Doc. No. 9162P01000002
Issue No. 12.2

INTERACTIVE LINK

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 Pty Ltd
Second Avenue
Technology Park
MAWSON LAKES SA 5095

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 Common Criteria Security Target

Security Target Documentation Number: 9162P01000002

Security Target Version:	Issue 12.2, 12 August 2005
Assurance Level:	EAL 5, augmented with AVA_CCA.2.
TOE Title:	Interactive Link
TOE Part Number:	NIM001
TOE Version:	5.1

1.2 Security Target Overview

The Interactive Link allows real time interaction of a USER at a secure WINDOW SERVER with applications executing on a LOW SIDE NETWORK, without compromising the confidentiality of the data on the HIGH SIDE NETWORK. Currently, people who perform work on a secure HIGH SIDE NETWORK and require regular access to the LOW SIDE NETWORK are circumventing the problem by having two machines on one desk or by physically moving to an accessible machine connected to the LOW SIDE NETWORK.

The Interactive Link consists of an Interactive Link Data Diode Device (IL-DDD), an Interactive Link Keyboard Switch (IL-KBS) and software. This Security Target defines the IT security requirements of the Interactive Link and specifies the functional and assurance measures offered by the IL-KBS and IL-DDD which meet those security requirements.

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 augmented with the EXT_IND.1, Indication Function, EXT_RIP.1, HIGH SIDE Information Protection and EXT_KYB.1, Keyboard Data Transmission. It also conforms with the assurance requirements of the CC part 3 for the assurance level EAL 5, augmented with AVA_CCA.2 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 CC part 1, Annex C: Specification of Security Targets. 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 of this security target.

b. Section 2 - Acronyms and Definitions; this section lists the acronyms, definitions and references used throughout this 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 objectives 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. Section7 – TOE Summary Specifications; this section defines the IT security functions and assurance measures of the TOE.

h. Section 8 – PP Claims; this section defines any 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 and Definitions

2.1 Acronyms

AISEF – Australasian Information Security Evaluation Facility.

CC – Common Criteria for Information Technology Security Evaluation, version 2.1.

CM – Configuration management.

COTS – Commercial Off-The-Shelf.

DD – Data Diode.

DSF – Data Switch Function.

EAL – Evaluation Assurance Level.

ERTZ – Equipment Radiation TEMPEST Zone.

HILS – HIGH SIDE Interactive Link Server.

HOL – Higher Order Logic.

IL-DDD – Interactive Link Data Diode Device.

IL-KBS – Interactive Link Keyboard Switch

ISSO – Information System Security Officer.

ITSEC - Information Technology Security Evaluation Criteria.

KMF – Keyboard Mouse Function.

LILS – Low side Interactive Link Server.

LHF – Local Host Function.

PP – Protection Profile.

RHF – Remote Host Function.

SF – Security Function.

SFP – Security Function Policy.

SFR – Security Function Requirements.

TCP/IP – Transmission Control Protocol/Internet Protocol

Tenix – Tenix Defence Systems, Systems Division.

TOE – Target of Evaluation

TSC – TSF Scope of Control.

TSF – TOE Security Functions.

TSP – TOE Security Policy.

UDP – User Datagram Protocol.

UNB – Unidirectional Network Bridge.

2.2 Definitions

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

Common Peripherals refers to the keyboard and mouse that are connected to a computer, but normally mounted outside of the computer enclosure.

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

High Mode indicates that the PERIPHERAL DATA is directed to the users HIGH SIDE WINDOW SERVER.

High side is a descriptor used to refer to items associated with the HIGH SIDE NETWORK.

High side Network refers to the network including computer of which the USER'S local WINDOW SERVER is part. It has a security level greater that the LOW SIDE NETWORK.

Information the INFORMATION is an object, it is considered in two forms: LOW SIDE INFORMATION and HIGH SIDE INFORMATION.

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.

Interface Ports are associated with the IL-DDD, 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.

Keyboard Switch refers to a device that allows the keyboard and mouse to connect to the USER'S local WINDOW SERVER on the HIGH SIDE NETWORK or an APPLICATION SERVER on the ***LOW SIDE NETWORK***. The KEYBOARD SWITCH has two buttons and two illuminators referred to in this document as HIGH and LOW. By pressing either button the keyboard and mouse will be connected to the appropriate network.

Low Mode indicates that the PERIPHERAL DATA is directed to the LOW SIDE NETWORK.

Low side is a descriptor used to refer to items associated with the LOW SIDE NETWORK.

Low side Network refers to the network that has a security level lower than the HIGH SIDE NETWORK.

Mode is the state of the IL-KBS, which can be in either LOW MODE or HIGH MODE. In LOW MODE the PERIPHERAL DATA is directed to the LOW SIDE NETWORK. While in HIGH MODE, the PERIPHERAL DATA is directed to the USERS WINDOW SERVER.

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

Peripheral Data refers to Keyboard and Mouse output.

Peripheral Port Group refers to Keyboard and Mouse peripheral interface port and is used to define the Information Flow Functionality exercised by the IL-KBS. There are three distinct port groups: ***Common*** – Keyboard and Mouse data input to the IL-KBS and the KMF; ***Low Side*** – Keyboard and Mouse data output from the IL-KBS via the RHF to the LOW SIDE NETWORK; ***High Side*** – Keyboard and Mouse data output from the IL-KBS via the LHF to the HIGH SIDE NETWORK.

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

System Management Staff is responsible for the installation and maintenance of the Interactive Link devices and software.

TEMPEST refers to electromagnetic emanations that can be related to the INFORMATION being processed by an INFORMATION system.

Unidirectional Network Bridge refers to the software that supports data to flow from the LOW SIDE NETWORK to the HIGH SIDE NETWORK via the DATA DIODE DEVICE.

User refers to the person who utilises the Interactive Link in performance of duties.

Window Server refers to a system that communicates with a USER on behalf of a Window Management System. A WINDOW SERVER may be a terminal, such as an X-Terminal, or a Workstation running a WINDOW SERVER Program.

Z a formal specification language.

2.3 References

5018/T16/1, (2000) EFA T010 Interactive Link Sanitized Evaluation Technical Report, Admiral Management Services, Issue 1.0.

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

9162P01000001, (2005) Interactive Link Data Diode Device Common Criteria Security Target, Tenix Defence Systems – Systems Division, Issue 5.0

9162P01000005, (2001) Interactive Link Common Criteria Requirement Reference, Tenix Defence Systems – Systems Division, Issue 1.0

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.

ITSEC (1991) Information Technology Security Evaluation Criteria, Commission of the European Communities, Version 1.2.

PSSPP (2000) Peripheral Sharing Switch (PSS) for Human Interface Devices, Protection Profile, National Security Agency, Version 1.0.

3 TOE Description

The Interactive Link allows a user in a HIGH SIDE environment to access and interact with applications and INFORMATION on the LOW SIDE without compromising the confidentiality of the HIGH SIDE INFORMATION. The Target of Evaluation (TOE) of the Interactive Link solution consists of hardware and firmware components. These hardware and firmware components satisfy the security objectives of the TOE.

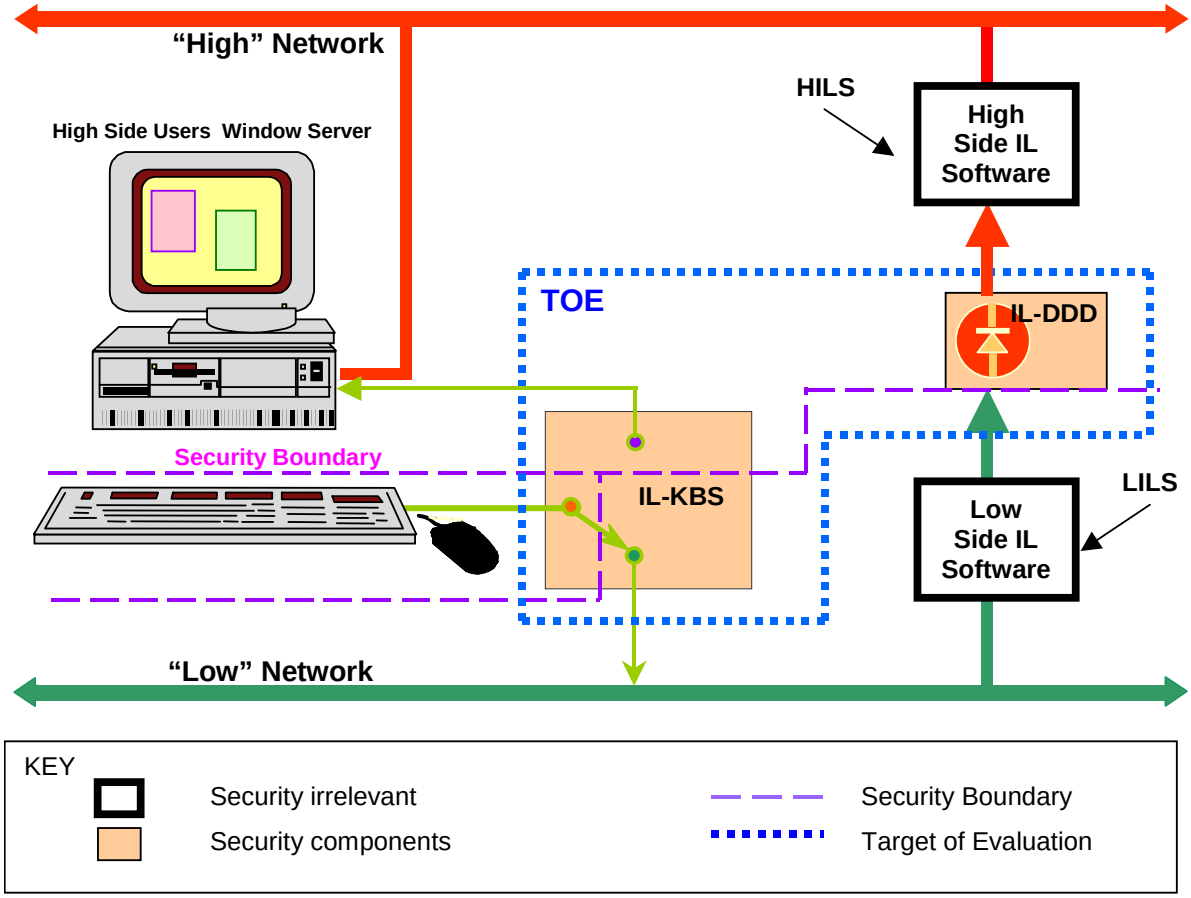

Figure 1 Interactive Link Architecture

3.1 Interactive Link Architecture

The TOE consists of the following components, as illustrated in Figure 1 Interactive Link Architecture:

IL-KBS

The Interactive Link Keyboard Switch (IL-KBS), device part number FID002 version 2.2 contains both firmware and hardware. The security functions have been implemented in firmware and hardware. Key features include:

- Keyboard buffers are protected from clandestine listeners on either side of the switch;

- Visual indication of the connected network.
- While in LOW MODE a session is conducted on a remote server on the LOW SIDE NETWORK.

