Secure Analogue and Digital KVM Switches

Black Box models
SW2008A-USB-EAL, SW4008A-USB-EAL, SW2006A-USB-EAL, SW4006A-USB-EAL, SW2009A-USB-EAL, SW4009A-USB-EAL

Adder models
AVSD1002-XX, AVSD1004-XX, AVSV1002-XX, AVSV1004-XX, AVSC1102-XX, AVSC1104-XX

Security Target
(EAL4 augmented by ALC_FLR.2 and ATE_DPT.2)

Version 1.2
Date: 26 November 2010

Prepared by: Logica UK Limited

Prepared for: Black Box Corporation
Adder Technology Limited

Black Box Corporation
1000 Park Drive
Lawrence PA 15055
US

Adder Technology Limited
Technology House
Trafalgar Way
Bar Hill, Cambridge
CB23 8SQ, UK

Contents

List of Tables

List of Figures

Revision History

Date	Version	Details
25 Sept 2009	0.1	First draft. Chapters 8 and 9 to be completed when all switch design details are finalised.
22 Oct 2009	0.2	Second draft addressing Certifier's comments on v0.1.
5 Feb 2010	0.3	Third draft addressing Observation Reports. (Note Chapter 9 is still to be completed.)
17 Nov 2010	0.4	Fourth draft addressing Protection Profile updates, and completion of Chapters 8 and 9.
18 Nov 2010	1.0	First complete issue.
23 Nov 2010	1.1	Date of reference [PPv21] corrected (section 1.2)
26 Nov 2010	1.2	Version number of this document corrected in section 2.1

1 Preamble

1.1 Document Purpose and Conventions

1 This document is the Security Target (ST) relating to twelve Keyboard-Video-Mouse (KVM) switches supplied by Black Box Corporation and Adder Technology Limited. It is written to conform to the requirements of the Common Criteria (CC) for Information Technology Security Evaluation (see [CC]).

2 The twelve KVM switches are identified in Section 2.2 below. Requirements placed on “the TOE” or “the TSF” in this ST apply to each one of these twelve switches; for example, a security requirement that specifies “The TSF shall ...” applies to each and every switch. In other words, each and every switch is to be evaluated in accordance with the CC evaluation methodology (see [CEM]).

3 If it is necessary to refer to all twelve switches collectively, the term “the set of TOEs” may be used as an alternative to “all twelve switches”.

4 A specific switch is identified as such (using the identifiers stated in Section 2.2).

5 References (see Section 1.2) are given as mnemonics within square brackets.

6 The use of italics (for some terminology) is explained at the start of the Glossary (Section 1.3).

7 Note that, for convenience, and in common with the approach generally adopted for STs concerned with IT products, this document uses “switch” when, strictly speaking, “type of switch” or “model” would be more accurate.

1.2 References

[CC] Common Criteria for Information Technology Security Evaluation, Parts 1-3, CCMB-2009-07-001-3, Version 3.1 Revision 3 Final, July 2009

[CEM] Common Methodology for Information Technology Security Evaluation, CCMB-2009-07-004, Version 3.1 Revision 3 Final, July 2009

[GPG] CESG Good Practice Guide No. 11, KVM switches, Issue 1.2, March 2009

[PD093] Precedent Database PD-0093: Questions concerning the Peripheral Sharing Switch PP, see http://www.niap-ccevs.org/PD/0093.html

[PD138] Precedent Database PD-0138: Sharing of Peripherals with Memory under the Peripheral Sharing PP, see http://www.niap-ccevs.org/PD/0138.html

[PP] Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile, IAD, Version 1.2, 21 August 2008 (see http://www.niap-ccevs.org/pp/archived/pp_psshid_v1.2/)

[PPv21] Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile, IAD, Version 2.1, 7 September 2010 (see www.commoncriteriaportal.org).

1.3 Glossary

1.3.1 Terms

8 This ST is (demonstrably) conformant with the Peripheral Sharing Switch (PSS) Protection Profile (PP), see [PP], which defines a number of terms that are used throughout the PP. Such of those terms which are considered to be pertinent to this ST are included amongst the following collection of terms; the PP terms are italicised in this ST document whenever they are used in statements (e.g. SFRs) that originate from [PP]. (The PP uses SMALL CAPITALS rather than *italics* to identify specific terms.)

9 The definitions of italicised terms below are generally repeated verbatim from [PP], apart from some changes to make the definitions specific to this ST and the TOE, and some editorial changes (including additional or alternative words which are either taken from other parts of the PP or which are added in order to resolve, for example, a circular definition).

10 However, the [PP] term *Peripheral Port Group ("Group")/ Peripheral Port Group ID* is renamed *port group (id*) - to remove any potential confusion related to the PP's use of *Peripheral Port Group* to relate to both peripherals and computers - and its definition is reworded to align more closely with the TOE description given in Chapter 2 of the PP. (See Section 3.2 below for further comments about the PP.)

attribute	Synonymous in this document with *port group id*, and equivalent to the [CC] Part 1 term "(information) security attribute".
authorised user	A *user* who has been granted permission to interact with the TOE and all of its attached *peripherals* and *computers*. This ST assumes that all *users* are *authorised users.*
computer	A programmable machine. The two principal characteristics of a *computer* are: It responds to a specific set of instructions in a well-defined manner, and It can execute a prerecorded list of instructions (a software program). For the purposes of this document, any programmable machine controlling a monitor and/or loudspeakers, and accepting signals from a keyboard and/or a mouse, will qualify as a *computer*.
channel change	A change (initiated by the *user*) of which *switched computer* is currently *connected* to the TOE.
connected	A state in which information can be intentionally transferred between *device(s)* and *computer(s)*.
connection	A path for information flow between two or more *device(s*) or between two or more *computer(s)* or between *device(s*) and *computer(s)*.
design constraint	In this ST, a design constraint is a contribution towards countering a threat by ruling out possible option(s) available to the TOE designers (e.g. to use re-programmable components), as opposed to specifying an explicit SFR to counter the threat.
device	A unit of hardware/firmware that is capable of providing input to a *computer* and/or of receiving output from a *computer*.
enumeration	The process by which a USB device is configured for use.
id	An identifier. See *port group (id)*.

object	Synonymous in this document with *peripheral data*.
peripheral	A *device* that may be attached to the TOE.
peripheral data	Information, including (buffered) *state information*, sent from or to a *peripheral*.
port group (id)	A subset of the TOE's *ports* that is treated as a single entity by the TOE. There is one *port group* for the set of *shared peripherals* and one *port group* for each *switched computer*. Each *switched computer port group* has a unique logical *id*. The *shared peripherals port group* also has an *id* which at any given time is the same as that of the *switched computer port group* that is currently *connected* to the TOE (as selected by the *authorised user*).
port	One of a number of external sockets on the TOE which are used for attaching *peripherals* and *computers* to the TOE.
residual data	Any *peripheral data* stored in a *switch*.
shared peripheral	A *peripheral* attached to the TOE. (See also *port group*.)
state information	The current or last-known status, or condition, of a process, transaction, or setting. "Maintaining state" means keeping track of such data over time.
subject	Synonymous in this document with *port group*.
switch	A *device* permitting a single set of *peripherals* to be shared among two or more *computers*. Synonymous with "the TOE" in this document.
switched computer	A *computer* attached to the TOE. (See also *port group*.)
TEMPEST	A synonym for Radiation Security.
TOE	See Paragraph 2.
user	The human operator of the TOE. (See also *authorised user*.)
user data	Data for the user, that does not affect the operation of the TSF. (This is taken from the [CC] Part 1 glossary.) Note that, in this ST, "user data" is equivalent to the term "*user* information", which appears without definition in [PP].

1.3.2 Abbreviations

11 Some of the following abbreviations are taken from the [CC] Part 1 glossary.

ARC	(security) Architecture
CAC	Common Access Card
CAD	Computer Aided Design
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme (US)
CEM	Common Criteria Evaluation Methodology
CESG	UK Government's National Technical Authority for Information Assurance (originally an abbreviation of Communications-Electronics Security Group)
CM	Configuration Management
DDC	Display Data Channel - a communication protocol between a graphics card (part of a computer in the context of this ST) and a monitor
DVI	Digital Video Interface
DVI-I	Digital Video Interface - Integrated

EDID	Extended Display Identification Data - a data structure provided by a monitor to describe its capabilities to a graphics card (part of a computer in the context of this ST)
GPG	Good Practice Guide
IAD	Information Assurance Directorate (part of the NSA)
IT	Information Technology
KVM	Keyboard-Video-Mouse
KVMA	Keyboard-Video-Mouse-Audio
LED	Light Emitting Diode
NIAP	National Information Assurance Partnership (US)
NSA	National Security Agency (US)
PCB	Printed Circuit Board
PD	Precedent Database
PP	Protection Profile
PS/2	Personal System/2
PSS	Peripheral Sharing Switch
RAM	Random Access Memory
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
UK	United Kingdom
US	United States
USB	Universal Serial Bus
VGA	Video Graphics Array
VIR	Visual Indication Rule

2 Introduction

2.1 ST Reference

12 This ST document is identified as:

Secure Analogue and Digital KVM Switches
Black Box models SW2008A-USB-EAL, SW4008A-USB-EAL, SW2006A-USB-EAL, SW4006A-USB-EAL, SW2009A-USB-EAL, SW4009A-USB-EAL
Adder models AVSD1002-XX, AVSD1004-XX, AVSV1002-XX, AVSV1004-XX, AVSC1102-XX, AVSC1104-XX
Security Target (EAL4 augmented by ALC_FLR.2 and ATE_DPT.2),
Version 1.2 of 26 November 2010,
prepared by Logica UK Limited for Black Box Corporation and Adder Technology Limited.

