Compucat Research Pty Limited
14 Wales St,
Belconnen ACT 2617
ABN 48 008 602 980

Secure Optical Switch
Version-01

Security Target

P/N 2066-0012-05

Table of Contents

List of Tables

1. Introduction

1.1 *Security Target Identification*

This document is the SECURITY TARGET (ST) for the Secure Optical Switch (SOS) developed by Compucat Research Pty Ltd, which is the Target of Evaluation (TOE) for the Common Criteria[i] (CC) evaluation that this Security Target is intended to support.

The relevant identification details for the ST and its associated TOE are as follows:

TOE	Compucat Secure Optical Switch local and remote variants with part numbers 1105-0062-04 (Secure Optical Switch with factory fitted local operation option) and 1105-0067-04 (Secure Optical Switch with factory fitted Remote Operation option)
ST title	Secure Optical Switch Version-01
CC Evaluation Assurance Level	Common Criteria level EAL 7
CC evaluators	CSC Australia
CC Certifiers	AISEP

1.2 *Security Target Overview*

1.2.1 Subject matter of the Security Target

This Security Target refers to the Compucat Secure Optical Switch, which is a hardware based, tamper evident physical switching device which provides for a common I/O port to be switched to any one of up to four selectable I/O ports while maintaining absolute isolation between the selectable ports within the body of the switch. Fibre Optical status and visual feedback (confirmation) of the current switch position to the user is also provided. Visual confirmation of port connection is provided to the user by the identity of the IO Port connected being indicated by the steady illumination of a light output on the switch case that unequivocally corresponds to the port currently connected by the switch. Optical feedback in the form of a 'port connected' signal on an optical connector output on the switch case is also provided to allow for remote feedback of switch status (for use by suitably accredited systems that can preserve the validity of the status output beyond the physical boundary of the TOE).. The trusted I/O port connection, tamper evidence and optical and visual feedbacks are certified to CC Assurance level (EAL) 7.

1.2.2 Document content and objectives

This Security Target is produced in accordance with the content requirements set out in Annex A of the Common Criteria Part 1. It provides the set of security requirements and a High Level Summary Specification for use in the evaluation of the TOE.

The objectives of this document are to:

[i] Common Criteria Version 2.2.

- unequivocally identify and describe the TOE;
- describe the security aspects of the environment in which it is intended to operate the TOE covering all relevant threats to assets protected by the TOE and assumptions relating to the secure operation of the TOE.
- specify the Security Objectives for the TOE and its environment;
- clearly enunciate the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) for the TOE that are needed for it to meet the stated TOE Security Objectives;
- provide a high level Summary Specification of the TOE which outlines the specific instantiation of the TOE security functions and a statement of assurance measures and maps them to the security requirements that they satisfy;
- provide a rationale that presents evidence that supports the claims that the ST is a complete and cohesive set of requirements, that a conformant TOE would provide an effective set of IT security countermeasures within the security environment, and that the TOE summary specification addresses the requirements.

1.2.3 Intended Audience

The intended audience for this security target includes personnel of the developer, evaluator/certifier and potential consumers.

1.2.4 Definitions

Compucat	Compucat Research Pty Limited (ABN 48 -008 602 980)
Secure Optical Switch	The product name used for the switching device developed by Compucat
CC	Common Criteria
TOE	Target of Evaluation - the Secure Optical Switch, (also referred to in this document as ‘the switch’ or as ‘the SOS')

1.3 *Common Criteria Conformance Claim*

1.3.1 CC Conformance

With respect to the Common Criteria version 2.2 dated January 2004, the TOE is:

Part 2 conformant;Part 3 conformant; and EAL 7 conformant.

1.3.2 Protection Profile claim (ASE_PPC)

This ST, and the TOE that is its subject, is not based upon any known Protection Profile.

2. TOE Description

2.1 *System type*

The Secure Optical Switch is a hardware-based switching device, which can provide a selectable common connection to otherwise separate systems. As a general-purpose switching device, the SOS could be used wherever a manually operated multi-pole - multi-throw secure switch is required to reliably control the flow of digitised optical data through a system.

2.2 *Switch functionality*

The Secure Optical Switch is designed to connect the common I/O port with any one of four selectable I/O ports by the physical alignment of fibre optic pathways through the switch. Once connected, the switch will pass digital optical signals between the two ports, with the directionality of the signals being dictated by the nature of the external connecting devices. This enables the switch to be employed with a high degree of flexibility regarding the direction of data flow. To prevent the switch from compromising the separation between networks connected to the selectable ports, direct interconnection of the selectable ports through the switch is prevented at all times.

2.3 *Physical Scope*

The SOS is physically encompassed within a tamper evident enclosure which has an array of 25 optical fibre interfaces to external systems arranged as five ports of five fibre interfaces each. The ports are arranged as one ‘Common Port’ and four Selectable Ports. The Common Port interface can be connected to any one of the other Selectable Ports at any given time with the user selecting which of the Selectable Ports is to be connected via a selector input on the front panel of the switch. The SOS also provides two sets of feedback signals. One provides fibre optic status outputs indicating which port is selected, and the other is a set of illuminated front panel indicators by which the user can visually confirm the identify of the Selectable Port currently connected to the Common Port.

2.4 *Logical Scope*

The SOS operates logically as a trusted switching device that connects a Common Port (X) to any one of four Selectable Ports (A,B,C,D). The nature of the switch is such that Common Port X can be connected to one and only one of the Selectable Ports at any time.

2.4.1 Security Functionality

Under normal operating conditions, the TOE can reliably connect the Common Port to any one of up to four Selectable Ports chosen and accurately indicate which Selectable Port is connected to it. The nature of the switch design offers the following claimable security functionality.

