DiCon Fiberoptics, Inc.

Secure Switching Unit Version D with firmware Version 4.1

Security Target

Release Date: October 31, 2008

Version: 0.10

Prepared By: Saffire Systems
P.O. Box 11154
Champaign, IL 61822-1154

Prepared For: DiCon Fiberoptics, Inc.
1689 Regatta Blvd.
Richmond, CA 94804

Table of Contents

List of Tables

List of Figures

1 Introduction

This section identifies the Security Target, Target of Evaluation (TOE), conformance claims, ST organization, document conventions, and terminology. It also includes an overview of the evaluated product.

1.1 Identification

TOE Identification:	Secure Switching Unit Version D with firmware Version 4.1
ST Identification:	DiCon Fiberoptics, Inc. Secure Switching Unit Version D Security Target
ST Version:	0.10
ST Publish Date:	October 31, 2008
ST Authors:	Michelle Ruppel, Saffire Systems
PP Identification:	None

1.2 CC Conformance Claim

The TOE is Common Criteria (CC) Version 2.3[1] Part 2 extended.

The TOE is Common Criteria (CC) Version 2.3 Part 3 conformant at EAL4, augmented with AVA_CCA.1 and AVA_VLA.3.

There are no applicable International (CCIMB) interpretations for CC Version 2.3 as of 25 July 2007.

The TOE is compliant with selected NIAP Interpretations. The selected NIAP Interpretations are identified as they are applied to the security requirements in Section 5.

This TOE is not conformant to any Protection Profiles (PPs).

1.3 Overview

The Secure Switching Unit (SSU) is an all-optical switch unit. All data flowing through the optical switches will be optical. Each switch has the capability to connect to optical fibers. These optical fibers are typically connected to optical transceivers on a computer or a signal processing/routing board on the other end. There is no requirement that the connection is to a host computer or a network. The SSU provides multiple point to point fiber connections.

The optical switches provide isolation between the output ports of the 1x3 switch block and between separate 1x3 switch blocks. There are 15 duplex pairs of 1x3 switches in the SSU. Two 1x3 switches make up a duplex 1x3 switch, so there are 30 actual switches in the SSU.

[1] Common Criteria (CC) for Information Technology Security Evaluation – August 2005, Version 2.3, CCMB-2005-08-001.

One way to think of the SSU is as an automated patch panel. Without the SSU, one would take an optical fiber and patch one optical port to another optical port (like the old telephone switchboards). The SSU provides a convenient way to switch ports with push buttons. However, unlike today's data/telecommunication routers, the SSU does not provide ANY sort of traffic or data packet management.

The SSU front LED panel provides switch position indicators. The front panel can be used to select the switch configuration modes, define user configurable modes[2], and to manually configure switch states. The console part on the back of the SSU can be used to define the programmable modes.

1.4 Organization

Section	Title	Description
1	Introduction	Provides an overview of the security target.
2	TOE Description	Defines the hardware and software that make up the TOE, and the physical and logical boundaries of the TOE.
3	TOE Security Environment	Contains the threats, assumptions and organizational security policies that affect the TOE.
4	Security Objectives	Contains the security objectives the TOE is attempting to meet.
5	IT Security Requirements	Contains the functional and assurance requirements for this TOE.
6	TOE Summary Specification	A description of the security functions and assurances that this TOE provides.
7	PP Claims	Protection Profile Conformance Claims
8	Rationale	Contains pointers to the rationales contained throughout the document.

Table 1: ST Organization and Description

1.5 Document Conventions

The CC defines four operations on security functional requirements. The conventions below define the conventions used in this ST to identify these operations. When NIAP Interpretations are included in requirements, the additions from the interpretations are displayed as refinements.

Assignment: indicated with bold text

[2] A "mode" is a pre-stored channel configuration setting.

Selection: indicated with underlined text

Refinement: ***additions and replacements indicated with bold text and italics***

deletions without replacing text indicated with strike-through ~~bold text and italics~~

Iteration: indicated with typical CC requirement naming followed by a lower case letter for each iteration (e.g., FMT_MSA.1a)

The explicitly stated requirements claimed in this ST are denoted by the "_EXP" extension in the unique short name for the explicit security requirement.

1.6 Document Terminology

Please refer to CC Part 1 Section 2.3 for definitions of commonly used CC terms.

1.6.1 ST Specific Terminology

All-optical switching	Switching in the optical domain, in which the switching action is obtained by redirecting light beams.
MEMS	Micro-electromechanical systems; a technology that embeds mechanical devices such as sensors, mirrors, actuators, and valves in semiconductor chips.
LED	Light emitting diode; a electronic device that lights up when electricity is passed through it.

1.6.2 Acronyms

CC	Common Criteria
EAL4	Evaluation Assurance Level 4
EAL4+	EAL4 augmented with AVA_CCA.1 and AVA_VLA.3
OSP	Organisational Security Policy
PP	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirement
SOF	Strength of Function

SSU	Secure Switching Unit
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

2 TOE Description

2.1 Overview

The TOE is the SSU optical switch that connects optical fibers to each other. All data flowing through the optical switches is optical. The SSU does not alter, process, or store any information going through the optical fiber. Each switch can only connect 2 optical fibers at one time.

2.2 Architecture Description

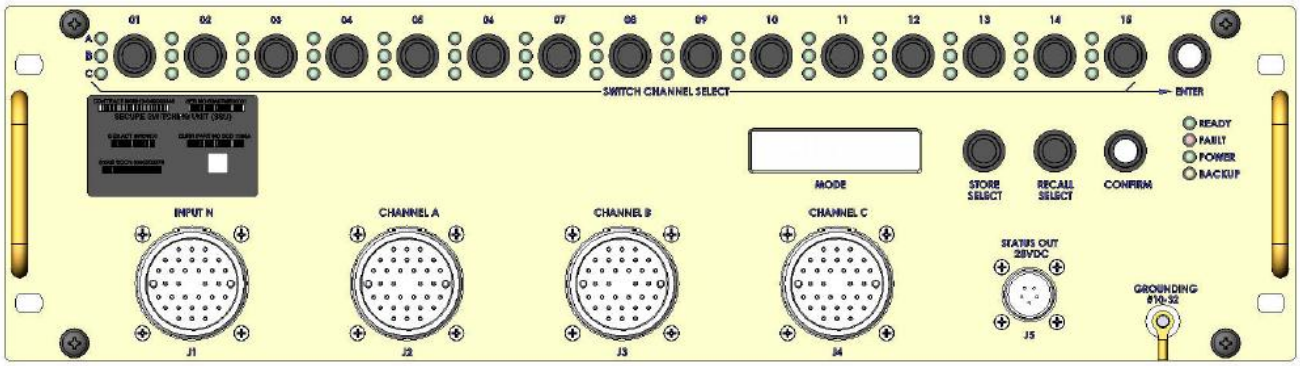

Figure 1: SSU Front Panel

Figure 2: SSU Rear Panel

The Secure Switching Unit (SSU) is an all-optical switch unit containing the following:

