Market Central
SecureSwitch® Fiber Optic A/B/C Switch Revision A Security Target
February 14, 2005
Document No. F4-0205-001

COACT, Inc.
Rivers Ninety Five
9140 Guilford Road, Suite G
Columbia, MD 21046-2587

Phone: 301-498-0150

Fax: 301-498-0855

COACT, Inc. assumes no liability for any errors or omissions that may appear in this document.

DOCUMENT INTRODUCTION

Prepared By:	Prepared For:
COACT, Inc. 9140 Guilford Road, Suite G Columbia, Maryland 21046-2587	Market Central, Inc. 500 Business Center Drive Pittsburgh, PA 15205-1333

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the SecureSwitch®[1] Fiber Optic A/B/C Switch Revision A. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

REVISION HISTORY

Rev	Description
	February 14, 2005 initial realease.

[1] SecureSwitch is a registered trademark of Market Central, Inc. All rights reserved.

TABLE OF CONTENTS

LIST OF FIGURES ... vii

LIST OF TABLES ... ix

LIST OF ACRONYMS ... xi

1. SECURITY TARGET INTRODUCTION ... 1
1.1 Security Target Reference ... 1
1.1.1 Security Target Name ... 1
1.1.2 TOE Reference ... 1
1.1.3 Security Target Evaluation Status ... 1
1.1.4 Evaluation Assurance Level ... 1
1.1.5 Keywords ... 1
1.2 TOE Overview ... 1
1.2.1 Security Target Organisation ... 1
1.3 Common Criteria Conformance ... 2
1.4 Protection Profile Conformance ... 2
1.5 Document Conventions ... 2

2. TOE DESCRIPTION ... 3
2.1 TOE Description ... 3
2.1.1 Physical Boundary ... 4
2.1.2 Logical Boundary ... 4

3. SECURITY ENVIRONMENT ... 5
3.1 Threats ... 5
3.1.1 Threats Addressed by the TOE ... 5
3.1.2 Threats Addressed by the IT Environment ... 5
3.2 Assumptions ... 5
3.2.1 Personnel Assumptions ... 5
3.2.2 Physical Environment Assumptions ... 6
3.2.3 IT Environment Assumptions ... 6
3.3 Organisational Security Policies ... 6

4. SECURITY OBJECTIVES ... 7
4.1 Security Objectives for the TOE ... 7
4.2 Security Objectives for the IT Environment ... 7
4.3 Rationale for Security Objectives of the TOE ... 7
4.4 Rationale for Security Objectives of the IT Environment ... 8

5. IT SECURITY REQUIREMENTS ... 9
5.1 Security Functional Requirements of the TOE ... 9
5.1.1 User Data Protection (FDP) ... 9
5.1.1.1 FDP_IFC.2 Complete Information Flow Control ... 9
5.1.1.2 FDP_IFF.1 Simple Security Attributes ... 9
5.1.2 Protection of the TSF (FPT) ... 10
5.1.2.1 FPT_RVM.1 Non-Bypassability of the TSP ... 10
5.1.2.2 FPT_SEP.1 TSF Domain Separation ... 10
5.1.3 Secure Switching Requirements (SSR) ... 10

5.1.3.1 SSR_ISO.1 Optical Isolation 10
5.2 Security Functional Requirements of the IT Environment 10
5.3 Security Assurance Requirements of the TOE 10
5.4 Strength of Function Claim of the TOE.. 12
5.5 Rationale for TOE Objectives Coverage 12
5.6 Rationale for IT Environment Objectives Coverage 13
5.7 Rationale for Security Assurance Requirements of the TOE 13
5.8 Rationale for Strength of Function Claim.. 14
5.9 Rationale for IT Security Requirement Dependencies 14
5.10 Rationale for IT Explicitly Stated SFRs 14

6. TOE SUMMARY SPECIFICATION 15
6.1 TOE Security Functions.. 15
6.1.1 Switching 15
6.1.2 Isolation.. 15
6.2 Assurance Measures.. 15
6.3 Rationale for Security Functional Requirements Coverage.. 17
6.4 Rationale for Satisfaction of Strength of Function Claim 17

7. PROTECTION PROFILE CLAIMS 19
7.1 Protection Profile Reference 19
7.2 Protection Profile Refinements.. 19
7.3 Protection Profile Additions 19
7.4 Protection Profile Rationale.. 19

