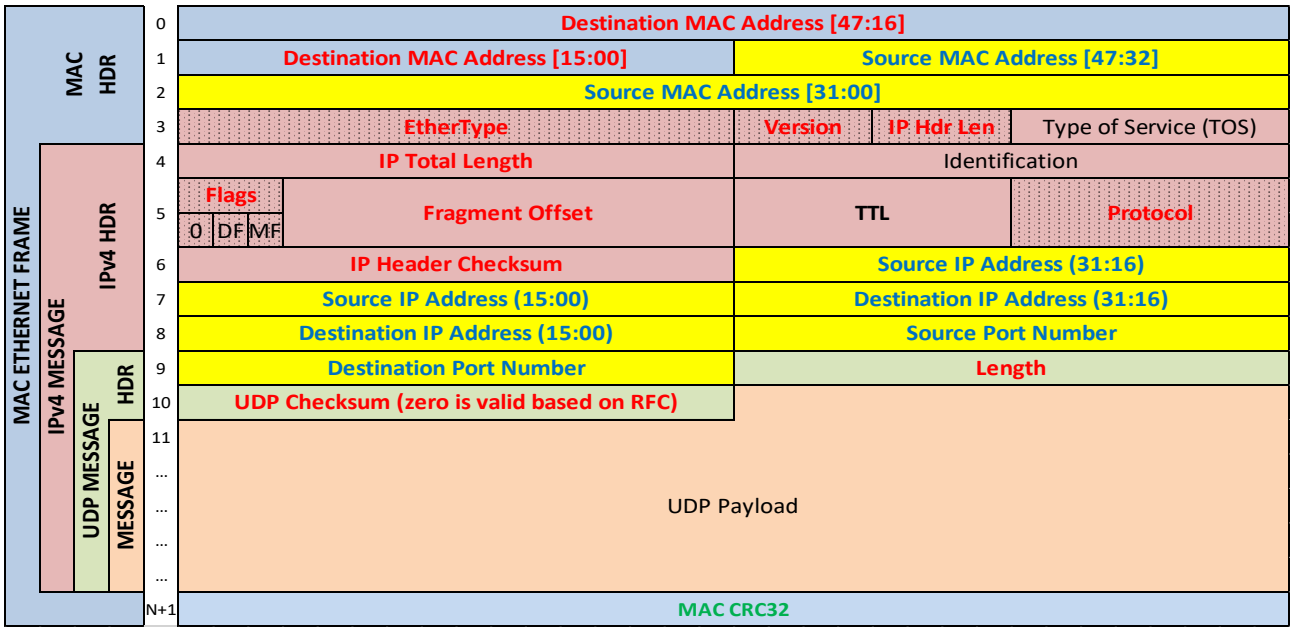


Figure 3 – Standard Ethernet Frame Received by XDE Radium

b. Steps 2 & 3: Each compliant packet's header content is validated against whitelist policy, and non-compliant packets are dropped. Compliant packet headers are transformed into a proprietary Owl Diode Frame before delivery to the hardware isolator. No MAC, IPv4, and UDP Header content is allowed to remain in the header; each packet's routing information is eliminated in the Owl Diode Frame, making each packet non-routable by virtue of a full protocol break. Owl FPGA Policy will allow certain header fields to pass as metadata, and the policy is implemented in HDL code. Figure 4 shows the transformed Owl frame with metadata that is delivered as a proprietary protocol to the hardware isolator.

[1] Compliance with NIST 800-53r5 is not validated as part of the EAL 4+ certification.

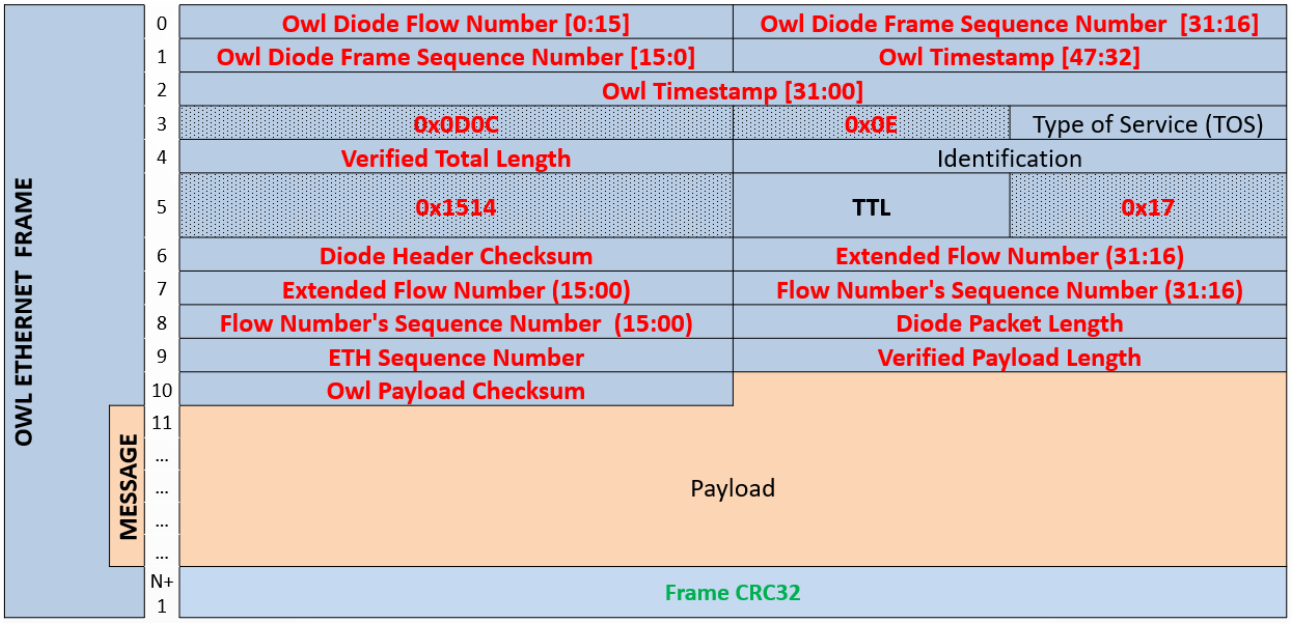


Figure 4 – Owl Proprietary Frame delivered to the Hardware Isolator

c. Step 4: HW Isolator Enforced Security; the Source side hardware isolator circuit is a transmit-only circuit. The Destination side has no transmit circuit; it is a receive-only circuit. Data can only flow from Source to Destination sides of the module.

d. Step 5: Owl FPGA filter policy performs a CRC32 and UDP payload checksum verification in the Destination side FPGA.

e. Step 6: A Flow ID lookup is performed to identify the new routing parameters. (Three verifications: parity, checksum, and CRC32).

f. Step 7: The Destination FPGA completes header regeneration that includes pre-defined routing information and performs a UDP checksum before delivering packets to their intended network destination.

