CAFE Lab

Voltaire 2in1 PC™

Security Target Report

Prepared for:
Voltaire Advanced Data Security, Ltd.
103 Medinat Hayehudim
P.O.B. 12534
Herzylia 46733, Israel

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

Registration No. TTAP-CC-0004
Document No. 010516(8)
04 June1999

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Chapter 1

Chapter 1 Introduction

This Chapter identifies the Target of Evaluation (TOE), the Common Criteria (CC) version number used, and the Evaluation Assurance Level (EAL) the TOE will be evaluated at by the lab. After this identification has been made, this Chapter defines any conformance claims and then provides a brief overview of the TOE.

1.1 Identification

Title: Voltaire 2in1 PC™ Security Target

TOE: 2in1 PC™ Version 1.21

Version Numbers for 2in1 PC™ Version 1.21: Installation Disk Version 1.21

2in1 PC™ Installation Guide Ver. 1.21

2in1 PC™ Board Ver. 1.21

2in1 PC™ Quick Installation Guide Ver. 1.21

2in1 PC™ User Guide Ver. 1.21

2in1 PC™ Application Notes Ver 1.21

EAL: Functional and Assurance claims conform to EAL-2 (Version 2 Final of the Common Criteria, May 1998)

Conformance Claim**:** The 2in1 PC™ Version 1.21 TOE is compliant with the Common Criteria, Part 2, functional requirements. The 2in1 PC™ Version 1.21 TOE is compliant with the Common Criteria, Part 3, assurance requirements for EAL2 augmented with ADV_SPM.1, Informal TOE Security Policy Model.

Registration: TTAP-CC-0004

Keywords: Multi-level security, COTS, access control, discretionary control, network security, network security hardware, networked information systems, data security, and information protection.

1.2 Security Target Overview

The TOE specifies a baseline for information protection in Commercial-Off-The-Shelf (COTS) information technology. The TOE couples this functionality with assurances selected to provide a maximum amount of confidence consistent with existing best practices for COTS development.

2in1 PC™ board is a hardware device that enables a single PC to securely connect to two physically separated networks. Physical separation is accomplished through the use of a hardware based security controller that is embedded in the 2in1 PC™ board (Figure 1-1). This controller manages both the PC's connection between the two networks and the access to the PC's configured disk partitions.

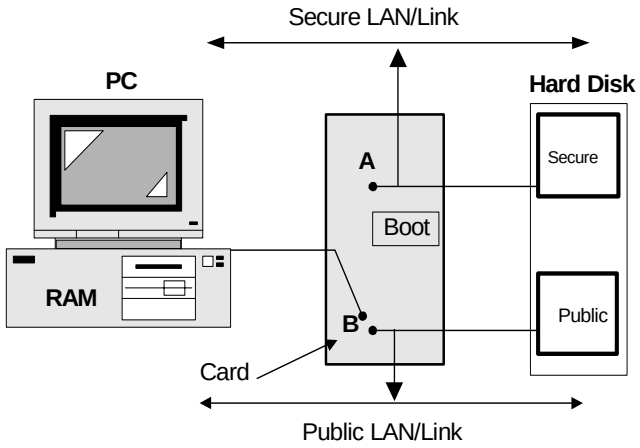

Figure 1-1

The TOE will:

a) Provide the ability to use a single PC to securely access two physically separated networks (“A” and ”B”) by using a firmware based security controller.

b) Divide the PC’s hard disk or disks into two parts (“A” and ”B”) and monitor all IDE commands, only allowing authorised access to be performed during set-up when the 2in1 PC™ set-up plug is inserted into the 2in1 PC™ board and the 2in1 PC™ installation program is loaded. During set-up, the board is transparent and IDE commands are not monitored.

c) Protect the user’s “A” network and “A” disk partition from malicious attacks, such as denial of service attacks, by individuals on the “B” network.

d) Provide mechanisms to ensure no operation in the event of a system failure, power failure, or forced shutdown.

e) Support all application protocols since the TOE operates on the Physical Layer (Layer 1) of the Open Systems Interconnection (OSI) model.

f) Support the ability to disable two devices, such as a floppy diskette drive, SCSI connection, or parallel port connection, provided the optional cables are installed and the board is configured accordingly. These two devices may be disabled when the machine is in either the "A" or "B" state, or one device may be disabled for each state.

The TOE is not expected to:

a) Provide "label-based controls" appropriate for protecting Multi-Level Secure (MLS) information (such as government classified, company proprietary, or export restricted data) in environments containing users who are not allowed access to such information.

b) Protect against malicious abuse of authorised privileges by Administrators.

c) Provide extensive protection against installation or administration errors.

Key environmental conditions that apply to the use of the TOE are:

a) Administrators must recognise the need for a secure Information Technology (IT) environment, understand what security is provided by the TOE, and recognise any further requirements to maintain security.

b) Administrators must be trusted to correctly apply the organisation's

security policies in their discretionary actions.

c) Basic physical security must be provided.

Chapter 2

Chapter 2 TOE Description

The Target of Evaluation (TOE) is the 2in1 PC™ ISA board, the supporting software provided on the installation floppy diskettes, and the documentation provided as part of the 2in1 PC™ product developed by Voltaire. The TOE is confined to a single host, intended to interface with a networked environment. The TOE will provide the secure transfer between the "A"and "B" network connections and protect from access to user data areas not related to the current network connection. The TOE supports a single AT compatible PC running MSDOS, Microsoft Windows 3.x, Windows 95, Windows 98, Windows NT (Versions 3.51 and 4), OS/2, and SCO and LINUX UNIX operating systems. It supports a single PC consisting of one or two IDE-ATA hard drives that are partitioned into separate areas during installation by using the Powerquest Partition Magic™ mechanism. The TOE itself does not restrict itself to the enforcement of only one security implementation. Instead, multiple security implementations are supported that allow an organisation to enforce its own security policy by customising the partitioned disk areas listed below. An example of one of the multiple organisational security implementations that can be enforced is listed following the disk partitions described below.

The partitioned areas created include:

a) "A" disk partition, disk access is controlled in firmware at the IDE bus physical layer to only allow access to the "A" disk partition when the TOE is connected to the "A" network connection. This partition contains its own operating system that

can be any one of the supported operating systems listed at the beginning of Chapter 2.

b) "B" disk partition, disk access is controlled in firmware at the IDE bus physical layer to only allow access to the "B" disk partition when the TOE is connected to the "B" network connection. This partition contains its own operating system that can be any one of the supported operating systems listed at the beginning of Chapter Two.

c) Functional disk partition, an optional disk partition appropriate for controlling the communication of information between the two disk partitions, "A" and "B". This communication link can only be configured when the 2in1 PC™ set-up plug is inserted into the 2in1 PC™ board. During configuration, the "A" state is configured to have either read, read\write, or no access to the Functional area. The "B" state is also configured at this time to have either read, read\write, or no access to the Functional area. If a given organisational security policy requires that no communication shall be interchanged between the "A" and "B" disk partitions, then the Functional disk partition can be omitted to enforce such a policy.

d) Transition, the partition area that is read only, unless the 2in1 PC™ set-up plug is inserted. Under normal operation, the Transition area is entered only after the system has been booted up via a hardware reset signal or powered on. The

Transition area is then loaded, pre-configured software stored in the Transition area is executed to totally erase the PC's Random Access Memory (RAM), and then the switch between machine states, "A" and "B", is performed. The same steps are performed in the event of system failure, power failure, or forced shutdown. Since the Transition area is the first partition loaded when the PC is turned on or when the PC switches between the "A" and "B" machine states, additional software can be placed into the area depending on an organisation's security requirements. As an example, if an organisational security implementation requires the use of a biometric device for authentication, the software for the device can be placed into the Transition area. With this in place, whenever turning the PC on or switching between the "A" or "B" machine states, authentication by the biometric device will be required before the PC loads the "A" or "B" disk partition and connects to the partition's corresponding network connection.

