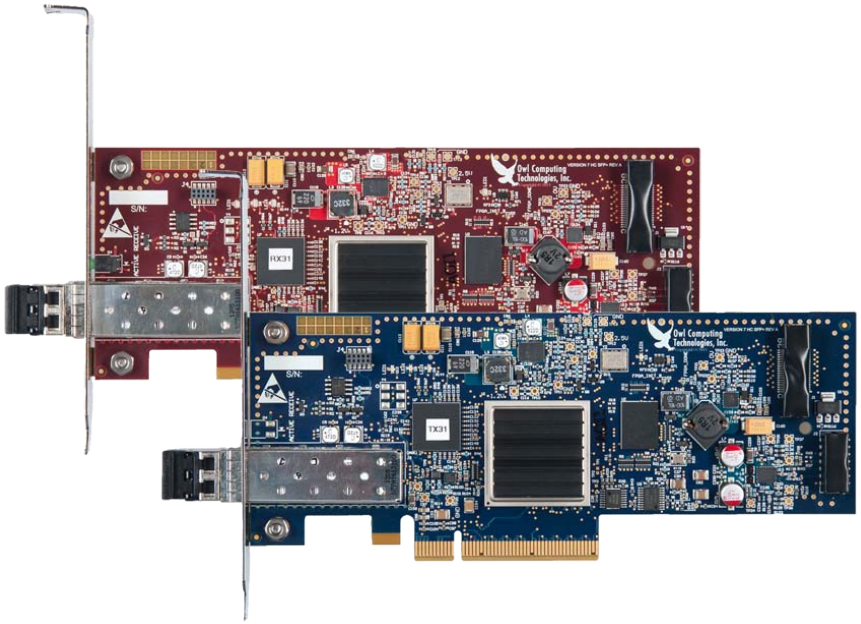
DualDiode Communication Cards 10G, 2.5G, 1.0G v.7 & v.7t Models

Security Target

Common Criteria - EAL 2 Certification



Document: OwlDualDiodeVer-7 Model-SecurityTarget-EAL2_v01l.doc
Version: 01l
Date: December 2014

Prepared By: Randall Colette
Prepared For: Owl Computing Technologies, Incorporated
38A Grove Street, Suite 101
Ridgefield CT 06877
USA
Web: http://www.owlcti.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	DualDiode Communication Cards 10G, 2.5G, 1.0G v.7 & v.7t Models Security Target
ST Version	r01l
ST Publication Date	12/11/14
Vendor and ST Author	Owl Computing Technologies, Inc.
CC Identification	Common Criteria for Information Technology Security Evaluation, Version 3.1 Rev 4, September 2012
TOE Identification	The TOE consists of one or more pairs of the following security hardware products.

Table 1 ST Identification

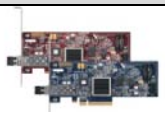
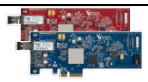
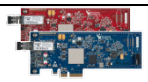
TOE Hardware Products		Maximum Speed	Channels	Part Number
Owl DualDiode **10G v.7** Communication Cards		10 Gbps	32	V7sfp+RO-6-D-C (Receive-Only Card) V7sfp+SO-6-D-C (Send-Only Card)
Owl DualDiode **v.7** Standard-Capacity **2.5G** Communication Cards in Commercial or Industrial Variations		2.5 Gbps	16	V7sc-RO-X-9-C (Red Card-Commercial Version) V7sc-SO-X-9-C (Blue Card-Commercial Version) V7sc-RO-X-G-I (Red Card-Extended Industrial Temperature) V7sc-SO-X-G-I (Blue 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 (Red Card-Commercial Version) V7sc-SO-X-E-C (Blue Card-Commercial Version) V7sc-RO-X-G-I (Red Card-Extended Industrial Temperature) V7sc-SO-X-G-I (Blue Card-Extended Industrial Temperature)
Owl DualDiode **v.7t** Commercial and Industrial **1.0G** Communication Cards		1.0 Gbps	8	V7t-RO-X-E-C (Red Card-Commercial Version) V7t-SO-X-E-C (Blue Card-Commercial Version) V7t-RO-X-G-I (Red Card-Extended Industrial Temperature) V7t-SO-X-G-I (Blue Card-Extended Industrial Temperature) V7t-RO-X-E-CP (Red Card-Commercial Stack Version) V7t-SO-X-E-CP (Blue Card-Commercial Stack Version.)

Table 2 TOE Hardware Products

1.2 TOE Reference

Developer Name	Owl Computing Technologies, Incorporated
TOE Identity	Owl DualDiode 10G v.7 Communication Cards
	Owl DualDiode v.7 Standard-Capacity 2.5G Communication Cards in Commercial Variation
	Owl DualDiode v.7 Standard-Capacity 2.5G Communication Cards in Industrial Variation
	Owl DualDiode v.7 Standard-Capacity 1.0G Communication Cards in Commercial Variation
	Owl DualDiode v.7 Standard-Capacity 1.0G Communication Cards in Industrial Variation
	Owl DualDiode v.7t Commercial 1.0G Communication Cards
	Owl DualDiode v.7t Industrial 1.0G Communication Cards
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 Computing Technologies, Incorporated (OwlCTI). 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 Owl 1U tamper resistant server platforms that use 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. OwlCTI 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. OwlCTI drivers provide the necessary device interrupt routines required for applications to use the DDCC on such OS platforms.