- 3U 19” rack-mount chassis
- 15 duplex pairs of 1x3 MEMS optical switches
- Front LED switch position indicators
- Unit status indicator (Ready, Fault, Power, and Backup LEDs)
- Built-In Self Test Capability

- Console Port used only to define Programmable Modes (via a direct serial connection to a PC or terminal – RS232) and cannot be used to control the switch. The console port is a DB-9 female connector implementing an RS232 interface on the back of the device. Figure 2: SSU Rear Panel shows the console port with a cover over it.
- Front Panel to select switch configuration modes, define User Configurable Modes, and to manually configure switch states
- Electrical Power / Status Out Connector

There are 15 duplex pairs (as shown in Figure 1: SSU Front Panel) of 1x3 switches (30 actual switches) in the SSU. Two 1x3 switches make up a duplex 1x3 switch. This means that the two 1x3 switch (e.g. Switch 1 and Switch 2) will operate synchronously (e.g. they will both switch to port A (or B, C, or Default) at the same time. Each of the thirty actual switches can only connect 2 optical fibers at one time.

Each of the 1x3 switches provides a point to point optical connection, where the input port is connected to only one output port (also referred to as a channel) at a time. There are three possible output ports – A, B, and C. This means that at any give time, there is a maximum of 30 inputs (or fibers) connected to 30 outputs (or fibers). Since the data flows through the switch in the form of a light beam, the optical connection is bi-directional, that is it works the same in either direction. Thus the designation of inputs and outputs in the figure below is arbitrary, and the flow of light can either be from input to output, or from output to input. There is also a state in which the input port is not connected to any of the output ports. This state is called the "Default" state. After power up or "Reset", the SSU will go to the Default state.

The following diagram is a representation of a duplex pair consisting of two 1x3 switches, where each switch is composed of a 1x3 MEMS component (SW1 and SW5) and 3 On-Off MEMS components (SW2-4 and SW6-8). The SSU consists of 15 of the duplex pairs depicted below.

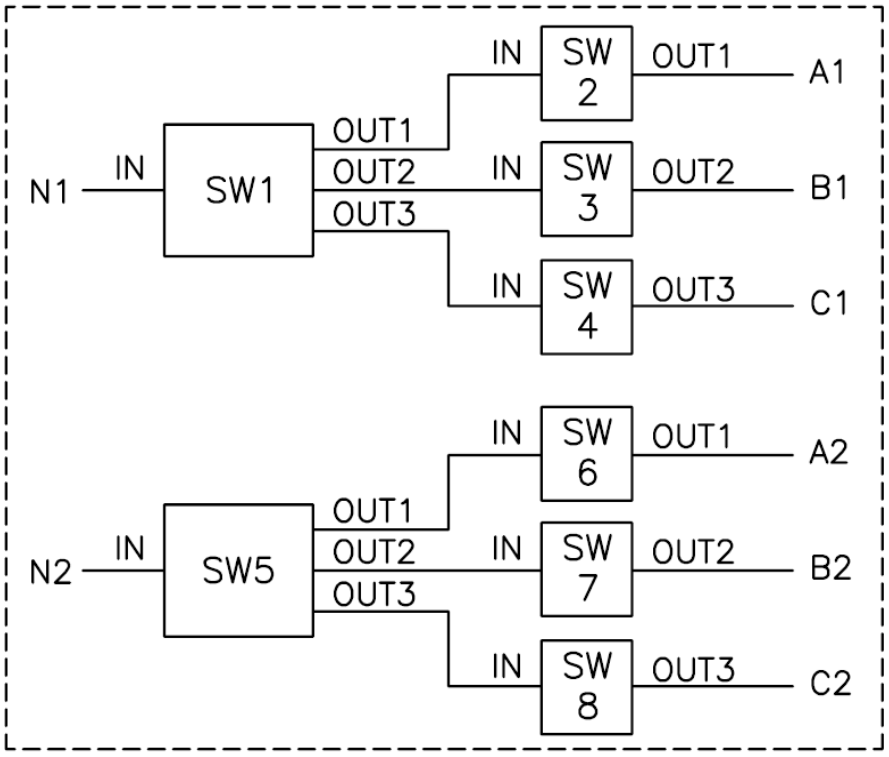

Figure 3: Duplex Pair

All input fibers (N1 to N30) are bundled into a common optical connector designated as INPUT N on the front panel. The output fibers A1 to A30, B1 to B30, C1 to C30, are also bundled into common optical connectors designated as CHANNEL A, CHANNEL B, CHANNEL C, respectively. The TOE has been tested using single wavelength, unmodulated 850nm test laser as the input.

The Electrical Power / Status Out connector provides grounding and power and serves as a fault indicator. The information conveyed by the status out pin is the same as the Fault LED, except when either the motherboard or user interface crashes in which case the one that did not crash signals a fault.

The SSU does not provide the ability to update the firmware without opening the SSU chassis. The chassis will contain a tamper evident seals to indicate any physical tampering.

The current channel for an individual switch is displayed on the LEDs on the front panel. To change the switch channels, the user pushes the pushbutton of the switch on the front panel. All switch control functions, except defining programmable modes, can only be accessed from the front panel.

There is no remote access allowed to the TOE other than the optical data which passes through the device unprocessed.

The TOE is transparent to the devices and the users of the devices on the other end of the optical

fibers; these users are considered end users of the TOE.

2.3 Physical Boundaries

The physical boundary of the TOE is the SSU device, including the SSU hardware Version D and SSU firmware Version 4.1. The hardware includes the chassis, front panel, motherboard, power back up, daughter board, user interface board, MEMS switch module. The firmware includes the backup power management, system firmware, main controller, power manager, and the user interface (UI) controller.

The key design specifications for the device are:

- Power: +28VDC
- Power Consumption: 50W maximum
- Back-up power hold-up time: 1 hour minimum
- Weight: 15 lbs. maximum
- Optical Crosstalk: -60dB maximum
- Startup Time: 30 seconds maximum

The PC or terminal directly connected to the SSU via the RS232 serial port is part of the IT environment. The optical fibers connected to the switches are also part of the IT environment.

2.4 Logical Boundaries

This section contains the product features and denotes which are in the TOE. There are no security features provided by the SSU device that have been excluded from the evaluation.

2.4.1 Security Management

The SSU provides the ability perform the following management functions on the SSU:

- Define programmable modes using the Console port.
- Select switch configuration modes, define User Configurable Modes, and manually configure switch states using the Front Panel of the SSU
- Store and recall a preset mode (a pre-stored channel configuration for all 15 switches) via the Front Panel

The TOE allows for 16 total switch configuration modes, 9 are programmable modes.