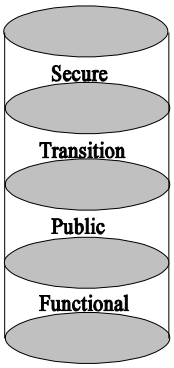

Figure 2-1

Single IDE-ATA Hard Disk Partitioned Areas

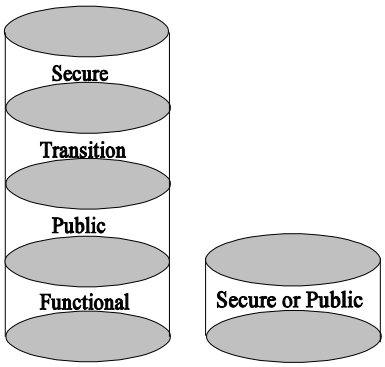

Figure 2-2

Two IDE-ATA Hard Disks Partitioned Areas

As referenced in figure 2-2 above, in a PC that contains two hard drives, the first drive will contain the Transition, Functional, "B", and "A" disk partitions. The second drive will contain only the "A" or "B" disk partition. The following is an example of how the TOE can be configured in a hypothetical organisation:

> The TOE supports the enforcement of one of many organisational security implementations depending upon how the device is configured. As an example, if an organisation was comprised of two physically separated networks, for instance a proprietary network and a "B" network, the TOE would enable a single PC to securely access each network. This example organisation would require that no information on the proprietary network shall escape to the "B" network, however information on the "B" network would be allowed to transfer into the proprietary network.
>
> Given this scenario, the TOE would be configured in the following manner:
>
> a) The TOE must enter set-up mode by inserting the 2in1 PC™ set-up plug into the 2in1 PC™ board and then running the 2in1 PC™ installation program.
> b) The "B" disk area would be configured to have read\write access to the Functional disk area.

c) The "A" disk area would be configured to have read access to the Functional disk area.

d) Set-up mode would then be exited by closing the installation program and then removing the 2in1 PC™ set-up plug from the 2in1 PC™ board.

In this example configuration, when the TOE is in the "B" state (i.e. in the "B" disk area and connected to the "B" network connection), the only other accessible disk partition would be the Functional disk area. By granting the "B" state read\write access to the Functional disk area, any data retrieved from the "B" network connection, or any data stored on the "B" disk partition, would be able to be written to the Functional disk area. The "B" state would also be allowed to read, from the Functional disk partition, any data that was placed there while in the "B" machine state. In order to switch to the "A" machine state, the following events would occur, the four electro-mechanical relays (two relays for the "A" and two relays for the "B" connections) that control the network connections will be opened, physically disabling all network access. The PC would then reboot, load into the Transition area, execute pre-configured software stored in the Transition area to clear all data previously stored in RAM, reboot into the "A" disk area, and then close the two relays for the proprietary network connection. Now that the machine is in the "A" machine state (i.e., in the "A" disk area and connected to the proprietary network connection) the only other accessible disk partition is the Functional area. In this example, the "A" state has only been granted read access from the Functional disk partition, therefore any data in the Functional disk partition can be copied into the "A" disk partition, however data stored in the "A" disk partition is blocked from being written to the functional disk partition. Thus, a one way tunnel has been created to only allow data to flow from the "B" machine state to the "A" machine state. This configuration would then satisfy the example organisation's security implementation.

The "A", "B", Functional, and Transition disk partitions each have a unique Master Boot Record (MBR), the "A" MBR is stored on the hard drive and the "B", Functional, and Transition MBR's are stored in an EEPROM chip that is on the 2in1 PC™ board. Permission to grant or deny access to specific disk areas is implemented by monitoring all IDE commands. These permission settings are stored in firmware on an EEPROM chip and are implemented by monitoring all IDE commands. Permissions can only be configured during set-up when the 2in1 PC™ set-up plug has been inserted into the 2in1 PC™ board and the 2in1 PC™ installation program has been loaded.

During initial startup, the PC is always booted into the Transition area. From that point, either the "A" or "B" disk area is loaded and any further access to the Transition area is denied. The Functional area is optionally active when the PC is in either the "A", Transition, or "B" disk area. When the PC is running in either the "A", Transition, or "B" disk area, communication to the Functional area is enforced by the permissions settings that were configured when the TOE was set-up by the Administrator.

The network connections for both the "A" and "B" disk areas are controlled by electro-mechanical relays. When in the "A" area, the"A" relays are closed and the "B" relays are open, physically disabling access to the "B" network. When moving from the "A" to "B" disk area there will be no network connection, all 4 relays will be open. The PC then reboots, loads into the Transition area, reboots into the "B" disk area, and switches to the "B" network connection. The same steps are performed when switching from "B" to "A" disk areas.

2.1 Product Class

The TOE can provide information protection for more than one operational environment. The operational environments supported include an "A" network and a "B" network connection. The TOE provides information protection in these environments by using a firmware based security controller that controls disk access and access to network connections. This enables a single PC to securely interface two separate networks, as if it were two separate PC's, one connected to each network.

2.2 Operational Environment

The TOE enables a single PC the ability to securely connect to two physically separated networks. The supported network connections include, Ethernet RJ-45, Fast Ethernet RJ-45, telephone line RJ-11, Token Ring, ISDN, 100Base-T4 Ethernet, or 100VGAnylan for both the "A" network and "B" network connections. In relation to the established network connection, disk access is controlled by a firmware based security controller that denies access to disk areas not related to the current machine state ("A" or "B").

The TOE recognises two distinct roles, the administrator and the user. Administrators are responsible for the installation and maintenance of the 2in1 PC™ board and users are individuals who operate a PC with the TOE installed.

During installation, the Administrator:

a) Installs the 2in1 PC™ board, inserts the 2in1 PC™ set-up plug, and runs the 2in1 PC™ installation program to configure the host PC.

b) Specifies the partition sizes for the Functional, "A", and "B" disk areas.

c) May define different name labels for the "A" and "B" disk areas.

d) Specifies the read/write, read, or no access option to the Functional area when the PC is running in the "A", "B", or Transition machine states.

e) Specifies the read/write or read only access to the Transition area when the PC is running in the Transition disk area.

f) Sets the power-up mode, to always boot to the Transition area and then reboot to either the "A" or "B" areas and corresponding network

connections. A menu can be added to choose “A” or “B” during transition.

g) Sets the reset signal initiation method to be used when switching between areas, the options are either Advanced or AT Compatible reset signals.

h) Installs programs into the Transition area, such as access control software, installs the operating system and/or applications into the “A” and “B” areas, and may install applications into the Functional area that can be utilised by both the “A” and “B” disk areas (depending upon the Functional access configuration for the “A” and “B” disk areas).

