MICROTECH M7245, M7246 and M7248 Security Target

Version 1.7
April 26, 2010

MICROTECH
8330 Boone Blvd., Suite 600
Vienna, VA 22182
http://www.MicroTech.net

DOCUMENT INTRODUCTION

Prepared By:

Common Criteria Consulting LLC
15804 Laughlin Lane
Silver Spring, MD 20906
http://www.consulting-cc.com

Prepared For:

MICROTECH
8330 Boone Blvd., Suite 600
Vienna, VA 22182
http://www.MicroTech.net

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the MICROTECH M7245 (Revision 7), M7246 (Revision 7) and M7248 (Revision 4). 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

Ver	Description
1.0	March 30, 2007 - Initial release
1.1	April 3, 2007 – Added information for M7248
1.2	April 5, 2007 – Updated the switch revision numbers
1.3	May 31, 2007 – Addressed OR 01
1.4	August 3, 2007 – Addressed OR 383-4-80-CB-OR-1.0
1.5	April 2, 2009- Added revision numbers and firmware versions to TOE’s
1.6	September 9, 2008 – Addressed OR 1.0
1.7	April 26, 2010 – Changed Sigcom name to MicroTech, Updated Photo’s of each unit, Updated TOE revision numbers, Isolation changed to 20dB for copper channels and -45dBM for fiber optic channels. Added Revision of HEX file code version for each TOE

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS LIST

ASCII	**American Standard Code for Information Interchange**
CC	**Common Criteria**
CM	**Configuration Management**
EAL4	**Evaluation Assurance Level 4**
IT	**Information Technology**
LED	**Light Emitting Diode**
PP	**Protection Profile**
SF	**Security Function**
SFP	**Security Function Policy**
SOF	**Strength of Function**
ST	**Security Target**
TOE	**Target of Evaluation**
TSC	**TSF Scope of Control**
TSF	**TOE Security Function**
TSFI	**TSF Interface**
TSP	**TOE Security Policy**

CHAPTER 1

1. Security Target Introduction

This Security Target (ST) describes the objectives, requirements and rationale for the MICROTECH M7245 (Revision 7), M7246 (Revision 7) and M7248 (Revision 4). The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation, Version 2.3*, the ISO/IEC JTC 1/SC27, *Guide for the Production of PPs and STs, Version 0.9* and all international interpretations through 5 April 2007. As such, the spelling of terms is presented using the internationally accepted English.

1.1 Security Target Reference

MICROTECH M7245, M7246 and M7248 Security Target, Version 1.7, dated April 23, 2010

1.2 TOE Reference

MICROTECH M7245 (Revision 7), M7246 (Revision 7) and M7248 (Revision 4).

1.3 Evaluation Assurance Level

Assurance claims conform to EAL4 (Evaluation Assurance Level 4) from the *Common Criteria for Information Technology Security Evaluation, Version 2.3*.

1.4 Keywords

Switch, Secure Switch, Optical Switch, Fiber Optic, Fiber Optic, Duplex.

1.5 TOE Overview

This Security Target defines the requirements for the MICROTECH M7245 (Revision 7), M7246 (Revision 7) and M7248 (Revision 4). The TOE provides switching functionality for two independently controlled data channels. Each data channel provides the ability to switch a Common port to one of two switch ports, or to a cutoff position which disables all connectivity between the Common and switch ports. The TOE security functionality consists of switching between the ports, isolation between the switch ports, management of the switching functionality, and self protection.

1.5.1 Security Target Organisation

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

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

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

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

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

Chapter 6 is the TOE Summary Specification, a description of the functions provided by the TOE to satisfy the security functional and assurance requirements.

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

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

1.6 Common Criteria Conformance

The MICROTECH M7245 (Revision 7), M7246 (Revision 7) and M7248 (Revision 4) is compliant with the Common Criteria (CC) Version 2.3, functional requirements (Part 2) extended and assurance requirements (Part 3) conformant for EAL4.

1.7 Protection Profile Conformance

The MICROTECH M7245 (Revision 7), M7246 (Revision 7) and M7248 (Revision 4) does/does not claim conformance to any registered Protection Profile.

1.8 Conventions

The CC defines operations on security requirements. The font conventions listed below state the conventions used in this ST to identify the operations.

Assignment: indicated in underlined text

Selection: indicated in italics

Assignments within selections: indicated in italics and underlined text

Refinement: indicated with bold text

Iterations of security functional requirements may be included. If so, iterations are specified at the component level and all elements of the component are repeated. Iterations are identified by numbers in parentheses following the component or element (e.g., FAU_ARP.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 Product Description

The MICROTECH M7245 (revision 7), M7246 (revision 7) and M7248 (revision 4) are three models in a family of rack mountable dual channel switches that operate at the physical layer. Each model provides two independently switched data channels. A Common port for each channel is switched between one of two switched ports (labeled "SECURE" and "NON-SECURE" on the M7245 and M7246 and "A" and "B" on the M7248) or a cutoff position (the common and switched ports are all isolated from one another). The following table summarizes the specifics of the data channels on the models.

