Doc. No. 96162D01000042
Issue No. 3.1
Copy No. ___

BAE SYSTEMS AUSTRALIA DATAGATE PTY LTD

INTERACTIVE LINK

MULTIPLE COMPUTER SWITCH

SECURITY TARGET

CAPO C438761

Prepared For: Multi-Level Information Security Projects
Electronic Systems Acquisition Division
Defence Acquisition Organisation

Prepared By: BAE Systems Australia Datagate Pty Ltd
Second Avenue
Technology Park
MAWSON LAKES SA 5095

Approved By: _____ Date: _____
Christopher M. Walsh
Chief Information Security Officer
BAE Systems Australia Pty Ltd

Amendment Status

As necessary, authorised amendments will be issued to all holders of this document. Amendments will take the form of replacement or additional pages.

The amendment status appears at the top right hand side of each page eg. Issue 1.0 signifies Issue 1, Amendment 0. Next amendment change will read Issue 1.1 (Issue 1, Amendment 1, etc).

Upon receipt, amendment pages are to be incorporated in this document, and superseded pages removed. The amendment number, the date of incorporation and the signature of the Amending Officer are to be entered in the table below, for each amendment incorporated.

Amendment No.	Date Incorporated	Entered By
3.1	8 May 2009	Chris Walsh

List Of Effective Pages

Page	Issue	Amendment No.	Comment
i	3	1	
ii	3	1	
iii	3	1	
iv	3	1	
v	3	1	
1	3	1	
2	3	1	
3	3	1	
4	3	1	
5	3	1	
6	3	1	
7	3	1	
8	3	1	
9	3	1	
10	3	1	
11	3	1	
12	3	1	
13	3	1	
14	3	1	
15	3	1	
16	3	1	
17	3	1	
18	3	1	
19	3	1	
20	3	1	
21	3	1	
22	3	1	
23	3	1	
24	3	1	
25	3	1	
26	3	1	

Contents

List of Figures

List of Tables

1 Scope

1.1 Identification

This Security Target defines the security being provided by the Interactive Link Multiple Computer Switch (IL-MCS), Part Number FID004 Version 2.0, which is being developed under Phase 1 of the Australian Defence Department Joint Project (JP) 2049, Multi-Level Information Security Project (MLISP).

1.2 Purpose

The purpose and objectives of this security target is to provide a specification of the security functionality of the IL-MCS. It also relates the system to the environment in which it is intended to operate. This security target is the basis for an Information Technology Security Evaluation Criteria (ITSEC) evaluation.

Note that unique numbers are assigned to the statements regarding method of use, environment, objectives, threats, security functions and mechanisms. This is for the purpose of explicit references in related evaluation documentation.

1.3 Document Overview

This security target has been developed in accordance with ITSEC sections 2.3–2.7, Security Target. This target describes the security functionality of the IL-MCS; it shall change, in accordance with the Configuration Management process of the project, as design decisions are ratified. These changes are due to the fact that the evaluation is concurrent with the design and development. The security target contains the following sections:

a. Section 1 - Scope; this section defines the document, its purpose, and objectives. It also defines the format of the document.

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

c. Section 3 - Product Rationale; this section defines the Target of Evaluation, the security objectives, assumed threats, and the intended environment in which the IL-MCS is to be used. It also defines the method of use and gives a summary of the Security Features.

d. Section 4 - Specifications of Security Enforcing Functions; this section defines the functions that contribute towards satisfying the security objectives of the IL-MCS.

e. Section 5 - Definition of Required Security Mechanisms; this section defines the mechanisms that shall make up the Security Enforcing Functions.

f. Section 6 - Minimum Strength of Mechanisms; this section defines the type of mechanisms and the minimum strength for the IL-MCS.

g. Section 7 - Target Evaluation Level; this section claims the ITSEC target evaluation level for the IL-MCS.

2 Acronyms & Definitions

2.1 Acronyms

- ADF – Australian Defence Force.
- COTS - Commercial Off-The-Shelf.
- DSTO – Defence Science and Technology Organisation.
- DSD – Defence Signals Directorate.
- DSF – Data Switch Function.
- ERTZ - Equipment Radiation TEMPEST Zone.
- HLHF – High Side Local Host Function
- IL-MCS – Interactive Link Multiple Computer Switch.
- ISSO - Information System Security Officer.
- ITSEC - Information Technology Security Evaluation Criteria.
- JP - Joint Project.
- KMF – Keyboard Mouse Function.
- LLHF – Low Side Local Host Function.
- MLISP - Multi-Level Information Security Project.
- MLS - Multi-Level Security.
- SCEC - Australian Government – Securities Construction and Equipment Committee.
- SEF - Security Enforcing Function.
- SEM - Security Enforcing Mechanism.
- TCB – Trusted Computing Base.
- TOE - Target of Evaluation.
- SoM - Strength of Mechanism.
- VSF – Video Switch Function.

2.2 Definitions

High Mode indicates that the video is being received from and the keyboard and mouse data is directed to, the User's High Side Computer.

High Side is a descriptor used to refer to all items associated with the information classified at high level this includes the High Side Computer.

High Side Computer refers to the computer on the High Side that the IL-MCS interfaces to. The information handled by the computer is classified greater than the Low Side and can optionally be connected to a network.

Infosec refers to Information System Security.

JP2049 Joint Project number 2049 is the Multi-Level Information Security Project.

Low Mode indicates that the video is being received from and the keyboard and mouse data is directed to, the User's Low Side Computer.

Low Side is a descriptor used to refer to all items associated with the information classified at low level this includes the Low Side Computer.