1.7 TOE Physical Architecture

The Owl Cyber Defense Solutions, LLC (Owl) XDE Radium V1.3 product provides an absolute one-way connection between a Source domain – the sending host system or network, and a Destination domain - a receiving host system or network. Information is permitted to flow from the sending host system or network to the receiving host system or network. Data, information, or communications originating at the receiving host system or network are not allowed to flow to the sending host system or network through the XDE Radium.

The Target of Evaluation (TOE) is an embeddable module that comes in two versions (optical isolator or digital isolator) designed and manufactured to Owl's specifications using standard network components which are available as commercial-off-the-shelf (COTS) components.

As mentioned in Section 1.6, XDE Radium's components and overall physical architecture, along with proprietary FPGA firmware, support NIST 800-53r5 Information Flow Enforcement controls AC-4 (7) and (8). XDE Radium's primary architectural feature is isolated Source and Destination PCB regions that are only bridged by a hardware isolator. Major board components of the Optical Isolator version include an optical

transmitter/receiver pair with fiber optic cable, RJ45 connectors, and FPGAs. Major board components of the Digital Isolator version include an digital isolator, RJ45 connectors, and FPGAs. Figures 5-7 are product images with the major components identified. Note that there is a "no-trace" zone providing physical separation of the Source and Destination sides bridged only by the hardware isolators.

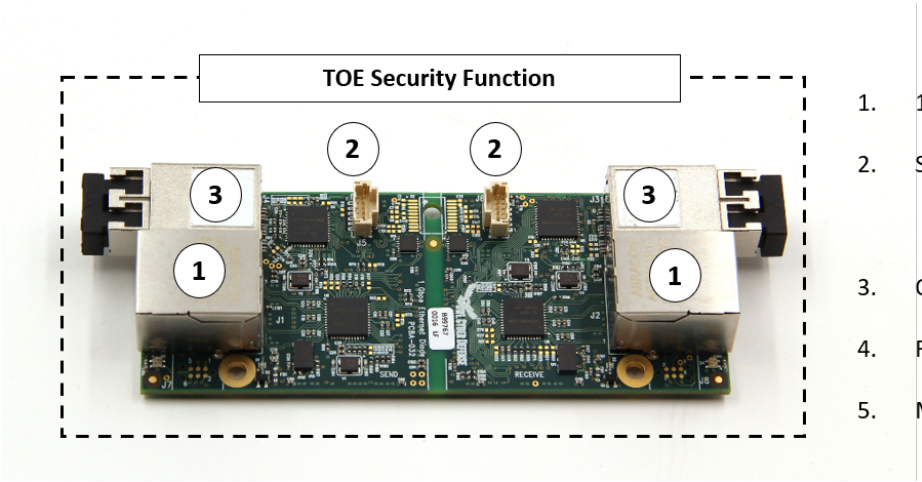


Figure 5 - XDE Radium Optical Model Top-Down View with Major Components Identified

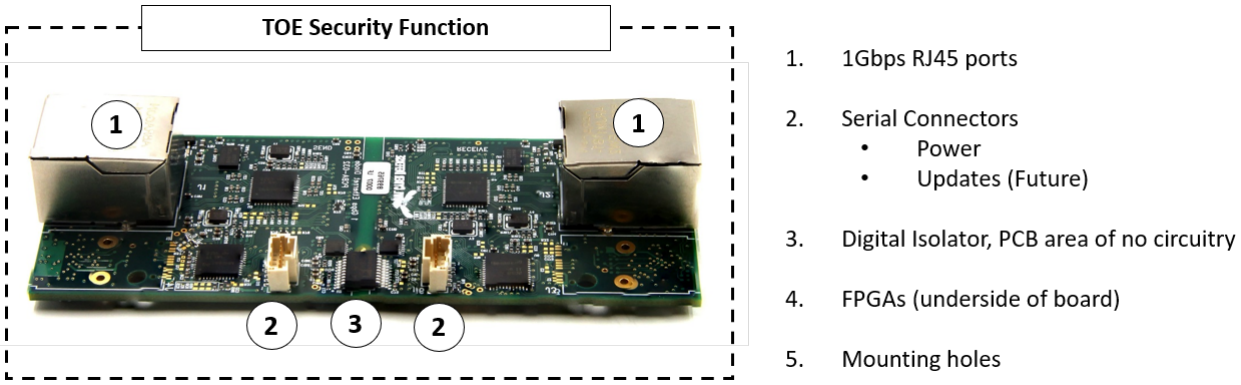


Figure 6 – XDE Radium Digital Model Top-Down View with Major Components Identified