After the installation of the 2in1 PC™ board, the Administrator provides maintenance for the TOE. Such maintenance includes updates to applications stored in the Transition area, 2in1 PC™ board reconfiguration, and changes in the access rights to the Functional area in relation to the current machine’s state, “A” or “B”. The user role on the other hand, pertains to any other user that has physical access to the PC with the TOE installed. Users are denied access to Administrator functions since they do not have the 2in1 PC™ set-up plug nor the 2in1 PC™ installation program to configure the card.

The TOE will control access to:

a) Printers or mass storage devices on separate networks by connecting or disconnecting the network connection where the device is located.

b) A single PC’s connection to a “A” and a “B” network.

c) A single PC’s disk partitions.

d) Two devices such as a floppy diskette drive, SCSI connection, or parallel port connection, provided the optional cables are installed and the 2in1 PC™ board is configured accordingly. These two devices may be disabled when the machine is in either the "A" or "B" state, or one device may be disabled for each state.

2.3 TOE Security Functionality

The TOE implements the following security functionality:

a) Allow the setting up and configuration of the TOE security attributes.

b) Provide storage for configuration data (including card configuration and MBRs).

c) Provide a state machine with three distinct states of operation: A, B, and T (Transition).

d) Provide a different MBR for each security state during boot.

e) Control access to disk partitions based on the current security state and the access security policy.

f) Control access to networks based on the current security state and the access security policy.

g) Control the flow of state changes.

h) Monitor access to the floppy drive during the Transition state and prevent state switching upon detection thereof.

i) Control access to external devices such as SCSI drives and floppy drives.

j) Detect the presence of a physical setup plug in order to switch into SETUP mode and allow configuration.

2.4 Target of Evaluation

The Target of Evaluation (TOE) is the 2in1 PC™ board, the supporting software provided on the installation floppy diskettes, and the documentation provided as part of the 2in1 PC™ Version 1.21 product developed by Voltaire.

Chapter 3

Chapter 3 Security Environment

3.1 Introduction

This chapter identifies the following:

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

b) Organisational security policies for the TOE is appropriate.

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

d) Environmental threats requiring controls to provide sufficient protection.

By providing the information described above, this chapter gives the basis for the security objectives described in Chapter 4, the specific security requirements listed in Chapter 5, and the specific assurance components listed in Chapter 6.

3.2 Secure Usage Assumptions

The specific conditions listed below 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.

Table 3.1 – Security Assumptions

Table Legend			
A = Assumption, P = Policy, T = Threat, O = Objective, .E = Environment, .T = Threat			
Type	**Name**	**Assumption**	**Discussion**
Physical	A.E.ACCESS	The processing resources of the TOE that depend on hardware security features will be located within controlled access facilities that mitigate unauthorised, physical access.	The TOE will not be able to meet its security requirements unless at least a minimum degree of physical security is provided.
Platform	A.E.INSTALL	The TOE must be installed on a AT compliant PC.	The TOE cannot enforce its security functionality if it is installed on a non-compliant PC.
Platform	A.E.OS-REQ	Two of the supported operating systems listed in Chapter 2must be installed on the PC. Note: one operating system for the Secure (A) machine state and a second installed for the Public (B) machine state.	The TOE cannot function if non-compliant operating systems are installed for the Secure (A) and Public (B) machine states.
Personnel	A.E.USER-NEED	Users recognise the need for a secure IT environment.	It is essential that the users appreciate the need for security.
Personnel	A.E.ADMIN	The security features of the TOE are competently administered during set-up and reconfiguration.	It is essential that security administration be competent.

3.3 Organisational Security Policies

The organisational security policies discussed below are addressed by the TOE.

Table 3.2 – Security Policies

Table Legend		
A = Assumption, P = Policy, T = Threat, O = Objective, .E = Environment, .T = Threat		
Name	**Policy**	**Discussion**
P.E.KNOWN	Users of the TOE must be identified and authenticated before TOE access can be granted.	In some environments, identification and authentication mechanisms may be required and therefore must be supplied by the operational environment, as the TOE only requires identification for Administrator privileges.
P.E.ADMIN-TRAIN	Administrators of the system will be adequately trained, enabling them to effectively implement organisational security policies.	Administrators are expected to use IT resources and information in accordance with the organisational security policy. In order for this to be possible, Administrators must be adequately trained to understand the purpose and need for security controls, and to be able to make secure decisions with respect to their discretionary actions.
P.E.USAGE	The organisation's IT resources must be used only for authorised purposes.	In conjunction with the TOE environment, users must ensure that the organisation's information technology is not used for unauthorised purposes.
P.E.DUE-CARE	The organisation's IT systems must be implemented and operated in a manner that represents due care and diligence with respect to any risks to the organisation.	It is important that the level of security afforded the IT system be in accordance with what is generally considered adequate within the business or government sector in which the organisation is placed.

3.4 Threats to Security

The threats facing the TOE are listed in Table 3.3-1 and the threats to the surrounding environment are listed in Table 3.3-2.

Table 3.3-1 – Security Threats Addressed by the TOE

Table Legend	
A = Assumption, P = Policy, T = Threat, O = Objective, .E = Environment, .T = Threat	
Name	**Threat**
T.T.CRASH	The secure state of the TOE could be compromised in the event of a system crash.
T.T.ENTRY	An individual on a network connection may gain unauthorised access to the TOE's other network connection via a technical attack.
T.T.DATA	An individual on a network connection may gain unauthorised access to information on the TOE's other disk partitions via a technical attack.
T.T.TRANSFER	Data that a TOE user moves between disk areas could be accessible by other network connections.
T.T.DEVICE.FAIL	In the event of a hardware failure or physical damage to the TOE, the TOE may not operate and disk access will be blocked.
T.T.COPY	The TOE user may reboot with a floppy diskette and automatically copy, via a cycle of events, data from the "A" to "B" disk areas.
T.T.DISK	The TOE user may transfer sensitive data from the "A" disk area to a floppy disk, SCSI connection, or parallel port connection.
T.T.MEMORY	The TOE user may change RAM clearing or access control software stored in the Transition area.
T.T.ATTACK	The TOE may be subjected to a malicious attack, such as a denial-of-service attack via network connections.
T.T.CONFIGURATION	The TOE user, or an individual on one of the network connections, could modify TOE configuration settings.

Table 3.3-2 – Security Threats Addressed by the TOE Operating Environment

Table Legend	
A = Assumption, P = Policy, T = Threat, O = Objective, .E = Environment, .T = Threat	
Name	**Threat**
T.E.INSTALL	The TOE may be delivered or installed in a manner that undermines security.
T.E.PHYSICAL	Security-critical parts of the TOE may be subjected to a physical attack that may compromise security.
T.E.SYSTEM-CORRUPTED	The security state of the TOE, as a result of another threat, may be intentionally corrupted to enable future insecurities.
T.E.ADMIN-ERROR	The security of the TOE may be reduced or defeated during installation or reconfiguration due to errors or omissions in the administration of the security features of the TOE.