Table 1 - Switched Data Channel Summary

Model	Data Channel 1	Data Channel 2
M7245 (revision 7)	RS530 Common port: DB25 Female Switched ports: DB25 Male Connects all 25 pins	10/100 Base-T on the Common side; Fiber optic 1300 nm on the switched side Common port: RJ45 Jack Switched ports: ST Connects Receive Data and Transmit Data
M7246 (revision 7)	RS530 Common port: DB25 Male Switched ports: DB25 Female Connects all 25 pins	Copper Common port: RJ45 Jack Switched ports: RJ45 Jack Connects all 8 pins
M7248 (revision 4)	RS530 Common port: DB25 Female Switched ports: DB25 Male Connects all 25 pins	RS530 Common port: DB25 Male Switched ports: DB25 Female Connects all 25 pins

With the M7245, data channel 2 provides electrical to optical conversion (and vice versa) in addition to switching.

The switches may be controlled locally by manually operating the front panel push buttons or remotely from the DB9 Control port located on the rear of the unit using either contact closures or an RS-232 ASCII command interface. The front panel LED displays indicate the respective switch position of each data channel and unit power status.

The following figures present front and rear views of the three switch models.

Figure 1 - M7245 Front View

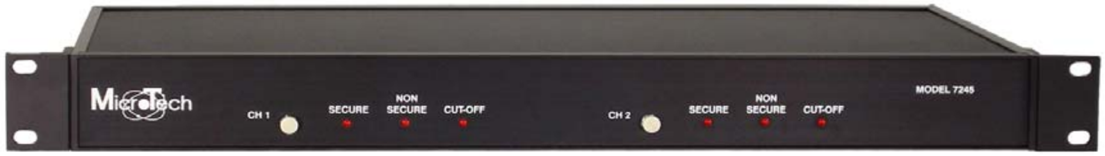


Figure 2 - M7245 Rear View

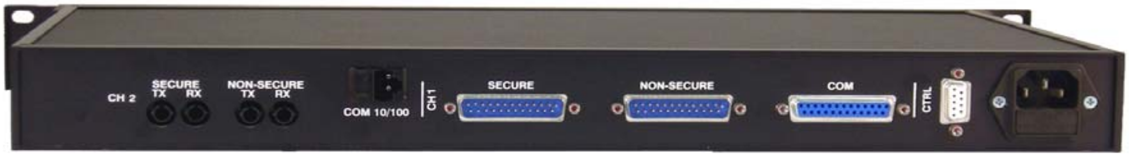


Figure 3 - M7246 Front View

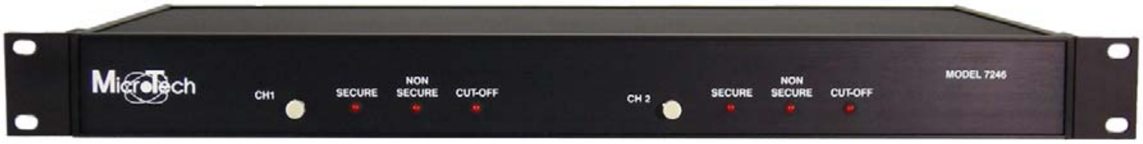


Figure 4 - M7246 Rear View

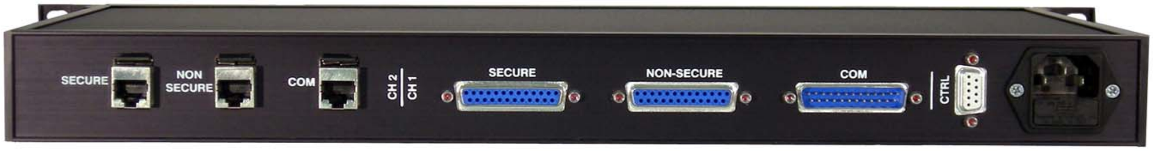


Figure 5 - M7248 Front View

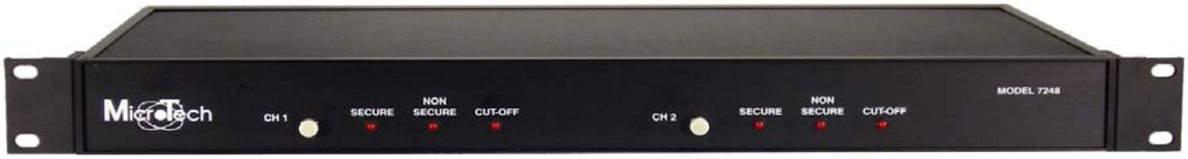
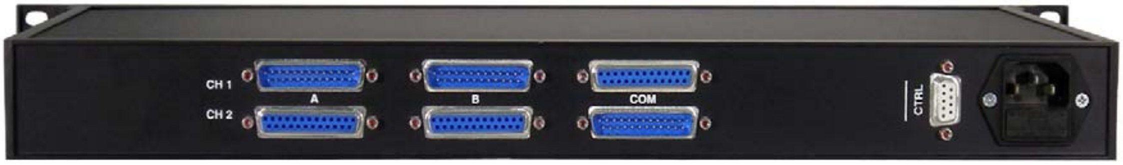


Figure 6 - M7248 Rear View



2.2 Physical Boundary

The physical boundary of the TOE is the complete switch (M7245, M7246 or M7248), including all software and firmware.

2.3 Logical Boundary

All of the switch models provide the same security functionality. The only difference between the models is in the channel type of data channel 2 and the physical interfaces of data channel 1.

The security functionality of each switch model is Switching, Isolation, Management, and Self Protection.

2.3.1 Switching

The TOE switches data signals between the Common ports of each of the data channels and the configured destination: the SECURE/A port, the NON_SECURE/B port, or the cutoff position. When the SECURE/A or NON-SECURE/B port is not configured to be the switched destination of the Common port, those ports have no connectivity to the Common port. When the unit is powered off, the SECURE/A and NON-SECURE/B ports have no connectivity to the Common port. There is no connectivity between any ports of different data channels.