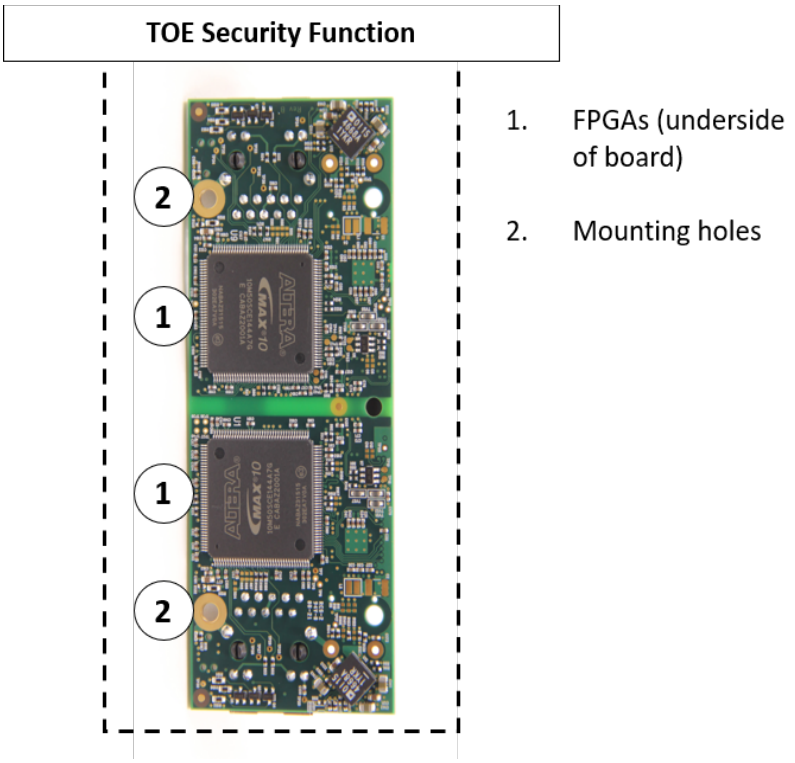


Figure 7 - XDE Radium Bottom View with Major Components Identified (Components and Lay-Out Common Between Optical & Digital Models)

The following text explains how XDE Radium's overall physical architecture contributes to one-way data flow:

1) Bi-directional, inter-component communication is permitted for proper functioning. The inter-component communication does not extend from Source to Destination side. Board traces ensure inter-component communications do not reach the Hardware Isolator and never crosses the Source/Destination boundary, as shown in Figure 8.

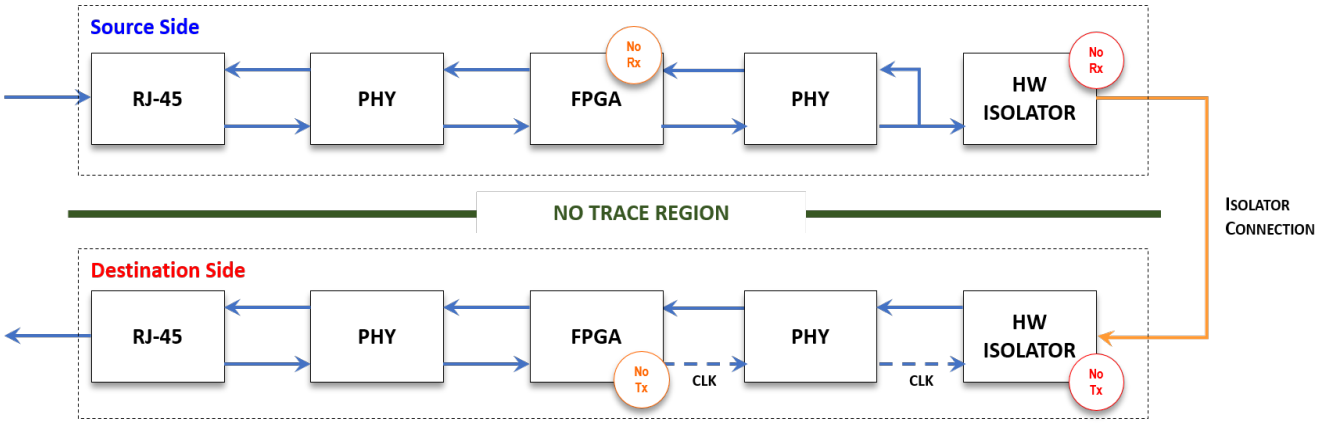


Figure 8 – Architectural Block Diagram Showing Inter-Component Communication and One-Way Flow Control from Source to Destination

2) The TOE has separate power circuitry on the Source and Destination sides. Power is supplied to the Source and Destination side via the host device to separate connectors attached to each side's serial connectors. Power loss to either side of XDE Radium results in a complete loss of functionality.

1.7.1 Physical Boundaries

The TOE's physical boundaries are defined by the circuit board's substrate and various components in both the Optical and Digital Isolation variants. The board's overall dimensions are 4" (L) x 1.5" (W) x 5/8" (H) in both versions. Power is delivered to the Source and Destination sides of the circuit board via separate power connectors – each of which plugs into separate UART connectors on the circuit board (shown in Fig. 6 above). The only network data connections during normal operations are the two RJ-45 ports. The serial UARTS do not have a network connection during normal operations.

1.7.2 Logical

This section will summarize the TOE Security Functions provided by the Owl XDE Radium module.

1.7.2.1 User data protection

The Owl XDE Radium module passes data from the Send-Only side to the Receive-Only side and provides the following security features:

Information Flow Control – The TOE directly interfaces with the source host and the destination host to transmit information in a unidirectional flow through a hardware isolator (optical or digital). The module's Send-Only side of the TOE is only capable of transmitting information and conversely the module's Receive-Only side is only capable of receiving information.

Residual Information – The TOE stores no user data in the board's data handling components. Intentional or unplanned power loss to the Source side will result in immediate dropping of all buffered user data, leaving no residual user information on the board. Intentional or unplanned power loss to the Destination side will likewise result in immediate dropping of all buffered user data, leaving no residual user information on the board. Simultaneous loss of power to both sides results in complete loss of any residual data, and prevents the TOE from passing and user data from Source to Destination networks.

1.7.2.2 Protection of the TSF

The design features provided below have been incorporated in the Owl XDE Radium module to ensure the integrity, reliability, and security of the TOE.

Fail Secure –XDE Radium's components and overall physical board architecture enforces one-way data flow from Source to Destination. Any major component failure in the TOE will stop data flow entirely, thus preventing unintended information flow from bypassing the TSF.

1.8 TOE Software

The TOE has no Central Processor Unit (CPU), and thus no Operating System (OS). The TOE does not require flanking or proxy servers to host software required to execute its core functions. The TOE relies on two firmware/software packages to function.

