Doc. No. 9162P01000001
Issue No. 5.1

INTERACTIVE LINK DATA DIODE DEVICE

COMMON CRITERIA SECURITY TARGET

Prepared For:

National Information Assurance Partnership (NIAP)
US Government Initiative between
National Institute of Standards and Technology (NIST) and
National Security Agency (NSA)

Prepared By:

Tenix Datagate Inc
Suite 155 1420 Spring Hill Road
McLean, VIRGINIA 22102
USA

Released By:

Mr Sam Maccherola
President
Tenix Datagate Inc

Contents

List of Figures

List of Tables

1. Introduction

1.1 Security Target Identification

Title: Interactive Link Data Diode Device Common Criteria Security Target

Security Target Documentation Number: 9162P01000001

Security Target Version:	5.1, 19 August 2005
Assurance Level:	EAL 7, augmented with AVA_CCA.3.
TOE Title:	Interactive Link Data Diode Device
TOE Part Number:	FID003
TOE Version:	2.1

1.2 Security Target Overview

The Interactive Link Data Diode Device (IL-DDD), as shown in Figure 1, is a hardware product providing a unidirectional data path between a source and destination. The IL-DDD inputs and outputs are connected to their servers via fibre-optic cables to minimise electromagnetic radiation. Circuitry within the unit ensures that signals can pass only from input to output, and not vice versa. This requires data transfers over the diode to be sent without acknowledgments.

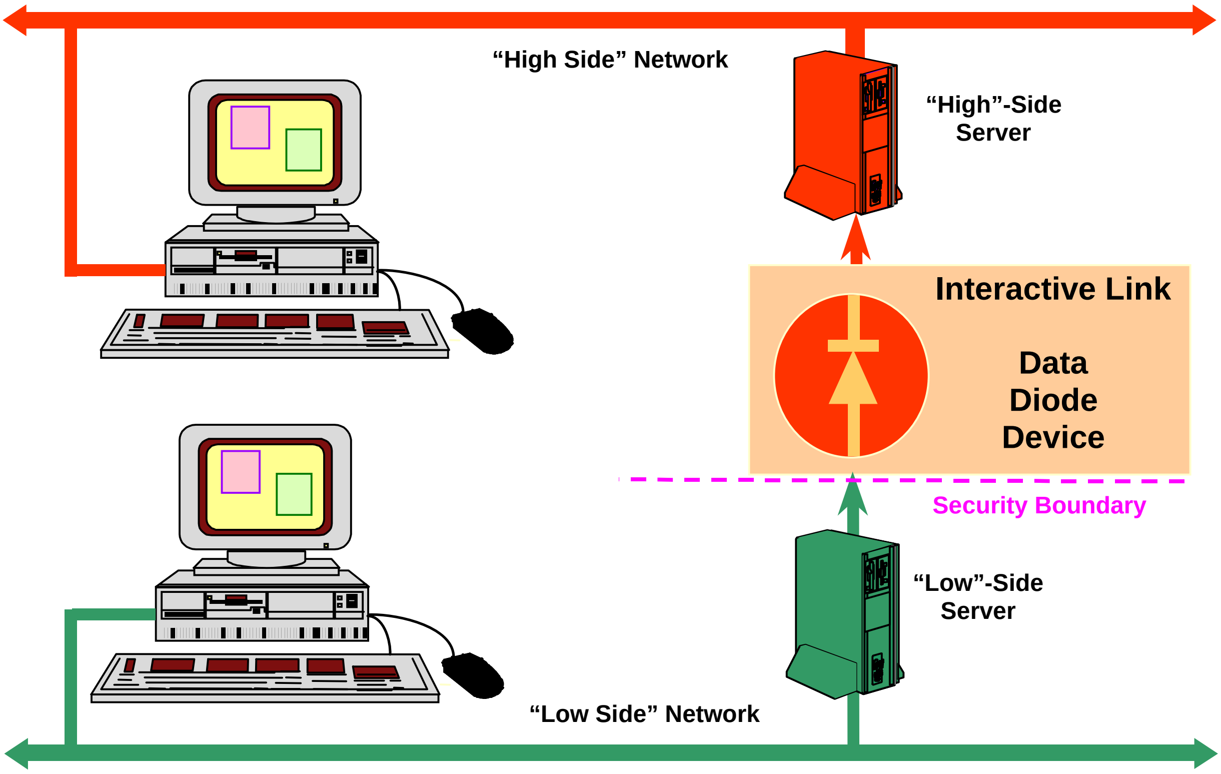

Figure 1: Interactive Link Data Diode Device Operational Concept.

The IL-DDD allows information to flow from a Security classified NETWORK (LOW SIDE source) to a higher Security classified NETWORK (HIGH SIDE destination), without compromising the confidentiality of the information on the HIGH SIDE.

The functionality of the IL-DDD provided HIGH SIDE USERS and programs with access to information pushed from the LOW SIDE. For example,

(a) WWW or news group information from the LOW SIDE may be transferred to the HIGH SIDE NETWORK so that browsers on the HIGH SIDE can access that information.

(b) Electronic mail for some USERS may be copied from the LOW SIDE NETWORK to the HIGH SIDE NETWORK, so that those USERS can read the email without going to a different NETWORK.

(c) Consider a USER who uses accounts on both LOW SIDE and HIGH SIDE NETWORKs. The arrival of LOW SIDE mail for that USER may trigger a signal to be sent via the IL-DDD to the HIGH SIDE NETWORK, to notify the USER that new mail has arrived on the LOW SIDE NETWORK.

(d) USERS on the LOW SIDE may direct files to be pushed to the HIGH SIDE NETWORK, to be available to themselves or other USERS.

(e) Database replication information, such as X.500 directory updates, or Sybase Replication Server data could be sent from a database server on the LOW SIDE source to a database server on the HIGH SIDE destination, so that updated LOW SIDE INFORMATION is available to HIGH SIDE database clients.

(f) Clipboard information from a LOW SIDE computer may be sent via the IL-DDD to a computer on the HIGH SIDE, so that the information may be pasted into a document or file.

(g) Other applications requiring a unidirectional data pipe, eg the "Interactive Link" as defined within its security target, makes use of the IL-DDD.

1.3 CC Conformance

The TOE is a product that has been developed with evaluation in mind it conforms with the Common Criteria version 2.1 (CC) part 2. It also conforms with the assurance requirements of the CC part 3 for the assurance level EAL 7, augmented with AVA_CCA.3 and all International and National Information Assurance Partnership (NIAP) interpretations through March 2004.

1.4 Document Overview

This security target has been developed in accordance with the requirements of the CC part 3, Class ASE: Security Target Evaluation and Annex C: Specification of Security Targets, of the CC part 1. The security target contains the following sections:

a. Section 1 – Introduction; this section identifies the security target and the Target of Evaluation (TOE), it provides an overview of the purpose and use of the TOE, it documents the CC conformance claim and defines the format this security target.

b. Section 2 – Acronyms & Definitions; this section lists the acronyms, definitions and references used throughout the document.

c. Section 3 – TOE Description; this section describes the product type and the scope and boundaries of the TOE in general terms both in a physical and logical way.

d. Section 4 – TOE Security Environment; this section defines assumptions about the intended environment within which the TOE is to be used, it identifies perceived threats to the HIGH SIDE INFORMATION and any organisational security policies with which the TOE must comply.

e. Section 5 – Security Objectives; this section defines the security objects for the TOE and its environment.

f. Section 6 – IT Security Requirements; this section defines the detailed IT security requirements that the TOE and its environment shall satisfy. It defines the TOE security functional requirements and its security assurance requirements.

g. Section 7 – TOE summary specifications; this section defines the IT security functions and the assurance measures of the TOE.

h. Section 8 – PP Claims; this section defines the Protection Profile claims of this Security Target.

i. Section 9 – Rationale; this section presents the evidence that supports the claims made in this security target and defines how the security requirements are complete and cohesive and provide an effective set of countermeasures within the nominated secure environment.

2. Acronyms & Definitions

2.1 Acronyms

AISEF – Australasian INFORMATION Security Evaluation Facility.

CC – Common Criteria for INFORMATION Technology Security Evaluation.

CM – Configuration management.

EAL – Evaluation Assurance Level.

ERTZ – Equipment Radiation TEMPEST Zone.

HOL – Higher Order Logic.

IL-DDD – Interactive Link Data Diode Device.

ISSO – Information System Security Officer.

IT – Information Technology.

NIAP – National Information Assurance Partnership.

OSI – Open System Interconnection.

PP – Protection Profile.

SFP – Security Function Policy.

Tenix – Tenix Datagate Inc.

TOE – Target of Evaluation.

TSC – TSF Scope of Control.

TSF – TOE Security Functions.

TSP – TOE Security Policy.

UDP - User Datagram Protocol.

2.2 Definitions

Application Server refers to a server computer, which executes application software that interacts with a USER.

High Side is a descriptor used to refer to items associated with the HIGH SIDE NETWORK. The HIGH SIDE is the destination of the information.

High SIDE NETWORK refers to a NETWORK with a security level greater that the LOW SIDE NETWORK.

