Owl Computing Technologies
Data Diode Network Interface Card Version 4
Security Target for EAL-4 Certification

Version r01g
12/08/06

Prepared by:
Owl Computing Technologies, Inc.

38A Grove Street
Ridgefield CT 06877

Based on document for Ver3 card EAL4 Prepared By:
Science Applications International Corporation

Common Criteria Testing Laboratory

7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

LIST OF TABLES

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. This ST describes a set of security requirements and specifications to be used as the basis for evaluation of an identified Information Technology (IT) product. The IT product described in this ST is the Owl Computing Technologies Data Diode Network Interface Card (DDNIC or Data Diode), herein called the DDNIC, developed by Owl Computing Technologies Incorporated, herein called Owl. The Owl Data Diode Network Interface Cards are the subject of this evaluation and are the TOE.

The DDNIC is a physical network interface card that physically connects to the PCI Bus of a host computer and has receptacles built on the card for fiber-optic connections. The DDNIC ensures an information flow policy where unidirectional communication is enforced between two gateways (i.e., host systems). Data Diodes are installed individually as a Send-Only DDNIC or a Receive-Only DDNIC, or in pairs where there is a Receive-Only DDNIC and a Send-Only DDNIC. Each DDNIC is installed into a host.

All information flow into a host system must flow into through a Receive-Only DDNIC that is restricted to only receive network traffic and cannot send network traffic. All traffic received is passed directly to the connected host. All information flow from a host system must flow through a Send-Only DDNIC that is restricted to only send network traffic and cannot receive network traffic. All traffic that is sent through the Send-Only DDNIC is sent at the request of the connected host.

Once manufactured, there is no way to alter the function of an Owl Data Diode Network Interface Card.

The Security Target contains the following additional sections:

- TOE Description (Section 2) – Physical and logical description of the TOE.
- Security Environment (Section 3) – Expected environment for the TOE.
- Security Objectives (Section 4) – Security objectives for both the TOE and its environment.
- IT Security Requirements (Section 5) – Security functional and assurance requirements.
- TOE Summary Specification (Section 6) – Description of security function and assurance measures.
- Protection Profile Claims (Section 7) – Claims of compliance for a specific Protection profile.
- Rationale (Section 8) – Rationale for correspondence and other aspects of this ST.

1.1 Security Target, TOE and CC Identification

ST Title – Owl Computing Technologies Data Diode Network Interface Card Version 4 Security Target for EAL-4 Certification

ST Version – Version r01g

ST Date – 12/08/06

TOE Identification – Owl Computing Technologies, Inc. Data Diode Network Interface Card Version 4

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.3, August 2005.

  - Part 2 Conformant
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.3, August 2005.
  - Part 3 Conformant
  - Assurance Level: EAL 4
  - Strength of Function Claim: SOF-Medium

1.3 Conventions, Terminology, Acronyms

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

1.3.1 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.

1.3.2 Terminology and Acronyms

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

ATM PHY	The Asynchronous Transfer Mode (ATM) Physical Interface Device (ATM PHY or PHY) is a high performance physical layer interface device on the Data Diode Network Interface Cards that generates and receives high-speed data streams. The ATM PHY receives 53-byte ATM cells from the SAR and produces analog signals that are passed to an optical transmitter or an optical receiver. The interface into the ATM PHY from the SAR uses the UTOPIA protocol and the interface to the transceiver is SONET over analog power pins.
CC	Common Criteria for Information Technology Security Evaluation
Data Diode Network Interface Card (DDNIC)	A network interface card consisting of three functional components; the Segmentation and Reassembly Controller (SAR), the ATM Physical Interface Device (PHY), and either the Fiber Optic Transmitter (in the Send-Only DDNIC only) or Fiber Optic Receiver (in the Receive-Only DDNIC only). The DDNICs are manufactured to Owl's specifications and use commercial-off-the-shelf (COTS) Asynchronous Transfer Mode network interface card

components. One Data Diode Network Interface Card (DDNIC) is used only for sending information, the Send-Only DDNIC. The other DDNIC is used only for receiving information, the Receive-Only DDNIC. The Send-Only DDNIC exports light pulses converted by the Optical Transmitter from electrical voltages. The Receive-Only DDNIC imports light pulses received at the photo detector of the Optical Receiver and converts the light pulses to electrical voltages.

Data Diode Host A computer system or network in which a Data Diode is installed. The host system or network is the system that provides power to the Data Diode. The Data Diode is digitally connected to the host via the Peripheral Component Interface (PCI).

EAL Evaluation Assurance Level

Gateway Also called a router, a gateway is a program or a special-purpose host that transfers network traffic with an identifiable network address from one network to another until the final destination is reached.

Host A general term for a computer system. Once specific application software or hardware is installed on a host it assumes the role of Data Diode Host, gateway, receiving Host, Sending Host.

NIC Network Interface Card that provides the physical interface to a network.

PCI The Peripheral Component Interface connects to the PCI Bus of the host system. .The PCI is the device driver interface into the TOE from the host computer. The PCI Bus is an open architecture bus structure to control devices. Composed of a PCI BIOS, CPU, CPU cache, system cache, system memory, PCI Bridge, and Peripheral Component Interface bus.

Receive-Only DDNIC The Receive-Only DDNIC only allows information for transfer to flow from its optical interface across the Receive-Only DDNIC and to the host system. All information presented for transfer to the Receive-Only DDNIC is subject to the unconditional unidirectional information flow. No information is able to flow from the host system across the Receive-Only DDNIC and through the optical interface of the Receive-Only DDNIC. This non-bypassability of the TOE is enforced at the physical level.

Receiving Host A host system or network in which a Receive-Only DDNIC is installed. The Receiving Host is to receive information through the Receive-Only Data Diode Network Interface Card.

SAR The Segmentation and Reassembly Controller (SAR). The SAR is a functional component of the Data Diode Network Interface Card. The SAR connects directly to the PCI bus of the host system and to the PHY. When transmitting, the SAR segments the data into 48 byte ATM data payloads or “cells.” The SAR then frames each cell with AAL5 headers for complete 53-byte ATM cells, which are then sent on for framing and serialization. When receiving, ATM data cells are transferred and reassembled directly into host memory by the SAR into pre-allocated memory buffers.