Low Side Computer refers to the computer on the Low Side that the IL-MCS interfaces to. The information handled by the computer is classified less than the High Side and can optionally be connected to a network.

Secure Area as defined in SECMAN3 has the essential security features of:

a. tamper evident barriers;
b. an approved means of limiting entry to authorised personnel only;
c. either
   (i) a SCEC endorsed Type 1 security alarm system providing after hours coverage; or
   (ii) the area is safeguarded by a combination of SCEC endorsed/ASIO approved physical barriers and guard patrols;
d. the reaction to an alarm by a response force should be within thirty minutes.

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

Trusted Computer Base refers to the combination of the security enforcing and security relevant components of the Target of Evaluation.

Type B mechanism is a security mechanism, which, if perfectly conceived and implemented, will have no weaknesses, and considered impregnable to direct attack regardless of the level of resource, expertise and opportunity deployed. Therefore type B mechanisms have no Strength of Mechanism (SoM) rating.

User refers to the person who utilises the IL-MCS in performance of duties.

2.3 References

- 96125P01000021, (1997) Interactive Link Risk and Threat Assessment, BAE Systems Australia Datagatel, Draft Issue 2.1.
- ACSI 33, (1998) Security Guidelines for Australian Government IT Systems, Defence Signals Directorate (DSD).
- ASSRO Supplement 1 Part A (September 1997) Australian SIGINT Security Regulations Orders, Security Standards for SI Computer Systems.
- ASSRO Supplement 1 Part B (September 1997) Australian SIGINT Security Regulations Orders, COMSEC Installation and Certification Standards for Special Intelligence (SI) Communications Systems.
- DSTO-TR-96162D01000043, (1998) Interactive Link Multiple Computer Switch Formal Policy and Architecture, Defence Science and Technology Organisation (DSTO), Issue 1.0.
- ITSEC (1991) Information Technology Security Evaluation Criteria, Version 1.2, Commission of the European Communities.
- ITSEM (1993) Information Technology Security Evaluation Manual, Version 1.0 Commission of the European Communities.
- SECMAN3 (1995) Information System Security, Edition 5, Defence Security Branch.
- UKSP 04, Part 3, (1996) UK IT Security Evaluation & Certification Scheme Developers' Guide - Part III: Advice to Developers, Issue 1.0.

3 IL-MCS - Product Rationale

3.1 Introduction

The purpose of this product rationale is to provide the security objectives and a statement describing the type of environment in which the IL-MCS should be used to preserve security. It also defines the intended method of use and provides an appraisal of threats to security. Finally the product rationale presents a summary of the security features employed by the IL-MCS.

A formal model of the security policy defining the underlying security to be enforced by the IL-MCS is provided in the IL-MCS Formal Policy and Architecture Document DSTO-TR-96162D01000043.

3.2 The IL-MCS Concept

The IL-MCS provides access to two computers of different security classification while preserving the confidentiality of the High Side information. The concept is based on keeping the two computers and associated classified data separate from each other. The IL-MCS switches the peripherals that provide the user interface (which consists of the monitor, keyboard and mouse) between the two computers with a high level of trust. Figure 1 shows a possible User's desktop configuration.

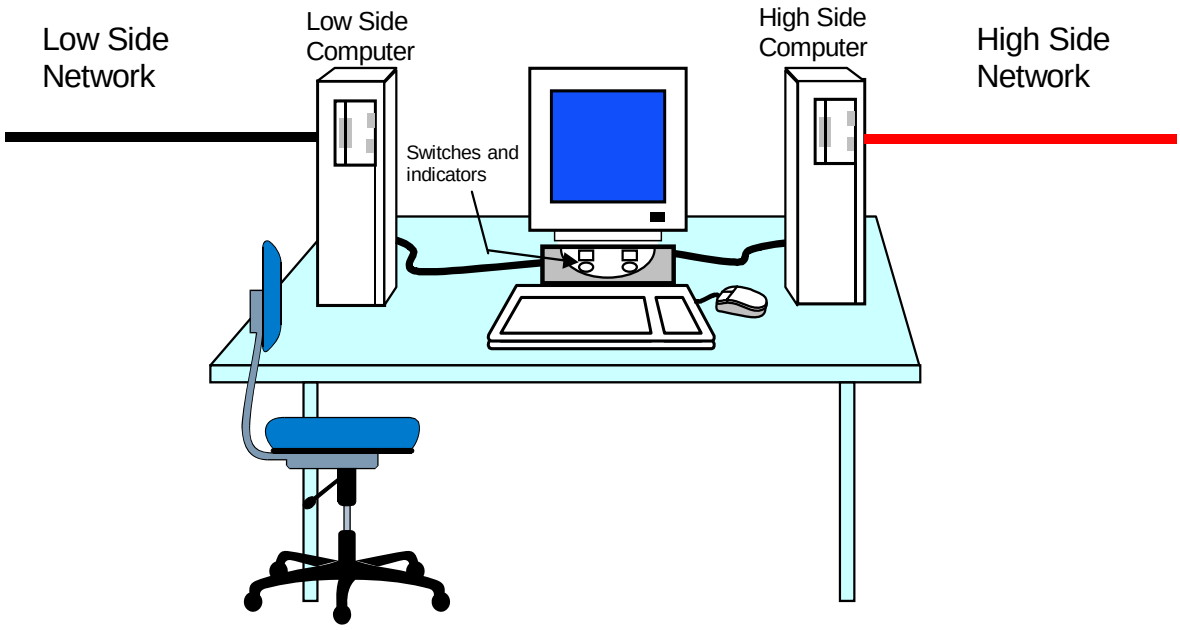

Figure 1: User's Desk Configuration

The User can access the information on either computer with a common keyboard, mouse and monitor. Keyboard and mouse data is directed by the IL-MCS to the selected computer, while the video output from the same computer is directed to a common monitor. When the User wishes to process information on the High Side Computer he or she would select the IL-MCS High Side connection. This High Side connection is made by pressing the High Side button,