8. RATIONALE 21
8.1 Security Objectives Rationale.. 21
8.2 Security Requirements Rationale.. 21
8.3 TOE Summary Specification Rationale.. 21
8.4 Protection Profile Claims Rationale.. 21

LIST OF FIGURES

Figure 1 - Front Panel of SecureSwitch® 3
Figure 2 - Back Panel of SecureSwitch® (SC Connectors) 3

LIST OF TABLES

Table 1 - Mappings of Threats to Security Objectives for the TOE 8

Table 2 - Mappings of Threats and Assumptions to Security Objectives for the IT Environment.. 8

Table 3 - Security Functional Requirements.. 9

Table 4 - Assurance Requirements.. 11

Table 5 - Mappings Between Functional Requirements to Objectives for the TOE.... 12

Table 6 - Functional Requirements Dependencies... 14

Table 7 - Assurance Correspondence.. 16

Table 8 - Mappings of Security Functional Requirements to TOE Security Functions17

ACRONYMS LIST

CC	Common Criteria
EAL4	Evaluation Assurance Level 4
IT	Information Technology
NIAP	National Information Assurance Partnership
PP	Protection Profile
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

CHAPTER 1

1. Security Target Introduction

This Security Target (ST) describes the objectives, requirements and rationale for the SecureSwitch® Fiber Optic A/B/C Switch Revision A. The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation, Version 2.1*, the ISO/IEC JTC 1/SC27, *Guide for the Production of PPs and STs, Version 0.9* and all NIAP and International Interpretations through December 12, 2003. As such, the spelling of terms is presented using the internationally accepted English.

1.1 Security Target Reference

This section provides identifying information for the *SecureSwitchÒ Fiber Optic A/B/C Switch Revision A Security Target* by defining the Target of Evaluation (TOE).

1.1.1 Security Target Name

SecureSwitchÒ Fiber Optic A/B/C Switch Revision A Security Target

1.1.2 TOE Reference

SecureSwitch® Fiber Optic A/B/C Switch Revision A

1.1.3 Security Target Evaluation Status

This ST is evaluated.

1.1.4 Evaluation Assurance Level

Assurance claims conform to Evaluation Assurance Level 4 (EAL4), augmented with AVA_CCA.1 and AVA_VLA.3, from the *Common Criteria for Information Technology Security Evaluation, Version 2.1*.

1.1.5 Keywords

Secure Switch, Optical Switch, Fiber Optic, Fibre Optic, Duplex

1.2 TOE Overview

This Security Target defines the requirements for the SecureSwitch® Fiber Optic A/B/C Switch Revision A (hereafter referred to as the "SecureSwitch®"). The TOE is an all-optical switch that connects one host with up to three other networks, one at time. The specially designed switching mechanism provides strong isolation between all ports on the device.

1.2.1 Security Target Organisation

Chapter 1 of this ST provides introductory and identifying information for the TOE.

Chapter 2 describes the TOE, its architecture, and provides some guidance on its use.

Chapter 3 provides a security environment description in terms of assumptions, threats and organisational security policies.

Chapter 4 identifies the security objectives of the TOE and of the Information Technology (IT) environment.

Chapter 5 provides the TOE functional and assurance requirements, as well as requirements on the IT environment.

Chapter 6 is the TOE Summary Specification, a description of the functions provided by the SecureSwitch® product to satisfy the security functional and assurance requirements listed in chapter five.

Chapter 7 identifies claims of conformance to registered Protection Profiles (PP).

Chapter 8 provides references to rationale for the security objectives, requirements, TOE summary specification and PP claims.

1.3 Common Criteria Conformance

This security target is compliant with the *Common Criteria for Information Technology Security Evaluation, Version 2.1*, functional requirements (Part 2) conformant, assurance requirements (Part 3) conformant for EAL4, augmented with AVA_CCA.1 and AVA_VLA.3, and all NIAP and International Interpretations through December 12, 2003.

1.4 Protection Profile Conformance

The SecureSwitch® does/does not claim conformance to any registered Protection Profile.

1.5 Document Conventions

The CC defines four operations on security functional requirements. The font conventions below identify the conventions for the operations defined by the CC.

Assignment:	**indicated with bold text**
<u>Selection:</u>	<u>indicated with underlined text</u>
Refinement:	***indicated with bold text and italics***
Iteration:	indicated with typical CC requirement naming followed by a number in parenthesis for each iteration (e.g., FMT_MOF.1 (1))

CHAPTER 2

2. TOE Description

This section provides the context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

2.1 TOE Description

The SecureSwitch® (the TOE) is an optical switch that connects up to three different networks, one at a time, to a full-duplex host).