INFORMATION is an object it is considered in two forms: LOW SIDE INFORMATION received at the INPUT PORT and HIGH SIDE INFORMATION transmitted at the OUTPUT PORT.

Infosec refers to Information System Security.

Interactive Link is the collection of products that provides the functionality of an interactive link between the High SIDE NETWORK and the Low SIDE NETWORK with out compromising the confidentiality of the information on the High Side. The Interactive Link consists of two prime components that provide the security, the Keyboard Switch and a Data Diode Device. For further details refer to the Interactive Link Security Target.

Interactive Link - Data Diode Device refers to a device that allows the flow of data in one direction only.

Interface Ports are the subjects that the object INFORMATION uses there are two forms of the subject INTERFACE PORTS the INPUT PORT and OUTPUT PORT.

Isabelle is a Formal Methods theorem prover that utilises HOL (Higher Order Logic) theory.

Low Side is a descriptor used to refer to items associated with the LOW SIDE NETWORK. The LOW SIDE is a source of information.

Low SIDE NETWORK refers to the NETWORK of a classification lower than the HIGH SIDE NETWORK.

Non-Interference is the formal security policy of the IL-DDD. The policy was defined in the papers written by Goguen and Meseguer in 1982 and 1984.

Security Authority refers to an independent third party that has been assigned the responsibility to mandate secure usage of the HIGH SIDE INFORMATION by the ultimate owner of the information.

TEMPEST refers to electromagnetic emanations that can be related to the information being processed by an information system. All electronic based information systems produce unwanted electromagnetic emanations, which in some cases can be related to the information being processed. This phenomenon is known as TEMPEST. The space within which a successful TEMPEST intercept is considered possible is termed the ERTZ. Information Systems where TEMPEST is a concern are required to have a TEMPEST Threat Assessment undertaken so as to determine the Secure Boundary of the System.

Unidirectional Flow SFP the security function policy that defines that data shall only flow in one direction.

User refers to the person who utilises the service being provided by the Data Diode Device.

Z a formal specification language.

2.2 References

5018/T16/2, (2000) EFA T010 Data Diode Device Sanitized Evaluation Technical Report, Admiral Management Services, Issue 1.0.

96125P01000021, (1997) Interactive Link Risk and Threat Assessment, Vision Abell, Draft Issue 2.1.

CCIMB-99-031, (1999) Common Criteria for Information Technology Security Evaluation Part 1 Introduction and General Model, Common Criteria Project Sponsoring Organisations, Version 2.1.

CCIMB-99-032, (1999) Common Criteria for Information Technology Security Evaluation Part 2 Security Functional Requirements, Common Criteria Project Sponsoring Organisations, Version 2.1.

CCIMB-99-033, (1999) Common Criteria for Information Technology Security Evaluation Part 3 Security Assurance Requirements, Common Criteria Project Sponsoring Organisations, Version 2.1.

DSTO-TR-96125P01000014, (1998) Interactive Link Formal Policy and Architecture, Defence Science and Technology Organisation (DSTO), Issue 3.0.

ISO/IEC PDTR 15446 (2000) Guide For The Production Of Protection Profiles And Security Targets, ISO/JTC 1/SC 27 Information Technology – Security Techniques, Version 0.9.

3. TOE Description

The Target of Evaluation (TOE) of the IL-DDD consists of the physical hardware of the device and contains no firmware or software. The IL-DDD allows information to flow through the device in a single direction from the input to the output. This is the only function performed by the IL-DDD and is its logical scope and boundary.

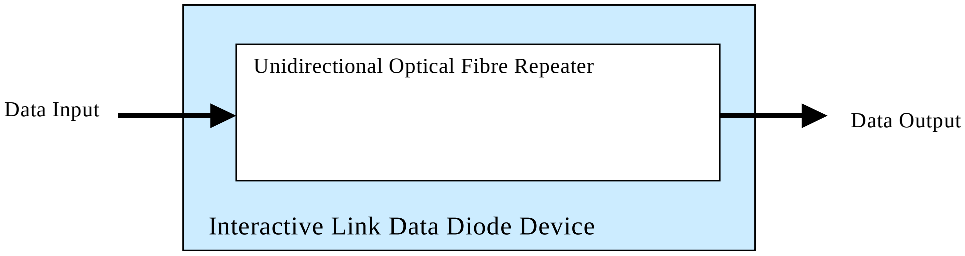
Unidirectional Optical Fibre Repeater
Data Input
Data Output
Interactive Link Data Diode Device

Figure 2 Interactive Link Data Diode Device Functional Block Diagram

The IL-DDD consists of a single function block as shown in Figure 2, the unidirectional optical fibre repeater, that ensures data is passed only from the input port to the output port. The data transfer is implemented in hardware, at the physical layer of the OSI reference model. It has been implemented using a purpose built fibre transmitter and receiver, constructed from discrete components. This approach has been adopted to minimise the emanation and the TEMPEST security threat.

There are no “back channels”, for communication hand shaking, which could be used as a covert channel. Any NETWORK protocol could be used to implement the transfer if no hand shaking across the IL-DDD is required. The User Datagram Protocol (UDP) is an example of an acceptable protocol that can accommodate a unidirectional flow of information.

The TSF Scope of Control (TSC) is limited to the hardware of the IL-DDD with its two operational interfaces, the input and output ports and is bound by its physical case.

The IL-DDD is not concerned with the information flowing from its input to its output therefore it does not assess any security attributes of the data. The primary concern is to ensure that the device is installed with the source at the input and the destination at the output.

IT Environment

The IT environment provides support for the TOE, allowing the TOE to operate with full functionality. The IT environment includes the HIGH and LOW SIDE servers and IL software. The IL-DDD is installed between the HIGH and LOW SIDE NETWORKS and is located with the HIGH SIDE SERVER, in the HIGH SIDE NETWORK space. The HIGH SIDE SERVER receives LOW SIDE INFORMATION transferred across the IL-DDD from the LOW SIDE SERVER. The HIGH SIDE SERVER distributes INFORMATION to the appropriate HIGH SIDE DESTINATION. The LOW SIDE SERVER packages up the display INFORMATION so that it can be transferred across the unidirectional IL-DDD.

3.1 Scope of Physical and Logical Boundaries

The physical boundary of the TOE is discussed above and as shown in Figure 2, Interactive Link Data Diode Device Functional Block Diagram. The physical boundary maintains two operational interfaces, Output port to the destination, HIGH SIDE SERVER and the Input port from the source, LOW SIDE SERVER

The logical boundary of the TOE provides the security features discussed below:

INFORMATION FLOW CONTROL

> The functionality of the TOE allows source LOW SIDE INFORMATION to flow to the destination, HIGH SIDE. The primary security features of the TOE serve to protect the HIGH SIDE INFORMATION from elements on the LOW SIDE. Protection of the HIGH SIDE INFORMATION is enforced through the non-interference TOE security policy.

INSTALLATION MANAGEMENT

> Correct installation ensures that the appropriate static attributes are established during installation.

SF INVOCATION AND ISOLATION

> The TOE security feature address the *always invoked* aspect of a traditional reference monitor. The goal of SF invocation and isolation ensures that the Non-interference TSP is enforced at all times during TOE operation and the TSP enforcing functions are always invoked. Additionally, the SF are protected from external interference and tampering by untrusted subjects.

PREVENTION OF UNINTENDED SIGNALLING CHANNELS

> The TOE has been designed to ensure that no unintended signalling channels from the HIGH SIDE to the LOW SIDE exist. Preventing unintended signalling channels is achieved by design decisions, which ensure that the TOE will not violate the Non-interference TSP in the event of hardware component failures.

3.2 TOE Security Policy

The TOE provides a unidirectional transmission of electronic signals (information) from a LOW SIDE network to a HIGH SIDE network. The information flow control policy can be summarized as:

Unidirectional Flow Security Function Policy (SFP)

> The asset of HIGH SIDE INFORMATION is to be kept confidential from processes, applications and users on the LOW SIDE while allowing information to flow from the LOW SIDE to the HIGH SIDE.

3.3 Evaluated Configuration

The evaluated configuration of the IL-DDD consists of single components as depictured above in Figure 2, Interactive Link Data Diode Device Functional Block Diagram.

4. TOE Security Environment

4.1 Assumptions

The IL-DDD will be connected between two NETWORKS of different levels known as the HIGH SIDE NETWORK and the LOW SIDE NETWORK. The assumptions made about the intended environment are:

A.PERSONNEL The IL-DDD shall be installed, administered and used by authorised personnel who possess the necessary privileges to access the HIGH SIDE INFORMATION.

A.PHYSICAL The intended environment shall be capable of storing and operating the IL-DDD in accordance with the requirements of the HIGH SIDE. Note there may also be a requirement for protecting critical system resources, within secure environments greater than the requirements of the HIGH SIDE e.g. a secured HIGH SIDE server room. The IL-DDD may be regarded as a critical resources if users of the HIGH SIDE NETWORK have a critical requirement to access information from the LOW SIDE NETWORK.