Software applications loaded on the host systems must be customized to operate and send data across the TOE. OwlCTI provides software application products like Secure Network Transfer Systems (SNTS) for transferring all data types through the TOE. For datagram transfer OwlCTI 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 OwlCTI, 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 OwlCTI 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 OwlCTI 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.

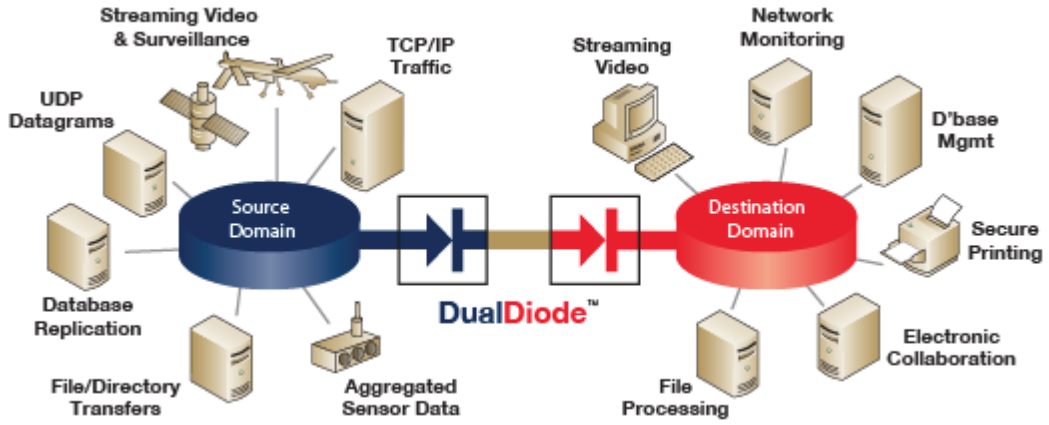


Figure 1 – Owl 10G DualDiode Communication Card Concept

Market Usage

Over 1400 DualDiode systems from OwlCTI have been deployed throughout the US Department of Defense, Intelligence Community, CSE Canada, U.S. Allies and the market continues to grow. OwlCTI 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.
Section 7	Protection Profile Claims	This section defines the Protective Profile claims of this Security Target.
Section 8	Rationale	This section presents the evidence that supports the claims made in this Security Target and defines how the requirements are complete and provides an effective set of countermeasures within the chosen secure environment.

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 Computing 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	Owl DualDiode v.7 Standard-Capacity 2.5G Communication Cards Industrial Variation or Owl DualDiode v.7 Standard-Capacity 1.0G Communication Cards Industrial Variation or Owl DualDiode v.7t Commercial and Industrial 1.0G Communication Cards or 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 OwlCTI to offer host systems with a v.7t 1.0G Communication Cards installed in a 1U size chassis.

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.

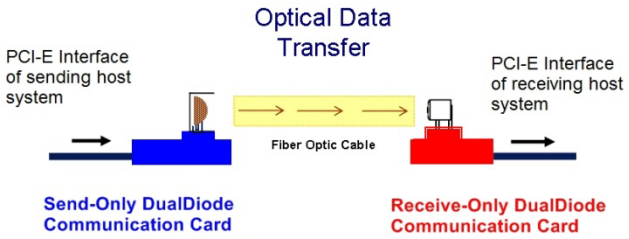


Figure 3 – High Level view of the DualDiode Interface

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 a 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 Computing Technologies, Incorporated (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.

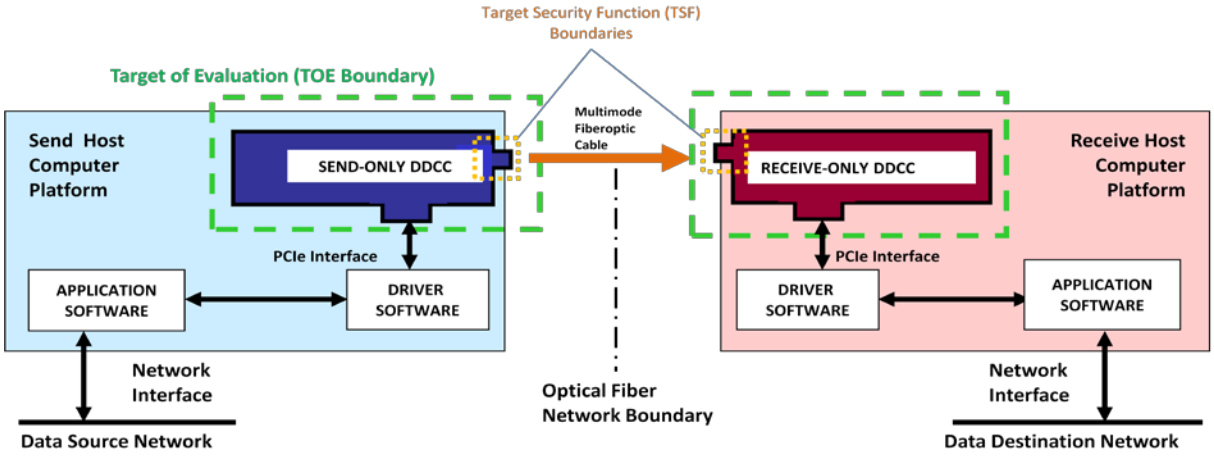


Figure 4: TOE Architecture

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 a OwlCTI tested and approved 64-bit Operating System to use the OwlCTI device drivers. A list of the Operating Systems that have been tested and approved as compatible with OwlCTI v.7 drivers are found in the "Owl Version 7 (Type 7000) Installation Manual". Though the v.7 DDCC models minimum requirements for a host may vary they share a common version 7 driver and Owl CTI 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.