placing the IL-MCS in to it's High Mode. Changing mode produces an audible beep to indicate that the change was successful. When the High Mode is selected the High Side indicator is illuminated and the keyboard, mouse and monitor are connected to the High Side Computer. Similarly when requiring the Low Side connection, the user presses the Low Side button on the IL-MCS. Following the audible beep and illumination of Low Side indicator from the IL-MCS, the keyboard and mouse data is directed to the Low Side Computer and its output is displayed on the monitor. No physical path exists within the IL-MCS for information to be transferred between the two computers.

3.3 Definition of the Target of Evaluation

The Target of Evaluation (TOE) consists of both firmware and hardware components. The hardware components contribute to satisfying the security objectives of the TOE, while the firmware provides support. Some of the firmware is security relevant and some of the hardware components are security enforcing. The security enforcing and relevant components make up the IL-MCS Trusted Computing Base (TCB).

The TOE consists of the following components as depictured in Figure 2:

a. Video Switch Function (VSF): switches video to the monitor, the source is dependent upon the mode that the DSF is in.

b. Data Switch Function (DSF): switches the output of the keyboard and mouse to either the LLHF or the HLHF, dependent upon its mode. The DSF contains the data switching function, the user-input push buttons, the visual indicators and the audible indicator. The mode is selected by the push buttons and displayed by the indicators.

c. Keyboard Mouse Function (KMF): is the interface to the keyboard and mouse. It provides the hand shaking required by the keyboard and mouse and is implemented using a micro-controller and embedded software.

d. Low Side Local Host Function (LLHF): is the interface to the Low Side Computer. It provides the hand shaking required by the Low Side Computer and is implemented using a micro-controller and embedded software.

e. High Side Local Host Function (HLHF): is identical to and has the same functionality as the LLHF, except that it interfaces to the High Side Computer.

The KMF, DSF, and VSF make up the TCB and contain all the security enforcing and relevant functionality of the device.

The High and Low Side Computers are Commercial Off The Shelf (COTS) software and hardware and are not part of the evaluation. They can be used standalone or connected to a network and in either case has no impact on the security being provided by the IL-MCS.