A.EMISSION It is intended that the IL-DDD operate in an environment where physical (or some other) security measures prevent any TEMPEST attack. This could be achieved by ensuring that the security boundary is outside the IL-DDD Equipment Radiation TEMPEST Zone (ERTZ). The IL-DDD operates at the edge of the secure boundary where the LOW SIDE meets the HIGH SIDE. Care should be taken to determine the relationship of the IL-DDD’s ERTZ to its secure boundary and to keep the ERTZ within it.

A.INSTALLATION The system management staff in accordance with the Administration Documentation shall install the IL-DDD. The appropriate SECURITY AUTHORITY shall accredit the installation of the IL-DDD.

A.TRAINING All staff who have access to HIGH SIDE INFORMATION systems shall be trained in the reasons for security, how the security has been implemented, why it has been implemented in that way and their responsibilities in ensuring that the information system security is maintained.

A.NETWORK IL-DDD’s i.e. either a singular or multiple devices, is the only method of interconnecting the LOW and HIGH SIDE NETWORKS. This prevents a threat agent from circumventing the security being provided by the IL-DDD through an untrusted product.

A.NO_EVIL Authorised users of the TOE are non-hostile and follow all usage guidance to ensure that the IL-DDD is configured and operated in a secure manner.

4.2 Threats

The assumed threats are threats to the IL-DDD, which could cause it to fail its security objective. The Interactive Link Risk and Threat Assessment, has assessed threats to the HIGH SIDE INFORMATION, new threats that have been introduced with the IL-DDD are listed in this section as potential threats. Appropriate countermeasures and the intended environment have countered all other previously identified threats. The relevant threats that could jeopardise the security objectives are:

T.TRANSFER A USER or process, e.g. a Trojan horse, on the HIGH SIDE NETWORK that accidentally or deliberately breaches the confidentiality of some HIGH SIDE INFORMATION by transmitting data through the IL-DDD to the LOW SIDE NETWORK.

T.TAMPER An adversary tampers with the contents of the IL-DDD during delivery, and/or after installation to cause the compromise of the confidentiality of some HIGH SIDE INFORMATION.

T.FAILURE The IL-DDD has a hardware failure that allows HIGH SIDE INFORMATION to be transmitted to the LOW SIDE NETWORK and thus makes the information available to LOW SIDE USERS.

T.LOGIC A USER or process on the LOW SIDE NETWORK transmits data to the TOE that causes a modification to the TSF.

4.3 Organisational Security Policies

There are no organisational security policies or rules with which the TOE must comply.

5. Security Objectives

5.1 Security Objectives for the TOE

The IL-DDD is intended to protect the asset, of HIGH SIDE INFORMATION, in accordance with the following objective:

O.CONFIDENTIALITY The information on the HIGH SIDE destination is kept confidential from the LOW SIDE source.

The LOW SIDE NETWORK consists of LOW SIDE USERS that haven’t been cleared to handle HIGH SIDE data. It also refers to hardware, processes and programs on the LOW SIDE NETWORK that could present a threat to the confidentiality of the HIGH SIDE INFORMATION.

O.INVOKE The SF is always invoked to protect the INFORMATION on the HIGH SIDE.

O.FAILSECURE The SF shall maintain a secure state should a single hardware failure occur within the TOE.

O.TAMPER_SEALS The IL-DDD shall be tamper evident.

O.ROM TSF shall be protected against unauthorised modification.

5.2 Security Objectives for the Environment

All of the secure usage assumptions are considered to be security objectives of the environment. These objectives are satisfied though the application of procedural or administrative measures.

OE.PERSONNEL The IL-DDD shall be installed, administered and used by authorised personnel who possess the necessary privileges to access the HIGH SIDE INFORMATION.

OE.NO_EVIL Authorised users of the TOE shall be non-hostile and shall follow all usage guidance to ensure that the Interactive Link is operated in a secure manner.

OE.PHYSICAL The intended environment shall be capable of storing and operating the IL-DDD in accordance with the requirements of the HIGH SIDE.

OE.EMISSION It is intended that the IL-DDD operate in an environment where physical (or some other) security measures prevent any TEMPEST attack.

OE.INSTALLATION The system management staff in accordance with the Administration Documentation shall install the IL-DDD. The appropriate SECURITY AUTHORITY shall accredit the installation of the IL-DDD.

OE.TRAINING All staff who have access to HIGH SIDE INFORMATION systems shall be trained in the reasons for security, how the security has been implemented, why it has been implemented in that way and their responsibilities in ensuring that the information system security is maintained.

OE.NETWORK IL-DDD’s are the only method of interconnecting the LOW and HIGH SIDE NETWORKS.

6. IT Security Requirements

6.1 TOE Security Functional Requirements

The IL-DDD functionality to prevent data from being transmitted from the HIGH SIDE NETWORK to the LOW SIDE NETWORK, while allowing data to be transmitted from the LOW SIDE NETWORK to the HIGH SIDE NETWORK is addressed by the following security functional requirements:

Family	Functional Components	Dependencies
FDP_IFC.2	Complete Information Flow Control	FDP_IFF.1
FDP_IFF.1	Simple Security Attributes	FDP_IFC.1, FMT_MSA.3†
FDP_IFF.5	No Illicit Information Flows	AVA_CCA.3, FDP_IFC.1
FPT_SEP.3	Complete Reference Monitor	No Dependencies
FPT_FLS.1	Failure with Preservation of Secure State	ADV_SPM.1
FPT_RVM.1	Non-bypassability of the TSP	

† FMT_MSA is a dependency that has not met as described in section 9.3.3.1.

Table 1 – Functional Requirements

The functional requirements that appear in Table 1 are described in more detail in the following subsections. Additionally, these requirements are derived verbatim from Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 2.1* with the exception of italicised items listed in brackets. These bracketed items include either “assignments” that are TOE specific or “selections” from the Common Criteria that the TOE enforces.

6.1.1 User Data Protection (FDP)

The functional requirements of this class relate to the protection of HIGH SIDE INFORMATION from elements on the LOW SIDE via the IL-DDD. The IL-DDD functionality requirements are based on two families of this class: the information flow control policy (FDP_IFC) and functions (FDP_IFF).

FDP_IFC Information Flow Control Policy

This family utilises the *Unidirectional Flow SFP,* an information flow control SFP. The *Unidirectional Flow SFP* is the single policy of the IL-DDD and its scope of control of maps directly to the TSC.

FDP_IFC.2 Complete Information Flow Control

Dependencies: FDP_IFF.1

FDP_IFC.2.1 The TSF shall enforce the [assignment: *Unidirectional Flow SFP*] on [assignment: *INTERFACE PORTS (subjects), USER DATA (information)*] and all operations that cause information to flow to and from the 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.

FDP_IFF Information Flow Control Functions

This family describes the rules for the specific functions that implement the *Unidirectional Flow SFP*. It consists of two kinds of requirements addressed by the following components: the first addressing the common information flow function issues, and the second addressing illicit information flows (i.e. Covert channels).

FDP_IFF.1-NIAP-0407 Simple Security Attributes

Dependencies: FDP_IFC.1, FMT_MSA.3‡

FDP_IFF.1.1 The TSF shall enforce the [assignment: *Unidirectional Flow SFP*] based on the following types of subject and information security attributes:

[assignment:

a. *INTERFACE PORT attributes: LOW SIDE INPUT, HIGH SIDE OUTPUT*

b. *USER DATA attributes: LOW SIDE, HIGH SIDE*].

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:

[assignment:

a. *All LOW SIDE USER DATA shall be allowed to flow from the LOW SIDE INPUT INTERFACE PORT to the HIGH SIDE OUTPUT INTERFACE PORT*].

FDP_IFF.1.3-NIAP-0407 The TSF shall enforce the following information flow control rules:

[selection: [assignment:

No information shall flow from the HIGH SIDE OUTPUT INTERFACE PORT to the LOW SIDE INPUT INTERFACE PORT]].

FDP_IFF.1.4-NIAP-0407 The TSF shall provide following:

[selection: no additional SFP capabilities].

FDP_IFF.1.5 -NIAP-0407 The TSF shall explicitly authorise an information flow based on the following rules:

[selection: no explicit authorisation rules].

FDP_IFF.1.6-NIAP-0407 The TSF shall explicitly deny an information flow based on the following rules:

[selection: no explicit denial rules]

FDP_IFF.5 No Illicit Information Flows

Dependencies: AVA_CCA.3, FDP_IFC.1

FDP_IFF.5.1 The TSF shall ensure that no illicit information flows exist to circumvent [assignment: *the Unidirectional Flow SFP*].

6.1.2 Protection of the TSF (FPT)

The IL-DDD functionality requirements of this class relate to the management and integrity of the mechanisms of the TSF and to the integrity of the TSF data.

FPT_FLS Fail Secure

The requirements of this family ensure that the TOE will not violate its TSP in the event of identified categories of failures in the TSF.

FPT_FLS.1 Failure with Preservation of Secure State

Dependencies: ADV_SPM.1

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [assignment: *a single hardware failure occurs*].