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

Component	*Fiber Optic Cable / (Jacket Color)*	*OS Req.*	*OS 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.

No Illicit information flows – By design the TOE only allows information to flow from the source host systems through the TOE to the destination host system. No information is able to flow from outside the Send-Only DDCC and by-pass the TOE to reach the source host system. Conversely no information from the destination host system will by-pass the Receive-Only DDCC of the TOE to flow to the outside.

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.

Passive detection of physical attack - All the TOE's TSFs operate at the physical level, therefore physically altering hardware and modifying the internal operations are the only real risk posed to possibly bypass the unidirectional flow security features. Designs and policies are implemented to make it self evident whether or not any tampering or substitution of either the Send-Only DDCC or Receive-Only DDCC had occurred.

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. OwlCTI 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 OwlCTI but are not a part of the TOE.

OwlCTI 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 effect the unidirectional information flow of the TOE.

1.9 TOE Documentation

While the TOE is substantially defined by the Owl DualDiode Communication Cards, the TOE also includes associated installation and operation guidance. See section 6 of this Security Target for more specific information about available documents and specific guides used for the evaluation of the TOE.

The following OwlCTI document is considered part of the TOE:

- Owl Version 7 Card (Type 7000) Installation Manual

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 4, CCMB-2012-09-002.
    - Part 2 Conformant
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1, Revision 4, CCMB-2009-09-003.
    - Part 3 Conformant
    - Assurance Level: EAL 2.

2.1.1 Protection Profile Conformance Claim

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

2.1.2 Package Claims

The DualDiode Version 7 TOE is conformant with Security Assurance Requirement:

- EAL2 conformant.

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 2 (EAL 2), 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 are the information and IT resources located on the host end of the Receive-Only DDCC side being protected by the TOE.

Note The summary of the applicable security environment is stated in terms of a policy and threat that directly correspond and a set of assumptions about the physical application of the TOE.

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.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.
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.FAILURE	The DDCC has a hardware failure that allows access to confidential information on the destination side through the TOE.
T.TAMPER	An attacker tampers with the DDCC during delivery and /or after installation that removes any restrictions of the TOE in order to compromise the confidentiality of the destination side.

3.3 Assumptions

A.ADMIN	Authorized personnel that posses the necessary privileges to access the secure side information shall install, administer and use the Owl DDCC by adhering to the security policies and practices regarding the usage of the TOE.
A.GUIDE	Authorized personnel shall ensure the TOE is delivered, installed and administered in a manner that maintains security. The appropriate security authority shall accredit the installation of the Owl DDCC.
A.NETBREAK	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.
A.CONNECTION	The TOE will be installed so only relevant network traffic will flow through the TOE and hence be subject to the organizational security policy.
A.PHYSICAL	The TOE and its operating environment will be physically protected to a degree commensurate with the value of the information it is intended to protect.

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.READONLY	The TOE must ensure that each interface designated as receive-only will only receive and not send information.
O.WRITEONLY	The TOE must ensure that each interface designated as send-only will only send and not receive information.
O.TAMPER_SEALS	The TOE must be designed with visible markings and a means of identification as proof the operation and function of information flow preserve the SF.
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.

4.2 Security Objectives for the TOE Environment

OE.ADMIN	Authorized personnel that posses the necessary privileges to access the secure side information shall install, administer and use the Owl DDCC by adhering to the security policies and practices regarding the usage of the TOE. The authorized administrators will properly adhere to the establishment and maintenance of the security policies and practices regarding the usage of the TOE.
OE.CONNECTION	The TOE will be installed such that all relevant network traffic will flow through the TOE and hence be subject to itself information flow policy.
OE.PHYSICAL	The TOE and its operating environment will be physically protected to a degree commensurate with the value of the information it is intended to protect.
OE.GUIDE	Authorized personnel shall ensure the TOE is delivered, installed and administered in a manner that maintains security. The appropriate security authority shall accredit the installation of the Owl DDCC. The administrative staff shall install and manage the TOE in a manner that maintains security.
OE.NETBREAK	The TOE is the only way of interconnecting the source network and destination network. The administrative staff shall install and operate the TOE to insure the security between the source network and destination network to maintain the appropriate security being provided by the TOE through an untrustworthy product.
OE.EMISSION	The TOE is installed and operated in an environment where physical or security measures prevent any Emissions Security attacks or Telecommunications Electronics Material Protected from Emanating Spurious Transmissions attacks.

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
	FPT_PHP.1: Passive detection of physical attack	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 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 is permitted;**
- **b) If the physical configuration of the DualDiode Communication Card permits it to receive data, then only the receiving of data packets 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 hardware failure]**.

5.1.2.2 Passive detection of physical attack (FPT_PHP.1)

FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or the TSF's elements has occurred.