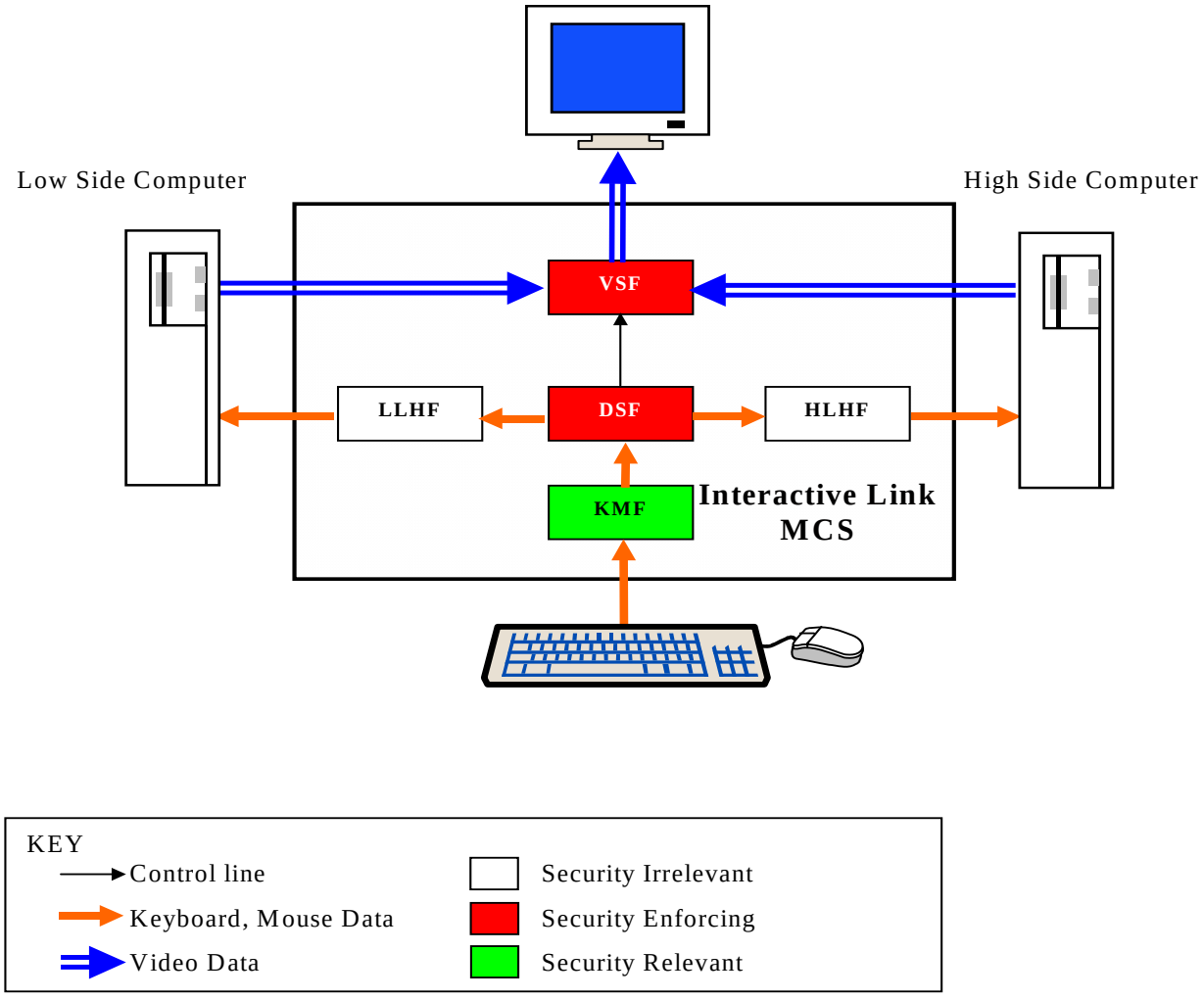

Figure 2: IL-MCS Block Diagram

3.4 Operational Environment

When the IL-MCS is used within a network configuration it should be noted that all High Side Users using an IL-MCS must be cleared to access the Low Side information. For example, it would not be appropriate for the High Side Network to be Secret Releasable and the Low Side Network to be Confidential AUSTEO, if all IL-MCS High Side Users do not have access to AUSTEO information. The operating environment in which the IL-MCS is to be used is characterised as follows:

IE1 The intended environment of the IL-MCS shall be an environment that meets the requirements of SECMAN3, ACSI33 or ASSRO Supplement 1. Classified systems have different environmental requirements, in terms of physical, personnel, media, communications, emanation security and management. These requirements also vary with different levels of classification. i.e. A connection from a Secret to an Unclassified network would have different requirements to that of a connection between a Confidential and a Restricted network. For the Australian Defence and Government systems, these requirements are defined in either SECMAN3, the Information Systems Security Manual for Australian Defence Force (ADF), ACSI 33, Security Guidelines for Australian Government

IT Systems or ASSRO Supplement 1, the Australian SIGINT Security Regulations Orders.

IE2 The intended environment will be capable of storing and operating the IL-MCS in accordance with the requirements of the High Side system. Information systems have different requirements for the storage of computer equipment used for processing information of different classifications. The IL-MCS has no long-term data storage devices from which classified information can be obtained, and is intended to be kept on the User's desk top, within the same environment as the High Side system.

IE3 It is intended that the product operate in an environment where physical (or some other) security measures prevent any TEMPEST attack. This could be achieved by ensuring that the security boundary is outside the IL-MCS Equipment Radiation TEMPEST Zone (ERTZ). All electronic based information systems produce unwanted electromagnetic emanations, which in some cases can be related to the information being processed. This phenomenon is known as TEMPEST. The space within which a successful TEMPEST intercept is considered possible is termed the ERTZ. Information Systems where TEMPEST is a concern are required to have a TEMPEST Threat Assessment undertaken so as to determine the Secure Boundary of the System. The IL-MCS operates at the edge of the secure boundary where the Low Side system meets the High Side system. Care should be taken to ensure that the IL-MCS ERTZ is within the secure boundary of the High Side system. This will ensure that any attempt to mount a TEMPEST attack would not compromise the security of the information system.

IE4 The IL-MCS will be sealed to be tamper evident. This can be achieved by using a seal that indicates if an adversary has gained access to the product. With access an adversary could change or disable the security enforcing functionality of the product. Seals that are Australian Government – Securities Construction and Equipment Committee (SCEC) endorsed, when removed, generate a random dot (measled) pattern which provides a visual indication to the operator or the Information System Security Officer (ISSO) of attempts to tamper with the device. The seal is to be in a clearly visible location on the product so that any attempt to access its contents will be clearly visible. The operator will be responsible for monitoring the seal, in the case of the IL-MCS.

IE5 The system management staff in accordance with the administration documentation shall install the IL-MCS. The installation of the IL-MCS is to be accredited by the appropriate security authority.

IE6 The intended environment includes virus scanners or appropriate mechanisms on the High and Low Side Computers to maintain integrity and availability to the desired level of assurance. Integrity and availability aspects of security are not part of the IL-MCS security objective. Integrity and availability need to be considered when addressing the total security of the combination of both the High and Low Side systems when connected by an IL-MCS product.

IE7 Equipment hardware and software procurement policies are to be followed to minimise the risk of installing malicious hardware and/or software.

IE8 All staff who have access to classified 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.

3.5 Intended Method of Use

The IL-MCS provides the User with access to information contained on the two computers with different classification. The IL-MCS provides the following methods of use:

U1. When the High Side button of the IL-MCS is pressed placing it in the High Mode, the User may interact with information and applications located on the High Side Computer. In this mode, keyboard and mouse data is passed via the IL-MCS to the User's High Side Computer to interact with applications. While in this mode the video generated from the High Side Computer is passed via the IL-MCS to the monitor.

U2. When the Low Side button of the IL-MCS is pressed placing it in the Low Mode, the User may interact with information and applications located on the Low Side Computer. In this mode, keyboard and mouse data is passed via the IL-MCS to the User's Low Side Computer to interact with applications. While in this mode the video generated from the Low Side Computer is passed via the IL-MCS to the monitor.

3.6 Security Objectives

The IL-MCS is intended to protect the asset, of High Side information, in accordance with the following objective:

O1. The information on the High Side Computer is kept confidential from the Low Side Computer.

When the IL-MCS is in High Mode information that the User enters via the keyboard and mouse is regarded as High Side information. Integrity and availability of the information on either the High or Low Side Networks is not within the scope of this evaluation. Third party products can be used to address these issues.

3.7 Assumed Threats

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

AT1 A User or process, e.g. a Trojan horse, on the High Side Computer that accidentally or deliberately breaches the confidentiality of some High Side information by transmitting data from a High Side Computer through the IL-MCS to the Low Side Computer.