Chapter 4

Chapter 4 Security Objectives

4.1 IT Security Objectives

The following Security Objectives are directly related to the TOE. All of the Objectives listed in this section ensure that all of the Security Threats listed in Table 3.3-1 have been countered.

Table 4.1 – IT Security Objectives

Table Legend	
A = Assumption, P = Policy, T = Threat, O = Objective, .E = Environment, .T = Threat	
IT Security Objective	**Corresponding Threats, Assumptions, and Policies**
O.T.INFO-FLOW: The TOE will ensure that any information flow between disk areas and network connections are controlled.	T.T.TRANSFER T.T.COPY
O.T.NETWORK: The TOE will not be able to connect to both networks at the same time.	T.T.ENTRY T.T.ATTACK
O.T.DISK: The TOE will protect information stored in the TOE's disk partitions not related to the state the machine is currently in.	T.T.DATA T.T.TRANSFER T.T.MEMORY
O.T.FLOPPY: The TOE will prevent switching between machine states upon detection of a floppy diskette being accessed during the Transition state.	T.T.COPY
O.T.TRANSFER: The TOE will be able to disable the transfer of information to floppy drives, SCSI connections, or parallel port connections in "A" or "B" state. *Note: This objective can only be accomplished if the optional TOE cables are installed and the card has been configured accordingly.	T.T.DISK
O.T.CONFIGURATION: The TOE will protect configuration settings from being altered by any individual other than the Administrator.	T.T.MEMORY T.T.CONFIGURATION

Table Legend	
A = Assumption, P = Policy, T = Threat, O = Objective, .E = Environment, .T = Threat	
IT Security Objective	**Corresponding Threats, Assumptions, and Policies**
O.T.BYPASS: The TOE will prevent malicious software or users from bypassing or circumventing TOE security function enforcement.	T.T.MEMORY
O.T.ATTACK: The TOE will protect its "A" network from malicious attacks, such as denial-of-service attacks, from individuals on the "B" network.	T.T.ATTACK
O.T.RECOVER: The TOE will provide for recovery to a secure state following a system failure, power failure, or forced shutdown.	T.T.CRASH T.T.DEVICE.FAIL

4.2 Non-IT Security Objectives

Some Assumptions, Policies, or Threats are beyond the capability of the TOE components to adequately mitigate without support from the operational environment. Therefore, the Objectives listed in this section ensure that the Security Assumptions in Table 3.1, the Security Policies listed in Table 3.2, and the Security Threats listed in Table 3.3-2 have been countered.

Table 4.2 – Non-IT Security Objectives

Table Legend	
A = Assumption, P = Policy, T = Threat, O = Objective, .E = Environment, .T = Threat	
Non-IT Security Objective	**Corresponding Threats, Assumptions, and Policies**
O.E.ACCESS: The TOE environment will support the inclusion of access control software, and needs to protect such software from modification	A.E.ACCESS P.E.KNOWN T.E.PHYSICAL
O.E.DELIVERY: Those responsible for the TOE must ensure that the TOE is delivered, installed, and operated in a manner which maintains IT security.	A.E.ADMIN A.E.INSTALL A.E.OS_REQ P.E.ADMIN-TRAIN

Table Legend	
A = Assumption, P = Policy, T = Threat, O = Objective, .E = Environment, .T = Threat	
	P.E.DUE-CARE T.E.INSTALL T.E.ADMIN-ERROR
O.E.MANAGE: Those responsible for the TOE must ensure that it is managed and administered in a manner that maintains IT security.	A.E.ADMIN P.E.ADMIN-TRAIN T.E.ADMIN-ERROR
O.E.PHYSICAL: Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from physical attack that might compromise IT security.	A.E.ADMIN A.E.USER-NEED A.E.ACCESS P.E.USAGE T.E.PHYSICAL T.E.SYSTEM-CORRUPTED T.E.PHYSICAL P.E.KNOWN
O.E.DUE-CARE: The TOE environment, in conjunction with the TOE itself, must be implemented and operated in a manner that clearly demonstrates due-care and diligence with respect to IT related risks to the organisation.	A.E.ADMIN A.E.USER-NEED P.E.DUE-CARE P.E.USAGE P.E.ADMIN-TRAIN

Chapter 5

Chapter 5 Functional Security Requirements

This section contains the functional requirements that must be satisfied by the TOE. These requirements consist of functional components from Part 2 Final of the Common Criteria (CC). Table 5.1 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 5.1 have been satisfied.

Table 5.1 – Functional Components

CC Component	Name	Hierarchical To	Dependency	Objectives Function Helps Address
FDP_ACC.1	Subset Access Control	No Other Component	FDP_ACF.1	O.T.DISK O.T.NETWORK O.T.ATTACK
FDP_ACF.1	Security Attribute Based Access Control	No Other Component	FDP_ACC.1, FMT_MSA.3	O.T.DISK O.T.NETWORK O.T.TRANSFER O.T.ATTACK
FDP_ITC.1	Import of User Data Without Security Attributes	No Other Component	[FDP_ACC.1, or FDP_IFC.1], FMT_MSA.3	O.T.TRANSFER O.T.INFO-FLOW
FIA_UID.2	User Identification Before Any Action	FIA_UID.1	None	O.T.CONFIGURATION O.E.ACCESS
FMT_MSA.1	Management of Security Attributes	No Other Component	[FDP_ACC.1, or FDP_IFC.1], FMT_SMR.1	O.T.CONFIGURATION O.E.MANAGE O.E.DUE-CARE O.E.DELIVERY
FMT_MSA.3	Static Attribute Initialisation	No Other Component	FMT_MSA.1, FMT_SMR.1	O.T.CONFIGURATION O.E.MANAGE O.E.DUE-CARE O.E.DELIVERY

CC Component	Name	Hierarchical To	Dependency	Objectives Function Helps Address
FMT_SMR.1	Security Roles	No Other Component	FIA_UID.1	O.E.ACCESS
FMT_SMR.3	Assuming Roles	No Other Component	FMT_SMR.1	O.T.CONFIGURATION O.T.BYPASS O.E.ACCESS
FPT_FLS.1	Failure with Preservation of Secure State	No Other Component	ADV_SPM.1	O.T.RECOVER O.E.PHYSICAL
FPT_RCV.4	Function Recovery	No Other Component	ADV_SPM.1	O.T.RECOVER
FPT_RVM.1	Non-Bypassability of the TSP	No Other Component	None	O.T.BYPASS O.T.FLOPPY
FPT_SEP.3	Complete Reference Monitor	FPT_SEP.2	None	O.T.BYPASS O.T.DISK O.E.PHYSICAL O.E.ACCESS

The functional requirements in the above table are described below in further detail. They are derived verbatim from the Common Criteria Version 2 Part 2 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.

5.1 User Data Protection (FDP)

5.1.1 FDP_ACC.1 Subset Access Control

Hierarchical to: No other component.

5.1.1.1 Partitioning Access Policy

FDP_ACC.1.1 The TSF shall enforce the [*Partitioning Access Policy*] on [*the user's current machine state: "A", "B" and "T"; disk partitions: Transition, Functional,"A", and "B"; network connections: "A" and "B"; and other devices controlled by the Partitioning Access Policy*].