The IL-KBS enables the USER to switch the keyboard and mouse (COMMON PERIPHERALS) to either the HIGH SIDE desktop or the LOW SIDE NETWORK. Keyboard and mouse data entered in the IL-KBS is processed by the Keyboard Mouse Function (KMF) before passing to the Data Switch Function (DSF). The DSF provides the switching functionality and passes the data onto either the Local Host Function (LHF), which interfaces to the USERS HIGH SIDE WINDOW SERVER, or the Remote Host Function (RHF) that interfaces to the LOW SIDE NETWORK.

IL-DDD

The Interactive Link Data Diode Device (IL-DDD), part number FID003 version 2.1 is implemented solely in hardware.

The IL-DDD is a trusted platform providing a unidirectional data path from the LOW SIDE NETWORK to the HIGH SIDE NETWORK. Key features include:

- Data transfer over the diode is sent without acknowledgment;
- Strategic redundancy and load management algorithms maximise reliability;
- Multiple workstations or PCs can share a single Data Diode.

The Interactive Link provides a one-way data flow from the LOW SIDE NETWORK to the HIGH SIDE NETWORK via the IL-DDD. The Interactive Link software provides the method for the keyboard and mouse data to interact with a LOW SIDE window session. The output is then packaged for transmission to the HIGH SIDE where it is forwarded to the USER'S HIGH SIDE WINDOW SERVER. The hardware provides the physical media for the Interactive Link operation and all the security functionality. USERS can interact with applications and INFORMATION on either the HIGH SIDE NETWORK or the LOW SIDE NETWORK by having the keyboard and mouse data switched to the appropriate output port of the IL-KBS.

Access to either the LOW or HIGH SIDE NETWORK is controlled by the USER pressing either the HIGH or LOW buttons on the front panel of the IL-KBS, thus changing the MODE of the IL-KBS. The USER can have multiple HIGH or LOW windows displayed on the HIGH SIDE WINDOW SERVER's screen, generated from applications running on both the HIGH and LOW SIDE NETWORKS.

The Interactive Link products are the only method of connecting the LOW or HIGH SIDE NETWORKS. This prevents a threat agent from circumventing the security provided by the IL-KBS or IL-DDD through an untrusted product or path.

When the USER selects the HIGH MODE, the keyboard and mouse are connected to the workstation or PC so that HIGH SIDE data is passed to the HIGH SIDE WINDOW SERVER allowing interaction with the HIGH SIDE. When the LOW MODE is selected, the keyboard and mouse are connected through the LOW SIDE NETWORK to an application server. The application output is passed to and displayed on the user's HIGH SIDE WINDOW SERVER via the IL-DDD. The IL-KBS provides visual indication as to which network is currently accessed.

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 Interactive Link servers, IL software and a keyboard and mouse. The software resident on the LILS gives the server the ability to interpret the keyboard and mouse information from the IL-KBS and conduct an interactive windows session on the LOW SIDE. The LOW SIDE software then pipes the display data to the HIGH SIDE via the IL-DDD. The software resident on the HIGH SIDE server then maps the session data to the appropriate USER'S HIGH SIDE WINDOW SERVER to be displayed. The following components are required for the IT environment and are necessary to deploy the complete Interactive Link architecture.

- The HIGH SIDE Interactive Link Server (HILS) consists of hardware, a commercial operating system and purpose built software, and contains no security functions.
- The LOW SIDE Interactive Link Server (LILS) consists of hardware, a commercial operating system and purpose built software which contains no security functions.
- The IL Software, is purpose built software it has different aspects resident on both the HILS and the LILS and contains no security functions.
- The HIGH SIDE USER'S WINDOW SERVER, consists of hardware, a commercial operating system and COTS software, and it contains no security functions.
- The Keyboard and Mouse utilises a standard 104-key keyboard, 3-button wheel mouse or a Sun™ standard keyboard and mouse combination.

The IL-DDD is installed between the HIGH and LOW SIDE NETWORKs and is located with the HILS, in the HIGH SIDE NETWORK space. The HILS receives LOW SIDE INFORMATION transferred across the IL-DDD from the LILS. The HILS distributes INFORMATION to the appropriate HIGH SIDE USER'S WINDOW SERVER. The LILS runs the LOW SIDE window session, though applications can be executed on any server on the LOW SIDE NETWORK. The LILS then packages up the display INFORMATION so that it can be transferred across the unidirectional IL-DDD.

The existing keyboard and mouse will be connected through the IL-KBS to the HIGH SIDE USER'S WINDOW SERVER. There will also be a connection between the IL-KBS and the LOW SIDE NETWORK. The connections with the IL-KBS are bi-directional to cater for the hand shaking required by the keyboard and mouse, the USER'S WINDOW SERVER and the LOW SIDE NETWORK protocol, TCP/IP.

3.2 Scope of Physical and Logical Boundaries

The physical boundary of the TOE consists of the IL-KBS and the IL-DDD as discussed above and as shown in Figure 1 Interactive Link Architecture. The physical boundary maintains nine operational interfaces, grouped in the following manner:

INTERFACE PORTS (IL-DDD)

- Output port to the HILS
- Input port from the LILS

PERIPHERAL PORT GROUPS (IL-KBS)

HIGH SIDE

- External Keyboard interface port to the USERS HIGH SIDE WINDOW SERVER
- External Mouse interface port to the USERS HIGH SIDE WINDOW SERVER

LOW SIDE

- External TCP/IP interface to the LOW SIDE NETWORK

COMMON

- Keyboard input port to the IL-KBS
- Mouse input port to the IL-KBS

USER INTERFACE (IL-KBS)

- Mode Select Interface
- Indication Interface

A group is a collection of PERIPHERAL PORTS treated as a single entity by the IL-KBS. There is one group for the set of COMMON PERIPHERALS and one group for each the LOW SIDE and HIGH SIDE NETWORKS. The HIGH SIDE GROUP is uniquely associated with the HIGH MODE and the LOW SIDE GROUP is uniquely associated with the LOW MODE. The PERIPHERAL PORT GROUP MODE is considered to be the same as that of the MODE currently selected by the TOE. PERIPHERAL DATA consists of keyboard and mouse data.

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

INFORMATION FLOW CONTROL

The functionality of the TOE allows LOW SIDE INFORMATION to flow to the 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.

MODE & INSTALLATION MANAGEMENT

The TOE provides supporting security features, which address mode and installation management. The indication functionality provides the user with an indication of the current mode of the TOE. Correct installation ensures that the appropriate static attributes are established during installation.

SF INVOCATION AND ISOLATION

The TOE provides supporting security features to 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, at least one security domain is available for the SFs own execution and that the SFs 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.

HIGH SIDE INFORMATION PROTECTION

The TOE provides a supporting security feature to ensure that keyboard and/or mouse data intended for the HIGH SIDE is not made available to the LOW SIDE.

3.3 TOE Security Policy

The TOE provides a Multiple Single Layer (MSL) solution with a single Non-Interference security functional policy (SFP). The TOE provides a unidirectional transmission of electronic signals (information) from a LOW SIDE network to a HIGH SIDE network. All security functions are provided by the IL-KBS and IL-DDD. The information flow control policy can be summarized as:

Non-Interference TOE Security Policy (TSP)

Non-interference can be stated informally a number of ways. For the Interactive Link application, it is suggested that the best statement of the theory is as follows. A system is said to be non-interfering if the (LOW) observed outputs of the system are completely determined by the LOW inputs. That is if we have two machines where the LOW inputs are the same, the observed outputs will be the same regardless of any HIGH inputs that may have occurred to one of the machines.

This is the common security policy for all functions of the TOE that cross the secure boundary between the HIGH and LOW SIDE, namely the IL-DDD and the IL-KBS.

3.4 Evaluated Configuration

The evaluated configuration of the Interactive Link consists of all components listed above in Section 3.1 Interactive Link Architecture and are configured and deployed in accordance with the parameters discussed in the guidance documentation. All components listed above are necessary to deploy a complete Interactive Link architecture. The components defined as elements of the IT environment are beyond the scope of this evaluation however, collectively serve to support the operational functionality of the Interactive Link.

The IL-KBS will be connected to a standard PC keyboard, 3-button wheel mouse or a Sun™ standard keyboard and mouse combination. The IL-KBS will be connected to a PC or Sun™ HIGH SIDE USER'S WINDOW SERVER, and to the LOW SIDE network.

The Interactive Link is scalable; the Interactive Link solution can consist of multiple IL-KBS, one for each USER. Multiple USERS can utilise one IL-DDD, and additional IL-DDDs could be introduced if the bandwidth needs to be increased. The need for deploying multiple IL-KBS and/or IL-DDD components should be considered on a case by case basis. The use of configuring multiple IL-KBS/IL-DDD components is dependent upon the number of USERS, their usage and bandwidth requirements.

4 TOE Security Environment

4.1 Assumptions

The Interactive Link provides a connection between two networks of different security levels; HIGH SIDE NETWORK and the LOW SIDE NETWORK. Note that all HIGH SIDE USERS must be cleared to use the LOW SIDE NETWORK. The assumptions made about the intended environment are:

A.PERSONNEL The Interactive Link 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 will be capable of storing and operating the devices of the Interactive Link TOE, comprising the IL-KBS and 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 of the Interactive Link 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. The IL-KBS has no long term data storage devices from which secure INFORMATION can be obtained, and is intended to be kept on the USER's desk top, within the same environment as the HIGH SIDE NETWORK.

A.EMISSION It is intended that the devices 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 Interactive Link Equipment Radiation TEMPEST Zone (ERTZ). The Interactive Link products operate at the edge of the secure boundary where the LOW SIDE NETWORK meets the HIGH SIDE NETWORK. Care should be taken to determine the relationship of the Interactive Link products ERTZ to their secure boundaries and to keep the ERTZ within them. This will ensure that any attempt to mount a TEMPEST attack would not compromise the security of the INFORMATION system.

A.INSTALLATION The SYSTEM MANAGEMENT STAFF will install the trusted devices of the Interactive Link correctly and in accordance with the Administration Documentation. The installation of the Interactive Link system is to be accredited by the appropriate SECURITY AUTHORITY.

A.PROCUREMENT Equipment hardware and software procurement policies are to be followed to minimise the risk of installing malicious hardware and software.

A.TRAINING All staff who have access to a secure 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.USER The USER while in HIGH MODE will stop typing HIGH SIDE data before selecting the button on the front of the IL-KBS to change it to LOW MODE. The user shall not type HIGH SIDE data until the IL-KBS has been changed back to HIGH MODE. Thus USER will not place HIGH SIDE data directly onto the LOW SIDE NETWORK.

A.NETWORK Interactive Link products are the only method of interconnecting the LOW and HIGH SIDE NETWORKs. This prevents a threat agent from circumventing the security being provided by the Interactive Link through an untrusted product/path.

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

4.2 Threats

The assumed threats discussed below are mitigated by the Interactive Link. The Interactive Link Risk and Threat Assessment, has assessed threats to the HIGH SIDE INFORMATION, new threats that have been introduced with the Interactive Link 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.TRANSMIT A USER or process on the HIGH SIDE NETWORK that accidentally or deliberately breaches the confidentiality of some HIGH SIDE INFORMATION by transmitting data from a HIGH SIDE WINDOW SERVER through the IL-KBS to the LOW SIDE NETWORK.