AT2 A User accidentally types High Side data into the keyboard while the IL-MCS is in the Low Mode and therefore puts the High Side data directly onto the Low Side Computer.

AT3 A User deliberately types High Side data into the keyboard while the IL-MCS is in the Low Mode and therefore puts the High Side data directly onto the Low Side Computer.

AT4 A rogue keyboard or mouse copies data intended for the High Side Computer, as it is entered, and re-transmits the data to the Low Side Computer when the IL-MCS is in the Low Mode.

AT5 A rogue monitor that stores High Side information, and forwards the information to the Low Side Computer when the IL-MCS is in the Low Mode.

AT6 The person responsible for the installation of the IL-MCS, installs it accidentally or deliberately to cause High Side information to be transmitted to the Low Side Computer and this make the information available to Low Side Users.

AT7 The IL-MCS emanates radiation that carries discernible classified information that can be reconstructed by a person who is not supposed to have access to the information. This threat is associated with products that bridge the boundary of two systems; the IL-MCS is such a device.

AT8 An adversary tampers with the contents of the IL-MCS during delivery, and/or after installation to cause the compromise of the confidentiality of classified information handled by the product.

AT9 A User or process on the Low Side Computer transmits data to the IL-MCS that changes firmware or executables to causes the devices to breach the confidentiality of some High Side information.

3.8 Summary of Security Features

The IL-MCS is a standalone product that links two computers optionally connected to different classified networks. It allows keyboard and mouse data to flow into either the Low Side Computer or the High Side Computer, while allowing video information from the selected computer to be displayed on the monitor. Embedded software provides the communications and hand shaking required between the computers and the Keyboard and Mouse. No software is required for the video switch function. The hardware provides all the security enforcing functionality of the IL-MCS.

The goal of the IL-MCS is to provide access to the information on the Low Side Computer without compromising the confidentiality of the information on the High Side Computer,

while using a single (common) keyboard, mouse and monitor. The security enforcing functions of the IL-MCS counter the assumed threats when the stated operational environment is provided.

4 Specification of Security Enforcing Functions

4.1 Introduction

The Security Enforcing Functions (SEFs) that contribute to satisfying the Security Objectives of the IL-MCS are explained in this section. They are specified using both an informal and formal style. The formal style can be found in IL-MCS Formal Policy and Architecture Document DSTO-TR-96162D01000043.

4.2 IL-MCS SEFs

The IL-MCS provides the following SEFs. The functions are resident within the IL-MCS and have been implemented through different Security Enforcing Mechanisms (SEMs).

SF1 **Data Path Switch Function: To transfer data from the keyboard and mouse to either the High Side Computer (denoted as "High Mode") or the Low Side Computer (denoted as "Low Mode"), according to the mode selected by the User.** This function ensures that the keyboard and mouse data is transmitted to its intended destination either the High Side Computer or the Low Side Computer. The function prevents data flowing from the High and Low Side Computers into the keyboard and mouse. This functionality prevents data flowing from the High Side to the keyboard and mouse and then on to the Low Side.

There are two possible modes that the Keyboard Switch can be in, High or Low. The High Mode represents a connection of the Keyboard and Mouse output, via the IL-MCS, to the High Side Computer. While in the High Mode the Data Path Switch guarantees that no data will flow to the Low Side Computer. While in the Low Mode the Keyboard and Mouse output, is connected via the IL-MCS, to the Low Side Computer. The mode is selected by one of two push button switches on the front panel of the IL-MCS. Due to the IL-MCS being housed in the High Side environment, the default mode at power-on is High mode.

The purpose of this switching function is to provide a means to access the information of both the High and Low Side Computers via one keyboard and mouse. The functionality shall be implemented in hardware and the destination of keyboard and mouse data is determined by the mode of the IL-MCS.

SF2 **Video Path Switch Function: To transfer video from either the High Side Computer (denoted as "High Mode") or the Low Side Computer (denoted as "Low Mode") to the monitor, according to the current mode of the Data Path Switch Function, SF1.** This function ensures that the video data is transferred from the source, either the High Side Computer or the Low Side Computer to the destination, the common monitor. SEF SF2 prevents video data from flowing between the High and Low Side computers by the switching function.

SEF SF1 provides the functionality that selects the mode of the keyboard switch. The mode, of which there are two, High and Low, is selected by one of the push buttons on the front panel. SEF SF1 controls SEF SF2 by the use of the current

mode and provides synchronisation with the direction of the keyboard and mouse data. In the High Mode, video data sourced from the High Side Computer is passed, via the IL-MCS, to the Monitor and no data can pass to the Low Side Computer. While in the Low Mode the video data sourced from the Low Side Computer is passed via the IL-MCS, to the monitor.

The purpose of this video switching function is to provide a means by which both the High and Low Side Computers can securely use the same monitor. The functionality shall be implemented in hardware within the IL-MCS and the source of the video data is determined by the IL-MCS's mode.

SF3 **Indication Function: To indicate the current mode to the User.** This function ensures that the User is aware of the current mode and thus the destination of the keyboard and mouse data and the source of the video data. This function also indicates that a change of mode has occurred successfully. The indication will be unambiguous to the User.

SEF SF1 provides the functionality that selects the mode of the IL-MCS. The mode, of which there are two, High and Low, is selected by one of the push buttons on the front panel. SEF SF1 controls SEF SF3 by the use of the current mode. SEF SF3 provides an indication of that mode by illuminating the display for the mode. The display for each mode is positioned directly above the appropriate push button switch. Each display consists of a light source positioned behind a coloured transparent film that has a label designating the computer or optionally the network to which it is connected printed upon it. A change of mode is also indicated by a short audible beep.

