Market Central SecureSwitch®
Security Target, V1.3
29 October, 2001
Document No. F4-1001-002

COACT, Inc.
Rivers Ninety Five
9140 Guilford Road, Suite L
Columbia, MD 21046-2587
Phone: 301-498-0150
Fax: 301-498-0855

Approved Signature Authority: _____ Date: 29 October 2001
Eric J. Grimes
Common Criteria Test Lab Manager

If problems or questions arise concerning the technical content of this report, please contact the responsible person whose signature appears above or contact James O. McGehee at:

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

Phone: 301-498-0150

Fax: 301-498-0855

E-mail: James O. McGehee (jom@coact.com)
Eric J. Grimes (ejg@coact.com)

DOCUMENT INTRODUCTION

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Market Central SecureSwitch®, Dual Network Switch, Model #5000600. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of assumptions about aspects of the environment, a list of threats that the product intends to counter, a set of security objectives and security requirements, and the IT security functions provided by the TOE which meet the set of requirements.

REVISION HISTORY

Rev	Description
1.0	14 February 2001, Review DRAFT.
1.1	25 June 2001, Changes made based upon results of ST evaluation.
1.2	02 October 2001, Additional changes made based upon TOE evaluation.
1.3	29 October 2001, Document updated based on Completion of the TOE evaluation.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACRONYMS

ST	Security Target
TOE	Target of Evaluation
EAL	Evaluation Assurance Level
PP	Protection Profile
IT	Information Technology
TSS	TOE Summary Specification
NIC	Network Interface Card
CC	Common Criteria
SFP	Security Function Policy
TSC	TOE Scope of Control
TSF	TOE Security Function
CM	Configuration Management

CHAPTER 1

1. Security Target Introduction

1.1 Security Target Identification

This section provides identifying information for the Market Central SecureSwitch® Security Target (ST), by identifying information regarding the Target of Evaluation (TOE).

1.1.1 Security Target Name

Market Central SecureSwitch® Security Target.

1.1.2 TOE Identification

Market Central SecureSwitch® Dual Network Switch, Model #5000600.

1.1.3 Evaluation Status

This ST has been evaluated.

1.1.4 Evaluation Assurance Level

Assurance claims conform to EAL4 (Evaluation Assurance Level 4) from the Common Criteria Version 2.1, August 1999.

1.1.5 Keywords

Switch

Network

1.2 Security Target Overview

This ST describes the objectives, requirements and rationale for the Market Central SecureSwitch®, Dual Network Switch, Model #5000600. The language used in this Security Target is consistent with the Common Criteria for Information Technology Security Evaluation, Version 2.1 and the ISO/IEC JTC 1/SC27, Guide for the Production

of PPs and STs, Version 0.8. As such, the spelling of several terms is the internationally accepted English, not always consistent with the current US English spelling norms.

1.2.1 Security Target Organisation

Chapter 1 of this ST provides introductory and identifying information for the SecureSwitch® 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 organisational security policies. Chapter 4 identifies the security objectives of the TOE and of the Information Technology (IT) environment. Chapter 5 provides the TOE security functional requirements, as well as requirements on the IT environment. Chapter 6 is the TOE Summary Specification, a description of the functions provided by SecureSwitch® to satisfy the security functional and assurance requirements. Chapter 7 provides a rationale for claims of conformance to a registered Protection Profile (PP). Chapter 8 provides a rationale, or pointers to rationale, for objectives, requirements, TSS, etc.

1.3 Common Criteria Conformance

The SecureSwitch® Dual Network Switch, Model #5000600 is compliant with the Common Criteria Version 2.1, functional requirements (Part 2) extended with two explicitly stated requirements and assurance requirements (Part 3) for EAL4 conformant.

1.4 Protection Profile Conformance

The SecureSwitch® Dual Network Switch, Model #5000600, does not claim conformance to any Protection Profile dated prior to 29 October 2001.

CHAPTER 2

2. TOE Description

2.1 SecureSwitch® TOE Description

The Market Central SecureSwitch® TOE is a mechanical switch assembly that controls the connections between two separate networks. The TOE provides the capability to connect to only one of the two networks at any given time, and prevents cross-talk or bleed-over from one network to the other. The TOE consists of two separate mechanical switches controlling each network connection. The separation between networks is isolated using a non-metallic bar that prevents both switches from being either open or closed at the same time. In addition, the housing of the TOE is non-metallic, to prevent the conduction of any signal between the two separate networks. Additionally, internal to the TOE, each of the switch mechanisms is encased in a composite copper/iron shielding, to prevent electromagnetic coupling between the two networks. The following figures show the front and rear housing of the TOE.

