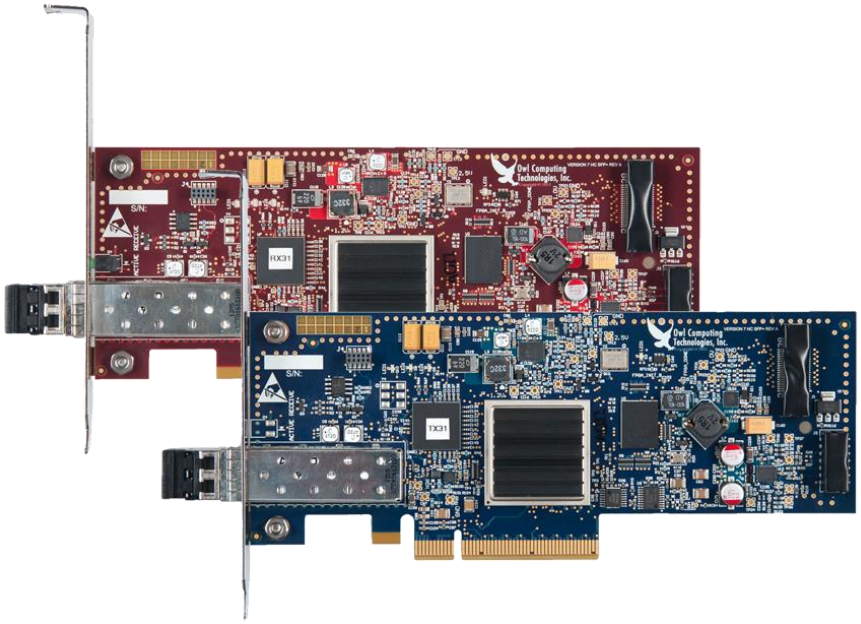
DualDiode Communication Cards 10G, 2.5G, 1.0G v.7 & v.7t Models

Security Target

Common Criteria - EAL4+ Certification



Document: OwlDualDiodeVer-7 Model-SecurityTarget-EAL4_v01l.doc
Version: 01m
Date: June 2019

Prepared By: Randall Colette
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

SECURITY TARGET **1**

COMMON CRITERIA - EAL4+ CERTIFICATION **1**

1 SECURITY TARGET INTRODUCTION (ASE_INT.1) **4**

1.1 SECURITY TARGET REFERENCE 4
1.2 TOE REFERENCE 5
1.3 TOE OVERVIEW 5
1.4 DOCUMENT OVERVIEW 7
1.5 CONVENTIONS, TERMINOLOGY, ACRONYMS 8
1.5.1 CONVENTIONS *8*
1.5.2 TERMINOLOGY, ACRONYMS AND ABBREVIATIONS *8*
1.6 TOE DESCRIPTION 11
1.7 TOE PHYSICAL ARCHITECTURE 12
1.7.1 PHYSICAL BOUNDARIES *13*
1.7.2 LOGICAL BOUNDARIES *15*
1.8 TOE SOFTWARE 15
1.9 TOE DOCUMENTATION 15

2 CONFORMANCE CLAIMS (ASE_CCL.1) **16**

2.1 COMMON CRITERIA CONFORMANCE CLAIM 16
2.1.1 PROTECTION PROFILE CONFORMANCE CLAIM *16*
2.1.2 PACKAGE CLAIMS *16*

3 SECURITY PROBLEM DEFINITION (ASE_SPD.1) **16**

3.1 ORGANIZATIONAL SECURITY POLICIES 16
3.2 THREATS 17
3.3 ASSUMPTIONS 17

4 SECURITY OBJECTIVES (ASE_OBJ.2) **17**

4.1 SECURITY OBJECTIVES FOR THE TOE 17
4.2 SECURITY OBJECTIVES FOR THE TOE ENVIRONMENT 18
4.3 SECURITY OBJECTIVES RATIONALE 18
4.3.1 SECURITY OBJECTIVES RATIONALE FOR THE TOE AND ENVIRONMENT *19*

5 SECURITY REQUIREMENTS (ASE_REQ.2) **21**

5.1 TOE SECURITY FUNCTIONAL REQUIREMENTS 22
5.1.1 USER DATA PROTECTION (FDP) *22*
5.1.2 PROTECTION OF THE TSF (FPT) *22*
5.2 TOE SECURITY ASSURANCE REQUIREMENTS 23
5.3 SECURITY REQUIREMENTS RATIONALE 24
5.3.1 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE *24*
5.3.2 SECURITY REQUIREMENTS RATIONALE *25*
5.4 REQUIREMENT DEPENDENCY RATIONALE 25
5.5 EXTENDED COMPONENT DEFINITION (ASE_ECD.1) 26

6 TOE SUMMARY SPECIFICATION (ASE_TSS.1) **26**

6.1 TOE SECURITY FUNCTIONS 26
6.1.1 USER DATA PROTECTION *26*
6.1.2 PROTECTION OF THE TSF *27*
6.2 TOE SUMMARY SPECIFICATION RATIONALE 28

7 REVISION HISTORY **29**

LIST OF TABLES

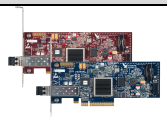
Table 1 ST Identification 4
Table 2 TOE Hardware Products 5
Table 3 TOE Identification 5
Table 4 Acronyms & Abbreviations 10
Table 5 TOE Environmental Requirements 14
Table 6 Environment to Objective Correspondence 19
Table 7 TOE Security Functional Components 22
Table 8 EAL4+ Assurance Components 23
Table 9 Objective to Requirement Correspondence 24
Table 10 Security Requirement Dependency Analysis 25
Table 11 Security Functions vs. Requirements Mapping 28

1 Security Target Introduction (ASE_INT.1)

1.1 Security Target Reference

ST Title	DualDiode Communication Cards 10G, 2.5G, 1.0G v.7 & v.7t Models Security Target
ST Version	01m
ST Publication Date	6/17/19
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 one or more pairs of the following security hardware products.