Administrators control the states of the switches using the front panel either by controlling individual duplex pairs or by recalling stored configuration modes.

2.4.2 Switching

Switching provides an optical connection between two ports by providing a low-loss path for a light beam to travel between two ports. The TOE provides all-optical switching using MEMS micro-mirrors in which the switching action is controlled by tilting the mirrors to redirect light beams. The mirror tilting mechanism is controlled electronically. This mechanism is proprietary. The signals are purely optical and the SSU does not alter, process, or store any information going through the optical fiber.

2.4.3 Protection of TOE Functions

Logical protection of the TOE is required to ensure the TOE security services are not bypassed or tampered with. In addition, the TOE provides a tamper evident seal and the ability to isolate ports from each other.

2.4.3.1 Isolation

The TOE provides the ability to isolate ports from each other to ensure that the security functions are executed on the correct port. Each of the 1x3 duplex pairs may connect the input port to only one output port (also referred to as channels) at a time.

Each of the 1x3 switches contains one optical On-off switch at each of the output ports. The 1x3 component provides optical isolation between the output ports by physical separation of output fibers. The On-off switch provides additional isolation by turning off (by optically cutting off the signal) the inactive output ports.

2.4.3.2 Tamper evident seal

All removable panels on the device will be protected by a tamper-evident seal. This tamper-evident seal will provide obvious signs of attempts to physically open the device.

3 TOE Security Environment

The TOE is intended to be used in environments in which sensitive information is processed.

This section contains assumptions regarding the security environment and the intended usage of the TOE and threats on the TOE and the IT environment.

3.1 Assumptions

The assumptions are organized into two categories: personnel assumptions and physical environment assumptions.

3.1.1 Personnel Assumptions

A.CONNECT The administrator has physically connected at least one of 15 pairs of distinct fibers to the input port and at least one of the 15 pairs of distinct fibers to the output port (A, B, and/or C).

A.NOEVIL The administrators are appropriately trained, not careless, not willfully negligent, non-hostile and follow and abide by the instructions provided in the guidance documentation.

3.1.2 Physical Environment Assumptions

A.LOCATE The TOE will be located in a location that provides physical security commensurate with the value of the optical data the TOE is switching, uninterruptible power, and the temperature control necessary for the reliable operation of the hardware. Only administrators will have physical access to the TOE.

3.2 Threats

The TOE addresses the threats identified in this section. The threat agents are authorized persons/processes, unauthorized persons/processes, or external IT entities not authorized to use the TOE itself. The threats identified assume that the threat agent is a person with a low attack potential who possesses an average expertise, few resources, and low to moderate motivation.

3.2.1 Threats Addressed by the TOE

The TOE addresses the threats discussed below.

T.BYPASS An entity[3] may bypass the TOE security, circumventing nominal switch functionality causing optical data to travel between the wrong ports or causing the TOE configuration data to be configured insecurely.

T.CROSSTALK A remote entity[4] captures data from a separate network while the TOE is not connecting the network on which the remote entity resides to that separate network.

T.MALICIOUS A remote entity attempts to perform unauthorized activities on a device connected to one of the ports on the SSU while the TOE is connecting the port on which the remote entity resides to that device.

T.MISCONFIG An entity may be able to violate the site's security policies, causing optical data to travel between the wrong ports or causing the TOE configuration data to be configured insecurely because the TOE is not configured appropriately.

3.2.2 Threats Addressed by IT Environment

There are no threats addressed by the IT environment that are defined for this TOE.

3.3 Organisational Security Policies

There are no organizational security policies defined for this TOE.

[3] An entity is a untrusted or trusted user, process, IT product, or system outside the TOE that interacts with the TOE.

[4] A remote entity is an entity that does not reside on the TOE, but on a connected network.

4 Security Objectives

This chapter describes the security objectives for the TOE and the TOE's operating environment. The security objectives are divided between TOE Security Objectives (i.e., security objectives addressed directly by the TOE) and Security Objectives for the Operating Environment (i.e., security objectives addressed by the IT domain or by non-technical or procedural means).

4.1 Security Objectives For The TOE

This section defines the IT security objectives that are to be addressed by the TOE.

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

O.MANAGE The TOE will provide the functions and facilities necessary to support authorized users in the management of the switch.

O.SELF_PROT The TOE will maintain a domain for its own execution that protects itself and its resources from external interference, tampering or unauthorized disclosures.

O.SWITCH The TOE will provide the administrator with the ability to connect the Input (Common) Port to each of the three Output Ports, one at a time.

4.2 Security Objectives For The Environment

The non-IT security objectives for the environment 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.CONNECT The administrator has physically connected at least one of 15 pairs of distinct fibers to the input port and at least one of the 15 pairs of distinct fibers to the output port (A, B, and/or C).

OE.LOCATE The TOE will be located in a location that provides physical security commensurate with the value of the data the TOE is switching, uninterruptible power, and the temperature control necessary for the reliable operation of the hardware. Only authorized administrative users of the TOE will have physical access to the TOE.

OE.NOEVIL The administrators are appropriately trained, not careless, not willfully negligent, non-hostile and follow and abide by the instructions provided in the guidance documentation.

4.3 Mapping of Security Environment to Security Objectives

The following table represents a mapping of the threats, assumptions, and OSPs to the security objectives defined in this ST.

	A.CONNECT	A.LOCATE	A.NOEVIL	T.BYPASS	T.CROSSTALK	T.MALICIOUS	T.MISCONFIG
O.ISOLATION					X		
O.MANAGE							X
O.SELF_PROT				X			
O.SWITCH						X	
OE.CONNECT	X						
OE.LOCATE		X					
OE.NOEVIL			X				X

Table 2 – Assumptions, Threats & IT Security Objectives Mappings

4.4 Rationale For Threat Coverage

This section provides a justification that for each threat, the security objectives counter the threat.

T.BYPASS O.SELF_PROT mitigates this threat by ensuring that the TSF can protect itself from end users.

T.CROSSTALK O.ISOLATION mitigates this threat by providing isolation between ports. The only way for information to pass between the input port and the output ports is if the information flow is allowed by the TOE's information flow control policy. It is physically impossible for information to pass between the output ports.

T.MALICIOUS O.SWITCH mitigates this threat by providing switch functionality that allows the user to disconnect from a network on which malicious activities originate.

T.MISCONFIG O.MANAGE contributes to mitigating this threat by providing the necessary functions and facilities needed to manage the security policy of the TOE. OE.NOEVIL contributes to mitigating this threat by requiring administrators to be trained and to follow the instructions provided in the guidance documentation

4.5 Rationale For Organizational Policy Coverage

This ST has no Organizational Security Policies.

4.6 Rationale For Assumption Coverage

This section provides a justification that for each assumption, the security objectives for the environment cover that assumption.