2.3.2 Isolation

The TOE is implemented so that all of the ports of similar type (electrical or fiber optic) are isolated from one another within the TOE.

2.3.3 Management

An administrator may control the switch settings for each of the data channels. The administrator may configure the current switch settings as well as the default settings to be used on power up of the TOE. The administrator may disable the front panel push buttons.

2.3.4 Self Protection

The TOE protects itself from bypass or interference involving actions within the TSC.

2.4 TSF Data

The TOE maintains the following TSF data:

1. Currently configured switch setting for each of the data channels.
2. Default switch setting for each of the data channels to be used on power up of the TOE.
3. State of the front panel push button functionality (enabled/disabled) for each data channel.

2.5 Evaluated Configuration

The evaluated configuration consists of a single unit of any of the three switch models.

M7245 (revision 7) with firmware version 724XF.HEX Ver 2.0 on the fiber board and 724XR.HEX Ver 2.0 on the relay, M7246 (revision 7) with firmware version 724XR.Hex. Ver 2.0, or M7248 (revision 4) with firmware version 724XR.HEX Ver 2.0.

CHAPTER 3

3. Security Environment

3.1 Introduction

This chapter defines the nature and scope of the security needs to be addressed by the TOE. Specifically this chapter identifies:

A) assumptions about the environment,

B) threats to the assets and

C) organisational security policies.

This chapter identifies assumptions as A.*assumption*, threats as T.*threat* and policies as P.*policy*.

3.2 Assumptions

The specific conditions listed in the following table are assumed to exist in the TOE environment.

Table 2 - Assumptions

A.Type	Description
A.ADMINACCESS	Access to the TOE’s serial interface is restricted to authorized administrators. If the front panel push buttons are enabled, access to the front panel is also restricted to authorized administrators.
A.ENVIRON	The TOE will be located in an environment that provides physical security and temperature control required for reliable operation.
A.INSTALL	The Administrator will install and configure the TOE according to the administrator guidance.
A.NOEVILADMIN	Administrators are non-hostile and follow the administrator guidance when using the TOE. Administration is competent and on-going.
A.USER	Users connected to any of the data channel interfaces of the TOE are assumed to possess the necessary privileges to access any information made accessible to them via the TOE switch configuration.

3.3 Threats

The threats identified in the following table are addressed by the TOE.

Table 3 - Threats

T.Type	TOE Threats
T.TSF_COMPROMISE	A user or process may cause, through an unsophisticated attack, TSF data or executable code to be modified without authorization.
T.DATACOMPROMISE	A malicious user connected to one data channel interface of the TOE may gain unauthorized access to data via a different data channel interface to which an administrator has not configured connectivity.

3.4 Organisational Security Policies

The organizational security policies identified in the following table are addressed by the TOE and/or the IT environment.

Table 4 - Organisational Security Policies

P.Type	Organisational Security Policies
P.CUTOFF	When a switch is configured to be in the cutoff position for a data channel, the TOE disables all connectivity between the Common, SECURE/A and NON-SECURE/B ports of that data channel.
P.ISOLATE	The TOE shall ensure isolation of similar type of at least 20 dB between copper ports. -45dBM isolation for Fiber ports. (electrical or fiber optic).
P.MANAGE	The TOE shall provide management capabilities to permit an administrator to configure the switch settings for each data channel.

CHAPTER 4

4. Security Objectives

This section identifies the security objectives of the TOE, the TOE's IT environment and the TOE's non-IT environment. The security objectives identify the responsibilities of the TOE, the TOE's IT environment, and the TOE's non-IT environment in meeting the security needs. Objectives of the TOE are identified as *O.objective*. Objectives that apply to the IT environment are designated as *OE.objective*. Objectives that apply to the non-IT environment are designated with an *ON.objective*.

4.1 Security Objectives for the TOE

The TOE must satisfy the following objectives.

Table 5 - Security Objectives for the TOE

O.Type	Security Objective
O.ISOLATE	The TOE shall ensure isolation of similar type of at least 20 dB between copper ports. -45dBM isolation for Fiber ports. (electrical or fiber optic).
O.LIMITCONNECTIVITY	The TOE shall limit connectivity between data channel ports to the switch configuration specified by the administrator.
O.MANAGE	The TOE shall provide administrators with the management functionality necessary to control the switching functionality provided by the TOE.
O.SELF_PROTECT	The TSF shall maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure.

4.2 Security Objectives for the IT Environment

No objectives are applicable to the TOE's IT environment.

4.3 Security Objectives for the Non-IT Environment

The TOE's Non-IT environment must satisfy the following objectives.

Table 6 - Security Objectives for the Non-IT Environment

ON.Type	Security Objectives for the Non-IT Environment
ON.ADMINACCESS	The administrator will install the TOE in such a way that access to the serial interface for management is restricted to authorized administrators. If the front panel push buttons are enabled, physical access to those buttons is also restricted to authorized administrators.
ON.ENVIRON	The administrator will install the TOE in an environment that provides physical security, uninterruptible power, and temperature control required for reliable operation.
ON.INSTALL	The administrator will install and configure the TOE according to the administrator guidance.
ON.NOEVILADMIN	Administrators are non-hostile and follow the administrator guidance when using the TOE. Administration is competent and on-going.
ON.USER	The administrator will only connect users to the data channel ports and configure the data channel port switching consistent with access privileges of the users.