Table 1 ST Identification

TOE Hardware Products		**Maximum Speed**	**Channels**	**Part Number / PCB Version PCB Number (Card Identity)**
Owl DualDiode **10G v.7** Communication Cards		10 Gbps	32	V7sfp+RO-6-D-C HC SFP+ Rev B PCB-0005 (Receive-Only Card) V7sfp+SO-6-D-C HC SFP+ Rev B PCB-0006 (Send-Only Card)
Owl DualDiode **v.7** Standard-Capacity **2.5G** Communication Cards in Commercial or Industrial Variations		2.5 Gbps	16	V7sc-RO-X-9-C SC Rev C PCB-0003 (Receive-Only Card-Commercial Version) V7sc-SO-X-9-C SC Rev C PCB-0002 (Send-Only Card-Commercial Version) V7sc-RO-X-G-I SC Rev C PCB-0003 (Receive-Only Card-Extended Industrial Temperature) V7sc-SO-X-G-I SC Rev C PCB-0002 (Send-Only Card-Extended Industrial Temperature)
Owl DualDiode **v.7** Standard-Capacity **1.0G** Communication Cards in Commercial or Industrial Variations		1.0 Gbps	8	V7sc-RO-X-E-C SC Rev C PCB-0003 (Receive-Only Card-Commercial Version) V7sc-SO-X-E-C SC Rev C PCB-0002 (Send-Only Card-Commercial Version) V7sc-RO-X-G-I SC Rev C PCB-0003 (Receive-Only Card-Extended Industrial Temperature) V7sc-SO-X-G-I SC Rev C PCB-0002 (Send-Only Card-Extended Industrial Temperature)

Owl DualDiode **v.7t** Commercial and Industrial **1.0G** Communication Cards		1.0 Gbps	8	V7t-RO-X-E-C v7tRev A PCB-0013 (Receive-Only Card-Commercial Version) V7t-SO-X-E-C v7t Rev A PCB-0013 (Send-Only Card-Commercial Version) V7t-RO-X-G-I v7tRev A PCB-0013 (Receive-Only Card-Extended Industrial Temperature) V7t-SO-X-G-I v7tRev A PCB-0013 (Send-Only Card-Extended Industrial Temperature) V7t-RO-X-E-CP v7tRev A PCB-0013 (Receive-Only Card-Commercial Stack Version) V7t-SO-X-E-CP v7tRev A PCB-0013 (Send-Only Card-Commercial Stack Version.)

Table 2 TOE Hardware Products

1.2 TOE Reference

Developer Name	Owl Cyber Defense Solutions, LLC	**Firmware Revision**
TOE Identity	Owl DualDiode 10G v.7 Communication Cards	V39
	Owl DualDiode v.7 Standard-Capacity 2.5G Communication Cards in Commercial Variation	V77
	Owl DualDiode v.7 Standard-Capacity 2.5G Communication Cards in Industrial Variation	V77
	Owl DualDiode v.7 Standard-Capacity 1.0G Communication Cards in Commercial Variation	V77
	Owl DualDiode v.7 Standard-Capacity 1.0G Communication Cards in Industrial Variation	V77
	Owl DualDiode v.7t Commercial 1.0G Communication Cards	V75
	Owl DualDiode v.7t Industrial 1.0G Communication Cards	V75
TOE Version Number	Version 7	

Table 3 TOE Identification

1.3 TOE Overview

The Target of Evaluation (TOE) is the Owl DualDiode Communication Cards (DDCC) which consists of the 10G v.7 DualDiode Communication Card, the v.7 Standard Capacity 2.5G Communication Cards, and the v.7 and v.7t Standard Capacity 1.0G Communication Cards, which are designed and manufactured by Owl Cyber Defense Solutions, LLC (Owl). The only function performed by the Owl DualDiode Communication Cards is to allow information to flow one-way-only. The DDCC provide an absolute one-way unidirectional flow of any data and information between a source domain, the sending host system or network to a destination domain, the receiving host system or network. Thereby protecting the destination host or network from any potential leaks of information or potential network probing attacks.

The 10G DualDiode Communications Card and the v.7 Standard Capacity 2.5G and 1.0G are half high and half length for installation into a variety of server platforms that have PCIe express serial expansion slots. Only high end servers with PCIe gen2 serial buses will be able to utilize the full capabilities of the 10G DualDiode Communications Card. The v.7t DDCC is a standard capacity card that is identical in components and abilities as the v.7 Standard Capacity 1.0G DDCC. The v.7t DDCC is designed to comply with the PC104 form factor and requires a CPU that has the PC104 PCIe connector. The v.7t DDCC form factor is used exclusively in the OPDS-1000 and OCDS-1000, an Owl 1U tamper resistant server platform that uses the TOE for one-way unidirectional flow of data between separate network domains.

The Owl DualDiode Communication Cards are the core to a secure one-way only unidirectional flow of information. Owl has created device drivers that provide the interface between the computer bus and the Owl DDCC which are dependent on 64 bit Operating Systems (OS) such as the Secure RedHat or CentoOS Linux OS. Owl drivers provide the necessary device interrupt routines required for applications to use the DDCC on such OS platforms.

Computers require a device driver program be installed before software applications can successfully communicate to external devices, such as the TOE. Because device drivers allow the computer to communicate to the TOE and are not contained or integrated into the TOE, they are considered outside the boundary and scope of the TOE.

Software applications loaded on the host systems must be customized to operate and send data across the TOE. Owl provides software application products like Secure Network Transfer Systems (SNTS) for transferring all data types through the TOE. For datagram transfer Owl offers the UDP Packet Transfer System (UDPS), for TCP transferring the TCP Packet Transfer System (TPTS), Files and Directory Transfer Service (DFTS), plus operations such as SMTP, OSI PI soft, Syslog, OPC server applications and Owl Performance Management Services (OPMS) are supported software services for use with the TOE.

When using the DDCC, the following are compatible uses of the TOE:

Internet	Information from a low security network source; the internet or news group, may be transferred to a high security destination to enable the gathering of information from around the world. This is achieved by using either a standard file –transfer protocol or browsers on the destination side to access the information.
E-mail	Electronic mail may be copied or transmitted from the source network and received on the destination network. This allows users access to e-mails without compromising the security to the destination network or forcing users to switch between networks.
Streaming Communications	Streaming video or audio telecommunication traffic data from mobile or stationary devices are intercepted and transformed into UDP network packets on the source side and transferred to the destination network to be made available for analysis by agencies like the police, intelligence or the justice department.
System Updates	Updates for the operating system, software or anti-virus software can be copied on the source network and transferred to the destination network for proper distribution.
Database Replication	Replication of database information or directory update data could be sent from a database server from the source network to the destination network to keep clients information up to date on the destination network.
Secure Printing	Information on the source network can be transmitted to a printer located on the destination network.

The most common setup for the TOE is to have information from a low level security source network flow through the TOE to a confidential high level security destination network. This gives users in the high level security network the ability to write and extract information from the low security network while preventing users on the low security network from writing or extracting information from the high security network.