- The Common Port can be connected to no more than one of the Selectable Ports at any one time.
- The Selectable Ports can never be connected to each other via the switch.

- When the indicator light on the front of the switch corresponding to a specific port is illuminated, it unequivocally confirms that the Common Port is connected to that specific Selectable Port.

- When the fibre optic status output of the switch corresponding to a specific port is illuminated, it unequivocally confirms that the Common Port is connected to that specific Selectable Port.

When a new port is selected the light associated with the previously selected port will go off and no lights will be lit for a brief period corresponding to the disconnected state between ports. If the port selected requires the switch to traverse intervening ports, the lights corresponding to those ports will flash briefly as the switch transits past them. Once the switch has connected the common port to the selected port the indicator light and fibre optic status output corresponding to the selected port will be steadily illuminated, indicating that the Common Port is definitely connected to the selected port.

2.5 *Switch applicability*

The Secure Optical Switch is intended to meet the requirement for reliably connecting otherwise separated systems to a common I/O port. This has applicability in circumstances where a user has the need to access a number of networks that, due to their content, cannot be linked together. An example of such a requirement could be the need for operational personnel in a coalition environment to access information from a classified coalition LAN, an eyes only national LAN and possibly from other restricted or unclassified sources such as the Internet. The Secure Optical Switch could allow a suitable interface to be switched between all of these networks without risk of compromise of any of them by direct interconnection since they would never be directly interconnected via the switch. The switch could also have application in switching digitised optical voice or data streams that need to be reliably switched with high confidence as to destination and /or source.

2.6 *Diagram of the Secure Optical Switch.*

Figure 1 is a block diagram of the switch showing the relationships of the ports and switch function. The external box defines the physical and logical boundary of the switch.
Application Note: Figure 1 does not show the user input to select which port will be connected to the Common Port as it is a usability feature not a security enforcing feature. The security critical aspects of the switch are its ability to maintain the isolation of Selectable Ports A through D from each other (and from the Common Port X when not selected to be connected to it) within the boundaries of the switch and to reliably indicate which of the Selectable Ports is connected to Common Port X.

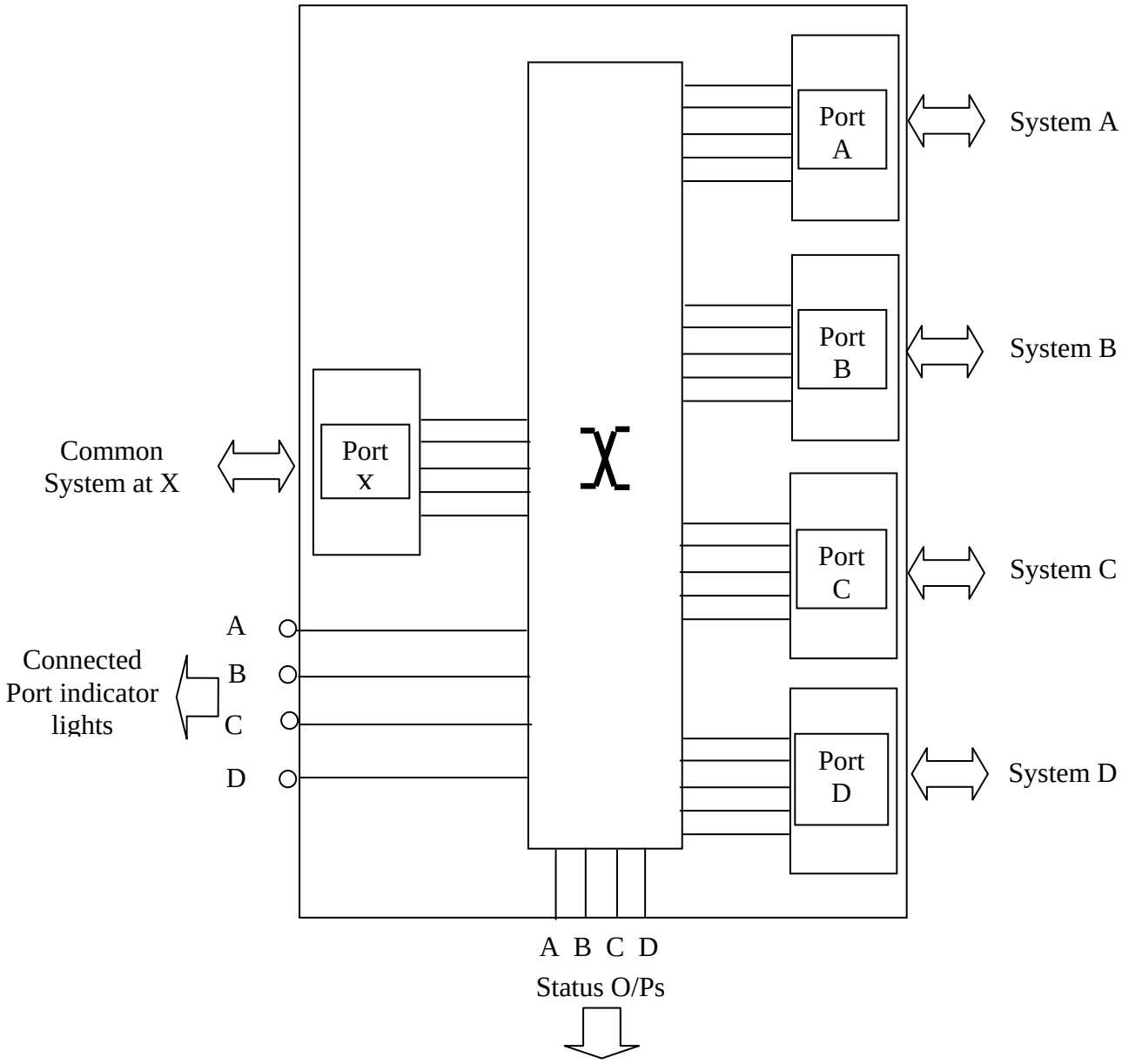

Figure 1 - Conceptual diagram of the Secure Optical Switch

3. The TOE Security Environment

This section describes the security aspects of the environment in which the TOE is intended to be used and the manner in which it is expected to be employed.