5.2 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL 2 conformant components 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.2	Security functional specification	ADV_TDS.1
	ADV_TDS.1	Basic design	ADV_FSP.2
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.2	Use of a CM system	ALC_CMS.1
	ALC_CMS.2	Parts of the TOE CM coverage	No dependencies
	ALC_DEL.1	Delivery procedures	No dependencies
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.1	Evidence of coverage	ADV_FSP.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.2	Vulnerability analysis	ADV_ARC.1, ADV_FSP.2, ADV_TDS.1, AGD_OPE.1, AGD_PRE.1

Table 7 EAL 2 Assurance Components

5.2.1 Security Architecture (ADV)

5.2.1.1 Security Architecture Description (ADV_ARC.1)

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.
ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.
ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.
ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.
ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.
ADV_ARC.1.3C The security architecture description shall describe how the TSF initialization process is secure.
ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.
ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.
ADV_ARC.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.1.2 Security-enforcing functional specification (ADV_FSP.2)

ADV_FSP.2.1D The developer shall provide a functional specification.
ADV_FSP.2.2D The developer shall provide a tracing from the functional specification to the SFRs.
ADV_FSP.2.1C The functional specification shall completely represent the TSF.
ADV_FSP.2.2C The functional specification shall describe the purpose and method of use for all TSFI.
ADV_FSP.2.3C The functional specification shall identify and describe all parameters associated with each TSFI.
ADV_FSP.2.4C For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.
ADV_FSP.2.5C For each SFR-enforcing TSFI, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions.
ADV_FSP.2.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.
ADV_FSP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_FSP.2.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.2.1.3 Basic design (ADV_TDS.1)

ADV_TDS.1.1D The developer shall provide the design of the TOE.
ADV_TDS.1.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.
ADV_TDS.1.1C The design shall describe the structure of the TOE in terms of subsystems.
ADV_TDS.1.2C The design shall identify all subsystems of the TSF.
ADV_TDS.1.3C The design shall describe the behavior of each SFR-supporting or SFR non-interfering TSF subsystem in sufficient detail to determine that it is not SFR-enforcing.
ADV_TDS.1.4C The design shall summarize the SFR-enforcing behavior of the SFR enforcing subsystems.
ADV_TDS.1.5C The design shall provide a description of the interactions among SFR enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.
ADV_TDS.1.6C The mapping shall demonstrate that all TSFIs trace to the behavior described in the TOE design that they invoke.
ADV_TDS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_TDS.1.2E The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

5.2.2 Guidance documents (AGD)

5.2.2.1 Operational user guidance (AGD_OPE.1)

AGD_OPE.1.1D The developer shall provide operational user guidance.
AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.
AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.
AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.
AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.
AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.
AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.
AGD_OPE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.2.2 Preparative procedures (AGD_PRE.1)

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.
AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.
AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.
AGD_PRE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.2.3 Life-cycle support (ALC)

5.2.3.1 Use of a CM system (ALC_CMC.2)

ALC_CMC.2.1D The developer shall provide the TOE and a reference for the TOE.
ALC_CMC.2.2D The developer shall provide the CM documentation.
ALC_CMC.2.3D The developer shall use a CM system.
ALC_CMC.2.1C The TOE shall be labeled with its unique reference.
ALC_CMC.2.2C The CM documentation shall describe the method used to uniquely identify the configuration items.
ALC_CMC.2.3C The CM system shall uniquely identify all configuration items.
ALC_CMC.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.2 Parts of the TOE CM coverage (ALC_CMS.2)

ALC_CMS.2.1D The developer shall provide a configuration list for the TOE.
ALC_CMS.2.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE.
ALC_CMS.2.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.2.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.
ALC_CMS.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.3 Delivery procedures (ALC_DEL.1)

ALC_DEL.1.1D The developer shall document and provide procedures for delivery of the TOE or parts of it to the consumer.
ALC_DEL.1.2D The developer shall use the delivery procedures.
ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.
ALC_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4 Security Target evaluation (ASE)

5.2.4.1 Conformance claims (ASE_CCL.1)

ASE_CCL.1.1D The developer shall provide a conformance claim.
ASE_CCL.1.2D The developer shall provide a conformance claim rationale.
ASE_CCL.1.1C The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.
ASE_CCL.1.2C The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.
ASE_CCL.1.3C The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.
ASE_CCL.1.4C The CC conformance claim shall be consistent with the extended components definition.
ASE_CCL.1.5C The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.
ASE_CCL.1.6C The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.
ASE_CCL.1.7C The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.
ASE_CCL.1.8C The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.
ASE_CCL.1.9C The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.
ASE_CCL.1.10C The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.
ASE_CCL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4.2 Extended components definition (ASE_ECD.1)

ASE_ECD.1.1D The developer shall provide a statement of security requirements.
ASE_ECD.1.2D The developer shall provide an extended components definition.
ASE_ECD.1.1C The statement of security requirements shall identify all extended security requirements.
ASE_ECD.1.2C The extended components definition shall define an extended component for each extended security requirement.
ASE_ECD.1.3C The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.
ASE_ECD.1.4C The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

ASE_ECD.1.5C The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.
ASE_ECD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ASE_ECD.1.2E The evaluator shall confirm that no extended component can be clearly expressed using existing components.