FPT_RVM Reference Mediation

The requirements of this family address the “always invoked” aspect of a traditional reference monitor. The goal of this family is to ensure, with respect to a given SFP, that all actions requiring policy enforcement are validated by the TSF against the SFP.

FPT_RVM.1 Non-bypassability of the TSP

Dependencies: none

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.

FPT_SEP Domain Separation

The components of this family ensure that at least one security domain is available for the SF’s own execution and that the SF is protected from external interference and tampering by untrusted subjects.

FPT_SEP.3 Complete Reference Monitor

Dependencies: none

FPT_SEP.3.1 The unisolated portion of the TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.3.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

FPT_SEP.3.3 The TSF shall maintain the part of the TSF that enforces the access control and/or information flow control SFP in a security domain for its own execution that protects them from interference and tampering by the remainder of the TSF and by subjects untrusted with respect to the TSP.

6.2 TOE Security Assurance Requirements

Assurance requirement components are those of Evaluation Assurance Level 7 (EAL 7; Formally Verified Design and Tested), augmented with the additional vulnerability assessment class AVA_CCA.3 Exhaustive Covert Channel Analysis. These requirements are listed in

Assurance Class	Assurance Components		Dependencies
ACM: Configuration Management	ACM_AUT.2	Complete CM automation	ACM_CAP.3
	ACM_CAP.5	Advanced support	ALC_DVS.2
	ACM_SCP.3	Development tools CM coverage	ACM_CAP.3
ADO: Delivery and operation	ADO_DEL. 3	Prevention of modification	ACM_CAP.3
	ADO_IGS.1	Installation, generation, and start-up procedures	AGD_ADM.1
ADV: Development	ADV_FSP.4	Formal functional specification	ADV_RCR.1
	ADV_HLD.5	Formal high-level design	ADV_FSP.4, ADV_RCR.3
	ADV_IMP.3	Structured implementation of the TSF	ADV_INT.1, ADV_LLD.1, ADV_RCR.1, ALC_TAT.1
	ADV_INT.3	Minimisation of complexity	ADV_IMP.2, ADV_LLD.1
	ADV_LLD.2	Semiformal low-level design	ADV_HLD.3, ADV_RCR.2
	ADV_RCR.3	Formal correspondence demonstration	
	ADV_SPM.3	Formal TOE security policy model	ADV_FSP.1
AGD: Guidance documents	AGD_ADM.1	Administrator guidance	ADV_FSP.1
	AGD_USR.1	User guidance	ADV_FSP.1
ALC: Life cycle support	ALC_DVS.2	Sufficiency of security measures	
	ALC_LCD.3	Measurable life-cycle model	
	ALC_TAT.3	Compliance with implementation standards - all parts	ADV_IMP.1
ATE: Tests	ATE_COV.3	Rigorous analysis of coverage	ADV_FSP.1, ATE_FUN.1
	ATE_DPT.3	Testing: implementation representation	ADV_HLD.2, ADV_IMP.2, ADV_LLD.1, ATE_FUN.1
	ATE_FUN.2	Ordered functional testing	

Assurance Class	Assurance Components		Dependencies
	ATE_IND.3	Independent testing - complete	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1
AVA: Vulnerability assessment	AVA_CCA.3	Exhaustive covert channel analysis	ADV_FSP.2, ADV_IMP.2, AGD_ADM.1, AGD_USR.1
	AVA_MSU.3	Analysis and testing for insecure states	ADO_IGS.1, ADV_FSP.1, AGD_ADM.1, AGD_USR.1
	AVA_SOF.1	Strength of TOE security function evaluation	ADV_FSP.1, ADV_HLD.1
	AVA_VLA.4	Highly resistant	ADV_FSP.1, ADV_HLD.2, ADV_IMP.1, ADV_LLD.1, AGD_ADM.1, AGD_USR.1

Table 2 – Assurance Requirements

Refer to CC part 3 for the detail associated with each of these assurance requirements.

7. TOE Summary Specifications

The goal of the IL-DDD is to provide INFORMATION flow from the LOW SIDE sourceto the HIGH SIDE destination without compromising the confidentiality of the INFORMATION on the HIGH SIDE NETWORK.

This section describes the TOE Security Functions (TSF) that meet the security functional requirements specified for the IL-DDD in Section 6.1. They are specified using both an informal and formal style. The formal style can be found in Interactive Link Formal Policy and Architecture Document DSTO-TR-961625P01000014.

7.1 Statement of TOE Security Functions

The IL-DDD provides the following security function (SF).

SF.DD **Data Diode Function:** The ***SF.DD*** prevents data from being transmitted from the HIGH SIDE NETWORK to the LOW SIDE NETWORK, while allowing data to be transmitted from the LOW SIDE NETWORK to the HIGH SIDE NETWORK.

The ***SF.DD*** function ensures that data flows from the LOW SIDE NETWORK to the HIGH SIDE NETWORK. The ***SF.DD*** ensures that processes, application or USERS on the LOW SIDE NETWORK cannot get access to INFORMATION on the HIGH SIDE NETWORK via the IL-DDD in accordance with the security objectives.

The data can be passed from the LOW SIDE NETWORK to the HIGH SIDE NETWORK via an IL-DDD and the data on the HIGH SIDE NETWORK is kept confidential from the LOW SIDE. The IL-DDD is implemented in hardware and guarantees that data cannot flow from the HIGH SIDE NETWORK to the LOW SIDE NETWORK. There is no “back channel” for communication hand shaking, which could be used as a covert channel.

The IL-DDD consists of a single functional block, the Unidirectional Optical Fibre Repeater implemented in hardware within an isolated security domain. It consists of a purpose built Fibre Optic Receiver, an integrated circuit Buffer and a Fibre Optic Transmitter, constructed from discrete components. The Unidirectional Optical Fibre Repeater functional block receives data input that it then retransmits as data output. It provides the security enforcing functionality of the Data Diode Device. The receiver (input only from the LOW SIDE) and transmitter (output only to the HIGH SIDE) provide the only interfaces to the IL-DDD. There is only a single data path from input to output and no separate control functionality.

The IL-DDD has been designed, developed and implemented so that if a component fails it will not violate the *Unidirectional Flow SFP*. This has been achieved in hardware, the lowest level of abstraction; the SF has been designed by ensuring that a single failure will not result in HIGH SIDE data being made available to the LOW SIDE. The ***SF.DD*** utilises redundant components providing the same security functionality. The redundant components have been placed in series within the SF. If a failure occurs the functionality of the unidirectional flow will not be available and the security of the HIGH SIDE INFORMATION shall be preserved.

7.2 Assurance Measures

This section describes the assurance measure of the TOE which meet the security assurance requirements specified for the IL-DDD in Section 0. The requirements are mapped to the actual deliverable that provide the information in section 9.3.2.

7.2.1 Configuration Management

1. Rationale Clearcase version 4.0 is the tool used by the automated CM system that has been established for the development and maintenance of the TOE.
2. The system is based on the CM plan.
3. The system ensures the integrity of the TOE by defining baselines and providing a method of tracking any changes.
4. All changes are authorised by the Configuration Control Board in accordance with CM plan.

7.2.2 Delivery and Operation

1. The IL-DDD is delivered to the end customer by a process that ensures non-repudiation and is documented in work instructions.
2. An approved courier distributes the product from the secure manufacturing facility and the end customers must acknowledge receipt.
3. Upon arrival the user installs and start-up the TOE in accordance with the Administration Manual.
4. The system within which the TOE has been installed needs to be accredited by its SECURITY AUTHORITY before it can be used.

7.2.3 Development

1. The IL-DDD has a functional specification.
2. There is a formal model of the TSP
3. The IL-DDD TSF are defined formally using both the Z specification language and HOL (Higher Order Logic) theory of the Isabelle theorem prover.
4. The High Level design of IL-DDD, its Architecture, is defined both formally and informally.
5. The Low-Level design, the detailed design, is defined using a semiformal method.
6. The design has been structured in a modular layered format that minimises complexity.
7. The Implementation representation is at the level of schematic diagram, printed circuit board layout and parts list of the hardware. This defines the TSF to a level that is an unambiguous and thus requires no further design decisions.
8. The implementation documentation defines the correspondence between the formal specifications of the TSF and how it has been implemented.

7.2.4 Guidance Documents

1. There is a single Administration Manual for the IL-DDD.
2. The system administrator is the only USER of the IL-DDD; all operations that use the IL-DDD are invisible to the end USER.
3. The Administration Manual defines the process for installing the IL-DDD for secure operation.
4. The Administration Manual describes the assumptions regarding the secure operation of the TOE.

7.2.5 Life Cycle Support

1. The Australian Department of Defence has accredited the development environment.
2. The development security is documented and includes physical, procedural, personnel and other security measures that are necessary to protect the confidentiality and integrity of the IL-DDD.
3. The life-cycle model is defined in a series of plans that describe the development and maintenance practices and procedures.
4. The life-cycle model is measured based on a Cost Schedule Control System.
5. A list of all tools used in the development of the IL-DDD is maintained.
6. Documented procedures define the implementation of the tools used to develop the IL-DDD.