T.ACCIDENTAL_ENTRY A USER accidentally types HIGH SIDE data into the keyboard while the IL-KBS is in the LOW MODE and therefore puts the HIGH SIDE data directly onto the LOW SIDE NETWORK.

T.KEYBOARD A rogue keyboard or mouse copies data intended for HIGH SIDE NETWORK, as it is entered, and re-transmits the data to the LOW SIDE NETWORK when the IL-KBS is in the LOW MODE.

T.TAMPER An adversary tampers with the contents of the IL-KBS or IL-DDD during delivery, and/or after installation, albeit prior to operation that may compromise the TOE objectives.

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

T.FAILURE The Interactive Link products (IL-KBS or IL-DDD) have 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.HIGH_DATA HIGH SIDE DATA entered by the user onto the HIGH SIDE through the keyboard and/or mouse may be stored in the KMF data buffer/s, prior to the user initiating

a mode change from HIGH to LOW, and later transferred to the LOW SIDE NETWORK.

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 Interactive Link is intended to protect the asset, of HIGH SIDE INFORMATION, in accordance with the following security objectives:

O.CONFIDENTIALITY The TSF will prevent information flow from the HIGH SIDE NETWORK to the LOW SIDE NETWORK, thus preserving the confidentiality of all HIGH SIDE data stored on the HIGH SIDE NETWORK.

O.INDICATE The USER shall receive an unambiguous indication of the current MODE, and hence the destination of keyboard and mouse data.

O.INVOKE The SFs are always invoked to protect the INFORMATION on the HIGH SIDE, independent of the state of the IL-KBS.

O.ROM TSF shall be protected against unauthorised modification.

O.SELECT An explicit action by the USER shall be used to select the MODE of the IL-KBS and the network to which the COMMON PERIPHERALS are connected.

O.CONNECT The Keyboard and Mouse shall be connected to at most one network at a time.

O.FLUSH The SF ensures that all HIGH SIDE keyboard and/or mouse data will be flushed from the KMF data buffers upon a HIGH to LOW mode change.

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

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

5.2 Security Objectives for the Environment

All of the secure usage assumptions are addressed by the security objectives of the environment. These objectives are satisfied though the application of procedural or administrative measures.

OE.PERSONNEL The Interactive Link products 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 Interactive Link products in accordance with the requirements of the HIGH SIDE system.

OE.EMISSION The Interactive Link products shall operate in an environment where the ERTZ of the products is within the secure boundary of the HIGH SIDE environment.

OE.INSTALLATION The Interactive Link will be installed by SYSTEM MANAGEMENT STAFF in accordance with the Guidance Documentation. An appropriate SECURITY AUTHORITY shall accredit the installation of the Interactive Link system.

OE.KEYBOARD The keyboard and mouse devices used will be conformant with the guidance documentation provided with the Interactive Link. The keyboard and mouse devices will transmit data to the IL-KBS within 249mS after a user enters a keystroke or moves the mouse and will not retransmit the data after this time.

OE.PROCUREMENT Equipment hardware and software procurement policies are to be followed to minimise the risk of installing malicious hardware and software.

OE.TRAINING All staff who have access to classified information systems and utilise the Interactive Link 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 Interactive Link products are the only method of interconnecting the LOW and HIGH SIDE NETWORKS.

6 Security Functional Requirements

The Interactive Link functionality, specified by the *Non-interference TSP* 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
FMT_MSA.3	Static Attribute Initialisation	FMT_MSA.1†, FMT_SMR.1†
FMT_SMF.1	Specification of Management Functions	No Dependencies
FPT_FLS.1	Failure with Preservation of Secure State	ADV_SPM.1
FPT_RVM.1	Non-bypassability of the TSP	No Dependencies
FPT_SEP.3	Complete Reference Monitor	No Dependencies
EXT_IND.1	Indication Function	No Dependencies
EXT_RIP.1	High Side Information Protection	No Dependencies
EXT_KYB.1	Keyboard Data Transmission	No Dependencies

† *Thesedependencies not met by the TOE, refer to section 9.3.3.1.*

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

Table 1 - Security Functional Requirements

The functional requirements that appear in Table 1 - Security Functional Requirements 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. Due to the Interactive Link TOE consisting of two devices that isolate the HIGH SIDE from the LOW SIDE there has been a need to iterate some components of the Security Functional Requirements (SFR) in accordance with CCIMB Interpretation 019. When a functional requirement is iterated, iteration (**A**) applies to the IL-DDD and iteration (**B**) applies to the IL-KBS.

6.1 TOE Security Functional Requirements

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 Interactive Link.

FDP_IFC Information Flow Control Policy

This family utilises the information flow control SFP *of Non-interference SFP*. The TOE trusted elements, the IL-KBS and IL-DDD, represent two points where information is transferred to the HIGH SIDE NETWORK. As a consequence there are two instances of the FDP_IFC and FDP_IFF SFRs delineated by the suffix (A) and (B) representing the IL-DDD and IL-KBS respectively.

FDP_IFC.2.(A) Complete Information Flow Control

Dependencies: FDP_IFF.1

FDP_IFC.2.1.(A) The TSF shall enforce the [assignment: *Data Diode Non-Interference 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.(A) 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_IFC.2. (B) Complete Information Flow Control

Dependencies: FDP_IFF.1

FDP_IFC.2.1.(B) The TSF shall enforce the [assignment: *Keyboard Switch Non-Interference SFP*] on [assignment: *PERIPHERAL PORT GROUPS (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.(B) 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 can implement the *Non-interference SFP*.

FDP_IFF.1.(A)-NIAP-0407 Simple Security Attributes

Dependencies: FDP_IFC.1, FMT_MSA.3‡

FDP_IFF.1.1.(A). The TSF shall enforce the [assignment: *Data Diode Non-Interference 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.(A) 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.(A)-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.(A)-NIAP-0407 The TSF shall provide following:

[selection: no additional SFP capabilities].

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

[selection: no explicit authorisation rules].

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

[selection: no explicit denial rules]

FDP_IFF.1.(B)-NIAP-0407 Simple Security Attributes

Dependencies: FDP_IFC.1, FMT_MSA.3

FDP_IFF.1.1.(B) The TSF shall enforce the [assignment: *Keyboard Switch Non-Interference SFP*] based on the following types of subject and information security attributes:

[assignment:

a. The PERIPHERAL PORT GROUP attributes: COMMON, LOW SIDE, HIGH SIDE

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

FDP_IFF.1.2.(B) 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 MODE DATA shall be allowed to flow to the LOW SIDE PERIPHERAL PORT GROUP

b. All HIGH MODE DATA shall be allowed to flow to the HIGH SIDE PERIPHERAL PORT GROUP].

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

[selection: [assignment:

a. No information shall flow from the low side peripheral port group to the high side peripheral port group

b. No information shall flow from the low side peripheral port group to the common peripheral port group

c. No information shall flow from the high side peripheral port group to the common peripheral port group

d. *No information shall flow from the high side peripheral port group to the low side peripheral port group*]].

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

[selection: no additional SFP capabilities].

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

[selection: no explicit authorisation rules].

FDP_IFF.1.6.(B)-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 the [assignment: *Keyboard Switch Non-Interference SFP and Data Diode Non-Interference SFP*].

6.1.2 Security Management (FMT)

This class specifies the management of the SFs and their security attributes.

FMT_MSA Management of Security Attributes

This family describes the security attributes of the SFs and how they are initialised.

FMT_MSA.3 Static Attributes Initialisation

Dependencies: FMT_MSA1†, FMT_SMR.1†

FMT_MSA.3.1 The TSF shall enforce the [assignment: *Keyboard Switch Non-Interference SFP*] to provide [selection: *restrictive*] default values for security attributes that are used to enforce the SFP.

Functionality comment: On start-up the IL-KBS MODE is HIGH MODE and the keyboard and mouse are connected to the HIGH SIDE COMPUTER.

FMT_MSA.3..2 The TSF shall allow [assignment: *no authorised identified roles*] to specify alternative initial values to override the default values when an object or information is created.

FMT_SMF.1 Specification of Management Functions

Dependencies: No Dependencies

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions:

[assignment:

A USER shall perform an explicit action to change the MODE of the IL-KBS and select either the HIGH SIDE or LOW SIDE PERIPHERAL PORT GROUP as the destination of the USER DATA presented to the COMMON PERIPHERAL PORT GROUP.]

6.1.3 Protection of the TSF (FPT)

The Interactive Link functionality requirements of this class relate to the management and integrity of the mechanisms of the SFs 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.

6.1.4 Extended Requirements (EXT)

These requirement specifies required functionality, which has not been defined within CC Part 2.

EXT_IND.1 Indication Function

Dependencies: none

EXT_IND.1.1 A visual indicator shall indicate the current MODE (either HIGH or LOW) of IL-KBS.

Functionality comment: The visual indicator indicates which network the keyboard and mouse are connected to.

EXT.IND.1.2 The audible indicator shall provide audible feedback when the MODE is changed.

EXT_RIP.1 High Side Information Protection

Dependencies: none

EXT_RIP.1.1 The TSF shall ensure that information intended for the HIGH SIDE is not made available to the LOW SIDE when the user changes mode.

6.2 TOE Security Assurance Requirements

Assurance requirement components are those of Evaluation Assurance Level 5 (EAL5 – semiformally designed and tested), augmented with the vulnerability assessment class AVA_CCA.2 Systematic Covert Channel Analysis. Refer to CC part 3 for the detail associated with each of the assurance requirements.

6.3 Security Functional Requirements for the IT Environment

The keyboard and mouse are third party Commercial Off The Self (COTS) devices that share both the high and low side data that is presented to the input of the IL-KBS. The TOE is dependent upon the keyboard and mouse to function as defined in the extended Security Functional Requirement EXT_KYB.1. The keyboard and mouse are not part of the TOE and EXT_KYB.1 is an SFR for the IT Environment.

6.3.1 Extended Requirements (EXT)

This requirement specifies required functionality, which has not been defined within CC Part 2 to be levied on the IT Environment.

EXT_KYB.1 Keyboard Data Transmission

Dependencies: none

EXT_KYB.1.1 HIGH SIDE information entered into the keyboard and mouse is transmitted to the IL-KBS within 249mS and will not retransmit the data after this time.

7 TOE Summary Specification

The goal of the Interactive Link is to provide interactive access to the INFORMATION on the LOW SIDE NETWORK 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 Interactive Link in Section 6. 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 Interactive Link provides the following security functions (SF). The functions are resident within the IL-DDD and IL-KBS.

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 Data Diode Non-interference 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.

SF.DP_SW **Data Path Switch Function:** The ***SF.DP_SW*** controls and performs the transfer of data from the keyboard and mouse to either the USER'S HIGH SIDE WINDOW SERVER via the LHF, a non TSF component, or the LOW SIDE NETWORK via the RHF, a non TSF component, according to the MODE selected by the USER.

The ***SF.DP_SW*** provides the switching of the keyboard and mouse data received by the ***SF.KMF*** (discussed below) to either the LHF and onto USER'S HIGH SIDE WINDOW SERVER or the RHF and onto the LOW SIDE NETWORK. The ***SF.DP_SW*** implements diode functionality and provides a unidirectional path for keyboard and mouse data (PERIPHERAL DATA) from the ***SF.KMF*** to either the LHF and onto USER'S HIGH SIDE WINDOW SERVER or the RHF and onto the LOW SIDE NETWORK. This functionality prevents HIGH SIDE data from being transmitted to to the keyboard and mouse and onto the LOW SIDE NETWORK through the IL-KBS.