2.2 TOE Reference

13 The set of TOEs is identified in the following table. “XX” in the Part No. indicates the mains lead country code, as follows:

a) UK = United Kingdom

b) US = United States

c) EURO = Europe

d) AUS = Australia.

Table 1 The set of TOEs

Model, i.e. switch (type)	Part No.	Identifier (in this ST)
Black Box ServSwitch Secure USB DVI 2 port switch	SW2008A-USB-EAL	BServD-2
Black Box ServSwitch Secure USB DVI 4 port switch	SW4008A-USB-EAL	BServD-4
Black Box ServSwitch Secure USB VGA 2 port switch	SW2006A-USB-EAL	BServV-2
Black Box ServSwitch Secure USB VGA 4 port switch	SW4006A-USB-EAL	BServV-4
Black Box ServSwitch Secure USB VGA 2 port switch with card reader	SW2009A-USB-EAL	BServC-2
Black Box ServSwitch Secure USB VGA 4 port switch with card reader	SW4009A-USB-EAL	BServC-4
AdderView Secure DVI 2 port switch	AVSD1002-XX	AViewD-2
AdderView Secure DVI 4 port switch	AVSD1004-XX	AViewD-4
AdderView Secure VGA 2 port switch	AVSV1002-XX	AViewV-2
AdderView Secure VGA 4 port switch	AVSV1004-XX	AViewV-4
AdderView Secure VGA 2 port switch with card reader	AVSC1102-XX	AViewC-2
AdderView Secure VGA 4 port switch with card reader	AVSC1104-XX	AViewC-4

2.3 TOE Overview

14 Each of the TOEs is a KVM switch (also known as a PSS switch). This is a set of hardware and firmware within a metal case, to which may be attached, via cables, two or four computers (depending on whether the TOE is a 2 port or 4 port switch) and a single set of peripherals (USB keyboard, video monitor and USB mouse). Each of the TOEs requires an external power supply.

15 The BServD-2/-4 and AViewD-2/-4 switches handle dual link DVI-I video traffic, i.e. both digital and analogue traffic; the other switches handle analogue video traffic only. The BServD-2/-4 and AViewD-2/-4 switches also handle computer audio output signals, i.e. they are actually KVMA switches to which loudspeaker(s) may be attached; the other switches are not KVMA switches.

16 The BServC-2/4 and the AViewC-2/4 switches also support a smartcard - e.g. Common Access Card (CAC) - reader, i.e. such a device may be attached to them (in addition to a keyboard, monitor and mouse); the other switches do not support a card reader.

17 A legacy computer which handles PS/2 (as opposed to USB) keyboard and mouse signals may be attached to a BServV-2/4, AViewV-2/4, BServC-2/4 or AViewC-2/4 switch (i.e. a switch that supports analogue video traffic only). The attachment is via a different type of cable from that normally supplied to connect computers to these switches; the conversion between the computer's PS/2 signals and the peripherals' USB signals is done automatically by the switch.

18 A representative 4 port KVM switch in its operational environment is depicted in Figure 1.

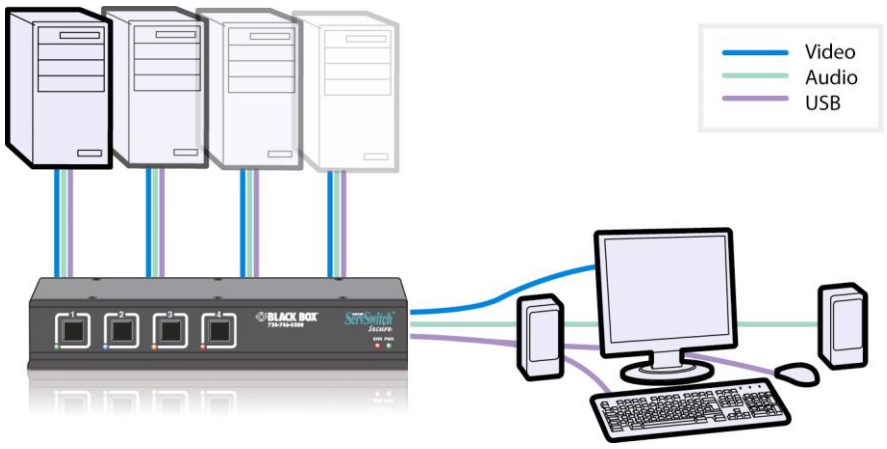

Figure 1 A typical 4 port KVM switch

19 At any one time, the peripherals are connected, through the TOE, to just one of the computers, as indicated by which light (out of 2 or 4) is illuminated on the TOE's front panel. A user can change the connection, i.e. switch the peripherals to connect to another computer attached to the TOE, by means of push buttons on the front panel.

20 The user interacts with the currently connected computer, via the peripherals, exactly as if the peripherals were connected directly to that computer. Hence, the purpose of the TOE is, in essence, to enable the user(s) to economise on peripheral equipment acquisition costs and operating space requirements.

21 Apart from requiring an external power supply, the TOE is entirely self-contained, i.e. it does not require any other hardware, firmware or software in order to function. (However, obviously, it can perform no useful function until a set of peripherals and more than one computer are attached to it.)

22 From a security viewpoint, the TOE has to ensure that user data cannot be shared or transferred between computers via the TOE. This is particularly important where user data processed on one computer is more highly classified (i.e. protectively marked) than data processed on another computer.

23 The TOE includes various design features to meet this security requirement, in particular:

a) Unidirectional flow of keyboard and mouse data;

b) Dedicated Display Data Channel (DDC) bus and Extended Display Identification Data (EDID) memory emulation;

c) Active erasing of USB host controller circuit RAM at each channel change;

d) Unambiguous channel selection.

24 Each of these security features is described further in Subsection 2.4.3. Note that PD-0138 (see [PD138]) recommends that potential consumers of a PSS PP-conformant switch are made aware that such a switch is assumed to operate in a “benign environment” (see the A.SCENARIO assumption in Section 4.3) - in other words, consumers should be aware that the switch does not counter the threat of data leakage through peripheral memory. However, the TOE’s security feature “unidirectional flow of keyboard and mouse data” - which is believed to be unique to the TOE - renders this assumption superfluous, to a large extent (as explained in Subsection 2.4.5).

25 Similarly, the CESG Good Practice Guide (GPG) to KVM switches (see [GPG]), discourages the use of “USB-enabled switches” (i.e. switches, such as the TOE, to which USB peripherals may be attached); but, again, many of the TOE’s security features mitigate against the GPG’s concerns (some of which are similar to those raised in PD-0138). Note also that most modern KVM switches are USB-enabled.

2.4 TOE Description

2.4.1 Taxonomy of the Set of TOEs

26 Apart from the livery on the cases, the six Black Box switches (BServD-2 through to BServC-4) listed in Table 1 are identical to the corresponding Adder switches (AViewD-2 through AViewC-4), and will not be described further in this ST.

27 The security features of the three Adder 2 port switches are identical to those of the corresponding Adder 4 port switches; in fact, the only difference between each pair of switches is that the circuitry and ports in the latter that deal with two of the four ports (to which computers may be attached) are not present in the former. Hence, the three Adder 2 port switches will also not be described further in this ST.

28 Similarly, the AdderView Secure VGA 4 port switch will not be described further in this ST, because this has the same security features as the AdderView Secure VGA 4 port switch with card reader; the only difference is that the circuitry and port in the latter that deals with an attached card reader is not present in the former.

29 Thus, the set of TOEs may be adequately described in this ST by considering:

a) the AdderView Secure DVI 4 port switch (AViewD-4), which is capable of handling dual link DVI-I digital and analogue video traffic; and

b) the AdderView Secure VGA 4 port switch with card reader (AViewC-4), which can handle analogue video traffic only.

30 The main security features of these two switches are described in Subsection 2.4.3. These features are, in essence, common to all twelve switches, and they are the primary means of satisfying the security functional requirements (SFRs) specified in Chapter 7 of this ST.