Sending Host A host system or network in which a Send-Only DDNIC is installed. The Sending Host is to send information through the Send-Only Data Diode Network interface Card.

Send-Only DDNIC The Send-Only DDNIC only allows information for transfer to flow from the host system across the DDNIC through the optical interface. All information presented to the Send-Only DDNIC is subject to the unconditional unidirectional information flow. No information is able to flow from outside the Send-Only DDNIC through the optical interface across the

Send-Only DDNIC and into the host system. This non-bypassability of the TOE is enforced at the physical level.

SONET Protocol The interface between the ATM PHY and the Optical Transmitter (Send-Only DDNIC) or the Optical Receiver (Receive-Only DDNIC) provides both Transmission Convergence (TC) and Physical Media Dependent (PMD) sub-layer functions of an ATM PHY suitable for ATM networks.

UTOPIA Protocol The UTOPIA (Universal Test and Operations PHY Interface for ATM) interface is the protocol used between the SAR and the ATM PHY. UTOPIA is a standard data path handshake protocol.

2. TOE Description

The Owl Computing Technologies, Inc. Data Diode Network Interface Card (NIC), Version 4, herein called DDNIC, is designed and manufactured by Owl Computing Technologies, Incorporated located at 38A Grove Street, Ridgefield CT 06877, U.S.A., herein called Owl.

The TOE comprises a pair of Owl Data Diode NIC network interface cards and associated driver software. Driver software is written and packaged (designed and manufactured) by Owl.

Each card has two external hardware interfaces. One external interface is the Peripheral Component Interface which connects to the PCI Bus of the host in which the DDNIC is installed. The other interface is the fiber optic network connection physically located on the card.

The PCI hardware interface is used to move data to and from the host computer platform in which the DDNIC is installed. The PCI interface hardware is associated with driver software that provides a standard logical interface for external software applications to move data across the PCI bus hardware interface. The fiber optic interface is controlled completely by hardware enforced logic on the DDNIC.

The purpose for the Data Diode NIC is to provide assurance of one-way operation across the DDNIC.

This Data Diode NIC was developed to support higher-level application software packages (apart from the TOE) to provide secure one-way network communications. Owl markets and sells application programs that utilize the Data Diode Technology for specific data transfers; however, the TOE is comprised only the Data Diode NIC and its associated driver software. The information flow policy enforced by the Data Diode NIC does not rely on passwords, authentication, or encryption to protect host data. Rather the physics of a photo-detector (in the Receive-Only DDNIC) and a light source (in the Send-Only DDNIC) enforce the TSP.

2.1 TOE Overview

The Target of Evaluation (TOE) is offered by Owl as a single Data Diode Network Interface Card (a Send-Only NIC or Receive-Only DDNIC) with its associated driver software, or as a pair of Data Diode Network Interface Cards with their associated driver software modules. Any host that supports a PCI Bus is sufficient for the correct operation of the TSF; therefore the host is not part of the TOE.

Each type Data Diode Network Interface Card allows information to move across it in only one direction, and therefore protects its Host System from information flow across the Data Diode Network Interface Card in the reverse direction. Data sent across the PCI Bus of sending host system (via driver software) are staged, queued, segmented and framed in the Send-Only DDNIC, and output through the Optical Transmitter of the Send-Only DDNIC. Data presented to the Optical Receiver of the Receive-Only DDNIC is reassembled into the original message in the Receive-Only DDNIC, and then transferred through the PCI Bus of the receiving host system to driver software in the receiving host system.

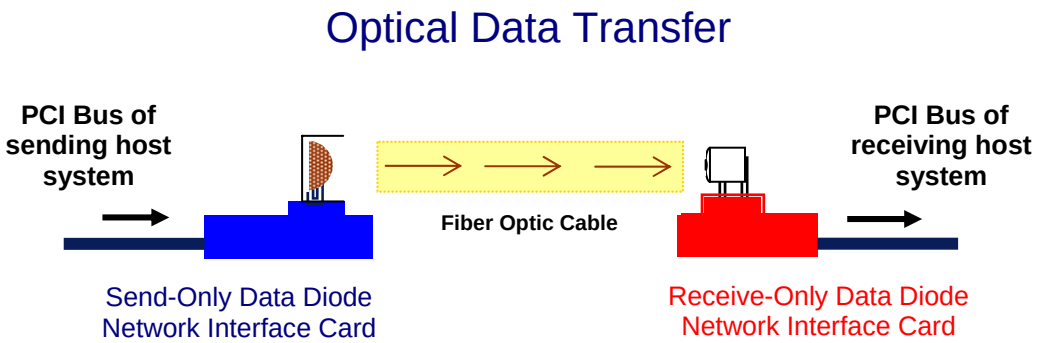

Figure 1 - High Level view of the Data Diode Interface

The Owl Data Diode System consists of a pair of Owl Computing Technologies, Inc. Data Diode Network Interface Cards (DDNICs) connected to each other through optical interfaces and a fiber optic cable, for unconditional and unidirectional information flow control between two separate host systems. The one-way information transfer occurs via an optical link consisting of one light source (at the source computer) and one light detector (at the destination computer) and using single one-way board component-level information paths in each DDNIC. No information of any kind, including handshaking protocols, (as in TCP/IP, SCSI, USB, Serial/Parallel Ports, etc.) travels from the destination computer back to the source computer.

The Owl Data Diode System moves packet data directly between a Send-Only DDNIC and a Receive-Only DDNIC via the optical interfaces of the DDNICs. Data sent across the PCI Bus of sending host system (via driver software) are staged, queued, segmented and framed in the Send-Only DDNIC, and output through the Optical Transmitter of the Send-Only DDNIC. The output of the Send-Only DDNIC is sent through a fiber optic cable connected to the Optical Receiver of the Receive-Only DDNIC. The data is then reassembled into the original message in the Receive-Only DDNIC, and then transferred through the PCI Bus of the receiving host system to driver software on the receiving host system.

2.2 TOE Architecture

The Owl Computing Technologies, Incorporated (Owl) Data Diode System provides an absolute one-way connection between a sending host system or network and 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 Data Diode System.