CHAPTER 5

5. IT Security Requirements

This section contains the functional requirements that are provided by the TOE. These requirements consist of functional components from Part 2 of the CC.

5.1 TOE Security Functional Requirements

The functional requirements are described in detail in the following subsections. Requirements of the form Fxx_xxx are derived verbatim from Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 2.3* with the exception of completed operations. Explicitly stated functional requirements are of the form Fxx_xxx_EXP.

5.1.1 User Data Protection (FDP)

5.1.1.1 FDP_IFC.1 Subset Information Flow Control

FDP_IFC.1.1 The TSF shall enforce the Switch Flow Control Policy on

a) Subjects: Physical interfaces on the data channels (Common, SECURE/A, NON_SECURE);

b) Information: Electrical and/or optical signals received on the physical interfaces of the data channels;

c) Operation: Forwarding signals between 2 physical interfaces.

5.1.1.2 FDP_IFF.1 Simple Security Attributes

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

a) Subjects: Common, SECURE/A, and NON-SECURE/B interfaces; security attribute: configured switch setting;

b) Information: Electrical and/or optical signals; security attribute: none.

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) If the switch setting is CUTOFF, no information flow is allowed between any of the three interfaces.

b) If the switch setting is SECURE/A, information is permitted to flow in both directions between the Common and SECURE/A interfaces. No information flow is permitted between the Common and NON-SECURE/B interface.

c) If the switch setting is NON-SECURE/B, information is permitted to flow in both directions between the Common and NON-SECURE/B interfaces. No information flow is permitted between the Common and SECURE/A interface.

FDP_IFF.1.3 The TSF shall enforce the no other rules.

FDP_IFF.1.4 The TSF shall provide the following no other capabilities.

FDP_IFF.1.5 The TSF shall explicitly authorise an information flow based upon the following rules: none.

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

a) Information flow between the SECURE/A and NON-SECURE/B interfaces is never permitted.

b) Information flow between interfaces of different data channels is never permitted.

5.1.1.3 FDP_ISO_EXP.1 Isolation

Rationale for explicitly stated SFR: Part 2 of the CC does not include any SFRs addressing isolation between ports of the data channels. It has been specified as a member of the Data protection class because it involves a form of information flow.

FDP_ISO_EXP.1.1 The TOE shall ensure isolation of similar type of at least 20 dB between copper ports and -45dBM isolation for Fiber ports. (electrical or fiber optic).

Application Note: This SFR applies to all ports of similar type (electrical and fiber optic).

5.1.2 Security Management (FMT)

5.1.2.1 FMT_MOF.1 Management of Security Functions Behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to *determine the behaviour of, disable, enable* the functions front panel push button operation to the administrator.

5.1.2.2 FMT_MSA.1 Management of Security Attributes

FMT_MSA.1.1 The TSF shall enforce the Switch Flow Control Policy to restrict the ability to *query, modify* the security attributes configured switch setting for each data channel to the administrator.

5.1.2.3 FMT_MSA.2 Secure Security Attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

5.1.2.4 FMT_MSA.3 Static Attribute Initialisation

FMT_MSA.3.1 The TSF shall enforce the Switch Flow Control Policy to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the administrator to specify alternative initial values to override the default values when an object or information is created.

Application Note: Initially the TOE is configured for CUTOFF for each data channel on power up; this is considered a restrictive setting. For this SFR, information is considered to be created when the TOE powers up.

5.1.2.5 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to *query, modify* the

a) Switch configuration setting for each data channel,

b) Switch configuration power up setting for each data channel,

c) Front panel push buttons enabled/disabled for each data channel to the administrator.

5.1.2.6 FMT_MTD.3 Secure TSF Data

FMT_MTD.3.1 The TSF shall ensure that only secure values are accepted for TSF data.

5.1.2.7 FMT_SMF.1 Specification of Management Functions

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

a) Configure the switch setting for each data channel,

b) Configure the switch power up setting for each data channel,

c) Enable/disable the functionality of the front panel push buttons for each data channel.

5.1.2.8 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles administrator and user.

Application Note: In this context, users refer to entities connected to the TOE via any of the data channel interfaces. The presence of the TOE is transparent to users. Administrators use the serial interface or front panel push buttons to control and monitor the operation of the TOE.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.1.3 Protection of the TSF (FPT)

5.1.3.1 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.

5.1.3.2 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 Security Requirements for the IT Environment

No security requirements are levied on the IT Environment.

5.3 TOE Security Assurance Requirements

The TOE meets the assurance requirements for EAL4. These requirements are summarized in the following table.

Table 7 - EAL4 Assurance Requirements

Assurance Class	Component ID	Component Title
Configuration Management	ACM_AUT.1	Partial CM automation
	ACM_CAP.4	Generation support and acceptance procedures
	ACM_SCP.2	Problem tracking CM coverage
Delivery and Operation	ADO_DEL.2	Detection of modification
	ADO_IGS.1	Installation, Generation, and Start-Up Procedures
Development	ADV_FSP.2	Fully defined external interfaces

Assurance Class	Component ID	Component Title
	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
Guidance Documents	AGD_ADM.1	Administrator Guidance
	AGD_USR.1	User Guidance
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
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
Vulnerability Assessment	AVA_MSU.2	Validation of analysis
	AVA_SOF.1	Strength of TOE Security Function Evaluation
	AVA_VLA.2	Independent vulnerability analysis

5.4 Strength of Function for the TOE

No probabilistic or permutational mechanisms are included in the TOE. The overall SOF claim for the TOE is SOF-Basic.