Rationale: In the TOE, the only subjects are users and processes running on behalf of users. The objects are disk partitions, network connections, and other devices controlled by the TOE Security Functions (TSF). The Partitioning Access Policy described in the 2in1 PC™ *Informal Security Policy Model* is enforced by a combination of security functions specified in the 2in1 PC™ *Functional Specification*. A state machine is maintained that provides three user states: A, B, and Transition. While in any given state, the IDE bus monitor permits only IDE hard disk addresses that are within the boundaries of disk partitions to which the user is allowed access, according to the Partitioning Access Policy. The state machine function sets and resets relays to permit network access in accordance with the Partitioning Access Policy. Other optional interfaces may be controlled by the TSF. The optional interfaces may be configured by the administrator with special ribbon cables supplied by Voltaire. These ribbon cables have a jumper that connects to pins on the 2in1 PC™ board to enable or disable their use. Devices so connected are controlled by the TSF.

5.1.1.2 Administrator Access Policy

FDP_ACC.1.1 The TSF shall enforce the [*Administrator Access Policy*] on [*the user roles: administrator and user; for write access to the EEPROM*].

Rationale: This is a role-based access policy providing the administrator the ability to set-up and modify some of the attributes and parameters used by the Partitioning Access Policy. Write access to the EEPROM is physically prohibited while in normal user mode. When the administrator has been identified, by detection of the set-up plug being inserted in the 2in1 PC™ board, write access to the EEPROM is physically enabled.

Dependencies: FDP_ACF.1 Security Attribute Based Access Control.

5.1.2 FDP_ACF.1 Security Attribute Based Access Control

Hierarchical to: No other component.

5.1.2.1 Partitioning Access Policy

FDP_ACF.1.1 The TSF shall enforce the [*Partitioning Access Policy*] to objects based on [*the user's currently active machine state, disk partition address, network connection type, and pin connection for external devices controlled by the TOE*].

Rationale: The allowable attributes are as follows:

Machine State	A, B, or T
Disk Partitions	A, B, T, or F
Network Connections	A or B
Floppy Disk or SCSI drive	A, B, !A, or !B

(Note: !A means available in all states except A, !B means available in all states except B. Either of these provides for the device to be available during the Transition state.)

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*users in a given state have access only to disk partitions, network connections, and other TOE controlled interfaces authorised for their current state*].

Rationale: In state A, users have access only to disk partition A, and possibly F (depending on the security policy settings selected by the administrator), network connection A, and possibly floppy disk and SCSI interfaces (depending on the security policy settings selected by the administrator and cables connecting the devices). In state B, users have access only to disk partition B, and possibly F (depending on the security policy settings selected by the administrator), network connection B, and possibly floppy disk and SCSI interfaces (depending on the security policy settings selected by the administrator and cables connecting the devices). The floppy disk and SCSI interfaces, if configured as part of the TSF Scope of Control (TSC), are not available in both state A and state B. The existence of, and access policy for, disk partition F is selectable by the administrator. If partition F exists, the default settings are read access from state A and read/write access from state B. An administrator selectable setting of read only from state A and read/write from state B would allow the passing of information from state B to state A, but not from state A to state B. The TOE enforces its Partitioning Access Policy, as shown in Table 5.2.

Table 5.2 - Partitioning Access Policy Rules

	State A	State B	State T
Four Separate Disk Partitions			
A	R/W	None	None
B	None	R/W	None
T	None	None	*
F	*	*	*
Two Network Connections			
A	Connected	Not Connected	Not Connected
B	Not Connected	Connected	Not Connected
Other Interface (e.g., Floppy and SCSI interfaces)-as configured.			
A	Connected	Not Connected	Not Connected
!A	Not Connected	Connected	Connected
B	Not Connected	Connected	Not Connected
!B	Connected	Not Connected	Connected

* Administrator selectable.

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*when the administrator has entered set-up mode, unconditional access is granted to the entire hard disk and to other controlled devices connected to the !A (Not A) and !B (Not B) jumper pins*].

Rationale: The administrator role is identified by the setup plug being inserted into the 2in1 PC™ board. In this role, access is allowed to all disk partitions. Typically, the administrator accesses only partitions associated with the partition he is booted from, but that access is not monitored or controlled by the TOE.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [*administrator having entered set-up mode, then no network connections are allowed and other controlled device access is not allowed to devices connected to the A and B jumper pins*].

Rationale: The state machine function causes relays to be thrown, disconnecting both A and B networks, when it detects the presence of the setup plug

5.1.2 Administrator Access Policy

The Administrator Access Policy provides the rules for write access to the EEPROM by the user roles. The following requirements apply to the Administrator Access Policy.

FDP_ACF.1.1 The TSF shall enforce the [*Administrator Access Policy*] to objects based on [*the user role: user or administrator, for write access to the EEPROM*].

Rationale: For the Administrator Access Policy, the attributes are the user roles: user (normal user) or administrator.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*administrators are allowed to write to the EEPROM; users are denied write access to the EEPROM*].

Rationale: The administrator role is identified by the setup plug being inserted into the 2in1 PC™ board. When the setup plug is in place, write access is physically enabled to the EEPROM. Typically, the administrator uses utilities provided on the 2in1 PC™ installation disks to manage EEPROM information. These utilities are part of the TOE, however are defined to be outside the scope of the TSF.

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*none*].

Rationale: There are no other rules that apply to write access to the EEPROM.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [*none*].

Rationale: There are no other rules that apply to write access to the EEPROM.

Dependencies: FDP_ACC.1 Subset Access Control,

FMT_MSA.3 Static Attribute Initialisation.

5.1.3 FDP_ITC.1 Import of User Data Without Security Attributes

Hierarchical to: No other components.

FDP_ITC.1.1 The TSF shall enforce the [*Partitioning Access Policy*] when importing user data, controlled under the SFP, from outside of the TSC.

Rationale: In user mode (i.e., states A or B), data may be imported only from devices that are authorised for the particular machine state, and will be stored in a disk partition appropriate for that machine state. For example: In machine state B, data may only be imported from network B or devices (e.g., floppy drive, SCSI disk) that have been properly set up for state B by the administrator. That data may be stored in disk partition B or, depending on the administrator provided security policy, in disk partition F.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

Rationale: External security attributes, such as security labels, are not recognised by the TOE. The only security attributes recognised by the TOE are the assignments associated with machine state, disk partition, or other devices controlled by the TOE (i.e., A, B, T, or F).

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [*user data imported under the control of the TSF is assigned the security attribute of the current machine state (i.e., A or B)*].

Rationale: In work mode, all data imported under control of the TSF is assigned the security attribute of the current machine state.

Dependencies: [**FDP_ACC**.**1** Subset Access Control,

or

FDP_IFC.1 Subset Information Flow Control],

FMT_MSA.3 Static Attribute Initialisation.

5.2 Identification and Authentication (FIA)

5.2.1 FIA_UID.2 User Identification Before Any Action

Hierarchical to: FIA_UID.1 Timing of Identification

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Rationale: The TOE identifies only user roles (i.e., user and administrator), not users as individuals. By definition, any individual operating without the setup plug in place is a user. Also by definition, any individual operating with the setup plug in place is an administrator.

Dependencies: No dependencies.