The less common setup for the TOE is to have the information flow from a high security source network through the TOE to a low security destination network. This setup will give users the ability to read information from the high security network but not be able to control or input information to the high security source network. This guarantees the integrity of data received while protecting from back channel tampering and viruses. The following scenario describes such a use of the TOE when the security level of the source and domain are reversed.

Industrial Data	Automated processes and sensor data such as SNMP traps or event records on the high security source network provide the low security destination network real-time information for monitoring critical processes and prohibits users any means of influencing the processes on the high security network.
Public Data	The process of releasing once high security source network information to provide the low security destination network information for dissemination into less classified networks for distribution, review or processing without allowing users any means of locating or retrieving additional information from or about the high security network.
Customer Usage	Owl Data Diodes are typically used by the US Department of Defense, US Intelligence Community, CSE Canada, and allies to transfer data into confidential networks while protecting the confidentiality of data already resident there.

Data Diodes are typically used by commercial industries to export state information from Industrial Control System (ICS) networks for remote monitoring via internet while maintaining the integrity of the ICS network.

DualDiode technology is a core product for Owl, that serves as a "building block" from which more complex products are created.

Requirements for data transfer between isolated networks of different security classification often include numerous, stringent security controls for connectivity screening, source authentication, data filtering, and audit logging. Devices certified and accredited by the US Department of Defense (DoD) to transfer data across network domains while satisfying the full suite of security requirements are called Cross Domain Solutions (CDS). Similar systems used by commercial business entities in Critical Infrastructure market sectors are often referred to as Perimeter Defense Solutions (PDS).

DualDiode communication cards from Owl are routinely installed in Commercial Off The Shelf (COTS) Computer Host Server Platforms (e.g. from Dell, HP, or Oracle) and integrated with a hardened Operating System (e.g. S.E. Linux or Solaris) and data filter software applications (e.g. McAfee VirusScan) to create a CDS capable of satisfying DoD security requirements. Two CDS products from Owl are listed as Validated Products by the Unified Cross Domain Management Office (UCDMO); a US Government policy-making body chartered to prevent waste and duplication of development and testing effort with respect to network security devices.

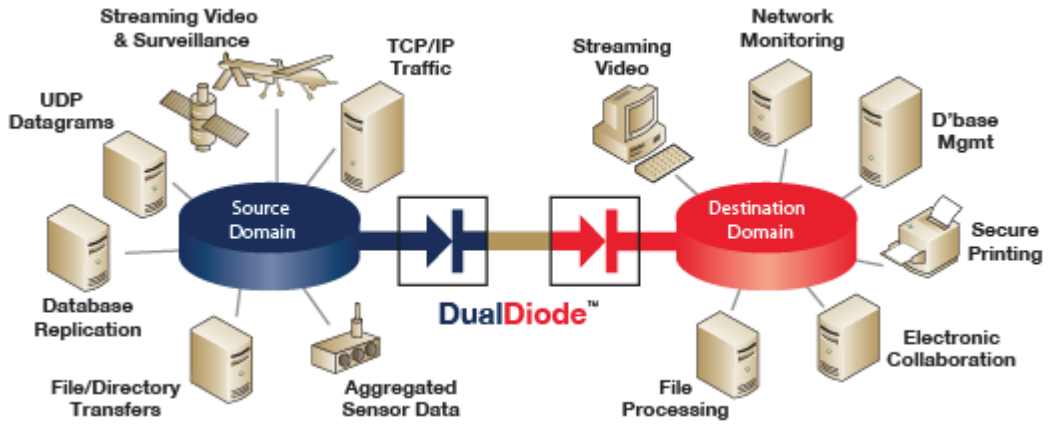


Figure 1 – Owl 10G DualDiode Communication Card Concept

Market Usage
Over 1400 DualDiode systems from Owl have been deployed throughout the US Department of Defense, Intelligence Community, CSE Canada, U.S. Allies and the market continues to grow. Owl increasingly sells DualDiode systems to commercial utility companies in order to protect Critical Infrastructures from cyber attack. While not as numerous as Operating Systems or Firewalls, Data Diodes present unique security features that are valuable for securing networks against a variety of cyber threats.

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
10G v.7 DDCC	Owl DualDiode 10G v.7 Communication Cards or v.7 High Capacity DDCC
CC	Common Criteria for Information Technology Security Evaluation
Destination Domain or Destination	The final destination host system or network to receive the information transmitted through the TOE. Part of the TOE; the Owl Receive-Only DDCC must be integrated into a receiving host system. See Receiving Host.
DualDiode	Deployment of two Data Diode protection mechanisms to enforce one-way transfer security policy at either end of cross-domain connection.
DDCC	**DualDiode Communications Card:** There are two distinct DualDiode Communication Cards, the Send-Only DDCC and the Receive-Only DDCC. The DDCCs are manufactured to Owl's specifications and use commercial-off-the-shelf (COTS) Asynchronous Transfer Mode Communication Card components. The Send-Only V.7 DualDiode Communications Card (DDCC) only has the FPGA imaged as a Segmentation Controller and Framer installed for sending information through the Fiber Optic Transmitter. The V.7 Receive-Only DDCC