5.2.4.3 ST introduction (ASE_INT.1)

ASE_INT.1.1D The developer shall provide an ST introduction.
ASE_INT.1.1C The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.
ASE_INT.1.2C The ST reference shall uniquely identify the ST.
ASE_INT.1.3C The TOE reference shall identify the TOE.
ASE_INT.1.4C The TOE overview shall summarize the usage and major security features of the TOE.
ASE_INT.1.5C The TOE overview shall identify the TOE type.
ASE_INT.1.6C The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.
ASE_INT.1.7C The TOE description shall describe the physical scope of the TOE.
ASE_INT.1.8C The TOE description shall describe the logical scope of the TOE.
ASE_INT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ASE_INT.1.2E The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

5.2.4.4 Security objectives (ASE_OBJ.2)

ASE_OBJ.2.1D The developer shall provide a statement of security objectives.
ASE_OBJ.2.2D The developer shall provide a security objectives rationale.
ASE_OBJ.2.1C The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.
ASE_OBJ.2.2C The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.
ASE_OBJ.2.3C The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.
ASE_OBJ.2.4C The security objectives rationale shall demonstrate that the security objectives counter all threats.
ASE_OBJ.2.5C The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.
ASE_OBJ.2.6C The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.
ASE_OBJ.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4.5 Derived security requirements (ASE_REQ.2)

ASE_REQ.2.1D The developer shall provide a statement of security requirements.
ASE_REQ.2.2D The developer shall provide a security requirements rationale.
ASE_REQ.2.1C The statement of security requirements shall describe the SFRs and the SARs.
ASE_REQ.2.2C All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.
ASE_REQ.2.3C The statement of security requirements shall identify all operations on the security requirements.
ASE_REQ.2.4C All operations shall be performed correctly.
ASE_REQ.2.5C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.
ASE_REQ.2.6C The security requirements rationale shall trace each SFR back to the security objectives for the TOE.
ASE_REQ.2.7C The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.
ASE_REQ.2.8C The security requirements rationale shall explain why the SARs were chosen.

ASE_REQ.2.9C The statement of security requirements shall be internally consistent.
ASE_REQ.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4.6 Security problem definition (ASE_SPD.1)

ASE_SPD.1.1D The developer shall provide a security problem definition.
ASE_SPD.1.1C The security problem definition shall describe the threats.
ASE_SPD.1.2C All threats shall be described in terms of a threat agent, an asset, and an adverse action.
ASE_SPD.1.3C The security problem definition shall describe the OSPs.
ASE_SPD.1.4C The security problem definition shall describe the assumptions about the operational environment of the TOE.
ASE_SPD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4.7 TOE summary specification (ASE_TSS.1)

ASE_TSS.1.1D The developer shall provide a TOE summary specification.
ASE_TSS.1.1C The TOE summary specification shall describe how the TOE meets each SFR.
ASE_TSS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ASE_TSS.1.2E The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.

5.2.5 Tests (ATE)

5.2.5.1 Evidence of coverage (ATE_COV.1)

ATE_COV.1.1D The developer shall provide evidence of the test coverage.
ATE_COV.1.1C The evidence of the test coverage shall show the correspondence between the tests in the test documentation and the TSFIs in the functional specification.
ATE_COV.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.5.2 Functional testing (ATE_FUN.1)

ATE_FUN.1.1D The developer shall test the TSF and document the results.
ATE_FUN.1.2D The developer shall provide test documentation.
ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.
ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.
ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.5.3 Independent testing – sample (ATE_IND.2)

ATE_IND.2.1D The developer shall provide the TOE for testing.
ATE_IND.2.1C The TOE shall be suitable for testing.
ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.
ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.2.2E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.
ATE_IND.2.3E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.2.6 Vulnerability assessment (AVA)

5.2.6.1 Vulnerability analysis (AVA_VAN.2)

AVA_VAN.2.1D The developer shall provide the TOE for testing.
AVA_VAN.2.1C The TOE shall be suitable for testing.
AVA_VAN.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_VAN.2.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.
AVA_VAN.2.3E The evaluator *shall perform* an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE.
AVA_VAN.2.4E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

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 Computing Technologies 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.

- FPT_PHP.1: The TOE is packaged and sealed at the manufacturing site and drop shipped to the customer. The TOE packaging has tamper evident or tamper resistant chassis for easy identification of possible tampering during the delivery process. User manuals are included with the TOE that includes a visual aids that identify the TOE or the tamper resistant chassis. Each TOE is marked and must match the paperwork listed on the Packing Slip and Sales Order.

6.2 TOE Security Assurance Measures

6.2.1 Development

The DualDiode Communication Card protects itself by not exporting any interface that can be used to modify the TOE, thereby safeguarding the integrity of the TSF. The only interfaces exported are the PCIe and the optical interface of the DDCC, which are not relevant to the TSF. Furthermore, no interface is exported which can alter the operation of the TOE since the TOE has been manufactured to physically enforce its policies and would have to be physically modified to change its behavior and violate the TSF. Since the TOE environment is assumed to provide adequate physical protection it is essentially impossible to modify the TOE.

Logically, the DDCC is protected by limiting the capabilities of its exported interfaces to support only network traffic. No reconfiguration capabilities are provided through any of its exported interfaces. The TOE operates at the physical level which is below the level or protocols or binary logic, so it is unaffected by buffer content or network traffic.

Given the assumption that all relevant data must pass through the TOE, and since all information received by the TOE is unconditionally subject to its unidirectional information flow policy, there is no path present to bypass this security mechanism. There is only one path for information flow through each Owl DualDiode Communication Card, and that path only allows unidirectional information flow across the card. As there is physically only one path available for information flow, that path cannot be bypassed.

For the unidirectional flow to occur across a given DDCC, the DDCC must function correctly. If a DDCC is not functioning or is malfunctioning, no information flow occurs in either direction, which is an inherently secure state. The Send-Only DDCC only allows information to flow from the host system across the card to the external optical interface. The Receive-Only DDCC only allows information to flow from the external optical interface across the card to the host system.