There is no direct peripheral data path within the ***SF.DP_SW*** from the HIGH to the LOW SIDE NETWORK, this prevents HIGH SIDE data from flowing to the LOW SIDE NETWORK.

There are two possible MODES that the ***SF.DP_SW*** can be in, HIGH or LOW. The HIGH MODE represents a connection of the PERIPHERAL DATA via the ***SF.DP_SW*** to the LHF and the USER'S HIGH SIDE WINDOW SERVER, connected to the HIGH SIDE NETWORK. When in the LOW MODE the PERIPHERAL DATA is passed via ***SF.DP_SW*** to the RHF that assembled data into TCP/IP packets for transmission to a server on the LOW SIDE NETWORK.

The ***SF.DP_SW*** receives data from the ***SF.KMF*** via a uni-directional parallel interface. The ***SF.DP_SW*** passes the PERIPHERAL DATA to either the LHF (HIGH SIDE) or the RHF (LOW SIDE). The mode of the ***SF.DP_SW*** is controlled by the user and is selected by pressing either of the HIGH or LOW buttons on the front of the IL-KBS. The ***SF.IND*** (discussed below) ensures that a single audible tone is generated when the user changes mode and that the classification label associated with the destination network of the PERIPHERAL DATA is illuminated. i.e. when in HIGH MODE the label representing the classification of the HIGH SIDE NETWORK is illuminated.

The ***SF.DP_SW*** assumes a default mode of HIGH when power is applied and the IL-KBS is first initialised. The ***SF.DP_SW*** provides the switching mechanism that enables the USER to select the MODE and thus the HIGH or LOW SIDE NETWORKS that they intend to interact with. The ***SF.DP_SW*** senses the state of two buttons (part of the ***SF.DP_SW***) on the IL-KBS front panel, by which the USER selects the MODE. When the user pushes a button, a change request is received and the ***SF.DP_SW*** controls the switching of the IL-KBS MODE. If the request is from LOW to HIGH the change occurs with ***SF.IND*** providing an audible indication of the successful mode change and visual indication of the new mode HIGH. If the request is from HIGH to LOW the ***SF.DP_SW*** enters a flush state for 250mS in conjunction with the audible indication. During the flush state any residual HIGH SIDE data in transit from the keyboard and mouse to the ***SF.DP_SW*** via the ***SF.KMF*** is overwritten while the ***SF.DP_SW*** is in a neutral position preventing data from passing to neither the HIGH or the LOW SIDE. After the flush state the ***SF.IND*** audible indication stops, the visual indication signify the new mode LOW of the IL-KBS. To switch back to the high

mode, the user must select the HIGH button. The IL-KBS will then returned to HIGH MODE and the COMMON PERIPHERALS are connected to the HIGH SIDE NETWORK. This explicit action by the user ensures the MODE of the IL-KBS cannot change without the USERS knowledge.

The IL-KBS DSF, which implements the ***SF.DP_SW***, has been designed, developed and implemented so that if a component fails it will not violate the Keyboard Switch Non-interference SFP. This has been achieved in hardware; 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.DP_SW*** utilises redundant components providing the same security functionality. The redundant components for the switching functionality have been placed in series within the SF. The redundant components were selected from different manufactures with slightly different functionality so that common flaws within the components will not result in all components failing at the same time.

SF.KMF **Keyboard Mouse Function:** The ***SF.KMF*** passes the peripheral data inputted by the keyboard and mouse into the ***SF.DP_SW.*** The data may be either HIGH or LOW side data. The ***SF.KMF*** is designed to utilise minimal memory and in conjunction with the flush functionality does not store HIGH SIDE data and pass it onto the LOW SIDE NETWORK following a MODE change.

SF.KMF following the mode change from HIGH to LOW enters the flush state where the data in transit through the KMF is overwritten and not passed to either the user's high window server nor low sides network.

Keyboard and mouse information generated by the User is received by ***SF.KMF*** and passed to the ***SF.DP_SW***. The ***SF.KMF*** emulates a connection to the computer. The ***SF.KMF*** receives keyboard and mouse data in either of two formats, serial Sun and PC. The data received from user input is translated to an internal parallel format and transmitted to the ***SF.DP_SW*** in a uni-directional manner. The ***SF.KMF*** is the only channel to provide keyboard and mouse data to the ***SF.DP_SW***. The ***SF.KMF*** does not receive any control or status information from the ***SF.DP_SW***. No information is received from the ***SF.DP_SW***, making the ***SF.KMF*** unable to determine the mode of the switch and ultimately has no knowledge of the destination of the keyboard and mouse data internal to the IL-KBS. The ***SF.KMF*** is designed to utilise minimal memory that could store HIGH SIDE data and ultimately pass it onto the LOW SIDE NETWORK. The flush functionality in conjunction with minimal memory prevents the storage of HIGH SIDE data and following a MODE change it being passed onto the LOW SIDE NETWORK.

SF.IND **Indication Function:** The ***SF.IND*** indicates the current mode to the USER. This function ensures that the USER is aware of the current MODE and thus the destination of the PERIPERAL DATA. This function also indicates that a change of MODE has occurred successfully. The indication will be unambiguous to the USER.

SF.DP_SW provides the functionality that selects the MODE of the IL-KBS. The MODE, of which there are two, HIGH and LOW, is selected by one of the push buttons on the front panel. ***SF.DP_SW*** controls the ***SF.IND*** by the use of the current MODE. ***SF.IND*** provides two visual indicators (one for high mode and one for low mode) and a reinforcing audible tone generator.

The User is able to control whether keyboard and mouse data is sent to the HIGH SIDE or to the LOW SIDE by pressing one of the two push button switches. The LOW SIDE visual indicator is lit when the IL-KBS is in LOW MODE and the HIGH SIDE visual indicator is lit when the IL-KBS is in HIGH MODE. A reinforcing audible tone is generated when changing from LOW MODE to HIGH MODE or from HIGH MODE to LOW MODE. This also alerts the User in the case of accidental button presses, prompting the User to check the visual MODE indicators.

It is important that the User be aware of the current mode of the IL-KBS (HIGH or LOW) at all times. This is achieved by locating the IL-KBS within the User's field of view so that the visual indication of MODE is always visible.

Visual MODE indication is colour coded to the security classification of the HIGH and LOW SIDE NETWORKS. The Visual MODE indication is located near the top of the front panel to ensure that it is within the user's field of view. This makes it easy to tell at a glance the MODE of the Keyboard Switch but forces the illumination backlighting colour to be white so that the security classification labels can be changed easily. The reinforcing audible tone is a supporting function that indicates the change of MODE. It does not have redundancy built-in as it supports the visual indication during a MODE change.

Regardless of whether the visual indication fails or the audible tone fails, the TOE will maintain its secure state and the confidentiality of the HIGH SIDE NETWORK. The user must be alert to the current MODE of the IL-KBS at all times during operation. Should either of these components fail, the user must follow the guidance provided in the troubleshooting section of the IL-KBS guidance documentation.

The ***SF.IND*** has been designed, developed and implemented in hardware; with a goal of ensuring that a single failure will not result in HIGH SIDE data being made available to the LOW SIDE. The ***SF.IND*** utilises redundant components providing the same security functionality. The components of the ***SF.IND*** have been placed in parallel. These parallel components include four light sources affixed behind the front panel of the IL-KBS chassis; two LEDs situated behind the LOW SIDE visual indicator and two LEDs situated behind the HIGH SIDE visual indicator. Should one LED fail, the second light source will maintain visual indication.

7.2 Assurance Measures

This section describes the assurance measure of the TOE which meet the security assurance requirements specified for the Interactive Link in Section 6.2. Further detail of the correlation between the assurance measures and assurance requirements can be seen in section 9.3.2 of this Security Target.

7.2.1 Configuration Management

1. Rational 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. Configuration.
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 Interactive Link is delivered to the end customer by a process that ensures non-repudiation.
2. An approved courier distributes the product from the secure manufacturing facility and the end customers must acknowledge receipt.
3. Upon arrival, the tamper evident seals are inspected to ensure that the delivery process in conjunction with O. TAMPER_SEAL have prevented modification of the trusted devices. The user then installs and starts-up the TOE in accordance with the Administration Manual.
4. The system within which the TOE has been installed needs to be re-accredited by its SECURITY AUTHORITY before it can be reused.

7.2.3 Development

1. The Interactive Link has a functional specification.
2. There is a formal model of the TSP
3. The Interactive Link functionality that implements the SFs and TSFI 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 Interactive Link, 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 SFs to a level that is unambiguous and thus requires no further design decisions.
8. The implementation documentation defines the correspondence between the formal specifications of the SFs and how they have been implemented.

7.2.4 Guidance Documents

1. There is a User and Administration Manual for the Interactive Link.
2. The Administration Manual defines the process for installing the Interactive Link for secure operation.
3. The User Manual describes the assumptions regarding the secure operation of the TOE.

7.2.5 Life Cycle Support

1. 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.
2. The Australian Department of Defence has accredited the development environment.
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 Interactive Link is maintained.
6. Documented procedures define the implementation of the tools used to develop the Interactive Link.

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 Interactive Link was independently tested by an Australasian Information Security Evaluation Facility (AISEF).

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 and firmware with multiple levels of redundancy that cannot be circumvented.
4. There are no permutational or probabilistic SFR and thus there is no strength of functionality claims.
5. An assessment of the operational vulnerabilities has been carried out and documented.
6. An assessment of the construction 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 2 - 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 3 - Threats/Objectives Rationale, demonstrates how the objectives of the TOE and the TOE environment counter the threats identified in Section 4.2.