31 Some other features of the twelve switches are outlined in Subsection 2.4.4. These features are security-related, but in general they do not play as direct a role as the main security features in satisfying the security requirements specified in this ST.

32 A summary of the TOE's design constraints is given in Section 8.4. This includes an outline of how the design of the TOE is constrained (i.e. influenced by) a detailed consideration of how best to counter the threat of information being transferred between computers attached to the TOE.

2.4.2 Scope of the TOE

33 The physical (and logical) scope of the TOE is the whole KVM switch, i.e. the metal case and all the hardware and firmware contained within it.

34 Chapter 9 provides, for each of the set of TOEs, further details of the TOE's components and guidance documentation, and of the peripherals and computers that may be attached to the TOE.

35 Note that this definition of the scope of the TOE does not conflict with the statements above regarding the extent to which the TOE's "Main Security Features" and "Other Features" will be examined during the evaluation of the TOE. In other words, following a successful evaluation of the TOE, potential consumers may have an EAL4 level of confidence that the TOE solves the security problem defined in Chapter 4, plus an additional (but unspecified) level of confidence engendered by the presence of the TOE's "Other Features".

2.4.3 Main Security Features

36 This subsection describes the four main security features of the TOE introduced earlier, which collectively ensure that user data cannot be shared or transferred between computers via the TOE. Further details of how these features are implemented are given in Chapter 8.

37 **Unidirectional flow of keyboard and mouse data**: Data can flow only from the attached keyboard and mouse devices to the TOE's computer ports. Data cannot flow from a computer port to the keyboard and mouse devices. This characteristic is enforced by the hardware design. This ensures that it is not possible for one computer to transfer data to another via means of the keyboard and mouse signalling channels.

38 **Dedicated DDC bus and EDID memory emulation**: The EDID memory device contained within a shared monitor and the DDC bus used to link this to computers can form a potential covert attack channel. To counter this, the TOE has dedicated DDC bus and EDID memory emulation circuitry per computer port. The EDID data is collected once from the monitor when the TOE is powered on and transferred to each of the TOE's computer port circuitry in a unidirectional manner. Since each computer port circuitry has its own copy of the EDID (which cannot be altered by the computer) it is not possible for one computer to transfer information to another via the DDC bus and EDID memory.

39 **Active erasing of USB host controller circuit RAM at each channel change**: At each channel change the TOE's USB host controller circuit (which controls the shared peripherals) erases its entire RAM. This helps guard against any possibility of residual data remaining after a channel change and being transferred to another computer.

40 **Unambiguous channel selection**: The TOE has a selection button per channel (i.e. per switched computer). This allows direct and unambiguous channel selection. In addition, each channel has colour coded visual feedback to confirm the selected channel. The selection buttons provide the only method for changing channel. Common KVM features such as hot key or mouse switching are excluded, preventing remote control of the switch. This policy also reduces the possibility of accidental channel change during normal use.

2.4.4 Other Features of the Switches

41 This subsection describes the "other" security-related features of the twelve switches introduced earlier.

42 **Power down of shared USB peripheral devices during a channel change**: Every time the channel is changed the shared USB peripherals are powered down, reset and re-enumerated. This minimizes the possibility of residual data persisting within buffers of the shared peripherals.

43 **Power down of USB host controller circuit during a channel change**: Every time the channel is changed the TOE's USB host controller circuit is powered down and reset. This - together with the active erasure of its RAM (see Paragraph 39) - minimizes the possibility of residual data persisting in buffers within the host controller circuit.

44 **Dedicated keyboard and mouse peripheral ports**: The TOE's USB host controller circuit will only allow keyboard and mouse devices to be enumerated at the keyboard and mouse ports. Any other type of device connected to the keyboard or mouse ports will be inhibited. Other devices such as USB flash memory drives will not be enumerated.

45 **Keyboard and mouse device emulation**: The TOE emulates a fixed keyboard and mouse device on its keyboard and mouse connections to the computer ports. Regardless of the actual device, or type of device connected to the keyboard or mouse peripheral ports, the computer will see only the emulated keyboard and mouse device. This logically isolates the computer from the attached peripheral devices. For instance, if a memory device was connected into the keyboard or mouse port, the computer would have no knowledge of it and no way to communicate with it.

46 **No common power supply**: To minimise the potential of signaling via the power supply, the TOE does not have a common power supply. Instead, the circuitry associated with each computer port is powered via that computer's USB port, and the shared keyboard, mouse and monitor circuitry is powered by the TOE's power supply.

47 **Non-upgradeable firmware**: Firmware within the TOE is protected from modification and contained in components that are permanently soldered to a PCB. Any changes to the firmware would therefore require intrusive hardware modification.

48 **High port to port electrical isolation**: The TOE exhibits high levels of port to port isolation to facilitate data separation (e.g. RED/BLACK data separation).

49 **Low radiated emissions profile**: The TOE meets the appropriate national requirements (in the country where used) for conducted/radiated electromagnetic emissions. Furthermore, the TOE has a low radiated emissions profile to mitigate against TEMPEST style attacks.

50 **No microphone connection**: Microphone circuitry within a computer enables sensitive recording of small analogue signals. Making a connection to a computer's microphone port therefore poses a potential security threat as very low crosstalk levels potentially could be "recorded" and act as a means by which a non-selected computer could read the data being sent to another computer. Therefore the TOE has no microphone connections to minimize the risk of the user connecting the switch to a sensitive analogue input.

51 **Active erasing of USB host controller circuit data buffers once used**: Once a piece of data has passed through the TOE's USB host controller circuit data buffer, it is erased from the buffer. This helps guard against RAM data remenance.

52 **Tamper-evident seals** (certain models only): The switch is fitted with external tamper-evident seals to give a rapid visual indication of a potential tamper attempt.

53 **Active authentication verification** (certain models only): The switch has an active authentication channel to allow the user to check the status of internal tamper detection circuits (see next paragraph), and to verify that the switch is authentic. User feedback is provided for this purpose.

54 **Active tamper detection** (certain models only): Upon detection of a tamper event, active tamper detection circuits will permanently inhibit normal switch operation and will cause subsequent authentication attempts to fail and to indicate a tampered state.

55 **Dedicated smartcard reader port** (certain models only): The switch has a dedicated port for connection of a smartcard (e.g. CAC) reader peripheral device. Only smartcard reader or combined keyboard and smartcard reader devices will be enumerated at the dedicated smartcard reader port. Any other type of device, e.g. a USB flash memory drive, that is connected to the smartcard reader port will not be enumerated.

56 Note that, although keyboard and mouse data is always sent across the TOE in a unidirectional manner, this is not possible with USB smartcard reader devices as these require bidirectional communication in order to function. The models with smartcard reader support are therefore designed on the principle that they should introduce no greater security risk than would be present if a USB smartcard reader and card were swapped between computers, or a smartcard was swapped between multiple USB smartcard readers (each one connected to a computer).

57 The models which have a dedicated smartcard reader port also have ports - one for each of the (two or four) computers that the model supports - dedicated to connecting the switch to computer(s) that require smartcard support. It is recommended that these ports are not connected (via cables) to any computer(s) that do not require smartcard support.

2.4.5 PD-0138 and CESG GPG Concerns

58 This subsection explains why:

a) The TOE's security feature "unidirectional flow of keyboard and mouse data" counters the threat of data leakage through peripheral memory, i.e. mitigates against the PD-0138 concern referenced earlier;

b) Various features of the TOE mitigate against the concerns expressed in the GESG GPG re the use of USB-enabled switches.

59 PD-0138 highlights the memory in attached devices (i.e. shared peripherals) as a covert channel, whereby data can be written from one computer, to an attached device, and then read by another computer after the channel has been changed. This is a valid concern because it is easy for a typical computer to write into a typical keyboard's memory using standard commands such as "update keyboard LEDs". The TOE prevents this from happening by preventing the computer from writing to the attached keyboard and mouse. Data can only flow from the keyboard and mouse to the computers.

60 The policy of actively powering down (at every channel change) not only the USB host controller but also the attached peripherals and re-enumerating them further helps to reinforce this aspect of the TOE's security features, since any embedded processor in an attached peripheral will be reset and reconfigured.

61 With regard to the CESG GPG: [GPG] Paragraph 32 raises concerns of covert channels existing within a switch; this is mitigated in the TOE by the unidirectional flow of keyboard and mouse data.

62 [GPG] Paragraph 30 raises concern over shared memory that could be used to transfer data from one computer to another; this is mitigated by actively powering down not only the TOE's USB host controller but also the attached peripherals, and also erasing data buffers and memory at each channel change.

63 [GPG] Paragraph 33 considers DDC connections as possible covert attack paths. As highlighted in Section 2.4.3 this is a very real threat that is mitigated by the TOE's dedicated DDC bus and EDID memory emulation.