The TOE uses a proprietary mirrored switching mechanism with specially designed spherical mirrors to provide isolation of a minimum 75 dB between all ports.

To control the switching mirrors, the user simply selects one of three radio buttons on the front of the device. These buttons are marked A, B, and C, and correspond to network ports A, B, and C on the back of the device (Network Ports). There are also three LEDs marked A, B, and C on the front of the device to indicate which Network Port is selected. Figures 1 and 2 below illustrate the front and back of the table-top version of the device. Rack-mount versions are also available.

Figure 1 - Front Panel of SecureSwitchÒ

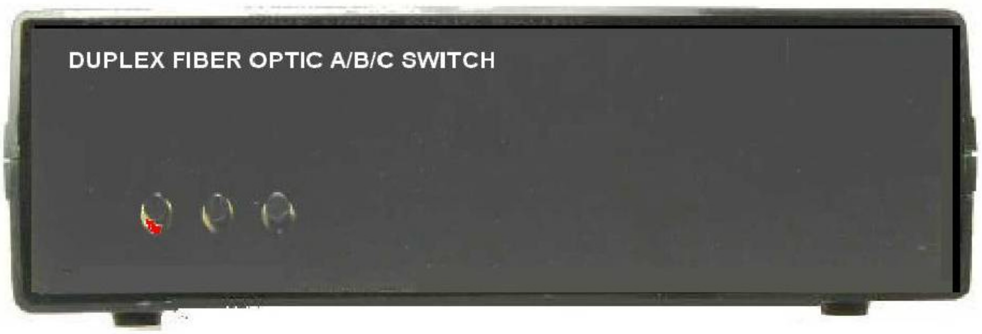
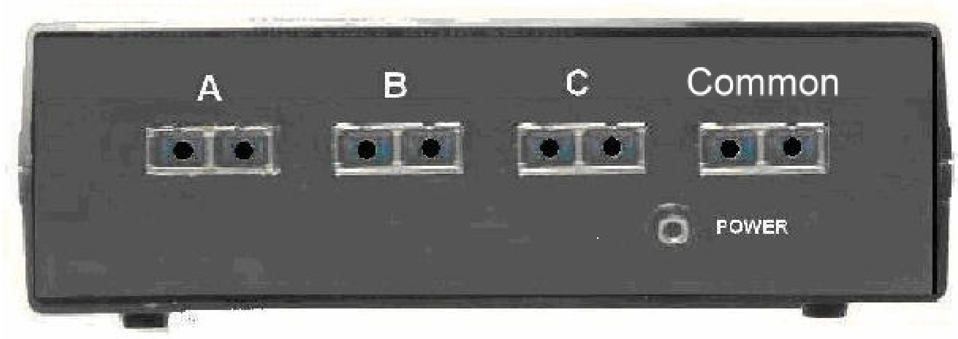


Figure 2 - Back Panel of SecureSwitchÒ **(SC Connectors)**



One or more of the Network Ports may be left disconnected (no fiber is connected) to provide a switch position that causes the Common Port to be disconnected from all networks.

The TOE features all-optical switching using a proprietary mechanism consisting of five independent mirrors (Mirror Switch). The switching action is controlled by rotating the mirrors. The rotation mechanism is managed electronically. The TOE is completely transparent to optical signalling rates and supports ST, and SC connectors for 62.5 / 125 micrometers multimode, dual fiber systems. Other size fiber systems are available as well.

The device specifications include:

A) Sensitivity: 750 to 1450 nanometers

B) Crosstalk Tolerance: exceeds 75 dB

C) Insertion Loss: 4.5 dB @ 1300 nm

D) Vibration Tolerance: 15 Gs on 3 axes per FOTP-11

E) Physical Shock: 15 Gs on 3 axes per FOTP-14

F) Switching Speed: 5 milliseconds typical, 10 milliseconds maximum

G) Operating Temperature: -10° C to +65° C

H) Size Table-top Enclosure: 2.5” H x 8” W x 6.3” D

I) Size Rack-mount Enclosure: 2U (3.5”) H x 19” W x 6.25” D

J) Weight Table-top: 3 pounds

K) Weight Rack-mount: 6 pounds including power supply

L) Power: 5 volts DC from included power module.