Table 4 - 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.TRANSMIT	T.ACCIDENTAL_ ENTRY	T.KEYBOARD	T.TAMPER	T.LOGIC	T.FAILURE	T.HIGH_DATA	A.PERSONNEL	A.PHYSICAL	A.EMISSION	A.INSTALLATION	A.PROCUREMENT	A.USER	A.NO_EVIL	A.TRAINING	A.NETWORK
O.CONFIDENTIALITY	✓	✓															
O.INDICATE			✓														
O.INVOKE	✓	✓															
O.ROM					✓	✓											
O.SELECT			✓														
O.CONNECT		✓															
O.FLUSH				✓				✓									
O.FAILSECURE							✓										
O.TAMPER_SEALS					✓												
OE.PERSONNEL					✓				✓			✓		✓	✓		
OE.PHYSICAL	✓				✓					✓	✓						
OE.EMISSION											✓						
OE.INSTALLATION												✓					✓
OE.KEYBOARD				✓									✓				
OE.PROCUREMENT				✓									✓				
OE.TRAINING			✓	✓					✓			✓		✓		✓	
OE.NETWORK																	✓
OE.NO_EVIL			✓	✓					✓			✓	✓	✓	✓		✓

Table 2 - 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.1.(A), FDP_IFF.1.(A), 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.TRANSMIT	O.CONFIDENTIALITY O.INVOKE O.CONNECT	The threat of transmitting data from the HIGH SIDE WINDOW SERVER through the IL-KBS to the LOW SIDE NETWORK is partially mitigated by O.CONFIDENTIALITY (FDP_IFC.1.(B), FDP_IFF.1.(B), FDP_IFF.5). O.CONFIDENTIALITY achieves this by explicitly prohibiting any flows from the HIGH SIDE NETWORK through the IL-KBS to the LOW SIDE, including flows that might take place through the use of covert channels. Thus both explicit and implicit flows are covered. ***** O.INVOKE ensures that all SFs are invoked at all time to protect the HIGH SIDE data. At no time, even when power is removed, can the IL-KBS SFs be bypassed to transfer data from the HIGH SIDE to the LOW SIDE. O.INVOKE thereby partially mitigates threat T.TRANSFER. ***** O.CONNECT mitigates the T.TRANSMIT threat by ensuring the keyboard and mouse (COMMON PERIPHERAL PORT GROUP) are connected to one of the networks at any one time. This objective prevents the situation where the

Threats	Objectives	Rationale
		mouse is connected to one network and the keyboard is connected to the other providing a potential of INFORMATION transfer between the HIGH SIDE NETWORK and the LOW SIDE NETWORK via the IL-KBS. O.CONNECT also prevents the situation where the keyboard and mouse are connected to both the high and low side concurrently, thus preventing a potential flow to occur from high to low. ***** O.CONFIDENTIALITY, O.INVOKE and O.CONNECT collectively serve to counter the threat of T.TRANSMIT.
T.ACCIDENTAL_ ENTRY	O.INDICATE O.SELECT OE.TRAINING OE.NO_EVIL	The threat that a USER accidentally types HIGH SIDE data into the keyboard while the IL-KBS is in the LOW MODE and therefore puts the HIGH SIDE data directly onto the LOW SIDE NETWORK is partially mitigated by O.INDICATE. O.INDICATE achieves this by providing the user with an unambiguous visual indication of the current MODE of the IL-KBS and in turn the destination of the keyboard and mouse data. O.INDICATE also provides an audible tone to indicate a successful MODE change. O.INDICATE reduces the threat T.ACCIDENTAL_ENTRY, as a user is less likely to accidentally enter HIGH SIDE data into the keyboard while the IL-KBS is in the low mode and consequently placing HIGH SIDE information directly onto the LOW SIDE network. ***** O.SELECT ensures that only an explicit action by the USER can change the MODE of the IL-KBS and thus select the network that the COMMON PERIPHERALS are connected to. This explicit action in conjunction with O.INDICATE ensures that the USER is aware of the current MODE of the IL-KBS. ***** OE.TRAINING ensures that all users are trained to know what security is provided by the Interactive Link, and how to operate it securely and correctly to prevent incorrect and/or accidental misuse of the IL-KBS in a way that may result in imposing the threat of T.ACCIDENTAL_ENTRY. A trained user will know: 1. the mode of the IL-KBS when it is initially powered up 2. how to change mode 3. how to determine the current mode of the IL-KBS. This knowledge provided by OE.TRAINING minimises a threat scenario where a user accidentally types high

Threats	Objectives	Rationale
		side data while in low mode. ***** OE.NO_EVIL ensures that authorised users of the TOE are non-hostile and will follow all usage guidance to ensure that the Interactive Link is operated in a secure manner. This objective ensures that users are trusted and will not pass HIGH SIDE INFORMATION to the LOW SIDE NETWORK. ***** Conscious enforcement of the objectives O.INDICATE, O.SELECT and OE.TRAINING, on behalf of the user, reduces the threat that HIGH SIDE data is accidentally entered into the keyboard while the IL-KBS is in the low mode. While OE.NO_EVIL ensures that the threat isn't instigated by a user with hostile intent.
T.KEYBOARD	OE.KEYBOARD O.FLUSH OE.PROCUREMENT OE.NO_EVIL OE.TRAINING	The threat that a rogue keyboard or mouse copies data intended for HIGH SIDE NETWORK, as it is entered, and re-transmits the data to the LOW SIDE NETWORK when the IL-KBS is in the LOW MODE is mitigated by keyboard requirements, procurement policies and USERS. ***** OE.KEYBOARD defines the performance requirements of the keyboard and mouse devices used to mitigate the threat. OE.KEYBOARD requires that all data entered into the keyboard and mouse has been transferred to the IL-KBS within 249mS. This ensure any residual HIGH SIDE data that has been entered into the keyboard and mouse has been passed to the IL-KBS before the MODE changes from HIGH to LOW MODE at the end of the 250mS O.FLUSH period. ***** O.FLUSH ensures that after a HIGH to LOW MODE change has occurred and during the flush period, all HIGH SIDE keyboard and mouse data passed into the IL_KBS is overwritten and not passed to either the user's high window server nor low sides network ***** OE.PROCUREMENT, further mitigates this threat for example by having a nondeterministic procurement policy which does not provide supplies with any knowledge associated with the end use of the products in this case the keyboard and mouse for the Interactive Link. This minimizes the possibility of installing a rogue keyboard and/or mouse in the intended operational environment. *****

Threats	Objectives	Rationale
		OE.TRAINING requires the USER while in HIGH MODE to stop typing HIGH SIDE data before selecting the button on the front of the IL-KBS to change it to LOW MODE. The user shall not type HIGH SIDE data until the IL-KBS has been changed back to HIGH MODE. Thus USER will not place HIGH SIDE data directly onto the LOW SIDE NETWORK. ***** T.KEYBOARD is partially mitigated by OE.NO_EVIL, which ensures that authorised users of the TOE are non-hostile and will follow all usage guidance to ensure that a USER will not introduce rogue devices into the operational environment of the Interactive Link. ***** OE.KEYBOARD, OE.PROCUREMENT and OE.NO_EVIL collectively serve as suitable countermeasures to mitigate the risk that an unauthorised user would introduce a rogue keyboard or mouse, that could copy data intended for the HIGH SIDE NETWORK and re-transmit the data to the LOW SIDE NETWORK when the IL-KBS is in the LOW MODE. OE.TRAINING ensures that users are aware of the requirement that they are to stop typing HIGH SIDE DATA before changing the MODE to LOW and not to type HIGH SIDE DATA until in HIGH MODE again. OE.TRAINING in conjunction with O.FLUSH, that overwrites any HIGH SIDE DATA in transit, provide the mitigation strategy to counter this threat.
T.TAMPER	O.ROM O.TAMPER_SEALS OE.PHYSICAL OE.PERSONNEL	The threat T.TAMPER is associated with an adversary tampering with the contents of the IL-KBS or IL-DDD to compromise the Interactive Link security functionality prior to operation. This threat is reduced by the objectives O.ROM and O.TAMPER_SEAL and supported by OE.PERSONNEL and OE.PHYSICAL. O.ROM reduces the risk because the TSF is protected against unauthorised modification. O.ROM partially mitigates the threat of T.TAMPER by preventing the functionality of the IL-KBS or the IL-DDD from being changed after the manufacturing process. ***** 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 either the IL-DDD or IL-KBS to cause the compromise of the confidentiality of some HIGH SIDE INFORMATION. This seal is monitored by the USER (IL-KBS) or the SYSTEM MANAGEMENT STAFF (IL-DDD). Any attempt to access the contents of either the devices

Threats	Objectives	Rationale
		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 Interactive Link devices at any time. 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-KBS or 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.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 and firmware. O.ROM prevents changes to the firmware or programmable logic. The threat T.LOGIC is mitigated by O.ROM.
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 Interactive Link has been designed with multiple levels of redundancy both in the hardware components of the IL-KBS and 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-KBS is 80,389 hours (9.18 years). The Mean Time

Threats	Objectives	Rationale
		Between Failures (MTBF) for the IL-DDD is 308, 790 hours (35.25 years).
T.HIGH_DATA	O.FLUSH	The threat that HIGH SIDE DATA may be stored in the KMF data buffer/s, prior to the user initiating a mode change from HIGH to LOW, and is then later transferred to the LOW SIDE network is mitigated by the O.FLUSH objective. When the user requests a mode change from HIGH to LOW, the IL-KBS enters a flush state, which allows any HIGH SIDE data in transit through the KMF to be overwritten in its data buffers. The O.FLUSH objective of the IL-KBS ensures that the SF will flush all keyboard and/or mouse data from the KMF data buffers, thus mitigating the T.HIGH_DATA threat.

Table 3 - Threats/Objectives Rationale

Assumptions	Objectives	Rationale
A.PERSONNEL	OE.PERSONNEL OE.NO_EVIL OE.TRAINING	A. PERSONNEL assumes that the Interactive Link 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 USERS and those personnel responsible for the installation of the Interactive Link, are vetted and cleared to the security level of the HIGH SIDE. ***** OE.NO_EVIL reduces the risk that users of the TOE are non-hostile and follow all usage guidance to ensure that the Interactive Link 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 Interactive Link 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 devices of the Interactive Link TOE before, during or after installation. They also further mitigate the risk of the deliberate introduction of a rogue peripheral device

Assumptions	Objectives	Rationale
		by an unauthorised user.
A.PHYSICAL	OE.PHYSICAL	A.PHYSICAL assumes that the intended environment will be capable of storing and operating the devices of the Interactive Link TOE, comprising the IL-KBS and 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 of the Interactive Link 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. The IL-KBS has no long term data storage devices from which secure INFORMATION can be obtained, and is intended to be kept on the USER's desk top, within the same environment as the HIGH SIDE NETWORK. OE.PHYSICAL ensures that the devices of the Interactive Link TOE 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 Interactive Link devices at any time, and requires the installation of the Interactive Link 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 Interactive Link TOE will operate in an environment where physical (or some other) security measures prevent any TEMPEST attack. OE.PHYSICAL ensures that the TSC devices of the Interactive Link are operated and stored within a physically secure environment that, at minimum, meets the requirements for the HIGH SIDE. ***** OE.EMISSION ensures that IL-DDD and IL-KBS are 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 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 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 prevents the incorrect installation of the HIGH and LOW SIDE INTERFACE PORTS and the HIGH and LOW SIDE PERIPHERAL PORTS, thus protecting the confidentiality of the HIGH SIDE

Assumptions	Objectives	Rationale
		INFORMATION. ***** OE.PERSONNEL ensures that all personnel, including USERS and those personnel responsible for the installation of the Interactive Link, 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 Interactive Link 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 devices of the Interactive Link will be installed correctly and in accordance with the guidance documentation.
A.PROCUREMENT	OE.PROCUREMENT OE.KEYBOARD OE.NO_EVIL	OE.PROCUREMENT ensures that procurement policies, and operational practices and procedures, are followed. This mitigates the risk of introducing/installing malicious hardware and/or software, which may compromise the Interactive Link. ***** OE.KEYBOARD ensures the third party keyboard and mouse devices procured will be conformant with the guidance documentation provided with the Interactive Link. ***** OE.NO_EVIL reduces the risk that authorised users of the TOE are non-hostile and follow all usage guidance to ensure that the Interactive Link is operated in a secure manner. This includes authorized personnel who are responsible for procuring third party hardware and