64 [GPG] Paragraph 33 also considers a microphone connection to be a possible covert attack path. There are no microphone connections on the TOE as they would connect to a sensitive analogue input where very low crosstalk levels could potentially be "recorded" by a computer.

65 [GPG] Paragraph 29 warns of the dangers of upgradeable firmware; the TOE has no re-programmable memory, which protects against modification of the firmware.

66 [GPG] Paragraphs 45 and 46 caution against USB devices that have built-in mass storage, or extra connections for devices such as webcams. The TOE will not enumerate such devices. Only keyboard or mouse devices will be enumerated at the keyboard and mouse ports, and only keyboard and mouse data will be passed across the switch. The smartcard port (certain models only) will only enumerate smartcard readers or combined smartcard and keyboard devices.

67 [GPG] Paragraph 51 recommends the use of tamper-evident seals. Certain models in the set of TOEs are fitted with tamper-evident seals during manufacture. Furthermore, certain models in the set of TOEs have active anti-subversion circuits providing tamper detection and product authentication verification. Any tamper event will disable the function of the switch, and cause subsequent authentication to fail and to indicate a tampered state.

3 Conformance Claims

3.1 Common Criteria Conformance

68 This ST is conformant to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3 Final of July 2009, as follows:

a) Part 2 extended with the EXT_VIR.1 component;

b) Part 3 conformant (EAL4 augmented by ALC_FLR.2 and ATE_DPT.2).

3.2 Protection Profile Conformance and Rationale

69 This ST is demonstrably conformant to the Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile, Version 1.2 of 21 August 2008. (See also Paragraph 74 below.)

70 This PP conformance claim is based on the following rationale:

a) There are fewer assumptions in this ST than in [PP];

b) Subject to the note below re clarifications, and the comments given at the start of Section 1.3 above regarding the definition of terms, the security objectives and requirements specified in this ST are, collectively, identical to or equivalent to or more restrictive than those in [PP] which are applicable to the TOE, and address the same threats as are defined in [PP].

71 In other words, the solution specified in this ST to the generic security problem defined in [PP] is more restrictive than that described in [PP], and hence this ST is demonstrably conformant to [PP] (as permitted by [CC], Part 1, Paragraph 484).

72 Note that the PSS PP Version 1.0 of 8 August 2000 raised several questions, which were listed and addressed in PD-0093 (see [PD093]). Many of these questions relate to the assumptions, threats and objectives defined in the PP v1.0, and their resolution was stated as “This should be clarified in an update to the PP. However, the PP needs not be corrected in order for it to be used in an evaluation”.

73 The assumptions, threats and objectives defined in the PP v1.0 appear to have been carried forward to PP v1.2 with no further clarifications; hence, this ST does not invariably repeat them verbatim, but modifies them where necessary in order to provide the clarifications outlined in PD-0093. Also, for conciseness, this ST replaces the PP words “*peripheral data* and *state information*” with “*peripheral data*” (which is defined, in the PP, to encompass *state information*).

74 Note that (on 18 November 2010) the CC’s official website, www.commoncriteriaportal.org, cites Version 2.1 (dated 7 September 2010, see [PPv21]) as the latest certified version of the PSS PP. This version made a minor correction to Version 2.0 (dated 1 June 2010); a summary of that Version 2.0 update (to PSS PP Version 1.2) is that it included “review and update to the assumptions, threats and objectives. Security functional requirements were adjusted to accommodate the adjustment in the security threats and objectives. A new requirement was added to restrict USB connections and the EAL was changed from four to two. This change also included updates based on questions in PD-0093”.

75 This ST claims conformance with Version 1.2 (rather than 2.x) of the PSS PP because the evaluation of the TOE was at an advanced stage when Version 2.0 was issued, and it was impractical to change the ST at that point (and thereby negate the benefit of the EAL4 evaluation activities that had been completed).

4 Security Problem Definition

4.1 Threats

76 The asset to be protected by the TOE is the information transiting the TOE (i.e. the user data). The threat agent is considered to be a person with physical access to the TOE (who is expected to possess “average” expertise, few resources, and moderate motivation).

77 [PP] also identifies “failure of the TOE or *peripherals*” as a possible threat agent, but does not elaborate on that statement. In this ST, failure of the TOE or of peripherals attached to the TOE is considered to be a topic for the evaluation’s vulnerability analysis, rather than a threat agent.

78 The identified threats to the asset are listed below; they are from [PP], with clarifications (e.g. from [PD093]).

79 **T.BYPASS** The TOE may be bypassed, circumventing nominal *switch* functionality, because it has not been installed and managed in accordance with the manufacturer’s instructions.

80 **T.INSTALL** The TOE may be delivered and installed in a manner which violates the security policy.

81 **T.LOGICAL** The functionality of the TOE may be changed by reprogramming in such a way as to violate the security policy.

82 **T.PHYSICAL** A physical attack on the TOE may violate the security policy.

83 **T.RESIDUAL** *Residual data* may be transferred between *port groups* with different *ids*.

84 **T.SPOOF** Via intentional or unintentional actions, a *user* may think the set of *shared peripherals* are *connected* to one *computer* when in fact they are connected to a different one. This does not mean that the TOE has to counter this threat by being able to determine what is connected to it; neither does it mean that this threat is to be addressed by the operational environment (despite what is stated in [PD093]).

85 **T.STATE** *State information* may be transferred to a *port group* with an *id* other than the selected one.

86 **T.TRANSFER** A *connection*, via the TOE, between *computers* may allow information transfer. In other words, information may flow, via the TOE, between *switched computers*.

4.2 Organisational Security Policies

87 No Organisational Security Policies are specified for the TOE.

4.3 Assumptions

88 Assumptions made on the operational environment are listed below; they are from [PP], with clarifications (e.g. from [PD093]).

89 **A.ACCESS** An *authorised user* possesses the necessary privileges to access the information transferred via the TOE. All *users* are *authorised users*.

90 **A.MANAGE** The TOE is received, installed and managed in accordance with the manufacturer's directions.

91 **A.NOEVIL** Each *authorised user* is non-hostile and follows all TOE usage guidance.

92 **A.PHYSICAL** The TOE is physically secure.

93 **A.SCENARIO** Vulnerabilities associated with *shared peripherals* or *switched computers*, or their *connection* to the TOE, are a concern of the application scenario and not of the TOE. (In other words, any such vulnerabilities are outside the scope of the TOE and of this ST.)

94 Recall that, to a large extent, the "unidirectional flow of keyboard and mouse data" security feature of the TOE renders the A.SCENARIO assumption superfluous (as explained in Subsection 2.4.5).

95 Note that the following assumptions listed in [PP] are not included in this ST:

a) A.EMISSION ("The TOE meets the appropriate national requirements ... for conducted/radiated electromagnetic emissions"), because assumptions should be made on the operational environment, not on the TOE. See Subsection 2.4.4 for a brief discussion of emissions, including TEMPEST issues;

b) A.ISOLATE ("Only the selected *computer's* video channel will be visible on the shared MONITOR"), because - as stated in PD-0093 - this is not appropriate wording for an assumption. (The intent of this "assumption" is subsumed by the TOE objective O.SWITCH, see Section 5.1 below.)

96 Note that omission of the above assumptions does not weaken this ST's claim of conformance to [PP] - because the design of the TOE does satisfy them - but rather ensures that this ST is conformant with [CC].

5 Security Objectives

5.1 Security Objectives for the TOE

97 The TOE's security objectives are listed below; they are from [PP], with clarifications (e.g. from [PD093]) and editorial changes.

98 **O.CONF** The TOE shall not violate the confidentiality of information which it processes. Information generated within any given *connection* between *shared peripherals* and a *switched computer* shall not be accessible within any other *shared peripherals - switched computer connection*.

99 **O.CONNECT** No information shall be shared between *switched computers* via the TOE. This includes *state information*, if such is maintained within the TOE.

100 **O.INDICATE** The *authorised user* shall receive an unambiguous indication of which *switched computer* has been selected.

101 **O.SELECT** An explicit action by the *authorised user* shall be used to select the *switched computer* to which the *shared peripherals* are *connected*.

102 **O.SWITCH** All *devices* in a *shared peripherals port group* shall be *connected* to at most one *switched computer* at any given time.

103 The following PP objectives are not included in the above list, because each is not applicable to the TOE, or is a design constraint (discussed further in Section 8.4):

a) O.INVOKE ("Upon switch selection, the TOE is invoked"); this objective "relates to a TOE which can be considered to be distinct from a physical switch" (see [PD093]), which is not the case here (see Subsection 2.4.2);

b) O.NOPROG ("Logic contained within the TOE shall be protected against unauthorized modification. Embedded logic must not be stored in programmable or re-programmable components"); this is a design constraint;

c) O.ROM ("TOE software/firmware shall be protected against unauthorized modification. Embedded software must be contained in mask-programmed or one-time-programmable read-only memory permanently attached (non-socketed) to a circuit assembly"); this is a design constraint.