2.1.1 Physical Boundary

The physical boundary of the TOE is the entire SecureSwitch® device. This includes the buttons, the LEDs, the Mirror Switch, the ports, as well as the internal electronics that operate the mirror rotation and optical transfers for the ports.

2.1.2 Logical Boundary

The logical boundaries of the TOE include the switching and isolation capabilities.

The SecureSwitch Flow Control Policy defines the switching capabilities and the User interface to control the switching.

The isolation capability defines the TOE’s ability to insulate the ports from one another. This capability guarantees the TOE’s security functions are executed.

CHAPTER 3

3. Security Environment

This chapter identifies the following:

A) IT related threats countered by the TOE and the IT Environment.

B) Significant assumptions about the TOE’s operational environment.

C) Organisational security policies for the TOE as appropriate.

Using the above listing, this chapter identifies threats countered by the TOE (T), threats countered by the IT environment (TE), assumptions on the operational environment (A), and organisational security policies (P).

3.1 Threats

The threats identified in the following subsections are addressed by the TOE and IT environment, respectively. For the threats below, attackers are assumed to be of low attack potential.

3.1.1 Threats Addressed by the TOE

T.DIRECT	A remote attacker captures data of a separate network while the attacker’s network is connected to that separate network by the TOE.
T.CROSSTALK	A remote attacker captures data of a separate network while the attacker’s network is not connected to that separate network by the TOE.
T.ATTACK	A remote attacker performs malicious activity against the Host computer while the attacker’s network is connected to the Host computer by the TOE.

3.1.2 Threats Addressed by the IT Environment

None

3.2 Assumptions

Assumptions are ordered into three groups. They are personnel assumptions, physical environment assumptions, and IT environment assumptions. Personnel assumptions describe characteristics of personnel who are relevant to the TOE. Physical environment assumptions describe characteristics of the non-IT environment that the TOE is deployed in. IT environment assumptions describe the technology environment that the TOE is operating within.

3.2.1 Personnel Assumptions

A.INSTALL	The User has connected between one and three distinct networks on Network Ports A, B, and C. The User has connected a computer on the Common Port that has a full-duplex network interface.
A.NOEVILUSER	The User is non-hostile.

A.COMPETENT The User follows all user guidance when using the TOE.

3.2.2 Physical Environment Assumptions

A.ENVIRON The TOE will be located in an environment that provides physical security, uninterruptible power, and temperature control required for reliable operation of the hardware.

3.2.3 IT Environment Assumptions

None

3.3 Organisational Security Policies

None

CHAPTER 4

4. Security Objectives

The objectives identified in the following subsections ensure that all the threats listed in chapter three are addressed by the TOE and the operating environment, respectively.

4.1 Security Objectives for the TOE

O.NOCONNECT The TOE will not allow two Network Ports to directly connect (i.e., no information flow is permitted).

O.ISOLATION The TOE will provide isolation between all ports.

O.SWITCH The TOE will provide the User with the ability to connect the Common Port to each of the three Network Ports, one at a time.

4.2 Security Objectives for the IT Environment

The security objectives listed below are to be satisfied without imposing technical requirements on the TOE. Thus, they will be satisfied through application of procedural or administrative measures.

OE.INSTALL The User has connected between one and three distinct networks on Network Ports A, B, and C. The User has connected a computer on the Common Port that has a full-duplex network interface.

OE.NOEVILUSER The User is non-hostile.

OE.COMPETENT The User follows all user guidance when using the TOE.

OE.ENVIRON The TOE will be located in an environment that provides physical security, uninterruptible power, and temperature control required for reliable operation of the hardware.

4.3 Rationale for Security Objectives of the TOE

This section provides the rationale that all security objectives are traced back to aspects of the addressed threats or policies.

O.NOCONNECT Addresses T.DIRECT. The TOE will not allow Network Ports to be connected to each other, directly addressing the threat of a direct connection.

O.ISOLATION Addresses T.CROSSTALK. By providing isolation between ports, the only way for information to pass between ports is according to the TOE’s information flow control policy.

O.SWITCH Addresses T.ATTACK. The User has the ability to disconnect from a network from which malicious activity originates.

Table 1 - Mappings of Threats to Security Objectives for the TOE

	T.DIRECT	T.CROSSTALK	T.ATTACK
O.NOCONNECT	X		
O.ISOLATION		X	
O.SWITCH			X

4.4 Rationale for Security Objectives of the IT Environment

This section provides the rationale that all security objectives for the operating environment are traced back to aspects of the addressed threats, policies, or assumptions.