The non-IT security objectives for the environment discussed below are, in part, a re-statement of the security assumptions. Therefore, the security objectives for the environment listed below obviously cover the corresponding assumption.

Assumption (Section 3.1)	**Non-IT Security Obejctive for the Environment (Section 4.2)**
A.CONNECT	OE.CONNECT
A.LOCATE	OE.LOCATE
A.NOEVIL	OE.NOEVIL

5 IT Security Requirements

The security requirements that are levied on the TOE are specified in this section of the ST. This ST does not define any security functional requirements to be levied on the IT environment. The security requirements levied on the TOE are defined in Sections 5.1 - 5.2.

TOE Security Functional Requirements (from CC Part 2)	
FDP_IFC.2	Complete Information Flow Control
FDP_IFF.1	Simple Security Attributes
FMT_SMF.1	Specification of Management Functions
FPT_PHP.1	Passive detection of physical attack
FPT_RVM.1	Non-bypassability of the TSP
FPT_SEP.1	TSF Domain Separation
Explicitly Stated TOE Security Functional Requirements	
FPT_ISO_EXP.1	Optical Isolation

Table 3 - Functional Requirements

5.1 TOE Security Functional Requirements

The SFRs defined in this section are taken from Part 2 of the CC.

5.1.1 User data protection (FDP)

5.1.1.1 FDP_IFC.2 Complete information flow control

FDP_IFC.2.1 The TSF shall enforce the **SSU flow control SFP** on

- **Subjects: Input port, Output ports (A, B, and C)**
- **Information: optical signals**

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.

5.1.1.2 FDP_IFF.1 Simple Security attributes

FDP_IFF.1.1 The TSF shall enforce the **SSU flow control SFP** based on the following types of subject and information security attributes: **switch configuration mode defined for the switch (input/output port pair).**

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:

information can only flow between the ports as defined by the switch configuration state, which only allows information flows between the Input port and at most one of the output ports (A, B, or C).

FDP_IFF.1.3 The TSF shall enforce the **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 authorize an information flow based on the following rules: **no explicit authorization rules**.

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

- **no information flow is allowed between output ports A, B, and C**
- **Default state is active (input port is not connected to any of the output ports)**

5.1.2 Security Management (FMT)

5.1.2.1 FMT_SMF.1 Specification of Management Functions

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

a. **Change the individual switch states (Manually configure switch states through the Front Panel of the SSU)**
b. **Configure programmable modes through the console port**
c. **Define user configurable modes through the Front Panel of the SSU**
d. **Store and recall (activate) a configuration mode through the Front Panel of the SSU**
e. **Report SSU functionality status via the Front Panel of the SSU**

5.1.3 Protection of TSF (FPT)

5.1.3.1 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 TSF's elements has occurred.

5.1.3.2 FPT_RVM.1 Non-bypassability of the TSP

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.

5.1.3.3 FPT_SEP.1 TSF Domain Separation

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.

5.2 Explicitly Stated TOE Security Functional Requirements

The SFRs defined in this section are explicitly stated and are derived from similar requirements in Part 2 of the CC.

5.2.1 Protection of TSF (FPT)

5.2.1.1 FPT_ISO_EXP.1 Optical Isolation

FPT_ISO_EXP.1.1 The TSF shall ensure that there is at least 60dB of optical isolation between all ports that are not connected by any of the 15 switch states.

5.3 TOE Strength of Function Claim

The TOE does not include any probabilistic or permutational mechanisms. As such, there is no claimed minimum strength of function for this TOE and there are no TOE security functional requirements that contain a probabilistic or permutational function.

5.4 TOE Security Assurance Requirements

The assurance security requirements for this Security Target are taken from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 4 as defined by the CC, augmented with AVA_CCA.1 and AVA_VLA.3, (EAL4+). The assurance components are summarized in the following table.

Assurance Class	Assurance Components	
ACM: Configuration management	ACM_AUT.1	Partial CM automation
	ACM_CAP.4	Generation support and acceptance procedures
	ACM_SCP.2	Problem tracking CM coverage
ADO: Delivery and operation	ADO_DEL.2	Detection of modification
	ADO_IGS.1	Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.2	Fully defined external interfaces
	ADV_HLD.2	Security enforcing high-level design
	ADV_IMP.1	Subset of the implementation of the TSF
	ADV_LLD.1	Descriptive low-level design
	ADV_RCR.1	Informal correspondence demonstration
	ADV_SPM.1	Informal TOE security policy model
AGD: Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
ALC: Life cycle support	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools

ATE: Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: high-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability assessment	AVA_CCA.1	Covert channel analysis
	AVA_MSU.2	Validation of analysis
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.3	Moderately resistant

Table 4 - Assurance Requirements: EAL4+

5.4.1 ACM_AUT.1 Partial CM automation

Developer action elements:

ACM_AUT.1.1D The developer shall use a CM system.

ACM_AUT.1.2D The developer shall provide a CM plan.

Content and presentation of evidence elements:

ACM_AUT.1.1C The CM system shall provide an automated means by which only authorised changes are made to the TOE implementation representation.

ACM_AUT.1.2C The CM system shall provide an automated means to support the generation of the TOE.

ACM_AUT.1.3C The CM plan shall describe the automated tools used in the CM system.

ACM_AUT.1.4C The CM plan shall describe how the automated tools are used in the CM system.

Evaluator action elements:

ACM_AUT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.2 ACM_CAP.4 Generation support and acceptance procedures

Developer action elements:

ACM_CAP.4.1D The developer shall provide a reference for the TOE.

ACM_CAP.4.2D The developer shall use a CM system.

ACM_CAP.4.3D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_CAP.4.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.4.2C The TOE shall be labeled with its reference.

ACM_CAP.4.3C The CM documentation shall include a configuration list, a CM plan, and an

acceptance plan.

ACM_CAP.4.4C The configuration list shall uniquely identify all configuration items that comprise the TOE.

ACM_CAP.4.5C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.4.6C The CM documentation shall describe the method used to uniquely identify the configuration items that comprise the TOE.

ACM_CAP.4.7C The CM system shall uniquely identify all configuration items that comprise the TOE.

ACM_CAP.4.8C The CM plan shall describe how the CM system is used.

ACM_CAP.4.9C The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

ACM_CAP.4.10C The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

ACM_CAP.4.11C The CM system shall provide measures such that only authorised changes are made to the configuration items.

ACM_CAP.4.12C The CM system shall support the generation of the TOE.

ACM_CAP.4.13C The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

Evaluator action elements:

ACM_CAP.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.3 ACM_SCP.2 Problem tracking CM coverage

Developer action elements:

ACM_SCP.2.1D The developer shall provide a list of configuration items for the TOE.

Content and presentation of evidence elements:

ACM_SCP.2.1C The list of configuration items shall include the following: implementation representation; security flaws; and the evaluation evidence required by the assurance components in the ST.