The purpose of the indication is to give the User a method of determining with a high level of confidence, which mode that the IL-MCS is in. The reinforcing, audible indication is to give the User positive feedback that the mode has actually been changed.

4.3 Correlation between the SEFs, and the Product Rationale

The SEFs are required to meet the security objective; the following table is a description of how the assumed threats are countered. It also correlates the SEFs and the intended environment to the assumed threats as defined within the product rationale:

Threats	SEFs	Environment Assumptions	Comments
AT1	SF1, SF2	IE1	Threat AT1: A User or process on the High Side Computer that accidentally or deliberately breaches the confidentiality of some High Side information by transmitting data from a High Side Computer through the IL-MCS to the Low Side Computer. SEF SF1: Data Path Switch Function: To transfer data from the keyboard and mouse to either the High Side Computer (denoted as "High Mode") or the Low Side Computer

Threats	SEFs	Environment Assumptions	Comments
			(denoted as "Low Mode"), according to the mode selected by the User. SEF SF2: Video Path Switch Function: To transfer video from either the High Side Computer (denoted as "High Mode") or the Low Side Computer (denoted as "Low Mode") to the monitor, according to the mode selected by the User. Intended Environment IE1: Classified systems have different environmental requirements, in terms of physical, personnel, media, communications, emanation security and management. These requirements are defined in SECMAN3, ACSI33 or ASSRO Supplement 1. The IL-MCS shall be utilised in an environment that meets these requirements. The information on the High Side Computer cannot be transmitted to the Low Side Computer through the IL-MCS. SF1 ensures that the product has one operational input port, the keyboard and mouse data input, and two operational output ports, the High and Low Side Computers. The SEF counters the threat by preventing data flowing from the High and Low Side Computers into the keyboard and mouse. It ensures that no data can flow from the High Side Computer into the keyboard and mouse when in High Mode and then into the Low Side Computer when in Low Mode. The analogue video data is transmitted from either the High Side Computer or the Low Side Computer into the IL-MCS and out to the monitor. The monitor receives the output from one of the two sources depending on the position of the video switch controlled by SEF SF1. There is no physical path for the video data to flow from the High Side Computer to the Low Side Computer. The operational environment by meeting the requirements of SECMAN3 ACSI33 or the ASSRO Supplement 1, further mitigates this threat.
AT2	SF3	IE8	Threat AT2: A User accidentally types High Side data into the keyboard while the IL-MCS is in the Low Mode and transfers the data to the Low Side Computer. SEF SF3: Indication Function: To indicate the current mode to the User. Intended Environment IE8: All staff who have access to classified Information Systems shall be trained in the

Threats	SEFs	Environment Assumptions	Comments
			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. The operator is made aware of the computer that the keyboard and mouse information is directed to, by SF3, which mitigates this threat. The environmental assumption ensures that the users are trained to operate the IL-MCS correctly and securely, which further mitigates this threat.
AT3	-	IE1	Threat AT3: A User deliberately types High Side data into the keyboard while the IL-MCS is in the Low Mode and therefore puts High Side data directly into the Low Side Computer. Intended Environment IE1: Classified systems have different environmental requirements, in terms of physical, personnel, media, communications, emanation security and management. These requirements are defined in SECMAN3, ACSI33 or ASSRO Supplement 1. The IL-MCS shall be utilised in an environment that meets these requirements. The environmental assumption that ensures that all personnel that have access to the IL-MCS are vetted and cleared to the classification of the High Side Computer. This environmental assumption is intended to mitigate this threat.
AT4	SF1	IE7, IE1	Threat AT4: A rogue keyboard or mouse copies data intended for the High Side Computer, as it is entered, and re-transmits the data to the Low Side Computer when the IL-MCS is in the Low Mode. SEF SF1: Data Path Switch Function: To transfer data from the keyboard and mouse to either the High Side Computer (denoted as “High Mode”) or the Low Side Computer (denoted as “Low Mode”), according to the mode selected by the User. The keyboard and mouse doesn’t know what mode the switch is in. Intended Environment IE7: Equipment hardware and software procurement policies are to be followed to minimise the risk of installing malicious hardware and software in the High or Low Side systems.

Threats	SEFs	Environment Assumptions	Comments
			Intended Environment IE1: Classified systems have different environmental requirements, in terms of physical, personnel, media, communications, emanation security and management. These requirements are defined in SECMAN3, ACSI33 or ASSRO Supplement 1. The Interactive Link VBBS shall be utilised in an environment that meets these requirements. This threat is reduced by SF1, which states that the keyboard and mouse has no knowledge of the mode that the IL-MCS is in. This is achieved by the SF1, by having the keyboard and mouse port as an input only and diode functionality at the outputs to both computers. IE1 helps to prevent the introduction of a rogue keyboard by an unauthorised intruder. The threat is further mitigated by procurement policies and operational practices and procedures, which will reduce the possibility of introducing a rogue keyboard.
AT5	SF2	IE7, IE1	Threat AT5: A rogue monitor that stores High Side display information, and forwards the information to the Low Side Network when the IL-MCS is in the Low Mode. SEF SF2: Video Path Switch Function: To transfer video from either the High Side Computer (denoted as “High Mode”) or the Low Side Computer (denoted as “Low Mode”) to the monitor, according to the mode selected by the User. The monitor never knows the mode of the switch. Intended Environment IE7: Equipment hardware and software procurement policies are to be followed to minimise the risk of installing malicious hardware and software in the High or Low Side systems. Intended Environment IE1: Classified systems have different environmental requirements, in terms of physical, personnel, media, communications, emanation security and management. These requirements are defined in SECMAN3, ACSI33 or ASSRO Supplement 1. The Interactive Link VBBS shall be utilised in an environment that meets these requirements. This threat is reduced by SF2, which states that the monitor has no knowledge of the mode that the IL-MCS is in. IE1 helps to prevent the introduction of a rogue monitor by an unauthorised intruder. The threat is further mitigated by procurement policies and operational practices and

