



Owl DualDiode® Communication Cards (002 & 010) M-Series Data Diode Family

Security Target

Common Criteria - EAL 2 Certification

Document: OwlDualDiodeVer-002_010-Family-SecurityTarget-EAL2_v01m.docx
Version: 01m
Date: September 2016

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

TABLE OF CONTENTS

SECURITY TARGET.....1

COMMON CRITERIA - EAL 2 CERTIFICATION.....1

1 SECURITY TARGET INTRODUCTION (ASE_INT.1)4

1.1 SECURITY TARGET REFERENCE.....4

1.2 TOE EVALUATION CONFIGURATION5

1.3 TOE OVERVIEW5

1.4 DOCUMENT OVERVIEW8

1.5 CONVENTIONS, TERMINOLOGY, ACRONYMS8

 1.5.1 CONVENTIONS8

 1.5.2 TERMINOLOGY, ACRONYMS AND ABBREVIATIONS9

1.6 TOE DESCRIPTION11

1.7 TOE PHYSICAL ARCHITECTURE.....12

 1.7.1 PHYSICAL BOUNDARIES13

 1.7.2 LOGICAL BOUNDARIES.....14

1.8 TOE DOCUMENTATION14

2 CONFORMANCE CLAIMS (ASE_CCL.1)14

2.1 COMMON CRITERIA CONFORMANCE CLAIM.....14

 2.1.1 PROTECTION PROFILE CONFORMANCE CLAIM15

 2.1.2 PACKAGE CLAIMS.....15

3 SECURITY PROBLEM DEFINITION (ASE_SPD.1)15

3.1 ORGANIZATIONAL SECURITY POLICIES15

3.2 THREATS15

3.3 ASSUMPTIONS15

4 SECURITY OBJECTIVES (ASE_OBJ.2)16

4.1 SECURITY OBJECTIVES FOR THE TOE.....16

4.2 SECURITY OBJECTIVES FOR THE TOE ENVIRONMENT16

5 SECURITY REQUIREMENTS (ASE_REQ.2).....17

5.1 TOE SECURITY FUNCTIONAL REQUIREMENTS17

 5.1.1 USER DATA PROTECTION (FDP).....17

 5.1.2 PROTECTION OF THE TSF (FPT).....18

5.2 TOE SECURITY ASSURANCE REQUIREMENTS18

6 TOE SUMMARY SPECIFICATION (ASE_TSS.1)19

6.1 TOE SECURITY FUNCTIONS19

 6.1.1 USER DATA PROTECTION.....19

 6.1.2 PROTECTION OF THE TSF20

6.2 TOE SECURITY ASSURANCE MEASURES.....21

 6.2.1 DEVELOPMENT.....21

 6.2.2 GUIDANCE DOCUMENTS (AGD)22

 6.2.3 LIFE CYCLE SUPPORT (ALC).....22

 6.2.4 TESTS (ATE)23

 6.2.5 VULNERABILITY ASSESSMENT (AVA).....23

7 RATIONALE.....23

7.1 SECURITY OBJECTIVES RATIONALE24

 7.1.1 SECURITY OBJECTIVES RATIONALE FOR THE TOE AND ENVIRONMENT24

7.2 SECURITY REQUIREMENTS RATIONALE.....26

 7.2.1 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE.....26

7.3 SECURITY ASSURANCE REQUIREMENTS RATIONALE27

7.4 REQUIREMENT DEPENDENCY RATIONALE.....28

7.5 EXPLICITLY STATED REQUIREMENTS RATIONALE28

7.6 TOE SUMMARY SPECIFICATION RATIONALE29

8 REVISION HISTORY30

LIST OF TABLES

Table 1 ST Identification 4

Table 2 TOE Hardware Products 4

Table 3 TOE Specification and Identification..... 5

Table 4 Acronyms & Abbreviations 11

Table 5 TOE Security Functional Components 17

Table 6 EAL 2 Assurance Components 18

Table 7 Environment to Objective Correspondence 24

Table 8 Objective to Requirement Correspondence 26

Table 9 Security Requirement Dependency Analysis..... 28

Table 10 Security Functions vs. Requirements Mapping..... 29

1 Security Target Introduction (ASE_INT.1)

1.1 Security Target Reference

ST Title	Owl DualDiode® Communication Cards (002 & 010) M-Series Data Diode Family Security Target
ST Version	01m
ST Publication Date	9/27/16
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	Owl DualDiode® Communication Cards (002 & 010) M-Series Data Diode Family

Table 1 ST Identification

The TOE consists of one of the cards in the following security hardware products:



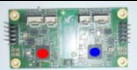





TOE DESCRIPTION	TOE PART NUMBER	PICTURE OF TOE	DATA SPEED (MAX)	CARD SIZE	ENCLOSED PRODUCTS	
Owl 010-Rev E DualDiode® Extended Temperature Communication Cards	Owl 010-150-RevE		104 Mbps	3 in x 1.50 in (7.6 cm x 3.8 cm)	MPDS USB	
Owl DualDiode® 002 Extended Temperature Communication Card	002TV-Rev A 02		2 Mbps	3 in x 1.50 in (7.6 cm x 3.8 cm)	MPDS USB-002 / 002TV Mobile CDS	
Owl DualDiode® 002 Extended Temperature Communication Card	002PD-Rev A 02		2 Mbps	3 in x 1.50 in (7.6 cm x 3.8 cm)	MPDS RS-232	
Owl WSCDS DualDiode® Extended Temperature Communication Card	WCDS 002 Rev B		2 Mbps	39.89 mm x 26.04 mm	MCDS (Miniaturized Cross Domain Solution)	

Table 2 TOE Hardware Products

1.2 TOE Evaluation Configuration

<i>TOE Identity</i>	<i>Required External Connection</i>	<i>Data Transfer Rates</i>	<i>Interface (bus) Type</i>	<i>Power Requirements</i>
Owl 010-150-RevE	USB [A]	10 Mbps - 104 Mbps	USB 2.0	5 VDC +0.25V / -0.55V 100 mA to 500 mA
002TV-Rev A 02	USB [A]	2 Mbps	USB 2.0	5 VDC +0.25V / -0.55V 100 mA to 500 mA
002PD-Rev A 02	Serial DB9	2 Mbps	RS-232	5 VDC +0.25V / -0.55V 100 mA to 500 mA
WCDS 002 Rev B	USB [A]	2 Mbps	USB 2.0	5 VDC +0.25V / -0.55V 100 mA to 500 mA

Table 3 TOE Specification and Identification

OwlCTI provides M-Series DDCC software drivers which when installed on the host system allows the system to communicate with the TOE and employ the TOE Security Functions (TSF) to pass data. The M-Series DDCC device drivers are provided by OwlCTI but are not a part of the TOE. OwlCTI currently has M-Series DDCC device drivers available for Linux OS versions 4, 5 and 6.

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

Performance and security testing of the M-Series DDCC employed two Linux OS systems; Red Hat ® and CentoOS ®, the OS is outside of the TOE, to verify the TSF deterministic one-way unidirectional flow of information.

1.3 TOE Overview

The Target of Evaluation (TOE) is the Owl M-Series DualDiode® Communication Card (DDCC) which consists of the Owl 010-Rev E DualDiode® Communication Card, the Owl 002 Communication Card and the WSCDS Communication Card, which are designed and manufactured by Owl Computing Technologies, Incorporated (OwlCTI). The only deterministic function performed by the miniaturized Owl M-Series DualDiode® Communication Cards is to allow information to flow one-way-only. The DDCC provide an absolute deterministic one-way unidirectional flow of any data and information between a source domain, the USB or serial communication sending host system, tablet, Android, laptop, PDA or network to a destination domain, the USB or serial communication receiving host system or network. Thereby protecting the destination host or network from any potential leaks of information or potential network probing attacks. This shows the TOE satisfies the 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".

The 010 and 002 DDCC are used in the Owl 1U tamper resistant server platforms that use the TOE for one-way unidirectional flow of data between separate network domains. Specifically the hardware is designed to be contained within the OPDS-100, OCDS-100 and OPDS-100D server product line where the DDCC is connected to the CPUs compliant USB 2.0 interface or a RS-232D compliant serial communication interface. The TOE also provides additional security in the following area:

- non-routable protocol break (The TOE only passes data packets at the physical level. No standard transport or networking layer protocols are applied or employed to the data packet to make the information flow through the TOE.)
- confined interface (The TOE has no exterior interface that would connect to a domain that would present an interface for modifying the operational programming)

OwlCTI 010 and 002 products are proven deterministic data diode cards that mitigate network attack threats by restricting information flow to a one-way data transfer only. The data diode one-way policies that are implemented with a hardware pipeline cannot be reconfigured by any software reconfiguration.

The Owl 010 and 002 DualDiode® Communication Cards is the core to a secure one-way only unidirectional flow of information. OwlCTI has created device drivers that provide the interface between a computer serial or USB bus and the Owl M-Series DDCC which are dependent on Operating Systems (OS) such as Red Hat® or CentoOS® Linux® OS. OwlCTI drivers provide the necessary device interrupt routines required for applications to use the M-Series 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 less 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 more 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) 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.