7.2.6 Tests

1. An analysis of the test coverage is provided in the test plan.
2. Testing occurs at the lowest level of design.
3. The testing consists of a plan, test procedures, expected results and actual results.
4. The IL-DDD was independently tested by an Australasian Information Security Evaluation Facility (AISEF) as described in EFA T010 Data Diode Device Sanitized Evaluation Technical Report.

7.2.7 Vulnerability Assessment

1. An exhaustive covert channel analysis was conducted and documented.
2. The guidance documentation has been assessed within the operational vulnerability assessment
3. The TOE security function has been implemented in hardware with multiple levels of redundancy, and cannot be circumvented.
4. There are no permutation or probabilistic SFR and thus there is no strength of function rating allocated to the SF..
5. During development an analysis into potential misuse scenarios has been conducted to determine whether the IL-DDD can be configured or used in a manner that is insecure but

that an administrator or user of the TOE would reasonably believe to be secure. Any potential misuse scenarios have been prevented by appropriate countermeasures.

6. An assessment of the operational vulnerabilities has been carried out and documented.
7. An assessment of the constructional vulnerabilities has been carried out and documented.

8. PP Claims

There are no Protection Profile claims.

9. Rationale

9.1 Introduction

This section provides the rationale for the manner in which the security objectives address the threats and assumptions associated with the TOE. The security objectives rationale is followed by the rationale for the adequacy of the security functional requirements and the security assurance requirements in meeting the security objectives of the TOE.

9.2 Security Objectives Rationale

Table 3 - Threats/Assumptions/Objectives Mapping, demonstrates how all threats and assumptions are covered by at least one of the security objectives of the TOE, and that each security objective covers at least one threat or assumption. The coverage of each of the security objectives of the TOE are discussed in Tables 4 and 5.

Table 4 - Threats/Objectives Rationale, demonstrates how the objectives of the TOE and the TOE environment counter the threats identified in Section 4.2.

Table 5 - Assumptions/Objectives Rationale demonstrates how the objectives of the TOE and the TOE environment address the assumptions identified in Section 4.1.

Threats Objective/Assumptions	T.TRANFER	T.TAMPER	T.FAILURE	T.LOGIC	A.PERSONNEL	A.PHYSICAL	A.EMISSION	A.INSTALLATION	A.TRAINING	A.NETWORK	A.NO_EVIL
O.CONFIDENTIALITY	✓										
O.INVOKE	✓										
O.FAILSECURE			✓								
O.TAMPER_SEALS		✓									
O.ROM				✓							
OE.PERSONNEL		✓			✓			✓			✓
OE.PHYSICAL	✓	✓				✓	✓				
OE.EMISSION							✓				
OE.INSTALLATION								✓		✓	
OE.TRAINING					✓			✓	✓		
OE.NETWORK										✓	
OE.NO_EVIL					✓			✓		✓	✓

Table 3 - Threats/Assumptions/Objectives Mapping

Threats	Objectives	Rationale
T.TRANSFER	O.CONFIDENTIALITY O.INVOKE OE.PHYSICAL	The threat that data will be transferred from the HIGH SIDE NETWORK to the LOW SIDE NETWORK through the IL-DDD is partially mitigated by O.CONFIDENTIALITY (FDP_IFC.2, FDP_IFF.1, FDP_IFF.5). O.CONFIDENTIALITY achieves this by explicitly prohibiting any flows from the HIGH SIDE NETWORK through the IL-DDD to the LOW SIDE, including flows that might take place through the use of covert channel. Thus both explicit and implicit flows are covered. ***** O.INVOKE ensures that all SFs are invoked at all times. At no time, even when power is removed, can the IL-DDD be bypassed to transfer data from the HIGH SIDE to the LOW SIDE, thereby partially mitigating T.TRANSFER. ***** OE.PHYSICAL ensures that the IL-DDD is operated and stored within a physically secure environment that, at minimum, meets the requirements for the HIGH SIDE. This mitigates the risk that unauthorised personnel have access to the Interactive Link devices at any time. ***** O.CONFIDENTIALITY, O.INVOKE and OE.PHYSICAL collectively serve to counter the threat of T.TRANSFER.
T.TAMPER	O.TAMPER_SEALS OE.PHYSICAL OE.PERSONNEL	The threat T.TAMPER is associated with an adversary tampering with the contents of the IL-DDD to compromise its security functionality prior to operation. This threat is reduced by the objectives O.TAMPER_SEAL and supported by OE.PERSONNEL and OE.PHYSICAL. ***** T.TAMPER is partially mitigated by the use of tamper evident seals, in accordance with O.TAMPER_SEALS. O.TAMPER_SEALS ensures that the TOE devices are tamper evident sealed. These seals provide an indication if an attempt has been made to tamper with the contents of the IL-DDD to cause the compromise of the confidentiality of some HIGH SIDE INFORMATION. This seal is monitored by the SYSTEM MANAGEMENT STAFF. Any attempt to access the contents of either the devices will be clearly visible. ***** T.TAMPER is alleviated further by the environmental object OE.PHYSICAL, which ensures that the TOE of the Interactive Link are operated and stored within a physically secure environment that, at minimum, meets the requirements for the HIGH SIDE. This mitigates the risk that unauthorised personnel have access to the IL-DDD at any time.

Threats	Objectives	Rationale
		Finally, OE.PERSONNEL ensures that personnel with access to the device are vetted and cleared to the classification of the HIGH SIDE Network. The countermeasures discussed above sufficiently mitigate the T.TAMPER threat, should an adversary attempt to tamper with the contents of the IL-DDD during delivery and/or after installation. The intrusion attempt would be clearly visible and appropriate actions would be taken to preserve the confidentiality of information stored on the HIGH SIDE network.
T.FAILURE	O.FAILSECURE	O.FAILSECURE mitigates the T.FAILURE threat scenario. In the event of a single component failure, O.FAILSECURE ensures that the TOE will preserve a secure state and the SFs, though they may not be operational, will remain secure. The IL-DDD has been designed with multiple levels of redundancy in the hardware components of the IL-DDD. Regardless of the type of failure, O.FAILSECURE ensures that information cannot pass from the HIGH SIDE NETWORK to the LOW SIDE NETWORK, thus countering T.FAILURE. *Note*: A Failure Modes Effects Analysis was conducted for all components of the SFs, which amplifies that a single failure shall not result in a violation of the Non-Interference TSP. Due to the fact that all failures may not be evident and undetected failures may exist, the probability of failures has been calculated. This information enables the user to determine the period within which potential multiple failures may occur. The Mean Time Between Failures (MTBF) for the IL-DDD is 308,790 hours (35.25 years).
T.LOGIC	O.ROM	The threat that a USER or process on the LOW SIDE NETWORK transmits data to the TOE that causes a modification to the TSF is a Logical attack. The TSF is implemented in hardware. O.ROM prevents changes to the hardware. The threat T.LOGIC is mitigated by O.ROM.

Table 4 - Threats/Objectives Rationale

Assumptions	Objectives	Rationale
A.PERSONNEL	OE.PERSONNEL OE.NO_EVIL OE.TRAINING	A.PERSONNEL assumes that the IL-DDD shall be installed, administered and used by authorised personnel who possess the necessary privileges to access the HIGH SIDE INFORMATION. OE.PERSONNEL ensures that all personnel, including those responsible for the installation of the IL-DDD, are vetted and cleared to the security level of the HIGH SIDE. *****

Assumptions	Objectives	Rationale
		OE.NO_EVIL reduces the risk that users of the TOE are non-hostile and follow all usage guidance to ensure that the IL-DDD is operated in a secure manner. ***** OE.TRAINING ensures that personnel who have access to secure Information Systems of the security level of the HIGH SIDE are trained in the reasons for security, how the security has been implemented, why it has been implemented in that way and their responsibilities in ensuring that the security of the Information System is maintained. This objective is intended to prevent incorrect installation and accidental misuse of the IL-DDD in a way that may result in a compromise of HIGH SIDE INFORMATION. ***** Collectively, these objectives mitigate the risk of unauthorised users gaining access to and interfering with the IL-DDD TOE before, during or after installation.
A.PHYSICAL	OE.PHYSICAL	A.PHYSICAL assumes that the intended environment will be capable of storing and operating the IL-DDD, in accordance with the requirements of the HIGH SIDE NETWORK. Information systems have different requirements for the storage of computer equipment used for processing information of different security levels. There may also be a requirement for protecting critical system resources within secured rooms. The IL-DDD is critical to all the USERS and requires no administrator control after it has been installed. It is the SYSTEM MANAGEMENT STAFF responsibility to protect it from accidental or deliberate tampering causing its functionality to be bypassed. OE.PHYSICAL ensures that the IL-DDD TOE is operated and stored within a physically secure environment that, at minimum, meets the requirements for the HIGH SIDE. This mitigates the risk that unauthorised personnel have access to the IL-DDD at any time, and requires the installation of the IL-DDD to be accredited by the SECURITY AUTHORITY of the HIGH SIDE NETWORK, which involves independent inspection of the installation.
A.EMISSION	OE.EMISSION OE.PHYSICAL	The A.EMISSION assumes that the IL-DDD TOE will operate in an environment where physical (or some other) security measures prevent any TEMPEST attack. OE.PHYSICAL ensures that the TSC of the IL-DDD is operated and stored within a physically secure environment that, at minimum, meets the requirements for the HIGH SIDE. ***** OE.EMISSION ensures that the IL-DDD is operated in an environment where their respective ERTZ is within the secure boundary of the HIGH SIDE system. This ensures that any attempts to mount a TEMPEST attack