104 Note that [PP], Table 2 (Mapping of SFRs to Objectives) maps the above three objectives solely to ADV_ARC.1, which is a SAR, not an SFR. ([CC] Part 3, Para 389 requires that "all security objectives for the TOE are effectively addressed by the SFRs".) Hence, omission of the above objectives does not weaken this ST's claim of conformance to [PP] - because the design of the TOE does satisfy O.NOPROG and O.ROM - but rather ensures that this ST is conformant with [CC].

5.2 Security Objectives for the Operational Environment

105 The security objectives for the operational environment are listed below; they are from [PP], with clarifications (e.g. from [PD093]) and editorial changes.

106 **OE.ACCESS** The operational environment (procedures) shall ensure that all *users* are *authorised users*, i.e. they possess the necessary privileges to access the information transferred via the TOE.

107 **OE.MANAGE** The operational environment shall include procedures (e.g. re staff vetting and training) to ensure that, as far as is reasonably possible, the TOE is received, installed and managed in accordance with the manufacturer's directions.

108 **OE.NOEVIL** The operational environment shall include procedures (e.g. re staff vetting and training) to ensure that, as far as is reasonably possible, each *authorised user* is non-hostile and follows all TOE usage guidance.

109 **OE.PHYSICAL** The operational environment shall include measures to ensure that the TOE is physically secure.

110 **OE.SCENARIO** The operational environment (including the validation/certification report for the TOE) shall make consumers of the TOE aware that vulnerabilities associated with *shared peripherals* or *switched computers*, or their *connection* to the TOE, are a concern of the application scenario and not of the TOE. (In other words, any such vulnerabilities are outside the scope of the TOE.)

111 Note that the following environmental objectives listed in [PP] are not part of this ST (because the corresponding assumptions are not part of this ST, for the reasons explained in Section 4.3):

a) OE.EMISSION ("The TOE shall meet the appropriate national requirements ... for conducted/radiated electromagnetic emissions. ...");

b) OE.ISOLATE ("Only the selected *computer's* video channel shall be visible on the shared MONITOR").

112 Note that omission of the above objectives does not weaken this ST's claim of conformance to [PP] - as explained in Section 4.3 - but rather ensures that this ST is conformant with [CC].

5.3 Rationale

113 The following table traces objectives to threats and assumptions. The entries in the "Notes" column justify why the objectives counter the threats.

114 Note that Table 2 differs somewhat from the corresponding table in [PP], which is criticised to some extent in [PD093]. Despite PD-0093 concluding that "The rationale section currently is sufficient" (sic), this ST claims that Table 2 is a more convincing rationale than that given in the PP.

Table 2 Tracing of objectives to threats and assumptions

Threat/Assumption	Objective(s)	Notes
T.BYPASS	OE.MANAGE, OE.NOEVIL	These objectives directly counter the threat.
T.INSTALL	OE.MANAGE, OE.NOEVIL	These objectives directly counter the threat.
T.LOGICAL	OE.MANAGE, OE.NOEVIL, OE.PHYSICAL	This combination of objectives counters the threat by diminishing the risk that a threat agent could or would physically tamper with the TOE and alter its functionality. The design of the TOE also diminishes this threat, as discussed in Section 8.4.
T.PHYSICAL	OE.PHYSICAL	This objective directly counters the threat.

Threat/Assumption	Objective(s)	Notes
T.RESIDUAL	O.CONF, O.CONNECT, O.SWITCH	O.CONF and O.CONNECT directly counter the threat (because *residual data* is encompassed by the term “information” used in their definition); O.SWITCH diminishes the threat because the risk of information being transferred between *port groups* with different *ids* is increased if a *shared peripheral* is connected to more than one *switched computer* at any given time.
T.SPOOF	O.INDICATE, O.SELECT	These objectives directly counter the threat.
T.STATE	O.CONF, O.CONNECT, O.SWITCH	O.CONF and O.CONNECT directly counter the threat (because *state information* is encompassed by the term “information” used in their definition); O.SWITCH diminishes the threat because the risk of information being transferred between *port groups* with different *ids* is increased if a *shared peripheral* is connected to more than one *switched computer* at any given time.
T.TRANSFER	O.CONF, O.CONNECT, O.SWITCH	O.CONF and O.CONNECT directly counter the threat; O.SWITCH diminishes the threat because the risk of information being transferred between *switched computers*, via the TOE, is increased if a *shared peripheral* is connected to more than one *switched computer* at any given time.
A.ACCESS	OE.ACCESS	This objective directly upholds the assumption.
A.MANAGE	OE.MANAGE	This objective directly upholds the assumption.
A.NOEVIL	OE.NOEVIL	This objective directly upholds the assumption.
A.PHYSICAL	OE.PHYSICAL	This objective directly upholds the assumption.
A.SCENARIO	OE.SCENARIO	This objective directly upholds the assumption.

115 By inspection of Table 2, it can be seen that:

a) Each security objective identified earlier traces to at least one threat or assumption;

b) Each threat or assumption identified earlier has at least one security objective tracing to it;

c) No objective for the TOE traces back to an assumption;

d) All threats will be adequately countered (i.e. removed, diminished or mitigated), and all assumptions upheld, if all the objectives are achieved.

6 Extended Components Definition

6.1 Introduction

116 [PP] specifies an extended component, identified as EXT_VIR.1, which this ST defines below.

117 Note that the PP words “A visual method ... shall be provided” in its definition of EXT_VIR.1.1 are amended in this ST to read “The TSF shall provide a visual means ...”.

6.2 The EXT_VIR.1 Component

118 The EXT (EXTended requirements) class contains a single VIR (Visual Indication Rule) family which contains a single component EXT_VIR.1: the TOE shall provide some visual feedback to the user to indicate which computer is currently connected to the TOE.

119 There are no management activities or auditable actions foreseen for this component.

120 **EXT_VIR.1 Visual feedback provided**

Hierarchical to: No other components.

Dependencies: No dependencies.

EXT_VIR.1.1 The TSF shall provide a visual means of indicating which *computer* is *connected* to the set of *shared peripherals*.

Application note: The indication shall persist for the duration of the *connection*.

7 Security Requirements

7.1 Security Functional Requirements

7.1.1 Introduction and the Data Separation SFP

121 The SFRs for the TOE are specified in the following subsections. The components are drawn from the CC Part 2 families FDP_ETC, FDP_IFF, FDP_ITC, FMT_MSA and FMT_SMF; and from the EXT_VIR family introduced in the preceding section.

122 Words which appear in square brackets are the result of permitted operations on components.

123 The information flow control SFP (Security Function Policy) that is assigned to some components is named in [PP] as the **Data Separation SFP**, and is defined as follows:

The TOE shall allow *peripheral data* to be transferred only between *port groups* with the same *id*.

124 Note that it follows from Section 1.3 above that "the user data's associated security attributes" equates to "*attributes*", and "the information controlled under the (Data Separation) SFP" equates to "*objects*".

7.1.2 User data protection (FDP)

125 **FDP_ETC.1** (Export of user data without security attributes)

Dependencies: FDP_ACC.1 (Subset access control) or FDP_IFC.1 (Subset information flow control).

FDP_ETC.1.1 The TSF shall enforce the [Data Separation SFP] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.1.2 The TSF shall export the user data without the user data's associated security attributes.

126 **FDP_IFC.1** (Subset information flow control)

Dependencies: FDP_IFF.1 (Simple security attributes).

FDP_IFC.1.1 The TSF shall enforce the [Data Separation SFP] on [the set of *port groups*, and the bi-directional flow of *peripheral data* between the *shared peripherals* and the *switched computers*].

127 **FDP_IFF.1** (Simple security attributes)

Dependencies: FDP_IFC.1 (Subset information flow control) and FMT_MSA.3 (Static attribute initialisation).

FDP_IFF.1.1 The TSF shall enforce the [Data Separation SFP] based on the following types of subject and information security attributes: [*port groups* (*subjects*) and *peripheral data* (*objects*); and *port group ids* (*attributes*)].

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: [Switching rule: *peripheral data* can flow to a *port group* with a given *id* only if it was received from a *port group* with the same *id*].

FDP_IFF.1.3 The TSF shall enforce the [none, i.e. no additional information flow control SFP rules].

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: [none].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [none].

128 **FDP_ITC.1** (Import of user data without security attributes)

Dependencies: (FDP_ACC.1 or FDP_IFC.1) and FMT_MSA.3.

FDP_ITC.1.1 The TSF shall enforce the [Data Separation SFP] when importing user data, controlled under the SFP, from outside the TOE.

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

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [none].