Figure 1 - SecureSwitch® Front

Figure 2 - SecureSwitch® Rear

The non-metallic housing of the TOE is assembled with tamper-resistant screws, to reduce the possibility of an individual from gaining physical access to the composite copper/iron shielding, switches and internal wiring.

CHAPTER 3

3. Security Environment

3.1 Introduction

This chapter identifies the following:

A) Significant assumptions about the TOE's operational environment.

B) IT related threats to the organisation countered by the TOE.

C) Environmental threats requiring controls to provide sufficient protection.

D) Organisational security policies for the TOE as appropriate.

Using the above listing, this chapter identifies threats (T), organisational security policies (P) and assumptions (A). For assumptions, threats or policies that apply to the environment, the initial character is followed by a period and then an 'E'. For example, O.E.PHYSICAL is an objective for the security environment of the TOE to provide physical protection for the TOE.

3.2 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

3.2.1 Connectivity Assumptions

A.CONNECT The TOE is assumed to be connected, via standard network connectors, to one computer and two separate networks or between two separate computers and two separate networks. When a single computer is connected to two

separate networks, that computer contains two separate network interface cards (NICs).

3.2.2 Personnel Assumptions

A.USER Users of the TOE are assumed to possess the necessary privileges to access the network connections managed by the TOE.

A.NOEVIL Users of the TOE are assumed to be non-hostile and follow all guidance, however they are capable of error.

3.2.3 Physical Assumptions

A.LOCATE The TOE is assumed to be located within controlled access facilities which will prevent unauthorised physical access.

3.3 Threats

3.3.1 Threats Against the TOE

T.T.DIRECT An undetected compromise of the IT assets may occur as a result of two networks being connected through the TOE at the same time.

T.T.CROSSTALK An attacker may capture data being transferred across the connected network from the unconnected network.

3.3.2 Threats Against the TOE Environment

T.E.PHYSICAL Security-critical parts of the TOE may be subject to physical attack which may compromise security.

3.4 Organisational Security Policies

There are no organisational security policies for this TOE.

CHAPTER 4

4. Security Objectives

4.1 Security Objectives for the TOE

All of the objectives listed in this section ensure that all of the security threats listed in Chapter 3 have been countered. The security objectives (O) for the SecureSwitch® are:

O.T.CONNECT The TOE will provide facilities to enable an authorised user to switch between two network connections.

O.T.CROSSTALK The TOE will provide separation between two network connections.

4.2 Security Objectives for the IT Environment

O.E.PHYSICAL Those responsible for the TOE environment must ensure that only authorised users have access to the TOE, and that it is protected from physical attack which might compromise IT security.

4.3 Security Objectives Rationale

Table 1 demonstrates the correspondence between the security objectives listed in Sections 4.1 and 4.2 to the assumptions identified in Section 3.2.

Table 1 - Correspondence Between Assumptions, Threats and Policies to Objectives

Table Legend		
A = Assumption, P = Policy, T = Threat, O = Objective, .E = Environment, .T = TOE		
Assumption, Threat or Policy	**Security Objective**	**Rationale**
A.CONNECT	O.T.CONNECT	The TOE has two pairs of RJ-45 Ethernet connectors, controlled through switches. One pair connects the computer and one network, through one switch. The other pair connects the same computer's other NIC with a second network, through the switch. Alternatively, one computer can be connected to its associated network through one of the two "sections" of the switch and a second computer can be connected to the other switch section. The user may switch between the connections.
A.USER	O.T.CONNECT	Physical access to the TOE implies that the individual has the privileges necessary to access the connected networks.
A.NOEVIL	O.T.CONNECT	TOE users are assumed to operate in accordance with guidance provided.
A.LOCATE	O.E.PHYSICAL	Only authorised TOE users have physical access to the TOE.
T.T.DIRECT	O.T.CONNECT	The user may switch between the network connections however, the TOE will only allow one network to be active at any given time.
T.T.CROSSTALK	O.T.CROSSTALK	The TOE will provide separation between two network connections, preventing cross-talk.
T.E.PHYSICAL	O.E.PHYSICAL	Restricting the TOE environment to only authorised users prevents physical attack which might compromise IT security.