Assumptions	Objectives	Rationale
		software to used with the TOE.
A.USER	OE.PERSONNEL OE.NO_EVIL OE.TRAINING	A.USER assumes that the USER while in HIGH MODE will stop typing HIGH SIDE data before selecting the button on the front of the IL-KBS to change it to LOW MODE. The user shall not type HIGH SIDE data until the IL-KBS has been changed back to HIGH MODE. Thus USER will not place HIGH SIDE data directly onto the LOW SIDE NETWORK. OE.PERSONNEL ensures that all personnel, including USERS and those personnel responsible for the installation of the Interactive Link, are vetted and cleared to the security level of the HIGH SIDE. Users who are vetted and cleared are by default, trusted users and will not deliberately type HIGH SIDE information while the KBS is in low mode. ***** 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 Interactive Link is operated in a secure manner. Non-hostile users will not deliberately type HIGH SIDE information while the KBS is in low mode. ***** 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. Non-hostile, vetted, cleared (and by extension trusted) users are trained in the correct installation and operation of the IL devices and these users will not deliberately type HIGH SIDE information while the IL-KBS is in low mode. ***** Collectively, OE.PERSONNEL, OE.NO_EVIL and OE.TRAINING mitigate the risk of users deliberately typing HIGH SIDE data into the keyboard while the IL-KBS is in the LOW MODE, thus placing HIGH SIDE data directly onto the LOW SIDE NETWORK.
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

Assumptions	Objectives	Rationale
		and accidental misuse of the Interactive Link 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 Interactive Link devices are 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 Interactive Link devices. ***** 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 Interactive Link products are installed to connect the high and LOW SIDE networks. Additionally, this objective prevents the incorrect installation of the HIGH and LOW SIDE INTERFACE PORTS and the HIGH and LOW SIDE PERIPHERAL PORTS, thus protecting the confidentiality of the HIGH SIDE INFORMATION. ***** OE.NO_EVIL reduces the risk that users of the TOE are non-hostile and follow all usage guidance to ensure that the Interactive Link 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 Interactive Link is operated in a secure manner. ***** OE.PERSONNEL ensures that all personnel, including USERS and those personnel responsible for the installation of the Interactive Link, 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 4 - 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 / SFRs	O.CONFIDENTIAITY	O.INVOKE	O.FLUSH	O.SELECT	O.CONNECT	O.ROM	O.INDICATE	O.FAILSECURE	OE.KEYBOARD	O.TAMPER_SEALS
FDP_IFC.2.(A)/ FDP_IFF.1.(A)	✓									
FDP_IFC.2.(B)/ FDP_IFF.1.(B)	✓				✓					
FDP_IFF.5	✓									
FMT_MSA.3				✓						
FMT_SMF.1				✓						
FPT_FLS.1								✓		
FPT_RVM.1		✓								
FPT_SEP.3						✓				
EXT_IND.1							✓			
EXT_RIP.1			✓							
EXT_KYB.1									✓	
AGD_ADM.1										✓
AGD_USR.1										✓
ADO_DEL.2										✓

Table 5 - 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 is a TOE Security Objective that is satisfied by security assurance requirements. Table 5 - Security Requirements/Objectives Mapping, provides a mapping between the security requirements and the objectives that have been defined in Section 6; Table 6 – Security Requirements/Objectives Rationale, provides a detailed rationale of this mapping.

Objectives	Security Functional Requirement	Rationale
O.CONFIDENTIALITY	FDP_IFC.2.(A) Complete Information Flow Control FDP_IFF.1.(A) Simple Security Attributes FDP_IFF.5 No Illicit Information Flows	**IL-DDD** O.CONFIDENTIALITY is achieved through the diode functionality implemented in the IL-DDD, which serves to enforce the FDP_IFC.2(A), FDP_IFF.1(A), and FDP_IFF.5 requirements. ***** FDP_IFC.2(A) defines that the policy of the *Data Diode Non-interference 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(A) helps achieve the objective of O.CONFIDENTIALITY. ***** FDP_IFF.1(A) identifies the rules for the IL-DDD that are required to enforce the *Data Diode Non-interference SFP*. FDP_IFF.1(A) is based on the IL-DDD INTERFACE PORT attributes and USER DATA security attributes. These attributes are defined through FDP_IFF.1(A) and are required to achieve the SFP rules and the O.CONFIDENTIALITY objective. FDP_IFF.1(A) 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(A) 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.(A) and FDP_IFC.2(A) 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.
	FDP_IFC.2.(B) Complete Information Flow Control FDP_IFF.1.(B) Simple Security Attributes FDP_IFF.5 No Illicit Information Flows	**IL-KBS** FDP_IFC.2(B), FDP_IFF.1(B), and FDP_IFF.5 achieve the O.CONFIDENTIALITY objective by explicitly prohibiting any flows from the high side network through the IL-KBS to the low side network, including flows that might occur through the use of covert channels, thus both explicit and implicit flows are addressed. ***** FDP_IFC.2(B) ensures the Keyboard Switch Non-

Objectives	Security Functional Requirement	Rationale
		interference policy within the IL-KBS by controlling the information flows between PERIPHERAL PORT GROUPS. Enforcing the Keyboard Switch Non-interference SFP. FDP_IFC.2(B) helps achieve the objective of O.CONFIDENTIALITY ***** FDP_IFF.1(B) identifies the rules for the IL-KBS that are required to enforce the *Keyboard Switch Non-interference SFP*. FDP_IFF.1(B) is based on the COMMON, LOW SIDE and HIGH SIDE security attributes of the IL-KBS PERIPHERAL PORT GROUP. These attributes as defined through FDP_IFF.1(B) which define the destination of the USER DATA required to achieve the O.CONFIDENTIALITY objective. The FDP_IFF.1(B) requirement implements the O.CONFIDENTIALITY objective through the following explicit rules 1. All low mode data shall be allowed to flow to the low side peripheral port group 2. All high mode data shall be allowed to flow to the high side peripheral port group 3. No information shall flow from the low side peripheral port group to the high side peripheral port group 4. No information shall flow from the low side peripheral port group to the common peripheral port group 5. No information shall flow from the high side peripheral port group to the common peripheral port group 6. No information shall flow from the high side peripheral port group to the low side peripheral port group ***** FDP_IFF.5 further maintains the objective by ensuring that at all times within the IL-KBS 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 non-interference TSP at all times. This ensures that at no time can the IL-KBS or 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.

Objectives	Security Functional Requirement	Rationale
		***** 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 *Non-interference TSP* will be enforced at all times during TOE operation and that the TSP enforcing functions are always invoked before power is applied and when each function within the IL-DDD and/or IL-KBS are executed, thus preserving the O.INVOKE objective.
O.FLUSH	EXT_RIP.1 High Side Information Protection	The O.FLUSH objective of the IL-KBS ensures that the SF will flush all keyboard and/or mouse data from the KMF data buffers. When the user requests a mode change from HIGH to LOW, the IL-KBS enters a flush state, which allows any HIGH SIDE data stored within the KMF prior to initiating the mode change, to be flushed out of its data buffers. The O.FLUSH objective of the IL-KBS is achieved via the EXT_RIP.1 requirement. ***** EXT_RIP.1 implements the flush objective by ensuring that information intended for the HIGH SIDE is not made available to the LOW SIDE when the user changes mode. Because Part 2 of the Common Criteria does not provide a component appropriate to express the requirement for residual information protection in terms of the *Keyboard Switch Non-Interference flow control policy*, EXT_RIP.1 has been explicitly stated.
O.SELECT	FMT_MSA.3. Static Attribute Initialisation FMT_SMF.1 Specification of Management Functions	O.SELECT ensures that only an explicit action by the USER can be used to change the MODE of the IL-KBS and thus select the network the COMMON PERIPHERAL PORT GROUP are connected to. Implementing FMT_MSA.3 defines the initial parameters of the O.SELECT objective, which is HIGH MODE when power is applied. FMT_SMF.1 implements the prime functionality of O.SELECT by the USER performing an explicit action to change the current MODE of the IL-KBS from either the HIGH to LOW or LOW to HIGH. ***** FMT_MSA.3 defines the initial MODE of the IL-KBS and this helps achieve the objective O.SELECT. FMT_MSA.3 ensures that the IL-KBS assumes a default MODE of HIGH when first initialised, with the COMMON PERIPHERAL PORT GROUP connected to the HIGH SIDE NETWORK. There are no roles that can override the default initialisation value. The default value of HIGH MODE has been implemented through the design of the IL-KBS and cannot be changed. *****

Objectives	Security Functional Requirement	Rationale
		O.SELECT is primarily achieved through enforcement of FMT_SMF.1. FMT_SMF.1 ensures that only the USER can perform the explicit action to change the MODE of the IL-KBS and select either the HIGH SIDE or LOW SIDE PERIPHERAL PORT GROUP as the destination of the USER DATA presented to the COMMON PERIPHERAL PORT GROUP.
O.CONNECT	FDP_IFC.2.(B) Complete INFORMATION Flow Control FDP_IFF.1.(B) Simple Security Attributes	O.CONNECT ensures the COMMON PERIPHERAL PORT GROUP are connected to either the HIGH or LOW SIDES at any one time. The HIGH SIDE PERIPHERAL PORT GROUP is uniquely associated with the HIGH MODE and the LOW SIDE PERIPHERAL PORT GROUP is uniquely associated with the LOW MODE. The current MODE of the TOE determines the PERIPHERAL PORT GROUP that the COMMON PERIPHERAL PORT GROUP is connected too. O.CONNECT is collectively achieved through the requirements of FDP_IFC.2.(B) and FDP_IFF.1.(B). ***** FDP_IFC.2.(B) ensures the *Keyboard Switch Non-Interference SFP* is enforced by the IL-KBS on the information flows between PERIPHERAL PORT GROUPS. ***** FDP_IFF.1.(B) identifies the rules for the IL-KBS that are required to enforce the *Keyboard Switch Non-interference SFP* based on the security attributes of USER DATA and the PERIPHERAL PORT GROUPS. The FDP_IFF.1(B) requirement implements the O.CONNECT objective through the following explicit rules 1. All low mode data shall be allowed to flow to the low side peripheral port group 2. All high mode data shall be allowed to flow to the high side peripheral port group 3. No information shall flow from the low side peripheral port group to the high side peripheral port group 4. No information shall flow from the low side peripheral port group to the common peripheral port group 5. No information shall flow from the high side peripheral port group to the common peripheral port group 6. No information shall flow from the high side peripheral port group to the low side peripheral port group

Objectives	Security Functional Requirement	Rationale
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 SFs to execute and that the SFs are protected from external tampering and interference by untrusted subjects. Hence the TSF is protected against unauthorised modification.
O.INDICATE	EXT_IND.1 Indication Function	O.INDICATE ensures that the USER receives an unambiguous indication of which MODE, and hence which network has been selected. In meeting this objective, EXT_IND.1.implements a visual indication of the current MODE the IL-KBS (i.e. either HIGH or LOW) and an audible tone indicates a successful mode change. ***** The explicitly stated requirement EXT_IND.1 ensures there is positive feedback from the IL-KBS to the USER by indication of the current MODE of the IL-KBS and by an audible indicator re-enforcing a MODE change has occurred. Because Part 2 of the Common Criteria does not provide a component appropriate to express the requirement for visual and audible indication, EXT_IND.1 has been explicitly stated.
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 SFs, though they 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. Both the IL-DDD and the IL-KBS meet the requirement by having built in redundancy to ensure that the *Non-interference TSP* is maintained should a single component failure occur.
OE.KEYBOARD	EXT_KYB.1 Keyboard Data Transmission	OE KEYBOARD is an objective of the environment that requires the keyboard and mouse used in conjunction with the TOE to conform with the requirements identified within the guidance documentation provided with the Interactive Link. The keyboard and mouse are not part of the TOE but are within the IT Environment. ***** EXT_KYB, is an explicit security functional requirement that amplifies a specific functional requirement of the keyboard and mouse that implements the objective and

Objectives	Security Functional Requirement	Rationale
		reduces the risk of T.KEYBOARD. It is not listed within part 2 of the CC, and is associated with the IT environment. EXT_KYB requires that all HIGH SIDE information entered into the keyboard and mouse is transmitted to the IL-KBS within 249mS. 250mS is the duration of the flush period, the period after the IL-KBS changes from HIGH to LOW MODE. The explicitly stated SFR, EXT_KYB ensures that the keyboard and mouse outputs all the HIGH SIDE INFORMATION within their buffers in less than 249mS after the HIGH to LOW MODE request has occurred.
O.TAMPER_SEALS	AGD_ADM.1 Administrator Guidance AGD_USR.1 User Guidance ADO_DEL.2 Detection of Modification	O.TAMPER_SEALS maps to the AGD_ADM.1, AGD_USR.1 and ADO_DEL.2 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-KBS and 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 both the IL-DDD and IL-KBS devices. Upon receipt of the Interactive Link, the customer must 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-KBS or 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 USER (IL-KBS) or the SYSTEM MANAGEMENT STAFF (IL-DDD). Any attempt to access the contents of either the devices will be clearly visible.