The Target of Evaluation (TOE) comprises two Owl Data Diode Network Interface Cards (DDNICs), the Send-Only DDNIC and the Receive-Only DDNIC, and their respective driver software. The DDNICs are manufactured to Owl's specifications using commercial-off-the-shelf (COTS) Asynchronous Transfer Mode network interface card components. Driver software is designed, written, and packaged by Owl. Each Data Diode NIC connects to a standard PCI slot in a host system and each is connected to each other using fiber optic network interfaces and a fiber optic cable. One Data Diode Network Interface Card (DDNIC) is used only for sending information, the Send-Only DDNIC. The other DDNIC is used only for receiving information, the Receive-Only DDNIC. The Send-Only DDNIC exports light pulses converted by the Optical Transmitter from electrical voltages. The Receive-Only DDNIC imports light pulses received at the photo detector of the Optical Receiver of the Receive-Only DDNIC and converts the light pulses to electrical voltages.

2.2.1 Physical Boundaries

The non-TSF portions of the Send-Only DDNIC and the Receive-Only DDNIC each include three functional components, the Asynchronous Transfer Mode (ATM) Segmentation and Reassembly Controller (SAR), the ATM Physical Interface Device (PHY), and the Optical Component (either the Fiber Optic Transmitter in theSend-Only DDNIC or the Fiber Optic Receiver in the Receive-Only DDNIC). The SAR connects directly to the PCI bus of the host system and to the PHY. Note that the Send-Only DDNIC's Optical Transmitter has only a light source and does not have a light detector and the Receive-Only DDNIC's Optical Receiver has only a light detector and does not have a light source. The absence of the light detector in the Send-Only DDNIC and the absence of the light source in the Receive-Only DDNIC are part of the TSF enforcing mechanism. The TSF is enforced at the physical level.

In addition to the physical enforcement of the TSF by having only an Optical Transmitter (the Send-Only DDNIC) or an Optical Receiver (the Receive-Only DDNIC), each Owl DDNIC provides a single one-way data path for information travel between the PHY and the Optical Component (either the Optical Transmitter in the Send-Only DDNIC or the Optical Receiver in the Receive-Only DDNIC). The path is physical in nature and consists of components at the board level. The components provide an impedance-matched electrically conductive path between the Physical Interface

Device (PHY) and the Optical Component.. The path between the PHY and the Optical Component in each DDNIC is the only impedance-matched electrically conductive path available between the two devices, and therefore cannot be bypassed.

In addition to providing an impedance-matched electrically conductive path between the PHY and the Optical Component of each DDNIC, there is provided an electrically conductive path between the host-system power and the Optical Component. (There is no electrically conductive path from the host-system power to the location of where there there is no installed Optical Component.)

Each Owl DDNIC has two external interfaces. One interface is the Peripheral Component Interface (PCI). The PCI of the DDNIC interfaces to the host system PCI bus. The PCI allows the exchange of information between the host system and its DDNIC. Information exchanged at the PCI consists of information to be transferred through the DDNIC and control and operation information used within a DDNIC and between DDNIC and its host system. The other interface of the DDNIC is the optical interface. The optical interface is used to connect the DDNIC to a fiber optic network. Typically in the Owl Data Diode System, the fiber optic network consists of a fiber optic cable connected to another DDNIC. These interfaces of the DDNIC do not enforce the TSF and cannot be used to modify the TSF, as the TSF are physically enforced by each DDNIC at the board-component level.

2.2.2 Logical Boundaries

The Owl Data Diode Network Interface Card is an information security tool that provides a way to send information in a fast (155 Mbps) one-way data stream from a source computer to a second destination computer. The one-way information transfer occurs via a one-way optical link consisting of a light source (at the source computer) and a light detector (at the destination computer).

Data sent across the PCI Bus (via driver software) of the sending host system are staged, queued, segmented and framed in the Send-Only DDNIC, and output through the Optical Transmitter of the Send-Only DDNIC. The output of the Send-Only DDNIC is sent through a fiber optic cable connected to the Optical Receiver of the Receive-Only DDNIC. The data is then reassembled into the original message in the Receive-Only DDNIC, and then transferred through the PCI Bus of the receiving host system to driver software on the receiving host system.

Each DDNIC has a single one-way data path that operates at the physical level. The Target Security Functions (TSF) are enforced at the board component level of each Owl Data Diode Network Interface Card (DDNIC). These board components make available only one impedance-matched electrically conducting path between the Optical Component (either the Optical Transmitter of the Send-Only DDNIC or the Optical Receiver of the Receive-Only DDNIC) and the Physical Interface Device and one electrically conducting path between the host-system power and the Optical Component.

2.2.2.1 User data protection

The Data Diode NIC protects itself by not exporting any interface that can be used to modify the Target Security Functions (TSF) of the TOE. The only interfaces exported for communication are the PCI and the optical interface of the DDNIC. The PCI interface is not relevant to the TSF. The optical interface presents Send-Only or Receive-Only capability, as determined by hardware component configurations that are inherent to the Target Security Functions (TSF) of the TOE. No interface is exported for communication which can significantly 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 TOE security policies. Since the TOE environment is assumed to provide adequate physical protection, it is impossible to breach the unconditional one-way data transfer security policies of the TOE.

Logically, the Data Diode NIC is protected largely by virtue of the fact that its interfaces are limited to primarily support only network traffic. While the TOE includes driver software for the Data Diode Network Interface Cards, all TSFs operate at the physical level which is below the level or protocols or binary logic, so it is unaffected by buffer content or network traffic. The TOE includes two Data Diode Network Interface Cards that are each connected to a standard PCI slot in a computer and may be connected to each other using fiber optic network interfaces and a fiber optic cable.

Given the assumption that all relevant data must pass through both interfaces (PCI and Optical) of the TOE, and since all information received by the TOE is unconditionally subject to its unidirectional information flow policy, there is no process present to bypass this security mechanism. There is only one path for information flow through each Owl Data Diode Network Interface 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 DDNIC, the DDNIC must function correctly. If a DDNIC is not functioning or is malfunctioning, only unidirectional information flow is permitted, or no information flow occurs. The Send-Only DDNIC only allows information to flow from the host system across the card to the external optical interface. The Receive-Only DDNIC only allows information to flow from the external optical interface across the card to the host system.