5.3 Security Management (FMT)

5.3.1 FMT_MSA.1 Management of Security Attributes

Hierarchical to: No other components.

FMT_MSA.1.1 The TSF shall enforce the [*Administrator Access Policy*] to restrict the ability to [*change_default and modify*] the security attributes [*partition boundary addresses, MBRs, access rights, switching policies, and internal setup information*] to [*the administrator that has entered set-up mode*].

Rationale: In normal user mode, no write access is allowed to the EEPROM, where most of the security attribute information, including partition boundary addresses, access rights, and switching policies, is stored. When the setup plug is in place, the administrator may modify these attributes

Dependencies: [**FDP_ACC.1** Subset Access Control,

or

FDP_IFC.1 Subset Information Flow Control],

FMT_SMR.1 Security Roles.

5.3.2 FMT_MSA.3 Static Attribute Initialisation

The TOE provides two different types of default accesses policies for the Functional partition, if one exists. For the Transition state, the defaults are restrictive. For states A and B, the default is for a "read down" access policy, where state B may read and write to the Functional partition and state A may only read from the Functional partition.

Hierarchical to: No other components.

5.3.2 Transition State

FMT_MSA.3.1 The TSF shall enforce the [*Partitioning Access Policy*] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.

Rationale: The SFP is enforced in the Transition state. Administrator selectable access rules for the transition state default to the most restrictive case, as shown in the access security policy. From the Transition state, the T partition is read only and no other partitions are accessible.

5.3.2 States A and B

FMT_MSA.3.1 The TSF shall enforce the [*Partitioning Access Policy*] to provide [*read down*] default values for security attributes that are used to enforce the SFP.

Rationale: The SFP is enforced in the Transition state. Administrator selectable access rules for states A and B default to a "read down" case, as shown in the access security policy. Where state A is assumed to be a more restrictive state than state B, state B may read and write to the Functional partition and state A may only read from the Functional partition. This will allow the flow of information from state B to state A, but not from A to B.

5.3.2 All States

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.

Rationale: In setup mode, write access is logically and physically enabled to the EEPROM, and the administrator has the capability to specify alternative initial values to override default values. Typically, the administrator uses utilities provided on the 2in1 PC™ installation disks to set initial values and/or override default values in the EEPROM. These utilities are part of the TOE, however are defined to be outside the scope of the TSF.

Dependencies: FMT_MSA.1 Management of Security Attributes,

FMT_SMR.1 Security Roles

5.3.3 FMT_SMR.1 Security Roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles [*Administrator and user*].

Rationale: There are two roles recognised by the TSF, the user role and the administrator role. There are specific actions that may only occur in one of the recognised roles.

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

Rationale: All users operating the TOE in work mode are in the user role. Anyone operating the system in setup mode are considered to be in the administrator role. There are specific actions that may only occur in these two recognised roles.

Dependencies: FIA_UID.1 Timing of Identification.

5.3.4 FMT_SMR.3 Assuming Roles

Hierarchical to: No other components.

FMT_SMR.3.1 The TSF shall require an explicit request to assume the following roles: [*Administrator*].

Rationale: Installation of the setup plug is the explicit action necessary to assume the administrator role. Anyone operating the system without being in setup mode is considered to be a normal user.

Dependencies: FMT_SMR.1 Security Roles.

5.4 Protection of the TOE Security Functions (FPT)

5.4.1 FPT_FLS.1 Failure with Preservation of Secure State

Hierarchical to: No other components.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [*forced shutdown, power failure, or system failure*].

Rationale: Under forced shutdown, power failure, or system failure while in work mode, the TSF does not respond until it has reached the Transition state.

Dependencies: ADV_SPM.1 Informal TOE Security Policy Model.

5.4.2 FPT_RCV.4 Function Recovery

Hierarchical to: No other components.

FPT_RCV.4.1 The TSF shall ensure that [*forced shutdown, power failure, or system failure while in work mode*] have the property that the SF either completes successfully, or for the indicated failure scenarios, recovers to a consistent and secure state.

Rationale: In work mode, the TSF recovers to, or through, the Transition state after any forced shutdown, power failure, or system failure.

Dependencies: ADV_SPM.1 Informal TOE Security Policy Model.

5.4.3 FPT_RVM.1 Non-Bypassability of the TSP

Hierarchical to: No other components.

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

Rationale:
There are four user visible functions that the TSF controls, they are:

a) Read or write access to a disk partition,
b) Read or write access to a network connection,
c) Read or write access to another (optional) TSF controlled device, and
d) Switch user states.

The TSF controls each of these functions and allows them to proceed only if they comply with the TOE access security policy. Additionally, the user state switch may occur only if no DMA2 activity has occurred during the Transition state.

Dependencies: No dependencies.

5.4.4 FPT_SEP.3 Complete Reference Monitor

Hierarchical to: FPT_SEP.2 SFP Domain Separation.

FPT_SEP.3.1 The unisolated portion of the TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

Rationale: The TOE security policy is enforced entirely by the 2in1 PC™ board. The TSF is isolated from interference or modification. The state machine implementation is in the Altera chip that is loaded from ROM and is not accessible by untrusted subjects. The

EEPROM is not writeable without the setup plug, and therefore not writeable by untrusted subjects. The IDE checking is also implemented in the Altera chip that is loaded from ROM, and its security attributes are on the EEPROM. The Altera chip has no input interface open to the PC.

FPT_SEP.3.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

Rationale: The user security domains are maintained by a combination of security features implemented on the 2in1 PC™ board. The 2in1 PC™ Partitioning Access Policy is intended to contain a user session to an authorised environment that includes a network connection, disk partition(s), and other local interfaces, depending on the local organisation security policy and the administrator controlled settings.

FPT_SEP.3.3 The TSF shall maintain the part of the TSF that enforces the access control and/or information flow control SFPs in a security domain for its own execution that protects them from interference and tampering by the remainder of the TSF and by subjects untrusted with respect to the TSP.

Rationale: The TOE security policy is enforced entirely by the 2in1 PC™ board. The access control SFPs covered in this requirement are the Partitioning Access Policy and the Administrator Access Policy. There are no information flow control policies for this TOE. That card is isolated from interference or modification. The state machine, IDE checking, and network and other hardware interface access control implementation is in the Altera chip that is loaded from ROM. The Altera chip has no input interface open to the PC. Object security attributes are on the EEPROM and are not writeable without the setup plug, and therefore not writeable by untrusted subjects.

Dependencies: No dependencies.

Chapter 6

Chapter 6 Assurance Requirements

The assurance requirements for EAL-2 are met by the TOE, including minor assurance requirement augmentations to EAL-2. 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 wide-spread acceptance, by expressing it's claims against EAL-2 from part 3 of the Common Criteria; augmented by the CC assurance component ADV_SPM.1.

The assurance components for the TOE are summarised in Table 6-1. Table 6-2 lists those components of the TOE that augment EAL-2 from part 3 of the CC. Section 6.1 lists the details of these assurance components.