OE.INSTALL	Addresses A.INSTALL. The objective satisfies the assumption by providing the assumed installation configuration.
OE.NOEVILUSER	Addresses A.NOEVILUSER. The objective satisfies the assumption by providing there will be no evil users.
OE.COMPETENT	Addresses A.COMPETENT. The objective satisfies the assumption by providing the User will follow guidance.
OE.ENVIRON	Addresses A.ENVIRON. The objective satisfies the assumption by providing the assumed operating conditions.

Table 2 - Mappings of Threats and Assumptions to Security Objectives for the IT Environment

	A.INSTALL	A.NOEVILUSER	A.COMPETENT	A.ENVIRON
OE.INSTALL	X			
OE.NOEVILUSER		X		
OE.COMPETENT			X	
OE.ENVIRON				X

CHAPTER 5

5. IT Security Requirements

This section contains the security requirements that are relevant to the TOE. These requirements consist of functional components from Part 2 of the CC and assurance components from Part 3 of the CC. SFRs beginning with “SSR” are explicitly stated SFRs.

This section also contains the Strength of Function claim and corresponding rationale for components that require such a claim.

Table 3 - Security Functional Requirements

Security Functional Requirements of the TOE	
FDP_IFC.2	Complete Information Flow Control
FDP_IFF.1	Simple Security Attributes
FPT_RVM.1	Non-Bypassability of the TSP
FPT_SEP.1	TSF Domain Separation
SSR_ISO.1	Optical Isolation

5.1 Security Functional Requirements of the TOE

5.1.1 User Data Protection (FDP)

5.1.1.1 FDP_IFC.2 Complete Information Flow Control

Hierarchical to: FDP_IFC.1 Subset Information Flow Control.

FDP_IFC.2.1 The TSF shall enforce the **SecureSwitch Flow Control Policy** on **optical signals on the Common Port and each of the Network Ports** and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TSC to flow to and from any subject in the TSC are covered by an information flow control SFP.

Dependencies: FDP_IFF.1 Simple Security Attributes.

5.1.1.2 FDP_IFF.1 Simple Security Attributes

Hierarchical to: No other components.

FDP_IFF.1.1 The TSF shall enforce the **SecureSwitch Flow Control Policy** based on the following types of subject and information security attributes **the Position of the Mirror Switch.**

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

a) **Information may only flow between the Common Port and a single Network Port if the Position of the Mirror Switch is in the single position that corresponds to that Network Port.**

FDP_IFF.1.3 The TSF shall enforce the following information flow control rules: **no additional information flow control SFP rules.**

FDP_IFF.1.4 The TSF shall provide the following: **no additional SFP capabilities**.

FDP_IFF.1.5 The TSF shall explicitly authorise an information flow based upon the following rules: **no explicit authorisation rules.**

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

Dependencies: FDP_IFC.1 Subset Information Flow Control,

FMT_MSA.3 Static Attribute Initialisation.

5.1.2 Protection of the TSF (FPT)

5.1.2.1 FPT_RVM.1 Non-Bypassability of the TSP

Hierarchical to: No other components.

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

Dependencies: No dependencies.

5.1.2.2 FPT_SEP.1 TSF Domain Separation

Hierarchical to: No other components.

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

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

Dependencies: No dependencies.

5.1.3 Secure Switching Requirements (SSR)

5.1.3.1 SSR_ISO.1 Optical Isolation

Hierarchical to: No other components.

SSR_ISO.1.1 The TOE shall ensure that there is 75 dB of isolation between all ports that are not currently connected by the Position of the Mirror Switch.

Dependencies: No dependencies.

5.2 Security Functional Requirements of the IT Environment

None

5.3 Security Assurance Requirements of the TOE

The TOE meets the assurance requirements for EAL4, augmented with AVA_CCA.1 and AVA_VLA.3. These requirements are summarised in the table below.