7.1.3 Security management (FMT)

129 **FMT_MSA.1** (Management of security attributes)

Dependencies: (FDP_ACC.1 or FDP_IFC.1]), FMT_SMR.1 (Security roles) and FMT_SMF.1 (Specification of management functions).

FMT_MSA.1.1 The TSF shall enforce the [Data Separation SFP] to restrict the ability to [modify] the security attributes [*port group ids*] to [the *user*].

130 [PP] includes the following application note:

An *authorised user* shall perform an explicit action to select the *computer* to which the shared set of *peripherals* is *connected*.

131 **FMT_MSA.3** (Static attribute initialisation)

Dependencies: FDP_MSA.1 and FMT_SMR.1.

FMT_MSA.3.1 The TSF shall enforce the [Data Separation SFP] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [none, i.e. no identified role] to specify alternative initial values to override the default values when an object or information is created.

132 [PP] includes the following application note re FMT_MSA.3.1:

On start-up, one and only one attached *computer* shall be selected.

133 Application note re FMT_MSA.3.2:

This ST (following [PP]) does not include the FMT_SMR.1 component (see Subsection 7.1.5). Hence, the *user* is not a role in the CC sense; however, the *user* is not exempt from the FMT_MSA.3.2 prohibition (on specifying initial values).

134 **FMT_SMF.1** (Specification of management functions)

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [selection via an explicit action by an *authorised user* of the *computer* to which the shared set of *peripherals* is *connected*].

135 Note that [PP] lists “none” in FMT_SMF.1.1, which appears to be inconsistent with the specification of FMT_MSA.1.1 (and also contravenes [CC] Part 1 Paragraph 246b re the use of “none” in assignment operations on SFRs).

7.1.4 Extended requirements (EXT)

136 **EXT_VIR.1** (Visual feedback provided)

Dependencies: No dependencies

EXT_VIR.1.1 The TSF shall provide a visual means of indicating which *computer* is *connected* to the set of *shared peripherals*.

Application note:

The indication shall persist for the duration of the *connection*.

7.1.5 Dependencies, management and audit

137 It can be seen by inspection that, with one exception, the dependencies of the above SFRs are satisfied. The exception is the absence of FMT_SMR.1 (Security roles), which is a dependency of FMT_MSA.1 (Management of security attributes) and FMT_MSA.3 (Static attribute initialisation).

138 The justification for this absence, as stated in [PP], is as follows:

The TOE is not required to associate *users* with roles; hence, there is only one “role”, that of *user*. This deleted requirement [i.e. omitted SFR] ... allows the TOE to operate normally in the absence of any formal roles.

139 After due consideration, and in the absence of any FAU_GEN (Security audit data generation) components for the TOE, there are (apart from MSA.1.1) no management activities or auditable actions specified in connection with the above SFRs.

7.2 Security Functional Requirements Rationale

140 Table 3 (overleaf) traces the above SFRs to the security objectives for the TOE. The entries in the “Notes” column justify why the SFRs meet the objectives.

141 Note that Table 3 differs somewhat from the corresponding table in [PP], for similar reasons to those stated re Table 2 (see Paragraph 114 above).

Table 3 Tracing of SFRs to objectives for the TOE

Objective	SFR(s)	Notes
O.CONF	FDP_ETC.1, FDP_IFC.1, FDP_IFF.1, FDP_ITC.1	These SFRs directly implement the objective, because they all enforce the Data Separation SFP. Also, FDP_ETC.1.2 and FDP_ITC.1.2 ensure that the TOE's security attributes are wholly under the control of the TOE.
O.CONNECT	FDP_ETC.1, FDP_IFC.1, FDP_IFF.1, FDP_ITC.1	These SFRs directly implement the objective, because they all enforce the Data Separation SFP. Also, FDP_ETC.1.2 and FDP_ITC.1.2 ensure that the TOE's security attributes are wholly under the control of the TOE.
O.INDICATE	EXT_VIR.1	This SFR directly implements the objective.
O.SELECT	FMT_MSA.1, FMT_SMF.1	The application notes for these SFRs state that these SFRs directly implement the objective.
O.SWITCH	FDP_IFC.1, FDP_IFF.1, FMT_MSA.3, FMT_SMF.1	These SFRs implement the objective, because they all enforce the Data Separation SFP. (See the definition of *port group (id)*; the crucial points are that: Each *switched computer port group* has a **unique** logical *id*; The *shared peripherals port group* also has an *id* which at any given time **is the same as** that of the *switched computer port group* that is currently *connected* to the TOE. In other words, if the SFP is enforced correctly, then by definition the *shared peripherals* can be *connected* to only one *switched computer* at any given time.) See also the application notes re FMT_MSA.3 and FMT_SMF.1, which support a robust implementation of the objective.

142 By inspection of Table 3, it can be seen that:

a) Each SFR specified earlier traces to at least one objective for the TOE;

b) Each objective for the TOE identified earlier has at least one SFR tracing to it;

c) All objectives for the TOE will be achieved (to the level of assurance specified by the following SARs) if all the SFRs are satisfied (to the specified assurance level).

7.3 Security Assurance Requirements

143 The SARs for the TOE are those specified in [PP], i.e. the TOE is to be assured to an EAL4 (augmented) level.

144 The assurance components that are relevant to the TOE itself are listed in Table 4 (overleaf), together with a summary of the "developer actions", i.e. a summary of what the TOE's developer (Adder Technology Ltd) has to provide to the evaluators. The components that augment EAL4 are indicated in bold.

145 In addition, the ST (this document) is to be evaluated against the “ASE_” components for EAL4 as listed in [CC], Part 3, Table 5.

146 Further details of the assurance components are given in [CC] Part 3. The “evaluator actions” for each component are elaborated in [CEM], which details, for example, how the evaluators should process what the developer provides to them.

Table 4 Assurance requirements

[CC] assurance component	Developer to provide	Notes
Development		
ADV_ARC.1	Security architecture description of the TSF (TOE Security Functionality)	The TOE design shall prevent the TSF being bypassed or tampered with by untrusted active entities. (In practice the ARC description will probably be a separate section or annex in the design description - see ADV_TDS.3).
ADV_FSP.4	Complete functional specification of the TSF	Include a tracing to the SFRs specified in the ST.
ADV_TDS.3	Design of the TOE (basic modular design, i.e. describe the design in terms of subsystems and modules)	Include a mapping from the TSFIs (TSF Interfaces, see ADV_FSP.4) through the subsystems to the modules (i.e. to the level of design before the implementation, see ADV_IMP.1).
ADV_IMP.1	Implementation representation for the entire TSF, e.g. schematic drawings (of hardware components), source code (as programmed into firmware components)	Include a mapping between the TOE design description (ADV_TDS.3) and the sample of the implementation representation (i.e. the TSF - which is that part of the TOE which implements the SFRs specified in the ST).
Guidance Documents		
AGD_OPE.1	Operational user guidance	Describes how to use the TOE in a secure manner, both for normal (unprivileged) users and for administrators (who are privileged to configure the TOE’s security functions - but this may not be applicable for this evaluation).
AGD_PRE.1	The TOE (i.e. an actual switch), including its preparative procedures	Procedures describe how to accept (i.e. receive), install and set-up the TOE in a secure manner. (Evaluators’ applying these procedures to the TOE can be done at the same time as penetration testing - see below, AVA_VAN.3).
(Intentionally blank)		

[CC] assurance component	Developer to provide	Notes
Life Cycle Support		
ALC_CMC.4	The TOE (i.e. an actual switch) and a reference for it; CM (configuration management) documentation and evidence that a CM system is being used	Component is entitled “Production support, acceptance procedures and automation”, i.e. the CM system needs to support TOE production by automated means (e.g. a tool that tracks software source code versions).
ALC_CMS.4	Configuration list for the TOE	List to include problem tracking CM coverage (i.e. security flaw reports and resolution status).
ALC_DEL.1	Delivery procedures	Include evidence that the developer follows the documented procedures.
ALC_DVS.1	Identification of security measures	Describe all the security measures (e.g. physical, procedural) present in the TOE’s development environment to protect the integrity (and the confidentiality, if necessary) of the TOE and its design and implementation.
ALC_FLR.2	Flaw (remediation) reporting procedures	Include guidance addressed to TOE users.
ALC_LCD.1	(Description of) developer defined life-cycle model	Covering both development and maintenance of the TOE.
ALC_TAT.1	(Details of) well-defined development tools	Identify each TOE development tool (e.g. CAD tool, programming language) and document its selected options (e.g. compiler options).
Tests		
ATE_COV.2	Analysis of test coverage	Analysis to show that developer’s tests cover all the TSFIs (see ADV_FSP.4).
ATE_DPT.2	Analysis of the depth of testing (security enforcing modules)	Analysis to show that developer’s tests cover all TSF subsystems and SFR-enforcing modules(see ADV_TDS.3).
ATE_FUN.1	Functional testing (of the TSF)	Developer’s test results (test plans and specifications, expected and actual results).
ATE_IND.2	The TOE (i.e. an actual switch) for independent testing, plus technical support and resources during the testing that are equivalent to those used in the developer’s functional testing of the TSF	Independent testing - sample, i.e. evaluators repeat a sample of the developer’s tests; the evaluators also conduct their own additional functional tests. Can be done at the same time as penetration testing - see AVA_VAN.3.
Vulnerability Assessment		
AVA_VAN.3	The TOE (i.e. an actual switch) for penetration testing, plus technical support and resources during the testing (see ATE_IND.2)	Evaluators carry out a focused vulnerability analysis (based on the ADV and AGD evidence in particular), then undertake penetration testing of the TOE.