Evaluator action elements:

ACM_SCP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.4 ADO_DEL.2 Detection of modification

Developer action elements:

ADO_DEL.2.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.2.2D The developer shall use the delivery procedures.

Content and presentation of evidence elements:

ADO_DEL.2.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

ADO_DEL.2.2C The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site.

ADO_DEL.2.3C The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.

Evaluator action elements:

ADO_DEL.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.5 ADO_IGS.1 Installation, generation, and start-up procedures

Developer action elements:

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

ADO_IGS.1.1C The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation, and start-up of the TOE.

Evaluator action elements:

ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.4.6 ADV_FSP.2 Fully defined external interaces

Developer action elements:

ADV_FSP.2.1D The developer shall provide a functional specification.

Content and presentation of evidence elements:

ADV_FSP.2.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.2.2C The functional specification shall be internally consistent.

ADV_FSP.2.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions, and error messages.

ADV_FSP.2.4C The functional specification shall completely represent the TSF.

ADV_FSP.2.5C The functional specification shall include rationale that the TSF is completely represented.

Evaluator action elements:

ADV_FSP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.2.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.4.7 ADV_HLD.2 Security enforcing high-level design

Developer action elements:

ADV_HLD.2.1D The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

ADV_HLD.2.1C The presentation of the high-level design shall be informal.

ADV_HLD.2.2C The high-level design shall be internally consistent.

ADV_HLD.2.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.2.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.2.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.2.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.2.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.2.8C The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_HLD.2.9C The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

Evaluator action elements:

ADV_HLD.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.2.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.4.8 ADV_IMP.1 Subset of the implementation of the TSF

Developer action elements:

ADV_IMP.1.1D The developer shall provide the implementation representation for a selected subset of the TSF.

Content and presentation of evidence elements:

ADV_IMP.1.1C The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.

ADV_IMP.1.2C The implementation representation shall be internally consistent.

Evaluator action elements:

ADV_IMP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_IMP.1.2E The evaluator shall determine that the least abstract TSF representation provided is an accurate and complete instantiation of the TOE security functional requirements.

5.4.9 ADV_LLD.1 Descriptive low-level design

Developer action elements:

ADV_LLD.1.1D The developer shall provide the low-level design of the TSF.

Content and presentation of evidence elements:

ADV_LLD.1.1C The presentation of the low-level design shall be informal.

ADV_LLD.1.2C The low-level design shall be internally consistent.

ADV_LLD.1.3C The low-level design shall describe the TSF in terms of modules.

ADV_LLD.1.4C The low-level design shall describe the purpose of each module.

ADV_LLD.1.5C The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.

ADV_LLD.1.6C The low-level design shall describe how each TSP-enforcing function is provided.

ADV_LLD.1.7C The low-level design shall identify all interfaces to the modules of the TSF.

ADV_LLD.1.8C The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.

ADV_LLD.1.9C The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_LLD.1.10C The low-level design shall describe the separation of the TOE into TSP-enforcing

and other modules.

Evaluator action elements:

ADV_LLD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_LLD.1.2E The evaluator shall determine that the low-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.4.10 ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Content and presentation of evidence elements:

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

Evaluator action elements:

ADV_RCR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.11 ADV_SPM.1 Informal TOE security policy model

Developer action elements:

ADV_SPM.1.1D The developer shall provide a TSP model.

ADV_SPM.1.2D The developer shall demonstrate correspondence between the functional specification and the TSP model.

Content and presentation of evidence elements:

ADV_SPM.1.1C The TSP model shall be informal.

ADV_SPM.1.2C The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.

ADV_SPM.1.3C The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.

ADV_SPM.1.4C The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.

Evaluator action elements:

ADV_SPM.1.1E The evaluator shall confirm that the information provided meets all requirements for

content and presentation of evidence.

5.4.12 AGD_ADM.1 Administrator guidance

Developer action elements:

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

Content and presentation of evidence elements:

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

Evaluator action elements:

AGD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.13 AGD_USR.1 User guidance

Developer action elements:

AGD_USR.1.1D The developer shall provide user guidance.

Content and presentation of evidence elements:

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

Evaluator action elements:

AGD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.14 ALC_DVS.1 Identification of security measures

Developer action elements:

ALC_DVS.1.1D The developer shall produce development security documentation.

Content and presentation of evidence elements:

ALC_DVS.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.1.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

Evaluator action elements:

ALC_DVS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.1.2E The evaluator shall confirm that the security measures are being applied.

5.4.15 ALC_LCD.1 Developer defined life-cycle model

Developer action elements:

ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2D The developer shall provide life-cycle definition documentation.

Content and presentation of evidence elements:

ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

Evaluator action elements:

ALC_LCD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.16 ALC_TAT.1 Well-defined development tools

Developer action elements:

ALC_TAT.1.1D The developer shall identify the development tools being used for the TOE.

ALC_TAT.1.2D The developer shall document the selected implementation-dependent options of the development tools.

Content and presentation of evidence elements:

ALC_TAT.1.1C All development tools used for implementation shall be well-defined.

ALC_TAT.1.2C The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.

ALC_TAT.1.3C The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.

Evaluator action elements:

ALC_TAT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.17 ATE_COV.2 Analysis of coverage

Developer action elements:

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

Content and presentation of evidence elements:

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

Evaluator action elements:

ATE_COV.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.18 ATE_DPT.1 Testing: high-level design

Developer action elements:

ATE_DPT.1.1D The developer shall provide the analysis of the depth of testing.

Content and presentation of evidence elements:

ATE_DPT.1.1C The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

Evaluator action elements:

ATE_DPT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.19 ATE_FUN.1 Functional testing

Developer action elements:

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation of evidence elements:

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

Evaluator action elements:

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.20 ATE_IND.2 Independent testing - sample

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.4.21 AVA_CCA.1 Covert channel analysis

Developer action elements:

AVA_CCA.1.1D The developer shall conduct a search for covert channels for each information flow control policy.

AVA_CCA.1.1D The developer shall provide covert channel analysis documentation.

Content and presentation of evidence elements:

AVA_CCA.1.1C The analysis documentation shall identify covert channels and estimate their capacity.

AVA_CCA.1.2C The analysis documentation shall describe the procedures used for determining the existence of covert channels, and the information needed to carry out the covert channel analysis.

AVA_CCA.1.3C The analysis documentation shall describe all assumptions made during the covert channel analysis.

AVA_CCA.1.4C The analysis documentation shall describe the method used for estimating channel capacity, based on worst case scenarios.

AVA_CCA.1.5C The analysis documentation shall describe the worst case exploitation scenario for each individual covert channel.

Evaluator action elements:

AVA_CCA.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_CCA.1.2E The evaluator shall confirm that the results of the covert channel analysis show that the TOE meets its functional requirements.

AVA_CCA.1.3E The evaluator shall selectively validate the covert channel analysis through testing.