3.1 *Impact of the Security Environment*

The security aspects of the environment in which the TOE will be used includes the threats to the assets that the switch will be used to protect and those security features of the environment which the TOE is assumed to operate within.
The perceived threats and assumed security related aspects of the TOE Security Environment are addressed in this section of the ST.

3.2 *Threats*

A number of threats that the users might employ the TOE to counter have been identified.

The identified threats to a system of this type are listed in Table 3.2-1 below. The likely sensitivity of the information that an EAL 7 device would be installed to protect would potentially attract well resourced, highly motivated experts. In view of this, the skill levels of the attacker are assumed to be HIGH for all instances. It is also assumed that in each case the asset under threat is the information on the highest grade of system connected to the switch.

Threat designation	Threat
T_PHYSICAL	**The TOE may be physically tampered with in such a way as to compromise its internal security functionality without this being readily apparent to the users or administrators**. (**Threat agent:** Person with physical access to the TOE. **Attack methods**: internally modifying the TOE to compromise its security performance without leaving traces of the tampering that are evident to users or administrators of the TOE. **Vulnerabilities:** Imperfect physical security of TOE environment, any aspect in the TOE physical casing that might permit undetectable tampering. **Opportunity:** Depends upon the TOE physical security environment.)
T_NETWORK-CONNECT	**The TOE might be used as a direct uncontrolled connection point between otherwise separate domains.** **(Threat Agent:** External attacker who compromises a system that is connected to one of the Ports of the TOE. **Attack methods**: Exploiting a weakness in TOE design to permit the direct interconnection of one or more selectable ports. **Vulnerabilities:** Any weakness in the TOE internal design permitting direct connection between selectable ports. **Opportunity**: Critically depends upon attacker's access to the TOE.)
T_SPOOF	The common port of the TOE may be connected to a domain other than the one that the user believes it to be connected. **(Threat Agent:** External attacker who compromises a system that is connected to one of the Ports of the TOE. **Attack methods**: An external attacker that has compromised one of the attached systems and claims it to be at a higher access level. **Vulnerabilities:** A failure of TOE Port connection indication. **Opportunity:** Depends upon TOE functionality, user training and the physical security environment.)

Table 3.2 - 1 - Security Threats

3.3 *Assumptions*

It is not generally possible, or desirable, to counter all of the threats identified above within the security functionality of the TOE alone. The physical, procedural and personnel security features of the environment within which the TOE is expected to operate can often adequately and cost-effectively counter some of those threats.

In view of this, the Security Target makes certain assumptions about the Security Environment within which the TOE must be operated. The assumptions regarding the Security Environment required for the TOE to operate securely are listed in Table 3.3- 1.

Designation	Assumption	Comment
A_PHYSICAL	The TOE is physically secure.	The TOE should be in a physically secure environment that at least corresponds to the level of protection of the highest security level data accessible through it.
A_INSTALLATION	Only a properly trained and authorised technician shall be used to install the TOE.	The cabling connections of the TOE are complex and security critical. Installation and testing of the TOE should be restricted to suitably trained and cleared personnel.
A_MANAGEMENT	Only properly trained and authorised personnel shall be permitted to administer, modify or physically reconfigure the TOE installation.	System administrators are assumed to be cleared and suitably trained to check the operational status of the switch. Where cabling configurations are to be changed this should be undertaken by a suitably trained, cleared and authorised technician.
A_TRAINING	All personnel, including users, are to be properly trained for their respective roles.	In addition to installer and administrator training, users must be trained in the secure use of the switch and to recognise indications of switch failure or improper operation.
A_TRUSTED	All personnel with access to the switch's environment are to be appropriately cleared and security aware.	All such personnel should be cleared to at least the highest level of data that they are capable of accessing within the switch's environment.

Table 3.3 - 1 - Assumptions re the TOE Security Environment

4. Security Objectives

This section of the ST defines the Security Objectives for the TOE and its expected environment. The Security Objectives reflect the intent to counter all of the threats and cover the assumptions identified in the TOE Security Environment (section 3).

4.1 *TOE Security Objectives*

The security objectives of the TOE are addressed in Table 4.1-1 below.

DESIGNATION	OBJECTIVE
O_ISOLATE	The TOE, whilst acting as an optical switch, precludes the possibility of direct connection between the selectable ports within the boundary of the switch.
O_INDICATE	The TOE provides illuminated front panel indication and a fibre optic status output of which selectable port is currently connected to the common port within the switch.
O_TAMPER	The TOE enclosure is designed to be Tamper evident thereby revealing any successful attempt to interfere with the internal functionality of the switch.

Table 4.1 - 1 - TOE Security Objectives

4.2 *Environmental Security Objectives*

The supporting security objectives to be provided by the TOE's environment are addressed in Table 4.2-1.