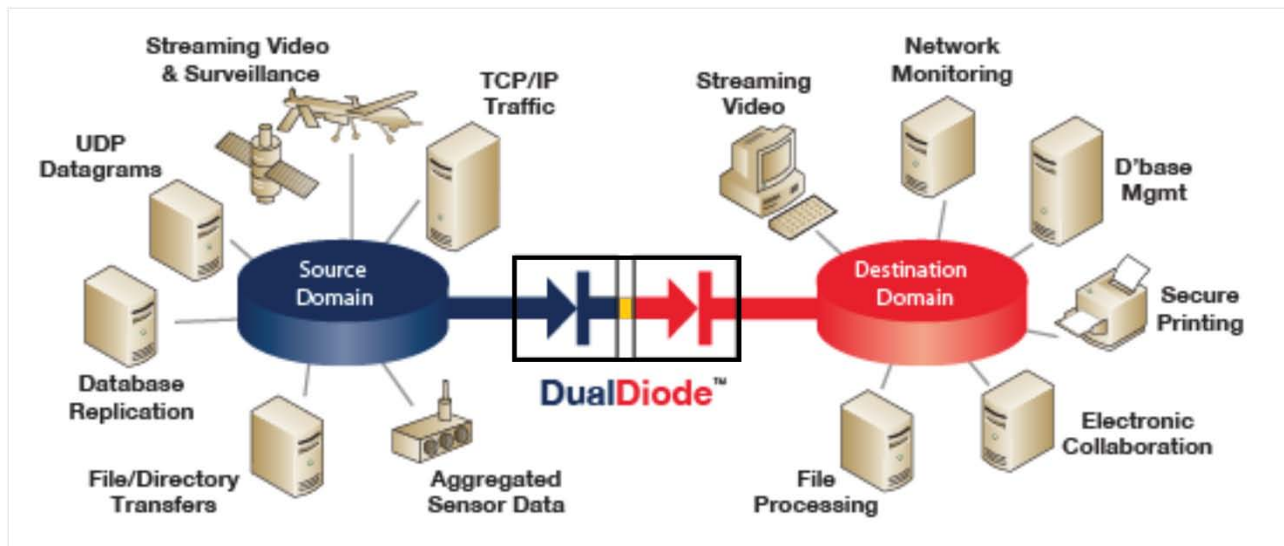


Figure 1 – Owl M-Series DualDiode® Communication Card Concept

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	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
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 half of the card must be affixed to a receiving host system. See Receiving Host.
DualDiode®	Deployment of a USB or serial Data Diode protection mechanism to enforce one-way transfer security policy at either end of cross-domain connection.
DDCC	M-Series DualDiode® Communications Card: There are several variations of the DualDiode® Communication Card, the Owl 010 DDCC variant and the Owl 002 DDCC variant. The DDCCs are manufactured to Owl's specifications and use commercial-off-the-shelf (COTS) Communication Card components. The Send-Only half of the DualDiode® Communications Card only has the FPGA imaged as a Segmentation Controller and Framer installed for sending information through the transmission side of the isolator. The Receive-Only half of the DDCC has the FPGA installed and imaged as a Reassembly Controller for only receiving information. The Send-Only DDCC will only export pulses of photons by the Transmitter from electrical voltages. The Receive-Only half of the DDCC will only import pulses of photons received at the detector and converts the pulses into electrical voltages.
DualDiode® Host	A computer system or network which has a DDCC 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 Universal Serial Bus (USB) or serial bus. See Host.
EAL	Evaluation Assurance Level
FPGA	Field Programmable Gate Array or microcontroller is a COTS semiconductor device containing programmable logic components, interconnects, and memory. When deployed, the FPGA connects directly to the USB or serial 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 Send-Only DDCC circuit 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.