7.4 Security Assurance Requirements Rationale

147 The combination of required assurance components (i.e. EAL4 augmented by ALC_FLR.2 and ATE_DPT.2) is that specified in [PP]. (Note that the ATE_DPT assurance component for EAL4 is now, in v3.1R3 of the CC, ATE_DPT.1.)

148 The CC characterises an EAL4-assured IT product as one that has been methodically designed, tested and reviewed; such assurance in a product is generally considered to be adequate unless the product is to be used as part of an IT system (or “application”) that handles very sensitive information, or is liable to be attacked by highly sophisticated threat agents.

7.5 Conclusion

149 The preceding rationales in this ST demonstrate that, if all the security requirements are satisfied, and all security objectives for the operational environment are achieved, then there exists assurance (to the EAL4 augmented level) that the TOE solves the security problem defined in Chapter 4.

8 TOE Summary Specification

8.1 Introduction

150 The next two sections summarise how each of the two switches identified in Subsection 2.4.1 (as being representative of the set of TOEs) satisfies all the SFRs specified in this ST.

151 General constraints on the design of the TOE (resulting from security considerations) are discussed in Section 8.4.

152 For each of the twelve switches in the set of TOEs, further details of its components and guidance documentation, and of the peripherals and computers that may be attached to it, are given in Chapter 9.

8.2 AdderView Secure DVI 4 port Switch (AViewD-4)

8.2.1 Switch Architecture Outline

153 Figure 2 (overleaf) depicts the switch's internal security architecture in terms of "controller" components (each constructed from hardware/firmware sub-components and circuitry). To avoid cluttering the diagram, just one computer controller is shown, but the other three computer controllers are identical to it, both in terms of their constituent sub-components and connections to other controllers.

154 The solid arrows indicate the flow of peripheral data (including peripheral control signals), and the dotted arrows indicate the flow of switch control signals. "W, X, Y, Z" are explained in the following paragraphs; note that in reality these sub-components are not inter-connected.

155 When the user powers up the switch the switch controller ensures that one computer only is connected to the shared peripherals. When the user presses a selection button the switch controller signals the USB host controller, the audio controller and the video controller to instigate a channel change (to the selected computer port); the switch controller also toggles the relevant LEDs on the switch's front panel. The USB host controller erases its entire RAM at every channel change.

156 The USB host controller and the computer controller implement a unidirectional flow of keyboard and mouse data as follows. When a USB peripheral sends a peripheral control signal to the USB host controller (e.g. when the keyboard's caps lock key is pressed) the controller responds as if it was a computer (e.g. it signals the keyboard to illuminate the caps light) before passing the peripheral's signal on to the computer via circuitry "Z" in the computer controller. The actual computer's response is also handled by "Z", which does not pass it back to the USB host controller.

157 The computer controller also has a dedicated DDC bus connecting it to the video controller. This bus carries EDID data from the video controller to the computer controller's EDID memory emulation circuitry "X" (when the switch is powered up). Video output from the computer is sent to the video peripheral via the computer controller's "Y" circuitry and the video controller.

158 Audio output from the computer is sent to the audio peripheral (i.e. to powered analogue audio speakers) via the computer controller's "W" circuitry and the audio controller.

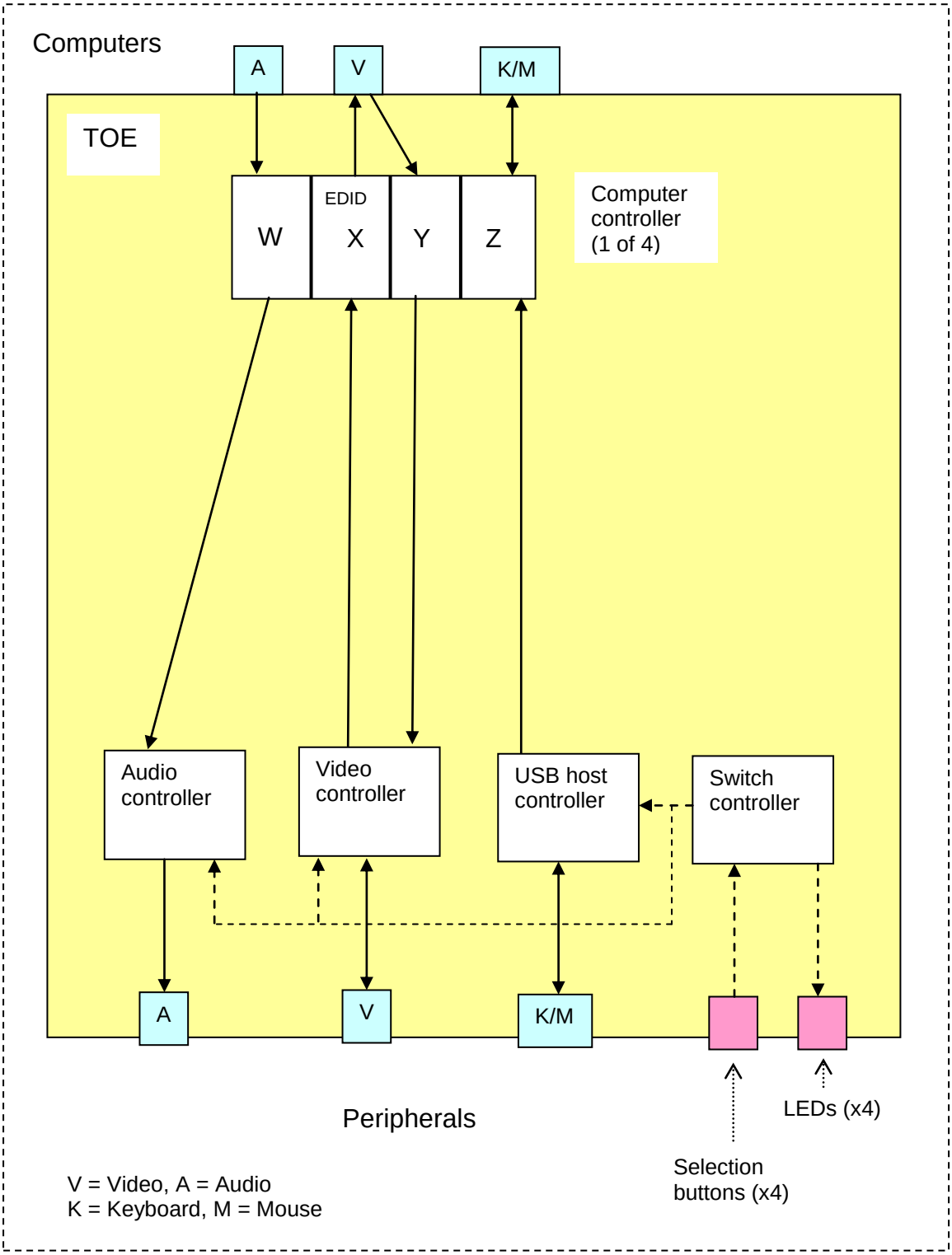

Figure 2 AViewD-4 architecture outline

159 The above description covers the switch's main security features that were introduced in Subsection 2.4.3, and also underpins Table 5 below.

8.2.2 Implementation of Security Functional Requirements

160 The following table indicates how - in terms of the preceding subsection's outline architecture description - the switch meets each of the SFRs specified in Section 7.1.

Table 5 AViewD-4 implementation of SFRs

SFR(s)	Component(s)	Additional Notes
FDP_ETC.1, FDP_ITC.1	Computer controller, USB host controller, Audio controller, Video controller	The only security attribute associated with user data is the id of the channel which was used to export or import it. This id is purely internal to the switch; the computers and peripherals attached to the switch are completely unaware of it.
FDP_IFC.1, FDP_IFF.1	Switch controller, USB host controller, Audio controller, Video controller	There is one computer controller per computer port; none is linked (directly, i.e. not via the USB controller or video controller) to another computer controller.
FMT_MSA.1, FMT_SMF.1	Switch controller	
FMT_MSA.3	Switch controller	
EXT_VIR.1	Switch controller	For each computer port, there is exactly one LED associated with it; each LED is illuminated only when its associated computer port is selected; each LED is colour-coded, i.e. is coloured differently from each of the other LEDs.