Table 4 - Assurance Requirements

Assurance Class	Component ID	Component Title
Configuration Management	ACM_AUT.1	Partial CM Automation
Configuration Management	ACM_CAP.4	Generation Support and Acceptance Procedures
Configuration Management	ACM_SCP.2	Problem Tracking CM Coverage
Delivery and Operation	ADO_DEL.2	Detection of Modification
Delivery and Operation	ADO_IGS.1	Installation, Generation, and Start-Up Procedures
Development	ADV_FSP.2	Fully Defined External Interfaces
Development	ADV_HLD.2	Security Enforcing High-Level Design
Development	ADV_IMP.1	Subset of the Implementation of the TSF
Development	ADV_LLD.1	Descriptive Low-Level Design
Development	ADV_RCR.1	Informal Correspondence Demonstration
Development	ADV_SPM.1	Informal TOE Security Policy Model
Guidance Documents	AGD_ADM.1	Administrator Guidance
Guidance Documents	AGD_USR.1	User Guidance
Life Cycle Support	ALC_DVS.1	Identification of Security Measures
Life Cycle Support	ALC_LCD.1	Developer Defined Life-Cycle Model
Life Cycle Support	ALC_TAT.1	Well Defined Development Tools
Tests	ATE_COV.2	Analysis of Coverage
Tests	ATE_DPT.1	Testing High-Level Design
Tests	ATE_FUN.1	Functional Testing
Tests	ATE_IND.2	Independent Testing - Sample
Vulnerability Assessment	AVA_CCA.1	Covert Channel Analysis
Vulnerability Assessment	AVA_MSU.2	Validation of Analysis
Vulnerability Assessment	AVA_SOF.1	Strength of TOE Security Function Evaluation
Vulnerability Assessment	AVA_VLA.2	Independent Vulnerability Analysis
Vulnerability Assessment	AVA_VLA.3	Moderately Resistant

5.4 Strength of Function Claim of the TOE

There are no probabilistic or permutational mechanisms implemented by the TOE, therefore no strength of function claim is made.

5.5 Rationale for TOE Objectives Coverage

This section provides the rationale that all TOE Objectives have been met by the Security Functional Requirements levied on the TOE.

O.NOCONNECT Satisfied by FDP_IFC.2, FDP_IFF.1, and SSR_ISO.1, because FDP_IFC.2 and FDP_IFF.1 specify that only information may flow between the Common Port and a single Network Port at a time, never two Network Ports. SSR_ISO.1 supports this objective, because it requires all ports be shielded 75 dB from each other. This includes one Network Port to the next, thereby supporting the objective of not allowing a connection between Network Ports.

O.ISOLATION Satisfied by SSR_ISO.1. Because that SFR requires that each port will be isolated from 75 dB of isolation. This will prevent cross-talk as required by O.ISOLATION.

O.SWITCH Satisfied by FDP_IFC.2, FDP_IFF.1, FPT_RVM.1, FPT_SEP.1, and SSR_ISO.1. FDP_IFC.2 and FDP_IFF.1 define the SecureSwitch Flow Control Policy that requires switching to exist as required by O.SWITCH. FPT_RVM.1 and FPT_SEP.1 require that the SecureSwitch Flow Control Policy always be invoked and have its own domain of execution, respectively. This ensures the TSF will be invoked and not interfered. Finally, SSR_ISO.1 requires that no data can traverse the switch except to and from the Network Port designated by the Position of the Mirror Switch. This supports the SecureSwitch Flow Control Policy.

Table 5 - Mappings Between Functional Requirements to Objectives for the TOE

	O.NOCONNECT	O.ISOLATION	O.SWITCH
FDP_IFC.2	X		X
FDP_IFF.1	X		X
FPT_RVM.1			X
FPT_SEP.1			X
SSR_ISO.1	X	X	X

5.6 Rationale for IT Environment Objectives Coverage

This section provides the rationale that all IT Environment Objectives have been met by the Security Functional Requirements levied on the IT Environment.

None

5.7 Rationale for Security Assurance Requirements of the TOE

The TOE meets the assurance requirements for EAL4. The CC states that EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices that, though rigorous, do not require substantial specialist knowledge, skills, and other resources. The EAL chosen is based on the statement of the security environment (assumptions, threats and organizational policy) and the security objectives defined in this ST.

The sufficiency of the EAL chosen, EAL4, is justified based on those aspects of the environment that have impact upon the assurance needed in the TOE. The administrative staff is conscientious, non-hostile and well trained (as evidenced in A.INSTALL, A.NOEVILUSER, and A.COMPETENT. The TOE is physically protected (as evidenced in O.NOCONNECT) and properly and securely configured (as evidenced in O.ISOLATION, and O.SWITCH).

Given these aspects, a TOE based on good commercial development practices is sufficient. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. EAL4 is, therefore, applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.