5.4.22 AVA_MSU.2 Validation of analysis

Developer action elements:

AVA_MSU.2.1D The developer shall provide guidance documentation.

AVA_MSU.2.1D The developer shall document an analysis of the guidance documentation.

Content and presentation of evidence elements:

AVA_MSU.2.1C The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AVA_MSU.2.2C The guidance documentation shall be complete, clear, consistent and reasonable.

AVA_MSU.2.3C The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.2.4C The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

AVA_MSU.2.5C The analysis documentation shall demonstrate that the guidance documentation is complete.

Evaluator action elements:

AVA_MSU.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_MSU.2.2E The evaluator shall repeat all configuration and installation procedures, and other procedures selectively, to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

AVA_MSU.2.3E The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

AVA_MSU.2.4E The evaluator shall confirm that the analysis documentation shows that guidance is provided for secure operation in all modes of operation of the TOE.

5.4.23 AVA_SOF.1 Strength of TOE security function evaluation

Developer action elements:

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

Content and presentation of evidence elements:

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the

specific strength of function metric defined in the PP/ST.

Evaluator action elements:

AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

5.4.24 AVA_VLA.3 Moderately resistant

Developer action elements:

AVA_VLA.3.1D The developer shall perform a vulnerability analysis.

AVA_VLA.3.2D The developer shall provide vulnerability analysis documentation.

Content and presentation of evidence elements:

AVA_VLA.3.1C The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for ways in which a user can violate the TSP.

AVA_VLA.3.2C The vulnerability analysis documentation shall describe the disposition of identified vulnerabilities.

AVA_VLA.3.3C The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.3.4C The vulnerability analysis documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

AVA_VLA.3.5C The vulnerability analysis documentation shall show that the search for vulnerabilities is systematic.

Evaluator action elements:

AVA_VLA.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.3.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure identified vulnerabilities have been addressed.

AVA_VLA.3.3E The evaluator shall perform an independent vulnerability analysis.

AVA_VLA.3.4E The evaluator shall perform independent penetration testing, based on the independent vulnerability analysis, to determine the exploitability of additional identified vulnerabilities in the intended environment.

AVA_VLA.3.5E The evaluator shall determine that the TOE is resistant to penetration attacks performed by an attacker possessing a moderate attack potential.

5.5 Rationale For TOE Security Requirements

5.5.1 TOE Security Functional Requirements

	O.ISOLATION	O. MANAGE	O. SELF_PROT	O. SWITCH
FDP_IFC.2				X
FDP_IFF.1				X
FMT_SMF.1		X		
FPT_PHP.1			X	
FPT_RVM.1			X	
FPT_SEP.1			X	
FPT_ISO_EXP.1	X			X

Table 5 – SFR and Security Objectives Mapping

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

FPT_ISO_EXP.1 requires that each port be isolated from the other ports with at least 60dB of optical isolation.

O.MANAGE The TOE will provide the functions and facilities necessary to support authorized users in the management of the switch.

FMT_SMF.1 requires that the TOE provide the capability to perform management functions to define configuration modes, change switch states, configure switch states, and store or recall configuration modes.

O.SELF_PROT The TOE will maintain a domain for its own execution that protects itself and its resources from external interference, tampering or unauthorized disclosures.

FPT_SEP.1 ensures that the TSF maintains a domain that protects itself from tampering by untrusted users and from interference that would prevent it from performing its functions. FPT_RVM.1 ensures that the functions are invoked and succeed before each function may proceed. FPT_PHP.1 provides for features that indicate when the TSF device has been physically tampered with.

O.SWITCH The TOE will provide the administrator with the ability to connect the Input (Common) Port to each of the three Output Ports, one at a time.

FDP_IFC.2 and FPD_IFF.1 define the SSU flow control SFP that requires switching to exist to create a point (input port) to point (output port) optical connection. FPT_ISO_EXP.1 requires that data cannot pass between the ports except as allowed by the SSU flow control SFP.

5.5.2 TOE Security Assurance Requirements

EAL4+ was chosen to provide a moderate level of independently assured security. The chosen assurance level is consistent with the threat environment. Specifically, that the threat of malicious attacks is not greater than moderate and the product will have undergone a search for flaws.

AVA_CCA.1 and AVA_VLA.3 were chosen to meet the needs of the target customers. The security environments in which this product is deployed typically have covert channel and strong vulnerability analysis requirements.

5.6 Rationale for Explicitly Stated Security Requirements

Table 6 presents the rationale for the inclusion of the explicit requirements found in this Security Target.

Explicit Requirement	Identifier	Rationale
FPT_ISO_EXP.1	Optical Isolation	This requirement is necessary because the CC does not contain an SFR that addresses isolation of data passing through optical ports.

Table 6 – Explicitly Stated SFR Rationale

5.7 Rationale For IT Security Requirement Dependencies

This section includes a table of all the security functional requirements and their dependencies and a rationale for any dependencies that are not satisfied.

Functional Component	Dependency	Included
FDP_IFC.2	FDP_IFF.1	Yes
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	Yes, via FDP_IFC.2 since FDP_IFC.2 is hierarchical to FDP_IFC.1. No. There are no objects or security attributes created by the switch that are used to enforce the SSU flow control SFP. The policy is enforced solely based on the corresponding switch configuration mode.
FMT_SMF.1	None	N/A
FPT_PHP.1	None	N/A
FPT_RVM.1	None	N/A
FPT_SEP.1	None	N/A
FPT_ISO_EXP.1	None	N/A

Table 7 – SFR Dependencies

5.8 Rationale For Internal Consistency and Mutually Supportive

The selected requirements are internally consistent. The ST includes all the SFRs provided by the TOE. All operations performed on the security requirements comply with the rules and intent required by the operation in the CC. The requirements defined in the ST are not contradictory.

The selected requirements together form a mutually supportive whole by:

- satisfying all dependencies as demonstrated in Table 7 – SFR Dependencies
- tracing security functional requirements to security objectives and justifying that tracing as demonstrated in Section 5.5.1
- including the SFRs FPT_SEP.1 and FPT_RVM.1 to protect the TSF
- including security management requirements to ensure that the TOE is managed and configured securely.

5.9 Rationale For Strength of Function Claim

This TOE does not claim a minimum strength of function because there are no probabilistic or permutational mechanisms provided by the TOE.

6 TOE Summary Specification

6.1 TOE Security Functions

6.1.1 Security Management

The TOE provides security management functions and tools to manage the security features it provides.