Threats	SEFs	Environment Assumptions	Comments
			procedures, which will reduce the possibility of introducing a rogue monitor.
AT6	-	IE5, IE1, IE8	Threat AT6: The person responsible for the installation of the IL-MCS, installs it accidentally or deliberately to cause High Side information to be transmitted to the Low Side Computer and make the information available to Low Side Users. Intended Environment IE5: The system management staff in accordance with the Administration Documentation shall install the trusted devices of the IL-MCS. Intended Environment IE1: Classified systems have different environmental requirements, in terms of physical, personnel, media, communications, emanation security and management. These requirements are defined in SECMAN3, ACSI33 or ASSRO Supplement 1. The IL-MCS shall be an environment that meets these requirements. Intended Environment IE8: All staff who have access to classified 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. The person who installs the IL-MCS shall be vetted and cleared to the level of classification of the High Side Computer in accordance with IE1. This threat is further mitigated by the training provided by IE8 and the instructions defined in the administration and installation documentation of IE5. The assumption of IE1 also requires the installation to be accredited by the security authority of the High Side system, which involves independent inspection of the installation.
AT7	-	IE3, IE2, IE1	Threat AT7: The IL-MCS emanates radiation that carries discernible classified information that can be reconstructed by a person who is not supposed to have access to the information. This threat is associated with products that bridge the boundary of the two systems; the IL-MCS is such a device. Intended Environment IE3: It is intended that the product operate in an environment where physical (or some other)

Threats	SEFs	Environment Assumptions	Comments
			security measures prevent any TEMPEST attack. Intended Environment IE2: The intended environment will be capable of storing and operating the IL-MCS in accordance with the requirements of the High Side system. Intended Environment IE1: Classified systems have different environmental requirements, in terms of physical, personnel, media, communications, emanation security and management. These requirements are defined in SECMAN3, ACSI33 or ASSRO Supplement 1. The IL-MCS shall be utilised in an environment that meets these requirements. Emanated Radiation carrying discernible information is not a threat when the trusted product are operated so as their ERTZ is within the Secure boundary of the High Side system. The device is also protected by physical and procedural countermeasures that have been selected following a tempest threat and risk assessment for the High Side system in accordance with the High Side security policy and standards.
AT8	-	IE4, IE2, IE1	Threat AT8: An adversary tampers with the contents of the IL-MCS during delivery, and/or after installation to cause the compromise of the confidentiality of classified information handled by the product. Intended Environment IE4: The IL-MCS will be sealed so it is tamper evident. Intended Environment IE2: The intended environment will be capable of storing and operating the IL-MCS in accordance with the requirements of the High Side system. Intended Environment IE1: Classified systems have different environmental requirements, in terms of physical, personnel, media, communications, emanation security and management. These requirements are defined in SECMAN3, ACSI33 or ASSRO Supplement 1. The IL-MCS shall be utilised in an environment that meets these requirements. Tampering with the contents of the IL-MCS in an attempt to compromise the High Side data is mitigated by the use of a tamper evident seal. It is further mitigated by the environmental assumption that it is stored and operated

Threats	SEFs	Environment Assumptions	Comments
			within a physically secure environment that meets the requirements for the High Side system in accordance with the appropriate security policy and standards. Finally there is the assumption that the personnel with access to the device, are cleared to the classification of the High Side system.
AT9	SF1, SF2, SF3.		Threat AT9: A User or process on the Low Side Computer transmits data to the IL-MCS that changes firmware or executables to causes the devices to breach the confidentiality of some High Side information. SEF SF1: Data Path Switch Function: To transfer data from the keyboard and mouse to either the High Side Computer (denoted as "High Mode") or the Low Side Computer (denoted as "Low Mode"), according to the mode selected by the User. SEF SF2: Video Path Switch Function: To transfer video from either the High Side Computer (denoted as "High Mode") or the Low Side Computer (denoted as "Low Mode") to the monitor, according to the mode selected by the User. SEF SF3: Indication Function: To indicate the current mode to the User. Logical attacks that changes firmware or executables within the IL-MCS in an attempt to causes it to breach of the confidentiality of some High Side information is not possible. The design, implementation, production and manufacture of the IL-MCS ensure that the SEFs contain no software or programmable components. SEFs 1, 2 and 3, are implemented in hardware and do not execute any software or firmware and therefore cannot be circumvented by any software threat.

Table 1 Relationship between Security Objectives, Threats, and SEFs.