EAL4 provides assurance by an analysis of the security functions, using a functional and complete interface specification, guidance documentation, the high-level and low-level design of the TOE, and a subset of the implementation to understand the security behaviour. Assurance is additionally gained through an informal model of the TOE security policy. This SecureSwitch product has undergone these tasks.

The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification and high-level design, selective independent confirmation of the developer test results, strength of function analysis, evidence of a developer search for vulnerabilities, and an independent vulnerability analysis demonstrating resistance to penetration attackers with a low attack potential. This SecureSwitch product has undergone these tasks.

EAL4 also provides assurance through the use of development environment controls and additional TOE configuration management including automation, and evidence of secure delivery procedures. This SecureSwitch product has undergone these tasks. It represents a meaningful increase in assurance from EAL3 by requiring more design description, a subset of the implementation, and improved mechanisms and procedures that provide confidence that the TOE will not be tampered with during development or delivery.

AVA.CCA.1 and AVA_VLA.3 were included because the target market for this product is within secure environments that typically have covert channel and strong vulnerability analysis requirements.

Given the amount of assurance deemed necessary to meet the security environment and objectives of the TOE and the intent of EAL 4, EAL 4 is an appropriate level of assurance for the TOE described in this ST.

5.8 Rationale for Strength of Function Claim

There are no probabilistic or permutational mechanisms implemented by the TOE, therefore no strength of function claim is made.

5.9 Rationale for IT Security Requirement Dependencies

The following table lists the claimed TOE and IT Environment security requirements and their dependencies. This section also contains a rationale for any dependencies that are not satisfied. For the purpose of dependencies, SFRs with NIAP or International Interpretations are considered to fulfil the dependency of their original SFR, as interpretations do not alter the scope of the SFR.

Table 6 - Functional Requirements Dependencies

SFR	Dependencies	Hierarchical To
FDP_IFC.2	FDP_IFF.1	FDP_IFC.1
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	None
FPT_RVM.1	None	None
FPT_SEP.1	None	None
SSR_ISO.1	None	None

FDP_IFF.1 is dependent upon FDP_IFC.1. FDP_IFC.2 is hierarchical to FDP_IFC.1; therefore, the dependency is satisfied.

FDP_IFF.1 is dependent upon FMT_MSA.3. FMT_MSA.3 is not included as there are no objects or attributes that can be created that affect the SecureSwitch Flow Control Policy. Rather, the policy is determined by one attribute alone, the Position of the Mirror Switch.

5.10 Rationale for IT Explicitly Stated SFRs

SSR_ISO.1	This SFR was created for this security target, because the Common Criteria does not currently have a requirement for hardware port shielding and isolation.

CHAPTER 6

6. TOE Summary Specification

6.1 TOE Security Functions

6.1.1 Switching

The SecureSwitch® has a front panel with three radio buttons labelled A, B, and C. Each button has a corresponding LED that indicates which if that button is currently selected. Only one button can be selected at a time.

Each button corresponds to a Network Port on the rear of the box. At least one network connection is assumed to be plugged into ports A, B, and C. There is a fourth port on the rear of the box for a local computer. This port is referred to in this ST as the Common Port. The information flows from each of these four ports are the only information flows in the TOE.

Inside the SecureSwitch® is a Mirror Switch. The Mirror Switch is a specially designed, set of spherical mirrors that allow optical communications to travel between the Common Port and one of the Network Ports at a time. When the Mirror Switch is repositioned, the Common Port can communicate with a different Network Port. There is a single position for each Network Port.

The radio buttons on the front of the device control the Position of the Mirror Switch. When button ‘A’ is pressed, an electric motor rotates the mirror to the position designated for Network Port ‘A’. The same applies to buttons ‘B’ and ‘C’.

The TOE is a self-contained unit that forwards information signals but is not affected by those signals. This provides an isolated domain for the execution of the TSF.

The Switching function of the SecureSwitch® meets the following SFRs:

A) FDP_IFC.2

B) FDP_IFF.1

C) FMT_RVM.1

D) FMT_SEP.1

6.1.2 Isolation

Due to the proprietary design including five specially designed mirrors. The TOE provides an average isolation of a minimum of 75 dB between all ports. This high isolation was designed to comfortably meet the industry standard 75 dB isolation rating.

The Isolation function of the SecureSwitch® meets the following SFRs:

A) SSR_ISO.1

6.2 Assurance Measures

The following table demonstrates the correspondence between the security assurance requirements listed in Chapter 5 to the developer evidence.