The operational firmware/software, loaded into the two FPGAs, will include a System Configuration file, a Flow file, and Policy file, and a System file. The four files will be consolidated into two download files stored on the TOE, as shown in Figure 9. The files are explained below.

a) The System file contains system configuration parameters for the customer network and will provide all configuration parameters to define the system options.

b) The Flow File defines all the mission data flows and is configured by the customer. On the source side the table defines all the permitted UDP ports and any additional validation parameters for that flow. On the destination side the Flow File will define the header fields that will be replaced.

c) The Owl Policy files will define how the mission data header is validated, identifies the fields that are cleared before passing over the diode, populates the header with metadata, and transforms the resultant packet into a proprietary Owl frame. On the destination side this policy file defines the fields that will be used to update the header or if the field is a pass through. The default values will be defined for fields that are to be updated.

d) The Owl System configuration parameters are specific to a setup that will not be changed. Examples of this will be Radium's MAC Addresses and encryption keys.

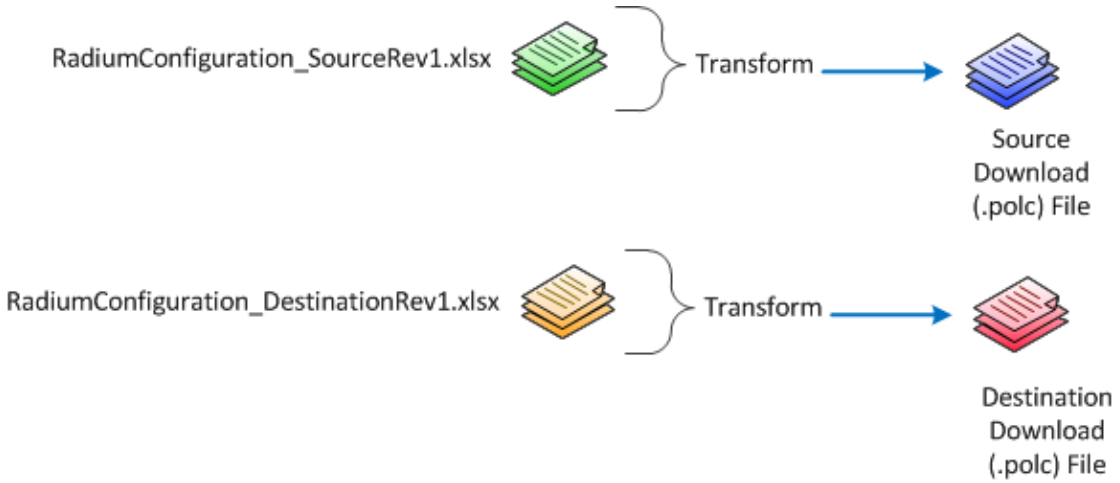


Figure 9 – XDE Radium Operational Files

Both the Source side and the Destination side FPGAs will require downloaded configuration information, as shown in Figure 10. Utilities will be provided to support an interface for configuring the field updated

parameters. This includes the System Configuration and the Flow File information. Owl Production will have a special utility that allows configuration of the Owl System Configuration and the Policy files in addition to the System Configuration and the Flow File.

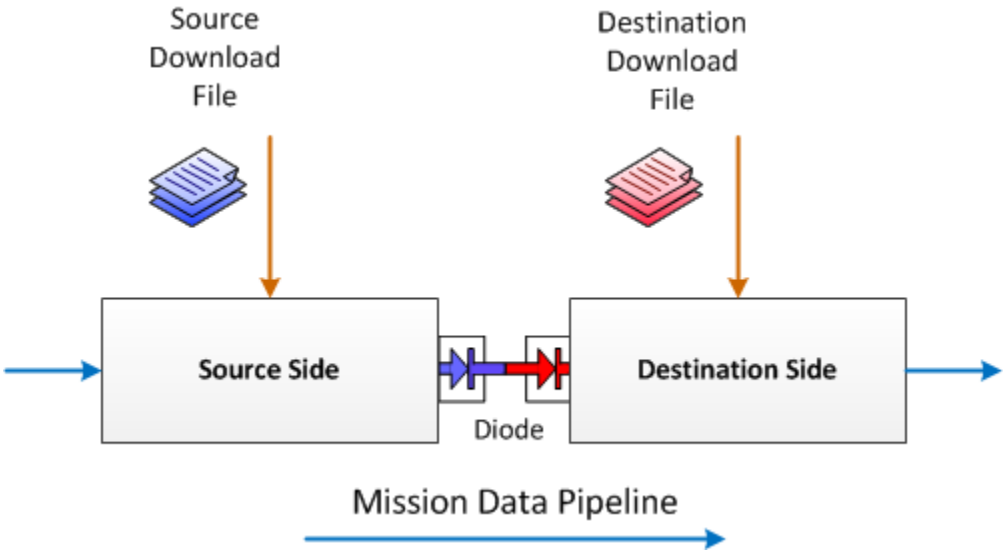


Figure 10 – XDE Radium Operational Files Loaded on Both Source and Destination Sides

1.9 TOE Documentation

XDE Radium shall have a User Guide. The User Guide provides a brief overview of XDE Radium and will describe procedures for unboxing, powering, and testing the unit. In addition, the User Guide will describe the procedure for writing new configurations, will explain how to load configuration updates using the Configuration Utility, and will list failure conditions and the recovery process.

XDE Radium shall also have a Production-related guides that describe product programming and testing that precedes customer delivery.

1.10 Product Delivery

It is envisioned that up to 10 TOE XDE Radium modules will be packed into a single product box. More than one product box may be packed into a product carton for shipment.

Each TOE will have a unique serial number attached to the board itself. There will be a bill of lading inside or attached to each product box listing the TOEs and their associated serial numbers. Customers will be able to compare the Invoice, Bill of Lading, and TOE serial numbers to validate the authenticity of the delivered Owl products. Product boxes will be sealed with tape in a manner that will make obvious any post-shipment attempt at tampering, product modification, or substitution. The secure packaging is done to give customers confidence that they are receiving unaltered, certified Owl products.