	has the FPGA installed and imaged as a Reassembly Controller for only receiving information. The Send-Only DDCC will only export light pulses converted by the Optical Transceiver from electrical voltages. The Receive-Only DDCC will only import light pulses received at the photo detector of the Optical Transceiver and convert the light pulses to electrical voltages.
DualDiode Host	A computer system or network in which a DDCC is installed. The host system or network is the system that provides power to the DDCC. The DDCC is digitally connected to the host via the Peripheral Component Interface (PCIe). See Host.
EAL	Evaluation Assurance Level
FPGA	Field Programmable Gate Array is a COTS semiconductor device containing programmable logic components, interconnects, and memory. When deployed, the FPGA connects directly to the PCIe interface of the host system. 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. Other FPGA application examples include special-purpose embedded processors for digital signal processing, pattern recognition, and parallel supercomputing. FPGAs are often used as prototype platforms for Very-Large-Scale Integration (VLSI) hardware designs. Segmentation and Reassembly software images created by Owl Cyber Defense and executed in the FPGA may be converted to custom VLSI hardware for additional security. A software image operating in an FPGA is functionally equivalent to a custom VLSI chip.
Framer	The Version 7 Send-Only DDCC uses the high level functionality of the FPGA as a Framer to frame each packet with Owl proprietary headers.
Host or Host System	A general term for a computer system that has been allocated for the installation and operation of the Owl DDCC. Once the Owl DDCC hardware is installed in a host it assumes the role of DualDiode host, gateway, receiving host of the destination domain and sending host of the source domain.
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. In Owl Version 7 DDCCs, the JTAG interface is used only once during manufacture of the DDCC to load the onboard Platform Flash with initialization data and is left unconnected thereafter. Use of the JTAG interface requires physical access to the DDCC. The JTAG interface is not exported during use of the DDCC.
Platform Flash	Platform Flash is a Programmable Read-Only Memory (PROM) used to load initialization data used by the Segmentation Controller (in Send-Only DDCC) or by the Reassembly Controller (in Receive-Only DDCC). Platform Flash is written once, in read/write-protection mode, during the DDCC manufacturing process through the JTAG interface. Once written in protected mode, the contents of the PROM cannot be read or rewritten through the JTAG interface. Configuration access to Platform Flash is solely through the JTAG interface, which is not exported. The Platform Flash cannot be configured through either the optical interface or PCIe interface of the DDCC.
PCIe	Peripheral Component Interface Express, officially abbreviated as PCIe (not to be confused with PCI-X, which is PCI Extended), is a computer expansion card interface format. It was designed as a much faster interface to replace PCI, PCI-X, and AGP interfaces for computer expansion cards and graphics cards. The PCIe is the device driver interface into the DDCC from the host computer. PCIe is based around serial links called lanes. Each lane carries 250 MB/s in each direction. The connection between card and motherboard consists of between one and 32 lanes giving a maximum transfer rate of 8 GB/s in each direction.

PP	Protection Profile (Does not exist for one way packet transfer systems)
Reassembly Controller	Exclusive to the Receive-Only DualDiode Communication Card, the FPGA functions as a Reassembly Controller that receives packet payloads and reassembles them directly into pre-allocated memory buffers in the host memory. The Reassembly controller is rendered as a platform flash software image operating in FPGA hardware.
Receive-Only DDCC	The Receive-Only DDCC only allows information for transfer to flow from its optical interface across the Receive-Only DDCC and to the host system. All information presented for transfer to the Receive-Only DDCC is subject to the unconditional unidirectional information flow. No information is able to flow from the host system across the Receive-Only DDCC and through the optical interface of the Receive-Only DDCC. This non-bypassability of the TOE is enforced at the physical level.
Receiving Host	The host system or network in which a Receive-Only DDCC is installed. The Receiving Host is to receive information through the Receive-Only DualDiode Communication Card.
Segmentation Controller	Exclusive to the Send-Only DualDiode Communication Card, the FPGA functions as a Segmentation Controller that segments data from the host into proprietary Owl packets or "cells". The cell payloads are then packaged and framed before transmission. The platform flash software image operating in FPGA hardware will operate as if it were a Segmentation Chip is used only in the Send-Only DualDiode Communication Card.
Sending Host	A host system or network in which a Send-Only DDCC is installed. The Sending Host is to send information through the Send-Only DualDiode Communication Card. See Source Domain.
Source or Source Domain	The originating network and / or source host system whence information is transmitted through the TOE. The Source or Source Domain must have a host system with an Owl Send-Only DualDiode Communication Card installed. See Sending Host.
Send-Only DDCC	The Send-Only DDCC only allows information for transfer to flow from the host system across the DDCC through the optical interface. All information presented to the Send-Only DDCC is subject to the unconditional unidirectional information flow. No information is able to flow from outside the Send-Only DDCC through the optical interface across the Send-Only DDCC and into the host system. This non-bypassability of the TOE is enforced at the physical level.
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation – The Owl Version 7 DualDiode Communication Card
TSF	TOE Security Function
TSP	TOE Security Policy
v.7 Standard Capacity	May refer to the Owl DualDiode v.7 Standard-Capacity 2.5G Communication Cards Commercial and Industrial Variation or Owl DualDiode v.7 Standard-Capacity 1.0G Communication Cards Commercial and Industrial Variation or Owl DualDiode v.7t Commercial and Industrial 1.0G Communication Cards or be used in place of the term v.7 Standard Capacity DDCC

Table 4 Acronyms & Abbreviations

1.6 TOE Description

Owl's Security Target focuses on the DualDiode Version 7 family of products, which comprises a specific set of configuration variants that include three different speed classes, two different form factors, and special circuit component selection capable of operating over extended temperature ranges.

The 10G DualDiode Communications Card and the v.7 Standard Capacity 2.5G and 1.0G cards are half high and half length for installation into server platforms that have PCIe express serial expansion slots. Only high end servers with PCIe gen2 serial buses will be able to utilize the full capabilities of the 10G DualDiode Communications Card.

The v.7t 1.0G Communication Card uses the same components as the v.7 Standard Capacity 1.G cards, is adapted to comply with the form factor PC104 that requires it have the stackable connector to join with a PC104 host CPU. This form factor allows Owl to offer host systems with a v.7t 1.0G Communication Cards installed in a 1U size chassis, such as the OPDS-1000 or OCDS-1000.

All DualDiode Version 7 products are based on a proprietary Segmentation/Reassembly chip design and faster components to maximize one-way channel capacity up to 10 Gbit/sec. High throughput performance is of interest to customers who move large files and/or multiple channels of full-motion video.

DualDiode Version 7 10Gbit configuration is shown below in Figure 2.

Figure 2 - Owl Data Diode Communication Cards, Version 7

Significantly, DualDiode Version 7 implements the same TOE Security Functions as all previous CC-certified DualDiode card versions 1 through 6.

The TOE is the hardware suite of Owl Send-Only DDCC paired with a Receive-Only DDCC. The TOE operating at either 1.0, 2.5 or 10 Gigabits per second (Gbs) will securely transfer data one-way-only between a discrete network domain (source domain) to another discrete network (destination domain). Any host or hosts server that supports a PCIe interface slot provides a sufficient environment for the correct operation of the TSF; therefore the host is not part of the TOE. The DDCC was designed to use a one-way dedicated point-to point link. This creates a trust-nothing design that ensures each network remains isolated and protected. This technology satisfies the National Institute of Standards and Technology policy NIST SP 800-53, AC-4(7) for "hardware enforced one-way flow control".