Isolator	An optocoupler also called a photocoupler or optical isolator or RF coupler is a component that transmits signals between isolated circuits using light or electromagnetic pulses. An isolator contains a source or electromagnetic emitter, and closed channel or dielectrical channel and an electromagnetic sensor which detects incoming photons and modulates electric current flowing from an external power source.
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 010 and 002 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.
Mbs	Megabits per second or 1,000,000 bits per second connection speed that will transfer approximately 100 pages of plain text per second
Platform Flash	Platform Flash is a Programmable Read-Only Memory (PROM) used to load initialization data used by the Segmentation Controller (in the Send-Only DDCC circuit) or by the Reassembly Controller (in the Receive-Only DDCC circuit). Platform Flash is written once, in read/write-protection mode, during the DDCC manufacturing process 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 USB or serial interface of the DDCC.
PP	Protection Profile (Does not exist for one way packet transfer systems)
Reassembly Controller	Exclusive to the Receive-Only DualDiode® Communication Card circuit, 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 half of the DDCC card that contains the Receive-Only DDCC circuitry that only allow information for transfer to flow from its isolator interface across the Receive-Only DDCC circuitry to the host system. All information presented for transfer to the Receive-Only DDCC circuit is subject to the unconditional unidirectional information flow. No information is able to flow from the host system across the Receive-Only DDCC circuit and through the isolator 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 circuit.
RS-232D	A subset of the RS-232 is the RS-232D that defines the pin out requirements of a DB-9 connector that is and for use with adapters for RS-232 connectors.
Segmentation Controller	Exclusive to the Send-Only DualDiode® Communication Card circuit, 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 circuitry.
Sending Host	A host system or network which is connected to the Send-Only DDCC circuit. The Sending Host is to send information through the USB or serial interface of the Send-Only DualDiode® Communication Card circuit. 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 connected to the USB or serial interface of the Owl Send-Only DualDiode® Communication Card circuit. See Sending Host.
Send-Only DDCC	The Send-Only DDCC circuit only allows information for transfer to flow from the host system across the DDCC through the isolator. All information presented to the Send-Only DDCC circuit is subject to the unconditional unidirectional information flow. No information is able to flow from outside the Send-Only DDCC circuit through the isolator across the Send-Only DDCC and into the host system. This non-bypassability of the TOE is enforced at the physical level.
Serial / Serial Communications	A standard for the serial port communication and transmission of data that defines the signals for connecting data transmission equipment and data circuit terminating equipment. Data transmitted serially is defined as transmitting data one bit at a time using the transmit and receive line on the connector. Refer to RS-232D.
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation – The Owl DualDiode® Communication Cards (002 & 010) M-Series Data Diode Family
TSF	TOE Security Function
USB	Universal Serial Bus is a standardized computer peripheral connection to communicate and supply electric power.
WSCDS	Worlds Smallest Cross Domain Solution is the smallest of the 002 Owl M-Series DualDiode® Communication Cards

Table 4 Acronyms & Abbreviations

1.6 TOE Description

Owl's Security Target focuses on the M-Series DualDiode® family of products, which comprises a specific set of configuration variants that include one variable and three different speed classes, two different form factors, and special circuit components capable of operating over extended temperature ranges.



Figure 2 - Owl 010-Rev E DualDiode Communication Card

Significantly, Owl M-Series DualDiode® Communication Cards implement the same TOE Security Functions as all previous CC-certified DualDiode® card versions 1 through 7.

The TOE is a single printed circuit board (PCB) that contains two separate electrically isolated circuits. One is the Owl Send-Only DDCC circuit and the second circuit is the Owl Receive-Only DDCC circuit. These two circuits paired together on one PCB form a logical hardware suite of two cards in one. The TOE consists of the 002 DDCC series that has a maximum operating transfer rate of 2 Megabits per second (Mbs) and the 010 DDCC series that operate from 10

Megabits per second to a high of 104 Megabits per second. This PCB design grants the TOE the means to securely transfer data one-way-only between a discrete network domain (source domain) to another discrete network domain (destination domain). Any host or hosts server or device that supports a USB or serial interface 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 like a standard serial interface. 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”.

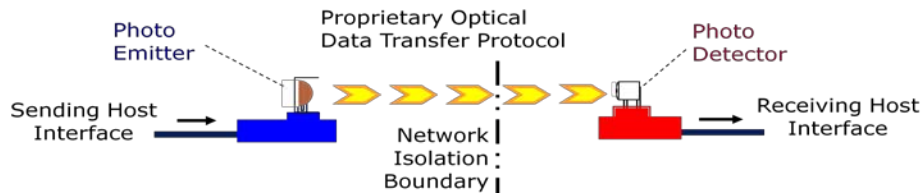


Figure 3 – High Level view of the DualDiode® Interface

Data from the Sending Host is sent through the USB or serial interface using the Owl device driver for the Owl DDCC cards Send-Only DDCC circuit. The device driver will provide a single data structure for the Send-Only DDCC circuitry and control messages indicating the state of the Send-Only DDCC half of the card. The Send-Only DDCC then queues, stages, and frames the data before forwarding it to the transmission side of the Isolator. The Send-Only DDCC Isolator then transmits the packet data. The Send-Only DDCC circuitry does not receive signals from the other half of the TOE as the other half of the Isolator can only receive signals. This is the single function performed by the electrically isolated circuitry of the Send-Only DDCC portion of the TOE.

The data transmitted from the Send-Only DDCC circuit is channeled through the transparent isolation material or air gap. The use of an Isolator 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 Isolator. No ready to receive handling signals are transmitted to the Send-Only DDCC circuit as the Receive-Only portion of the Isolator is photo-sensitive. The receiving portion of the Isolator forwards the packet data to the Receive-Only DDCC portion of the card where it is then reassembled. The reassembled data is then transferred through the USB or serial interface to the Receiving Host. The Receiving Host using the Receive-Only DDCC device drivers is able to take delivery of the information from the Receive-Only DDCC circuitry using the USB or serial 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) M-Series DualDiode® System provides a deterministic 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 M-Series DualDiode® System.