The Owl Data Diode System becomes part of the security domains of the two separate host systems for its own execution. The Owl Data Diode 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 DDNIC is hosted protects the DDNIC from interference and tampering by untrusted subjects. Furthermore, each DDNIC protects itself by not exporting any interface that can be used to modify the Target Security Functions (TSF) of the DDNIC. The only interfaces exported are the PCI Bus interface and the optical interface of the DDNIC, 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.

2.2.2.2 Protection of the TSF

All Target Security Functions (TSF) in the TOE operate at the physical level which is below the level or protocols or binary logic, so are unaffected by buffer content or network traffic. The Data Diode NIC protects itself by not exporting any interface that can be used to modify the TSF. The only interface exported to directly to the host platforms is the PCI interface of the DDNIC, which is not relevant to the TSF. Each Data Diode NIC presents only a single Optical interface to the outside world, which is either an Send-Only or Receive-Only interface, but not both. The Optical interface interacts with another DDNIC on a separate network; possibly through an ATM switch.

The use of Send-Only or Receive-Only optical interface hardware components is inherent to the TSF, and renders the TSF impervious to software attack. 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 impossible to modify the TOE in a manner that breaches its one-way-only data flow security policy. While reconfiguration of driver software may result in failure to transmit data in the forward direction, it is impossible to bypass or breach Target Security Functions and transmit data in the reverse direction without physically altering hardware.

Logically, the Data Diode NIC is protected largely by virtue of the fact that its interface is limited to primarily only support network traffic. The Target Security Functions (TSF) 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.

2.3 TOE Software

While the TOE is substantially defined by the Owl Data Diode Network Interface Cards, the TOE also includes associated DDNIC driver software, which is required to exercise Target Security Functions (TSF) in the TOE.

The DDNICs are ATM devices, and the ATM AAL5 protocol requires that formatted data be sent across the Dual Diode interface at all times. This constant low-level data stream, which verifies framing and other ATM-cell related communication processes necessary to keep the communication channel open, is controlled in hardware and may be examined using an ATM hardware analyzer.

In order to transfer data of interest to end users, Owl provides DDNIC driver software whose function is to convey user data to and from the DDNICs across the PCI bus interface. DDNIC driver software functions are not relevent to the TSF.

2.4 TOE Documentation

While the TOE is substantially defined by the Owl Data Diode Network Interface Cards, the TOE also includes associated installation and operation guidance. See section 6.2 of this Security Target for more specific information about available guidance documents.

3. Security Environment

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

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 Policies

P.ONEWAY	Information must be able to flow only in a single direction between attached hosts.

3.2 Threats

T.WRONGWAY	An attacker may be able to cause Information to flow inappropriately from one attached host to another.

3.3 Assumptions

A.ADMIN	The administrator will properly adhere to the TOE guidance.
A.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.
A.PHYSICAL	The TOE will be physically protected to a degree commensurate with the value of the information it is intended to protect.

4. Security Objectives

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.PROTECT	The TOE must be designed to protect itself from logical attacks that might attempt to bypass its information flow policy.

4.2 Security Objectives for the TOE Environment

OE.ADMIN	The administrator will properly adhere to the TOE guidance.
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 will be physically protected to a degree commensurate with the value of the information it is intended to protect.

5. IT Security Requirements

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 permutational or probabilistic security functional requirements and as a result there are no applicable strength of function claim.

5.1 TOE Security Functional Requirements

The following table describes the SFRs that are satisfied by Data Diode NIC.

Requirement Class	Requirement Component
FDP: User data protection	FDP_IFC.2: Complete information flow control
	FDP_IFF.1: Simple security attributes
FPT: Protection of the TSF	FPT_RVM.1: Non-bypassability of the TSP
	FPT_SEP.1: TSF domain separation

Table 1 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 TSC to flow to and from any subject in the TSC 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 Data Diode NIC]**.

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 Data Diode Network Interface Card permits it to send data, then only the sending of data packets is permitted;**
- **b) If the physical configuration of the Data Diode Network Interface 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 provide the following **[no additional SFP capabilities]**.

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

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: **[no explicit denial rules]**.

5.1.2 Protection of the TSF (FPT)

5.1.2.1 Non-bypassability of the TSP (FPT_RVM.1)

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.1.2.2 TSF domain separation (FPT_SEP.1)

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

5.2 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL 4 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

Requirement Class	Requirement Component
ACM: Configuration management	ACM_AUT.1: Partial CM automation
	ACM_CAP.4: Generation support and acceptance procedures
	ACM_SCP.2: Problem tracking CM coverage
ADO: Delivery and operation	ADO_DEL.2: Detection of modification
	ADO_IGS.1: Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.2: Fully defined external interfaces
	ADV_HLD.2: Security enforcing high-level design
	ADV_IMP.1: Subset of the implementation of the TSF
	ADV_LLD.1: Descriptive low-level design
	ADV_RCR.1: Informal correspondence demonstration
	ADV_SPM.1: Informal TOE security policy model
AGD: Guidance documents	AGD_ADM.1: Administrator guidance
	AGD_USR.1: User guidance
ALC: Life cycle support	ALC_DVS.1: Identification of security measures
	ALC_LCD.1: Developer defined life-cycle model
	ALC_TAT.1: Well-defined development tools
ATE: Tests	ATE_COV.2: Analysis of coverage
	ATE_DPT.1: Testing: high-level design
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing - sample
AVA: Vulnerability assessment	AVA_MSU.2: Validation of analysis
	AVA_SOF.1: Strength of TOE security function evaluation
	AVA_VLA.2: Independent vulnerability analysis

Table 2 EAL 4 Assurance Components

5.2.1 Configuration management (ACM)

5.2.1.1 Partial CM automation (ACM_AUT.1)

ACM_AUT.1.1d The developer shall use a CM system.

ACM_AUT.1.2d The developer shall provide a CM plan.

ACM_AUT.1.1c The CM system shall provide an automated means by which only authorised changes are made to the TOE implementation representation.