Table 6 – 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 7 - Assurance Measures, defines how the assurance requirements of the TOE are equal too or greater than those required for EAL5. Table 7 also provides a reference between each TOE assurance requirement and the related documentation that satisfies each requirement.

Assurance Component	Documents Satisfying Components	Rational
ACM_AUT.1	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.4	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. 2	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 Interactive Link is installed and configured securely in the user environment.
ADV_FSP.3	B217P00002002 Functional Specification	The Functional Specification documentation provides a formally defined high-level description of the user-visible interface and behavior of the Interactive Link TSF.
ADV_HLD.3	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.2	B217P00002006 Implementation for Interactive Link 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.1	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.1	B217P00002004 Semiformal Low-level Design for Interactive Link 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.2	B217P00002007 Correspondence	The Correspondence Demonstration provides an analysis of correspondence between all adjacent pairs of TSF

Assurance Component	Documents Satisfying Components	Rational
	Demonstration for Interactive Link	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.1	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.2	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.2	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.2	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.
ATE_DPT.2	B217P00004001 Tests	The Test documentation tests the IL at all functional subsystems down to the basic components.
ATE_FUN.1	B217P00004001 Tests	The Test documentation demonstrates that all security functions perform as specified.
ATE_IND.2	B217P00004001 Tests	The Test documentation demonstrates that all security functions perform as specified.
AVA_CCA.2	B217P00005001 Binding and Covert Channel Analysis	The Binding and Covert Channel Analysis identifies potential vulnerabilities through an exhaustive search for covert channels.
AVA_MSU.2	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.

Assurance Component	Documents Satisfying Components	Rational
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-KBS or the IL-DDD; therefore, no strength of function claim has been made.
AVA_VLA.3	B217P00005006 Vulnerability Analysis – Highly Resistant for Interactive Link 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 7 - Assurance Measures

9.3.2.1 Rationale for TOE Assurance Requirements

The Interactive Link is a clip on security product that 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 Interactive Link is expected 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.

9.3.3 Dependencies Analysis

The dependencies of the security functional requirements of the Interactive Link are defined in Table 8. With the exception of FMT_SMR.1, FMT_MSA.1 and, an iteration of FMT_MSA.3 all dependencies have been met.

Dependencies / SFRs	FDP_IFC.1.(A)	FDP_IFC.1.(B)	FDP_IFF.1.(A)	FDP_IFF.1.(B)	FMT_MSA.1†	FMT_MSA.3‡	FMT_SMR.1†	AVA_CCA.3†	ADV_SPM.1
FDP_IFC.2.(A)			✓						
FDP_IFC.2.(B)				✓					
FDP_IFF.1.(A)	✓					✓			
FDP_IFF.1.(B)		✓				✓			
FDP_IFF.5	✓	✓						✓	
FMT_MSA.3					✓		✓		
FMT_SMF.1									
FPT_FLS.1									✓
FPT_RVM.1									
FPT_SEP.3									
EXT_IND.1									
EXT_RIP.1									
EXT_KYB.1									

† *These dependencies have not been met by the Interactive Link, refer to section 9.3.3.1.*

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

Table 8 - Mapping of Security Functional Requirements Dependencies

9.3.3.1 Dependencies Not Met

The Interactive Link does not meet the dependency of FMT_SMR.1 - Security Roles.

The IL-KBS does not require the association of users with roles; hence, there is only one “role”, that of the USER. This deleted requirement, a dependency of FMT_MSA.3, allows the IL-KBS to operate normally in the absence of any formal roles.

The IL-KBS does not meet the dependency of FMT_MSA.1 - Management of Security Attributes.

The requirement of FMT_MSA.1 for the IL-KBS SFs is to enforce the Keyboard Switch Non-Interference SFP to restrict the ability of a user to modify the mode of the IL-KBS is not being met. The normal operation of the IL-KBS allows the users to change the mode at anytime.

SFR FMT_SMF.1 allows a USER to perform an explicit action to change the MODE of the IL-KBS to either the HIGH or LOW MODE.

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 of AVA_CCA.3 for the IL-KBS SF FDP_IFF.5 has been met by AVA_CCA.2; at EAL5 a systematic search of covert channels that is structured and repeatable is commensurate with the level of assurance being provided.

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 9 - Classification of Mutually Supportive Requirements, demonstrate that the SFRs are complete and internally consistent.

The primary function of the IL-KBS, is to allow INFORMATION flows only from the COMMON PERIPHERALS to either the USERS HIGH SIDE WINDOW SERVER or the LOW SIDE NETWORK, dependent upon the MODE. While 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 in both cases the protecting the asset, HIGH SIDE INFORMATION, is provided by the SFRs from the FDP class.

The FMT class provides supporting functions to the FDP class. FMT_MSA.3 provides the USER with a known initial MODE of the IL-KBS. FMT_SMF.1 ensures that a USER can perform an explicit action to change the MODE of the IL-KBS and select either the HIGH MODE or LOW MODE. EXT_IND supports this USER function by providing unambiguous indication to the user of the current MODE of the IL-KBS and when the MODE has successfully been changed.

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) and ensuring isolation of the SF (FPT_SEP.3). While FPT_FLS.1 ensures that a single failure of the TOE will not result in a compromise of HIGH SIDE INFORMATION. A systematic covert channel analysis as defined by AVA_CCA.2 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 objectives ***O.CONFIDENTIALITY*** and ***O.CONNECT.***
	FDP_IFF.1 Simple Security Attributes	

Purpose	Security Requirement	Description
Mode & Installation Management	FMT_SMF.1 Specification of Management Functions FMT_MSA.3 Static Attribute Initialisation	These provide supporting functionality to help the TOE in meeting the objectives ***O.CONNECT, O.INDICATE*** and ***O.SELECT.***
	EXT_IND.1 Indication Function	
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.SELECT, 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.CONNECT, O.FAILSECURE, O.TAMPER_SEALS and O.INVOKE.***
	AVA_CCA.2 Systematic 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.2 Detection of Modification	
High Side Information Protection	EXT_RIP.1 High Side Information Protection	This requirement provides supporting functionality to help the TOE achieve its primary functionality and meet the ***O.FLUSH*** objective.

Table 9 - Classification of Mutually Supportive Requirements

9.3.5 Strength of Function Claim

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

9.4 TOE Summary Specification Rationale

Table 10 - Mapping between SFs 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 10 is discussed below in Section 9.4.1 Correlation between SFs 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 Security Functional Requirements.

Components	IL-KBS			IL-DDD
Security Functions / **SFRs**	SF.DP_SW	SF.IND	SF.KMF	SF.DD
FDP_IFC.2.(A) / FDP_IFF.1.(A)				✓
FDP_IFC.2.(B) / FDP_IFF.1.(B)	✓			
FDP_IFF.5	✓			✓
FMT_MSA.3	✓			
FMT_SMF.1	✓			
FPT_FLS.1	✓	✓	✓	✓
FPT_RVM.1	✓			✓
FPT_SEP.3	✓		✓	✓
EXT_IND.1	✓	✓		
EXT_RIP.1	✓		✓	

Table 10 - Mapping between SFs and SFRs

9.4.1 Correlation between SFs and SFRs

FDP_IFC.2.(A) & FDP_IFF.1.(A) The *Data Diode Non-interference 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(A) SFR is definitional and is used to set up the parameters to be used in the FDP_IFF.1.(A) requirement. FDP_IFC.2(A) defines that the *Data Diode Non-interference SFP*, which is the the Information flow control policy used within the ***SF.DD***. FDP_IFC.2(A) also defines the *subjects*: INTERFACE PORTS and *information*: USER DATA that implement the information flow control policy. The *Data Diode Non-interference 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.(A) 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 *Data Diode Non-interference SFP* within the FDP_IFF.1(A) 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 *Data Diode Non-interference 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(A) SFR.

FDP_IFC.2.(B) & FDP_IFF.1.(B) The *Keyboard Switch Non-interference SFP* is enforced by ***SF.DP_SW***.

SF.DP_SW allows keyboard and mouse data to pass to either the HIGH SIDE or the LOW SIDE (via the LHF and the RHF respectively) dependent upon the MODE of the ***SF.DP_SW.*** Within the ***SF.DP_SW*** there is no direct link from the high side to the low side.

SF.DP_SW prevents data flowing from the USER'S HIGH SIDE WINDOW SERVER and LOW SIDE NETWORK into the keyboard and mouse. It ensures that no data can flow from the USER'S HIGH SIDE WINDOW SERVER into the keyboard and mouse when in HIGH MODE and then into the LOW SIDE NETWORK when in LOW MODE. The ***SF.DP_SW*** enforces a unidirectional data path between itself and the each of the other functions. The ***SF.DP_SW*** provides the diode functionality, which prevents HIGH SIDE data from being transmitted to the LOW SIDE NETWORK through the IL-KBS. The MODE of the IL-KBS (HIGH/LOW) is the parameter that is tested to determine which port the USER DATA will flow to.

As with the ***SF.DD*** iteration of the SFR, FDP_IFC.2(B) is definitional and is used as a basis for the FDP_IFF.1.(B) requirement. FDP_IFC.2(B) defines that the *Keyboard Switch Non-interference SFP* as the Information flow control policy used within the ***SF.DP_SW***. FDP_IFC.2(B) also defines the *subjects*: PERIPHERAL PORT GROUPS and *information*: USER DATA that the information flow control policy is enforced upon. The *Keyboard Switch Non-interference SFP* has been defined as: LOW SIDE *subjects* and *information* are not influenced by HIGH SIDE *subjects* and *information*, this includes HIGH SIDE *information* presented to the keyboard and mouse. The HIGH SIDE does not interfere with the LOW SIDE.