The Target of Evaluation (TOE) comprises one Owl M-Series DualDiode® Communication Card (DDCC). One half of the card is a Send-Only DDCC circuit and the other half is a Receive-Only DDCC circuit. The M-Series DDCCs are manufactured to Owl’s specifications using standard 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 through the universal serial bus. All Owl device driver software are designed, written, and packaged by OwlCTI. Each independent circuit of the M-Series DualDiode® Communication Card is attached to its host system; Send-Only DDCC side is connected to the source host and the Receive-Only side is connected to the destination host, both of which are connected through the Isolator.

The Owl M-Series DDCC design consists of the circuitry for a Send-Only DDCC device and a Receive-Only DDCC combined onto a single PCB. The Send-Only DDCC circuitry is electrically isolated from the Receive-Only DDCC circuitry.

The Send-Only DDCC half of the card exports signal pulses converted by the transmission side of the Isolator from electrical voltages. The Receive-Only DDCC half of the card imports those signal pulses received at the detector side of the Isolator of the Receive-Only DDCC and converts the signal pulses received into electrical voltages.

In the Send-Only DDCC circuit, the TSF Module connects to the Universal Serial Bus Device of the host through which it will transmit the information packets to the Send-Only DDCC half of the card. The input transmission of information will be buffered, managed and scheduled by the module before being sent to the transmitter side of the Isolator. The design used on the Send-Only DDCC circuit has no traces to the input and output for the receiver portion of the Isolator.

The Send-Only DDCC module of the TOE has designed circuitry that removes any circuit traces near the Receive-Only DDCC module and vice versa for the Receive-Only DDCC module thus forming a 2.5 mm electrical moat. Each was designed to remove any possible physical connection between the receive side of the card with the send side and only allow a connection through the Isolator.

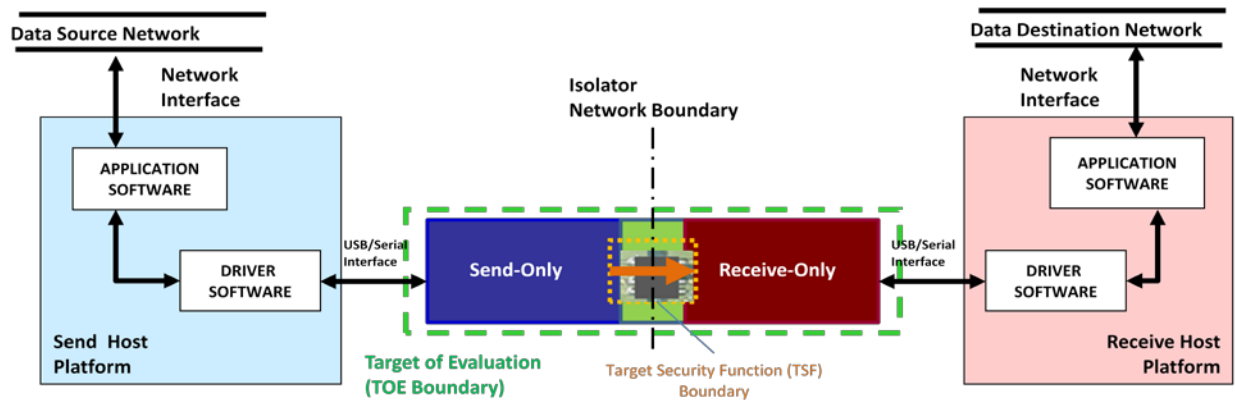


Figure 4: TOE Architecture

1.7.1 Physical Boundaries

The TOE is used to isolate two information processing domains; the Send-Only DDCC half of the card that is affixed to the Data Source information processing domain and the Receive-Only DDCC half of the card that is affixed to the Data Destination information processing domain.

The TOE consists of a Send circuit and Receive circuit on a single DDCC card tied together through an Isolator. The Send-Only DDCC portion and Receive-Only DDCC portion must be connected to the USB or serial interface of the host server that meets the minimum requirements listed in **Table 3**. The server must be running an OwlCTI tested and approved Operating System to use the OwlCTI device drivers. A list of the Operating Systems that have been tested and approved as compatible with OwlCTI drivers are found in the installation guides. Though the M-Series DDCC models minimum requirements for a host may vary they share a common device 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 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.

1.7.2 Logical Boundaries

This section will summarize the TOE Security Functions provided by the Owl M-Series DualDiode® Communication Cards.

1.7.2.1 User data protection

The Owl M-Series DualDiode® Communication Card passes data from the Send-Only DDCC circuit to the Receive-Only DDCC circuit and provides the following security features:

Information Flow Control – The TOE directly interfaces with the source host and the destination host to transmit information in a unidirectional flow through an isolator. The Send-Only DDCC circuit of the TOE is only capable of transmitting information and conversely the Receive-Only DDCC circuit of the TOE is only capable of receiving information.