An Owl-proprietary transport protocol is employed to ensure a non-routable, true protocol break between sending and receiving network domains as described by the NIST 800-53, AD-4(16) is employed by the TOE. The Owl-proprietary transport protocol eliminates handshaking protocols used in TCP/IP, SCSI, USB, serial/parallel port communications, etc. and creates a high-efficiency packet format. This high-efficiency packet format will optimize the 1.0Gps, 2.5Gps or 10Gbps card set to create a non-routable proprietary communication protocol, one-way-only flow of streaming video, surveillance images, files, sensor and directory data or any data type between network domains through the TOE as indicated in Figure 1. This approach removes any backchannel or return channels which can be used as a covert channel security threat.

By design the DDCC cannot be altered to change the function of the TOE. When the TOE is used to connect one discrete network domain (source) with another discrete network domain (destination), the TOE and corresponding servers can be deployed to push information from the source network to the destination network without compromising the confidentiality of the destination network. Per NIST SP 800-53, AC-4(21), the TOE provides a non-bypass optical

isolation to protect against covert data flow channels that are not subject to flow controls between network domains. This approach has been developed to minimize any security threats from transient electromagnetic pulse emanations.

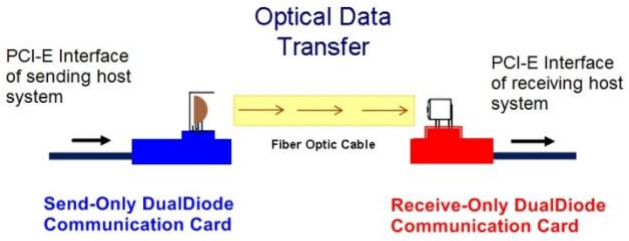


Figure 3 – High Level view of the DualDiode Interface

Data from the Sending Host is sent through the PCIe interface using the software driver for the Send-Only DDCC. The Send-Only DDCC then queues, stages, segments and frames the data before forwarding it to the Optical Transceiver. The Send-Only DDCC Optical Transceiver then transmits the packet data. Only the traces to the photo-transmitter half of the Send-Only DDCC Optical Transceiver are fully operational to transmit the packet data through the optical fiber. The Send-Only DDCC does not wait for a ready to receive signal from the other half of the TOE as the photo-receiver half of the Optical Transceiver has been disabled and permanently sealed with opaque material. This is the single function performed by the Send-Only DDCC portion of the TOE.

The data transmitted from the Send-Only DDCC goes through an optical fiber. The use of an optical interface was implemented as an approach to eliminate any possible emanation security threats when using the TOE. The data arriving to the Receive-Only DDCC portion of the TOE is passed from the receiving portion of the Optical Transceiver. No ready to receive signals are transmitted to the Send-Only DDCC as only power and operational traces in the card go to operate the photo-sensitive receiver portion of the Optical Transceiver. The traces that operate the photo-transmitter are removed and the port is permanently sealed with opaque material. The Optical Transceiver forwards the packet data to the card where it is then reassembled. The reassembled data is then transferred through the PCIe interface to the Receiving Host. The Receiving Host using the Receive-Only DDCC software drivers is able to take delivery of the information from the Receive-Only DDCC using the PCIe port. This is the single function performed by the Receive-Only DDCC portion of the TOE.

1.7 TOE Physical Architecture

The Owl Cyber Defense Solutions, LLC (Owl) DualDiode System provides an absolute one-way connection between a source domain; sending host system or network, and 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 via the Owl DualDiode System.

The Target of Evaluation (TOE) comprises two Owl DualDiode Communication Cards (DDCCs), the Send-Only DDCC and the Receive-Only DDCC. The DDCCs are manufactured to Owl's specifications using standard network components which are available as commercial-off-the-shelf (COTS) components. The device driver software allows the host system a means of communicating with the DDCC though the PCIE bus. All device driver software are designed, written, and packaged by Owl. Each DualDiode Communication Card connects to a standard PCIe slot in a host system and each is connected to each other using fiber optic network interfaces and a fiber optic cable. One DualDiode Communication Card (DDCC) is used only for sending information, the Send-Only DDCC. The other DDCC is used only for receiving information, the Receive-Only DDCC.

The Send-Only DDCC exports light pulses converted by the Optical Transmitter from electrical voltages. The Receive-Only DDCC imports light pulses received at the photo detector of the Optical Receiver of the Receive-Only DDCC and converts the light pulses to electrical voltages.

In the Send-Only DDCC, the TSF Module connects to the Physical Interface Device of the host through which it will transmit the information packets to the DDCC. The input transmission of information will be buffered, managed and scheduled by the module before being sent to the transmitter side of the Optical Transmitter. The Send-Only DDCC module of the TSF has designed circuitry that renders the receive side of the transceiver unusable. The design used on the Send-Only 10G v.7 DDCC has the traces to the input and output for the receiver portion of the Optical Transceiver

removed. The other design used on the Send-only v.7 Standard Capacity and v.7t DDCC module places the Optical Transceiver in a unique send only footprint that is without any power traces going to the receive portion of the Optical Transceiver.

The Send-Only DDCC module of the TSF has designed circuitry that eliminates power to the transceiver or removes any circuit traces that would tie into the input signal side of the transceiver. Each design has removed any possible physical connection between the receive side of the transceiver on the card and only allow the circuitry a connection with the output side of the Optical Transceiver.

In the Receive-Only DDCC, the TSF Module interfaces for information transfer connect to the output of the receiver side of the Optical Transceiver and to the input of the Physical Interface Device. The Receive-Only DDCC module of the TSF is designed so the circuitry eliminates power to the transceiver or removes any circuit traces that would tie into the output signal side of the transceiver. Each design has removed any possible physical connection between the send side of the transceiver on the card and only allow the circuitry a connection with the input side of the Optical Transceiver. There is no physical connection between the output of the transmission side of the Optical Transceiver and the input of the receiver side.