CHAPTER 5

5. Security Functional Requirements

This section contains the functional requirements that are provided by the TOE and the IT environment. These requirements consist of functional components from Part 2 of the Common Criteria (CC), extended with explicitly stated requirements.

There is no strength of function claim for the Security Functional Requirements. There are no functions that are realized by probabilistic or permutational mechanisms.

5.1 TOE Security Functional Requirements

Table 2 lists the TOE functional requirements and the security objectives each requirement helps to address. All functional and assurance dependencies associated with the components in Table 2 have been satisfied.

Table 2 - TOE Functional Components

CC Component	Name	Hierarchical To	Dependency	Objectives Function Helps Address
FDP_IFC.2	Complete Information Flow Control	FDP_IFC.1	FDP_IFF.1	O.T.CROSSTALK O.T.CONNECT
FDP_IFF.1	Simple Security Attributes	No Other Components	FDP_IFC.1[1], FMT_MSA.3	O.T.CROSSTALK O.T.CONNECT
FPT_SEP.1	TSF Domain Separation	No Other Components	None	O.T.CROSSTALK O.T.CONNECT
ESP_ISO.1	Isolation	No Other Components	None	O.T.CROSSTALK
ESP_ISO.2	Isolation	No Other Components	None	O.T.CROSSTALK
ESP_SHL.1	Shielding	No Other Components	None	O.T.CROSSTALK

[1] The FDP_IFC.1 dependency is met by FDP_IFC.2, since FDP_IFC.2 is hierarchical to FDP_IFC.1.

The functional requirements that appear in Table 2 are described in more detail in the following subsections. Additionally, these requirements are derived verbatim from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 2.1 with the exception of italicised items listed in brackets, and the two explicitly stated requirements. These bracketed items include either "assignments" that are TOE specific or "selections" from the Common Criteria that the TOE enforces.

5.1.1 User Data Protection (FDP)

5.1.1.1 FDP_IFC.2 Complete Information Flow Control

Hierarchical to: FDP_IFC.1 Subset Information Flow Control.

FDP_IFC.2.1 – The TSF shall enforce the [assignment: *Complete Separation Flow Control Policy*] on [assignment: *electronic 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.

Dependencies: FDP_IFF.1 Simple Security Attributes.

Rationale: The TOE provides a set of inverse switches that are mechanically controlled. When a switch is closed for one network connector, allowing electronic signals to flow through the switch to that network connector, the inverse switch is open for the other network connector, preventing any flow of signals through the switch to that network connector.

5.1.1.2 FDP_IFF.1 Simple Security Attributes

Hierarchical to: No other components.

FDP_IFF.1.1 – The TSF shall enforce the [assignment: *Complete Separation Flow Control Policy*] based on the following types of subject and information security attributes: [assignment: *the position of the switch*].

FDP_IFF.1.2 – The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: *information flow will be permitted on a given side, only when the switch is in the proper position*].

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

FDP_IFF.1.4 The TSF shall provide the following [assignment: none].

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

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based upon the following rules: [assignment: none].

Dependencies: FDP_IFC.1 Subset Information Flow Control,

FMT_MSA.3 Static Attribute Initialisation.

Rationale: The TOE provides a set of inverse switches that are mechanically controlled. When a switch is closed for one network, allowing electronic signals to flow through the switch to that network, the inverse switch is open for the other network, preventing any flow of signals through the switch to that network. Switch position is the only attribute the TOE recognizes. A change of switch position will cause information flow to one network to be interrupted and flow to the other network to commence. There are no exceptions.

5.1.2 Protection of the TSF (FPT)

5.1.2.1 FPT_SEP.1 TSF Domain Separation

Hierarchical to: No other components.

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

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

Dependencies: No dependencies

Rationale: By providing isolation and shielding between the two network sides, the TOE provides domain separation.

5.1.3 Explicitly Stated Requirements (ESP)

The following requirements were not derived from the CC. They are needed because the CC does not currently provide any requirements on electronic isolation and shielding, two of the main security features of this TOE.

5.1.3.1 ESP_ISO.1 Electronic Isolation – Network Sides

Hierarchical to: No other components.

ESP_ISO.1.1 The TOE shall ensure that there are no electronic paths between the two network sides.