ACM_AUT.1.2c The CM system shall provide an automated means to support the generation of the TOE.

ACM_AUT.1.3c The CM plan shall describe the automated tools used in the CM system.

ACM_AUT.1.4c The CM plan shall describe how the automated tools are used in the CM system.

ACM_AUT.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.1.2 Generation support and acceptance procedures (ACM_CAP.4)

ACM_CAP.4.1d The developer shall provide a reference for the TOE.
ACM_CAP.4.2d The developer shall use a CM system.
ACM_CAP.4.3d The developer shall provide CM documentation.
ACM_CAP.4.1c The reference for the TOE shall be unique to each version of the TOE.
ACM_CAP.4.2c The TOE shall be labelled with its reference.
ACM_CAP.4.3c The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.
ACM_CAP.4.4c The configuration list shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.4.5c The configuration list shall describe the configuration items that comprise the TOE.
ACM_CAP.4.6c The CM documentation shall describe the method used to uniquely identify the configuration items.
ACM_CAP.4.7c The CM system shall uniquely identify all configuration items.
ACM_CAP.4.8c The CM plan shall describe how the CM system is used.
ACM_CAP.4.9c The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.
ACM_CAP.4.10c The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.
ACM_CAP.4.11c The CM system shall provide measures such that only authorised changes are made to the configuration items.
ACM_CAP.4.12c The CM system shall support the generation of the TOE.
ACM_CAP.4.13c The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.
ACM_CAP.4.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.1.3 Problem tracking CM coverage (ACM_SCP.2)

ACM_SCP.2.1d The developer shall provide a list of configuration items for the TOE.
ACM_SCP.2.1c The list of configuration items shall include the following: implementation representation; security flaws; and the evaluation evidence required by the assurance components in the ST.
ACM_SCP.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.2 Delivery and operation (ADO)

5.2.2.1 Detection of modification (ADO_DEL.2)

ADO_DEL.2.1d The developer shall document procedures for delivery of the TOE or parts of it to the user.
ADO_DEL.2.2d The developer shall use the delivery procedures.
ADO_DEL.2.1c The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.
ADO_DEL.2.2c The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site.
ADO_DEL.2.3c The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.
ADO_DEL.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.2.2 Installation, generation, and start-up procedures (ADO_IGS.1)

ADO_IGS.1.1d The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.
ADO_IGS.1.1c The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.
ADO_IGS.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADO_IGS.1.2e The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.2.3 Development (ADV)

5.2.3.1 Fully defined external interfaces (ADV_FSP.2)

ADV_FSP.2.1d The developer shall provide a functional specification.
ADV_FSP.2.1c The functional specification shall describe the TSF and its external interfaces using an informal style.
ADV_FSP.2.2c The functional specification shall be internally consistent.
ADV_FSP.2.3c The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.
ADV_FSP.2.4c The functional specification shall completely represent the TSF.
ADV_FSP.2.5c The functional specification shall include rationale that the TSF is completely represented.
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 TOE security functional requirements.

5.2.3.2 Security enforcing high-level design (ADV_HLD.2)

ADV_HLD.2.1d The developer shall provide the high-level design of the TSF.
ADV_HLD.2.1c The presentation of the high-level design shall be informal.
ADV_HLD.2.2c The high-level design shall be internally consistent.
ADV_HLD.2.3c The high-level design shall describe the structure of the TSF in terms of subsystems.
ADV_HLD.2.4c The high-level design shall describe the security functionality provided by each subsystem of the TSF.
ADV_HLD.2.5c The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.
ADV_HLD.2.6c The high-level design shall identify all interfaces to the subsystems of the TSF.
ADV_HLD.2.7c The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.
ADV_HLD.2.8c The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.
ADV_HLD.2.9c The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.
ADV_HLD.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_HLD.2.2e The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.2.3.3 Subset of the implementation of the TSF (ADV_IMP.1)

ADV_IMP.1.1d The developer shall provide the implementation representation for a selected subset of the TSF.
ADV_IMP.1.1c The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.
ADV_IMP.1.2c The implementation representation shall be internally consistent.
ADV_IMP.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_IMP.1.2e The evaluator shall determine that the least abstract TSF representation provided is an accurate and complete instantiation of the TOE security functional requirements.

5.2.3.4 Descriptive low-level design (ADV_LLD.1)

ADV_LLD.1.1d The developer shall provide the low-level design of the TSF.
ADV_LLD.1.1c The presentation of the low-level design shall be informal.
ADV_LLD.1.2c The low-level design shall be internally consistent.
ADV_LLD.1.3c The low-level design shall describe the TSF in terms of modules.
ADV_LLD.1.4c The low-level design shall describe the purpose of each module.
ADV_LLD.1.5c The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.

ADV_LLD.1.6c The low-level design shall describe how each TSP-enforcing function is provided.
ADV_LLD.1.7c The low-level design shall identify all interfaces to the modules of the TSF.
ADV_LLD.1.8c The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.
ADV_LLD.1.9c The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions and error messages, as appropriate.
ADV_LLD.1.10c The low-level design shall describe the separation of the TOE into TSP-enforcing and other modules.
ADV_LLD.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_LLD.1.2e The evaluator shall determine that the low-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.2.3.5 Informal correspondence demonstration (ADV_RCR.1)

ADV_RCR.1.1d The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.
ADV_RCR.1.1c For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.
ADV_RCR.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.6 Informal TOE security policy model (ADV_SPM.1)

ADV_SPM.1.1d The developer shall provide a TSP model.
ADV_SPM.1.2d The developer shall demonstrate correspondence between the functional specification and the TSP model.
ADV_SPM.1.1c The TSP model shall be informal.
ADV_SPM.1.2c The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.
ADV_SPM.1.3c The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.
ADV_SPM.1.4c The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.
ADV_SPM.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4 Guidance documents (AGD)

5.2.4.1 Administrator guidance (AGD_ADM.1)

AGD_ADM.1.1d The developer shall provide administrator guidance addressed to system administrative personnel.
AGD_ADM.1.1c The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.
AGD_ADM.1.2c The administrator guidance shall describe how to administer the TOE in a secure manner.
AGD_ADM.1.3c The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.
AGD_ADM.1.4c The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.
AGD_ADM.1.5c The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.
AGD_ADM.1.6c The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
AGD_ADM.1.7c The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8c The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.
AGD_ADM.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4.2 User guidance (AGD_USR.1)