5.5 CC Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified SFRs include the appropriate hierarchy and dependencies. The following table lists the TOE SFRs and the SFRs each are hierarchical to, dependent upon and any necessary rationale.

Table 8 - TOE SFR Dependency Rationale

SFR	Hierarchical To	Dependency	Rationale
FDP_IFC.1	No other components.	FDP_IFF.1	Satisfied
FDP_IFF.1	No other components.	FDP_IFC.1, FMT_MSA.3	Satisfied Satisfied
FDP_ISO_EXP.1	No other components.	None	n/a
FMT_MOF.1	No other components.	FMT_SMF.1, FMT_SMR.1	Satisfied Satisfied
FMT_MSA.1	No other components.	[FDP_ACC.1 or FDP_IFC.1], FMT_SMF.1 FMT_SMR.1	Satisfied Satisfied Satisfied
FMT_MSA.2	No other components.	ADV_SPM.1, [FDP_ACC.1 or FDP_IFC.1], FMT_MSA.1, FMT_SMR.1	Satisfied Satisfied Satisfied Satisfied
FMT_MSA.3	No other components.	FMT_MSA.1, FMT_SMR.1	Satisfied Satisfied
FMT_MTD.1	No other components.	FMT_SMF.1, FMT_SMR.1	Satisfied Satisfied
FMT_MTD.3	No other components.	ADV_SPM.1, FMT_MTD.1	Satisfied Satisfied

SFR	Hierarchical To	Dependency	Rationale
FMT_SMF.1	No other components.	None	n/a
FMT_SMR.1	No other components.	FIA_UID.1	Not satisfied. Rationale: All access to the TOE via the front panel push buttons or serial interface is assumed to be by an administrator (A.ADMINACCESS). All access to the TOE via any data channel interface is (by definition) by a user. The role for any user is inherent in the interface being used and identification is not required in this environment.
FPT_RVM.1	No other components.	None	n/a
FPT_SEP.1	No other components.	None	n/a

CHAPTER 6

6. TOE Summary Specification

6.1 Security Functions

6.1.1 Switching

Each of the models of the TOE provide two (2) independently switched data channels. Each data channel includes a Common port that may be switched to either of the SECURE/A or NON-SECURE/B ports. The data channel may also be configured for CUTOFF, meaning the Common port is not switched to either the SECURE/A or NON-SECURE/B port.

The nature of the switching function varies based on the types of interfaces supported on the each data channel:

1. RS530 Copper – All 25 pins on the Common port are electrically connected to the same pin on the SECURE/A or NON-SECURE/B port (or none for the CUTOFF position)
2. RJ45 Copper – The Transmit Data and Receive Data pins on the Common port are electrically connected to the same pin on the SECURE/A or NON-SECURE/B port.
3. RJ45 Copper/Fiber Optic ST – Electrical signals from the Receive Data pins on the RJ45 port are converted to fiber optic signals are transmitted via the TX ST connector on the SECURE/A or NON-SECURE/B port. Fiber optic signals on the RX ST connector of the SECURE/A or NON-SECURE/B port are converted to electrical signals and transmitted out the Receive Data pins of the RJ45 Common port. When configured for the CUTOFF position, no information is transmitted out the Receive Data pins on the Common port of the TX ST connectors of the SECURE/A and NON-SECURE/B ports.

At any given time, the Common port may be switched to at most one other port (or it may be in the CUTOFF configuration). The SECURE/A and NON-SECURE/B ports are never connected to one another. If power to the TOE is removed, the switches for both data channels automatically move to the CUTOFF position.

There is no connectivity between ports of the two different data channels.

6.1.2 Isolation

The TOE is implemented so that all of the ports of similar type (electrical or fiber optic) are isolated from one another within the TOE. The TOE provides a minimum isolation of 20 dB between all ports copper ports and -45dBM for Fiber ports.

6.1.3 Management

An administrator may control the operation of the TOE. All input from the administrator is validated to ensure the values being specified for any configurable parameter are appropriate. Three distinct management mechanisms are available:

1. ASCII commands via the serial interface – commands may be issued to configure the current and/or power up switch settings for each of the data channels, and to enable/disable the front panel push buttons. The administrator may also issue commands to view the configurable settings. Responses are returned via the serial interface to indicate actions taken in response to commands entered. A message is also transmitted via this interface when a switch setting is changed via the front panel push buttons.
2. Contact connections via the serial interface – three pins on the connector are used for each data channel. One pin is used to indicate the contact connection mechanism is in use; the remaining pins are edge sensitive and indicate the switch configuration for a data channel. No feedback is provided when using this mechanism. This mechanism can't be used to configure the switch power up setting or to enable/disable the front panel push buttons.
3. Front panel push buttons – two front panel push buttons are present on the TOE, one for each data channel. The front panel push buttons are used by simply pressing and holding the button corresponding to the data channel the administrator wants to configure. The LEDs for the switch positions for the corresponding data channel ("SECURE"/"A", "NONSECURE"/"B" or "CUTOFF") will light up in a rotating manner with a half-second interval between each LED. When the button is released, the LED currently lit will flash. The user then has up to 5 seconds to push and release the button to confirm the new switch position. If no confirming button push is made, the switch will revert to its last set position. Upon a manual switch change, the unit sends ASCII text over the RS-232 interface to notify the user of the new switch position just as if the user made the switch with the Remote ASCII Commands.