The Owl DualDiode System becomes part of the security domains of the two separate host systems for its own execution. The Owl DualDiode System works in conjunction with the separation that exists between the security domains of two separate host networks. The security domain in which each Owl DDCC is hosted protects the DDCC from interference and tampering by untrustworthy subjects. Furthermore, each DDCC protects itself by not exporting any interface that can be used to modify the TOE Security Functions (TSF) of the DDCC. The only interfaces exported are the PCIe interface and the optical interface of the DDCC, which are not relevant to the TSF. No interface is exported which can alter the operation of the TOE since the TOE has been manufactured to physically enforce its policies and would have to be physically modified to violate the TSF.

- These activities are documented in:
    - The Owl DualDiode Version 7 – Functional Specification
    - The Owl DualDiode Version 7 – High Level Design

The Configuration management assurance measure satisfies the following EAL 2 assurance requirements:

- ADV_ARC.1
- ADV_FSP.2
- ADV_TDS.1

6.2.2 Guidance Documents (AGD)

Owl provides administrator and user guidance on how to utilize the TOE security functions and warnings to administrators and users 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. The Guidance Documents for the TOE are:

- Owl Version 7 Card (Type 7000) OEM Installation Manual

Owl may provide numerous additional documents describing all facets of the design of the TOE. In particular, they have a functional specification that describes the accessible TOE interfaces; a high-level design that decomposes the TOE architecture into subsystems and describes each subsystem and their interfaces; a low-level design that further decomposes the TOE architecture into modules and describes each module and their interfaces; and, correspondence documentation that explains how each of the design abstractions correspond from the TOE summary specification in the Security Target to the actual implementation of the TOE. Furthermore, Owl has a security model that describes each of the security policies implemented by the DualDiode. Of course, the implementation of the TOE itself is also available as necessary.

These activities are documented in:

- Owl Version 7 Card (Type 7000) OEM Installation Manual
- The Owl DualDiode Version 7 – Functional Specification
- The Owl DualDiode Version 7 – High Level Design

The Guidance Documents assurance measure satisfies the following EAL 2 assurance requirements:

- AGD_OPE.1
- AGD_PRE.1

6.2.3 Life cycle support (ALC)

The well-defined development tools used in the creation of the TOE during the life-cycle process help yield consistent and predictable results to deliver quality products that meet the TSF. This life-cycle support plan of the TOE is defined by a series of documents listed below that define the configuration management, life-cycle management and documented procedures that control and track changes made to the TOE. Tools used to design, develop, configure and upgrade the TOE are used throughout the life-cycle process. These tools used in the design and development are strictly controlled, maintained and supported with the help of automated tools contained in a protected secure development environment that provides confidentiality and integrity of the TOE.

These activities are documented in:

- The Owl DualDiode Version 7 Life-Cycle
- Owl Version 7 Card (Type 7000) OEM Installation Manual
- The Owl DualDiode Version 7 – Functional Specification
- The Owl DualDiode Version 7 Configuration Management Plan
- The Owl DualDiode Version 7 – Tests
- The Owl DualDiode Version 7 – Tests Results
- Testing the Security Features of the DualDiode
- Test Report

The Life cycle support assurance measure satisfies the following EAL 2 assurance requirements:

- ALC_CMC.2
- ALC_CMS.2

- ALC_DEL.1
- ASE_CCL.1
- ASE _ECD.1
- ASE _INT.1
- ASE _OBJ.2
- ASE_REQ.2
- ASE_SPD.1
- ASE_TSS.1

6.2.4 Tests (ATE)

Owl has a test plan that describes how each of the necessary security functions is tested, along with the expected test results. Owl has documented each test as well as an analysis of test coverage and depth demonstrating that the security aspects of the design evident from the functional specification and high-level design are appropriately tested. Actual test results are created on a regular basis to demonstrate that the tests have been applied and that the TOE operates as designed.

These activities are documented in:

- The Owl DualDiode Version 7 – Tests
- The Owl DualDiode Version 7 – Tests Results
- Testing the Security Features of the DualDiode
- Test Report

The Tests assurance measure satisfies the following EAL 2 assurance requirements:

- ATE_COV.2
- ATE_FUN.1
- ATE_IND.2

6.2.5 Vulnerability assessment (AVA)

The TOE administrator and user guidance documents describe the operation of DualDiode and how to maintain a secure state. These guides also describe all necessary operating assumptions and security requirements outside the scope of control of the TOE. They have been developed to serve as complete, clear, consistent, and reasonable administrator and user references. Furthermore, Owl has conducted a misuse analysis demonstrating that the provided guidance is complete.

Since no permutation or probabilistic security mechanisms have been identified, there is no applicable analysis.

Owl performs regular vulnerability analyses of the entire TOE (including documentation) to identify weaknesses that can be exploited in the TOE.

The Vulnerability assessment assurance measure satisfies the following EAL 2 assurance requirements:

- ADV_VAN.2

7 Protection Profile Claims

There are no Protection Profile claims.

Owl Computing Technologies, Inc (OwlCTI) certifies a specific family of network security products that rely on hardware technology to enforce one-way information flow control security policy; also known generally as Data

Diodes. Owl Data Diode products feature hardware-enforced sender component and a separate hardware-enforced receiver component, and are marketed as "DualDiode" products.