Assumptions	Objectives	Rationale
		will not compromise the security of the information system.
A.INSTALLATION	OE.INSTALLATION OE.PERSONNEL OE.NO_EVIL OE.TRAINING	OE.INSTALLATION ensures that the IL-DDD is installed by SYSTEM MANAGEMENT STAFF in accordance with the administration manuals and the installation is to be accredited by the appropriate SECURITY AUTHORITY. This prevents the incorrect installation of the HIGH and LOW SIDE INTERFACE PORTS, thus protecting the confidentiality of the HIGH SIDE INFORMATION. ***** OE.PERSONNEL ensures that all personnel, including the personnel responsible for the installation of the IL-DDD, are vetted and cleared to the security level of the HIGH SIDE. ***** OE.NO_EVIL ensures that users of the TOE are non-hostile and follow all usage guidance to ensure that the IL-DDD is operated in a secure manner. This objective helps to ensure a correct and secure installation. ***** OE.TRAINING ensures that personnel who have access to secure Information Systems of the security level of the HIGH SIDE are trained in the reasons for security, how the security has been implemented, why it has been implemented in that way and their responsibilities in ensuring that the security of the Information System is maintained. This objective is intended to prevent incorrect installation and accidental misuse of the Interactive Link in a way that may result in a compromise of HIGH SIDE INFORMATION. ***** Collectively, OE.INSTALLATION, OE.PERSONNEL, OE.NO_EVIL and OE.TRAINING ensures that the trusted IL-DDD will be installed correctly and in accordance with the guidance documentation.
A.TRAINING	OE.TRAINING	OE.TRAINING ensures that personnel who have access to secure Information Systems of the security level of the HIGH SIDE are trained in the reasons for security, how the security has been implemented, why it has been implemented in that way and their responsibilities in ensuring that the security of the System is maintained. This objective is intended to prevent incorrect installation and accidental misuse of the IL-DDD in a way that may result in a compromise of HIGH SIDE INFORMATION.
A.NETWORK	OE.NETWORK OE.INSTALLATION OE.NO_EVIL	OE.NETWORK ensures that the IL-DDD is the only method of interconnecting the LOW and HIGH SIDE NETWORKs. If an untrusted product is used to connect the LOW SIDE to the HIGH SIDE NETWORKs it may result in a compromise of HIGH SIDE INFORMATION and thus circumvent the security being provided by the IL-DDD.

Assumptions	Objectives	Rationale
		***** OE.INSTALLATION ensures that the Interactive Link is installed by SYSTEM MANAGEMENT STAFF in accordance with the user and administration manuals and the installation is to be accredited by the appropriate SECURITY AUTHORITY. This objective ensures that only IL-DDD is installed to connect the HIGH and LOW SIDE networks. Additionally, this objective prevents the incorrect installation of the HIGH and LOW SIDE INTERFACE PORTS, thus protecting the confidentiality of the HIGH SIDE INFORMATION. ***** OE.NO_EVIL reduces the risk by ensuring that users of the TOE are non-hostile and follow all usage guidance to ensure that the IL-DDD is installed, configured and operated in a secure manner. No other methods of interconnecting the high and LOW SIDE networks are installed
A.NO_EVIL	OE.NO_EVIL OE.PERSONNEL	OE.NO_EVIL reduces the risk that authorized users of the TOE are non-hostile and will follow all usage guidance to ensure that the IL-DDD is installed and operated in a secure manner. ***** OE.PERSONNEL ensures that all personnel, including the personnel responsible for the installation of the IL-DDD, are vetted and cleared to the security level of the HIGH SIDE. This objective provides further assurance that authorised users of the TOE are non-hostile. A user who is vetted and cleared is assumed to be non-hostile.

Table 5 - Assumptions/Objectives Rationale

9.3 Security Requirements Rationale

This section provides the evidence that demonstrates that the security requirements of the Interactive Link are a complete and cohesive set that is suitable to meet the security objective.

Objectives	O.CONFIDENTIAITY	O.INVOKE	O.FAILSECURE	O.TAMPER_SEALS	O.ROM
SFRs					
FDP_IFC.2/ FDP_IFF.1	✓				
FDP_IFF.5	✓				
FPT_FLS.1			✓		
FPT_SEP.3					✓
FPT_RVM.1		✓			
AGD_ADM.1				✓	
AGD_USR.1				✓	
ADO_DEL.3				✓	

Table 6 - Security Requirements/Objectives Mapping

9.3.1 Functional Security Requirements Rationale

All security objectives as defined in Section 5.1 Security Objectives for the TOE are met by functional security requirements with one exception; O.TAMPER_SEALS which is a TOE Security Objective that is satisfied by security assurance requirements. Table 6 - Security Requirements/Objectives Mapping, provides a mapping between the security requirements and the objectives that have been defined in Section 6; Table 7 – Security Requirements/Objectives Rationale, provides a detailed rationale of this mapping.

Objectives	Security Functional Requirement	Rationale
O.CONFIDENTIALITY	FDP_IFC.2 Complete Information Flow Control FDP_IFF.1 Simple Security Attributes FDP_IFF.5 No Illicit Information Flows	O.CONFIDENTIALITY is achieved through the diode functionality implemented in the IL-DDD, which serves to enforce the FDP_IFC.2, FDP_IFF.1, and FDP_IFF.5 requirements. ***** FDP_IFC.2 defines that the policy of the *Unidirectional Flow SFP:* USER DATA cannot flow from the HIGH SIDE PORT to the LOW SIDE PORT; while USER DATA can flow from the LOW SIDE PORT to the HIGH SIDE PORT via the IL-DDD is enforced by the ***SF.DD***. Enforcing the Data Diode Non-interference SFP through FDP_IFC.2 helps achieve the objective of O.CONFIDENTIALITY. ***** FDP_IFF.1 identifies the rules for the IL-DDD that are required to enforce the *Unidirectional Flow SFP*. FDP_IFF.1 is based on the IL-DDD INTERFACE PORT

Objectives	Security Functional Requirement	Rationale
		attributes and USER DATA security attributes. These attributes are defined through FDP_IFF.1 and are required to achieve the SFP rules and the O.CONFIDENTIALITY objective. FDP_IFF.1 requires that all low side information be allowed to flow from the LOW SIDE INPUT INTERFACE PORT to the HIGH SIDE OUTPUT INTERFACE PORT. Additionally, FDP_IFF.1 requires that no information flow from the HIGH SIDE OUTPUT INTERFACE PORT to the LOW SIDE INPUT INTERFACE PORT. This is how the FDP_IFF.1 and FDP_IFC.2 help achieve the O.CONFIDENTIALITY objective. ***** FDP_IFF.5 further maintains the objective by ensuring that at all times within the IL-DDD there are no covert channels or unintended signalling channels from the HIGH SIDE to the LOW SIDE that would compromise the confidentiality of the HIGH SIDE INFORMATION.
O.INVOKE	FPT_RVM.1 Non-bypassability of the TSP	O.INVOKE ensures that the TOE is invoked in accordance with the *Unidirectional Flow SFP* at all times. This ensures that at no time can the IL-DDD be bypassed to transfer data through the TOE from the HIGH SIDE to the LOW SIDE. O.INVOKE is achieved by enforcement of FPT_RVM.1. ***** FPT_RVM.1 requires that the TSP is invoked and the SFs cannot be bypassed, even in the event that power is removed from the TOE. The FPT_RVM.1 requirement ensures that the *Unidirectional Flow SFP* will be enforced at all times during TOE operation and that the TSP enforcing functions are always invoked before power is applied and when the function within the IL-DDD is executed, thus preserving the O.INVOKE objective.
O.FAILSECURE	FPT_FLS.1 Failure with Preservation of Secure State	In the event of a single component failure, O.FAILSECURE ensures that the TOE will preserve a secure state and the SF, though it may not be operational, will remain secure. FPT_FLS.1 implements the O.FAILSECURE objective by ensuring that, in the event of a single hardware component failure, the TOE will preserve a secure state. The IL-DDD meet this requirement by having built in redundancy to ensure that the *Unidirectional Flow SFP* is maintained should a single component failure occur.
O.TAMPER_SEALS	AGD_ADM.1 Administrator Guidance AGD_USR.1 User Guidance ADO_DEL.3 Prevention of Modification	O.TAMPER_SEALS maps to the AGD_ADM.1, AGD_USR.1 and ADO_DEL.3 Security Assurance Requirements. Security labels featuring the Tenix logo are affixed across the join between the metal case and the plastic front panel of the IL-DDD devices. These labels are Australian Government Securities Construction and Equipment Committee endorsed tamper-evident seals. A detailed discussion of the tamper-evident seals is located in Section 2 of the guidance documentation supplied with the IL-DDD. Upon receipt of the IL-DDD, the customer must

Objectives	Security Functional Requirement	Rationale
		inspect each device in the shipment to ensure that the tamper-evident seals are intact. In order to gain access to the internal hardware of the IL-DDD, the seals must be broken. If broken, the seals generate a random dot (measled) pattern, providing a visual indication of the attempt to tamper with and modify the device. The tamper evident seals are monitored by the SYSTEM MANAGEMENT STAFF. Any attempt to access the contents of either the devices will be clearly visible.
O.ROM	FPT_SEP.3 Complete Reference Monitor	O.ROM ensures that the TSF shall be protected against unauthorised modification. ***** FPT_SEP.3 requirement, which ensures that there is a security domain available for the SF to execute and that the SF is protected from external tampering and interference by untrusted subjects. Hence the TSF is protected against unauthorised modification.