DESIGNATION	OBJECTIVE
OE_PHYSICAL	The TOE operating environment is to be physically secured to at least the level of protection required for the highest security level system accessible through it.
OE_INSTALLATION	All TOE installation work is to be undertaken by properly trained and authorised technical personnel.
OE_MANAGEMENT	Only properly trained and authorised personnel are to be permitted to administer TOE operation or have access to modify or physically reconfigure the TOE installation.
OE_PERSONNEL	TOE user, maintenance and administration personnel are to be appropriately cleared and properly trained in the operation, maintenance and security aspects of the switch.

Table 4.2 - 1 - Environmental Security Objectives

5. IT Security Requirements

This section lists the specific security requirements satisfied by the TOE and its environment in accordance with the applicable SFRs and SARs as prescribed in Parts 2 and 3 of the CC.
SFRs describe the requirements for security functionality provided by the TOE, while the SARs describe the assurance that the TOE will consistently meet its security objectives

5.1 *TOE Security Functional Requirements (SFRs)*

The SFRs, drawn from CC Part 2 that are met by the TOE are listed in Table 5.1-1 below.

Function Designation	Title
FDP_IFC.1	Subset information flow control
FDP_IFF.1	Simple security attributes
FMT_MSA.1	Management of security attributes
FMT_SMF.1	Specification of management functions
FPT_PHP.1	Passive detection of physical attack

Table 5.1 - 1 - TOE Security Functional Requirements

5.1.1 FDP_IFC.1 Subset information flow control

FDP_IFC 1.1 **The TSF shall enforce the** [**assignment:** *SINGLE CONNECTION POLICY*] **on** [**assignment**: *Subjects: Ports A,B,C,D, and X.*
Information: The data at the ports
Operations: Allowed Connection].

5.1.2 FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 **The TSF shall enforce the** [**assignment:** *SINGLE CONNECTION POLICY*] **based on the following types of subject and information security attributes: [assignment:**
Subjects: Port A, Port B , Port C, Port D, Port X.
Information: Information at Ports A, B, C, D & X
Attribute Name: Connected Port].

FDP_IFF.1.2 **The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment:** *For the operation 'Allowed Connection' the TSF shall have established a connection between Common Port X and a Selectable Port given by Connected Port.*

The attribute Connected Port determines the operation Allowed Connection such that the permitted states are as listed in the table below:

Value of Connected Port	*State of Allowed Connection*
None	*Port X not connected*
A	*Port X connected only to Port A*
B	*Port X connected only to Port B*
C	*Port X connected only to Port C*
D	*Port X connected only to Port D*

*When the user changes the attribute by selecting a different port this causes the switch to change states accordingly***].**

FDP_IFF.1.3 **The TSF shall enforce the [assignment:** *NONE*].

FDP_IFF.1.4 **The TSF shall provide the following [assignment:** *A Clear and unambiguous visual indication either directly on the front panel of the switch or via a fibre optic status output of the Connected Port attribute value*].

FDP_IFF.1.5 **The TSF shall explicitly authorise an information flow based on the following rules: [assignment:** *NONE*].

FDP_IFF.1.6 **The TSF shall explicitly deny an information flow based on the following rules: [assignment:** *Selectable Ports A, B, C and D shall not directly connect to each other at any time(regardless of the value of the connected port attribute)*].

5.1.3 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 **The TSF shall enforce the** [**assignment**: *SINGLE CONNECTION POLICY*] **to restrict the ability to [selection: [assignment:** *select***]] the security attributes [assignment:** *Connected Port (A, B, C, D)***] to [assignment:** *User***].**

5.1.4 FMT_SMF.1 Specification of management functions

FMT_SMF.1.1 **The TSF shall be capable of performing the following security management functions:** [**assignment**: *Change Connected Port*].

5.1.5 FPT_PHP.1 Passive detection of physical attack

FPT_PHP.1.1 **The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.**

FPT_PHP.1.2 **The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or the TSF's elements has occurred.**

5.2 *Security Assurance Requirements (SARs)*

The documents, processes, and activities that support the TOE meet the Security Assurance Requirements (SARs) as specified in the CC Part 3 by Class, Family and Component level for the EAL 7 level of assurance. For reader convenience the list of SARs for EAL 7 is provided in Table 5.2 below. For detailed descriptions of the class, family and specific component requirements, refer to CC Part 3.

Assurance class	Assurance Family	Component (corresponding to Evaluation Assurance Level 7)
Configuration Management	ACM_AUT	2
	ACM_CAP	5
	ACM_SCP	3
Delivery and operation	ADO_DEL	3
	ADO_IGS	1
Development	ADV_FSP	4
	ADV_HLD	5
	ADV_IMP	3
	ADV_INT	3
	ADV_LLD	2
	ADV_RCR	3
	ADV_SPM	3
Guidance documents	AGD_ADM	1
	AGD_USR	1
Life cycle support	ALC_DVS	2
	ALC_LCD	3
	ALC_TAT	3
Tests	ATE_COV	3
	ATE_DPT	3
	ATE_FUN	2
	ATE_IND	3
Vulnerability Assessment	AVA_CCA	2
	AVA_MSU	3
	AVA_SOF	1
	AVA_VLA	4

Table 5.2 - 1 - Assurances by Class, Family, and Component to meet EAL 7

6. TOE Summary Specification

This section defines the instantiation of the security requirements for the TOE and describes the assurance measures and security functions of the TOE that meet the TOE security requirements.

6.1 *Statement of TOE Security Functions*

6.1.1 TSF to SFR Mappings

The TSF implemented within the TOE and their mappings to the TOE Security Functional Requirements are listed in table 6.1.1-1 below.