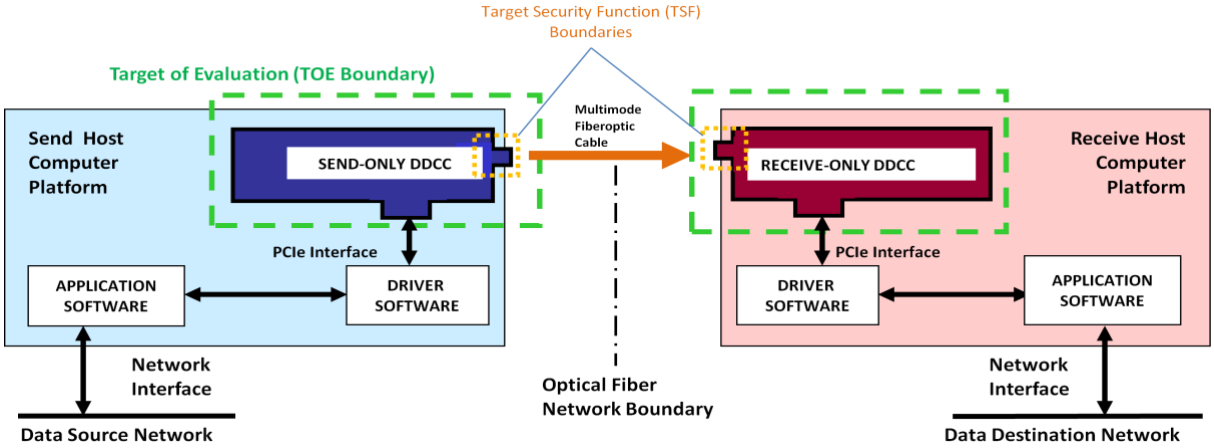


Figure 4: TOE Architecture

1.7.1 Physical Boundaries

The TOE maintains two physical boundaries, the Send-Only DDCC that is hosted by the Data Source Network and the Receive-Only DDCC hosted by the Data Destination Network.

The TOE consists of a Send and Receive pair of v.7 DDCC tied together with a Fiber Optic cable. The v.7 Send-Only DDCC and Receive-Only DDCC pair must be installed into the PCIe slot of the host server that meets the minimum requirements listed in Table 5. The server must be running an Owl tested and approved 64-bit Operating System to use the Owl device drivers. A list of the Operating Systems that have been tested and approved as compatible with Owl v.7 drivers are found in the "Owl Version 7 (Type 7000) Installation Manual". The endorsed operating systems listed in the manual are Red Hat® Enterprise Linux® (RHEL) or CentOS®: Version 6 or Version 7. It is not recommended to employ other operating systems with the Owl v.7 drivers. Though the v.7 DDCC models minimum requirements for a host may vary they share a common version 7 driver and Owl has developed several software trademarked applications such as:

- Secure Directory File Transfer System (DFTS®)
- TCP Packet Transfer System (TPTS™)
- Secure Network Transfer System (SNTS®)
- Owl ScanFile Management System (OSMS™)
- Remote File Transfer Service (RFTS™)

The software applications will run on the host systems 64 bit-OS whilst utilizing the TOEs unique TSF. The above servers and software are considered to be outside the TOE and cannot affect the TOEs unidirectional information flow.

Each shipment of a TOE is packaged with all the necessary components; low profile brackets, fiber optic cable, manuals, etc. and any requested optional software applications that are essential for a seamless installation. To confirm and maintain confidence that the TOE and components are from Owl and the package has not been tampered with, a secure packaging method is implemented to make it easily detectable should tampering, modification or substitution occur.

Each boxed kit containing the TOE is labeled per government requirements and secured with security tape. All interior boxes of the DDCC are labeled and have fields that relate directly to the sales order. The Send-Only DDCC and Receive-Only DDCC will be boxed and labeled showing the serial number of the individual DDCC contained in the box along with the part number for the card from the sales order.

The exterior boxes will have the collective field information from the interior labeling of the TOE. When a pair of v.7t DDCC is shipped, it comes with a selection of pre-installed customer chosen Owl applications inside a rack mountable 1U chassis as an Owl solution. The Owl solution is then packaged, security taped and treated in a similar fashion as the other v.7 DDCC boxed kits.

For the Owl customer an additional security measure is the shipment notification. The shipment notification tells the customer when the TOE is shipped and alerts them of the impending arrival date. The notification includes the purchase order number with a notice to indicate if the DDCC is CC evaluated, equipment sent and the recorded delivery services shipping tracking number (e.g., FedEx), date of shipment and the expected date of arrival. The point of contact will receive additional information, including the serial numbers of the TOE or items sent.

Standard carriers like FedEx will forward tracking information 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 the shipments ETA. These methods are employed by Owl to limit the opportunity an untrustworthy individual would have to 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.

The TOE requires the following hardware, software, and firmware in its environment:

Component	*Fiber Optic Cable / (Jacket Color)*	*OS Req.*	*OS DDCC Driver*	*Minimum Server Requirements*	*Interface (bus) Type (Non-Graphics)*
Owl DualDiode 10G v.7 Communication Cards					
	multi-mode LC–LC simplex patch cable (Aqua)	64-bit OS	Version 7	3.3GHz Multi-core Processor /Xeon	PCIe Express x8
Owl DualDiode v.7 Standard-Capacity 2.5G Communication Cards in Industrial or Commercial Variation					
	single-mode LC–LC simplex patch cable (Yellow)	64-bit OS	Version 7	3.3GHz Multi-core Processor /Pentium core i5	PCIe Express x4
Owl DualDiode v.7 Standard-Capacity 1.0G Communication Cards in Industrial or Commercial Variation					
	multi-mode LC–LC simplex patch cable (Orange)	64-bit OS	Version 7	3.0 GHz Multi-core Processor /Pentium core i3	PCIe Express x4
Owl DualDiode v.7t Industrial or Commercial 1.0G Communication Cards					
	multi-mode LC–LC simplex patch cable (Orange)	64-bit OS	Version 7	1.8 GHz Dual-core Processor (PC104 Form Factor)	PC104 PCIe Express x1

Table 5 TOE Environmental Requirements

1.7.2 Logical Boundaries

This section will summarize the TOE Security Functions provided by the Owl DualDiode Communication Cards.

1.7.2.1 User data protection

The Owl DualDiode Communication Cards pass data from the Send-Only DDCC to the Receive-Only DDCC and provide 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 fiber-optic cable. The Send-Only DDCC of the TOE is only capable of transmitting information and conversely the Receive-Only DD of the TOE is only capable of receiving information.

1.7.2.2 Protection of the TSF

The design features provided below have been incorporated in the Owl DualDiode Communication Cards to ensure the integrity, reliability and security of the TOE.

Fail Secure – Each DDCC was designed as a single functioning mechanism that only operates a photo-transmitter for transmitting information via light signals; the Send-Only DDCC, or as a single functioning mechanism that activates a photo-detector that retrieves light signals; the Receive-Only DDCC. The only information flow between the source network and destination network is through the TOE, any failure within one or both components will prevent all data flows. Thus any component failure in the TOE will prevent any means of unintended information flow from bypassing the TSF.