Table 7 – Security Requirements/Objectives Rationale

9.3.2 Assurance Security Requirements Rationale

The assurance measures provided by the TOE satisfy all of the assurance requirements listed in Section 6.2, TOE Security Assurance Requirements. Table 8 - Assurance Measures, provides a reference between each TOE assurance requirement and the related documentation that satisfies each requirement.

Assurance Component	Documents Satisfying Components	Rational
ACM_AUT.2	B217P00001001 Configuration Management Documentation	The Configuration Management Documentation defines how Rational ClearCase the automated Configuration Management tool is able to support the numerous changes that occur during development and ensure that those changes were authorised.
ACM_CAP.5	B217P00001001 Configuration Management Documentation	The Configuration Management Documentation defines the Interactive Link Configuration Management (CM) System and how the TOE is referenced.
ACM_SCP.3	B217P00001001 Configuration Management Documentation	The Configuration Management Documentation defines how the development environment is maintained under configuration management
ADO_DEL. 3	B217P00001003 Delivery and Operation Procedures	The Delivery and Operation Procedures documentation defines delivery procedures and technical measures that prevent modification and maintain the integrity of the TOE from the secure manufacturing facility to the end user.
ADO_IGS.1	B217P00001003 Delivery and Operation Procedures	The Delivery and Operation Procedures documentation defines the installation procedures to ensure that the IL-DDD is installed and configured securely in the user

Assurance Component	Documents Satisfying Components	Rational
		environment.
ADV_FSP.4	B217P00002002 Functional Specification	The Functional Specification documentation provides a formally defined high-level description of the user-visible interface and behavior of the IL-DDD TSF.
ADV_HLD.5	B217P00002003 High Level Design	The High Level Design documentation provides a description of the TSF in terms of major structural units (i.e. subsystems) and relates these units to the functions that they provide.
ADV_IMP.3	B217P00002008 Implementation for Data Diode Device	The Implementation documentation provides hardware schematics and circuit board layout of the detailed internal workings of the TSF.
ADV_INT.3	B217P00002005 TSF Internals	This document defines how the TSF of the Interactive Link have been implemented within the TOE at the lowest level of abstraction, in hardware & firmware.
ADV_LLD.2	B217P00002009 Semiformal Low-level Design for Data Diode Device	The Semiformal Low-level Design documentation provides a semi-formal low-level design of the TOE and describes the internal workings of the TSF in terms of modules and their interrelationships and dependencies.
ADV_RCR.3	B217P00002007 Correspondence Demonstration for Interactive Link	The Correspondence Demonstration provides an analysis of correspondence between all adjacent pairs of TSF representations.
ADV_SPM.3	B217P00002001 Security Policy Model	The Security Policy Model Documentation provides the TSP, and establishing a correspondence between the functional specification and the security policy model of the TSP.
AGD_ADM.1	B217P00003001 Guidance Documentation	The Guidance Documentation provides written material that is intended to be used by those persons responsible for configuring, maintaining, and administering the TOE in a correct manner for maximum security.
AGD_USR.1	B217P00003001 Guidance Documentation	The Guidance Documentation describes the security functions provided by the TSF and provides instructions and guidelines, including warnings, for its secure use.
ALC_DVS.2	B217P00001004 Life Cycle Support Documentation	The Life Cycle Support documentation references development security measures of the TOE. It is concerned with physical, procedural, personnel, and other security measures that have been used in the development environment to protect the TOE.
ALC_LCD.3	B217P00001004 Life Cycle Support Documentation	The Life Cycle Support documentation describes how a standardised and measurable life-cycle model was used to develop and maintain the TOE.
ALC_TAT.3	B217P00001004 Life Cycle Support Documentation	Within the Life Cycle Support documentation all programming languages, compiles and other tools used to develop the TOE are documented.
ATE_COV.3	B217P00004001 Tests	The Test documentation lists all the tests associated with the Interactive Link and references them all back to the formal functional requirements as defined in the Formal Architecture and Security Policy document.

Assurance Component	Documents Satisfying Components	Rational
ATE_DPT.3	B217P00004001 Tests	The Test documentation tests the IL at all functional subsystems down to the basic components.
ATE_FUN.2	B217P00004001 Tests	The Test documentation demonstrates that all security functions perform as specified.
ATE_IND.3	B217P00004001 Tests	The Test documentation demonstrates that all security functions perform as specified.
AVA_CCA.3	B217P00005001 Binding and Covert Channel Analysis	The Binding and Covert Channel Analysis identifies potential vulnerabilities through an exhaustive search for covert channels.
AVA_MSU.3	B217P00005005 Analysis and Testing for Insecure States for Interactive Link B217P00005002 Analysis and Testing for Insecure States for Data Diode Device	This analysis documentation defines how misleading, unreasonable and conflicting guidance is absent from the guidance documentation, and that secure procedures for all modes of operation have been addressed.
AVA_SOF.1	B217P00005004 Vulnerability Analysis – Highly Resistant for Data Diode Device	The Vulnerability Analysis justifies that there are no probabilistic or permutational mechanisms within the IL-DDD; therefore, no strength of function claim has been made.
AVA_VLA.4	B217P00005004 Vulnerability Analysis – Highly Resistant for Data Diode Device	The Vulnerability Analysis ascertains the minimal presence of security vulnerabilities, and confirms that they cannot be exploited in the intended environment for the TOE.

Table 8 - Assurance Measures

9.3.2.1 Rationale for TOE Assurance Requirements

The IL-DDD provides a high level of assurance for systems made up of COTS products. Such systems normally run using the System-High mode of operation. The IL-DDD is to bridge the secure boundary of such a system, this represents an extremely high risk of potential for INFORMATION of the system to be compromised. EAL7 is applicable to the development of security TOEs for application in extremely high risk situation. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis; the IL-DDD is such a product.

9.3.3 Dependencies Analysis

The dependencies of the security functional requirements of the Interactive Link are defined in Table 9.

Dependencies	FDP_IFC.1	FDP_IFF.1	FMT_MSA.3‡	AVA_CCA.3	ADV_SPM.1
SFRs					
FDP_IFC.2		✓			
FDP_IFF.1	✓		✓		
FDP_IFF.5	✓			✓	
FPT_FLS.1					✓
FPT_RVM.1					
FPT_SEP.3					

‡ *This dependency has not been met by the IL-DDD, refer to section 9.3.3.1.*

Table 9 - Mapping of Security Functional Requirements Dependencies

9.3.3.1 Dependencies Not Met

The dependency of FMT_MSA.3 - Static Attributes Initialisation is not met by the IL-DDD.

There are no management requirements for the IL-DDD INTERFACE PORTS. The attributes of LOW SIDE INPUT and HIGH SIDE OUTPUT are established at the initial installation of this hardware device.

The dependency ADV_SPM.1 - Informal TOE Security Policy Model and FDP_IFC.1 – Subset Information Flow Control is met by meeting the requirements of the components higher within the family hierarchical structure namely, ADV_SPM.3 and FDP_IFC.2 respectively.

9.3.4 Mutually Supportive Requirements

The dependency analysis provided in Section 9.3.3, Dependencies Analysis, Section 9.3.3.1 Dependencies Not Met, and Table 10 - Classification of Mutually Supportive Requirements, demonstrate that the SFRs are complete and internally consistent.

The primary function of the IL-DDD is to prevent HIGH SIDE data from flowing to the LOW SIDE while allowing LOW SIDE data to flow to the HIGH SIDE. Thus protecting the asset, HIGH SIDE INFORMATION, is provided by the SFRs from the FDP class.

SFRs from the FPT class provide further support to the primary function by providing appropriate protection of the TSF, preventing bypass of the TOE security policy (FPT_RVM.1). While FPT_FLS.1 ensures that a single failure of the TOE will not result in a compromise of HIGH SIDE INFORMATION. An exhaustive covert channel analysis as defined by AVA_CCA.3 is provided in support of FDP_IFF.5.

By definition, all assurance requirements support all SFRs since they provide confidence in the correct implementation and operation of the SFRs.