FDP_IFF.1.(B) defines the attributes of the different instances of the subjects and information before defining the rule set for information flow. The ***SF. DP_SW*** has three PERIPHERAL PORT GROUPS:

a. The COMMON PERIPHERAL PORT GROUP which is the interface that receives data originated from the keyboard and mouse and presented to the ***SF.DP_SW*** via the ***SF.KMF,*** this interface is an input;

b. The LOW SIDE PERIPHERAL PORT GROUP, which is an output for keyboard and mouse data to be passed to the RHF and onto the LOW SIDE.

c. The HIGH SIDE PERIPHERAL PORT GROUP, which is the HIGH SIDE output where keyboard and mouse data to be passed to the USERS HIGH SIDE WINDOW SERVER via the LHF.

There are four forms of USER DATA defined for the ***SF.DP_SW*** LOW SIDE and HIGH SIDE associated with the data resident on the LOW and HIGH SIDE NETWORKS respectively and the LOW MODE and HIGH MODE DATA associated with the keyboard and mouse data in transition from the COMMON PERIPHERAL PORT GROUP to the LOW SIDE PERIPHERAL PORT GROUP and the HIGH SIDE PERIPHERAL PORT GROUP respectively.

The following "permit" rules have been defined for the *Keyboard Switch Non-interference SFP* within the FDP_IFF.1(B) requirement:

1. *All LOW MODE DATA shall be allowed to flow to the LOW SIDE PERIPHERAL PORT GROUP.*
2. *All HIGH MODE DATA shall be allowed to flow to the HIGH SIDE PERIPHERAL PORT GROUP.*

The following "deny" rules have been defined for the *Keyboard Switch Non-interference SFP* within the FDP_IFF.1(B) requirement:

3. *No information shall flow from the LOW SIDE PERIPHERAL PORT GROUP to the HIGH SIDE PERIPHERAL PORT GROUP.*
4. *No information shall flow from the LOW SIDE PERIPHERAL PORT GROUP to the COMMON PERIPHERAL PORT GROUP.*
5. *No information shall flow from the HIGH SIDE PERIPHERAL PORT GROUP to the COMMON PERIPHERAL PORT GROUP.*
6. *No information shall flow from the HIGH SIDE PERIPHERAL PORT GROUP to the LOW SIDE PERIPHERAL PORT GROUP.*

The *Keyboard Switch Non-interference SFP* is implemented by the ***SF.DP_SW.***

SF.DP_SW is implemented within the IL-KBS DSF. Due to the diode functionality between the keyboard and mouse interface and the high and low side and employed within the ***SF.DP_SW*** the above rule set has been implemented.

FMT_MSA.3 This requirement is implemented by ***SF.DP_SW***.

The ***SF.DP_SW*** provides the switching mechanism that enables the USER to select the MODE and thus the HIGH or LOW SIDE NETWORKS that they intend to interact with. The ***SF.DP_SW*** senses the state of two buttons on the IL-KBS front panel, by which the USER selects the MODE, and when a change request is received controls the switching of the IL-KBS MODE as appropriate.

SF.DP_SW is responsible for implementing FMT_MSA.3 within the IL-KBS. FMT_MSA.3 requires that the IL-KBS assumes a default MODE of HIGH when first initialised, with the

keyboard and mouse connected to the HIGH SIDE NETWORK. While in HIGH MODE, HIGH SIDE USER DATA entered into the keyboard and mouse is passed to the HIGH SIDE PERIPHERAL PORT GROUP onto the USER HIGH SIDE WINDOW SERVER. There are no roles that can override the default initialisation value set to HIGH. HIGH MODE default is a requirement that has been defined during the design of the IL-KBS and cannot be changed.

FMT_SMF.1 This requirement is implemented by ***SF.DP_SW*.**

By design, the IL-KBS assumes a default MODE of HIGH when first initialised. The user must select the LOW button to switch from the HIGH SIDE NETWORK to the LOW SIDE NETWORK. Once the user selects the LOW button, the IL-KBS is switched to LOW MODE and the COMMON PERIPHERALS are connected to the LOW SIDE NETWORK. To switch back to the HIGH MODE, the user must select the HIGH button. The IL-KBS is then returned to HIGH MODE and the COMMON PERIPHERALS are connected to the HIGH SIDE NETWORK. This explicit action by the user ensures the MODE of the IL-KBS cannot change without the USERS knowledge.

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

The SFs of the IL-KBS and 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-KBS and IL-DDD, ensuring the TOE does not violate its *Non-interference TSP.*

The Interactive Link has been designed, developed and implemented so that if a single component fails, the failure will not result in a violation of the Non-interference TSP. Assurance of secure state preservation has been achieved in hardware; the SFs 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.DP_SW, SF.IND*** and ***SF.DD*** SFs. The components of the ***SF.DP_SW*** have been placed in series to ensure that when one component fails there is another component responsible for maintaining security. The components of the ***SF.IND*** have been placed in parallel. These parallel components include four light sources affixed behind the front panel of the IL-KBS chassis; two LEDs situated behind the LOW SIDE visual indicator and two LEDs situated behind the HIGH SIDE visual indicator. Should one LED fail, the second light source will maintain visual indication. 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 *Data Diode Non-Interference 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 Non-interference TSP.

The ***SF.KMF*** provides residual information protection and is a supportive SF. The objective of the ***SF.KMF*** is by design to minimise the amount of memory utilized by the KMF function. The result of single hardware failure will not increase the amount of residual memory within the KMF, which maintains its secure functionality.

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

The FPT_RVM.1 requirement is realised by the ***SF.DP_SW*** and the ***SF.DD*** SFs. These primary SFs implement the TSP and ensure that it is always invoked and cannot be bypassed. The SF.KMF and SF.IND are supportive SFs. The FPT_RVM.1 requirement applies to three states of the IL-KBS and/or 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 SFs are implemented in the hardware and firmware within the IL-KBS and the hardware of IL-DDD, both devices maintain secure state behaviour when power is removed. While the IL-KBS is in the *power-off* state, there is no power supplied to the ***SF.DP_SW*** thus, PERIPHERAL DATA cannot be transferred between PERIPHERAL PORT GROUPS. 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-KBS enters the *power-on* state, the ***SF.DP_SW*** ensures that the MODE of the IL-KBS defaults to HIGH MODE. This MODE cannot be changed until explicit action by the USER is applied to the IL-KBS. The ***SF.KMF*** provides the only input channel to the ***SF.DP_SW***. Data is sent from the ***SF.KMF*** and passed through the ***SF.DP_SW*** to either the HIGH SIDE network or the LOW SIDE network, dependant on the current mode of the IL-KBS. The ***SF.DP_SW*** is implemented in hardware within an isolated security domain and provides the only interface between the ***SF.KMF*** and the high and LOW SIDE networks. This ensures that untrusted subjects cannot bypass the ***SF.DP_SW***. Within the ***SF.DP_SW*** there is no channel for a direct path from the HIGH SIDE to the LOW SIDE so a compromise to bypass the SF cannot be realized within the ***SF.DP_SW.***

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***.

FDP_IFF.5 No illicit data flows exist to circumvent the Non-interference TSP.

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.DP_SW and ***SF.DD,*** these SFs provide the interface to the LOW SIDE. The ***SF.DP_SW*** provides the only interface between the ***SF.KMF*** and the HIGH and LOW SIDE networks. Keyboard and mouse data sent to the ***SF.KMF***, which is forwarded onto the ***SF.DP_SW,*** is an output to either the LHF (HIGH SIDE) or RHF (LOW SIDE), dependant on the current MODE of the IL-KBS. Within the ***SF.DP_SW***, diode functionality is implemented at the output ports to both the HIGH and LOW SIDE NETWORKS to prevent data from flowing back through the ***SF.DP_SW*** from either the HIGH SIDE or LOW SIDE**.** The data sourced from the ***SF.KMF*** intended for the LOW SIDE is LOW SIDE data. Since the source is low side and the destination is low side there is no illicit data flow from the ***SF.DP_SW*** 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.

EXT_RIP.1 The EXT_RIP.1 requirement ensures that there is no available high side keyboard and/or mouse data contained in the ***SF.KMF*** data buffers, which could compromise the objectives of the TOE.

The security functionality of the IL-KBS prevents data flowing between the HIGH or LOW SIDE NETWORKs via the keyboard and mouse. The EXT_RIP requirement is implemented via the ***SF.KMF*** and ***SF.DP_SW*** within the IL-KBS. The KMF has been designed to minimise its memory utilisation this reduces its storage capability of residual HIGH SIDE data. ***SF.DP_SW*** enters a flush state to ensure that no high side keyboard and/or mouse data is retained within the ***SF.KMF*** data buffers when the IL-KBS changes from HIGH to LOW MODE. The flush state is represented by a neutral connection to the HIGH SIDE and LOW SIDE to allow any HIGH SIDE data entered into the keyboard and/or mouse, prior to a mode change, to be flushed out of any data buffers that may exist prior to the ***SF.DP_SW*** changing mode. The flush period is greater than the time required to allow any HIGH SIDE data entered into the keyboard and/or mouse to be flushed out.

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 Interactive Link has two purpose built security devices; the IL-KBS and the IL-DDD. The ***SF.DP_SW, SF.IND*** and ***SF.KMF*** are implemented in the hardware of the IL-KBS while the ***SF.DD*** is implemented in the hardware of the IL-DDD.

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.DP_SW, SF.IND, SF.KMF*** and ***SF.DD*** SFs maintain a distinct security domain for execution to protect against changes that might compromise the TOE's security objectives. This is accomplished via implementing the ***SF.DP_SW, SF.IND*** and ***SF.DD*** SFs solely in hardware. In so doing, the SFs do not execute any software or firmware and therefore cannot be circumvented by any software threat. ***SF.KMF*** has been implemented in firmware executed on a standalone microcontroller that is solely restricted to KMF functionality.

FPT_SEP.3 also requires that the TSF shall maintain the part of the TSF that enforces the information flow control SFPs in a security domain there are two information flow control SFPs within the Interactive Link. The *Data Diode Non-interference SFP*, of the ***SF.DD,*** is implement in the standalone IL-DDD and the *Keyboard Switch Non-interference SFP,* of the ***SF.DP_SW*** is implemented within the IL-KBS. Though the ***SF.DP_SW*** is implemented on the same Printed Circuit Board (PCB) as the other modules within the IL-KBS it is compartmented to a distinct area for its own independent execution.

EXT_IND.1 This requirement is implemented by ***SF.DP_SW*** and ***SF.IND***.

The ***SF.DP_SW*** controls ***SF.IND*** by the use of the current MODE. ***SF.IND*** exclusively activates the relevant backlit label on the IL-KBS front panel to signify the current MODE and to indicate when a MODE change is occurring. The ***SF.IND*** activates a short duration audible indicator to notify the USER of the MODE change. The visual and audible indicators are implemented as described in the TSS Section 7.

10 Conclusion

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

The assurance requirements are those of EAL 5 augmented with AVA_CCA.2 as defined within the CC part 3. The following additional Security Functional Requirements outside the scope of the CC part 2 have also been defined and utilised: EXT_IND, EXT_RIP and EXT_KYB.