AGD_USR.1.1d The developer shall provide user guidance.
AGD_USR.1.1c The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.
AGD_USR.1.2c The user guidance shall describe the use of user-accessible security functions provided by the TOE.
AGD_USR.1.3c The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.
AGD_USR.1.4c The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.
AGD_USR.1.5c The user guidance shall be consistent with all other documentation supplied for evaluation.
AGD_USR.1.6c The user guidance shall describe all security requirements for the IT environment that are relevant to the user.
AGD_USR.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.5 Life cycle support (ALC)

5.2.5.1 Identification of security measures (ALC_DVS.1)

ALC_DVS.1.1d The developer shall produce development security documentation.
ALC_DVS.1.1c The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.
ALC_DVS.1.2c The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.
ALC_DVS.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ALC_DVS.1.2e The evaluator shall confirm that the security measures are being applied.

5.2.5.2 Developer defined life-cycle model (ALC_LCD.1)

ALC_LCD.1.1d The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.
ALC_LCD.1.2d The developer shall provide life-cycle definition documentation.
ALC_LCD.1.1c The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.
ALC_LCD.1.2c The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.
ALC_LCD.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.5.3 Well-defined development tools (ALC_TAT.1)

ALC_TAT.1.1d The developer shall identify the development tools being used for the TOE.
ALC_TAT.1.2d The developer shall document the selected implementation-dependent options of the development tools.
ALC_TAT.1.1c All development tools used for implementation shall be well-defined.
ALC_TAT.1.2c The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.
ALC_TAT.1.3c The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.

ALC_TAT.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.6 Tests (ATE)

5.2.6.1 Analysis of coverage (ATE_COV.2)

ATE_COV.2.1d The developer shall provide an analysis of the test coverage.
ATE_COV.2.1c The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.
ATE_COV.2.2c The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.
ATE_COV.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.6.2 Testing: high-level design (ATE_DPT.1)

ATE_DPT.1.1d The developer shall provide the analysis of the depth of testing.
ATE_DPT.1.1c The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.
ATE_DPT.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.6.3 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, test procedure descriptions, expected test results and actual test results.
ATE_FUN.1.2c The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.
ATE_FUN.1.3c The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.4c The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.5c The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.
ATE_FUN.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.6.4 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 test a subset of the TSF as appropriate to confirm that the TOE operates as specified.
ATE_IND.2.3e The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.2.7 Vulnerability assessment (AVA)

5.2.7.1 Validation of analysis (AVA_MSU.2)

AVA_MSU.2.1d The developer shall provide guidance documentation.

AVA_MSU.2.2d The developer shall document an analysis of the guidance documentation.
AVA_MSU.2.1c The guidance documentation 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.
AVA_MSU.2.2c The guidance documentation shall be complete, clear, consistent and reasonable.
AVA_MSU.2.3c The guidance documentation shall list all assumptions about the intended environment.
AVA_MSU.2.4c The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).
AVA_MSU.2.5c The analysis documentation shall demonstrate that the guidance documentation is complete.
AVA_MSU.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_MSU.2.2e The evaluator shall repeat all configuration and installation procedures, and other procedures selectively, to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.
AVA_MSU.2.3e The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.
AVA_MSU.2.4e The evaluator shall confirm that the analysis documentation shows that guidance is provided for secure operation in all modes of operation of the TOE.

5.2.7.2 Strength of TOE security function evaluation (AVA_SOF.1)

AVA_SOF.1.1d The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.
AVA_SOF.1.1c For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.
AVA_SOF.1.2c For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.
AVA_SOF.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_SOF.1.2e The evaluator shall confirm that the strength claims are correct.

5.2.7.3 Independent vulnerability analysis (AVA_VLA.2)

AVA_VLA.2.1d The developer shall perform a vulnerability analysis.
AVA_VLA.2.2d The developer shall provide vulnerability analysis documentation.
AVA_VLA.2.1c The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for ways in which a user can violate the TSP.
AVA_VLA.2.2c The vulnerability analysis documentation shall describe the disposition of identified vulnerabilities.
AVA_VLA.2.3c The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.
AVA_VLA.2.4c The vulnerability analysis documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.
AVA_VLA.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_VLA.2.2e The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure the identified vulnerabilities have been addressed.
AVA_VLA.2.3e The evaluator shall perform an independent vulnerability analysis.
AVA_VLA.2.4e The evaluator shall perform independent penetration testing, based on the independent vulnerability analysis, to determine the exploitability of additional identified vulnerabilities in the intended environment.
AVA_VLA.2.5e The evaluator shall determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low attack potential.

6. TOE Summary Specification

This chapter describes the security functions and associated assurance measures.

6.1 TOE Security Functions

The TOE provides two security functions:

- User Data Protection
- Protection of the TSF

6.1.1 User data protection

The unidirectional information flow control of each Owl Data Diode Network Interface Card (DDNIC) is complete and unconditional. The DDNIC enforces unidirectional flow control on any request from an external interface to move data packets through the DDNIC and all operations that cause that information to flow through the Owl Data Diode System.

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

Each Owl Computing Technologies Data Diode Network Interface Card (Owl DDNIC) physically can only provide network traffic flow in one direction through the card. The Send-Only DDNIC allows only the one-way transfer of information *from* a host system through the DDNIC *to* outside the host system, and there is no transfer of information *from* outside the host system, through the DDNIC *into* the host system. The Receive-Only DDNIC allows only the one-way transfer of data *from* outside a host system through the DDNIC and *into* the host system and there is no transfer of information *from* the host system through the DDNIC *to* outside the host system.

If a host system attempts to receive information using a Send-Only DDNIC, there will be no transfer of information *from* outside the host system, through the Send-Only DDNIC *into* the host system. In the Send-Only DDNIC, the output of the transmitter side of the Physical Interface Device connects to the input of the Optical Transmitter. Furthermore, the Send-Only DDNIC has physically unavailable a light detector and has physically unavailable an impedance-matched electrically conductive path to the input of the receiver side of the PHY. Furthermore, the Send-Only DDNIC connects the host-system power to the Optical Transmitter and leaves unpowered the not present light detector. When the host system does not receive information using the Send-Only DDNIC, 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 DDNIC.