6.1.1.1 Security Management: FMT_SMF.1

The SSU provides the ability perform the following management functions on the SSU:

- Manually configure switch states using the Front Panel of the SSU
- Define programmable modes using the Console port by sending a string of configuration mode settings that conforms to a predefined format through the RS232 port
- Define User Configurable Modes through the Front Panel of the SSU
- Store and recall (activate) a configuration mode via the Front Panel of the SSU

The TOE allows for 16 total switch configuration modes:

- 1 reset mode (Permanent[5])
    - SSU will go through the startup procedures, setting all switches to off (default) state, and clear all User Configuration modes
- 5 predefined modes (Permanent)
    - Requires a firmware upgrade to change
- 9 programmable modes
    - Preprogrammed modes
        - Can be preprogrammed through the console port. Preprogrammed modes will be permanent until they are reprogrammed via the Console port.
    - User configurable modes
        - User Configurable modes are modes that are not preprogrammed and are stored in volatile memory
- 1 DiCon Reserved Mode (Permanent)

[5] Permanent modes can only be changed by a firmware change.

- Sets all switches to off state without resetting
- Only accessible via the internal I/O port

Administrators control the states of the switches using the front panel either by controlling individual duplex pairs or by recalling stored configuration modes. Individual switch channels are manually changed by pressing the button of the switch to be changed and pressing Enter when the desired channel LED is flashing. The Recall Select button on the Front panel is used to recall a configuration mode. Once all switches are set as desired, the Store Select and Confirm buttons on the Front panel are used to store a user configurable configuration mode.

The SSU front panel has 3 channel LEDs for each duplex pair which indicates which output port is currently active for each duplex pair.

The SSU Status Display shows the status of the overall functionality of the SSU, such as the readiness of operation (Ready), detection of faults (Fault), the usage of power (Power), and the usage of backup power (Backup). Each of these aspects of the SSU is indicated by the color of the corresponding LED. The faults detected include hardware component communication failures and checksum mismatches.

The status out pin on the front panel conveys the same information as the Fault LED, except when either the motherboard or user interface crashes. If either the motherboard or user interface crashes, the one that did not crash will signal a fault.

6.1.2 Switching

Switching provides an optical connection between two ports by providing a low-loss path for a light beam to travel between two ports. The TOE provides all-optical switching using MEMS micro-mirrors in which the switching action is controlled by tilting the mirrors to redirect light (optical) beams to the configured output fiber. The mirror tilting mechanism is controlled electronically by the drive voltage. This mechanism is proprietary. The signals are purely optical and the TOE does not alter, process, or store any information going through the optical fiber.

The switching mechanism does not allow information to flow between the output ports. In the "Default" state, the input port is not connected to any of the output ports and information flows are denied.

6.1.2.1 SSU Flow Control Policy: FDP_IFC.2, FDP_IFF.1

The flow of optical data through the switch is controlled by the switch configuration. Information cannot flow between the output ports (A, B, C). Information can only flow between the ports as defined by the switch configuration state, which only allows information flows between the Input port and at most one of the output ports (A, B, or C). In the Default state, the input port is not connected to any of the output ports, so no information flows are allowed.

6.1.3 Protection of TOE functions

The TOE provides detection of physical attacks and protection for itself from untrusted subjects and from subjects attempting to bypass the TSF. In addition, it provides the ability to isolate

ports from each other to ensure that the security functions are executed on the correct port. The protections are described in more detail below.

6.1.3.1 Detection of physical attacks: FPT_PHP.1

The TOE detects physical tampering attempts that might compromise the TSF by protecting all removable panels on the device with a tamper-evident seal. This tamper-evident seal will provide obvious signs of attempts to physically open the device.

6.1.3.2 Non-bypassability of the TSP: FPT_RVM.1

The TOE protects its management functions by physical security assumptions. The switching capabilities only allow information flow between input and output ports as defined by the switch configuration state. This information flow policy is always enforced, so the security functions cannot be bypassed.

6.1.3.3 TSF Domain Separation: FPT_SEP.1

Data (signals) passing to the TOE via the input port and output ports do not affect the operation of the TOE. The TOE does not alter process or store any information going through the optical fiber. Therefore, external entities cannot interfere with the switch mechanism configuration or operation, so domain separation is provided. Only administrators with access to the Front Panel or Console port can define and configure switch states.

6.1.3.4 Optical Isolation: FPT_ISO_EXP.1

The TOE provides the ability to isolate ports from each other to ensure that the security functions are executed on the correct port. Each of the 1x3 duplex pairs may connect the input port to only one output port (also referred to as channels) at a time. Isolation is provided by a "break-before-make" scheme using the On-Off switches as depicted in Figure 3: Duplex Pair.

The break-before-make scheme, while adding extra security to the SSU, is not necessary to meet the optical isolation specifications, and thus should not be considered a claim of this security target. The details of the break-before-make scheme are provided for informative purposes only.

When the SSU is first powered up, all switches are in the Default (no connect) state. To switch from Default state to A1 the duplex pair goes through the following sequence:

1. SW1 switches to OUT1.
2. SW2 goes from off to on

Since this is a duplex pair, the other 1x3 switch (SW5,6,7,8) go through the equivalent steps and go from Default state to A2.

To switch from A1 to B1, here are the steps:

1. SW2 goes from on to off
2. SW1 goes from OUT1 to OUT 2

3. SW3 goes from off to on.

Again the other 1x3 switch will automatically do the same thing. The two blocks move synchronously.

The TOE provides a minimum of 60 dB of optical isolation between all ports that are not connected by any of the 15 switch states.

6.2 Security Assurance Measures & Rationale

The documentation titles in the table below will be updated with new titles and version numbers during the course of the evaluation.

The assurance documents listed below were developed to meet the developer action and content and presentation of evidence elements for each assurance required defined in the CC.

Assurance Requirement	Assurance Measures	Assurance Rationale
ACM_AUT.1	*DiCon Fiberoptics Boeing SSU Configuration Management Document*	The CM plan defines the automated tools used in the CM system to ensure that only authorized changes are made to the TOE implementation representation and to generate the TOE. The CM plan also describes how these tools are used in the CM system
ACM_CAP.4	*DiCon Fiberoptics Boeing SSU Configuration Management Document*	The configuration management documents defines the configuration items(CIs), provides measures for ensuring that all changes to CIs are authorized and contains the necessary information to demonstrate that a CM system is used and that there is a unique reference for the TOE. A CM plan describes how the CM system is used and how it supports the TOE generation. An acceptance plan includes procedures to accept changes to the CIs. Evidence that the CM system is operating in accordance with the CM plan and that all configuration items are under CM control is also provided.
ACM_SCP.2	*DiCon Fiberoptics Boeing SSU Configuration Management Document*	The CI list provided includes the implementation representation, security flaws, and CC evaluation evidence.