With each mechanism, the TOE validates the input from the administrator to ensure that only appropriate settings may be specified for each configurable value. These mechanisms may be used to configure the following:

1. Switch setting for data channel 1 – SECURE/A, NON-SECURE/B or CUTOFF
2. Switch setting for data channel 2 – SECURE/A, NON-SECURE/B or CUTOFF
3. Power up switch setting for data channel 1 – SECURE/A, NON-SECURE/B, CUTOFF, or resume the last switch setting prior to power off
4. Power up switch setting for data channel 2 – SECURE/A, NON-SECURE/B, CUTOFF, or resume the last switch setting prior to power off
5. Enable/disable the front panel push buttons for data channel 1
6. Enable/disable the front panel push buttons for data channel 2

Initially the power up switch setting for both data channels is CUTOFF.

6.1.4 Self Protection

The TOE provides for self protection and non-bypassability of functions within the TOE's scope of control (TSC). The TOE controls actions carried out by an administrator by implementing well defined administrator interfaces and validating the configuration values supplied during a session. Users have only passive interaction with the TOE and are not able to influence operation of the TOE. By maintaining and controlling administrator and user interactions, the TOE ensures that no security functions within the TSC are bypassed. Since the TOE is a stand-alone system with no support for general purpose users interacting actively with the TOE, it inherently maintains a separate domain for its own execution that prevents the TOE from being interfered with or tampered with. No mechanism is available to modify the TOE firmware via the TSFIs.

6.2 Assurance Measures

The following table provides a high-level description of the documents that satisfy each of the security assurance requirements.

Table 9 - EAL4 Assurance Measures

Assurance Class	Component ID	Documentation Satisfying Component
Configuration Management	ACM_AUT.1	Configuration Management Plan The developer performs configuration management on configuration items of the TOE. Automated processes are utilized to ensure that only authorized changes are made.
	ACM_CAP.4	Configuration Management Plan The developer performs configuration management on configuration items of the TOE. Configuration management is performed on the TOE, the implementation representation of the TOE, security flaws pertinent to the TOE, and all documentation submitted as evidence for the CC evaluation. The configuration items are uniquely identified and each release of the TOE has a unique reference. The processes include an acceptance plan that describes the procedures used to accept modified or newly created configuration items as part of the TOE.
	ACM_SCP.2	Configuration Item List The Configuration Items include the TOE, the implementation representation of the TOE, security flaws pertinent to the TOE, and all documentation submitted as evidence for the CC evaluation.
Delivery and Operation	ADO_DEL.2	Delivery Processes and Procedures The developer documents the delivery procedure for the TOE to include how components of the TOE are delivered to the user. The delivery procedure detail how the end-user may determine if they have the TOE and if the integrity of the TOE has been maintained.
	ADO_IGS.1	Installation Document The developer documents the installation, generation, and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.
Development	ADV_FSP.2	Functional Specification The external TSFIs are fully documented along with the description of the security functions and a correspondence between the interfaces and the security functions.

Assurance Class	Component ID	Documentation Satisfying Component
	ADV_HLD.2	High Level Design The subsystems of the TOE are documented in the High Level Design. The TOE identifies the TSP-enforcing subsystems and provides interface details for those subsystems.
	ADV_IMP.1	Source Code and Schematics The source code for the switch firmware and the schematics for the switches provide the implementation representation.
	ADV_LLD.1	Low Level Design The Low Level Design provides a description of the internal workings of the TSF in terms of modules and their interrelationships and dependencies. For each module of the TSF, the Low Level Design describes its purpose, function, interfaces, dependencies, and the implementation of any TSP-enforcing functions.
	ADV_RCR.1	Correspondence Mapping The Correspondence Mapping between the various TSF representations addresses the correct and complete instantiation of the requirements starting with the ST and continuing to the implementation representation.
	ADV_SPM.1	Security Policy Model The Security Policy Model describes the correspondence between the functional specification, the security policy model, and the policies of the TSP.

Guidance Documents	AGD_ADM.1	Operation Guide: Model 7245 (revision 3) Dual Channel RS-530 Secure/Non-Secure Switch With Cutoff And Fiber Optic St Duplex Secure/Nonsecure Switch/Converter With Cutoff w/ Remote Control Port;
		Operation Guide: Model 7246 (revision 4) Dual Channel RS-530 Secure/Non-Secure Switch With Cutoff And RJ45 Secure/Non-Secure Switch With Cutoff w/ Remote Control Port;
		Operation Guide: Model 7248(revision 2) Dual Channel RS-530 A/B Switch With Cutoff w/ Remote Control Port
		The administrative guidance is detailed to provide descriptions of how administrative users of the TOE can securely administer the TOE using those functions and interfaces detailed in the guidance.

	AGD_USR.1	n/a The TOE is transparent to users of the TOE. No instructions, guidance or warnings to the users are necessary. Therefore, user guidance is not necessary.
Life Cycle Support	ALC_DVS.1	Life Cycle Document The developer implements development security mechanisms during the development and maintenance of the TOE.
	ALC_LCD.1	Life Cycle Document The Life Cycle Document defines the procedures, tools and techniques used to develop and maintain the TOE.