Table 7 - Assurance Correspondence

Component ID	Developer Evidence
ACM_AUT.1	*“Configuration Management”*
ACM_CAP.4	*“Configuration Management”*
ACM_SCP.2	*“Configuration Management”*
ADO_DEL.2	*“Delivery and Operation”*
ADO_IGS.1	*“Delivery and Operation”*
ADV_FSP.2	*“Development”*
ADV_HLD.2	*“Development”*
ADV_IMP.1	*“Development”* *“Bill of Material and Assembly Instructions, 5101180”* *“Bill of Material and Assembly Instructions, 5101182”* *“ssfoabc.asm, Control Software Source Code”*
ADV_LLD.1	*“Development”*
ADV_RCR.1	*“Development”*
ADV_SPM.1	*“Development”*
AGD_ADM.1	“Secure*Switch® Fiber Optic A/B/C Switch Revision A Manual”*
AGD_USR.1	“Secure*Switch® Fiber Optic A/B/C Switch Revision A Manual”*
ALC_DVS.1	*“Life Cycle Support”*
ALC_LCD.1	*“Life Cycle Support”*
ALC_TAT.1	*“Life Cycle Support”*
ATE_COV.2	*“Testing”*
ATE_DPT.1	*“Testing”*
ATE_FUN.1	*“Testing”*
ATE_IND.2	*“Testing”*
AVA_MSU.2	*“Vulnerability Assessment”*
AVA_SOF.1	*“Vulnerability Assessment”*
AVA_VLA.2	*“Vulnerability Assessment”*

6.3 Rationale for Security Functional Requirements Coverage

The following section provides a rationale showing that each SFR is fully implemented by the security functions of the TOE.

FDP_IFC.2 Is implemented by the Switching function. The Switching function defines the information flows within the TOE and subjects them to the SecureSwitch Flow Control Policy. This fulfills the SFR.

FDP_IFF.1 Is implemented by the Switching function. The Switching function describes how buttons on the device control the Position of the Mirror Switch. Also that only the Common Port can communicate with each of the Network Ports one at a time. This agrees with the SecureSwitch Flow Control Policy as defined by this SFR.

FPT_RVM.1 Is implemented by the Switching function. The Switching function describes that information flow only occurs when traversing the Mirror Switch in a proper position. For this reason, the SecureSwitch Flow Control Policy is always invoked. This fulfills the SFR.

FPT_SEP.1 Is implemented by the Switching function. The Switching function describes that the TOE is in an isolated control environment. Considering the isolation, it is not possible for other processes or communications to interfere with the Mirror Switch. This fulfills the domain separation SFR.

SSR_ISO.1 Is implemented by the Isolation function. The Isolation function describes that the ports have a 75 dB cross-talk tolerance between each other. This fulfills the SFR.

Table 8 - Mappings of Security Functional Requirements to TOE Security Functions

	Switching	Isolation
FDP_IFC.2	X	
FDP_IFF.1	X	
FPT_RVM.1	X	
FPT_SEP.1	X	
SSR_ISO.1		X

6.4 Rationale for Satisfaction of Strength of Function Claim

There are no probabilistic or permutational mechanisms implemented by the TOE, therefore no strength of function claim is made.

CHAPTER 7

7. Protection Profile Claims

This chapter provides detailed information in reference to the Protection Profile conformance identification that appears in Chapter 1, Section 1.4 Protection Profile Conformance.

7.1 Protection Profile Reference

This Security Target does not claim conformance to any registered Protection Profiles.

7.2 Protection Profile Refinements

This Security Target does not claim conformance to any registered Protection Profiles.

7.3 Protection Profile Additions

This Security Target does not claim conformance to any registered Protection Profiles.

7.4 Protection Profile Rationale

This Security Target does not claim conformance to any registered Protection Profiles.

CHAPTER 8

8. Rationale

This chapter provides rationale or references to rationale required for this Security Target.

8.1 Security Objectives Rationale

Sections 4.3 - 4.4 provide the security objectives rationale.

8.2 Security Requirements Rationale

Sections 5.5 – 5.9 provide the security requirements rationale.

8.3 TOE Summary Specification Rationale

Sections 6.3 – 6.4 provide the TSS rationale.

8.4 Protection Profile Claims Rationale

Section 7.4 provides the Protection Profile Claims rationale.