For OwlCTI, CC certification provides a valuable form of Independent Verification and Validation (IV&V) for Owl Data Diode security features, even in the absence of a Protection Profile. No Protection Profile (PP) has ever existed for one-way data transfer systems.

8 Rationale

This section provides the rationale for completeness and consistency of the Security Target. The rationale addresses the following areas:

- Security Objectives;
- Security Functional Requirements;
- Security Assurance Requirements;
- Strength of Functions;
- Requirement Dependencies;
- TOE Summary Specification; and,
- PP Claims.

8.1 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.

8.1.1 Security Objectives Rationale for the TOE and Environment

This section provides evidence demonstrating the coverage of organizational policies and usage assumptions by the security objectives.

	P.ONEWAY	T.WRONGWAY	A.ADMIN	A.CONNECTION	A.PHYSICAL	T.FAILURE	T.OLD_INF	T.TAMPER	A.NETBREAK	A.GUIDE
O.READONLY	X	X				X				
O.WRITEONLY	X	X				X				
OE.ADMIN			X					X		
OE.CONNECTION				X						
OE.PHYSICAL					X			X		
O.TAMPER_SEALS								X		
O.NON_ROUTABLE	X						X			
OE.GUIDE										X
OE.NETBREAK	X								X	
OE.EMISSION					X					

Table 8 Environment to Objective Correspondence

8.1.1.1 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: The TOE changes any layer data pertaining to the source domain before it is transmitted through the send-only DDCC using a Owl-proprietary transfer protocol.
- OE.NETBREAK: The TOE is the only way of interconnecting the source network and destination network. The administrative staff shall install and operate the TOE to insure the integrity and confidentiality is maintained between the source network and destination network.

8.1.1.2 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.

8.1.1.3 T.FAILURE

The DDCC 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.READ_ONLY: Interfaces of the TOE designated as receive-only can only receive and not send any information. In the event of a single or multiple component failure the TOE may not be operational and therefore by default preserve TSF.
- O.WRITE_ONLY: Interfaces of the TOE designated as send-only can only send and not receive any information. In the event of a single or multiple component failure the TOE may not be operational and therefore by default preserve TSF.

8.1.1.4 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: The TOE changes any layer data pertaining to the source domain before it is transmitted through the send-only DDCC using a Owl-proprietary transfer protocol.

8.1.1.5 T.TAMPER

An attacker tampers with the DDCC during delivery and /or after installation that removes any restrictions of the TOE in order to compromise the confidentiality of the destination side.

This Threat is satisfied by ensuring that:

- O.TAMPER_SEALS The DDCC is shipped with tamper evident devices and is marked and documented for verification of authenticity of the TOE. Authorized personnel will receive the documentation for use in the verification process.

- OE.ADMIN: Authorized personnel will use the documentation provided by OwlCTI to verify the authenticity and integrity of the TOE.
- OE.PHYSICAL: The facility that receives the TOE is responsible for the physical protection of the TOE. This includes verification that the TOE was received with the physical tamper evident seals intact and physical markings and attributes match those listed in OwlCTI documentation.

8.1.1.6 A.NETBREAK

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 TOE is the only way of interconnecting the source network and destination network. The administrative staff shall install and operate the TOE to insure the integrity and confidentiality is maintained between the source network and destination network.

8.1.1.7 A.GUIDE

Authorized personnel shall ensure the TOE is delivered, installed and administered in a manner that maintains security. The appropriate security authority shall accredit the installation of the Owl DDCC.

This Assumption is satisfied by ensuring that:

- OE.GUIDE: Personnel will ensure that the TOE is installed and administered in accordance to security policies for protecting critical computer equipment and systems. The TOE will be installed as the only flow of information between the two domains. The administrative staff shall install and manage the TOE in a manner that maintains security.

8.1.1.8 A.ADMIN

Authorized personnel that posses the necessary privileges to access the secure side information shall install, administer and use the Owl DDCC by adhering to the security policies and practices regarding the usage of the TOE.

This Assumption is satisfied by ensuring that:

- OE.ADMIN: The environment is responsible to ensure that the administrator will properly adhere to the TOE guidance.

8.1.1.9 A.CONNECTION

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

This Assumption is satisfied by ensuring that:

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

8.1.1.10 A.PHYSICAL

The TOE and its operating environment will be physically protected to a degree commensurate with the value of the information it is intended to protect.

This Assumption is satisfied by ensuring that:

- OE.PHYSICAL: The environment is responsible to ensure that the TOE will be physically protected to a degree commensurate with the value of the information it is intended to protect.

8.2 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.

8.2.1 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.READONLY**	**O.WRITEONLY**	**O.TAMPER_SEALS**	**O.NON_ROUTABLE**
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		
FPT_PHP.1: Passive detection of Physical Attack			X	

Table 9 Objective to Requirement Correspondence

8.2.1.1 O.READONLY

The TOE must ensure that each interface designated as receive-only will only receive and not send 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.

8.2.1.2 O.WRITEONLY

The TOE must ensure that each interface designated as send-only will only send and not receive 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.

8.2.1.3 O.TAMPER_SEALS

The TOE must be designed with visible markings and a means of identification as proof the operation and function of information flow preserve the SF.

This TOE Security Objective is satisfied by ensuring that:

- FPT_PHP.1: The TSF element will be self evident and identifiable if tampering or modifications to the TOE were made to violate the SFs by untrusted individuals.