The following table indicates the relationship between the intended methods of use, as defined within the product rationale, and SEFs:

Method of Use	SEFs	Comments
U1	SF1, SF2, SF3	Method of Use U1: When the High Side button of the IL-MCS is pressed placing it in the High Mode, the User may interact with information and applications located on the High Side Computer. In

Method of Use	SEFs	Comments
		this mode, keyboard and mouse data is passed via the IL-MCS to the User's High Side Computer to interact with applications. While in this mode the video generated from the High Side Computer is passed via the IL-MCS to the monitor. SEF SF1: Data Path Switch Function: To transfer data from the keyboard and mouse to either the High Side Computer (denoted as "High Mode") or the Low Side Computer (denoted as "Low Mode"), according to the mode selected by the User. SEF SF2: Video Path Switch Function: To transfer video from either the High Side Computer (denoted as "High Mode") or the Low Side Computer (denoted as "Low Mode") to the monitor, according to the mode selected by the User. SEF SF3: Indication Function: To indicate the current mode to the User. After pressing the high button and following an audible beep, which signifies that the change of mode, provided by SEF SF1, was successful, the IL-MCS is placed in High Mode. An indication of the mode is provided to the User by the illuminated display positioned above the high button, which is implemented by SF3. In the High Mode, the keyboard and mouse data is passed via the data path switch of SF1 directly to the High Side Computer to interact with applications of the High Side. The High Side Computer's video is displayed on the monitor via the video data switch SF2. Note SF1 stops information being transmitted from the keyboard and mouse to the Low Side Network when in the High Mode. Finally it should be noted that when the IL-MCS is powered up, it is in High Mode.
U2	SF1, SF2, SF3	Method of Use U2: When the Low Side button of the IL-MCS is pressed placing it in the Low Mode, the User may interact with information and applications located on the Low Side Computer. In this mode, keyboard and mouse data is passed via the IL-MCS to the User's Low Side Computer to interact with applications. While in this mode the video generated from the Low Side Computer is passed via the IL-MCS to the monitor. SEF SF1: Data Path Switch Function: To transfer data from the keyboard and mouse to either the High Side Computer (denoted as "High Mode") or the Low Side Computer (denoted as "Low Mode"), according to the mode selected by the User. SEF SF2: Video Path Switch Function: To transfer video from either the High Side Computer (denoted as "High Mode") or the Low Side Computer (denoted as "Low Mode") to the monitor, according to the

Method of Use	SEFs	Comments
		mode selected by the User. SEF SF3: Indication Function: To indicate the current mode to the User. After pressing the low button and following an audible beep, which signifies that the change of mode, provided by SEF SF1, was successful, the IL-MCS is placed in Low Mode. An indication of the mode is provided to the User by the illuminated display positioned above the low button, which is implemented by SF3. In the Low Mode, the keyboard and mouse data is passed to the Low Side Computer to interact with applications on the Low Side. The Low Side Computer's video is displayed on the monitor via the video switch function, SF2. The User is able to change between Low and High Modes as required by pressing the buttons on the front panel of the IL-MCS.

Table 2 Relationship between the Method of Use and SEFs.

5 Definition of Required Security Mechanisms

5.1 Introduction

This section identifies the mechanisms provided by the IL-MCS to implement the Security Enforcing Functions. Definition of these mechanisms shall be dynamic and shall be updated throughout the design phase.

5.2 Security Mechanisms

The IL-MCS uses the following Security Enforcing Mechanisms (SEMs) to implement the SEFs.

SM1. **Data Path Switch Mechanism**: The Data Path Switch switches the output from the keyboard and mouse to either the High Side Computer (High Mode), or the Low Side Computer (Low Mode). It also prevents data being transmitted from the High Side Computer keyboard or mouse ports to the keyboard and mouse. This is achieved by the unidirectional nature of the Data Path Switch, which all keyboard and mouse data must pass through. This feature is turn prevents data being transmitted to the Low Side Computer. The mechanism is implemented in hardware within the IL-MCS.

SM2. **Video Switch Mechanism**: The Video Switch switches the video output of the High Side Computer (High Mode), or the video output of the Low Side Computer (Low Mode) to a common monitor. The mechanism is implemented in hardware within the IL-MCS.

SM3. **Visual Indicator Mechanism**: The Visual Indicator provides an indication to the User of the current mode the IL-MCS is in. It will consist of labels in 12 point size capital letters to indicate the current classification of the connected network/computer system. The label will be illuminated and clearly visible and easily read by the operator at a normal working distance from the display. It will be colour coded ie. a distinctly different colour indication for the two labels. The label text shall be provided against a contrasting background. The indicator shall be implemented in hardware.

SM4. **Reinforcing Indicator Mechanism**: The reinforcing indicator provides confirmation that a mode change within the IL-MCS has occurred. It consists of a short duration audible indication to the User and will be implemented using a piezoelectric transducer.

5.3 Correlation between SEMs and SEFs

The following table indicates which Security Enforcing Mechanisms are used to implement the Security Enforcing Functions:

SEFs	SEMs	Comments
SF1	SM1	The Data Path Switch Mechanism provides the functionality of switching the output from the keyboard and mouse to either the High Side Computer (High Mode), or the Low Side Computer (Low Mode), as required by SF1.
SF2	SM2	The Video Switch Mechanism provides the functionality of switching the video output of either the High or Low Side Computer to a common monitor dependant upon the mode of the IL-MCS, as required by SF2.
SF3	SM3, SM4	The Visual Indicator Mechanism provides an indication to the User of the current mode that the IL-MCS is in. The reinforcing indicator mechanism provides confirmation that a mode change has occurred. These mechanisms provide an indication to the User of the current mode of the IL-MCS, as required by SF3.

Table 3 Relationship between SEFs and SEMs

6 Minimum Strength of Mechanisms

The IL-MCS utilises *type B mechanisms*. These mechanisms, if perfectly conceived and implemented, are considered to be impregnable to direct attack regardless of the level of resources, expertise and opportunity deployed and have no minimum strength of mechanism (SoM) rating.

7 Target Evaluation Level

The IL-MCS will be evaluated to an assurance level of E6 in accordance with the Information Technology Security Evaluation Criteria (ITSEC), Version 1.2, dated 28 June 1991 and the Defence Signals Directorate (DSD), Australian Information Security Evaluation Programme.