Limited Illicit Information Flows – By design the TOE does not add a padding layer of information that could disclose the source or destination of the data being transmitted. Therefore the TOE helps in maintaining the confidentiality of the domains and prevents any illicit flow of information between the domains.

1.7.2.2 Protection of the TSF

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

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

1.8 TOE Documentation

While the TOE is substantially defined by the Owl M-Series DualDiode® Communication Card, 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:

- Miniaturized Perimeter Defense Solution (MPDS) RS-232 Quick Start Guide
- Miniaturized Perimeter Defense Solution (MPDS) USB Quick Start Guide
- Miniature Cross Domain Solution (MCDS-USB) and 002TV Quick Start Guide

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 M-Series DualDiode® TOE is conformant with Security Assurance Requirement:

- EAL2 conformant.

3 Security Problem Definition (ASE_SPD.1)

The TOE is designed for environments where a deterministic one-way flow of information 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.FAILURE The DDCC has a hardware failure that allows data to flow through the TOE from the destination side to the source 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.NON_BYPASSABLE 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 external interface designated as receive-only will only receive and not send information.

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

O.NON_DISCLOSURE The TOE must neither disclose information about the source network to the destination network nor disclose information about the destination network to the source network.

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 M-Series DDCC. The administrative staff shall install and manage the TOE in a manner that maintains security.

OE.NON_BYPASSABLE The TOE is the only way of interconnecting the source host or network and destination host or 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.3: Limited illicit information flows	FDP_IFC.1
FPT: Protection of the TSF	FPT_FLS.1: Failure with Preservation of Secure State	No Dependencies

Table 5 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 connection of the each Read-Only module interface and Send-Only module interface of the 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: **[the information flow is only permitted to pass through the Send-Only DDCC circuitry to the Receive-Only DDCC circuitry to pass the data packets to the destined domain interface]**.

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 Limited illicit information flows (FDP_IFF.3)

FDP_IFF.3.1 The TSF shall enforce the **[unidirectional information flow SFP]** to ~~limit the capacity of forbid~~ **[TOE generated network routing information flow]** to a ~~assignment: maximum capacity~~.

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: **[any hardware failure]**.

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 6 EAL 2 Assurance Components

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 isolator with one-way enforcement at each end)
- (3) fail-secure (the Send-Only and Receive-Only power and components are isolated and independent)

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 M-Series 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's hardware is designed to enforce the unidirectional information flow at the component level; FPGA and Isolator. 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 M-Series DualDiode® Communication Card physically can only provide information traffic flow in one direction through the card. The Send-Only DDCC circuitry allows only the one-way transfer of information from a host system through the M-Series DDCC to outside the host system, and there is no transfer of information from outside the host system, through the M-Series DDCC into the host system. The Receive-Only DDCC circuitry allows only the one-way transfer of data from outside a host system through the M-Series 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.

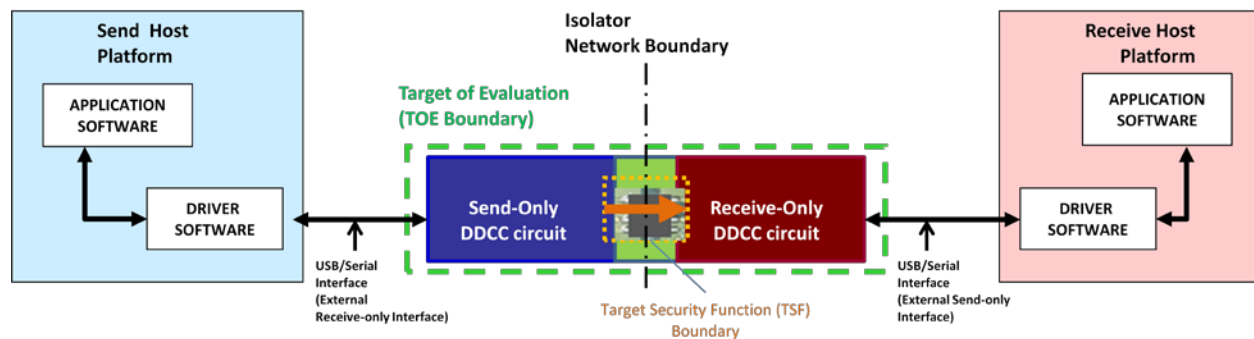


Figure 5 – Owl M-Series DualDiode® Communication Card Interface with Host Concept

If a host system attempts to receive information using the Send-Only DDCC half of the M-Series DDCC, there will be no transfer of information from outside the host system, through the Send-Only DDCC circuitry into the host system. The host system will be connected to the external interface of the Send-Only DDCC circuit which is designed to receive data from the host. In the Send-Only DDCC circuit, the output of the transmitter side of the Framer is connected to the photo-transmitter of the Isolator. Furthermore, the Send-Only DDCC circuitry only connects to the host-system power and to the photo-transmitter of the Isolator. When the host system does not receive information using the Send-Only DDCC circuit, 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 circuit.