8.2.1.4 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.

8.3 Security Assurance Requirements Rationale

This ST contains the assurance requirements from the CC EAL 2 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.

8.4 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.1; 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.1
FPT_PHP.1	None	None
ADV_ARC.1 Security Architecture Description	ADV_FSP.1 Basic functional specification ADV_TDS.1 Basic design	ADV_FSP.1 ADV_TDS.1
ADV_FSP.2 Security-enforcing functional specification	ADV_TDS.1 Basic design	ADV_TDS.1
ADV_TD.1 Basic design	ADV_FSP.2 Security-enforcing functional specification	ADV_FSP.2
AGD_OPE.1: Operational user guidance	ADV_FSP.1 Basic functional specification	ADV_FSP.1
AGD_PRE.1: Preparative procedures	None	None
ALC_CMC.2 Use of a CM system	ALC_CMS.1 TOE CM coverage	ALC_CMS.1
ALC_CMS.2 Parts of the TOE CM coverage	None	None
ALC_DEL.1 Delivery procedures	None	None
ASE_CCL.1 Conformance claims	ASE_INT.1 ST introduction ASE_ECD.1 Extended components definition ASE_REQ.1 Stated security requirements	ASE_INT.1 ASE_ECD.1 ASE_REQ.1
ASE_ECD.1 Extended components definition	None	None
ASE_INT.1 ST introduction	None	None
ASE_OBJ.2 Security objectives	ASE_SPD.1 Security problem definition	ASE_SPD.1
ASE_REQ.2 Derived security requirements	ASE_OBJ.2 Security objectives	ASE_OBJ.2

	ASE_ECD.1 Extended components definition	ASE_ECD.1
ASE_SPD.1 Security problem definition	None	None
ASE_TSS.1 TOE summary specification	ASE_INT.1 ST introduction ASE_REQ.1 Stated security requirements ADV_FSP.1 Basic functional specification	ASE_INT.1 ASE_REQ.1 ADV_FSP.1
ATE_COV.1: Evidence of coverage	ADV_FSP.2 Security-enforcing functional specification ATE_FUN.1 Functional testing	ADV_FSP.2 ATE_FUN.1
ATE_FUN.1: Functional testing	ATE_COV.1 Evidence of coverage	ATE_COV.1
ATE_IND.2: Independent testing – sample	ADV_FSP.2 Security-enforcing functional specification AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures ATE_COV.1 Evidence of coverage ATE_FUN.1 Functional testing	ADV_FSP.2 AGD_OPE.1 AGD_PRE.1 ATE_COV.1 ATE_FUN.1
AVA_VAN.2 Vulnerability analysis	ADV_ARC.1 Security architecture description ADV_FSP.2 Security-enforcing functional specification ADV_TDS.1 Basic design AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures	ADV_ARC.1 ADV_FSP.2 ADV_TDS.1 AGD_OPE.1 AGD_PRE.1

Table 10 Security Requirement Dependency Analysis

8.5 Explicitly Stated Requirements Rationale

There are no explicitly stated requirements in this Security Target.

8.6 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
FPT_PHP.1		X

Table 11 Security Functions vs. Requirements Mapping

8.7 PP Claims Rationale

See Section 7, Protection Profile Claims.

9 Revision History

Version	Date	Changes / Reason for changes
r01a	8/21/2013	Original draft document for the DDCC Ver. 7
r01b	9/5/2013	Formatting and editing corrections.
r01c	9/18/2013	Editing corrections
r01d	11/6/2013	Editing corrections to Section 1.3, 1.3.1, 1.4, 1.5.2, 1.6, 17, 2.1.1, 2.1.2, 3.1, 3.3, 6.1.1, 8.1.1.1, 8.2.1.6, 8.2.1.7, 8.1.1.3, 8.4. Table 1, 2, 3, 5. Added Table 4.
r01e	11/21/2013	Edited 1.7, 1.71, 1.7.1.1, 1.7.1.2, 1.8, 1.9, 2.1.2, 2.1.3, 6.2.18.2.1.3, 8.2.1.6, 8.2.1.7, Added mapping for FPT_PHP.1
r01f	1/2/2014	Changed Figure 4, Edited 1.7.2.1, 1.7.2.2, 1.8, 2.1.3. Removed all occurrences of O.Protect, Edited FPT_PHP.1. Removed AGD.PRE.1, AGD.OPE.1 from Table 9. Removed 2.1.2, Removed all occurrences of FDP_RIP.2
r01g	1/7/2014	Removed Full Residual Information Protection in 1.7.2.1, defined 8.1.1.3, 8.1.1.4, 8.1.1.5, 8.1.1.6 – 10 to match sec. 3, Removed O.PROXY from sec. 4.1, 8.1.1.4 and Table 8 & 9, Deleted 8.2.1.5. Edited all occurrences of FDP_IFF.5.
r01h	2/11/2014	Removed all occurrences of O.PROTOCOL_BREAK, Edit 1.6
r01i	4/28/2014	Edited sentence to remove the mention of Red Hat and CentOS and replace with OwlCTI tested and approved in section 1.7.1.
r01j	4/29/2104	Editing and formatting to add clarity in section 1.7.1.
r01k	12/11/2014	ST information update in 1.1, Updated table in 5.1, Edit correction in 6.0
r01l	12/11/2014	Minor editing, remove confidential and proprietary

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