TSF ID	SFR's addressed
Opto-mechanical Switch	FDP_IFC.1 FDP_IFF.1 FMT_MSA.1 FMT_SMF.1
Switch Position Visual Indication	FDP_IFC.1 FDP_IFF.1
Switch Position Status Output	FDP_IFC.1 FDP_IFF.1
Tamper Evident Case	FPT_PHP.1

Table 6.1.1-1 - TSF to SFR Mappings

6.1.2 Informal Definition of the TSF

a. The Opto-mechanical Switch

The Opto-mechanical Switch is an electromechanically operated optical switch, which functions to selectively connect groups of optical fibres. For convenience each group of optical fibres is termed a 'Port'. The Opto-mechanical Switch is designed to ensure that just one selectable group of optical fibres is connected to the corresponding fibres of the Common Port at any one time. The physical arrangement of the Opto-mechanical Switch is such that only the fibres of one port can be connected to the common port and that all other groups of fibres are blanked off. Thus, if the internal configuration of the switch has not been compromised, the following will hold true:

(i) The physical arrangement of the fibres of the Selectable Ports within the switch precludes all possibility of the interconnection of any Selectable Port to any other Selectable Port either by accidental or intentional means.

(ii) The Common Port can be connected only to one Selectable Port at a time.

b. Switch Position Visual Indication

Within the boundaries of the TOE an LED light source is used to provide a light signal on an optical fibre that connects to part of the Common Port's group of optical fibres. When a Selectable Port is connected the signal is passed through the Opto-mechanical Switch to an optical fibre that

corresponds to the connected Port. This fibre is then directly connected to illuminate the telltale visual indicator on the switch casing that corresponds to the connected port. Thus, if the internal configuration of the switch has not been compromised, when a port connection indicator is illuminated, the user can be confident that the Common Port is connected to that Selectable Port and to no other port.

c. Switch Position Status Output

Whereas the Switch Position Visual Indication function provides a visual indication of switch position directly to the user, the Switch Position Status Output provides an equivalent optical output to a set of optical connectors on the case of the switch. As with the Switch Position Visual Indication, the Switch Position Status Output illuminates one optical output corresponding to the specific Selectable Port connected to the Common Port at that time. As with the Switch Position Visual Indication previously described, if the internal configuration of the switch has not been compromised, when a Switch Position Status optical output is illuminated, the Common Port will be connected to the corresponding Selectable Port and to no other port.

d. Tamper Evident Case

The veracity of the three foregoing TOE Security Functions is reliant upon the correct working of the switch. Hence it is important that the users can be confident that the internal functionality of the switch has not been compromised. To this end, the security functionality of the TOE is contained within the confines of the physical casing of the switch and the case of the switch is constructed so as to provide clear and unambiguous evidence of any tampering that might result in the compromise of TOE Security functionality.

6.1.3 Strength of Function

In the case of this TOE, no security functionality is realised by the use of probabilistic or permutational mechanisms, therefore no Strength of Function claims are made for any IT security functions.

6.2 *Statement of Assurance Measures*

This section outlines how the assurance measures applied to the TOE relate to the stated assurance requirements corresponding to the EAL 7 level of assurance as specified in Part 3 of the CC and outlined in section 5.2 of this ST.

6.2.1 Mapping of Security assurance measures to SARs

Table 6.2.1-1 provides a description of the assurance measures specified to be implemented and traces them to the stated assurance requirements that they fulfil. A more detailed description and discussion of the suitability of the proposed measures is provided in the TOE Summary Specification Rationale.

Assurance class	Assurance Family and EAL 7 Component	Assurance Measures
Configuration management	ACM_AUT.2	Compucat will apply its established automated Configuration Management (CM) system that controls the design, modification, documentation, manufacture, testing, installation and management of the TOE.
	ACM_CAP.5	The Compucat CM system uniquely identifies the TOE and all of its configuration items and ensures that no unauthorised changes can be made to the TOE.
	ACM_SCP.3	The CM system shall record all changes to the TOE as well as any security flaws discovered and steps taken to eliminate them. As the TOE contains no security related software, no software development tools are relevant. All test and measurement tools used to develop, test and manufacture the TOE will be kept in calibration in accordance to Compucat standard operational processes.
Delivery and operation	ADO_DEL.3	TOE delivery shall be undertaken in accordance with Compucat's documented procedures for the 'safe hands' delivery of classified material.
	ADO_IGS.1	TOE Installation and Operation are covered in the SOS User and Administrators Guide, which covers the expected environment, secure installation, testing, set to work, operating procedures and administration of the TOE.
Development	ADV_FSP.4	The TOE requirements are expressed in a functional specification that applies formal methods to unambiguously describe the TOE.
	ADV_HLD.5	The High Level Design provides a formal representation of the TOE at the sub system level, addressing all sub system interfaces and TSP enforcing subsystems.
	ADV_IMP.3	A complete Technical Data Pack fully describing the TOE to the level of detail required to implement the design is held as part of the Configuration Management system
	ADV_INT.3	The design of the TOE deliberately minimises complexity by eliminating all components from the switch other than those essential to its operation.
	ADV_LLD.2	The Low Level Design documentation provides a semiformal description of the purpose of each module within the switch that contributes to the TSF and describes its interfaces, dependencies and mode(s) of operation
	ADV_RCR.3	A Correspondence Demonstration is formally documented to establish that, for each TSF, the relevant security functionality can be traced from the high levels of abstraction in the ST down to the physical instantiation of the device.
	ADV_SPM.3	A formal TSP model addressing the information flow control policy is provided and the correct correspondence between that model and the formal functional specification is established.
Guidance documents	AGD_ADM.1 AGD_USR.1	The SOS User and Administration Guide provides full instructions on the installation, set to work and use of the TOE including those elements of security that are to be provided by its environment. The Guide provides full instructions to both administrators and users regarding the security relevant processes and procedures required to operate the TOE