If a host system attempts to send information to the exterior interface (USB/serial) of the Receive-Only DDCC half of the M-Series DDCC, there will be no transfer of information through the Receive-Only DDCC half over to the Send-Only DDCC half to be transmitted to an outside host system. In the Receive-Only DDCC circuit, the host is connected to the external communications interface where the data is sent out. The internal circuitry of the Receive-Only DDCC is communications interface connects to the data buffer and Reassembler which is connected to the detector side of the Isolator. Furthermore, the Receive-Only DDCC half of the M-Series DDCC only connects the host-system power to the photo-detector side of the Isolator which is unable to transmit data to the other side of the Isolator. The host system that attempted to send information through the Receive-Only DDCC half of the M-Series DDCC will not receive a response indicating no information was sent. The unidirectional informational flow policy is maintained given no data was sent through the Receive-Only DDCC half of the M-Series 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 circuit connected to the Receive-Only DDCC circuit. The Send-Only DDCC circuit directly interfaces with the source host to only transmit information through the Isolator. No external electronic or light signals are admitted back through the Send-Only DDCC circuitry to the source host. Conversely, the Receive-Only DDCC circuit directly interfaces with the destination host and only receives information through the Isolator. The Receive-Only DDCC circuitry 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 circuitry only allows information for transfer to flow from the host system across the DDCC through the Isolator. All information presented to the Send-Only DDCC circuit is subject to the unconditional unidirectional information flow. No information is able to flow from outside the Send-Only DDCC circuit through the Isolator across the Send-Only DDCC circuit and into the host system. Conversely, the Receive-Only DDCC circuitry only allows information for transfer to flow from the Isolator across the Receive-Only DDCC circuit and to the host system. All information presented for transfer to the Receive-Only DDCC circuit is subject to the unconditional unidirectional information flow. No information is able to flow from the host system across the Receive-Only DDCC circuit and through the Isolator of the Receive-Only DDCC circuit. This non-bypassability of the TOE ensures the SFP is enforced at the physical level.
- FDP_IFF.3: The TOE (a M-Series DDCC) 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. The TOE helps in maintaining the confidentiality of the domains and prevents any illicit flow of information between the domains.

6.1.2 Protection of the TSF

The M-Series DDCC has been designed, developed and implemented so a component module (Send-Only DDCC circuit or Receive-Only DDCC circuit) or hardware failure of any kind will not change the unidirectional flow or create a Fail-Open within the circuit, therefore the SFP will not be violated. This is achieved by designing each component of the TOE as a single purpose communication circuit; Send-Only DDCC circuit or Receive-Only DDCC circuit. 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 it will prevent all data flow; no data will flow forward or backward, between domains thereby preserving the confidentiality and integrity of each domain. The benefit of a hardware based TSF is if portion or component of the TOE malfunctions or loses power, the TOE will never forward information in the reverse (wrong) direction. Just as an electrical circuit when power is lost or a short occurs, no electricity will flow, no data will flow through the TOE, thus providing isolation between domains. Even though the TOE may not be operational it will remain secure.

6.2 TOE Security Assurance Measures

6.2.1 Development

The M-Series 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 USB for the Send-Only and Receive-Only circuitry of the M-Series 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 M-Series 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 of protocols or binary logic, so it is unaffected by buffer content or network traffic.

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 or SCSI communications, etc. and creates a high-efficiency packet format. This high-efficiency packet format optimizes the 104 Mbps 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.

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 M-Series 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.

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 isolator for separation 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 in a small form factor.

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

The Owl M-Series DualDiode® System becomes part of the security domains of the two separate host systems for its own execution. The Owl M-Series 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 USB or serial interfaces 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 M-Series DualDiode® – Functional Specification
 - The Owl M-Series DualDiode® – High Level Design

The Development 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:

- Miniaturized Perimeter Defense Solution (MPDS) USB Quick Start Guide - Ver. 03b
- Miniaturized Perimeter Defense Solution (MPDS) RS-232 Quick Start Guide - Ver. 02b
- Miniature Cross Domain Solution (MCDS-USB) and 002TV Quick Start Guide - Ver. 01b

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 M-Series DualDiode® Configuration Management Plan
- The Owl M-Series DualDiode® Delivery and Operation

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

- ALC_CMC.2
- ALC_CMS.2
- ALC_DEL.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 M-Series DualDiode® Communications Card – Tests
- The Owl M-Series DualDiode® Communications Card – Tests Results
- Testing the Security Features of the DualDiode®
- Test Report

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

- ATE_COV.1
- 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 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; and,
- TOE Summary Specification.

7.1 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.