8.3 AdderView Secure VGA 4 port Switch with Card Reader (AViewC-4)

8.3.1 Switch Architecture Outline

161 Figure 3 (overleaf) depicts the switch's internal security architecture in terms of "controller" components (following the same approach and conventions used for Figure 2). In essence, the AViewC-4 switch architecture is the same as the AViewD-4 switch architecture, with the addition of a smartcard controller, which handles the USB smartcard reader device (or combined reader and keyboard device) attached to the switch, an additional sub-component in the computer controller to handle the smartcard-related interface to the computer (indicated by "ZS" in Figure 3), and the removal of the audio-handling capability.

162 The smartcard controller functions in a similar manner to the USB host controller; however, if it is handling a combined reader and keyboard device then it passes the keyboard peripheral data to the computer controller via the USB host controller (and receives power from the USB host controller, although this is not shown explicitly in Figure 3).

163 The switch also includes an anti-subversion subsystem, which implements the active authentication verification and tamper detection features outlined in Subsection 2.4.4 above. These features support all the SFRs specified in Section 7.1, but do not directly implement any of them; further description of the subsystem is outside the scope of this ST document.

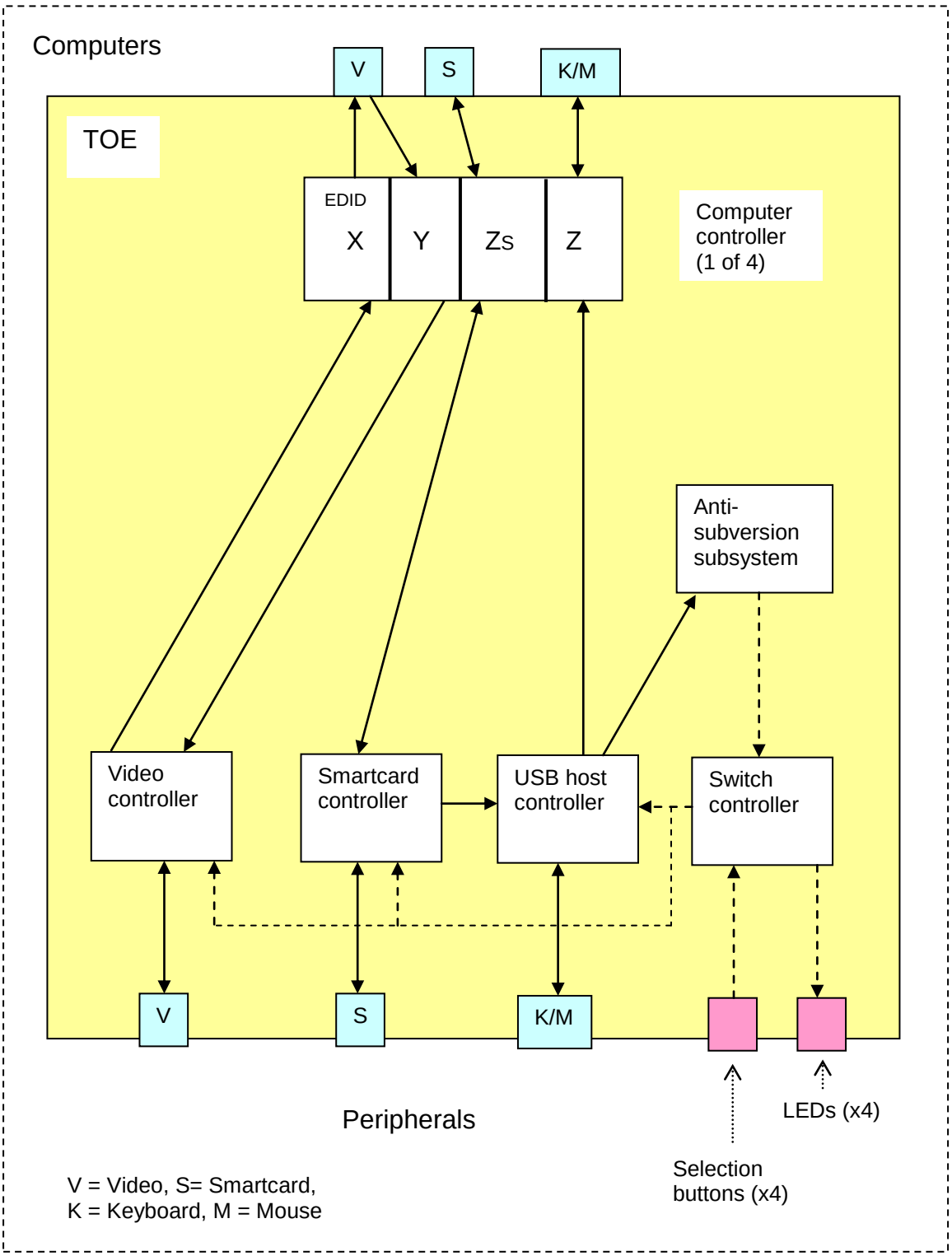

Figure 3 AViewC-4 architecture outline

164 The above description covers the switch's main security features that were introduced in Subsection 2.4.3, and also underpins Table 6 below.

8.3.2 Implementation of Security Functional Requirements

165 The following table indicates how - in terms of the preceding subsection's outline architecture description - the switch meets each of the SFRs specified in Section 7.1.

Table 6 AViewC-4 implementation of SFRs

SFR(s)	Component(s)	Additional Notes
FDP_ETC.1, FDP_ITC.1	Computer controller, USB host controller, Video controller, Smartcard controller	The only security attribute associated with user data is the id of the channel which was used to export or import it. This id is purely internal to the switch; the computers and peripherals attached to the switch are completely unaware of it.
FDP_IFC.1, FDP_IFF.1	Switch controller, USB host controller, Video controller, Smartcard controller	There is one computer controller per computer port; none is linked (directly, i.e. not via the USB controller or video controller) to another computer controller.
FMT_MSA.1, FMT_SMF.1	Switch controller	
FMT_MSA.3	Switch controller	
EXT_VIR.1	Switch controller	For each computer port, there is exactly one LED associated with it; each LED is illuminated only when its associated computer port is selected; each LED is colour-coded, i.e. is coloured differently from each of the other LEDs.

8.4 Design Constraints and Further Threat Considerations

166 As stated in Section 5.1, [PP] includes two "TOE objectives" which are, in effect design constraints, namely:

a) **O.NOPROG** Logic contained within the TOE shall be protected against unauthorized modification. Embedded logic must not be stored in programmable or re-programmable components;

b) **O.ROM** TOE software/firmware shall be protected against unauthorized modification. Embedded software must be contained in mask-programmed or one-time-programmable read-only memory permanently attached (non-socketed) to a circuit assembly.

167 The TOE's electronic components are either hardware or firmware components. The hardware components are standard items (e.g. resistors) that are incapable of being programmed; the firmware components are standard items (e.g. microprocessors) that include no programmable memory capability apart from one-time-programmable read-only memory which is permanently attached (non-socketed) to a PCB. The TOE does not contain any programmable logic arrays, nor does it contain any software apart from the code which is one-time-programmed into its firmware as the last stage of its manufacturing process (prior to final testing and packaging).

168 [PD093] states that O.NOPROG “applies to TOEs that use programmable logic arrays or hardware-only TOEs; O.ROM applies to TOEs with microprocessors.” Hence, the TOE satisfies O.ROM and trivially satisfies O.NOPROG (which is not applicable to this TOE).

169 The above shows how a design constraint (reducing the available choices for the TOE’s components) contributes to countering a threat (T.LOGICAL). Further design constraints have been identified by the TOE designers during their consideration of how best to counter T.TRANSFER (the threat of information being transferred between computers attached to the TOE).

170 Describing these constraints is beyond the scope of this ST (which is not intended to be a detailed design specification), but as an indication of their extent the following list gives what may be called “some of the variations on the T.TRANSFER theme” that the TOE designers have taken into account:

a) Firmware “holes” or malfunction;
b) Common storage;
c) Timing analysis;
d) Electrical crosstalk;
e) Forced malfunction;
f) User error;
g) Faulty installation;
h) Faulty electronics;
i) Shorting or loading the power supply;
j) Faulty or subverted cabling;
k) Subverted switch;
l) Electromagnetic emissions snooping;
m) Light emissions snooping;
n) Power surges (e.g. lightning strikes).

171 See also Subsection 2.4.4 above.

9 TOE Component Details

172 For each of the twelve switches in the set of TOEs, further details of its components and guidance documentation, and of the peripherals and computers that may be attached to it, are given on the Black Box and Adder web sites, see http://www.blackbox.com/ and http://www.adder.com/.