1.8 TOE Software

While the TOE is defined as a pair of Owl DualDiode Communication Cards, the TOE requires a host that is able to interface with the TOE. Owl provides DDCC software drivers which when installed on the host allows the system to interface across the PCIe interface to the TOE and employ the TOE Security Functions (TSF) to pass data. The DDCC drivers are provided by Owl but are not a part of the TOE.

Owl offers end users software to convey user data across the PCIe interface to the Send-Only DDCC and from the Receive-Only DDCCs across the PCIe interface (See Section 1.7.1.). This is due to the interface abilities of the Owl driver software that allows the host to work with the TOE. The host server, DDCC drivers and software are considered to be outside the TOE and cannot affect the unidirectional information flow of the TOE.

1.9 TOE Documentation

Owl provides an administrator and user manual as a .PDF file. The manual provides guidance and information on how to utilize the TOE security functions and warnings about actions that can compromise the security of the TOE. Guidance documents for the TOE describe procedures for secure delivery, installation, operation, and flaw remediation.

Customers will also receive a Purchase Order describing the product purchased and the uniquely identified S/N of the DDCC. The S/N shown on the permanent label of the DDCC must match the S/N shown on the Purchase Order.

The following Owl document is considered part of the TOE:

- "*Owl Version 7 Card (Type 7000) Installation Manual*" v.05a (6/11/2019)

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)

The TOE is designed for environments where a one-way flow of information at high speeds between attached host computing systems is required. Given that the TOE is based strictly on hardware, and that its target Evaluation Assurance Level is 4 (EAL4) augmented with AVA_VAN.4, the TOE is suitable for environments that are subject to a broad range of logical attacks, regardless of attack potential, since the TOE is subject only to physical type attacks. Hence, the TOE is essentially as strong as the physical environment into which it is placed.

The asset to be protected is the information and IT resources located on the host end of the Receive-Only DDCC side being protected by the TOE.

Less common but just as secure is the protection of the assets by the TOE on the Send-Only DDCC side where the IT resources are located and the source of information is immune from external tampering.

Note: The security problem definition defines the security problem in terms of threats and policies that are addressed by the TOE together with the operational environment of the TOE. It also specifies the assumptions on the operational environment necessary for the TOE to be able to address the security problem.

3.1 Organizational Security Policies

P.ONEWAY	Information from the source host must only flow one-way to the attached destination host.
P. SEALS	The installation of the TOE in its operational environment shall be done with visible tamper detection markings that can be manually inspected to detect any tampering.

3.2 Threats

T.FAILURE	The TOE has a hardware failure that allows access to confidential information on the destination side through the TOE.
T.OLD_INF	An attacker may gather residual information by monitoring the IP stack at the Transport Layer from previous information transmissions or from internal TOE data.
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 destination 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 through the TOE 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 of guidance. The appropriate security authority shall accredit the installation of the TOE before taking 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.
OE.TAMPER_SEALS	The installation of the TOE in its operational environment shall be done with visible tamper detection markings that can be manually inspected to detect any tampering.

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	P.SEAL	T.FAILURE	T.OLD_INF	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			X								
O.FAILSAFE			X									
OE.ADMIN		X			X		X					
OE.CONNECTION								X				
OE.EMISSION									X			
OE.GUIDE		X								X		
OE.NETBREAK	X										X	
OE.PHYSICAL					X							X
OE.TAMPER_SEALS		X			X							

Table 6 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 through the TOE 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 P.SEALS

The installation of the TOE in its operational environment shall be done with visible tamper detection markings that can be manually inspected to detect any tampering.

This Organizational Policy is satisfied by ensuring that:

- OE.TAMPER_SEALS: The installation of the TOE in its operational environment shall be done with visible tamper detection markings that can be manually inspected to detect any tampering.
- OE.ADMIN: Authorized personnel that are used to install, administer and use the TOE are trustworthy, competent and follow the guidance.
- 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.

4.3.1.3 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.

4.3.1.4 T.OLD_INF

An attacker may gather residual information by monitoring the IP stack at the Transport Layer from previous information transmissions or from internal TOE data.

This Threat is satisfied by ensuring that:

- O.NON_ROUTEABLE: Information packets that flow through the TOE are void of any standard protocols and data that would contain information to making packets routable on the internet.

4.3.1.5 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.
- OE.TAMPER_SEALS: The installation of the TOE in its operational environment shall be done with visible tamper detection markings that can be manually inspected to detect any tampering.

4.3.1.6 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.

4.3.1.7 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.

4.3.1.8 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.

4.3.1.9 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.

4.3.1.10 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.

4.3.1.11 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.

4.3.1.12 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 subsequently. 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 DualDiode Communication Card.

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 7 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 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 DualDiode Communications Card]**.

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **[**

a) **If the physical configuration of the DualDiode Communication Card permits it to send data, then only the sending of data packets from the external interface to the TOE is permitted;**

b) **If the physical configuration of the DualDiode Communication Card permits it to receive data, then only the receiving of data packets through the TOE to the external interface is permitted]**.

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: **[no explicit authorization rules]**.

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: **[no explicit denial rules]**.

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]**.

5.1.2 Protection of the TSF (FPT)

5.1.2.1 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 cards 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,**

b) A failure of the TOE's PCIe component will prevent the host from recognizing the TOE as an external device and execute operations,

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

d) A failure of the TOE's identity (Send-only identity or Receive-only identity) to communicate with the TSF will prevent the TOE from being able start any communication through the TOE.]

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 8 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 9** 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 9 Objective to Requirement Correspondence

5.3.1.1 O.FAILSAFE

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

This TOE Security Objective is satisfied by ensuring that:

- 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.

5.3.1.2 O.NON_ROUTABLE

Information packets that flow through the TOE are void of any standard protocols that would make the information packets routable on the Internet.

This TOE Security Objective is satisfied by ensuring that:

- FDP_IFF.5: Only a single exterior interface through the TSF shall exist to allow the unidirectional flow of information by means of a proprietary transfer protocol through the TOE.

5.3.1.3 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 a proprietary transfer protocol 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.

5.3.1.4 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 a proprietary transfer protocol 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
FDP_IFF.5	FDP_IFC.1 Subset information flow control	FDP_IFC.2

Table 10 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 DualDiode products address the following security attributes:
(1) one-way information flow security policy
(2) non-bypassability (all data flows through optical fiber with one-way enforcement at each end)
(3) non-routable protocol break (derived from proprietary ATM-like protocol implemented in hardware)
(4) total IP network isolation (due to protocol break described above; testable at the optical interfaces of Send and Receive DDCCs)
(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 Owl DualDiode Communication Card (DDCC) is complete and unconditional. The DDCC enforces unidirectional flow control on any request from an external interface to move data packets through the DDCC and all operations that cause that information to flow through the Owl DualDiode System.