Owl works with trusted carriers to ensure accurate tracking and delivery of product boxes/cartons to customers' delivery destination. Standard carriers like FedEx will forward tracking information and delivery notifications to the customer including an ETA and the last known location of the TOE or solution that was sent. If another carrier is used, Owl will confirm with the customer point of contact a shipment's ETA. These methods are employed by Owl to limit the opportunity an untrustworthy individual could modify or substitute the TOE or solution. This would virtually guarantee the TOE or solution received by the customer came directly from Owl and has not been tainted or altered.

TOE documentation will be delivered to customer separately from the physical products via secure electronic means. Firmware or software updates to deployed systems will be signed and accompanied by a valid X.509 certificate to ensure the firmware/software provenance. All updates will be delivered via secure electronic means.

2 Conformance Claims (ASE_CCL.1)

2.1 Common Criteria Conformance Claim

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, Version 3.1, Revision 5, CCMB-2017-04-002.
    - Part 2 Conformant
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1, Revision 5, CCMB-2017-04-003.
    - Part 3 Conformant
    - Assurance Level: EAL4 augmented by AVA_VAN.4

2.1.1 Protection Profile Conformance Claim

This ST does not claim conformance to any identified Protection Profile.

2.1.2 Package Claims

The ST is conformant with Security Assurance Requirement:

- EAL4 conformant and is augmented by AVA_VAN.4.

3 Security Problem Definition (ASE_SPD.1)

There are two common (envisioned) security problems the TOE is designed to address.

- The first security problem XDE Radium protects against is threats originating in the Destination network. This XDE Radium security feature protects the Host Device and the Source network.
- The second security problem XDE Radium protects against is malicious code embedded in packet headers. The XDE Radium security feature protects Destination network from malicious content embedded in packet headers.

3.1 Organizational Security Policies

P.ONEWAY	Information from the source host must only flow one-way to the attached destination host.

3.2 Threats

T.FAILURE	The TOE has a hardware failure that allows access to confidential or proprietary information on the source side through the TOE.
T.TAMPER	An attacker tampers with the TOE to in order to bypass the unidirectional interface of the TOE or otherwise compromise or influence the behavior of the TOE.
T.WRONGWAY	An attacker or process, e.g. “Trojan Horse”, deliberately or accidentally transfers information from the source host or network back through the TOE to the originating source host or network.

3.3 Assumptions

A.ADMIN	Authorized personnel that are used to install, administer and use the TOE are trustworthy, competent and follow the guidance regarding the usage of the TOE.
A.CONNECTION	The TOE must be installed so all relevant network traffic will only flow through the TOE and hence be subject to the organizational security policy.
A.EMISSION	The TOE must be installed and operated in an environment where physical or other security measures prevent any Emissions Security attacks or Telecommunications Electronics Material Protected from Emanating Spurious Transmissions attacks.
A.GUIDE	Authorized personnel shall ensure that the TOE has been delivered, installed and is administered in accordance with security guidance, in a manner that maintains security. The appropriate security authority shall accredit the installation of the TOE before taking it into operation.
A.NETBREAK	The operational environment of the TOE shall ensure that information cannot flow between the source network and destination network without going through the TOE. This prevents a threat agent from circumventing the security provided by the TOE.
A.PHYSICAL	The TOE must be operated in a protected environment prevents unauthorized physical access to the TOE.

4 Security Objectives (ASE_OBJ.2)

The security objectives for the TOE are designed to address the policy and threat associated with the direction of flow of information between attached host computing systems. The security objectives for the TOE environment are designed to address assumptions about the physical application or use of the TOE.

4.1 Security Objectives for the TOE

O.FAILSAFE	In case of hardware malfunction the TOE must always maintain a secure state and prevent illicit information flow.
O.NON_ROUTABLE	Information packets that flow from Source side to Destination Side through the TOE’s hardware isolator are void of any standard protocols that would make the information packets routable on the Internet.

O.READ_ONLY	Interfaces of the TOE designated as receive-only can only receive and not send any information.
O.WRITE_ONLY	Interfaces of the TOE designated as send-only can only send and not receive any information.

4.2 Security Objectives for the TOE Environment

OE.ADMIN	Authorized personnel that are used to install, administer and use the TOE are trustworthy, competent and follow the guidance.
OE.CONNECTION	The TOE must be installed such that all relevant network traffic will only flow through the TOE and hence be subject to itself information flow policy.
OE.EMISSION	The TOE is installed and operated in an environment where physical or other security measures prevent any Emissions Security attacks or Telecommunications Electronics Material Protected from Emanating Spurious Transmissions attacks.
OE.GUIDE	The authorized personnel shall ensure the TOE has been delivered, installed and is administered in accordance with guidance. The appropriate security authority shall accredit the installation of the TOE before placing it into operation.
OE.NETBREAK	The operational environment of the TOE shall ensure that information cannot flow between the source network and destination network without going through the TOE. This prevents a threat agent from circumventing the security provided by the TOE.
OE.PHYSICAL	The TOE must be operated in a protected environment that prevents unauthorized physical access to the TOE.

4.3 Security Objectives Rationale

This section shows that all secure usage assumptions, organizational security policies, and threats are completely covered by security objectives. In addition, each objective counters or addresses at least one assumption, organizational security policy, or threat.

4.3.1 Security Objectives Rationale for the TOE and Environment

This section provides evidence by mapping security objectives to the threats, organizational security policies and assumptions described in the Security Problem Definition chapter. All security objectives address or counter at least one threat, organizational security policy or sustains one assumption.

	P.ONEWAY	T.FAILURE	T.TAMPER	T.WRONGWAY	A.ADMIN	A.CONNECTION	A.EMISSION	A.GUIDE	A.NETBREAK	A.PHYSICAL
O.READ_ONLY	X			X						
O.WRITE_ONLY	X			X						
O.NON_ROUTABLE	X									
O.FAILSAFE		X								
OE.ADMIN			X		X					
OE.CONNECTION						X				
OE.EMISSION							X			
OE.GUIDE								X		
OE.NETBREAK	X								X	
OE.PHYSICAL			X							X

Table 5 Environment to Objective Correspondence

4.3.1.1 P.ONEWAY

Information from the source host must only flow one-way to the attached destination host.