Dependencies: No dependencies

Rationale: The TOE uses only non-metallic, non-conductive materials between the two network sides.

5.1.3.2 ESP_ISO.2 Electronic Isolation – Open Switch

Hierarchical to: No other components.

ESP_ISO.2.1 The TOE shall ensure that there is a minimum isolation between the two sides of an open switch that comply with Table 3.

Frequency	dB
200-300 kHz	> 78 dB
0.3-1.3 MHz	> 78 dB
1.0-11.0 MHz	> 79 dB
10.0-110.0 MHz	> 75 dB

Table 3 - Isolation

Dependencies: No dependencies

Rationale: The TOE provides a passive composite copper/iron shielding around each of the network sides, dampening the flow of electrically-coupled signals between the two separate networks.

5.1.3.3 ESP_SHL.1 Electronic Shielding

Hierarchical to: No other components.

ESP_SHL.1.1 The TOE shall ensure that electromagnetic coupling between the two network sides is sufficient to provide the isolation as shown in Table 3, measured at the TOE boundary.

Dependencies: No dependencies

Rationale: The TOE provides a passive composite copper/iron shielding around each of the network sides, dampening the flow of magnetically-coupled signals between the two separate networks.

5.2 IT Security Functional Requirements

Table 4 lists the IT functional requirements and the security objectives each requirement helps to address. All functional and assurance dependencies associated with the components in Table 4 have been satisfied.

Table 4 - IT Functional Components

CC Component	Name	Hierarchical To	Dependency	Objectives Function Helps Address
FMT_MSA.1	Management of Security Attributes	No Other Components	FDP_IFC.1[2], FMT_SMR.1	O.T.CROSSTALK O.T.CONNECT
FMT_MSA.3	Static Attribute Initialisation	No Other Components	FMT_MSA.1, FMT_SMR.1	O.T.CROSSTALK O.T.CONNECT

The IT functional requirements that appear in Table 4 are described in more detail in the following subsections. Additionally, these requirements are derived verbatim from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 2.1 with the exception of italicised items listed in brackets. These bracketed items include either "assignments" that are TOE specific or "selections" from the Common Criteria that the TOE enforces.

The dependency of FMT_MSA.1 and FMT_MSA.3 on FMT_SMR.1 is not satisfied because there is only one role provided by this TOE, and that is the user. Furthermore, the only function provided to the user is the ability to change the switch position, and that function may be performed without identification by the TOE. Therefore, FMT_SMR.1 is not required by this TOE.

[2] The FDP_IFC.1 dependency is met by FDP_IFC.2, since FDP_IFC.2 is hierarchical to FDP_IFC.1.

5.2.1 Security Management (FMT)

5.2.1.1 FMT_MSA.1 Management of Security Attributes

Hierarchical to: No other components.

FMT_MSA.1.1 The TSF shall enforce the [assignment: *Complete Separation Flow Control Policy*] to restrict the ability to [selection: *modify*] the security attributes [assignment: *switch position*] to [assignment: *the user*].

Dependencies: FDP_IFC.1 Subset Information Flow Control,

FMT_SMR.1 Security Roles.

Rationale: Switch position is the only attribute the TOE recognizes. A change of switch position will cause information flow to one network to be interrupted and then flow to the other network to commence, in accordance with the Complete Separation Flow Control Policy.

5.2.1.2 FMT_MSA.3 Static Attribute Initialisation

Hierarchical to: No other components.

FMT_MSA.3.1 The TSF shall enforce the [assignment: *Complete Separation Flow Control Policy*] to provide [selection: *restrictive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [assignment: user] to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of Security Attributes,

FMT_SMR.1 Security Roles.

Rationale: Switch position is the only attribute the TOE recognizes. A change of switch position will cause information flow to one network to be interrupted and then flow to the other network to commence, in accordance with the Complete Separation Flow Control Policy.

5.3 TOE Security Assurance Requirements

The TOE meets the assurance requirements for EAL4. EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.

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

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

potential.

EAL4 also provides assurance through the use of development environment controls and additional TOE configuration management including automation, and evidence of secure delivery procedures.

This EAL represents a meaningful increase in assurance from EAL3 by requiring more design description, a subset of the implementation, and improved mechanisms and/or procedures that provide confidence that the TOE will not be tampered with during development or delivery.

The assurance components for the TOE are summarised in Table 5.