		securely.
Life cycle support	ALC_DVS.2	The development and support environment for the TOE is fundamentally the same as that used for other Compucat high grade trusted products. The relevant security processes are documented and the adequacy of the security measures to protect and maintain the confidentiality and integrity of the TOE can be demonstrated if required.
	ALC_LCD.3	A suitable life cycle model will be adapted to provide useful outputs in the context of a low complexity hardware based product.
	ALC_TAT.3	The engineering tools used to develop the TOE and any implementation-dependant options used will be clearly identified and documented as part of the SOS implementation documents.
Tests	ATE_COV.3	TOE acceptance testing is systematic and comprehensive in nature, covering all aspects of the Functional specification confirming full correspondence between the TOE Security Functions stated in the FSP and those implemented in the finished product.
	ATE_DPT.3	Tests will confirm the correct operation of all TSF and validate the instantiation of both the high and low level designs.
	ATE_FUN.2	The test plan, test procedures and test results will be provided for analysis
	ATE_IND.3	A fully functional TOE will be provided to the evaluator for confirming the validity of in house developer tests.
Vulnerability assessment	AVA_CCA.2	Searching for possible covert channels within the TOE has established that the design of the TOE effectively precludes the possibility of covert channels between the Selectable Ports in a properly constructed TOE.
	AVA_MSU.3	An analysis of the SOS User and Administrators Guide confirming its validity will be made available for evaluation
	AVA_SOF.1	None of the security mechanisms used in the TOE needs to be the subject of a SOF claim.
	AVA_VLA.4	A vulnerability analysis will be performed and the documentation will be provided establishing that any security vulnerabilities found cannot be exploited in the intended environment for the TOE. A TOE will also be provided for independent penetration testing by the evaluators.

Table 6.2.1-1 Mapping of Security measures to SARs

7. Rationale

7.1 *Security Objectives Rationale*

This section correlates the stated security objectives to the identified aspects of the security environment and demonstrates that they are suitable to cover them.

7.1.1 Security Threats

Table 7.1.1 -1 below addresses the correlation between the identified Threats and their countervailing Security Objectives.

Threat designation	Countervailing Objectives
T_PHYSICAL	**O_TAMPER & OE_PHYSICAL.** The tamper evident design of the TOE together with the expected security level of its environment effectively removes the threat T_PHYSICAL.
T_NETWORK-CONNECT	**O_ISOLATE** The design of the TOE precludes the possibility of direct connection between the selectable ports. This removes the threat T_NETWORK-CONNECT
T_SPOOF	**O_INDICATE &OE_PERSONNEL** The provision of reliable external indication, including an illuminated front panel indication, of which selectable port is currently connected to the common port, coupled with the use of properly trained and cleared personnel, removes the threat T_SPOOF.

Table 7.1.1-1 - Security Threats Vs Countervailing Security Objectives

7.1.2 Security Assumptions

Table 7.1.2 -1 below addresses the correlation between the identified Security Assumptions and their corresponding Security Objectives

Designation	Required Objectives
A_PHYSICAL	**OE_PHYSICAL** The TOE operating environment is to be physically secured to at least the level of protection required for the highest security level system accessible through it. This meets the requirement A_PHYSICAL
A_INSTALLATION	**OE_INSTALLATION** All TOE installation work is to be undertaken by properly trained and authorised technical personnel. This meets the requirement A_INSTALLATION.
A_MANAGEMENT	**OE_MANAGEMENT** Only properly trained and authorised personnel are to be permitted to administer TOE operation or access to modify or physically reconfigure the TOE installation. AND **OE_INSTALLATION** All TOE installation work is to be undertaken by properly trained and authorised technical personnel. Together these two objectives meet the requirement A_MANAGEMENT
A_TRAINING	**OE_PERSONNEL** TOE user, maintenance and administration personnel are to be appropriately cleared and properly trained in the operation, maintenance and security aspects of the switch. **OE_INSTALLATION** All TOE installation work is to be undertaken by properly trained and authorised technical personnel. Together these two objectives meet the requirement A_TRAINING
A_TRUSTED	**OE_PERSONNEL** TOE user, maintenance and administration personnel are to be appropriately cleared and properly trained in the operation, maintenance and security aspects of the switch. This meets the requirement A_TRUSTED.

Table 7.1.2-1 Correlation of TOE Security Environment Assumptions to Security Objectives

7.2 *Security Requirements Rationale*

This section demonstrates that the set of security requirements (TOE and Environment) is suitable to meet and traceable to the security objectives.

7.2.1 Consistency of the security requirements

The set of IT security requirements specified within this ST derive from the TOE security functionality enumerated at paragraph 2.4.1. The requirement for connecting only one selectable port to the common port does not conflict with the requirement for preventing the interconnection of selectable ports nor do those requirements conflict in any way with the requirement for the provision of fibre-optical and visual feedback signals to confirm which port is connected to the common port. The requirements aimed at preventing covert physical compromise of the TOE are addressed by a combination of the TOE security requirement for passive detection of tampering, and environmental security assumptions covering physical, personnel and procedural aspects of the TOE environment. These requirements are mutually supportive and none conflicting.

Therefore the set of TOE IT security requirements together forms a mutually supportive and internally consistent whole.

7.2.2 Functional and Environmental Requirements

This subsection demonstrates that the stated functional and assurance requirements meet the required security objectives.