Table 6.1 – TOE Assurance Components

Assurance Class	Component ID	Component Title
Configuration Management	ACM_CAP.2	Configuration Items
Delivery and Operation	ADO_DEL.1	Delivery Procedures
Delivery and Operation	ADO_IGS.1	Installation, Generation, and Start-Up Procedures

Assurance Class	Component ID	Component Title
Development	ADV_FSP.1	Informal Functional Specification
Development	ADV_HLD.1	Descriptive High-Level Design
Development	ADV_RCR.1	Informal Correspondence Demonstration
Guidance Documents	AGD_ADM.1	Administrator Guidance
Guidance Documents	AGD_USR.1	User Guidance
Tests	ATE_COV.1	Evidence of Coverage
Tests	ATE_FUN.1	Functional Testing
Tests	ATE_IND.2	Independent Testing - Sample
Vulnerability Assessment	AVA_SOF.1	Strength of TOE Security Function Evaluation
Vulnerability Assessment	AVA_VLA.1	Developer Vulnerability Analysis

Table 6.2 – TOE Augmentation to EAL-2

Assurance Class	Component ID	Component Title	Augmentation to EAL2
Development	ADV_SPM.1	Informal TOE Security Policy Model	Added Security Policy Model

6.1 Assurance Measures

The assurance measures provided by the TOE satisfy all of the assurance requirements listed in Chapter 6, Table 6.1 and Table 6.2. These assurance requirements have been reiterated below along with the titles of vendor documentation that satisfy such requirements. Table 6.3 provides a reference between each TOE assurance requirement and all related documentation that satisfies each requirement.

6.1.1 Configuration Management (ACM)

6.1.1 ACM_CAP.2 Configuration Items

Documentation: Configuration Items, 2in1 PC™ Installation Guide Ver.1.21.

Dependencies: No dependencies.

6.1.2 Delivery and Operation (ADO)

6.1.2 ADO_DEL.1 Delivery Procedures

Documentation: Product Approval Tests for 2in1 PC™ , Delivery Procedures.

Dependencies: No dependencies.

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

Documentation: 2in1 PC™ Installation Guide Ver. 1.21, 2in1 PC™ Quick Installation Guide Ver. 1.21, Application Notes Ver. 1.21, 2in1 PC™ User Guide Ver. 1.21.

Dependencies: AGD_ADM.1 Administrator Guidance.

6.1.3 Development (ADV)

6.1.3 ADV_FSP.1 Informal Functional Specification

Documentation: 2in1 PC™ System Design Document, 2in1 PC™ Functional Specification, 2in1 PC™ Updates to the SYD EEPROM Mapping Section.

Dependencies: ADV_RCR.1 Informal Correspondence Demonstration.

6.1.3 ADV_HLD.1 Descriptive High-Level Design

Documentation: 2in1 PC™ System Design Document, 2in1 PC™ Addendum to the System Design Document - High-Level Design, 2in1 PC™ Updates to the SYD EEPROM Mapping Section.

Dependencies: ADV_FSP.1 Informal Functional Specification,
ADV_RCR.1 Informal Correspondence Demonstration.

6.1.3 ADV_RCR.1 Informal Correspondence Demonstration

Documentation: System Design Document, Functional Specification, Mapping of Assurance Elements, Updates to the SYD EEPROM Mapping Section, Addendum to the System Design Document - High-Level Design.

Dependencies: No dependencies.

6.1.3 ADV_SPM.1 Informal TOE Security Policy Model

Documentation: Informal Security Policy Model, Functional Specification.

Dependencies: ADV_FSP.1 Informal Functional Specification.

6.1.4 Guidance Documents (AGD)

6.1.4 AGD_ADM.1 Administrator Guidance

Documentation: 2in1 PC™ Installation Guide Ver. 1.21, 2in1 PC™ Quick Installation Guide Ver. 1.21, Application Notes Ver. 1.21, 2in1 PC™ User Guide Ver. 1.21., Administrative Rights, Physical Data Security : 2in1 PC™, Security Policy, Flow Policy, 2in1 PC™ White Paper.

Dependencies: ADV_FSP.1 Informal Functional Specification.

6.1.4 AGD_USR.1 User Guidance

Documentation: 2in1 PC™ User Guide Ver. 1.21.

Dependencies: ADV_FSP.1 Informal Functional Specification.

6.1.5 Tests (ATE)

6.1.5 ATE_COV.1 Evidence of Coverage

Documentation: Coverage Tests.

Dependencies: ADV_FSP.1 Informal Functional Specification,
ATE_FUN.1 Functional Testing.

6.1.5 ATE_FUN.1 Functional Testing

Documentation: Functional Tests, Functional Specification, Test Coverage.

Dependencies: No dependencies.

6.1.5 ATE_IND.2 Independent Testing - Sample

Documentation: Hacking Tests, Vulnerability Analysis, Functional Specification, Functional Tests, Test Coverage.

Dependencies: ADV_FSP.1 Informal Functional Specification,
AGD_ADM.1 Administrator Guidance,
AGD_USR.1 User Guidance,
ATE_FUN.1 Functional Testing.

6.1.6 Vulnerability Assessment (AVA)

6.1.6 AVA_SOF.1 Strength of TOE Security Function Evaluation

Documentation: None, the TOE claims no strength of function.

Dependencies: ADV_FSP.1 Informal Functional Specification,
ADV_HLD.1 Descriptive High-Level Design.

6.1.6 AVA_VLA.1 Developer Vulnerability Analysis

Documentation: White Box Checks, Hacking Testing.

Dependencies: ADV_FSP.1 Informal Functional Specification,
ADV_HLD.1 Descriptive High-Level Design,
AGD_ADM.1 Administrator Guidance,
AGD_USR.1 User Guidance.

Table 6.3 – Assurance Measures

Assurance Component	Documentation Satisfying Component
ACM_CAP.2	Configuration Items, 2in1 PC™ Installation Guide Ver.1.21
ADO_DEL.1	Product Approval Tests for 2in1 PC™, Delivery Procedures
ADO_IGS.1	2in1 PC™ Installation Guide Ver.1.21, 2in1 PC™ Quick Installation Guide Ver. 1.21, Application Notes Ver. 1.21, 2in1 PC™ User Guide Ver. 1.21
ADV_FSP.1	2in1 PC™ System Design Document, 2in1 PC™ Functional Specification, 2in1 PC™ Updates to the SYD EEPROM Mapping Section
ADV_HLD.1	2in1 PC™ System Design Document, 2in1 PC™ Addendum to the System Design Document - High-Level Design, 2in1 PC™ Updates to the SYD EEPROM Mapping Section

ADV_RCR.1	2in1 PC™ System Design Document, Functional Specification, Mapping of Assurance Elements, Updates to the SYD EEPROM Mapping Section, Addendum to the System Design Document - High-Level Design
ADV_SPM.1	Informal Security Policy Model, Functional Specification
AGD_ADM.1	2in1 PC™ Installation Guide Ver. 1.21, 2in1 PC™ Quick Installation Guide Ver. 1.21, Application Notes Ver. 1.21, 2in1 PC™ User Guide Ver. 1.21., Administrative Rights, Physical Data Security : 2in1 PC™, Security Policy, Flow Policy, 2in1 PC™ White Paper
AGD_USR.1	2in1 PC™ User Guide Ver. 1.21.
ATE_COV.1	Coverage Tests
ATE_FUN.1	Functional Tests, Functional Specification, Test Coverage
ATE_IND.2	Hacking Tests, Vulnerability Analysis, Functional Specification, Functional Tests, Test Coverage
AVA_SOF.1	None, the TOE claims no strength of function
AVA_VLA.1	White Box Checks, Hacking Testing

Chapter 7

Chapter 7 TOE Summary Specification

7.1 TOE Security Functions

The major functions implemented by the TOE are:

SETUP – Allow the setting up and configuration of the TOE attributes:

When the 2in1 PC™ board is determined to be in Setup mode (Setup plug is inplace), the EEPROM is made writeable. The attributes (partition access settings / partition size settings / configuration settings, hard disk parameters) are input through the IDE bus and stored on the EEPROM.