Table 5 - Assurance Components

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

Tests	ATE_FUN.1	Functional Testing
Tests	ATE_IND.2	Independent Testing – Sample
Vulnerability Assessment	AVA_MSU.2	Validation of Analysis
Vulnerability Assessment	AVA_SOF.1	Strength of TOE Security Function Evaluation
Vulnerability Assessment	AVA_VLA.2	Independent Vulnerability Analysis

The following subsections provide more detail for the assurance components listed in Table 4.

5.3.1 Configuration Management (ACM)

5.3.1.1 ACM_AUT.1 Partial CM Automation

Dependencies: ACM_CAP.3 Authorisation controls.

5.3.1.2 ACM_CAP.4 Generation Support and Acceptance Procedures

Dependencies: ACM_SCP.1 TOE CM coverage,

ALC_DVS.1 Identification of security measures.

5.3.1.3 ACM_SCP.2 Problem Tracking CM Coverage

Dependencies: ACM_CAP.3 Authorisation controls.

5.3.2 Delivery and Operation (ADO)

5.3.2.1 ADO_DEL.2 Detection of Modification

Dependencies: ACM_CAP.3 Authorisation controls.

5.3.2.2 ADO_IGS.1 Installation, Generation, and Start-Up Procedures

Dependencies: AGD_ADM.1 Administrator Guidance.

5.3.3 Development (ADV)

5.3.3.1 ADV_FSP.2 Fully Defined External Interfaces

Dependencies: ADV_RCR.1 Informal Correspondence

Demonstration.

5.3.3.2 ADV_HLD.2 Security Enforcing High-Level Design

Dependencies: ADV_FSP.1 Informal Functional Specification,

ADV_RCR.1 Informal Correspondence Demonstration.

5.3.3.3 ADV_IMP.1 Subset of the Implementation of the TSF

Dependencies: ADV_LLD.1 Descriptive Low-Level Design,

ADV_RCR.1 Informal Correspondence Demonstration,

ADV_TAT.1 Well Defined Development Tools.

5.3.3.4 ADV_LLD.1 Descriptive Low-Level Design

Dependencies: ADV_HLD.2 Security Enforcing High-Level Design,

ADV_RCR.1 Informal Correspondence Demonstration.

5.3.3.5 ADV_RCR.1 Informal Correspondence Demonstration

Dependencies: No dependencies.

5.3.3.6 ADV_SPM.1 Informal TOE Security Policy Model

Dependencies: ADV_FSP.1 Informal Functional Specification.

5.3.4 Guidance Documents (AGD)

5.3.4.1 AGD_ADM.1 Administrator Guidance

Dependencies: ADV_FSP.1 Informal Functional Specification.

5.3.4.2 AGD_USR.1 User Guidance

Dependencies: ADV_FSP.1 Informal Functional Specification.

5.3.5 Life Cycle Support (ALC)

5.3.5.1 ALC_DVS.1 Identification of Security Measures

Dependencies: No dependencies.

5.3.5.2 ALC_LCD.1 Developer Defined Life Cycle Model

Dependencies: No dependencies.

5.3.5.3 ALC_TAT.1 Well-Defined Development Tools

Dependencies: ADV_IMP.1 Subset of the Implementation of the TSF.

5.3.6 Tests (ATE)

5.3.6.1 ATE_COV.2 Analysis of Coverage

Dependencies: ADV_FSP.1 Informal Functional Specification,

ATE_FUN.1 Functional Testing.

5.3.6.2 ATE_DPT.1 Testing: High-Level Design

Dependencies: ADV_HLD.1 Descriptive High-Level Design,

ATE_FUN.1 Functional Testing.

5.3.6.3 ATE_FUN.1 Functional Testing

Dependencies: No dependencies.

5.3.6.4 ATE_IND.2 Independent Testing – Sample

Dependencies: ADV_FSP.1 Informal Functional Specification,

AGD_ADM.1 Administrator Guidance,

AGD_USR.1 User Guidance,

ATE_FUN.1 Functional Testing.

5.3.7 Vulnerability Assessment (AVA)

5.3.7.1 AVA_MSU.2 Validation of Analysis

Dependencies: ADO_IGS.1 Installation, Generation, and Start-Up

Procedures,

ADV_FSP.1 Informal Functional Specification,

AGD_ADM.1 Administrator Guidance,

AGD_USR.1 User Guidance.