DESIGNATION	Security Requirements
O_ISOLATE	**FDP_IFC.1** **FDP_IFF.1** **FMT_MSA.1** **FMT_SMF.1** FDP_IFF.1 **(**called out by FDP_IFC.1**)** contains the major requirement that the Selectable Ports A, B, C, and D shall not directly connect to each other. The functionality described by FDP_IFC.1, FDP_IFF.1, FMT_MSA.1, and FMT_SMF.1 concerns the connection of any single Selectable Port to the Common Port, as selected by the user.
O_INDICATE	**FDP_IFF.1** FDP_IFF.1 contains a requirement for 'Clear visual indication and a fibre optic status output of the Connected Port attribute value' this meets the objective O_INDICATE.
O_TAMPER	**FPT_PHP.1** FPT_PHP.1 contains the requirement that '*The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF'* and *' The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or the TSF's elements has occurred'* This SFR describes the characteristics required to meet the objective O_TAMPER.

Table 7.2.1-1 Correlation security objectives to functional and environmental requirements

7.2.3 Assurance Requirements

It was decided that the TOE would be evaluated to CC assurance level EAL 7 as this level will maximise its applicability as a component in trusted secure systems and the essential simplicity of the TOE makes an evaluation at that level practical.

7.2.4 Dependencies Not Met

FMT_MSA.3 **Static attribute initialisation**

Justification: *The TOE simply switches data, it does not create objects or information hence this function is not applicable.*

FMT_SMR.1 **Security roles**

Justification: *As the TOE is a very simple hardware device that is not designed to have the capacity to discriminate between users, there is only one role assigned to all users. As there is only one user type, this function is not required.*

7.2.5 Internally consistent and mutually supportive SFRs

The SFRs FDP_IFC.1, FDP_IFF.1, FMT_MSA.1 and FMT_SMF.1 describe a simple switch with one common I/O port and four selectable ports. There is a single

security attribute “Connected Port” that is central to FDP_IFC.1 and FDP_IFF.1 and is simply described in FMT_SMF.1 and FMT_MSA.1.
FPT_PHP.1 simply acts as a shielding requirement to support the other SFRs.

Hence, the Security enforcing functions within the TOE work together to provide the security functionality but the operation, of any one function does not result in a weakening of the security enforcing nature of any other.

7.3 *TOE Summary Specification Rationale*

7.3.1 Adequacy of IT security Functionality

FDP_IFC.1 Subset information flow control

The policy stated in FDP_IFC.1 and expanded upon in FDP_IFF.1 is implemented by the security functions Opto-mechanical Switch, Switch position Visual Indication and Switch position Status Output as described under FDP_IFF.1 below. It covers the connection of the Common Port to a single Selectable Port at a time and the prevention of the interconnection of the Selectable Ports and the provision of direct visual feed back to the user as well as the provision for fibre optically remoting the feed back in those systems that can make use of that feature and satisfactorily guarantee the veracity of the remote outputs once they are reticulated outside of the boundary of the TOE.

Note: The veracity of the Switch position Status Output is not enforced by the TOE once it leaves the physical boundary of the device.

FDP_IFF.1 Simple security attributes

FDP_IFF.1.1
This is implemented by the use of the Opto-Mechanical Switch, which mechanically connects the optical pathways associated with connecting the Common Port to the user-selected Selectable Port while physically blocking the passage of all optical signals other than those associated with the selected port, its associated visual indicator and switch status outputs.

FDP_IFF.1.2
This is implemented by the use of the Opto-Mechanical Switch under control of the user. The user sets the switch to connect the chosen Selectable Port to the Common Port by operating the switch selection input on the switch enclosure.

FDP_IFF.1.4
This is implemented by the use of a signal path through the Opto-Mechanical Switch in combination with passive optical connections from the switch to the switch case and light sources internal to the switch enclosure to illuminate the Switch position Visual Indication and Switch position Status Output associated with the selected port.

FDP_IFF.1.6
This is implemented by the Opto Mechanical switch mechanically blocking the passage of all optical signals other than those associated with connecting the selected port to the Common Port. This blocking mechanism is arranged such that the switch passes through a

disconnected stage between each selected port. This disconnected (null) state precludes cross connection between Selectable Ports.

FMT_MSA.1 management of security attributes

FMT_MSA.1.1
The fundamental nature of the Opto-Mechanical Switch in the TOE limits the user selectable connection attributes of the TOE to those provided during manufacture (A, B, C, D).

FMT_SMF.1 Specification of management functions

FMT_SMF.1.1
The TSF is capable of changing the Connected Port by use of the Opto mechanical switch.

FPT_PHP.1 Passive detection of physical attack
The functionality requirements for FPT_PHP.1 are met by the provision of the Tamper Evident case, which fully encloses the security functionality of the TOE.

The nature of the four IT security functions listed in Table 6.1.1-1 of the summary specification enables them to work together to jointly meet the TOE security functional requirements without mutual conflict and without introducing any potential security weaknesses. The Opto Mechanical switch operation supports but is not constrained or compromised by the Switch Position Visual Indication function and the Switch Position Status Output Function, which are also independent of each other. Nor are they compromised or weakened by the function of the Opto mechanical switch. Similarly the functioning of the Tamper evident case has no impact upon the functionality of any of the other three security functions nor do they impact upon it.

7.3.2 Compliance of stated Assurance Measures Claims

*a. **Configuration Management -***

(ACM_AUT.2) The configuration management of the TOE will be implemented in accordance with Compucat Research's established configuration Management Regime for the production of evaluated and High Grade products. This utilises an automated configuration management system that controls the design, modification, documentation, manufacture, testing, installation and management of the TOE

(ACM_CAP.5) The configuration management system as it is specifically applied to the production and configuration control of the TOE is provided in the Secure Optical Switch Configuration Management Plan. The Compucat CM system uniquely identifies the TOE and will ensure that there is no ambiguity as to which instance of the TOE is being evaluated.