Assurance Class	Component ID	Documentation Satisfying Component
	ALC_TAT.1	Life Cycle Document, Development Tool Documentation The Life Cycle Document identifies all tools used in the development of the TOE. The documentation for those tools defines all statements and options used.
Tests	ATE_COV.2	Test Plan The developer demonstrates the external interfaces tested during functional testing using a coverage analysis. The analysis includes information describing how the interfaces are tested.
	ATE_DPT.1	Test Plan The developer demonstrates the internal subsystem interfaces tested during functional testing using a depth analysis. The analysis includes information describing how the interfaces are tested.
	ATE_FUN.1	Test Plan, Test Procedures, Test Results The developer functional testing documentation contains a test plan, a description of the tests, along with the expected and actual results of the test conducted against the functions specified in the ST.
	ATE_IND.2	Test Plan, Test Procedures, Functional Specification, Operation Guides The developer documentation provides the necessary information for the evaluators to develop independent tests.
Vulnerability Assessment	AVA_MSU.2	Operation Guides, Installation Document, Functional Specification The documentation provides descriptions of how administrators of the TOE can correctly administer the TOE.
	AVA_SOF.1	n/a The TOE does not contain any probabilistic or permutational mechanisms and does not include any security mechanisms with strength of function claims. Therefore, no strength of function analysis is required.
	AVA_VLA.2	Vulnerability Analysis The developer documents their vulnerability analysis search for flaws and weaknesses in the TOE.

6.3 Strength of Function Claim

No probabilistic or permutational mechanisms are included in the TOE. The overall SOF claim for the TOE is SOF-Basic.

CHAPTER 7

7. Protection Profile Claims

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

7.1 Protection Profile Reference

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

7.2 Protection Profile Refinements

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

7.3 Protection Profile Additions

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

7.4 Protection Profile Rationale

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

CHAPTER 8

8. Rationale

This chapter provides the rationale for the selection of the IT security requirements, objectives, assumptions and threats. It shows that the IT security requirements are suitable to meet the security objectives, Security Requirements, and TOE security functional.

8.1 Rationale for IT Security Objectives

This section of the ST demonstrates that the identified security objectives are covering all aspects of the security needs. This includes showing that each OSP, threat and assumption is addressed by a security objective.

The following table identifies for each OSP, threat and assumption, the security objective(s) that address it.

Table 10 - OSPs, Threats and Assumptions to Security Objectives Mapping

	O.ISOLATE	O.LIMITCONNECTIVITY	O.MANAGE	O. SELF_PROTECT	ON.ADMINACCESS	ON.ENVIRON	ON.INSTALL	ON.NOEVILADMIN	ON.USER
A.ADMINACCESS					X				
A.ENVIRON						X			
A.INSTALL							X		
A.NOEVILADMIN								X	
A.USER									X
P.CUTOFF		X							
P.ISOLATE	X								
P.MANAGE			X						
T.DATACOMPROMISE	X	X							
T.TSF_COMPROMISE			X	X					

8.1.1 Rationale Showing Threats to Security Objectives

The following table describes the rationale for the threat to security objectives mapping.

Table 11 - Threats to Security Objectives Rationale

T.TYPE	Security Objectives Rationale
T.DATACOMPROMISE	**O.ISOLATE** mitigates this threat by limiting the possibility of information flow between connectors that are not actively connected within the TOE. **O.LIMITCONNECTIVITY** counters this threat by requiring that information only flow between the ports configured by the administrator.

T.TYPE	Security Objectives Rationale
T.TSF_COMPROMISE	**O. SELF_PROTECT** contributes to countering this threat by ensuring that the TSF can protect itself from users within the TSC. If the TSF could not maintain and control its domain of execution, it could not be trusted to control access to the resources under its control, which includes the audit trail. Ensuring that the TSF is always invoked is also critical to the mitigation of this threat. **O.MANAGE** is necessary because an access control policy is not specified to control access to TSF data. This objective is used to define the appropriate access to TSF data, which clarifies the “inappropriate access” from the threat.

8.1.2 Rationale Showing Assumptions to Environment Security Objectives

The following table describes the rationale for the assumption to security objectives mapping.

Table 12 - Assumptions to Security Objectives Rationale

A.TYPE	Environment Security Objective Rationale
A.ADMINACCESS	**ON.ADMINACCESS** addresses this assumption by restating it as an objective for the Administrator to satisfy.
A.ENVIRON	**ON.ENVIRON** addresses this assumption by restating it as an objective for the Administrator to satisfy.
A.INSTALL	**ON.INSTALL** addresses this assumption by restating it as an objective for the Administrator to satisfy.
A.NOEVILADMIN	**ON.NOEVILADMIN** addresses this assumption by restating it as an objective for the Administrator to satisfy.
A.USER	**ON.USER** addresses this assumption by restating it as an objective for the Administrator to satisfy.

8.1.3 Rationale Showing OSPs to Environment Security Objectives

The following table describes the rationale for the organisational security policies to security objectives mapping.

Table 13 - OSPs to Security Objectives Rationale

P.TYPE	Environment Security Objective Rationale
P.CUTOFF	**O.LIMITCONNECTIVITY** addresses this policy by requiring that information not flow between any ports when that option is configured by the administrator.
P.ISOLATE	**O.ISOLATE** addresses this policy by requiring a minimum isolation between ports.
P.MANAGE	**O.MANAGE** addresses the policy by requiring the functionality necessary to manage the TOE to be provided by the TOE.

8.2 Security Requirements Rationale

8.2.1 Rationale for Security Functional Requirements of the TOE Objectives

This section provides rationale for the Security Functional Requirements demonstrating that the SFRs are suitable to address the security objectives.

The following table identifies for each TOE security objective, the SFR(s) that address it.