This Organizational Policy is satisfied by ensuring that:

- O.READ_ONLY: Interfaces of the TOE designated as receive-only can only receive and not send any information.
- O.WRITE_ONLY: Interfaces of the TOE designated as send-only can only send and not receive any information.
- O.NON_ROUTEABLE: Information packets that flow from Source side to Destination Side through the TOE's hardware isolator are void of any standard protocols that would make the information packets routable on the Internet.
- OE.NETBREAK: The operational environment of the TOE shall ensure that information cannot flow between the source network and destination network without going through the TOE. This prevents a threat agent from circumventing the security provided by the TOE.

4.3.1.2 T.FAILURE

The TOE has a hardware failure that allows access to confidential information on the destination side through the TOE.

This Threat is satisfied by ensuring that:

- O.FAILSAFE: In case of hardware malfunction the TOE must always maintain a secure state and prevent illicit information flow.

4.3.1.3 T.TAMPER

An attacker tampers with the TOE in order to bypass the unidirectional interface of the TOE or otherwise compromise or influence the operations of the TOE.

This Threat is satisfied by ensuring that:

- OE.ADMIN: Authorized personnel that are used to install, administer and use the TOE are trustworthy, competent and follow the guidance.
- OE.PHYSICAL: The TOE must be operated in a protected environment that prevents unauthorized physical access to the TOE.

4.3.1.4 T.WRONGWAY

An attacker or process, e.g. "Trojan Horse", deliberately or accidentally transfers information from the destination host or network back through the TOE to the originating source host or network.

This Threat is satisfied by ensuring that:

- O.READ_ONLY: Interfaces of the TOE designated as receive-only can only receive and not send any information.
- O.WRITE_ONLY: Interfaces of the TOE designated as send-only can only send and not receive any information.

4.3.1.5 A.ADMIN

Authorized personnel that are used to install, administer and use the TOE are trustworthy, competent and follows the guidance.

This Assumption is satisfied by ensuring that:

- OE.ADMIN: Authorized personnel that are used to install, administer and use the TOE are trustworthy, competent and follow the guidance.

4.3.1.6 A.CONNECTION

The TOE must be installed so all relevant network traffic will only flow through the TOE and hence be subject to the organizational security policy.

This Assumption is satisfied by ensuring that:

- OE.CONNECTION: The TOE must be installed such that all relevant network traffic will only flow through the TOE and hence be subject to itself information flow policy.

4.3.1.7 A.EMISSION

The TOE must be installed and operated in an environment where physical or other security measures prevent any Emissions Security attacks or Telecommunications Electronics Material Protected from Emanating Spurious Transmissions attacks.

This Assumption is satisfied by ensuring that:

- OE.EMISSION: The TOE is installed and operated in an environment where physical or other security measures prevent any Emissions Security attacks or Telecommunications Electronics Material Protected from Emanating Spurious Transmissions attacks.

4.3.1.8 A.GUIDE

Authorized personnel shall ensure that the TOE has been delivered, installed and is administered in accordance with security guidance, in a manner that maintains security. The appropriate security authority shall accredit the installation of the TOE before taking it into operation.

This Assumption is satisfied by ensuring that:

- OE.GUIDE: The authorized personnel shall ensure the TOE has been delivered, installed and is administered in accordance of guidance. The appropriate security authority shall accredit the installation of the TOE before taking it into operation.

4.3.1.9 A.NETBREAK

The operational environment of the TOE shall ensure that information cannot flow between the source network and destination network without going through the TOE. This prevents a threat agent from circumventing the security being provided by the TOE through an untrustworthy product.

This Assumption is satisfied by ensuring that:

- OE.NETBREAK: The operational environment of the TOE shall ensure that information cannot flow between the source network and destination network without going through the TOE. This prevents a threat agent from circumventing the security provided by the TOE.

4.3.1.10 A.PHYSICAL

The TOE must be operated in a protected environment prevents unauthorized physical access to the TOE.

This Assumption is satisfied by ensuring that:

- OE.PHYSICAL: The TOE must be operated in a protected environment that prevents unauthorized physical access to the TOE.

5 Security Requirements (ASE_REQ.2)

The security requirements for the TOE include both security functional requirements (SFRs) and security assurance requirements (SARs), as defined in detail below. Note that there are no permutations or probabilistic security functional requirements and as a result there is no applicable strength of function claim.

5.1 TOE Security Functional Requirements

The following table describes the SFRs that are satisfied by the XDE Radium.

Requirement Class	Requirement Component	Dependencies
FDP: User data protection	FDP_IFC.2: Complete information flow control	FDP_IFF.1
	FDP_IFF.1: Simple security attributes	FDP_IFC.1, FMT_MSA.3
	FDP_IFF.5: No Illicit Information Flows	FDP_IFC.1
FPT: Protection of the TSF	FPT_FLS.1: Failure with Preservation of Secure State	No Dependencies

Table 6 TOE Security Functional Components

5.1.1 User data protection (FDP)

5.1.1.1 Complete information flow control (FDP_IFC.2)

FDP_IFC.2.1 The TSF shall enforce the **[unidirectional information flow SFP]** on **[any request from an external interface to move UDP data packets through the TOE]** and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

5.1.1.2 Simple security attributes (FDP_IFF.1)

FDP_IFF.1.1 The TSF shall enforce the **[unidirectional information flow SFP]** based on the following types of subject and information security attributes: **[physical configuration of each XDE Radium module]**.

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled source system and a controlled destination system via a controlled one-way operation if the following rules hold: **[**

a) **If the physical connection from the source network is connected to the source side of the XDE Radium module, then data will be passed through the TOE to the destination side of the module.**

b) **If the physical connection from destination side of the XDE Radium is connected to a destination network, then data will pass through the TOE to the destination network**.