(ACM_SCP.3) The CM system shall record all changes to the TOE as well as any security flaws discovered and steps taken to eliminate them. The Compucat CM system uniquely identifies the TOE and all of its configuration items and ensures that no unauthorised changes can be made to the TOE.

b. Delivery and Operation

(ADO_DEL.3) TOE delivery shall be undertaken in accordance with a documented delivery process based upon established procedures for the delivery of items of similar sensitivity and adapted to the specific requirements of the TOE. Essentially the delivery process will apply the procedures used in the safe hands delivery of sensitive material in accordance with Compucat Research's documented operational procedures. Delivery procedures are fully covered in the SOS Delivery Process Document.

(ADO_IGS.1) TOE Installation and Operation are covered in the SOS User and Administrators Guide, which is included as a deliverable with every TOE. This documentation covers the secure installation, testing, set to work, administration and operating procedures for the TOE as well as describing the expected security environment in which a TOE can be securely operated.

c. Development

(ADV_FSP.4) The TOE requirements are expressed in a functional specification, which applies formal methods to fully describe the TSF unambiguously, describing the TSF and including a rational that demonstrates that the TSF is fully represented.

(ADV_SPM.3) A formal TSP model addressing the information flow control policy is provided and the correct correspondence between that model and the formal functional specification is established.

(ADV_HLD.5) The High Level Design provides a formal representation of the TOE at the sub system level, addressing all sub system interfaces and the separation of the TSP enforcing subsystems from other sub systems.

(ADV_IMP.3) A complete Technical Data Pack fully describing the TOE to the level of detail required to implement the design is held as part of the Configuration Management system and will be provided for evaluation.

(ADV_INT.3) The design of the TOE deliberately minimises complexity by eliminating all components from the switch other than those essential to its operation.

(ADV_LLD.2) The Low Level Design documentation provides a semiformal description of the purpose of each module within the switch that contributes to the TSF and describes its interfaces, dependencies and mode(s) of operation.

(ADV_RCR.3) A Correspondence Demonstration is formally documented to establish that, for each TSF, the relevant security functionality can be traced from the high levels of abstraction in the ST down to the physical instantiation of the device, establishing the correctness of the refinement process between each intervening level of abstraction and its immediate neighbours.

d. Guidance Documents

(AGD_ADM.1 & AGD_USR.1) The SOS User and Administration Guide provides full instructions on the installation, set to work and use of the TOE including those elements of security that are to be provided by its environment covering security relevant processes and procedures as well as the physical security features assumed to be present. The guide also provides full instructions to both administrators and users on how to operate the TOE securely and how to recognise potentially security-threatening situations. It also identifies indicators of potential failure conditions under which the TOE and its supporting devices should be examined for correct operation and what to do in the event that a TOE failure has occurred or evidence of possible tampering is detected. A copy of the guide will be provided for evaluation.

e. Life Cycle Support

(ALC_DVS.2) The development and support environment for the TOE is fundamentally the same as that used for other Compucat high grade trusted products. The relevant security processes are documented and the adequacy of the security measures to protect and maintain the confidentiality and integrity of the TOE can be demonstrated if required. The aspects of this environment that relate to the Life cycle support aspects of the EAL 7 environment are documented and will be demonstrated as required.

(ALC_LCD.3) The requirement for the provision of a measurable lifecycle model is more relevant to the development of complex software, but since the TOE is not software based and is optimally simple in its design, a life cycle model will be adapted to provide useful outputs in the context of a low complexity hardware based product.

(ALC_TAT.3) The engineering tools used to develop the TOE and any implementation-dependant options used shall be clearly identified and documented as part of the SOS implementation documentation.

f. Tests

(ATE_COV.3) In accordance with the requirements for the EAL 7 level of assurance, the TOE acceptance testing is systematic and comprehensive in nature, covering all aspects of the Functional specification and confirming the correct operation of all TSFs and confirming the validity of the instantiation of both the high and low level designs.

(ATE_DPT.3) Acceptance testing will be performed at a level of detail required to confirm that the subsystems of the HLD have been correctly realised in the TOE.

(ATE_FUN.2) All testing will be accurately documented and the test plan, test procedures and test results will be provided for analysis.

(ATE_IND.3) A fully functional TOE will be provided to the evaluator for confirming the validity of in house developer tests.

g. Vulnerability Assessment

(AVA_CCA.2) Systematic searching for possible covert channels within the TOE has established that the design of the TOE effectively precludes the possibility of covert channels between the Selectable Ports in a properly constructed TOE.

(AVA_MSU.3) The SOS 'User and Administrators Guide' provides clear and unequivocal instructions regarding the secure use of the TOE and how to properly install it. A copy of the Guide and an analysis of it confirming its validity will be made available for evaluation.

(AVA_SOF.1) The implementation of the TOE security functionality is hardware based and is both non-probabilistic and non-permutational in nature. As such, none of the security mechanisms used in the TOE is the subject of a SOF claim.

(AVA_VLA.4) Vulnerability analysis demonstrates that the only way for a user to circumvent the proper operation of the TOE is by deliberate interference in the way that it has been installed or by tampering with the TOE itself. These risks are adequately countered by the assumed security environment and by the Tamper evident nature of the TOE respectively. A copy of the vulnerability analysis will be provided for evaluation.

Thus, taken in aggregate the IT security functions, environmental assumptions and assurance measures are sufficient to fulfil the claimed security functionality of the TOE.