STORE – Provide storage for configuration data (including card configuration and MBRs):

When queried by either internal or external clients, the data stored on the EEPROM is provided.

STATE – In Work mode, provide a state machine with three distinct states of operation: A, B and T (Transition):

The card's logic core (Altera chip) knows what state it is currently in and what the allowable state changes are. Founded on pre-configured properties, it is initialised to a certain state at power-up, and from that point onwards has to adhere to a strict protocol in order to change the state.

BOOT – In Work mode, provide a different MBR for each security state during boot:

As the card's logic core (Altera chip) monitors the IDE bus, it listens for the READ MBR (0,0,1) command. Upon detection thereof, it responds by sending back either an MBR from the EEPROM, or (when the AMO option is set and the card is in state A), the actual hard-disk based A MBR, thereby enabling booting from a different partition after every state change. *Note:* this behavior is not BIOS dependent – the card is indifferent to whom the originator of the READ/WRITE (0,0,1) is, and is only aware of the IDE traffic itself.

AC_DISK – In Work mode, control access to disk partitions based on the current security state and the access security policy:

The card's logic core (Altera chip) monitors the disk commands and addresses, and compares the requested address and command to borders, functional partition settings and other configuration data stored on the EEPROM. Based upon that information and the current security state, it decides whether to block the signal or allow it to proceed to the hard disk itself.

AC_NW – In Work mode, control access to networks based on the current security state and the access security policy:

Based upon the current security state, the Altera chip controls the electro-mechanical relays which sever or connect the communication cables.

CHANGE – In Work mode, control the flow of state changes:

When the switch command is received by the card (whether originated by the user or automatically), it awaits a reset signal either on the ISA bus or on the IDE bus to ensure that an actual reboot is occurring before the logic core actually switches the security state. If the card is connected to the motherboard's reset pins using the provided cable, the card will actually initiate the reset (by generating a reset signal on the jumper pins), and not only monitor it. If the switch disable signal is detected, switching would be prevented, and the card would remain in its current state.

FLOPPY – In Work mode, monitor access to the floppy disk during the Transition state and prevent state switching upon detection thereof:

Upon detection of floppy access during the Transition state, the card's logic core (Altera chip) prevents further switching during the current session. To clear this condition, the PC must be rebooted (a soft reboot is sufficient) and the Transition state must be repeated without any floppy access.

AC_DEV – In Work mode, Control access to external devices such as floppy drives and SCSI disks:

Based upon the current security state, the logic core opens and closes electro-mechanical relays. If a device is connected to the A jumpers, it will be unavailable in all states except A. If a device is connected to the Not-A (!A) jumpers, it will be available in all states except A. If a device is connected to the B jumpers, it will be unavailable in all states except B. If a device is connected to the Not-B (!B) jumpers, it will be available in all states except B.

MODE – Detect the presence of a physical setup plug in order to switch into Setup mode and allow configuration:

The 2in1 PC™ board logic core (Altera chip) monitors the Setup connector pins for a specific short pattern, and thus determines that the Setup plug is in fact inserted on the connector. In Setup mode, the state machine is disabled (internal).

Figure 7.1 shows the mapping between the functions above and the security functional requirements.

Table 7.1 – Functions to Security Functional Requirements Mapping

Functions	Security Functional Requirements
SETUP	FDP_ACC.1, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3, FPT_RVM.1,
STORE	FDP_ACC.1, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3, FPT_RVM.1,
STATE	FDP_ACC.1, FDP_ACF.1, FDP_ITC.1, FPT_FLS.1, FPT_RCV.4, FPT_RVM.1, FPT_SEP.3
BOOT	FDP_ACC.1, FDP_ACF.1, FPT_FLS.1, FPT_RVM.1
AC_DISK	FDP_ACC.1, FDP_ACF.1, FDP_ITC.1, FPT_FLS.1, FPT_RCV.4, FPT_RVM.1, FPT_SEP.3
AC_NW	FDP_ACC.1, FDP_ACF.1, FDP_ITC.1, FPT_FLS.1, FPT_RCV.4, FPT_RVM.1, FPT_SEP.3
CHANGE	FDP_ACC.1, FDP_ACF.1, FPT_RVM.1
FLOPPY	FPT_RVM.1
AC_DEV	FDP_ACC.1, FDP_ACF.1, FDP_ITC.1, FPT_FLS.1, FPT_RCV.4, FPT_RVM.1, FPT_SEP.3
MODE	FIA_UID.2, FMT_SMR.1, FMT_SMR.3, FPT_RVM.1, FPT_SEP.3

Figure 7.2 shows the mapping between the security functional requirements and the functions listed above.

Table 7.2 – Security Functional Requirements to Functions Mapping

Security Functional Requirements	Functions
FDP_ACC.1	SETUP, STORE, STATE, BOOT, AC_DISK, AC_NW, CHANGE, AC_DEV,
FDP_ACF.1	SETUP, STORE, STATE, BOOT, AC_DISK, AC_NW, CHANGE, AC_DEV,
FDP_ITC.1	STATE, AC_DISK, AC_NW, AC_DEV
FIA_UID.2	MODE
FMT_MSA.1	SETUP, STORE
FMT_MSA.3	SETUP, STORE
FMT_SMR.1	MODE
FMT_SMR.3	MODE
FPT_FLS.1	STATE, BOOT, AC_DISK, AC_NW, AC_DEV,

FPT_RCV.4	STATE, AC_DISK, AC_NW, AC_DEV,
FPT_RVM.1	SETUP, STORE, STATE, BOOT, AC_DISK, AC_NW, CHANGE, FLOPPY, AC_DEV, MODE,
FPT_SEP.3	STATE, AC_DISK, AC_NW, AC_DEV, MODE

The assurances presented for the TOE are shown in Table 7.3.

Table 7.3 – Assurance Requirements

Assurance Requirement	Description
ACM_CAP.2	Configuration Items
ADO_DEL.1	Delivery Procedures
ADO_IGS.1	Installation, Generation, and Start-Up Procedures
ADV_FSP.1	Informal Functional Specification
ADV_HLD.1	Descriptive High-Level Design
ADV_RCR.1	Informal Correspondence Demonstration
ADV_SPM.1	Informal TOE Security Policy Model
AGD_ADM.1	Administrator Guidance
AGD_USR.1	User Guidance
ATE_COV.1	Evidence of Coverage
ATE_FUN.1	Functional Testing
ATE_IND.2	Independent Testing – Sample
AVA_SOF.1	Strength of TOE Security Function Evaluation
AVA_VLA.1	Developer Vulnerability Analysis

Appendix A

Appendix A Acronyms