5.3.7.2 AVA_SOF.1 Strength of TOE Security Function Evaluation

Dependencies: ADV_FSP.1 Informal Functional Specification,

ADV_HLD.1 Descriptive High-Level Design.

5.3.7.3 AVA_VLA.2 Independent Vulnerability Analysis

Dependencies: ADV_FSP.1 Informal Functional Specification,

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,

AGD_ADM.1 Administrator Guidance,

AGD_USR.1 User Guidance.

5.4 Security Requirements for the IT Environment

There are no security requirements on the IT environment.

CHAPTER 6

6. TOE Summary Specification

6.1 TOE Security Functions

The major functions implemented by the TOE are:

SWITCH Mechanical inverse switches that control the flow of information through the TOE in accordance with the Complete Separation Flow Control Policy. The switch may be changed by the user without identification. There are no other operations or attributes of this function. This function implements FDP_IFC.2, FDP_IFF.1, FMT_MSA.3, FMT_SMR.1, and partially implements FPT_SEP.1.

SHIELD Passive composite copper/iron shielding around each of the network sides, dampening the flow of electronic signals between the two separate networks. This function implements ESP_SHL.1 and partially implements FPT_SEP.1.

ISOLATION Physical isolation of the two network sides with non-metallic, non-conductive materials. This function implements ESP_ISO.1, ESP_ISO.2, and partially implements FPT_SEP.1.

Table 6 shows the mapping between the security functions listed above and the security functional requirements.

Table 6 - Functions to Security Functional Requirements Mapping

Functions	Security Functional Requirements
SWITCH	FDP_ IFC.2, FDP_IFF.1, FMT_MSA.1, FMT_MSA.3, and partially implements FPT_SEP.1.
SHIELD	ESP_SHL.1 and partially implements FPT_SEP.1.
ISOLATION	ESP_ISO.1, ESP_ISO.2, and partially implements FPT_SEP.1.

Table 7 shows the mapping between the security functional requirements and the functions listed above.

Table 7 - Security Functional Requirements to Functions Mapping

Security Functional Requirement	Functions
FDP_IFC.2	SWITCH
FDP_IFF.1	SWITCH
FMT_MSA.1	SWITCH
FMT_MSA.3	SWITCH
FPT_SEP.1	SWITCH, SHIELD, and ISOLATION
ESP_ISO.1	ISOLATION
ESP_ISO.2	ISOLATION
ESP_SHL.1	SHIELD

6.2 Assurance Measures

The assurance measures provided by the TOE satisfy all of the assurance requirements listed in Chapter 5, Table 5.

6.3 Strength of Function (SOF)

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

6.4 Rationale for TOE Assurance Requirements

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 EAL4 from part 3 of the Common Criteria.

CHAPTER 7

7. Protection Profile Claims

The SecureSwitch® Dual Network Switch, Model #5000600, does not claim conformance to any Protection Profile dated prior to 29 October 2001.

CHAPTER 8

8. Rationale

8.1 Security Objectives Rationale

The rationale for the security objectives of the TOE is defined in Chapter 4, Section 4.3 Security Objectives Rationale.

8.2 Security Requirements Rationale

The rationale for the security requirements of the TOE is defined in two sections. Rationale for the security functional requirements is given after each functional component description in Chapter 5, Section 5.1 Security Functional Requirements. Rationale for the security assurance requirements is given in Chapter 6, Section 6.3 Rationale for TOE Assurance Requirements.

8.2.1 Rationale for Explicitly Stated Requirements

The Common Criteria, Version 2.1, does not contain any requirements specifically addressed at electronic isolation. The two explicitly stated requirements were added to provide testable requirements, consistent with the CC model, to meet this user need.

8.2.2 Rationale for Dependencies Not Met

The dependency of FMT_MSA.1 and FMT_MSA.3 on FMT_SMR.1 is not satisfied because there is only one role provided by this TOE, and that is the user. Furthermore, the only function provided to the user is the ability to change the switch position, and that function may be performed without identification. Therefore, FMT_SMR.1 is not required by this TOE.

8.3 TOE Summary Specification Rationale

The rationale for the TOE Summary Specification is defined in Chapter 6, Section 6.1 TOE Security Functions.

8.4 PP Claims Rationale

The SecureSwitch® Dual Network Switch, Model #5000600, does not claim conformance to any Protection Profile dated prior to 29 October 2001.