The DDCC enforces the unidirectional information flow based on its physical attributes at the component level. The DDCC permits information flow between a controlled subject and controlled information via controlled operation, according to rules defined by the physical design of the DDCC.

Each Owl Cyber Defense DualDiode Communication Card (Owl DDCC) physically can only provide network traffic flow in one direction through the card. The Send-Only DDCC allows only the one-way transfer of information from a host system through the DDCC to outside the host system, and there is no transfer of information from outside the host system, through the DDCC into the host system. The Receive-Only DDCC allows only the one-way transfer of data from outside a host system through the DDCC and into the host system and there is no transfer of information from the host system through the DDCC to outside the host system.

If a host system attempts to receive information using a Send-Only DDCC, there will be no transfer of information from outside the host system, through the Send-Only DDCC into the host system. In the Send-Only DDCC, the output of the transmitter side of the Framer is connected to the photo-transmitter of the Optical Transceiver. The Send-Only DDCC has physically unavailable an impedance-matched electrically conductive path to the input of the receiver side of the Optical Transceiver. Furthermore, the Send-Only DDCC connects the host-system power to the photo-transmitter of the Optical Transceiver and leaves unpowered the photo-detector. When the host system does not receive information using the Send-Only DDCC, it is up to the host system protocol to deal with not receiving any information. The unidirectional information flow policy is maintained even though the host system has attempted to receive information through a Send-Only DDCC.

If a host system attempts to send information over a Receive-Only DDCC, buffers of data may be sent through the host device driver over the PCIe interface to the Receive-Only DDCC, but no information will flow from the host system through the DDCC to outside the host system. The Receive-Only DDCC has physically unavailable an impedance-matched electrically conductive path to the transmitter side. Furthermore, the Receive-Only DDCC connects the host-system power to the photo-detector of the Optical Transceiver and leaves unpowered the photo-transmitter. The host

system will receive no response that the information was not sent. The unidirectional information flow policy is maintained even though the host has attempted to send information through a Receive-Only DDCC.

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

- FDP_IFC.2: The TOE is composed of a Send-Only DDCC connected to the Receive-Only DDCC. The Send-Only DDCC directly interfaces with the source host to only transmit information through a fiber-optic cable. No external electronic or light signals are admitted back through the Send-Only DDCC to the source host. Conversely, the Receive-Only DDCC directly interfaces with the destination host and only receives information through a fiber-optic cable. The Receive-Only DDCC is not able to transmit electronic or light signals to any external sources. This ensures all send and receive information flows through the TOE and are subject to the unidirectional SFP.
- FDP_IFF.1: By design the Send-Only DDCC only allows information for transfer to flow from the host system across the DDCC through the optical interface. All information presented to the Send-Only DDCC is subject to the unconditional unidirectional information flow. No information is able to flow from outside the Send-Only DDCC through the optical interface across the Send-Only DDCC and into the host system. Conversely, the Receive-Only DDCC only allows information for transfer to flow from its optical interface across the Receive-Only DDCC and to the host system. All information presented for transfer to the Receive-Only DDCC is subject to the unconditional unidirectional information flow. No information is able to flow from the host system across the Receive-Only DDCC and through the optical interface of the Receive-Only DDCC. This non-bypassability of the TOE ensures the SFP is enforced at the physical level.
- FDP_IFF.5: The TOE (Receive-Only and Send-Only DDCC) only has two external interfaces. One photo-transmitter on the Send-Only DDCC and one photo-detector on the Receive-Only DDCC. 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 informational policy between domains uses a proprietary communication protocol that does not add a padding layer of information that would disclose the source or destination of the data being transmitted. 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 DDCC has been designed, developed and implemented so a component (Send-only DDCC or Receive-Only DDCC) 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 component of the TOE as a single purpose communication card; Send-only DDCC or Receive-only DDCC. 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 is 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 of the security functions and assurance requirements. Furthermore, all of 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 11 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 11 Security Functions vs. Requirements Mapping

7 Revision History

Version	Date	Changes / Reason for changes
01a	8/13/2018	Draft document for the DDCC Ver. 7 EAL 4
01b	8/23/2018	Delete Sections 5.2.1 – 5.2.6, 6.2, 7, Section 8.1 is now Section 4.3, Section 8.2 is now 5.3, Section 8.3 is now 5.4, Section 8.4 is now 5.5, Deleted SARs from Section 5.5, Section 8.5 is now Section 5.6, Section 8.6 is now Section 6.2, Minor edit to Sec. 7
01c	9/4/2018	Minor edit to Sec. 1.4, Delete Section 7, Section 7.1 is now Section 5.5, Section 5.5 is now Section 5.6
01d	10/2/2018	Minor edit to Sec. 1.1,1.3, 1.5, 1.7.1, 1.7.2.1, 1.9, 3.0, 5.6
01e	10/13/2018	Minor edit to Sec. 1.1, 1.2, 1.7.1, 1.9, 3.2, 4.2, 4.3.1, 5.1.1.2, added 5.3.2, removed 5.5
01f	11/13/2018	Minor edit to Sec. 1.1, 1.2, 1.7.1, 3.1, 3.3, 4.1, 4.2, 4.3.1, 4.3.1.5, 4.3.1.7, 4.3.1.9, 4.3.1.10, 5.1.2.1, 5.3.1
01g	11/26/2018	Rewrite of chapter 3 and 4, mainly to sort out some of the mapping and the rationale. Then we have to adjust the mapping of the security objectives of the TOE to the SFRs.
01h	11/27/2018	Minor edit to Sec. 4, Removed SFR FPT_PHP.1 from Sec. 5 & 6, Added to SFR.
01i	12/4/2018	Minor edit to Sec. 1.1, 1.2, 1.7.1, 5.1.2.1, 5.3.1
01j	2/25/2019	Minor edit to Sec. 1.7.1
01k	5.22.2019	Minor edit to Sec. 1.1, 1.9
01l	6/11/2019	Minor edit to Sec. 1.1, 1.9, 2.1, 3, 5.2, 5.3.2 replaced EAL 4 with EAL4+ and updated Installation Manual version and release date
01m	6/17/2019	Minor edit to Sec. 2

E N D O F D O C U M E N T