Assurance Requirement	Assurance Measures	Assurance Rationale
ADO_DEL.2	*The Boeing Company P-8A Multi-Mission Maritime Aircraft Secure Switching Unit (MMA-SSU) Operation and Maintenance Manual*	The delivery document describes the steps performed to deliver the TOE. It describes the process used to create distribution copies of the TOE software and the steps taken to ensure consistent, dependable delivery of the TOE to the customer. Procedures for detecting modification or discrepancies between the master copy and the version received by the customer are described, along with procedures for detecting attempts to masquerade as the vendor (developer) when communicating with the customer.
ADO_IGS.1	*DiCon Fiberoptics Boeing SSU Installation, Generation and Start-up*	The installation, documents describe the steps necessary for secure installation, generation and start-up of the TOE.
ADV_FSP.2	*DiCon Fiberoptics Boeing SSU Common Criteria Evaluation Design Document* *The Boeing Company P-8A Multi-Mission Maritime Aircraft Secure Switching Unit (MMA-SSU) Operation and Maintenance Manual*	The informal functional specification (FSP) document identifies the external interfaces that completely represent the TSF and describes the purpose and method of use of all external TSF interfaces. It also describes details of all effects, exceptions, and error messages for each of the external TSF interfaces, as well as a rationale that the TSF is completely represented by the FSP.
ADV_HLD.2	*DiCon Fiberoptics Boeing SSU Common Criteria Evaluation Design Document* *The Boeing Company P-8A Multi-Mission Maritime Aircraft Secure Switching Unit (MMA-SSU) Operation and Maintenance Manual*	The security enforcing high-level design (HLD) describes the complete TSF in terms of subsystems, separating the TOE into TSP-enforcing and other subsystems. The security functions for each subsystem are described. The purpose and method of use for all subsystem interfaces are described and the externally visible interfaces are identified.
ADV_IMP.1	*DiCon Fiberoptics Boeing SSU Source Code*	A selected subset of the TSF implementation representation is provided at a level such that the TSF can be generated without further design decisions.
ADV_LLD.1	*DiCon Fiberoptics, Inc. SSU Version D Low-Level Design*	The descriptive low-level design describes the. complete TSF in terms of modules, separating the TOE into TSP-enforcing and other subsystems. The security functions for each subsystem are described. The purpose and method of use for all module interfaces are described and the externally visible interfaces are identified

Assurance Requirement	Assurance Measures	Assurance Rationale
ADV_RCR.1	*DiCon Fiberoptics Boeing SSU Common Criteria Evaluation Design Document*	The informal correspondence analysis demonstrates that the security functionality as described in the FSP and ST is correct and complete. Likewise for the functionality described in the FSP and HLD, in the HLD and LLD, and in the LLD and implementation representation.
ADV_SPM.1	*DiCon Fiberoptics Boeing SSU Informal Security Policy Model*	The informal TOE security policy model describes the rules and characteristics of all policies in the TSP, including a rationale demonstrating its consistency and correctness with the FSP.
AGD_ADM.1	DiCon Fiberoptics, Inc. SCD 7396 – Switch Control Instructions, Rev C, June 23, 2006. *The Boeing Company P-8A Multi-Mission Maritime Aircraft Secure Switching Unit (MMA-SSU) Operation and Maintenance Manual*	The administrator guidance documents provide complete administrative guidance for the TOE, including all security features and configuration items.
AGD_USR.1	N/A	The TOE is transparent to the entities sending optical data through the TOE and as such, there is no User Guide. Therefore, this SAR is vacuously satisfied (not applicable).
ALC_DVS.1	*DiCon Fiberoptics Boeing SSU Life Cycle Support*	The identification of security measures document describes the physical, procedural, personnel, and other security measures used to protect the confidentiality and integrity of the TOE design and implementation. Evidence that these measures are used will also be provided.
ALC_LCD.1	*DiCon Fiberoptics Boeing SSU Life Cycle Support*	The developer defined life-cycle model describes the model used to provide control over the development and maintenance of the TOE.
ALC_TAT.1	*DiCon Fiberoptics Boeing SSU Life Cycle Support*	The well-defined development tools document will define the development tools used to implement the TOE, as well as all statements and options used to develop the TOE
ATE_COV.2	*DiCon Fiberoptics Boeing SSU Test Analysis, Plan, Procedures and Results*	The test coverage analysis document provides a mapping of the test cases performed against the TSF, demonstrating that the correspondence between the TSF described in the FSP and the tests is complete.
ATE_DPT.1	*DiCon Fiberoptics Boeing SSU Test Analysis, Plan, Procedures and Results*	The depth of testing document demonstrates that the tests are sufficient to demonstrate that the TSF operates in accordance with the HLD.

Assurance Requirement	Assurance Measures	Assurance Rationale
ATE_FUN.1	*DiCon Fiberoptics Boeing SSU Test Analysis, Plan, Procedures and Results*	The functional testing document includes the test plans, test procedures, and associated test cases of the TOE functional testing effort.
ATE_IND.2	*Developer Test Plan* *TOE*	The TOE hardware, software, guidance, and testing documentation were made available to the CC testing laboratory for independent testing.
AVA_CCA.1	*DiCon Fiberoptics Boeing SSU Covert Channel Analysis*	The covert channel analysis identifies discovered covert channels and estimates their capacity. The document will describe the approach used to identify covert channels as well as the information needed to perform the analysis. It will also describe the worst case scenarios for the covert channels.
AVA_MSU.2	*DiCon Fiberoptics Boeing SSU Validation of Analysis* Guidance assurance measures identified in AGD_ADM.1	The misuse analysis document demonstrates that the guidance documentation is complete.
AVA_SOF.1	N/A	The TOE does not include any probabilistic or permutational mechanisms, so this SAR is vacuously satisfied (not applicable).
AVA_VLA.3	*DiCon Fiberoptics Boeing SSU Vulnerability Analysis*	The vulnerability analysis document identifies and describes the systematic process used to discover vulnerabilities, the results of the vulnerability analysis, and the mitigation of each identified vulnerability. It also justifies that the TOE is resistant to obvious penetration attacks.

Table 8 - Assurance Measures & Rationale: EAL4+

6.3 Rationale for TOE Security Functions

This section provides a table demonstrating the tracing of TOE security functions back to aspects of the security functional requirements (SFRs).

A justification that the security functions are suitable to cover the SFRs can be found in Section 6.1.

	Security Management	Switching	Protection of TOE functions
FDP_IFC.2		X	
FDP_IFF.1		X	
FMT_SMF.1	X		
FPT_PHP.1			X
FPT_RVM.1			X
FPT_SEP.1			X
FPT_ISO_EXP.1			X

Table 9 – TOE Security Function to SFR Mapping

6.4 Appropriate Strength of Function Claim

This TOE does not claim a minimum strength of function because there are no probabilistic or permutational mechanisms provided by the TSF.

7 Protection Profile Claims

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

8 Rationale

This section provides references to other sections of the ST that contain the corresponding rationales.

8.1 Security Objectives Rationale

Sections 4.3 - 4.6 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 6.2 - 6.4 provide the TOE summary specification rationale.

8.4 Protection Profile Claims Rationale

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