If a host system attempts to send information over a Receive-Only DDNIC, buffers of data may be sent through the host device driver over the PCI Bus to the Receive-Only DDNIC, but no information will flow *from* the host system through the DDNIC *to* outside the host system.. In the Receive-Only DDNIC, the output of the Optical Receiver connects to the input of the receiver side of the PHY. The Receive-Only DDNIC has physically unavailable an impedance-matched electrically conductive path to the transmitter side of the PHY. Furthermore, the Receive-Only DDNIC connects the host-system power to the Optical Receiver and leaves unpowered the not present light source. 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 DDNIC.

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

- FDP_IFC.2: All attempts to send and receive information are subject to the unidirectional information flow policy.
- FDP_IFF.1: The unidirectional information flow policy is enforced by ensuring that send-only interfaces can only send and receive-only interfaces can only receive.

6.1.2 Protection of the TSF

The Data Diode NIC protects itself by not exporting any interface that can be used to modify the TOE, and thereby the Target Security Functions (TSF) of the TOE. The only interfaces exported are the PCI and the optical interface of the DDNIC, 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 Data Diode NIC is protected largely by virtue of the fact that its interfaces are limited to primarily only support network traffic. 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 process present to bypass this security mechanism. There is only one path for information flow through each Owl Data Diode Network Interface 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 DDNIC, the DDNIC must function correctly. If a DDNIC is not functioning or is malfunctioning, only unidirectional information flow is permitted, or no information flow occurs. The Send-Only DDNIC only allows information to flow from the host system across the card to the external optical interface. The Receive-Only DDNIC only allows information to flow from the external optical interface across the card to the host system.

The Owl Data Diode System becomes part of the security domains of the two separate host systems for its own execution. The Owl Data Diode 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 DDNIC is hosted protects the DDNIC from interference and tampering by untrusted subjects. Furthermore, each DDNIC protects itself by not exporting any interface that can be used to modify the Target Security Functions (TSF) of the DDNIC. The only interfaces exported are the PCI Bus interface and the optical interface of the DDNIC, 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.

The Protection of the TSF function is designed to satisfy the following security functional requirements:

- FPT_RVM.1: All information passing through the TOE is unconditionally subject to its unidirectional information flow policy.
- FPT_SEP.1: The TOE is a physically distinct entity that cannot be modified except through physical means that are assumed to be obviated by the environment. Subjects of the TOE are differentiated by their distinct connections to the Receive-Only or Send-Only Data Diode NICs.

6.2 TOE Security Assurance Measures

6.2.1 Configuration management

The configuration management measures applied by Owl ensure that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE. Owl ensures changes to the implementation representation are controlled with the support of automated tools and that TOE associated configuration item modifications are properly controlled. Owl performs configuration management on the TOE implementation representation, design documentation, tests and test documentation, user and administrator guidance, delivery and operation documentation, life-cycle documentation, vulnerability analysis documentation, configuration management documentation, and security flaws.

These activities are documented in:

- The Owl Data Diode Version 4 – Configuration Management Plan

The Configuration management assurance measure satisfies the following EAL 4 assurance requirements:

- ACM_AUT.1
- ACM_CAP.4
- ACM_SCP.2

6.2.2 Delivery and operation

Owl provides delivery documentation and procedures to identify the TOE, allow detection of unauthorized modifications of the TOE and installation and generation instructions at start-up. Owl's delivery procedures describe all applicable procedures to be used to detect modification to the TOE. Owl also provides documentation that describes the steps necessary to install Data Diode in accordance with the evaluated configuration.

Documentation of evaluation configuration comes in two parts:

1. Installation procedures for the TOE are documented in an installation manual, "Owl Computing Technologies, Inc. Version 4 Card OEM Installation and User Manual". This TOE-specific OEM installation manual addresses all configuration items that affect TOE security functions.
2. Users interact with the TOE through interfacing software that is not part of TOE and does not affect any TOE security functions. However, interfacing software is required for testing the TOE. Interfacing software is delivered with the TOE and is subject to stringently controlled delivery and installation procedures which are documented in separate user manuals.

The Delivery and operation assurance measure satisfies the following EAL 4 assurance requirements:

- ADO_DEL.2
- ADO_IGS.1

6.2.3 Development

Owl has numerous 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 Data Diode. Of course, the implementation of the TOE itself is also available as necessary.

These activities are documented in:

- "Owl Computing Technologies, Inc. Version 4 Card OEM Installation and User Manual"
- The Owl Data Diode Version 4 – Functional Specification
- The Owl Data Diode Version 4 – High Level Design
- The Owl Data Diode Version 4 – Low Level Design
- The Owl Data Diode Version 4 – Implementation Representation
- The Owl Data Diode Version 4 – Architectural Description (modularity)
- The Owl Data Diode Version 4 – Security Policy Model
- The Owl Data Diode Version 4 – Informal Correspondence (mapping of design to functional specs)

The Development assurance measure satisfies the following EAL 4 assurance requirements:

- ADV_FSP.2
- ADV_HLD.2

- ADV_IMP.1
- ADV_LLD.1
- ADV_RCR.1
- ADV_SPM.1

6.2.4 Guidance Documents

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. Guidance document for the TOE is: "Owl Computing Technologies, Inc. Version 4 Card OEM Installation and User Manual"

Owl may provide additional documentation that describes interfacing software that supports the TOE, but is not depended on by the TOE for its security functions.

The Guidance documents assurance measure satisfies the following EAL 4 assurance requirements:

- AGD_ADM.1
- AGD_USR.1

6.2.5 Life cycle support

Owl ensures the adequacy of the procedures used during the development and maintenance of the TOE through the use of a comprehensive life-cycle management plan. Owl includes security controls on the development environment that are adequate to provide the confidentiality and integrity of the TOE design and implementation that is necessary to ensure the secure operation of the TOE. Owl achieves this through the use of a documented model of the TOE life cycle and well-defined development tools that yield consistent and predictable results.