7.1.1 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	A.NON_BYPASSABLE	A.GUIDE
O.READONLY	X	X				X		
O.WRITEONLY	X	X				X		
O.NON_DISCLOSURE	X							
OE.ADMIN			X					
OE.CONNECTION				X				
OE.PHYSICAL					X			
OE.GUIDE								X
OE.NON_BYPASSABLE	X						X	
OE.EMISSION					X			

Table 7 Environment to Objective Correspondence

7.1.1.1 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_DISCLOSURE: The TOE does not disclose information about the source network to the destination network or vice versa, preventing attackers from using this information to directly attack the networks and bypass the one-way information flow control.
- OE.NON_BYPASSABLE: 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.

7.1.1.2 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.

7.1.1.3 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.

7.1.1.4 A.NON_BYPASSABLE

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.NON_BYPASSABLE: 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.

7.1.1.5 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 M-Series 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.

7.1.1.6 A.ADMIN

Authorized personnel that posses the necessary privileges to access the secure side information shall install, administer and use the Owl M-Series 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.

7.1.1.7 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.

7.1.1.8 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.
- 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

7.2 Security Requirements Rationale

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

7.2.1 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	O.READONLY	O.WRITEONLY	O.NON_DISCLOSURE
SFRs			
FDP_IFC.2: Complete information flow control	X	X	X
FDP_IFF.3: Limited illicit information flows	X	X	X
FDP_IFF.1: Simple security attributes	X	X	X
FPT_FLS.1: Failure with Preservation of Secure State	X	X	

Table 8 Objective to Requirement Correspondence

7.2.1.1 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.3: The TOE must transfer information through the TSF in a unidirectional information flow and not add details pertaining to the attached network into the flow of data.
- 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.

7.2.1.2 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.3: The TOE must transfer information through the TSF in a unidirectional information flow and not add details pertaining to the attached network into the flow of data.
- 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.

7.2.1.3 O.NON_DISCLOSURE

The TOE must not draw and attach network information from the joined host networks in order to transfer data from the source host to the destination host.

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.3: The TOE must transfer information through the TSF in a unidirectional information flow and not add details pertaining to the attached network into the flow of data.

7.3 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.

7.4 Requirement Dependency Rationale

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

ST Requirement	CC Dependencies	ST Dependencies
FDP_IFC.2	FDP_IFF.1 Simple security attributes	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialization	FDP_IFC.2; FMT_MSA.3 and its dependencies have been excluded from this Security Target because the information flow security policy is pre-defined and static, i.e. there is no means to change the information flow policy in the evaluated configuration
FDP_IFF.3	FDP_IFC.1 Subset information flow control	FDP_IFC.2
FPT_FLS.1	None	None

Table 9 Security Requirement Dependency Analysis

7.5 Explicitly Stated Requirements Rationale

There are no explicitly stated requirements in this Security Target.

7.6 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 10 Security Functions vs. Requirements Mapping** demonstrates the relationship between security requirements and security functions.

	User data protection	Protection of the TSF
FDP_IFC.2	X	
FDP_IFF.3	X	
FDP_IFF.1	X	
FPT_FLS.1:		X

Table 10 Security Functions vs. Requirements Mapping

8 Revision History

Version	Date	Changes / Reason for changes
01a	12/21/2015	Original draft document for the M-Series DDCC
01b	12/22/2015	Change of naming convention and new filename of document, minor editing
01c	1/22/2016	Rename title of ST, Merge data in Table 2 with Table 3. Delete Table 3, editing in sections 1,2,3,4,5,6,7,8,9
01d	2/9/2016	Delete FDP_IFF.5, minor editing, edit Table 7, Table 8, Table 9
01e	2/12/2016	Minor editing in sections 1.3, 1.6 and 6.2
01f	2/16/2016	Minor editing in sections 1.3 and 6.2
01g	2/22/2016	Add new Figure 5, Delete Chapter 5.2, 7, 8.7. Delete ADV_ARC.1 from Table 9
01h	3/31/2016	Add Sect. 5.2 back, Delete from Table 9
01i	6/10/2016	Delete obsolete cards, delete installation manual from text
01j	6/28/2016	Minor edit in Table 2 & 3. Delete 010-RevB from Sect. 1.3, delete error in Sect. 1.4
01k	7/25/2016	Updated Table 5 & 7. Edited or added to Sect. 1.7.2.1, 4.1, 5.1.1.3, 6.1.1, 7.1.1.1, 7.1.1.2, 7.2.1, 7.2.1.3, 7.4
01l	7/29/2016	Edited Table 5, 7, 8,9 & 10. Edited Sect. 1.7.2.1, 5.1.1.3, 6.1.1, 7.1.1.2, 7.2.1, 7.2.1.3, 7.4
01m	9/27/2016	Replace manuals Sec. 1.8, 6.2.2

END OF DOCUMENT