Table 14 - SFRs to Security Objectives Mapping

	O.ISOLATE	O.LIMITCONNECTIVITY	O.MANAGE	O.SELF_PROTECT
FDP_IFC.1		X		
FDP_IFF.1		X		
FDP_ISO_EXP.1	X			
FMT_MOF.1			X	
FMT_MSA.1			X	
FMT_MSA.2			X	
FMT_MSA.3			X	
FMT_MTD.1			X	
FMT_MTD.3			X	
FMT_SMF.1			X	
FMT_SMR.1			X	
FPT_RVM.1				X
FPT_SEP.1				X

The following table provides the detail of TOE security objective(s).

Table 15 - Security Objectives to SFR Rationale

Security Objective	SFR and Rationale
O.ISOLATE	**FDP_ISO_EXP.1** defines the isolation requirements between the ports required to satisfy the objective.
O.LIMITCONNECTIVITY	**FDP_IFC.1** and **FDP_IFF.1** define the rules for information flow between ports required to satisfy the objective.
O.MANAGE	**FMT_MOF.1** states that the administrator may control the functionality of the front panel push buttons. **FMT_MSA.1** states that the only the administrator may view and change the switch settings for the data channels. **FMT_MSA.2** states that the TOE validates all input from the administrator to ensure that any configuration commands include appropriate values. **FMT_MSA.3** states that the default value for the switch configurations is the CUTOFF position, providing a restrictive value since no information may flow. **FMT_MTD.1** itemizes the TSF data that must be manageable via the administrator interfaces. **FMT_MTD.3** states that the TOE validates all input from the administrator to ensure that any configuration commands include appropriate values. **FMT_SMF.1** defines the specific security management functions to be supported. **FMT_SMR.1** defines the specific security roles to be supported.
O.SELF_PROTECTION	**FPT_SEP.1** ensures the TSF provides a domain that protects itself from untrusted users. If the TSF cannot protect itself it cannot be relied upon to enforce its security policies.

Security Objective	SFR and Rationale
	FPT_RVM.1 ensures that the TSF makes policy decisions on all interfaces that perform operations on subjects and information that are within the TSC. Without this non-bypassability requirement, the TSF could not be relied upon to completely enforce the security policies, since an interface(s) may otherwise exist that would provide a user with access to TOE resources (including TSF data and executable code) regardless of the defined policies.

8.2.2 Rationale for Security Functional Requirements of the IT Environment Objectives

No objectives are levied on the IT Environment.

8.2.3 Security Assurance Requirements Rationale

8.2.3.1 TOE Security Assurance Requirements Rationale

The TOE meets the assurance requirements for EAL4.

The TOE stresses assurance through vendor actions that are within the bounds of current best commercial practice. The TOE provides, primarily via review of vendor-supplied evidence, independent confirmation that these actions have been competently performed.

The general level of assurance for the TOE is:

A) Consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.

B) The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against part 3 of the Common Criteria.

8.3 TOE Summary Specification Rationale

This section demonstrates that the TOE’s Security Functions completely and accurately meet the TOE SFRs.

The following tables provide a mapping between the TOE’s Security Functions and the SFRs and the rationale.

Table 16 - SFRs to TOE Security Functions Mapping

	Switching	Isolation	Management	Self Protection
FDP_IFC.1	X			
FDP_IFF.1	X			
FDP_ISO_EXP.1		X		
FMT_MOF.1			X	
FMT_MSA.1			X	
FMT_MSA.2			X	

	Switching	Isolation	Management	Self Protection
FMT_MSA.3			X	
FMT_MTD.1			X	
FMT_MTD.3			X	
FMT_SMF.1			X	
FMT_SMR.1			X	
FPT_RVM.1				X
FPT_SEP.1				X

Table 17 - SFR to SF Rationale

SFR	SF and Rationale
FDP_IFC.1	**Switching** – the SF states that all connectivity between ports within each of the data channels is controlled by the TOE.
FDP_IFF.1	**Switching** – the SF states the rules for connectivity (information flow) between the ports within each data channel. No connectivity between ports of different data channels is provided.
FDP_ISO_EXP.1	**Isolation** – the SF states the minimum isolation between ports of similar type.
FMT_MOF.1	**Management** – the SF states that the ASCII interface may be used enable/disable the front panel push button operation as well as query the current setting.
FMT_MSA.1	**Management** – the SF states the mechanisms that may be used by an administrator to query and modify the switch settings for the two data channels.
FMT_MSA.2	**Management** – the SF states that all input from the administrator is validated before being acted upon.
FMT_MSA.3	**Management** – the SF states that the default switch position is CUTOFF.
FMT_MTD.1	**Management** – the SF states the parameters that may be altered via the administrator mechanisms.
FMT_MTD.3	**Management** – the SF states that all input from the administrator is validated before being acted upon.
FMT_SMF.1	**Management** – the SF states the functions that may be performed via the administrator mechanisms.
FMT_SMR.1	**Management** – the SF states the roles supported by the TOE. Only administrators may perform management actions since the TOE is transparent to users.
FPT_RVM.1	**Self Protection** – the SF states that the TSF can’t be bypassed because all interactions of the users and administrators are controlled by the TOE. The administrator interfaces are well defined and administrator input is validated.
FPT_SEP.1	**Self Protection** – the SF states that the TOE is a stand-alone system with no active users.

8.4 PP Claims Rationale

The rationale for the Protection Profile conformance claims is provided in Chapter 7.

8.5 Strength of Function Rationale

The TOE does not include any probabilistic or permutational mechanisms. SOF-basic is defined in CC Part 1 section 2.3 as: "A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential." Because this ST identifies threat agents with low attack potential, SOF-basic was chosen for the overall level.