These activities are documented in:

- The Owl Data Diode Version 4 – Life-Cycle

The Life cycle support assurance measure satisfies the following EAL 4 assurance requirements:

- ALC_DVS.1
- ALC_LCD.1
- ALC_TAT.1

6.2.6 Tests

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 Data Diode Version 4 – Tests
- The Owl Data Diode Version 4 – Tests Results
- Testing the Security Features of the Data Diode
- Test Report

The Tests assurance measure satisfies the following EAL 4 assurance requirements:

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

6.2.7 Vulnerability assessment

The TOE administrator and user guidance documents describe the operation of Data Diode 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 permutational 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.

These activities are documented in:

- The Owl Data Diode Version 4 – Covert Channel Analysis
- The Owl Data Diode Version 4 – Vulnerability Analysis

The Vulnerability assessment assurance measure satisfies the following EAL 4 assurance requirements:

- AVA_MSU.2
- AVA_SOF.1
- AVA_VLA.2

7. Protection Profile Claims

This Security Target does not claim conformance with any Protection Profile.

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
O.READONLY	X	X			
O.WRITEONLY	X	X			
O.PROTECT	X	X			
OE.ADMIN			X		
OE.CONNECTION				X	
OE.PHYSICAL					X

Table 3 Environment to Objective Correspondence

8.1.1.1 P.ONEWAY

Information must be able to flow only in a single direction between attached hosts.

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.PROTECT: The TOE protects itself and ensures that all information flowing through it is subject to its information flow policy.

8.1.1.2 T.WRONGWAY

An attacker may be able to cause Information to flow inappropriately from one attached host to another.

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.
- O.PROTECT: The TOE protects itself and ensures that all information flowing through it is subject to its information flow policy.

8.1.1.3 A.ADMIN

The administrator will properly adhere to the TOE guidance.

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.

8.1.1.4 A.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.

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.

8.1.1.5 A.PHYSICAL

The TOE 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 4** 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 are fully addressed in this section and each SFR is mapped to the objective for which it is intended to satisfy.

	O.READONLY	O.WRITEONLY	O.PROTECT
FDP_IFC.2	X	X	
FDP_IFF.1	X	X	
FPT_RVM.1			X
FPT_SEP.1			X

Table 4 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.

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.

8.2.1.3 O.PROTECT

The TOE must be designed to protect itself from logical attacks that might attempt to bypass its information flow policy.

This TOE Security Objective is satisfied by ensuring that:

- FPT_RVM.1: The TSF ensures that TSP enforcement functions are invoked and succeed before any read request from the host is serviced by the TSF.
- FPT_SEP.1: The TSF maintains a security domain for its own execution that protects it from interference and tampering and also appropriately separates the security domains of its subjects.

8.3 Security Assurance Requirements Rationale

This ST contains the assurance requirements from the CC EAL 4 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 Strength of Functions Rationale

The TOE provides no IT security function for which a strength of function claim is appropriate. If a strength of function claim could be made, then an appropriate level would be SOF-medium since the assurance level for the TOE is determined to be EAL 4.

8.5 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	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1 and **FMT_MSA.3**	FDP_IFC.2
FPT_RVM.1	none	none
FPT_SEP.1	none	none
ACM_AUT.1	ACM_CAP.3	ACM_CAP.4
ACM_CAP.4	ALC_DVS.1	ALC_DVS.1
ACM_SCP.2	ACM_CAP.3	ACM_CAP.4
ADO_DEL.2	ACM_CAP.3	ACM_CAP.4
ADO_IGS.1	AGD_ADM.1	AGD_ADM.1
ADV_FSP.2	ADV_RCR.1	ADV_RCR.1
ADV_HLD.2	ADV_FSP.1 and ADV_RCR.1	ADV_FSP.2 and ADV_RCR.1
ADV_IMP.1	ADV_LLD.1 and ADV_RCR.1 and ALC_TAT.1	ADV_LLD.1 and ADV_RCR.1 and ALC_TAT.1
ADV_LLD.1	ADV_HLD.2 and ADV_RCR.1	ADV_HLD.2 and ADV_RCR.1
ADV_RCR.1	none	none
ADV_SPM.1	ADV_FSP.1	ADV_FSP.2
AGD_ADM.1	ADV_FSP.1	ADV_FSP.2
AGD_USR.1	ADV_FSP.1	ADV_FSP.2
ALC_DVS.1	none	none
ALC_LCD.1	none	none
ALC_TAT.1	ADV_IMP.1	ADV_IMP.1
ATE_COV.2	ADV_FSP.1 and ATE_FUN.1	ADV_FSP.2 and ATE_FUN.1
ATE_DPT.1	ADV_HLD.1 and ATE_FUN.1	ADV_HLD.2 and ATE_FUN.1
ATE_FUN.1	none	none
ATE_IND.2	ADV_FSP.1 and AGD_ADM.1 and AGD_USR.1 and ATE_FUN.1	ADV_FSP.2 and AGD_ADM.1 and AGD_USR.1 and ATE_FUN.1
AVA_MSU.2	ADO_IGS.1 and ADV_FSP.1 and AGD_ADM.1 and AGD_USR.1	ADO_IGS.1 and ADV_FSP.2 and AGD_ADM.1 and AGD_USR.1
AVA_SOF.1	ADV_FSP.1 and ADV_HLD.1	ADV_FSP.2 and ADV_HLD.2
AVA_VLA.2	ADV_FSP.1 and ADV_HLD.2 and ADV_IMP.1 and ADV_LLD.1 and AGD_ADM.1 and AGD_USR.1	ADV_FSP.2 and ADV_HLD.2 and ADV_IMP.1 and ADV_LLD.1 and AGD_ADM.1 and AGD_USR.1

Table 5 Security Requirement Dependency Analysis

8.6 Explicitly Stated Requirements Rationale

There are no explicitly stated requirements in this Security Target.

8.7 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 6 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	
FPT_RVM.1		X
FPT_SEP.1		X

Table 6 Security Functions vs. Requirements Mapping

8.8 PP Claims Rationale

See Section 7, Protection Profile Claims.