FDP_IFF.1.3 The TSF shall enforce the **[no additional information flow control SFP rules]**.

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: **[source to destination]**.

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: **[destination to source]**.

5.1.1.3 No Illicit information flows (FDP_IFF.5)

FDP_IFF.5.1 The TSF shall ensure that no illicit information flows exist to circumvent **[the unidirectional information flow SFP]**.

5.1.1.4 Fail Secure (FPT_FLS.1)

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: **[a single module's hardware component failure i.e.**

a) A failure of the TOE's power component will prevent the TOE from initializing, powering up and executing operations,

c) A failure of the TOE's TSF isolator component (optical or digital) will prevent the TOE's FPGA component from being able to correctly transmit and communicate through the TOE and thereby discard any transmission.

5.2 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL4 conformant components and augmented with AVA_VAN.4 as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components. These requirements are listed in the following table:

Assurance Class	ID	Assurance Components	Dependencies
ADV: Development	ADV_ARC.1	Security architecture description	ADV_FSP.1, ADV_TDS.1
	ADV_FSP.4	Complete functional specification	ADV_TDS.1
	ADV_IMP.1	Implementation representation of the TSF	ADV_TDS.3, ALC_TAT.1
	ADV_TDS.3	Basic modular design	ADV_FSP.4
AGD: Guidance documents	AGD_OPE.1	Operational user guidance	ADV_FSP.1
	AGD_PRE.1	Preparative procedures	No dependencies
ALC: Life-cycle support	ALC_CMC.4	Production support, acceptance procedures and automation	ALC_CMS.1, ALC_DVS.1, ALC_LCD.1
	ALC_CMS.4	Problem tracking CM coverage	No dependencies
	ALC_DEL.1	Delivery procedures	No dependencies
	ALC_DVS.1	Identification of security measures	No dependencies
	ALC_LCD.1	Developer defined life-cycle model	No dependencies
	ALC_TAT.1	Well-defined development tools	ADV_IMP.1
ASE: Security Target Evaluation	ASE_CCL.1	Conformance claims	ASE_INT.1, ASE_ECD.1, ASE_REQ.1
	ASE_ECD.1	Extended components definition	No dependencies
	ASE_INT.1	ST introduction	No dependencies
	ASE_OBJ.2	Security objectives	ASE_SPD.1
	ASE_REQ.2	Derived security requirements	ASE_OBJ.2, ASE_ECD.1
	ASE_SPD.1	Security problem definition	No dependencies
	ASE_TSS.1	TOE summary specification	ASE_INT.1, ASE_REQ.1, ADV_FSP.1

ATE: Tests	ATE_COV.2	Analysis of coverage	ADV_FSP.2, ATE_FUN.1
	ATE_DPT.1	Testing: basic design	ADV_ARC.1, ADV_TDS.2, ATE_FUN.1
	ATE_FUN.1	Functional testing	ATE_COV.1
	ATE_IND.2	Independent testing – sample	ADV_FSP.2, AGD_OPE.1, AGD_PRE.1, ATE_COV.1, ATE_FUN.1
AVA: Vulnerability assessment	AVA_VAN. 4	Methodical vulnerability analysis	ADV_ARC.1, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1

Table 7 EAL4+ Assurance Components

5.3 Security Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the components (requirements) in the Security Target. Note that **Table 8** indicates the requirements that effectively satisfy the individual objectives.

5.3.1 Security Functional Requirements Rationale

All Security Functional Requirements (SFR) identified in this Security Target is fully addressed in this section and each SFR is mapped to the objective for which it is intended to satisfy.

Objectives **SFRs**	**O.FAILSAFE**	**O.NON_ROUTABLE**	**O.READ_ONLY**	**O.WRITE_ONLY**
FDP_IFC.2: Complete information flow control			X	X
FDP_IFF.1: Simple security attributes			X	X
FDP_IFF.5: No Illicit Information Flows		X	X	X
FPT_FLS.1: Failure with Preservation of Secure State	X		X	X

Table 8 Objective to Requirement Correspondence

5.3.1.1 O.NON_ROUTABLE

All routable header information is eliminated by the Source FPGA before passing the Owl Frame across the hardware isolator to the Destination FPGA.

This TOE Security Objective is satisfied by ensuring that:

- FDP_IFF.5: The TSF shall ensure that no illicit information flows exist to circumvent the elimination of routable information in packet headers.

5.3.1.2 O.READ_ONLY

Interfaces of the TOE designated as receive-only can only receive and not send any information.

This TOE Security Objective is satisfied by ensuring that:

- FDP_IFC.2: The TSF must enforce a unidirectional information flow SFP on all requests to move data packets through the TOE.
- FDP_IFF.1: The TSF must ensure that receive-only interfaces can only receive and not send data and send-only interfaces can send and not receive data.
- FDP_IFF.5: Only a single exterior interface through the TSF shall exist to allow the unidirectional flow of information by means of an optical or digital isolator and FPGA firmware through the TOE.
- FPT_FLS.1: In the event of any single component failure the TOE will preserve a secure state and the SF. Though the TOE may not be operational it will remain secure.

5.3.1.3 O.WRITE_ONLY

Interfaces of the TOE designated as send-only can only send and not receive any information.

This TOE Security Objective is satisfied by ensuring that:

- FDP_IFC.2: The TSF must enforce a unidirectional information flow SFP on all requests to move data packets through the TOE.
- FDP_IFF.1: The TSF must ensure that receive-only interfaces can only receive and not send data and send-only interfaces can send and not receive data.
- FDP_IFF.5: Only a single exterior interface through the TSF shall exist to allow the unidirectional flow of information by means of an optical or digital isolator and FPGA firmware through the TOE.
- FPT_FLS.1: In the event of any single component failure the TOE will preserve a secure state and the SF Though the TOE may not be operational it will remain secure.

5.3.2 Security Requirements Rationale

This ST contains the assurance requirements from the CC EAL4+ assurance package and is based on good commercial development practices. This ST has been developed for a generalized environment with a low to medium level of risk to the applicable assets, although given the relatively simple and entirely physical nature of the TOE it is resistant to essentially any logical attacks potential.