Purpose	Security Requirement	Description
Information Flow	FDP_IFC.2 Complete Information Flow Control	These provide the primary security functionality of the TOE, which is based on the objective ***O.CONFIDENTIALITY.***
	FDP_IFF.1 Simple Security Attributes	
SF Invocation and Isolation	FPT_RVM.1 Non-bypassability of the TSP	Protection of the SF through invocation and isolation are also supportive type functions based on the objectives ***O.INVOKE*** and ***O.ROM.***
	FPT_SEP.3 Complete Reference Monitor	
Prevention of Unintended Signalling Channels	FDP_IFF.5 No Illicit INFORMATION Flows	These requirements further support the primary functionality by ensuring that there is no way to circumvent the primary functionality. These requirements are based on ***O.CONFIDENTIALITY, O.FAILSECURE, O.TAMPER_SEALS and O.INVOKE.***
	AVA_CCA.3 Exhaustive Covert Channel Analysis	
	FPT_RVM.1 Non-bypassability of the TSP	
	FPT_FLS.1 Failure with Preservation of a Secure State	
	AGD_ADM.1 Administrator Guidance	
	AGD_USR.1 User Guidance	
	ADO_DEL.3 Prevention of Modification	

Table 10 - Classification of Mutually Supportive Requirements

9.3.5 Strength of Function Claim

There are no probabilistic or permutational mechanism within the IL-DDD; therefore, no strength of function claim has been made.

9.4 TOE Summary Specification Rationale

Table 11 - Mapping between SF and SFRs, demonstrates that each SFR is mapped onto at least one security function and that each security function is mapped onto at least one SFR. An explanation of the mapping provided by Table 11 is discussed below in Section 9.4.1 Correlation between SF and SFRs. Section 9.4.1 details how the specified security functions identified in Section 7.1, Statement of TOE Security Functions are suitable to meet all the SFRs specified in Section 6.1 TOE Security Functional Requirements.

Security Functions **SFRs**	SF.DD
FDP_IFC.2 / FDP_IFF.1	✓
FDP_IFF.5	✓
FPT_FLS.1	✓
FPT_RVM.1	✓
FPT_SEP.3	✓

Table 11 - Mapping between SF and SFRs

9.4.1 Correlation between SF and SFRs

FDP_IFC.2 & FDP_IFF.1 The *Unidirectional Flow SFP* is enforced by ***SF.DD***.

SF.DD ensures that information flows from the LOW SIDE to the HIGH SIDE while preventing HIGH SIDE INFORMATION from flowing to the LOW SIDE.

The FDP_IFC.2 SFR is definitional and is used to set up the parameters to be used in the FDP_IFF.1 requirement. FDP_IFC.2 defines that the *Unidirectional Flow SFP*, which is the Information flow control policy used within the ***SF.DD***. FDP_IFC.2 also defines the *subjects*: INTERFACE PORTS and *information*: USER DATA that implement the information flow control policy. The *Unidirectional Flow SFP* has been defined as: LOW SIDE *subjects* and *information* are not influenced by HIGH SIDE *subjects* and *information*, the HIGH SIDE does not interfere with the LOW SIDE.

FDP_IFF.1 define the attributes of the different instances of the subjects and information before defining the rule set for information flow. The ***SF.DD*** has two INTERFACE PORTS; the LOW SIDE INPUT and the HIGH SIDE OUTPUT INTERFACE PORTS. There are two forms of USER DATA defined for the ***SF.DD*** LOW SIDE and HIGH SIDE associated with the data resident on the LOW and HIGH SIDE NETWORKS respectively.

The following rules have been defined for the *Unidirectional Flow SFP* within the FDP_IFF.1 requirement the first is the single “permit” rule while the second is the only “deny” rule:

1. All LOW SIDE USER DATA shall be allowed to flow from the LOW SIDE INPUT INTERFACE PORT to the HIGH SIDE OUTPUT INTERFACE PORT
2. No information shall flow from the HIGH SIDE OUTPUT INTERFACE PORT to the LOW SIDE INPUT INTERFACE PORT

The *Unidirectional Flow SFP* is implemented by the ***SF.DD***.

SF.DD is implemented within the IL-DDD. The IL-DDD has two data interfaces an input and an output, which map to the LOW SIDE INPUT INTERFACE PORT and the HIGH SIDE OUTPUT INTERFACE PORT respectively. Due to the diode functionality which ensures a unidirectional data flow from the input to the output the ***SF.DD*** implements the rule set defined in the FDP_IFF.1 SFR.

FPT_FLS.1 The SF preserve a secure state in the face of identified failures to ensure the TOE does not violate its TSP.

The SF of the IL-DDD will maintain their secure state in the event of a component failure. Failure may result in functionality being diminished or non existent though the preservation of a secure state is maintained by the TSF through the implementation of redundant components that enforce the FPT_FLS.1 requirement. The implementation of FPT_FLS.1 ensures that the TSF will uphold the objectives of the IL-DDD, ensuring the TOE does not violate its *Unidirectional Flow SFP*.

The IL-DDD has been designed, developed and implemented so that if a single component fails, the failure will not result in a violation of the *Unidirectional Flow SFP*. Assurance of secure state preservation has been achieved in hardware; the SF have been designed by ensuring that a single component failure will not result in HIGH SIDE data being made available to the LOW SIDE. The method utilises redundant components, within the ***SF.DD*** SF. The components of the ***SF.DD*** have been placed in series using a unidirectional optical fibre receiver, buffer and unidirectional optical fibre transmitter, constructed from discrete commercial components. If a component fails by becoming short circuit the unidirectional functional shall be maintained by the other components. If the component fails by going open circuit the functionality will also fail but the security as defined by the *Unidirectional Flow SFP* shall be preserved. The redundant components discussed herein, have been selected such that flaws within the common components will not result in a violation of the *Unidirectional Flow SFP*.

FPT_RVM.1 The SF ensure that the TSP enforcement functions are invoked at all times.

The FPT_RVM.1 requirement is realised by the ***SF.DD*** SF. This SF implements the TSP and ensure that it is always invoked and cannot be bypassed. The FPT_RVM.1 requirement applies to three states of the IL-DDD; *power-off* state, *power-on* state *and power-on fault* state. The *power-on fault* state is addressed by FPT_FLS.1 (discussed in the preceding section).

As the SF is implemented in the hardware within the IL-DDD, it maintains a secure state behaviour when power is removed. While the IL-DDD is in the *power-off* state, there is no power supplied to the ***SF.DD*** thus, INFORMATION will not flow from the HIGH SIDE to the LOW SIDE.

When the IL-DDD enters the *power-on* state, the ***SF.DD*** ensures INFORMATION only flows from the LOW SIDE to the HIGH SIDE. This unidirectional data flow is achieved via a unidirectional Optical Fibre Repeater, which provides the security functionality of the ***SF.DD***. The unidirectional Optical Fibre Repeater utilises a unidirectional optical fibre receiver, buffer and unidirectional optical fibre transmitter, constructed from discrete commercial components. The unidirectional Optical Fibre Repeater is implemented in hardware within an isolated security domain. The receiver (input only from the LOW SIDE) and transmitter (output only to the HIGH SIDE) provide the only interfaces to the IL-DDD. There is only a single data path from input to output and no separate control functionality. This provides assurance that untrusted subjects cannot bypass or interfere with the operation of the ***SF.DD***.

FPT_SEP.3 Domain separation of the security functions have been implemented in the hardware of the dedicated security devices of the Interactive Link.

The implementation of the FPT_SEP.3 requirement ensures that there is a security domain available for the SFs to execute and that the SFs are protected from external tampering and interference. The ***SF.DD*** maintains distinct security domain for execution to protect against changes that might compromise the TOE's security objectives. This is accomplished via implementing the ***SF.DD*** solely in hardware. In so doing, the SF do not execute any software or firmware and therefore cannot be circumvented by any software threat. FPT_SEP.3 also requires that the TSF shall maintain the part of the TSF that enforces the information flow control SFP in a security domain, which is the case in the IL-DDD.

FDP_IFF.5 No illicit data flows exist to circumvent the *Unidirectional Flow SFP*.

FDP_IFF.5 requires that within the TOE there are no covert channels or unintended signalling channels from the HIGH SIDE to the LOW SIDE at any time. FDP_IFF.5 is realised through ***SF.DD,*** this SF provide the interface to the LOW SIDE.

The ***SF.DD*** has two external interfaces, one input port and one output port. The ***SF.DD*** provides a single unidirectional path for data to flow from the LOW SIDE to the HIGH SIDE. The design specifically prohibits data flow from the HIGH SIDE to the LOW SIDE, thus there is no illicit data flow from the HIGH SIDE to the LOW SIDE.

10. Conclusion

The IL-DDD security function and assurance measures are suitable to meet its security requirements. The analysis within this Security Target demonstrates how the combination of specified IT security functions work together as a whole to satisfy the security functional requirements, and thus are mutually supportive and provide an integrated and effective whole.

The functionality of the SF is very simple based on a state machine and have been implemented using discrete hardware components within the security functions. Thus the security function is neither probabilistic or based on permutations and therefore no strength of function can be claimed.

The assurance requirements are those of EAL 7 augmented with AVA_CCA.3 as defined within the CC part 3.