5.4 Requirement Dependency Rationale

The following table shows that all dependencies, except FMT_MSA.3, are satisfied within this Security Target. As indicated in the table below, FMT_MSA.3 is not applicable to the TOE because the information flow policy is pre-determined and is unchangeable, i.e. there is no means to change the information flow policy in the evaluated configuration.

ST Requirement	CC Dependencies	ST Dependencies
FDP_IFC.2	FDP_IFF.1 Simple security attributes	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialization	FDP_IFC.2; FMT_MSA.3 and its dependencies have been excluded from this Security Target because the information flow security policy is pre-defined and static, i.e. there is no means to change the information flow policy in the evaluated configuration

ST Requirement	CC Dependencies	ST Dependencies
FDP_IFF.5	FDP_IFC.1 Subset information flow control	FDP_IFC.2

Table 9 Security Requirement Dependency Analysis

5.5 Extended Component Definition (ASE_ECD.1)

There are no extended component definition requirements in this Security Target.

6 TOE Summary Specification (ASE_TSS.1)

This chapter describes the security functions and associated assurance measures.

Security Target for XDE Radium V1.3 modules addresses the following security attributes:
(1) one-way information flow security policy
(2) non-bypassability (all data flows through optical or digital isolator with one-way enforcement at each end)
(3) non-routable protocol break (derived from proprietary FPGA firmware implemented in hardware)
(4) total IP network isolation (due to protocol break described above; testable at the interfaces of Send and Receive FPGAs)
(5) satisfies National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 security control AC-4, Paragraph 7, "hardware-enforced one-way information flow control".

6.1 TOE Security Functions

The TOE provides the following security functions:

- User Data Protection
- Protection of the TSF

6.1.1 User data protection

The unidirectional information flow control of each XDE Radium V1.3module is complete and unconditional. The XDE Radium V1.3module enforces unidirectional flow control on any request from an external interface to move data packets through the module and all operations that cause that information to flow through the module.

The XDE Radium V1.3module enforces the unidirectional information flow based on its physical attributes at the component level. The XDE Radium V1.3 module permits information flow between a known Source and a known Destination according to rules defined by the physical design of the module's overall architecture, enforced by the optical or digital isolator and associated Source and Destination FPGA firmware.

Each Owl XDE Radium V1.3module physically can only provide network traffic flow in one direction through the device. The XDE Radium V1.3 module allows only the one-way transfer of information from a Source system through the module to an external Destination system, and there is no transfer of information from a Destination system through the XDE Radium V1.3 module's optical or digital isolator back into the Source system because such transfer is physically impossible.

The User data protection function is designed to satisfy the following security functional requirements:

- FDP_IFC.2: The TOE is composed of a Source-side FPGA connected via optical or digital isolator to a Destination-side FPGA. The Source-side FPGA interfaces directly with the source host to deliver data one-way through the isolator. No external electronic or light signals are admitted back through the optical or digital isolator and Source-side FPGA to the source host. Conversely, the Destination-FPGA directly interfaces with the destination host and only receives information through an optical or digital isolator. The Destination-side FPGA is not able to affect data transmission across the isolator to the Source-side FPGA. This ensures all send and receive information flows through the TOE and are subject to the unidirectional SFP.

- FDP_IFF.1: By design, the XDE Radium module enforces one-way data flow originating in a source system to a destination system through an optical or digital isolator and FPGA firmware. All information originating in the source network is delivered to XDE Radium's Source-side FPGA where packets are evaluated against a whitelist, compliant packets headers are deconstructed, and packets are passed across an optical or digital isolator to the Destination-side FPGA. This physical process enforces unconditional unidirectional information flow. No information can flow from outside the Send-Only network into the host system except through XDE Radium's verifiably enforced one-way transfer. Conversely, no information is able to flow from the Destination-side system through the XDE Radium V1.3module to the Source-side host. This non-bypassability of the TOE ensures the SFP is enforced at the physical level.
- FDP_IFF.5: The TOE has only two external network interfaces. The design of the TOE strictly maintains a unidirectional path of the information from the source host to the destination host, thereby ensuring that at all times there are no covert channels or unintended signaling channels through the TOE. The unidirectional information policy between domains uses proprietary FPGA firmware that enforces a protocol break on every packet transiting from Source to Destination sides of the module via the optical or digital isolator. The protocol break itself occurs when the module's Source-side FPGA deconstructs the packer header and eliminates all routable information before passing the proprietary Owl frame with metadata data across the isolator to the Destination FPGA. Therefore, the SFP of the TOE maintains the confidentiality of the destination domain and prevents any illicit flow of information to the source domain.

6.1.2 Protection of the TSF

The XDE Radium V1.3module has been designed, developed and implemented so a component or hardware failure of any kind will not change the unidirectional flow, therefore the SFP will not be violated. This is achieved by designing each FPGA of the TOE as a single purpose component; Source-only FPGA or Destination-only FPGA. A hardware failure will not be able to convert the functionality of the unidirectional flow of either component. If a failure occurs the functionality of the unidirectional flow will cease and the security of the source and destination domains shall be preserved.

- FPT_FLS.1: If a hardware failure occurs this would prevent data flow between domains thereby preserving the confidentiality and integrity of each domain. Even though the TOE may not be operational it will remain secure.

6.2 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all the security functions and assurance requirements. Furthermore, all the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. **Table 10 Security Functions vs. Requirements Mapping** demonstrates the relationship between security requirements and security functions.

	User data protection	**Protection of the TSF**
FDP_IFC.2	X	
FDP_IFF.1	X	
FDP_IFF.5	X	
FPT_FLS.1		X

Table 10 Security Functions vs. Requirements Mapping

7 Revision History

Version	Date	Changes / Reason for changes
01	3/17/2021	Draft document for the XDE Radium V1.3Module
02	5/7/2021	Revisions to the original document
02	11/29/21	Revisions to the original document
02	02/11/22	Revisions to the original document
02	07/05/22	Revisions to the original document

END OF DOCUMENT